Server & Application Monitor

Version 6.8
© 2018 SolarWinds Worldwide, LLC. All rights reserved.

This document may not be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the prior written consent of SolarWinds. All right, title, and interest in and to the software, services, and documentation are and shall remain the exclusive property of SolarWinds, its affiliates, and/or its respective licensors.

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS, OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON THE DOCUMENTATION, INCLUDING WITHOUT LIMITATION NONINFRINGEMENT, ACCURACY, COMPLETENESS, OR USEFULNESS OF ANY INFORMATION CONTAINED HEREIN. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS, NOR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY, EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

The SolarWinds, SolarWinds & Design, Orion, and THWACK trademarks are the exclusive property of SolarWinds Worldwide, LLC or its affiliates, are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other SolarWinds trademarks, service marks, and logos may be common law marks or are registered or pending registration. All other trademarks mentioned herein are used for identification purposes only and are trademarks of (and may be registered trademarks) of their respective companies.
## Table of Contents

*Welcome to the SAM Template Reference* ................................................................. 24

Learn more .................................................................................................................. 26

Linux/Unix system configurations for component monitors ....................................... 26

  Apache configurations ............................................................................................. 27
  Tomcat configurations ............................................................................................. 28
  JMX ......................................................................................................................... 30
  Squid ....................................................................................................................... 30
  Nagios ....................................................................................................................... 31
  ODBC configurations .............................................................................................. 31
  PostgreSQL configurations ....................................................................................... 32
  MySQL configurations .............................................................................................. 33
  IBM DB2 with ODBC configurations ....................................................................... 35
    Linux-based computers ......................................................................................... 35
    Configure DB2 on AIX devices ............................................................................. 37

**AIX templates** ................................................................................................... 40

  AIX template .......................................................................................................... 41
    Monitored Components ......................................................................................... 41
  AIX LPD template .................................................................................................. 44
    Monitored Components ......................................................................................... 44
  Nagios Linux File & Directory Count Script ........................................................... 44
    Monitored Components ......................................................................................... 45
    Field Descriptions ............................................................................................... 46

**Apache templates** ............................................................................................ 49

  Apache template .................................................................................................... 50
    Monitored Components ......................................................................................... 51
  Apache (Windows) template .................................................................................... 53
    Monitored Components ......................................................................................... 54

**APC PowerChute Agent (Windows)** ................................................................. 55
Monitored Components ................................................................. 55

AppInsight .................................................................................. 59
AppInsight for Active Directory ..................................................... 59
  Monitored components ............................................................. 59
AppInsight for Exchange ............................................................... 67
  Monitored Components ............................................................. 67
  Performance counters ............................................................... 83
    Category: \\MSExchange Store Interface\(\_Total\)\ ......................................................... 83
    Category: \\MSExchange RpcClientAccess\ ................................................................. 83
    Category: \\MSExchange Database\(Information Store)\ ............................................. 83
    Category: \\MSExchange Replication\(\_total\)\ ......................................................... 83
    Category: \\MSExchange Calendar Attendant\ ....................................................... 83
    Category: \\MSExchange Resource Booking ......................................................... 84
    Category: \\MSExchange Database => instances\(information store/\_Total\)\ ......................... 84
AppInsight for IIS ....................................................................... 84
  Monitored Components ............................................................. 84
AppInsight for SQL .................................................................. 94
  Monitored Components ............................................................. 94

Barracuda Spam and Virus Firewall .............................................. 120
  Monitored Components ........................................................... 120

Bind ......................................................................................... 123
  Bind (Linux - v9.5 and earlier) ..................................................... 124
    Monitored Components ............................................................ 124
  Bind (Linux - v9.6 and higher) .................................................... 126
    Monitored Components ............................................................ 126

BizTalk .................................................................................... 132
  BizTalk Server 2010-2013 Adapters Performance Counters ................ 132
    Monitored Components ............................................................ 132
  BizTalk Server 2010-2013 Availability Status ..................................... 135
    Monitored Components ............................................................ 135
BizTalk Server 2010-2013 Host Throttling Performance Counters ................................................. 137
Monitored Components .............................................................................................................. 137
BizTalk Server 2010-2013 Message Box and Orchestrations Performance Counters .................. 143
Monitored Components .............................................................................................................. 143
Blackberry ............................................................................................................................... 147
Blackberry Delivery Confirmation .............................................................................................. 148
Customizing Script Variables ...................................................................................................... 148
Monitored Components .............................................................................................................. 149
Blackberry Enterprise Server ..................................................................................................... 150
Monitored Components .............................................................................................................. 150
Blackberry Enterprise Server 10 Services (Windows) ................................................................. 151
Monitored Components .............................................................................................................. 151
Blackberry Enterprise Server 10 Statistic (SNMP) .................................................................... 154
Monitored Components .............................................................................................................. 154
Blackberry Enterprise Server 12 Services (Windows) ................................................................. 158
Monitored Components .............................................................................................................. 158
Blackberry Enterprise Server 12 Statistics (SNMP) .................................................................... 161
Monitored Components .............................................................................................................. 161
Cisco ......................................................................................................................................... 170
Cisco CallManager ...................................................................................................................... 171
Monitored Components .............................................................................................................. 171
CiscoSecure ACS (via SNMP) ...................................................................................................... 173
Monitored Components .............................................................................................................. 173
CiscoWorks LAN Management Solution .................................................................................... 174
Monitored Components .............................................................................................................. 174
Citrix templates .......................................................................................................................... 179
Citrix XenApp 5.0 Core WMI Counters ....................................................................................... 180
Monitored Components .............................................................................................................. 180
Citrix XenApp 5.0 ICA WMI Session Counters .......................................................................... 184
Monitored Components .............................................................................................................. 184
Citrix XenApp 5.0 Presentation Server WMI Counters .................................................. 189
  Monitored Components ................................................................. 189
Citrix XenApp 5.0 Services ............................................................... 193
  Monitored Components ................................................................. 193
Citrix XenApp 6.0 Core Counters ...................................................... 196
  Monitored Components ................................................................. 196
Citrix XenApp 6.0 ICA Session .......................................................... 199
  Monitored Components ................................................................. 199
Citrix XenApp 6.0 Presentation Server .............................................. 204
  Monitored Components ................................................................. 204
Citrix XenApp 6.0 Services ............................................................... 208
  Monitored Components ................................................................. 208
Citrix XenApp and Xen Desktop 7.x (Advanced)................................. 210
  Monitored Components ................................................................. 210
Citrix XenApp and Xen Desktop 7.x (Events) ....................................... 210
  Monitored Components ................................................................. 211
Citrix XenApp and Xen Desktop 7.x (Performance Counters) .................. 212
  Monitored Components ................................................................. 212
Citrix XenApp and Xen Desktop 7.x (Services) ..................................... 215
  Monitored Components ................................................................. 215
Clam AV ......................................................................................... 219
  Monitored Components ................................................................. 219
CUPS ............................................................................................ 220
  Monitored Components ................................................................. 220
DHCP User Experience Monitor ...................................................... 222
  Monitored Components ................................................................. 222
Directory Size .............................................................................. 223
  Monitored Components ................................................................. 223
Distributed File System (DFS) ......................................................... 224
  Monitored Components ................................................................. 224
DNS User Experience ................................................................. 230
  Monitored Components ......................................................... 230

Download Speed Monitor .......................................................... 231
  Installing the Microsoft Windows Character Generator Service ................ 231
  Enabling the Unix/Linux Character Generator Service ............................ 232
  Monitored Components ......................................................... 232

Errors in Application Event Log ................................................ 233
  Monitored Components ......................................................... 233

Files ......................................................................................... 234
  File Age Monitor ................................................................. 235
    Monitored Components ......................................................... 235
  File Change Monitor ............................................................. 236
    Monitored Components ......................................................... 236
  File Count ............................................................................ 237
    Monitored Components ......................................................... 237
  File Count Script .................................................................. 238
    Monitored Components ......................................................... 238
  File Existence Monitor ........................................................... 239
    Monitored components ........................................................ 239
  File Size Monitor ................................................................. 240
    Monitored Components ......................................................... 240

FTP User Experience .................................................................. 241
  Monitored Components ......................................................... 241

GlassFish (JMX) .......................................................................... 242
  Monitored Components ......................................................... 243

GoodLink Server for Microsoft Exchange ....................................... 246
  Monitored Components ......................................................... 246

Group Policy Object (System and Application Logs) ....................... 249
  Monitored Components ......................................................... 249

Helix ......................................................................................... 253
Helix Universal Media Server (Linux/Unix) ................................................................. 254
  Monitored Components ....................................................................................... 254
Helix Universal Media Server (Windows) .............................................................. 262
  Monitored Components ....................................................................................... 262
HP-UX .................................................................................................................. 270
  Monitored Components ....................................................................................... 270
HTTP ...................................................................................................................... 274
  HTTP template .................................................................................................... 275
    Monitored Components ..................................................................................... 275
  HTTPS Monitor template .................................................................................... 276
    Monitored Components ..................................................................................... 276
  HTTP Form Login template ................................................................................ 277
    Monitored Components ..................................................................................... 277
IBM ....................................................................................................................... 278
  IBM DB2 ............................................................................................................. 279
    Configure DB2 on AIX devices ...................................................................... 281
      Monitored Components .................................................................................. 283
  IBM DB2 HADR Health ....................................................................................... 287
    Configure DB2 on AIX devices ...................................................................... 289
      Monitored Components .................................................................................. 291
  IBM Informix ...................................................................................................... 294
    Minimum Permissions ...................................................................................... 294
      Creating the group informix and user informix ......................................... 294
      For IBM Informix installed on Windows ..................................................... 295
        For IBM Informix installed on Linux ........................................................ 298
      Monitored Components: ............................................................................. 301
  IBM WebSphere (JMX) ....................................................................................... 305
    Monitored Components ..................................................................................... 306
IMAP4 Round Trip Email ..................................................................................... 308
    Monitored Components ..................................................................................... 308
<table>
<thead>
<tr>
<th>Component Name</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISC DHCP Server (Linux)</td>
<td>309</td>
</tr>
<tr>
<td>Monitored Components</td>
<td>309</td>
</tr>
<tr>
<td>Java Application Server (SNMP)</td>
<td>311</td>
</tr>
<tr>
<td>Monitored Components</td>
<td>311</td>
</tr>
<tr>
<td>JBoss (JMX)</td>
<td>317</td>
</tr>
<tr>
<td>Monitored Components</td>
<td>318</td>
</tr>
<tr>
<td>Configuring Java Application Servers for JMX</td>
<td>322</td>
</tr>
<tr>
<td>Java Arguments</td>
<td>322</td>
</tr>
<tr>
<td>Configuring a Standalone Java Virtual Machine</td>
<td>323</td>
</tr>
<tr>
<td>Windows</td>
<td>323</td>
</tr>
<tr>
<td>Linux</td>
<td>324</td>
</tr>
<tr>
<td>Testing a Standalone JVM</td>
<td>325</td>
</tr>
<tr>
<td>Configuring JBoss (tested on version 6.1)</td>
<td>325</td>
</tr>
<tr>
<td>Linux</td>
<td>326</td>
</tr>
<tr>
<td>Configuring GlassFish (tested on version 3.1)</td>
<td>327</td>
</tr>
<tr>
<td>Configuring IBM WebSphere (tested on version 8.0)</td>
<td>328</td>
</tr>
<tr>
<td>Configuring Oracle WebLogic (tested on version 12)</td>
<td>329</td>
</tr>
<tr>
<td>Windows</td>
<td>329</td>
</tr>
<tr>
<td>Linux</td>
<td>330</td>
</tr>
<tr>
<td>Java Application Server (JMX)</td>
<td>331</td>
</tr>
<tr>
<td>Monitored Components</td>
<td>331</td>
</tr>
<tr>
<td>JD Edwards EnterpriseOne Server Manager (Windows)</td>
<td>336</td>
</tr>
<tr>
<td>Monitored Components</td>
<td>336</td>
</tr>
<tr>
<td>Kaspersky Security Center Antivirus</td>
<td>338</td>
</tr>
<tr>
<td>Monitored Components</td>
<td>338</td>
</tr>
<tr>
<td>LDAP User Experience Monitor</td>
<td>341</td>
</tr>
<tr>
<td>Monitored Components</td>
<td>341</td>
</tr>
<tr>
<td>Linux templates</td>
<td>342</td>
</tr>
<tr>
<td>Linux CPU Monitoring Perl</td>
<td>343</td>
</tr>
<tr>
<td>Monitored Components</td>
<td>343</td>
</tr>
</tbody>
</table>
Linux Disk Monitoring Perl ................................................................. 345
Monitored Components ................................................................. 345
Linux Memory Monitoring Perl ....................................................... 348
Monitored Components ................................................................. 348
Linux Sendmail Monitoring Perl ...................................................... 351
Monitored Components ................................................................. 351
Log Parser ......................................................................................... 353
Log Parser (PowerShell) ................................................................. 354
Monitored Components ................................................................. 354
Log Parser (Perl) ............................................................................. 356
Monitored Components ................................................................. 356
Lotus templates ............................................................................ 358
Lotus Domino Server Processes and Network Ports (Windows) ........ 359
Monitored Components ................................................................. 359
Lotus Domino Server Processes and Network Ports (Linux) .......... 362
Monitored Components ................................................................. 362
Lotus Domino Server Statistics ...................................................... 365
Monitored Components ................................................................. 365
MAPI Round Trip Email ................................................................. 368
Monitored Components ................................................................. 368
Memcached ....................................................................................... 369
Monitored Components ................................................................. 369
Active Directory ............................................................................ 373
Active Directory 2003-2008 Services and Counters ...................... 374
Monitored Components ................................................................. 374
Active Directory 2008 R2-2012 Services and Counters ................. 379
Monitored Components ................................................................. 379
Active Directory 2016 Domain Controller Security ...................... 383
Active Directory 2016 Services and Counters ................................ 384
Monitored Components ................................................................. 384
Exchange 2007 Hub Transport Role Counters (Advanced) ........................................... 442
  Monitored Components ................................................................. 442
Exchange 2007 Mailbox Role Counters (Advanced) ............................................... 446
  Monitored Components ................................................................. 446
Exchange 2007 Outlook Web Access (OWA) Form Login ........................................ 451
  Monitored Components ................................................................. 451
Exchange 2007 Unified Messaging Role Counters (Advanced) .................................. 452
  Monitored Components ................................................................. 452
Exchange 2007 — 2010 Client Access Role Services and Counters (Basic) ............ 454
  Monitored Components ................................................................. 454
Exchange 2007 — 2010 Common Performance Counters ....................................... 456
  Monitored Components ................................................................. 456
Exchange 2007 — 2010 Edge Transport Role Services and Counters (Basic) ....... 459
  Monitored Components ................................................................. 459
Exchange 2007 — 2010 Hub Transport Role Services and Counters (Basic) .......... 461
Exchange 2007 — 2010 Unified Messaging Role Services and Counters (Basic) .... 464
  Monitored Components ................................................................. 464
Exchange 2010 Client Access Role Counters (Advanced) ........................................ 466
  Monitored Components ................................................................. 466
Exchange 2010 Edge Transport Role Counters (Advanced) .................................... 468
  Monitored Components ................................................................. 468
Exchange 2010 Hub Transport Role Counters (Advanced) ..................................... 472
  Monitored Components ................................................................. 472
Exchange 2010 OWA Form Login (PowerShell) ............................................... 476
  Monitored Components ................................................................. 476
Exchange 2016 Unified Messaging Role Counters (Advanced) ................................ 477
  Monitored Components ................................................................. 477
Exchange 2013 Client Access Role Counters (Advanced) ..................................... 478
  Monitored Components ................................................................. 479
Exchange 2013 Client Access Role Services and Counters (Basic) ....................... 482
Monitored Components ................................................................. 482
Exchange 2016 Client Access Role Services and Counters (Basic) ............... 484
Monitored Components ................................................................. 484
Exchange 2016 Client Access Role Services and Counters (Advanced) ............ 486
Monitored Components ................................................................. 486
Exchange 2016 Hub Transport Role Counters (Advanced) .......................... 488
Monitored Components ................................................................. 488
Exchange 2016 Hub Transport Role Services and Counters (Basic) ................ 491
Exchange Active Sync Connectivity .................................................. 493
Monitored Components ................................................................. 494
Troubleshooting ............................................................................. 494
Exchange Server 2000 and 2003 ........................................................ 495
Monitored Components ................................................................. 496
Exchange Web Services User Experience monitor ..................................... 496
Field Descriptions ........................................................................ 497
Microsoft Forefront ........................................................................ 499
Microsoft Forefront Endpoint Protection 2010 (Client) ............................... 500
Monitored Components ................................................................. 500
Microsoft Forefront Endpoint Protection 2010 (Server) ............................... 504
Monitored Components ................................................................. 504
Microsoft Forefront Threat Management Gateway 2010 ............................ 506
Monitored Components ................................................................. 506
Microsoft IIS ................................................................................... 511
IIS templates .................................................................................. 512
Monitored Components ................................................................. 512
Microsoft IIS SMTP Server template .................................................... 513
Monitored Components ................................................................. 514
Microsoft Lync ............................................................................... 517
Microsoft Lync Server (Edge Role) ...................................................... 518
Monitored Components ................................................................. 518
Microsoft Lync Server (Front-End Role) ................................................................. 522
Monitored Components ....................................................................................... 522
Microsoft Lync Server (Mediation Role) ............................................................. 527
Monitored Components ....................................................................................... 527
Microsoft Lync Server 2013 (Front-End Role) ...................................................... 529
Monitored Components ....................................................................................... 529
Microsoft Lync Server 2013 (Edge Role) ............................................................. 535
Monitored Components ....................................................................................... 535
Microsoft Lync Server 2013 (Mediation Role) ...................................................... 539
Monitored Components ....................................................................................... 539

Microsoft Message Queuing .............................................................................. 541
Microsoft Message Queuing Events .................................................................... 542
Monitored Components ....................................................................................... 542
Microsoft Message Queuing (Performance) ......................................................... 555
Monitored Components ....................................................................................... 555

Microsoft Network Policy .................................................................................. 558
Microsoft Network Policy Server Events ............................................................ 559
Monitored Components ....................................................................................... 559
Microsoft Network Policy Server RADIUS Proxy .............................................. 564
Monitored Components ....................................................................................... 564
Microsoft Network Policy Server RADIUS Server ............................................ 567
Monitored Components ....................................................................................... 567

Microsoft Office 365 ......................................................................................... 570
Microsoft Office 365 Exchange Mailboxes ......................................................... 570
Microsoft Office 365 Exchange Mobile Device Statistics ................................ 571
Microsoft Office 365 Exchange Online .............................................................. 572
Microsoft Office 365 Group Statistics ................................................................. 572
Microsoft Office 365 License Statistics ............................................................... 573
Microsoft Office 365 Mail Traffic Statistics ...................................................... 574
Microsoft Office 365 Mobile Device Management ........................................... 574
Microsoft Office 365 Portal ................................................................. 575
Microsoft Office 365 Subscription ......................................................... 575
Microsoft Office 365 Security Statistics .................................................. 576
Office 365 User Statistics with PowerShell .............................................. 577
Monitored Components ................................................................. 577

**Microsoft Routing and Remote Access** ........................................... 579

Microsoft Routing and Remote Access 2008-2012 R2 .................................. 579
Monitored Components ................................................................. 579

Microsoft Routing and Remote Access 2008 - 2016 (Events) ....................... 583
Monitored Components ................................................................. 583

Microsoft Routing and Remote Access 2016 ........................................... 584
Monitored Components ................................................................. 584

Microsoft Routing and Remote Access 2016 (Events) ................................ 588
Monitored Components ................................................................. 588

**Microsoft SharePoint** ....................................................................... 590

Microsoft SharePoint Server 2016 ......................................................... 590
Monitored Components ................................................................. 590

SharePoint Server (MOSS) 2007 ............................................................ 594
Monitored Components ................................................................. 594

SharePoint Server 2010 ........................................................................ 597
Monitored Components ................................................................. 597

SharePoint Server 2013 ........................................................................ 600
Monitored Components ................................................................. 600

SharePoint Services (WSS) 3.0 ............................................................... 604
Monitored Components ................................................................. 604

SharePoint Services (WSS) 6.0 ............................................................... 605
Monitored Components ................................................................. 605

**Microsoft Skype for Business templates** ........................................... 607

Skype for Business Server 2015 (Edge Role) .......................................... 607
Monitored Components ................................................................. 607
Skype for Business Server 2015 (Front-End Role) ................................................................. 608
  Monitored Components ........................................................................................................ 609
Skype for Business Server 2015 (Mediation Role) ............................................................. 609
  Monitored Components ........................................................................................................ 610
Microsoft SQL Server ........................................................................................................... 611
  SQL Server 2005 Analysis Services ...................................................................................... 611
  SQL Server 2008 Analysis Services ...................................................................................... 616
    Monitored Components ...................................................................................................... 616
  SQL Server 2008 Reporting Services ................................................................................... 620
    Monitored Components ...................................................................................................... 620
  SQL Server 2008 Reporting Services R2 .............................................................................. 623
    Monitored Components ...................................................................................................... 623
  SQL Server 2008-2012 Reporting Services (Events) ........................................................... 626
    Monitored Components ...................................................................................................... 626
  SQL Server 2012 Analysis Services ...................................................................................... 630
    Monitored Components ...................................................................................................... 630
  SQL Server 2012 Reporting Services ................................................................................... 634
    Monitored Components ...................................................................................................... 634
Microsoft Windows Internet Name Service (WINS) ........................................................... 638
  Microsoft Windows Internet Name Service (WINS) Events .................................................. 638
    Monitored Components ...................................................................................................... 638
  Microsoft Windows Internet Name Service (WINS) Statistic .................................................. 644
    Monitored Components ...................................................................................................... 644
Microsoft Windows Server .................................................................................................... 646
  Microsoft Windows Server 2003 Failover Cluster ............................................................... 647
    Monitored Components ...................................................................................................... 647
  Windows 2003 -2008 FTP Service ........................................................................................ 654
    Monitored Components ...................................................................................................... 655
  Microsoft Windows Server 2008 Failover Cluster ............................................................... 657
    Monitored Components ...................................................................................................... 657
Microsoft Windows Server 2008 R2-2016 Failover Cluster (Advanced) .................................................. 666
Monitored Components .................................................................................................................. 666
Microsoft Windows Server 2012 - 2016 Failover Cluster .............................................................. 667
Monitored Components .................................................................................................................. 667
Microsoft Windows Server 2012 Failover Cluster ......................................................................... 677
Monitored Components .................................................................................................................. 677
Microsoft Windows 2016 FTP service ............................................................................................. 679
Monitored Components .................................................................................................................. 679
Windows Update Monitoring ........................................................................................................ 680
Configuring Windows Remote Management (WinRM) .................................................................... 681
Monitored Components .................................................................................................................. 681
Windows 2008 R2 - 2012 FTP Service ............................................................................................. 682
Monitored Components .................................................................................................................. 682
Microsoft Windows DHCP Server .................................................................................................. 684
Monitored Components .................................................................................................................. 684
Windows DNS Server ..................................................................................................................... 688
Monitored Components .................................................................................................................. 688
Windows Network Load Balancing ................................................................................................. 691
Monitored Components .................................................................................................................. 691
Microsoft Windows Servers Print Services ..................................................................................... 697
Monitored Components .................................................................................................................. 698
Windows Print Services 2016 ........................................................................................................ 699
Monitored Components .................................................................................................................. 699
Windows Remote Desktop Services (Session Host Role) ............................................................... 700
Monitored Components: ................................................................................................................ 700
Windows Scheduled Tasks template ............................................................................................... 707
Windows Server 2003 Domain Controller Security ....................................................................... 708
Microsoft Windows Server 2003-2012 Services and Counters ....................................................... 713
Monitored Components .................................................................................................................. 713
Microsoft Windows Server 2008 - 2016 Domain Controller Security ............................................ 716
<table>
<thead>
<tr>
<th>Component</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Windows Remote Management (WinRM)</td>
<td>716</td>
</tr>
<tr>
<td>Monitored Components</td>
<td>716</td>
</tr>
<tr>
<td>Microsoft Windows Server 2016 Services and Counters</td>
<td>721</td>
</tr>
<tr>
<td>Monitored Components</td>
<td>721</td>
</tr>
<tr>
<td><strong>Microsoft System Center</strong></td>
<td>724</td>
</tr>
<tr>
<td>Microsoft System Center Operations Manager 2012 (Agent)</td>
<td>724</td>
</tr>
<tr>
<td>Monitored Components</td>
<td>724</td>
</tr>
<tr>
<td>Configuring Windows Remote Management (WinRM)</td>
<td>725</td>
</tr>
<tr>
<td>Microsoft System Center Operations Manager 2012 (Management Server)</td>
<td>725</td>
</tr>
<tr>
<td>Monitored Components</td>
<td>726</td>
</tr>
<tr>
<td>Configuring Windows Remote Management (WinRM)</td>
<td>730</td>
</tr>
<tr>
<td>Microsoft System Center Configuration Manager 2012</td>
<td>730</td>
</tr>
<tr>
<td>Monitored Components</td>
<td>731</td>
</tr>
<tr>
<td>Configuring Windows Remote Management (WinRM)</td>
<td>735</td>
</tr>
<tr>
<td><strong>Mongo</strong></td>
<td>736</td>
</tr>
<tr>
<td>MongoDB (Windows)</td>
<td>737</td>
</tr>
<tr>
<td>Monitored Components</td>
<td>737</td>
</tr>
<tr>
<td>MongoDB (Linux)</td>
<td>741</td>
</tr>
<tr>
<td>Monitored Components</td>
<td>741</td>
</tr>
<tr>
<td><strong>MySQL templates</strong></td>
<td>745</td>
</tr>
<tr>
<td>MySQL (5.7.9 or later) for Linux/Unix</td>
<td>745</td>
</tr>
<tr>
<td>Monitored Components</td>
<td>747</td>
</tr>
<tr>
<td>MySQL (5.7.9 or later) for Windows</td>
<td>754</td>
</tr>
<tr>
<td>Monitored Components</td>
<td>755</td>
</tr>
<tr>
<td>MySQL (pre 5.7.9) for Linux/Unix</td>
<td>762</td>
</tr>
<tr>
<td>Monitored Components</td>
<td>764</td>
</tr>
<tr>
<td>MySQL (pre 5.7.9) for Windows</td>
<td>771</td>
</tr>
<tr>
<td>Monitored Components</td>
<td>771</td>
</tr>
<tr>
<td><strong>Nagios Linux File &amp; Directory Count Script</strong></td>
<td>779</td>
</tr>
<tr>
<td>Monitored Components</td>
<td>779</td>
</tr>
</tbody>
</table>
Create a Linux or Unix script monitor .................................................. 785
Adapt an existing Perl script to a Linux/Unix Script component monitor in a new template .... 785
Linux/Unix scripts ................................................................................. 787
Example scripts .................................................................................. 787
Scripts must report status through exit codes ..................................... 787
Scripts with Text Output ....................................................................... 788
Nagios scripting .................................................................................. 789
Nagios Script monitor .......................................................................... 789
Field Descriptions ................................................................................ 790
Scripts must report status through return codes .................................. 792
Test script output .................................................................................. 792

**Novell GroupWise** ........................................................................... 794

Novell GroupWise Message Transfer Agent (Unix) ................................ 795
Monitored Components ......................................................................... 795
Novell GroupWise Message Transfer Agent (Windows) ......................... 798
Monitored Components ......................................................................... 798
Novell GroupWise Post Office Agent (Unix) .......................................... 801
Monitored Components ......................................................................... 801
Novell GroupWise Post Office Agent (Windows) ..................................... 806
Monitored Components ......................................................................... 806

**OpenLDAP** .................................................................................... 811
Monitored Components ......................................................................... 812

**Oracle** .......................................................................................... 814

Oracle Automatic Storage Management ............................................ 814
Monitored components ......................................................................... 814
Oracle Database monitor ...................................................................... 818
Monitored components ......................................................................... 818
Oracle WebLogic (JMX) ................................................................. 824
  Monitored Components ...................................................... 825

**POP3 Round Trip Email** ......................................................... 830
  Monitored Components ...................................................... 830

**Postfix** ............................................................................. 831
  Monitored Components ...................................................... 831

**PostgreSQL** ...................................................................... 834
  Monitored Components ...................................................... 835

**Progress Database (Linux and Unix sh script)** .................... 839
  Monitored Components ...................................................... 839

**RADIUS User Experience Monitor** ...................................... 843
  Monitored Components ...................................................... 843

**Remote Desktop Services Licensing** .................................... 844
  Monitored Components ...................................................... 844

  Configuring Windows Remote Management (WinRM) ............. 847

**Server Clock Drift** .............................................................. 849

  Server Clock Drift (PowerShell) ......................................... 850
  Monitored Components ...................................................... 850

  Server Clock Drift (Perl) ................................................... 851
  Monitored Components ...................................................... 851

**SOAP/JSON Example** .......................................................... 852
  Monitored Components ...................................................... 852

**Solaris** .............................................................................. 853

  Solaris ............................................................................. 854
  Monitored Components ...................................................... 854

  Solaris LPD ....................................................................... 857
  Monitored Components ...................................................... 857

**SolarWinds templates** .......................................................... 859

  Orion Server 2017.3 ........................................................... 860
  Monitored components ...................................................... 860
SolarWinds Failover Engine .......................................................... 863
  Monitored Components .......................................................... 863
SolarWinds NetFlow Traffic Analyzer Database ................................ 866
  Monitored Components .......................................................... 866
SolarWinds NetFlow Traffic Analyzer .............................................. 869
  Monitored Components .......................................................... 869
SolarWinds Web Performance Monitor (WPM) Player ....................... 873
  Monitored Components .......................................................... 873
Kiwi Syslog Server ................................................................. 876
  Monitored Components .......................................................... 876
**Squid** .................................................................................... 878
  Squid (Windows) ................................................................. 879
    Monitored Components ....................................................... 879
  Squid (Linux and Unix) ........................................................... 885
    Monitored Components ....................................................... 885
**SSL Certificate Expiration Date Monitor** .................................. 892
  Monitored Components .......................................................... 892
**Streaming Media Services 2008** ............................................. 893
  Monitored Components .......................................................... 893
**Sybase** .................................................................................. 897
  Sybase ASE ........................................................................... 898
    Monitored Components ....................................................... 899
  Sybase SQL Anywhere ............................................................ 901
    Monitored Components ....................................................... 901
**Symantec** ............................................................................. 905
  Symantec Backup Exec Remote Agent ....................................... 906
    Monitored Components ....................................................... 906
  Symantec Backup Exec Server ............................................... 907
    Monitored Components ....................................................... 907
  Symantec Endpoint Protection Client ..................................... 913
Monitored Components ................................................................. 913
Symantec Endpoint Protection Server ........................................... 916
Monitored Components ................................................................. 916
Symantec NetBackup Server .......................................................... 918
Monitored Components ................................................................. 918
Symantec NetBackup Client ............................................................ 922
Monitored Components ................................................................. 922
**TACACS+ User Experience Monitor** ...................................................... 923
Monitored Components ................................................................. 923
**Terminal Licensing Server** ............................................................ 924
Monitored Components ................................................................. 924
**Tomcat Server** ................................................................. 928
Monitored Components ................................................................. 929
Tomcat Server monitor ................................................................. 930
Field Descriptions ................................................................. 932
Install and configure Tomcat ............................................................ 933
Troubleshoot Tomcat ................................................................. 934
**Trend Micro** ................................................................. 935
Trend Micro OfficeScan Client .......................................................... 935
Monitored Components ................................................................. 935
Trend Micro OfficeScan Server .......................................................... 936
Monitored Components ................................................................. 936
Trend Micro Server Protect (Windows) ...................................................... 938
Monitored Components ................................................................. 938
**UniData Database (Windows)** .......................................................... 941
Monitored Components ................................................................. 941
**Unix** ................................................................. 946
Unix CPU Monitoring Perl ............................................................... 947
Monitored Components ................................................................. 947
Unix Disk Monitoring Perl ............................................................... 950
Monitored Components ......................................................................................................................... 950
Unix Memory Monitoring Perl .................................................................................................................. 952
Monitored Components .......................................................................................................................... 952
Unix Sendmail Monitoring Perl .................................................................................................................. 954
Monitored Components .......................................................................................................................... 955

**Veeam Backup and Replication Server** .................................................................................................. 957
Monitored Components .......................................................................................................................... 957
Configuring Windows Remote Management (WinRM) .............................................................................. 959

**VMWare** ............................................................................................................................................... 960
VMware vCenter Server 5.5 ......................................................................................................................... 960
Monitored Components .......................................................................................................................... 960
VMware ESX Host ....................................................................................................................................... 963
Monitored Components .......................................................................................................................... 963

**Web Link** ............................................................................................................................................... 966
Monitored Components .......................................................................................................................... 966

**Websense Web Security** ......................................................................................................................... 967
Monitored Components .......................................................................................................................... 967
Welcome to the SAM Template Reference

SolarWinds SAM provides over 250 predefined templates to help get you started monitoring servers and applications. As described in the SAM Administrator Guide, component monitors are the building blocks of SAM templates. Each template consists of multiple component monitors designed to poll for specific metrics about an application, process, or event.

This reference provides details about the out-of-the-box templates included in SAM, organized into the following categories:

- AIX templates
- Apache templates
- APC PowerChute Agent (Windows)
- AppInsight
- Barracuda Spam and Virus Firewall
- Bind
- BizTalk
- Blackberry
- Cisco
- Citrix templates
- Clam AV
- CUPS
- DHCP User Experience Monitor
- Directory Size
- Distributed File System (DFS)
- DNS User Experience
- Download Speed Monitor
- Errors in Application Event Log
- Files
- FTP User Experience
- GlassFish (JMX)
- GoodLink Server for Microsoft Exchange
- Group Policy Object (System and Application Logs)
- Helix
- HP-UX
- HTTP
- IBM
- Internet Information Services (IIS)
- IMAP4 Round Trip Email
- ISC DHCP Server (Linux)
- Java Application Server (SNMP)
• JBoss (JMX)
• JD Edwards EnterpriseOne Server Manager (Windows)
• Kaspersky Security Center Antivirus
• LDAP User Experience Monitor
• Linux templates
• Log Parser
• Lotus templates
• MAPI Round Trip Email
• Memcached
• Active Directory
• Microsoft Direct Access
• Microsoft Dynamics
• Exchange templates
• Microsoft Forefront
• Microsoft IIS
• Microsoft Lync
• Microsoft Message Queuing
• Microsoft Network Policy
• Microsoft Office 365
• Microsoft Routing and Remote Access
• Microsoft SharePoint
• Microsoft Skype
• Microsoft SQL Server
• Microsoft System Center
• Microsoft Windows Internet Name Service (WINS)
• Microsoft Windows Server
• Mongo
• MySQL templates
• Nagios Linux File & Directory Count Script
• Novell GroupWise
• Office 365 User Statistics with PowerShell
• OpenLDAP
• Oracle
• POP3 Round Trip Email
• Postfix
• PostgreSQL
• Progress Database (Linux and Unix sh script)
• Remote Desktop Services Licensing
• RADIUS User Experience Monitor
• Server Clock Drift
Learning Application Templates (video)
- Creating a New Application Template (video)
- Managing Assigned Application Monitors (video)
- Building & Implementing Custom Application Templates (SolarWinds Academy)
- Expert Series: SAM - Alerting and troubleshooting templates (SolarWinds Academy)
- Using Automation to Apply SAM Templates (video)

Linux/Unix system configurations for component monitors

To effectively monitor Linux/Unix systems with the Orion agent for Linux/Unix, consider and complete the following configurations for component monitor and templates. You may need to reference vendor documentation, as well as work with your NOC and server management groups to complete modifications.
Apache configurations

You should have the following packages installed:

- Apache httpd
- LWP::UserAgent (Perl)

To install and configure:

1. Log into your Apache server using SSH or telnet client. Grant yourself root permissions (so root).
2. Use the command: `yum install perl-libwww-perl`
3. Locate `httpd.conf`: `find /etc -iname httpd.conf`. The file is typically located in `/etc/httpd/conf/httpd.conf`.
4. Locate the following section:

   ```
   #<Location /server-status>
   #  SetHandler server-status
   #  Order deny,allow
   #  Deny from all
   #  Allow from .example.com
   </Location>
   ```

5. Uncomment the code. Edit the `Allow from` rule, substituting the IP address or hostname of your Apache server for localhost. Use localhost only if the Apache server services the loopback interface. Also make sure the `ExtendedStatus` is On.

   ```
   <Location /server-status>
   SetHandler server-status
   Order deny,allow
   Deny from all
   Allow from localhost
   </Location>
   ExtendedStatus On
   ```
6. Restart the Apache service httpd restart
or
Reload the configuration: service httpd reload

Tomcat configurations

Apache Tomcat is an open-source web server, implementing several Java EE specifications.

The following information walks through installing and configuring Tomcat servers to work with SAM component monitors. If you have Tomcat installed, you can skip to step 4 to create an account used for polling.

1. Determine the version of Tomcat you want to install. You may have multiple versions available to install. To locate all versions, use this command:

```bash
yum search tomcat
```

2. After determining the version, you can install the tomcat package and the admin webapps package. Locate the versions to install from the search results. For example:

```
tomcat5.i386 : Apache Servlet/JSP Engine, RI for Servlet 2.4/JSP 2.0 API
tomcat5-admin-webapps.i386 : The administrative web applications for Jakarta Tomcat
```

3. Install the versions using the located versions. To install the example above:

```bash
yum install tomcat5 tomcat5-admin-webapps
```

4. Next, you need to modify the tomcat-users.xml file to create and provide a user account to access the web manager ('manager','manager-gui'). To locate, use this command:

```bash
find /etc -iname tomcat-users.xml
```

5. Edit the file and locate the <tomcat-users> section. If commented out, uncomment the configuration. Edit to add a user of tomcat with the password of tomcat. The template uses this account to access data.

```xml
<tomcat-users>
    <user name="tomcat" password="tomcat" roles="tomcat,manager,manager-gui" />
    <user name="role1" password="tomcat" roles="role1" />
    <user name="both" password="tomcat" roles="tomcat,role1" />
</tomcat-users>
```
6. Restart the service. The command depends on the version you installed. For example, this command restarts the installed service above:

```
service tomcat5 restart
```
For JMX configurations, install and configure WebSphere per your Linux/Unix distribution. See the IBM Knowledge Center for details. The overall steps include:

1. Install WebSphere and note the following details:
   - You may need to create an administrator account and a new package group.
   - During installation, turn off the secure storage option as this is not needed.
   - Make sure to select the Application Server during installation.
2. Start and stop the WebSphere AppServer.
3. Use a browser to access the WebSphere AppServer console at http://websphere-host:9060/ibm/console
   - You may need to open a port to 9060 on the Websphere host.
   - Use the credentials for the account created during installation.
4. In the console, expose the JMX platform mbeans in the WebSphere AppServer by:
   - Clicking Servers > Server Types > WebSphere application servers.
   - Selecting the listed application server.
5. Locate the Java and Process Management > Process definition. In the Generic JVM arguments dialog box, enter the following code:

   ```
   Djavax.management.builder.initial=
   Dcom.sun.management.jmxremote=true
   Dcom.sun.management.jmxremote.port=8686
   Dcom.sun.management.jmxremote.ssl=false
   Dcom.sun.management.jmxremote.authenticate=false
   Djava.rmi.server.hostname=localhost
   ```

   Note: There is nothing after the = sign.
6. Restart the AppServer.

### Squid

Squid is a caching and forwarding web proxy. It has a wide variety of uses, from speeding up a web server by caching repeated requests; to caching web, DNS and other computer network lookups for a group of people sharing network resources, to aiding security by filtering traffic.

To configure Squid for agent polling:

- **SNMP is required** - Enable the SNMP feature for Squid. If using Squid-3, this feature is available to enable by adding a configuration option to `squid.conf`. If using Squid-2, you will need to enable the feature using a series of scripts then configure.
- **perl-switch is required** - Add per your Linux distribution vendor's documentation.

Nagios

Nagios monitors systems, networks, and infrastructure. It offers monitoring and alerting servers, switches, applications, and services. Refer to your vendor's documentation to properly install and configure Nagios according to your Linux distribution.

You can use the Nagios Script monitor and Linux/Unix Script monitor for monitoring Nagios.

If you are using this component monitor with Nagios and polled by Orion agent for Linux, you need to enter a script as follows. The argument would be `python $(SCRIPT)` with a body of:

```python
from random import randint
STAT_PAIRS_COUNT = 10

for stat_id in range(STAT_PAIRS_COUNT):
    print 'Statistic.random%d: %d
Message.random%d: %s' % (stat_id, randint(1,100), stat_id, 'random number: ' + str(randint(1,100)))
```

ODBC configurations

To monitor a database with an ODBC connector, install an ODBC driver for your installed database type, create a user, and test access. Use the new account credentials in your SAM template and component monitors. For a full list of available templates, see the SAM Template Reference.

For the following instructions, you should have a database installed such as MySQL or PostgreSQL.

1. (Required) To begin, you should have unixODBC installed to support Microsoft Windows ODBC. If not, download and install the unixODBC driver to the Linux/Unix-based computer.
2. Install the DBMS driver.
3. Download and install an ODBC driver for your installed database type.
4. Create a user account for the database.
5. Configure the user access privileges with administrative privileges.
6. Test access to the database using the newly created account credentials.

Configure and assign a SAM template with the credentials.

1. In the Orion Web Console, click Settings > All Settings > SAM Settings > Manage Templates.
2. Search for a template based on the database type such as ODBC or Oracle. SolarWinds recommends creating a copy of the template. Select a template and click Copy.
3. Modify the settings of the template and component monitors based on the metrics you want to monitor.
4. To enter credentials, select the component monitor checkboxes and click Assign Credentials.
5. Enter the credentials you created for the database and click OK.
6. Test the access for the template by assigning it to a node. Click Test Node to assign and test the access. If you encounter issues, verify the credentials and privileges for the account.
PostgreSQL configurations

To monitor a PostgreSQL database server with component monitors, you need to install an ODBC driver, create a user, and test access. Use the new account credentials in your SAM template and component monitors.

SAM provides a PostgreSQL template and component monitors for PostgreSQL 9.

For the following instructions, you should have PostgreSQL installed on a Linux-based computer.

1. Login to the Linux-based computer with administrator privileges.
   You will need to create a user account on the server and in the PostgreSQL database.
2. (Required) To begin, you should have unixODBC installed to support Microsoft Windows ODBC. If not, download and install the unixODBC driver to the Linux-based computer.
   Command: yum install unixODBC
3. Download and install the PostgreSQL ODBC driver on the target Linux-based computer.
   Command: yum install postgresql-odbc
4. Create a user account for the database.
   The example of commands adds a user account dbuser with the password Password1 to the Linux-based computer. The next commands login as the database superuser to the ProgreSQL server and modify the created user.

```
# adduser dbuser
# passwd Password1
# su - postgres
$ psql -d template1 -U postgres
```

At the prompt, create the dbuser account with the Password1 password:

```
template1=# CREATE USER dbuser WITH PASSWORD 'Password1';
```

Next, grant privileges for your PostgreSQL database (TestDatabase) to the user account:

```
template1=# GRANT ALL PRIVILEGES ON DATABASE TestDatabase to dbuser;
```

Close the template:

```
template1=# \q
```

5. Test access to the database using the newly created account credentials.

```
$ su - dbuser
$ psql -d TestDatabase -U dbuser
```

Configure and assign a SAM template with the credentials.
1. In the Orion Web Console, click Settings > All Settings > SAM Settings > Manage Templates.

2. Search for the PostgreSQL template. SolarWinds recommends creating a copy of the template. Select the template and click Copy.

3. Modify the settings of the template and component monitors based on the metrics you want to monitor.

4. To enter credentials, select the component monitor checkboxes and click Assign Credentials.

5. Enter the credentials you created for the database and click OK.

6. Test the access for the template by assigning it to a node. Click Test Node to assign and test the access. If you encounter issues, verify the credentials and privileges for the account.

**Troubleshooting**

If you receive the error "FATAL: Peer authentication method failed for user 'postgresuser'", change the authentication method to md5.

**MySQL configurations**

To configure MySQL, you need to install and configure the appropriate MySQL repository, create a user account, and test access. Use the new account credentials in your SAM template and component monitors.

SAM templates include two options for MySQL 5.7.9 and earlier and 5.7.9 and later.

For the following instructions, you should have MySQL installed on a Linux-based computer.

1. Login to the Linux-based computer with administrator privileges.
   
   You will need to create a user account on the server and in the MySQL database.

2. (Required) To begin, you should have unixODBC installed to support Microsoft Windows ODBC. If not, download and install the unixODBC driver to the Linux-based computer.

3. Install the MySQL ODBC driver.
   
   Command: `yum install mysql-connector-odbc`

4. Create a user account for the database.
   
   The following commands create a MySQL account of dbuser with the password Password1 for the database dbtest. The commands also grant all access to the user account.

   ```
   create database testdb;
   create user 'dbuser'@'localhost' identified by 'Password1';
   grant all on dbtest.* to 'dbuser' identified by 'Password1';
   ```

5. (Required) Grant the following access for local access to monitor through SAM and the Orion Platform.
Enter the IP address of this MySQL Linux-based computer, replacing the example value of 10.100.100.100.

```
mysql -uroot -p
CREATE USER 'dbuser'@'%' IDENTIFIED BY 'Password1';
GRANT ALL ON testdb.* TO dbuser@'%' IDENTIFIED BY 'Password1';
GRANT SELECT ON performance_schema.* TO dbuser@'10.100.100.100' IDENTIFIED BY 'Password1';
```

6. Test access to the database using the newly created account credentials.

   **Command:** mysql -u testuser -p

Configure and assign a SAM template with the credentials.

1. In the Orion Web Console, click Settings > All Settings > SAM Settings > Manage Templates.
2. Search for the MySQL templates. SolarWinds recommends creating a copy of the template. Select a template based on version and click Copy.
3. Modify the settings of the template and component monitors based on the metrics you want to monitor.
4. To enter credentials, select the component monitor checkboxes and click Assign Credentials.
5. Enter the credentials you created for the database and click OK.
6. Test the access for the template by assigning it to a node. Click Test Node to assign and test the access. If you encounter issues, verify the credentials and privileges for the account.

**Troubleshooting**

**Error:** Data source name not found and no default driver specified. This error occurs on a CentOS system.

**Solution:** Verify the CentOS system has the mysql-connector-odbc installed. Use the following command to receive a package and version name on the target Linux-based computer: `rpm -q mysql-connector-odbc`

Verify you have the appropriate credentials assigned for each component monitor.

1. In the Orion Web Console, click Settings > All Settings > SAM Settings > Manage Templates.
2. Search for the SAM template. Select and click Edit.
3. Select the component monitor to check assigned credentials.
4. To modify, click Assign Credentials, enter credentials, and click OK.
5. Test the template.

If you continue to encounter issues, verify the appropriate driver is defined on the CentOS system to match the connection string, as shown in the next example.

```
cat /etc/odbcinst.ini
[MySQL]
```
IBM DB2 with ODBC configurations

For IBM DB2, you need to download, install, and configure DB2. (See the IBM DB2 documentation site.) SAM provides two IBM DB2 templates: IBM DB2 and IBM DB2 HADR Health.

Linux-based computers

Here are prerequisites for the following steps:

- IBM DB2 is installed on a Linux-based computer.
- A user account exists on the server and in the IBM DB2 database.

To run commands, you will need the instance users for the database. The instance user connects to the DB and should have the sqllib directory set up.

1. Log into the Linux-based computer with administrator privileges.
2. Use the following command to install the unixODBC package:
   ```bash
   yum -y install unixODBC
   ```
3. Update the ODBC config files by adding the following settings to `/etc/odbcinst.ini`:
   ```ini
   [DB2]
   Description = DB2 Driver
   Driver = /opt/ibm/db2/V10.5/lib64/libdb2.so
   FileUsage = 1
   DontDLClose = 1
   ```
   ![Verify that libdb2.so has the correct file path.]
4. Add the following settings to `/etc/odbc.ini`:
   ```ini
   [dbname]
   Driver = DB2
   ```
   ![The drivers should match in both files.]
5. Connect locally to the database with the instance user credentials. For example:
   ```bash
   isql -v dbname db2inst1 Password1
   ```
6. Log into the DB2 database with the instance user credentials and open the DB2 command line tool.
7. Enable the required following setting used by the SAM IBM DB2 template:
   UPDATE DBM CFG USING DFT_MON_BUFPOOL ON
   UPDATE DBM CFG USING DFT_MON_LOCK ON
   UPDATE DBM CFG USING DFT_MON_STMT ON
   UPDATE DBM CFG USING DFT_MON_UOW on

8. Use the GRANT EXECUTE ON FUNCTION statement to grant privileges for the SYSPROC.MON_GET_TABLE function to *user*, where *user* is the username that SAM as shown in this example:
   GRANT EXECUTE ON FUNCTION SYSPROC.MON_GET_TABLE TO *user*
Configure DB2 on AIX devices

Prerequisites

Important: Do not install the 64-bit ODBC drivers; use the 32-bit drivers instead to support Python distributed on the Orion agent.

  The commands use the following driver bundle: v11.1.1fp1_aix64_odbc_cli_32.tar.gz.
- Install the ODBC driver manager package and its dependencies from www.perzl.org/aix (Obtained from www.perzl.org/aix, on February 1, 2018). Dependencies include:
  - info-6.4-1.aix5.1.ppc.rpm
  - libiconv-1.15-1.aix5.1.ppc.rpm
  - libtool-ltdl-1.5.26-2.aix5.1.ppc.rpm
  - readline-7.0-3.aix5.1.ppc.rpm
  - libffi-3.1.1.aix5.1.ppc.rpm (not a direct dependency, but needed by the SAM monitor plugin)
- The gunzip utility, which is part of the AIX 5L™ default installation setup. You can also download gzip for AIX 5L from http://www.ibm.com/servers/aix/products/aixos/linux/rpmgroups.html (© 2018 IBM Corp.; https://www-01.ibm.com; link acquired on August 2, 2018)
- Verify that the IBM rpm.rte package exists in the /usr/bin/rpm directory

Configure ODBC for AIX

1. Log into the AIX-based computer with administrator privileges.
2. Install the RPM packages.
   Run the following command as root: rpm -ivh unixODBC-2.3.4-1.aix5.1.ppc.rpm
   To install all dependencies as root: rpm -ivh *.rpm

3. Install the DB2 ODBC driver. The example code creates a directory odbc_cli_32 in the /opt directory.
   gunzip v11.1.1fp1_aix64_odbc_cli_32.tar.gz
   tar -x -f v11.1.1fp1_aix64_odbc_cli_32.tar -C /opt
4. Add the following lines to /opt/freeware/etc/odbcinst.ini:
   [DB2]
   Description = DB2 Driver
   Driver = /opt/odbc_cli_32/clidriver/lib/libdb2.so
   FileUsage = 1
   DontDLClose = 1

Verify libdb2 has the correct file path.
5. Add the following settings to /opt/freeware/etc/odbc.ini:

[dbname]
Description = IBM DB2 ODBC data source
Driver = DB2
DMEnvAttr = SQL_ATTR_UNIXODBC_ENVATTR=\{/opt/odbc_cli_32/clidriver\}

- In [dbname], enter the name of the database to be monitored.
- DMEnvAttr value depends on the installation directory for the DB2 ODBC CLI driver.

6. Run the following command as root. It allows the unixODBC manager driver to find the DB2 ODBC file.

```
ar -X32 x libdb2.a shr.o
mv shr.o libdb2.so
```

7. Verify that the SAM python plugin can connect to the DB2 database to monitor it. Save the following script as verifyodbc.py.
The script is written for Orion agents in the default location /opt/SolarWinds/Agent.

```
Important: If you are not using the default port, add server hostname and port number to the connection string.

import sys
sys.path.insert(0, "/opt/SolarWinds/Agent/bin/Plugins/SharedPythonLibs")
import pypyodbc

# Set Database, Uid, and Pwd to the database name, username, and user's password to access said database respectively.
# In this example, database name, username, and the user's password are TEST, db2inst1, and Password1 respectively.

conn_str = 'Driver={DB2};Database=TEST;Uid=db2inst1;Pwd=Password1;'

You can also use the following script to verify that the SAM python plugin can connect to the DB2 database:

```
conn = pypyodbc.connect(conn_str, ansi=True)
conn.close()
except Exception, ex:
    print ex
    print "Failure"
```

8. Run the script using the following command:

```
/opt/SolarWinds/Agent/bin/python2 verifyodbc.py
```
9. SolarWinds recommends that you configure the utilities bundled in the DB2 ODBC CLI bundle. Create the db2cli.ini configuration file in /opt/odbc_cli_32/clidriver/cfg/db2cli.ini:

```
Replace TEST with your database name.
```

```
TEST
Database=TEST
dbalias=TEST
Protocol=TCPIP
Hostname=127.0.0.1
ServiceName=50000
```

Configure and assign the SAM IBM DB2 template to your Linux/Unix-based computer with the instance user credentials.

1. In the Orion Web Console, click Settings > All Settings > SAM Settings > Manage Templates.
2. Search for a IBM DB2 template. SolarWinds recommends creating a copy of the template. Select a template based on version and click Copy.
3. Modify the settings of the template and component monitors based on the metrics you want to monitor.
4. To enter credentials, select the component monitor check boxes and click Assign Credentials.
5. Enter the credentials for the instance user account and click OK.
6. Modify the connection strings for monitors to match your DB. Use one of the following methods:
   - Specify the actual DB and driver:
     ```
     Driver={DB2};Database=TESTDB;Hostname=${IP};Port=50000;Protocol=TCPIP;Uid=${USER};Pwd=${PASSWORD};
     ```
   - Specify the existing data source in odbc.ini:
     ```
     DSN=testdb;Uid=${USER};Pwd=${PASSWORD};
     ```
AIX templates

The following templates are available for AIX, an enterprise-class UNIX OS for the POWER processor architecture found in IBM Power Systems:

- **AIX template**
- **AIX LPD template**
- **Nagios Linux File & Directory Count Script**

The following component monitors are available for AIX:

- Directory Size monitor
- DNS User Experience monitor
- File Age Monitor
- File Change Monitor
- File Count monitor
- File Existence Monitor
- File Size Monitor
- HTTP monitor
- HTTPS monitor
- JMX monitor
- Linux/Unix Script monitor
- Nagios Script monitor
- ODBC User Experience monitor
- Oracle User Experience monitor
- Process monitor
- SNMP monitor
- SOAP Monitor
- TCP Port monitor
- Tomcat Server monitor

See [Linux/Unix system configurations for component monitors](#) for details.
AIX template

This template assesses the performance of the AIX operating system installed on the target server. Perl scripts are used for monitoring the performance of queries.

The template supports all versions of IBM AIX. SolarWinds recommends installing and using the NET-SNMP to monitor. Download and install the NET-SNMP agent on the AIX server.

Prerequisite

SSH and Perl installed on the target server.

Credentials

Root credentials on the target server.

Port

Use port 1161 for the template.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

You need to set thresholds for counters according to your environment. It is recommended to monitor counters for some period of time to understand potential value ranges and then set the thresholds accordingly.

CPU statistic (%)

This monitor returns the percentage of CPU time used. The returned values are as follows:

- User – This component returns the percentage of CPU time spent running non-kernel code (user time). This represents the time spent executing user code. This statistic depends on the programs that the user is running. It is recommended to use the lowest threshold possible.
- System – This component returns the percentage of CPU time spent running the system kernel code (system time). It is recommended to use the lowest threshold possible.
- Wait – This component returns the percentage of CPU time waiting for I/O. It is recommended to use the lowest threshold possible.
- Idle – This component returns the percentage of CPU time spent idle. It is recommended to use the highest threshold possible at all times.

System faults statistic/sec

This monitor returns the rate of system faults, per second. The returned values are as follows:

- Interrupts – This component returns the number of interrupts per second. The threshold for this component depends on the processor. For modern CPUs, a threshold of 1,500 interrupts/sec is a acceptable. A dramatic increase in this value, without a corresponding
increase in system activity, indicates a hardware problem.

- **System_Calls** – This component returns the number of system calls per second. This is a measure of how busy the system is handling applications and services. High System Calls/sec indicates high utilization caused by software. With today's faster CPUs, 20,000 would represent a reasonable threshold.

- **Context_Switches** – This component returns the number of context switches per second. High activity rates can result from inefficient hardware or poorly designed applications. The normal amount of Context Switches/Sec depends on your servers and applications. The threshold for Context Switches/sec is cumulative for all processors, so you need a minimum of 14,000 per processor (single=14,000, dual=28,000, quad=56,000, and so forth).

**Kernel threads statistic**

This monitor returns the number of kernel threads in different states. The returned values are as follows:

- **In_Run_Queue** – This component returns the average number of runnable kernel threads over the sampling interval. This should be as low as possible. If the run queue is constantly growing, it may indicate the need for a more powerful CPU or more CPUs. Set the thresholds appropriately for your environment.

- **Waiting_For_resources** – This component returns the average number of kernel threads placed in the VMM wait queue (awaiting resource, awaiting input/output) over the sampling interval. This should be as low as possible. Set the thresholds appropriately for your environment.

**Memory and Swap statistic (MB)**

This monitor returns the memory and swap statistic in MB. The returned values are as follows:

- **Free_Memory** – This component returns the amount of available memory in MB. Use the highest threshold possible at all times. Set the thresholds appropriately for your environment.

- **Used_Memory** – This component returns the amount of used memory in MB. Use the lowest threshold possible.

- **FreeSwap** – This component returns the amount of available swap in MB. Use the highest threshold possible at all times. Set the thresholds appropriately for your environment.

- **UsedSwap** – This component returns the amount of used swap in MB. Use the lowest threshold possible.

**Paging statistic/sec**

This monitor returns the different paging statistics. The returned values are as follows:

- **Page_Faults** – This component shows the number of page faults per second. This is not a count of page faults that generate I/O. Some page faults can be resolved without I/O. Use the lowest threshold possible.

- **Paged_In** – This component returns the rate of pages "paged in" from paging space in kB, per second. The operation of reading one inactive page or a cluster of inactive memory pages from the disk is called a "page in." Use the lowest threshold possible.
• Paged_Out – This component returns the rate of pages "paged out" from paging space in kB, per second. The operation of writing one inactive page or a cluster of inactive memory pages to the disk is called a "page out." Use the lowest threshold possible. Values above 20 pages (80 kB), or so, indicate a significant performance problem. In this situation, more memory should be installed.

Processes in different states

This monitor returns the different paging statistics. The returned values are as follows:

• Zombie – This component returns the number of processes that are terminated and where the parent is not waiting. This should always be zero. If it is not zero, you should manually kill zombie processes. Use the following commands to see these zombie processes:
  
  \[
  \text{ps \ -ef | grep defunct.}
  \]

• Active – This component returns the number of processes that are on run queue.

• Swapped – This component returns the number of processes that are currently in swap.

• Idle – This component returns the number of processes that are idle (waiting for startup).

• Canceled – This component returns the number of processes that were canceled.

• Stopped – This component returns the number of processes that are stopped, either by a job control signal or because it is being traced.

Space on root (/) partition (MB)

This monitor returns the available and used space of the root (/) partition in MB. The returned values are as follows:

• Available_Space – This component returns the available space on the root (/) partition in MB. Use the highest threshold possible at all times.

• Used_Space – This component returns the used space on the root (/) partition in MB.

Percentage of using system devices

This monitor returns the name of the system device and the percentage of time the device was busy servicing a transfer request.

\[\text{After applying this template on the target node, you should navigate to, Edit Application Page and click Get Script Output in the Script section. This will build the list of system devices that should be monitored.}\]

Disk operations/sec of system devices

This monitor returns the name of the system device and its read/write transfers to or from the device.

\[\text{After applying this template on the target node, you should navigate to, Edit Application Page and click Get Script Output in the Script section. This will build the list of system devices that should be monitored.}\]

Top 10 active processes

This monitor returns the top 10 active processes and share of CPU usage in percent.
AIX LPD template

This template assesses the status and performance of an AIX LPD print service and uses Perl scripts to retrieve performance data. AIX is an enterprise-class UNIX operating system (OS) for the POWER processor architecture found in IBM Power Systems.

The AIX LPD template supports all versions of IBM AIX. SolarWinds recommends installing and using the NET-SNMP to monitor. Download and install the NET-SNMP agent on the AIX server. Visit the SolarWinds Success Center and see the Configure Net-SNMP for Linux devices article for details.

Prerequisites

- SSH and Perl installed on the target server.

Credentials

- Root credentials on the target server.

Port

- Use port 1161 for the template.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Daemon: lpd

This monitor returns the status of an AIX LPD print server daemon.

Possible values:

- 0 – Print server daemon is stopped.
- 1 – Print server daemon is running.

Print queue

This monitor returns the current length of the default print queue.

Print Server Listening TCP Port

This component monitor tests the ability of an LP print service to accept incoming sessions.

By default, it monitors the TCP 515 port. If your print server listens on another port, you should manually change it.

Nagios Linux File & Directory Count Script

This template uses one Nagios script monitor to provide file and directory count statistics using multiple value script outputs.
Works with the Orion agents for Linux and AIX.

Prerequisites

SSH and Perl installed on the target server.

Credentials

Root credentials on the target server.

A maximum of 10 output pairs can be returned. The monitor in this template uses three.

Prerequisites for Orion agent for Linux

This template uses the Nagios Script monitor. You need to include credentials that can run scripts on the monitored Linux-based computer. Agentless monitoring does not require these credentials.

If you are using this component monitor with Nagios and polled by Orion agent for Linux, you need to enter a script as follows. The argument would be `python $(SCRIPT)` with a body of:

```python
from random import randint
STAT_PAIRS_COUNT = 10

for stat_id in range(STAT_PAIRS_COUNT):
    print 'Statistic.random%d: %d\nMessage.random%d: %s' % (stat_id, randint(1,100), stat_id, 'random number: ' + str(randint(1,100)))
```

For details on the component monitor, see Nagios Script monitor.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

File & Directory Count Monitor

This component monitor uses SSH to upload a script to a server, runs the script, then processes the script exit code and text output. Statistic: Defined by the script. This component monitor has the ability to return multiple results and has the ability to process Nagios resulting output.

If you are using this component monitor with Nagios and polled by Orion agent for Linux, you need to enter a script as follows. The argument would be `python $(SCRIPT)` with a body of:

```python
from random import randint
STAT_PAIRS_COUNT = 10

for stat_id in range(STAT_PAIRS_COUNT):
    print 'Statistic.random%d: %d\nMessage.random%d: %s' % (stat_id, randint(1,100), stat_id, 'random number: ' + str(randint(1,100)))
```
```python
print 'Statistic.random%d: %d\nMessage.random%d: %s' % (stat_id, randint(1,100), stat_id, 'random number: ' + str(randint(1,100)))
```

Field Descriptions

**Description**

This field allows you to provide a description as to what this monitor will actually do for easy reference.

**Component Type**

This describes the type of monitor you are using.

**Enable Component**

This option determines if the component is enabled. Disabling this component leaves it in the application as deactivated and does not influence application availability or status.

**Credential for Monitoring**

Select a credential that can access the Linux or Unix server over SSH and that has sufficient rights to run scripts.

Click a credential in the list, or use the `<Inherit credential from node>` option. If the credential you need is not in the credentials list, add it in the Credentials Library that you can access by clicking Settings > All Settings > SAM Settings in the Orion Web Console.

**Port Number**

This field allows you to specify the port number used for the SSH connection. The default value is 22.

**Script Working Directory**

This field allows you to specify the working directory of the script process.

**Check Type**

This determines how the return code is evaluated.

<table>
<thead>
<tr>
<th>RETURN CODE</th>
<th>SERVICE STATE</th>
<th>HOST STATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Ok</td>
<td>Up</td>
</tr>
<tr>
<td>1</td>
<td>Warning</td>
<td>Up or Down/Unreachable†</td>
</tr>
<tr>
<td>2</td>
<td>Critical</td>
<td>Down/Unreachable</td>
</tr>
<tr>
<td>3</td>
<td>Unknown</td>
<td>Down/Unreachable</td>
</tr>
</tbody>
</table>

† If the Use Aggressive Host Checking option is enabled, return codes of 1 will result in a host state of DOWN, otherwise return codes of 1 will result in a host state of UP.
Command Line

This field is in the script editing window and allows you to specify the script you want to run on the target node followed by the arguments. To enter your script, click the Edit button that reveals the script editing window. For more information, see http://nagios.sourceforge.net/docs/3.0/pluginapi.html.

In this template, the following code is used in the Command Line field:

```perl
perl ${SCRIPT} /etc -sub
```

Body

This field is in the script editing window and allows you to enter your script via typing or pasting. In this template, the following code is used in the Script Body field to provide three script outputs:

Parameters:

- directory - This is the path of the directory (e.g. /bin,/etc,/usr/local,/).
- -sub - Include subdirectories. This parameter is optional.

This Perl script counts the number of files, directories, and symbolic links in a given directory.

```perl
#!/usr/bin/perl
if ($#ARGV != 0 & & $#ARGV != 1)
{
   print "Invalid arguments count. Usage: perl FileCount.pl directory\n";
   exit 3;
}
$dir=$ARGV[0];
$sub="";
if ($#ARGV == 1)
{
   $sub=$ARGV[1];
}
if ($sub ne "-sub")
{
   $fcount=`find $dir -maxdepth 1 -type f | wc -l`; 
   $dcount=`find $dir -maxdepth 1 -type d | wc -l`; 
   $lcount=`find $dir -maxdepth 1 -type l | wc -l`; 
}
else
{
   $fcount=`find $dir -depth -type f | wc -l`; 
   $dcount=`find $dir -depth -type d | wc -l`; 
   $lcount=`find $dir -depth -type l | wc -l`; 
}
```
$exit=`echo $?`; 

# remove the last character (new line symbol)
chop($fcount);
chop($dcount);
chop($lcount);

# find list also parent directory, so we need to remove them
$dcount=$dcount-1;
exit 0;

**Script Output #X**

Each script output has the following fields:

- **Unique ID** - This is the statistic identifier from the script output.
- **Display Name** - This is the name displayed in the User Interface. After generation of the script output, the Unique ID and Display Name become the same. You can change the Display Name to something more user friendly if you so desire.
- **Convert Value** - If this option is selected, you can convert your output with a variety of mathematical functions to suit your needs using either a selection from the drop down menu or selecting Custom Conversion. With the Custom Conversion option, you can enter your own formulas to manipulate the data output further.
- **Warning threshold** - Select a threshold level in conjunction with the logical operators to alert you when the warning threshold has been breached.
- **Critical Threshold** - Select a threshold level in conjunction with the logical operators to alert you when the critical threshold has been breached.

**Status Roll-Up**

This option allows you to choose how you would like the monitor to report based on the output provided by the script. The default selection is “Show worst status.”

**User Notes**

This field allows you to add notes for easy reference. You can access this field by using the variable, ${UserNotes}.
Apache templates

The following templates are available:

- Apache (Windows) template
- Apache template

If you receive a "Cannot connect to local host" message, refer to this article.
Apache template

This template retrieves Apache server statistics from the built-in Apache server-status web page using Perl scripts.

Works with the Orion Agent for Linux.

Prerequisites

Perl, access to the Apache server-status page.

You need libwww-perl installed. You can install on CentOS using this command: `yum install perl-libwww-perl.noarch`

Credentials

SSH account on the web server.

Prerequisites for Orion agent for Linux

If using this template with the Orion agent for Linux, you may need to configure the Apache server for access. See the section for Access Configuration. The Linux/Unix Script monitor is used for all component monitors. See the [Linux/Unix Script monitor](#) for full details and configurations.

Access Configuration

You need to configure Apache to allow access to the server-status page:

1. Log into your Apache server using SSH or telnet client. Grant yourself root permissions (so root).
2. Use the command: `yum install perl-libwww-perl`
3. Locate `httpd.conf`: `find /etc -iname httpd.conf`. The file is typically located in `/etc/httpd/conf/httpd.conf`.
4. Locate the following section:

```
  <$Location /server-status>
  # SetHandler server-status
  # Order deny,allow
  # Deny from all
  # Allow from .example.com
  </$Location>
```

5. Uncomment the code. Edit the `Allow from` rule, substituting the IP address or hostname of your Apache server for localhost. Use localhost only if the Apache server services the loopback interface. Also make sure the `ExtendedStatus` is On.
<Location /server-status>
SetHandler server-status
Order deny,allow
Deny from all
Allow from localhost
</Location>
ExtendedStatus On

6. Restart the Apache httpd: service httpd restart
   or
   Reload the configuration: service httpd reload

Arguments for monitors

Before using this template, the correct arguments should be set in all monitors.

All monitors require the following arguments:

perl ${SCRIPT} server server_port

where

- server - This is the hostname or IP address of the target Apache server. You should set this argument to ${IP} which automatically replaces this argument with the target host IP address.
- server_port - This is the Apache port under which the site is running. By default it is set to port 80.

The following is an example using the Scripts Arguments field:

perl ${SCRIPT} ${IP} 8080

ℹ️ If you receive the error Cannot connect to local host, refer to this article to solve.

Monitored Components

ℹ️ For details on monitors, see SAM Component Monitor Types.

ServerUptime

This counter returns the time that the server has been up.

Format of time: (days)d (hours)h (minutes)m (seconds)s

IdleWorkers

This counter returns the number of free workers ready to handle client connections. This counter should be as high as possible.
If you have no idle workers, or very few, Apache may be using all the processes it is allowed and new incoming requests must wait for older requests to finish before they can be handled. If this is the case, increasing the maximum allowed processes in your configuration file might help with performance.

**TotalAccess**

This counter returns the total number of accesses.

**TotalTraffic**

This counter returns the total number of kilobytes this server has served.

**ServerRequestPerSecond**

This counter returns the average rate of all requests per second.

1. The result is calculated as the total number of requests throughout the life of the server (count) and divided by the total uptime in seconds (up_time).

**ServerKbytesPerSec**

This counter returns the average rate of kilobytes served per second.

**ServerKbytesPerRequest**

This counter returns the average number of bytes per request.

**BusyWorkers**

This counter returns the number of busy workers serving requests. This counter should be as low as possible.
Apache (Windows) template

This template retrieves Apache server statistics from the built-in Apache server-status web page using PowerShell script.

Prerequisites:

Perl, access to the Apache server-status page.

You need libwww-perl installed. You can install using this command: `yum install perl-libwww-perl.noarch`

Access Configuration

Configuring Apache to allow access to the server-status page:

1. Log on to your Apache Windows server.
2. Locate the Apache configuration file, typically in `httpd.conf`.
3. Append the following lines to your `httpd.conf`. You should allow access to server-page for your domain. Replace `APM_host` with the IP address or hostname of Orion server.

   ```
   <Location /server-status>
   SetHandler server-status
   Order Deny,Allow
   Deny from all
   Allow from APM_host
   </Location>
   ExtendedStatus On
   ```

4. Ensure that following line is uncommented and present in the `httpd.conf` file: `LoadModule status_module modules/mod_status.so`

5. Restart the Apache server.

Credentials

Administrator on the SolarWinds server (all monitors run locally).

Before using this template, the correct arguments should be set in all monitors. All monitors require the following arguments:

`server, server_port`

where

- `server` - This is the hostname or IP address of the target Apache server. You should set this argument to `${IP}` which automatically replaces this argument with the target host IP address.
- `server_port` - This is the Apache port under which the site is running. By default, it is set to port 80.

The following is an example using the Scripts Arguments field: `${IP},8080`
Monitored Components

If you receive the error Cannot connect to local host, refer to this article to solve.

For details on monitors, see SAM Component Monitor Types.

Server Uptime

This counter returns the time, in seconds, that the server has been up.

Idle Workers

This counter returns the number of free workers ready to handle client connections. This value should be as high as possible. If you have no idle workers, or very few, Apache may be using all of the processes it is allowed and new, incoming requests must wait for older requests to finish before they can be handled. If this is the case, increasing the maximum number of allowed processes in your configuration file might help with performance.

Total Accesses

This counter returns the total number of accesses.

Total Traffic

This counter returns the total number of kilobytes this server has served.

Server Requests Per Second

This counter returns the average rate of all requests per second. The result is calculated as the total number of requests throughout the life of the server (count) and divided by the total uptime in seconds (up_time).

Server kB Per Second

This counter returns the average rate of kilobytes served per second.

Server kB Per Request

This counter returns the average number of kilobytes per request.

Busy Workers

This counter returns the number of busy workers serving requests. This counter should be as low as possible.
APC PowerChute Agent (Windows)

This template assesses the status and overall performance of APC PowerChute Agent installed on Windows by checking for different event log events.

**Prerequisites**
- WMI access to the target server.

**Credentials**
- Windows Administrator on the target server.

**Monitored Components**

- For details on monitors, see [SAM Component Monitor Types](#).

All monitors should return zero values. Returned values other than zero indicate an abnormality. Examining the Windows application log files with source name APCPBEAgent should provide information pertaining to the issue.

**Service: APC PBE Agent**

This monitor returns the CPU and memory usage of the APC PowerChute Agent.

**APC PowerChute Agent TCP port**

This component monitor tests the ability of the APC PowerChute Agent service to accept incoming sessions. By default it monitors TCP port 2161.

**Events: Hardware Errors**

This monitor returns hardware error events such as:

- Base Module Fan Fault
- Base Power Supply Failure
- Battery Needs Replacing
- System Level Fan Fault
- Main Relay Malfunction
- Site Wiring Fault
- Battery Charger Failure
- Inverter Fault
- Battery Communication Lost
- Contact Fault
Type of event:

Error and Warning. Event ID: 3014, 3015, 3016, 3017, 3018, 3020, 3021, 3022, 3006, 3103, 3104, 3105, 3106.

For the Base Module Fan Fault event: Ensure that the fan events are not blocked.

For the Base Power Supply Failure event: If utility power fails during this condition, a Matrix-UPS, Smart-UPS, or Back-UPS Pro runs for less than half its normal run-time. A failed battery in a Symmetra Power Array reduces normal run-time in proportion to the number of batteries the system contains.

For the Battery Needs Replacing event: Replace the battery.

For other events you should contact UPS manufacturer support.

Events: Bypass

This monitor returns the number of bypass events such as:

- Bypass Contactor Failed
- Bypass Relay Malfunction
- Bypass Internal Fault

Type of event:

Error and Warning. Event ID: 2037, 2040, 2044.

The Bypass Contactor Failed event occurs when the bypass switch failed to put the Symmetra Power Array into bypass, or failed to take it out of bypass.

The Bypass Relay Malfunction event occurs when low or high voltage, or a blackout, has tripped the input circuit breaker at the Symmetra Power Array.

For these events you should contact UPS manufacturer support.

Events: Environmental

This monitor returns the number of environmental errors events such as:

- Maximum Internal Temperature has been exceeded
- Humidity Out of Range
- Temperature Out Of Range.

Type of event

Error and Warning. Event ID: 3107, 3110, 3111, 3120, 3121.

For these events, ensure that the fan inside the UPS is working. Check with the UPS documentation about UPS working environmental issues.

Events: Battery

This monitor returns the number of battery events such as:
- UPS On Battery
- Low Battery Condition
- UPS Battery Is Discharged

**Type of event**


**Events: Output Overload**

This monitor returns the number of output overload events such as:

- UPS Output Overload
- Output Load threshold Exceeded

**Type of event**

Error and Warning. Event ID: 3001, 3031.

Reduce the load by unplugging equipment from the UPS and then run a self-test.

**Events: Communication with UPS**

This monitor returns the number of communications with UPS events such as:

- Communication Not Established
- Lost Communication With UPS

**Type of event**

Error and Warning. Event ID: 3005, 3000.

Check the connection cable.

**Event: System Shutdown**

This monitor returns the number of "system shutdown" starting events.

**Type of event**


The system is shutting down because an event occurred for which the Shut Down Server action is enabled.

**Event: Monitoring Stopped**

This monitor returns the number of "monitoring stopped" events.

**Type of event**

Error and Warning. Event ID: 1000.

Check if UPS monitoring is enabled.

**Event: UPS Self-Test Failed**

This monitor returns the number of "self-test errors" events.
Type of event

Error and Warning. Event ID: 3002.

The UPS failed a self-test for one of the following reasons: Bad Battery - the battery is discharged or defective; the UPS is not in a condition to complete a meaningful test. For an overload condition, unplug equipment that is not in use and try the self-test again.

Event: Insufficient Runtime Available

This monitor returns the number of "insufficient runtime available" events.

Type of event

Error and Warning. Event ID: 3030.

You should reduce the load or change runtime configuration.
AppInsight

The following templates are available:

- AppInsight for Active Directory
- AppInsight for Exchange
- AppInsight for IIS
- AppInsight for SQL

AppInsight for Active Directory

This template monitors and reports on physical and virtual Active Directory environments to identify issues about domain controllers, replication, and more. You can use it to track many key aspects of Active Directory by getting relevant performance data from the server level.

When working with component monitors, note that AppInsight for Active Directory uses domain controller IP addresses instead of domain names for polling; LDAP components do not include the $DomainName parameter in configuration fields. This use of IP address enables different applications to get data from all monitored domain controllers in a single domain.

WMI is the preferred polling method for AppInsight polling. Some information, such as DISK I/O, is tied to volumes only available for nodes managed via WMI.

To learn more about monitoring Active Directory, see AppInsight for Active Directory in the SAM Administration Guide.

Monitored components

For details on monitors, see SAM Component Monitor Types.

Naming Contexts

Total number of naming contexts in the domain.

Replication Details

TBD

FSMO Role - Schema Master

Total number of Schema Master roles in the domain.

FSMO Role - Domain Naming Master

Total number of Domain Naming Master roles in the domain.

FSMO Role - RID Master

Total number of RID Master roles in the domain.
FSMO Role - Infrastructure Master
Total number of Infrastructure Master roles in the domain.

FSMO Role - PDC Emulator
Total number of PDC Emulator roles in the domain.

Total User Accounts
Total number of Active Directory users in the domain.

Total Disabled Accounts
Total number of disabled user accounts in the domain.

Total Computer Accounts
Total number of computer accounts in the domain.

Total Domain Controllers
Total number of domain controllers in the domain.

Total Inactive Users
Total number of inactive users in the domain.

Total Inactive Computers
Total number of inactive computers in the domain.

Sites
Total number of sites in the domain.

Subnets
Total number of subnets in the domain.

Links
Total number of site links in the domain.

Servers
Total number of Active Directory servers in the domain.

Total Expired Password User Accounts
Total number of user accounts which currently have an expired password.

Machine Account authentication failure event
This monitor returns the number of events that indicate a machine account failed to authenticate, which is usually caused by either multiple instances of the same computer name, or the computer name has not replicated to every domain controller.

If you do not find multiple instances of the computer name, verify that replication is functioning for the domain that contains the computer account.
Replication Duplicate Object found event

This monitor returns the number of events that indicate a duplicate object is present in the Active Directory of the replication partner of the local domain controller, so updating it is impossible. See Troubleshooting Directory Data problems to learn more. (©2019 Microsoft Corp., available at http://technet.microsoft.com, obtained on March 4, 2019)

Failed Replication Event

This monitor returns the number of events that indicate replication failed for the reason stated in the message text. Use the Windows Server tool Repadmin.exe to further identify the problem.

Replication configuration does not reflect topology event

This monitor returns the number of events that occur when the replication configuration information in Active Directory Sites and Services does not accurately reflect the physical topology of the network.

Lingering objects disconnection error event

This monitor returns the number of events usually generated by a lingering object which resulted from disconnecting a domain controller for too long.

If the domain controller does not also function as a global catalog server, see "Remove Lingering Objects from an Outdated Writable Domain Controller" in Troubleshooting Active Directory Replication Problems. If the domain controller also functions as a global catalog server, see "Remove Lingering Objects from a Global Catalog Server." (©2019 Microsoft Corp., available at http://technet.microsoft.com, obtained on March 4, 2019)

Replication Link GUID mismatch event

This monitor returns the number of events that occur over an existing replication link when the GUID of the NTDS Settings object of a replication partner does not match the GUID defined in the Service Principal Name (SPN) attributes of the computer object of this replication partner.

User Account cannot be resolved event

This monitor returns the number of events that indicate a user account in one or more Group Policy objects (GPOs) cannot be resolved to a security identifier (SID). This error is possibly caused by a mistyped or deleted user account referenced in either the User Rights Assignment or Restricted Groups branch of a GPO.

User Account was created event

This monitor returns the number of events of creating new user accounts. Event ID: 4720.

Only authorized people and processes should create network accounts. Examine the Primary User Name field to detect whether an authorized person or process created an account. This event also detects if administrators create accounts outside organizational policy guidelines.

Attempt to change Account password event

This monitor returns the number of events when somebody tries to change accounts password. Event ID: 4723.
This event is logged as a failure if his new password fails to meet the password policy. This event results from a password change request in which the user supplies the original password to the account. Compare Primary Account Name to Target Account Name to determine whether the account owner or someone else attempted to change the password. If Primary Account Name does not equal Target Account Name, someone other than the account owner tried to change the password.

**Attempt to reset Account password**

This monitor returns the number of events when a user or process resets an account password through an administrative interface such as Active Directory Users and Computers, rather than through a password change process. Event ID: 4724.

This event is logged as a failure if the new password fails to meet the password policy.

Only authorized people or processes should carry out this process, such as help desk or user self-service password reset.

**Account was disabled event**

This monitor returns the number of events when account becomes disabled. Event ID: 4725. Always investigate this event.

**Account was deleted event**

This monitor returns the number of events of deleting user accounts. Event ID: 4726.

Only authorized people and processes should delete network accounts. Search for these events and examine the Primary Account Name field to detect if unauthorized people have deleted accounts.

**An attempt was made to set the Directory Services Restore Mode administrator password**

This monitor returns the number of events when someone attempts to change the Directory Services Restore Mode password on a domain controller. Event ID: 4794.

Check Workstation IP and Account Name and investigate immediately.

**Clearing the Security Event Logs event**

This monitor returns the number of times security logs have been cleared. Event ID: 517.

Administrators should not clear security event logs without authorization. Check Client User Name and Client Domain, then cross-correlate with authorized personnel.

**Changing system time event**

This monitor returns the number of times the system time has been changed. Event ID: 520.

This action can mislead forensic investigation or provide an attacker with a false alibi. The process name is %windir%\system32\svchost.exe. Check Client User Name and Client Domain, then cross-correlate with authorized personnel.

**Changing audit policy event**

This monitor returns the number of times audit policies have been changed. Event ID: 612.
This event does not necessarily indicate a problem. However, an attacker can change audit policy as part of a computer system attack. You should monitor for this event on high value computers and domain controllers.

**Changing the domain security policy event**

This monitor returns the number of attempts to modify a password policy or other domain security policy settings. Event ID: 643.

Check user name of subject and correlate with authorization.

**LDAP Active Threads**

The current number of threads in use by the LDAP subsystem of the local directory service.

You can provide a value for the warning and critical thresholds based on your current environment and your requirements.

**LDAP Bind Time**

The time (in milliseconds) required for the completion of the last successful LDAP binding.

This counter should be as low as possible. If it is not, it usually indicates that hardware or network-related problems are occurring.

**LDAP Client Sessions**

The number of currently connected LDAP client sessions.

This counter should show activity over time. If it does not, it usually indicates that network-related problems are occurring.

You can provide a value for the warning and critical thresholds based on your current environment and your requirements.

**Directory Service Threads in Use**

The current number of threads in use by the directory service.

This counter should show activity over time. If it does not, it usually indicates that network problems are hindering client requests.

You can provide a value for the warning and critical thresholds based on your current environment and your requirements.

**Address Book Client Sessions**

The number of connected Address Book client sessions.

**Directory Service Notify Queue Size**

The number of pending update notifications that are queued, but not yet transmitted to clients.

This counter should be as low as possible.
**DRA Inbound Full Sync Objects Remaining**

The number of objects remaining until the full synchronization is completed (while replication is done).

![Note] This counter should be as low as possible.

**DRA Inbound Values (DNs only)/sec**

The number of object property values received from inbound replication partners that are distinguished names (DNs) that reference other objects. DN values, such as group or distribution list memberships, are generally more expensive to apply than other types of values.

**DRA Outbound Values (DNs only)/sec**

The number of object property values containing DN sent to outbound replication partners. DN values, such as group or distribution list memberships, are generally more expensive to read than other kinds of values.

**DS Threads in Use**

Indicates the current number of threads in use by the directory service.

**LDAP successful binds/sec**

The number of LDAP bindings (per second) that occurred successfully.

This counter should show activity over time. If it does not, it usually indicates that network-related problems are occurring.

**LDAP searches/sec**

The number of search operations per second performed by LDAP clients.

This counter should show activity over time. If it does not, it usually indicates that network problems are hindering client requests.

**Directory Services directory reads/sec**

The number of directory reads per second.

**Directory Services directory writes/sec**

The number of directory writes per second.

**DRA pending replication synchronizations**

The number of directory synchronizations that are queued for this server but not yet processed.

**Context switches/sec**

Used to determine if the processor handles an excessive amount of applications.
Interpret this data cautiously. A thread that is heavily using the processor lowers the rate of context switches because it does not allow much processor time for other process threads. A high rate of context switching means that the processor is being shared repeatedly—for example, by many threads of equal priority. It is a good practice to minimize the context switching rate by reducing the number of active threads on the system. The use of thread pooling, I/O completion ports, and asynchronous I/O can reduce the number of active threads. Consult your in-house developers or application vendors to determine if the applications you are running provide tuning features that include limiting the number of threads.

A context switching rate of 300 per second per processor is a moderate amount; a rate of 1000 per second or more is high. Values at this high level may be a problem.

You can provide a value for the warning and critical thresholds based on your current environment and your requirements.

**Processor Queue Length**

Indicates if the system can handle processing requests.

This counter is a rough indicator of the number of threads each processor is servicing. The processor queue length, sometimes called processor queue depth, reported by this counter is an instantaneous value that is representative only of a current snapshot of the processor, so it is necessary to observe this counter over a long period of time.

This counter reports a total queue length for all processors, not a length per processor. To learn more, see [http://technet.microsoft.com/en-us/library/cc938643.aspx](http://technet.microsoft.com/en-us/library/cc938643.aspx).

**Distributed File System**

Enables you to group shared folders located on different servers into one or more logically structured namespaces. Each namespace appears to users as a single shared folder with a series of subfolders.

**DNS Server**

Enables DNS clients to resolve DNS names by answering DNS queries and dynamic DNS update requests. If this service is stopped, DNS updates will not occur. If this service is disabled, any services that explicitly depend on it will fail to start.

**Intersite Messaging**

Enables messages to be exchanged between computers running Windows Server sites. If this service is stopped, messages will not be exchanged, nor will site routing information be calculated for other services. If this service is disabled, any services that explicitly depend on it will fail to start.

**Kerberos Key Distribution Center**

On domain controllers, this service enables users to log on to the network using the Kerberos authentication protocol. If this service is stopped on a domain controller, users will be unable to log on to the network. If this service is disabled, any services that explicitly depend on it will fail to start.
Windows Time

Maintains date and time synchronization on all clients and servers in the network. If this service is stopped, date and time synchronization will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

DNS Client

The DNS Client service (dnscache) caches Domain Name System (DNS) names and registers the full computer name for this computer. If the service is stopped, DNS names will continue to be resolved. However, the results of DNS name queries will not be cached and the computer’s name will not be registered. If the service is disabled, any services that explicitly depend on it will fail to start.

Security Accounts Manager

The startup of this service signals other services that the Security Accounts Manager (SAM) is ready to accept requests. Disabling this service will prevent other services in the system from being notified when the SAM is ready, which may in turn cause those services to fail to start correctly. This service should not be disabled.

Server

Supports file, print, and named-pipe sharing over the network for this computer. If this service is stopped, these functions will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

Workstation

Creates and maintains client network connections to remote servers using the SMB protocol. If this service is stopped, these connections will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

Remote Procedure Call (RPC)

The RPCSS service is the Service Control Manager for COM and DCOM servers. It performs object activation requests, object exporter resolutions, and distributed garbage collection for COM and DCOM servers. If this service is stopped or disabled, programs using COM or DCOM will not function properly. It is strongly recommended that you have the RPCSS service running.

Net Logon

Maintains a secure channel between this computer and the domain controller for authenticating users and services. If this service is stopped, the computer may not authenticate users and services, and the domain controller cannot register DNS records. If this service is disabled, any services that explicitly depend on it will fail to start.

Active Directory Domain Services

This is a core AD DS Domain Controller service. If this service is stopped, users will be unable to log on to the network. If this service is disabled, any services that explicitly depend on it will fail to start.
Active Directory Web Services

This service provides a Web Service interface to instances of the directory service (AD DS and AD LDS) that are running locally on this server. If this service is stopped or disabled, client applications, such as Active Directory PowerShell, will not be able to access or manage any directory service instances that are running locally on this server.

AppInsight for Exchange

This template monitors and reports on Microsoft Exchange. The template collects and reports multiple metrics to give a full view in the health, status, and performance of Microsoft Exchange.

Metrics for Database Availability Groups (DAG) are for the entire group, inclusive of all databases. You cannot edit these component monitors to exclude or include specific databases. To monitor specific databases, and not the entire DAG, you may want to review the Exchange templates. These templates provide a starting point for PowerShell scripting options for monitoring database specific metrics.

WMI is the preferred polling method for AppInsight polling. Some information, such as DISK I/O, is tied to volumes only available for nodes managed via WMI.

For details on AppInsight, see AppInsight for Exchange.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

To be added

To display a list of component monitors in the SAM 6.8 RC, navigate to the Manage Application Monitor templates page, select the AppInsight for Active Directory

You can add notes only to the component monitor.

DAG info

Collects and provides Database Availability Group (DAG) information of Exchange servers. This group acts as High Availability for Exchange, grouping Exchange servers and database mount points to fail over or switch to for HA support, performance, and access rules.

You can add notes only to the component monitor.

Replication Status

Collects and provides data for replication status and health checks for active and passive databases in the DAG. The data is displayed in the Replication Status Checks widget, displaying each health check and the status.

You can enable/disable and add notes.

RPC Requests sent/sec

RPC Requests sent/sec is the current rate of initiated RPC requests per second.
You can modify warning and critical thresholds and add notes.

**RPC Slow requests latency average (msec)**

Shows the average latency in ms of slow requests.

You can modify warning and critical thresholds and add notes.

**RPC Slow requests (%)**

RPC Slow requests (%) is the percent of slow RPC requests among all RPC requests.

You can modify warning and critical thresholds and add notes.

**RPP Requests Outstanding**

RPP Requests outstanding shows the total number of outstanding remote operations requests.

You can modify warning and critical thresholds and add notes.

**Database Backup**

Collects data for the database backup service, which performs backup operations.

You can modify warning and critical thresholds and add notes.

**Database Copies**

Collects data for the status of database copies for the monitored Exchange server including: status of the copies, copy queue, replay queue, inspected log time, content index, and activation preference.

You can add notes only to the component monitor.

**Database Copy Queue Length**

Collects data for the copy queue length, showing the number of transaction log files waiting to be copied to the passive copy log file folder.

You can modify warning and critical thresholds and add notes.

**Exchange Information Store Worker Process**

Collects data for the Worker Processes for databases within the Information Store service.

You can modify enable/disable, fetching method, warning and critical thresholds, and add notes.

**Exchange Search Host Controller**

Collects data for the search host controller, which provides host level deployment and management services for applications.

You can modify enable/disable, fetching method, warning and critical thresholds, and add notes.

**Exchange Active Directory Topology**

Collects data for the active directory topology service, which provides active directory topology information to several Exchange Server components.

You can modify enable/disable, fetching method, warning and critical thresholds, and add notes.
Exchange Anti-spam Update
Collects status and data for the anti-spam update service.
You can modify enable/disable, fetching method, warning and critical thresholds, and add notes.

Exchange Mailbox Transport Delivery
Collects status and data for the mailbox transport delivery service, which receives and submit emails for processing and committing to the mailbox database.
You can modify enable/disable, fetching method, warning and critical thresholds, and add notes.

Exchange Diagnostics
Collects status and data for the diagnostics service, which monitors server health for Exchange.
You can modify enable/disable, fetching method, warning and critical thresholds, and add notes.

Exchange EdgeSync
Collects status and data for the EdgeSync service, which replicates configuration and recipient data from the Hub Transport servers to the Edge Transport servers.
You can modify enable/disable, fetching method, warning and critical thresholds, and add notes.

Exchange Search
Collects status and data for the search service, which drives indexing and querying of data for Exchange.
You can modify enable/disable, fetching method, warning and critical thresholds, and add notes.

Exchange Health Manager
Collects status and data for the health manager service, which provides server health status.
You can modify enable/disable, fetching method, warning and critical thresholds, and add notes.

Exchange IMAP4 Backend
Collects status and data for the IMAP4 service to mailboxes.
You can modify enable/disable, fetching method, warning and critical thresholds, and add notes.

Exchange Information Store
Collects data for the Information Store service that controls all of the Store Worker processes for databases.
You can modify enable/disable, fetching method, warning and critical thresholds, and add notes.

Exchange Mailbox Assistants
Collects data for the mailbox assistant service, which performs background processing of mailboxes in the Exchange store.
You can modify enable/disable, fetching method, warning and critical thresholds, and add notes.
Exchange Mailbox Replication
Collects data for the mailbox replication service, which manages mailbox move requests.
You can modify enable/disable, fetching method, warning and critical thresholds, and add notes.

Exchange Monitoring
Collects data for the monitoring service, which allows applications to call the Exchange diagnostic cmdlets.
You can modify enable/disable, fetching method, warning and critical thresholds, and add notes.

Exchange POP3 Backend
Collects data for the POP3 backend service, which provides the POP3 service to the mailboxes.
You can modify enable/disable, fetching method, warning and critical thresholds, and add notes.

Exchange Replication
Collects data for the replication process for mailbox databases on Mailbox servers in a DAG and database mount functionality for all Mailbox servers.
You can modify enable/disable, fetching method, warning and critical thresholds, and add notes.

Exchange RPC Client Access
Collects data for the RPC client access service, which manages client RPC connections for Exchange.
You can modify enable/disable, fetching method, warning and critical thresholds, and add notes.

Exchange Service Host
Collects data for the host for Exchange services (internal and external servers).
You can modify enable/disable, fetching method, warning and critical thresholds, and add notes.

Exchange Mailbox Transport Submission
Collects data for the mailbox transport submission service running on mailbox servers, which receives the Submit events, processing messages by converting from MAPI to MIME, and provides them over to the Exchange Transport service.
You can modify enable/disable, fetching method, warning and critical thresholds, and add notes.

Exchange Throttling
Collects data for the throttling service, limiting the rate of user operations.
You can modify enable/disable, fetching method, warning and critical thresholds, and add notes.

Exchange System Attendant
Collects data for the system attendant service, which forwards directory lookups to a global catalog server for legacy Outlook clients, generates email addresses and OABs, updates free/busy information for legacy clients, and maintains permissions and group memberships for the server.
You can modify enable/disable, fetching method, warning and critical thresholds, and add notes.
Exchange Search Indexer

Collects data for the search indexer service, which drives indexing of mailbox content.

You can modify enable/disable, fetching method, warning and critical thresholds, and add notes.

Search (Exchange)

Collects data for the Microsoft Exchange customized version of Microsoft Search. This service creates full-text indexes on content and properties of structured and semi-structured data for quick linguistic searches on this data.

You can modify enable/disable, fetching method, warning and critical thresholds, and add notes.

Exchange Migration Workflow

Collects data for the Exchange Migration Workflow service. You may have this service disabled in the Microsoft Exchange application and may not be relevant. If you have this service disabled, you could disable the component monitor not to display in the AppInsight for Exchange view.

You can modify enable/disable, fetching method, warning and critical thresholds, and add notes.

Exchange DAG Management

Collects data for Database Availability Groups in your Exchange environment.

You can modify enable/disable, fetching method, warning and critical thresholds, and add notes.

Exchange Transport

Collects data for the transport service, routing messages between the Mailbox Transport Submission server and the Front End Transport service. The services does not contact the mailbox database directory.

You can modify enable/disable, fetching method, warning and critical thresholds, and add notes.

Exchange Transport Log Search

Collects data for the remote search capability for Exchange Transport log files.

You can modify enable/disable, fetching method, warning and critical thresholds, and add notes.

Exchange Unified Messaging

Collects data for the unified messaging service, which enables voice and fax messages to be stored in Exchange and gives users telephone access to email, voice mail, calendar, contacts, and auto attendant.

You can modify enable/disable, fetching method, warning and critical thresholds, and add notes.

Exchange Server Extension for Windows Server Backup

Collects data for the server extension for Windows Server backup, which enables the server backup users to back up and recover application data for Exchange.

You can modify enable/disable, fetching method, warning and critical thresholds, and add notes.
Exchange Mail Submission
- Collects data for the mail submission service, which submits messages from the mailbox server to the Exchange hub transport servers (according to version).
- You can modify enable/disable, fetching method, warning and critical thresholds, and add notes.

Cluster Service
- Collects data for the cluster service on the DAG or the local server if a DAG is not used.
- You can modify enable/disable, fetching method, warning and critical thresholds, and add notes.

Connection Count
- Is the total number of client connections maintained.
- You can modify warning and critical thresholds and add notes.

Active User Count
- Number of user connections that have shown some activity in the last 2 minutes.
- You can modify warning and critical thresholds and add notes.

RPC Requests
- Indicates the overall RPC requests currently executing within the information store process.
- You can modify warning and critical thresholds and add notes.

RPC Averaged Latency
- Indicates the RPC latency, in ms, averaged for all operations in the last 1,024 packets.
- You can modify warning and critical thresholds and add notes.

Active Connection Count
- Number of connections that have shown some activity in the last 10 minutes.
- You can modify warning and critical thresholds and add notes.

Active User Account
- Number of unique users which have performed some activity on the server within the last 10 minutes.
- You can modify warning and critical thresholds and add notes.

RPC Client Backoff/sec
- The rate at which the server notifies a client to withdraw (backoff).
- You can modify warning and critical thresholds and add notes.
Client: RPCs Failed: Server Too Budy/sec

Shows the client-reported rate of failed RPCs (since the store was started) due to the Server Too Busy ROC error. Should be 0 at all times. This counter is only available in Exchange 2010 and Exchange 2016.

You can modify warning and critical thresholds and add notes.

Possible Issues: Higher values may indicate RPC threads are exhausted or client throttling is occurring for clients running versions of Outlook earlier than Microsoft Office Outlook 2007. This can cause user mail clients experiencing slowness.

Resolution: Check if RPC latencies are high and determine the cause of the performance issue (e.g. poorly performing disk I/O, excessive load, insufficient memory, high number of users).

Active Client Logins

Number of logons that are active (issued any MAPI requests) within the last 10 minute time interval. Active client logons can be high if users are logging on and logging off frequently. This counter is only available in Exchange 2010 and 2016.

You can modify warning and critical thresholds and add notes.

Possible Issue: May cause memory bottlenecks on the server if the number is excessively high.

Resolution: Determine if users are running applications not required for business use, and request they do not run these applications which is causing an increase in server logons. If this does not help, or is not possible, reduce the number of server hosted on the server and move any Public Folders on the server to a different server.

Slow Find Rate

Shows the rate at which the slower FindRow needs to be used in the mailbox store. This monitor should be no more than 10 for any specific mailbox store. This counter is only available in Exchange 2010 and 2016.

You can modify warning and critical thresholds and add notes.

Possible Issue: Higher values indicate applications are crawling or searching mailboxes, which is affecting server performance. These include desktop search engines, customer relationship management (CRM), or other third-party applications.

Resolution: Run the ResetSearchIndex.ps1 script which is located in the scripts directory at the root of the Exchange installation. Alternatively, you can perform the process manually:

1. Rebuild index catalog using Update-MailboxDatabaseCopy $DBName -CatalogOnly command.
2. Stop the Microsoft Exchange Search Service.
3. Delete old catalog files.
**Database Cache Size (MB)**

Shows the amount of system memory, used by the database cache manager to hold commonly used information from the database files to prevent file operations. This and Database Cache Hit % are useful counters for gauging whether a server's performance problems might be resolved by adding more physical memory. Use this counter along with store private bytes to determine if there are store memory leaks.

You can modify warning and critical thresholds and add notes.

Possible issues: Situation when the database cache size seems too small for optimal performance and there is little available memory on the system (check the value of Memory/Available Bytes) could negatively impact on performance. If there is ample memory on the system and the database cache size is not growing beyond a certain point, the database cache size may be capped at an artificially low limit. Increasing this limit may increase performance.

Resolution: Adding more memory to the system and/or increasing database cache size may increase performance.

**Database Page Fault Stalls/sec**

Shows the rate that database file page requests require of the database cache manager to allocate a new page from the database cache. The value should be 0 at all times.

You can modify warning and critical thresholds and add notes.

Possible issues: If this value is nonzero, this indicates that the database is not able to flush dirty pages to the database file fast enough to make pages free for new page allocations.

Resolution: If the disk subsystem is not meeting demand, correcting the problem may require additional disks, faster disks, or modifying the disk configuration.

**Version buckets allocated**

Shows the total number of version buckets allocated. The value should be less than 12,000 at all times. The maximum default version is 16,384. If version buckets reach 70% of maximum, the server is at risk of running out of the version store.

You can modify warning and critical thresholds and add notes.

Possible issues: Typically indicates a database transaction which is taking a long time to save to disk. During Online database defrags, the version buckets may increase.

Resolution: Verify if the server has any applications running that have a long running transaction which has not been saved to disk, causing the version store memory resource to be exhausted.

**Log Record Stalls/sec**

Shows the number of log records that cannot be added to the log buffers per second because the log buffers are full. If this counter is nonzero for a long period of time, the log buffer size may be in a bottleneck situation. The average value should be below 10 per second. Spikes (maximum values) should not be higher than 100 per second.

You can modify warning and critical thresholds and add notes.
Possible issues: Check for high I/O log write latencies. Check disk configuration (RAID/JBOD) and performance. Check RPC counters for high latency.

Resolution: You can also use the MSExchange Database Instances (Information store/${Database Name})\log record stalls/sec counter to determine which database(s) may be having issues. This will assist you in determining which drive(s) to focus on. This counter is an extended Exchange counter in Performance Monitor. Solution can include additional disks, reconfigured RAID configuration, adding new database(s), or rebalancing mailboxes across databases or servers.

Log Threads Waiting

Shows the number of threads waiting for their data to be written to the log to complete an update of the database. If this number is too high, the log may be a bottleneck. This value should be less than 10 on average.

You can modify warning and critical thresholds and add notes.

Possible issues: If this number is too high, the log may be a bottleneck. Regular spikes concurrent with log record stall spikes indicate that the transaction log disks are a bottleneck. If the value for log threads waiting is more than the spindles available for the logs, there is a bottleneck on the log disks.

Resolution: If the disk subsystem is not meeting demand, correcting the problem may require additional disks, faster disks, or modifying the disk configuration.

RPC Requests failed (%)

Shows the percentage of failed requests in the total number of RPC requests. Failed means the sum of failed with error code plus failed with exception. Value should be less than 1 at all times

You can modify warning and critical thresholds and add notes.

Possible issues: Users may report slow performance, disconnects, or failures within their client performing certain activities.

Resolution: Review the Windows Event logs for any related events. Use ExBPA to perform a Health scan of your server and review any issues reported. In Exchange 2010, verify SP 1 or higher is installed on your system.

RPC Requests outstanding

Shows the current number of outstanding RPC requests. Value should be 0 at all times.

You can modify warning and critical thresholds and add notes.

Possible issues: Server may stop accepting RPC requests.

Resolution: Review the Windows Event logs for any related events. Use ExBPA to perform a Health scan of your server and review any issues reported. Use Exchange Server User Monitor application to review user sessions. In Exchange 2010, verify SP 1 or higher is installed on your system.

RPC Latency average (msec)

Shows the average latency, in ms, of RPC requests. The average is calculated over all RPCs since exrpc32 was loaded. Should be less than 100 ms at all times.

You can modify warning and critical thresholds and add notes.
Possible issues: Users may report slow performance issues.

Resolution: If the disk subsystem is not meeting demand, correcting the problem may require additional disks, faster disks, or modifying the disk configuration.

**Hub Servers In Retry**

Shows the number of Hub Transport servers in retry mode. The value should be 0 at all times. This counter is only available in Exchange 2010 and 2016.

You can modify warning and critical thresholds and add notes.

Possible issues: An external domain where you send a large amount of e-mail is unavailable/unresponsive due to DNS resolution or network connectivity issues to the destination servers. Another possibility is a virally infected machine on your network sending messages.

Resolution: Determine the root cause and verify there are not any network connectivity issues.

**CopyQueueLength**

The copy queue length is an integer indicating number of files. Shows the number of transaction log files waiting to be copied to the passive copy log file folder. A copy isn't considered complete until it has been checked for corruption. All nodes in a Database Availability Group (DAG) should be monitored for this counter depending on the passive node. Should be less than 1 at all times for continuous replication.

You can modify warning and critical thresholds and add notes.

Possible issues: Server recently rebooted or services restarted, network connectivity issues, or multiple mailbox moves are in process.

Resolution: Verify network connectivity between the various nodes in the DAG. Verify Replication Service is running on all DAG members.

**ReplayQueueLength**

Shows the number of transaction log files waiting to be replayed into the passive copy. With DAG replication, transaction logs are shipped to the other DAG members. They then replay the log file.

1. Thresholds should be manually removed for DAG members configured to be 'lagged copies'.

You can modify warning and critical thresholds and add notes.

Possible issues: The replay queue length should be as low as possible, otherwise this could indicate a (performance) issue with the DAG member containing the Copy database. A high number could also negatively affect failover with some loss of data as a possibility.

Resolution: Check Memory, CPU, and Disk I/O for any bottlenecks. Review the Windows Event logs for any related events.
Avg Log Copy Latency (msec)

Average number of milliseconds observed by the log copier when sending messages over the network. No additional information is available for this counter. This counter is only available in Exchange 2010 and 2016.

You can modify warning and critical thresholds and add notes.

Log Copy KB/sec

The size of the log files (in KB) that are copied per second. The value shows the size in KB/sec of the transaction logs being copied to passive copies.

You can modify warning and critical thresholds and add notes.

Log Replay Rate (generations/sec)

The number of log files that are replayed per second. Value shows the number of Transaction Logs being replayed on the passive copies of a database.

You can modify warning and critical thresholds and add notes.

Log Replay is Not Keeping Up

LogReplayNotKeepingUp is 1 when log replay is falling behind and not able to keep up with log copying and inspection. Exchange 2010/2013 uses continuous replication to create and maintain database copies. To maintain a synchronized copy of a mailbox database, transaction log files from the active mailbox server are replayed into the passive database of another server in the DAG. This provides high availability and resiliency in the Exchange environment.

You can modify warning and critical thresholds and add notes.

Possible issues: Indicates a replication issue may exist with the mailbox database copies in the DAG. If Transaction Log replay isn't able to keep up with the active copy, passive copies will not be up to date.

Resolution: Review the Windows Event logs for any related events. Examine network topology between DAG members and verify connectivity and network latency is below 250 ms. Examine CPU utilization by the Information Store service on passive copies. Examine the replication status for each replica database using the Get-MailboxDatabaseCopyStatus cmdlet.

Average Calendar Attendant Processing Time

Shows the average time to process an event in the Calendar Attendant. Value should be a relatively low value at all times.

You can modify warning and critical thresholds and add notes.

Possible issues: High values may indicate a performance bottleneck.

Resolution: Check Memory & CPU for any bottlenecks. Review Event logs for related events examining log entries for each Assistants Infrastructure and its corresponding assistant. Use the Exchange Troubleshooting Assistant (ExTRA) to obtain Event Tracing for Windows traces.
Calendar Attendant Requests Failed

Shows the total number of failures that occurred while the Calendar Attendant was processing events. (1) Value should be 0 at all times.

You can modify warning and critical thresholds and add notes.

Average Resource Booking Processing Time

Shows the average time to process an event in the Resource Booking Attendant. Value should be a relatively low value at all times.

You can modify warning and critical thresholds and add notes.

Possible issues: High values may indicate a performance bottleneck.

Resolution: Check Memory & CPU for any bottlenecks. Review Event logs for related events examining log entries for each Assistants Infrastructure and its corresponding assistant. Use the Exchange Troubleshooting Assistant (ExTRA) to obtain Event Tracing for Windows traces.

Resource Booking Requests Failed

Shows the total number of failures that occurred while the Resource Booking Attendant was processing events. Value should be 0 at all times.

You can modify warning and critical thresholds and add notes.

Possible issues: Meeting Room bookings or updates may not be processed for some users.

Resolution: Review Event logs for related events examining log entries for each Assistants Infrastructure and its corresponding assistant. Use the Exchange Troubleshooting Assistant (ExTRA) to obtain Event Tracing for Windows traces. Verify your resource mailboxes are properly configured.

Mailboxes Processed/sec

Shows the rate of mailboxes processed by time-based assistants per second. Value determines current load statistics for this counter.

You can modify warning and critical thresholds and add notes.

Active Client Logons

The number of clients that performed any action within the last 10 minute interval. Active client logons can be high if users are logging on and logging off frequently.

You can modify warning and critical thresholds and add notes.

Possible issues: May cause memory bottlenecks on the server if the number is excessively high.

Resolution: Determine if users are running applications not required for business use, and request they do not run these applications which is causing an increase in server logons. If this does not help, or is not possible, reduce the number of server hosted on the server and move any Public Folders on the server to a different server.
**Slow Findrow Rate**

Shows the rate at which the slower FindRow needs to be used in the mailbox store. Value should be no more than 10 for any specific mailbox store.

You can modify warning and critical thresholds and add notes.

Possible issues: Higher values indicate applications are crawling or searching mailboxes, which is affecting server performance. These include desktop search engines, customer relationship management (CRM), or other third-party applications.

Resolution: Run the `ResetSearchIndex.ps1` script which is located in the scripts directory at the root of the Exchange installation. Alternatively, you can perform the process manually:

1. Rebuild index catalog using `Update-MailboxDatabaseCopy ${DBName} -CatalogOnly` command.
2. Stop the Microsoft Exchange Search Service.
3. Delete old catalog files.

**I/O Database Reads Average Latency**

Shows the average length of time, in ms, per database read operation.

- Exchange 2010 and 2016: Should be 20 ms on average. Spikes should not exceed 50 ms.
- Exchange 2013: Should be 50 ms on average. Spikes of up to 100 ms are acceptable if not accompanied by database page fault stalls.

You can modify warning and critical thresholds and add notes.

Possible issues: Users may experience decreased performance, including delayed message deliveries.

Resolution: If the disk subsystem is not meeting demand, correcting the problem may require additional disks, faster disks, or modifying the disk configuration. Review the Event logs for related events. Verify network topology between mailbox servers & storage resources. Examine CPU & Memory usage to determine possible bottlenecks. Examine replication status for replica database.

**I/O Database Writes Average Latency**

Shows the average length of time, in ms, per database write operation.

You can modify warning and critical thresholds and add notes.

For more information, list of counters and definition for each was retrieved from Microsoft TechNet (http://technet.microsoft.com/en-us/library/ff367871(v=exchg.141).aspx).

Should be 50 ms on average. Spikes of up to 100 ms are acceptable if not accompanied by database page fault stalls.
**I/O Log Reads Average Latency**

Indicates the average time, in ms, to read data from a log file. Specific to log replay and database recovery operations. Average should be less than 200 ms with spikes up to 1000 ms.

You can modify warning and critical thresholds and add notes.

Possible issues: Users may experience decreased performance, including delayed message deliveries.

Resolution: If the disk subsystem is not meeting demand, correcting the problem may require additional disks, faster disks, or modifying the disk configuration. Review the Event logs for related events. Verify network topology between mailbox servers & storage resources. Examine CPU & Memory usage to determine possible bottlenecks. Examine replication status for replica database.

**I/O Log Wrties Average Latency**

Indicates the average time, in ms, to write a log buffer to the active log file. This count should be 10 ms or less on production servers.

You can modify warning and critical thresholds and add notes.

Possible issues: Indication that the MSExchange Database\I/O Database Writes Average Latency is too high

Resolution: If the disk subsystem is not meeting demand, correcting the problem may require additional disks, faster disks, or modifying the disk configuration. Review the Event logs for related events. Verify network topology between mailbox servers & storage resources. Examine CPU & Memory usage to determine possible bottlenecks. Examine replication status for replica database.

**Log Threads Waiting**

Shows the number of threads waiting for their data to be written to the log to complete an update of the database. If this number is too high, the log may be a bottleneck. Value should be less than 10 on average.

You can modify warning and critical thresholds and add notes.

Possible issues: If this number is too high, the log may be a bottleneck. Regular spikes concurrent with log record stall spikes indicate that the transaction log disks are a bottleneck. If the value for log threads waiting is more than the spindles available for the logs, there is a bottleneck on the log disks.

Resolution: If the disk subsystem is not meeting demand, correcting the problem may require additional disks, faster disks, or modifying the disk configuration. Review the Event logs for related events. Verify network topology between mailbox servers & storage resources. Examine CPU & Memory usage to determine possible bottlenecks.

**Messages Sent/sec**

Shows the rate that messages are sent to transport. Value is used to determine current messages sent to transport.

You can modify warning and critical thresholds and add notes.
Messages Delivered/sec

Shows the rate that messages are delivered to all recipients. Value indicates current message delivery rate to the store.

You can modify warning and critical thresholds and add notes.

Average Event Processing Time In Seconds

Shows the average processing time of the events chosen. Value should be less than 2 at all times.

You can modify warning and critical thresholds and add notes.

Possible issues: Indicates the Mail Submission Assistant isn't able to handle the number of submission requests being made to the database. May occur when server is experiencing a heavy load which can cause messages to queue on the server.

Resolution: Review Event logs for related events examining log entries for each Assistants Infrastructure and its corresponding assistant.

Events in queue

Shows the number of events in the in-memory queue waiting to be processed by the assistants. Value should be a low value at all times.

You can modify warning and critical thresholds and add notes.

Possible issues: High values may indicate a performance bottleneck.

Resolution: Review Event logs for related events. Monitor CPU & Memory for bottlenecks.

Events Polled/sec

Shows the number of events polled per second. Value determines current load statistics for this counter.

You can modify warning and critical thresholds and add notes.

Exchange Event Log Monitor

Shows the event log for the Exchange server.

You can modify component status based on event ID, warning and critical thresholds, and add notes.

Database File And Transaction Logs Dir Info

Provides information on the directory for the database file and transaction logs. The transaction log can increase in size requiring management and monitoring for performance and consumed space.

You can modify warning and critical thresholds and add notes.

Server Mailboxes

Collects and provides data for all mailboxes on an Exchange server.

You can modify warning and critical thresholds and add notes.

Server Mailboxes Statistics

Collects and provides statistics for mailboxes on an Exchange server.
You can modify enable/disable and add notes.

**Server Mailbox Account Statistics**

Collects and provides data for mailbox accounts, including messages sent and received. This data is used by the Server Mailbox Account Statistics, Messages Sent, and Messages Received widgets display this data.

You can modify enable/disable and add notes.

**I/O Database Reads Average Latency**

Shows the average length of time, in ms, per database read operation. The value should be 20 ms on average. Spikes should not exceed 50 ms.

You can modify warning and critical thresholds and add notes.

Possible issues: Users may report sluggish responsiveness within their email client.

Resolution: If the disk subsystem is not meeting demand, correcting the problem may require additional disks, faster disks, or modifying the disk configuration.

**I/O Database Writes Average Latency**

Shows the average length of time, in ms, per database write operation. The value should be 50 ms on average. Spikes of up to 100 ms are acceptable if not accompanied by database page fault stalls.

You can modify warning and critical thresholds and add notes.

Possible issues: Users may report sluggish responsiveness within their email client.

Resolution: If the disk subsystem is not meeting demand, correcting the problem may require additional disks, faster disks, or modifying the disk configuration.

**I/O Log Reads Average Latency**

Indicates the average time, in ms, to read data from a log file. This is specific to log replay and database recovery operations. The average value should be less than 200 ms with spikes up to 1000 ms.

You can modify warning and critical thresholds and add notes.

Possible issues: Users may report sluggish responsiveness within their email client.

Resolution: If the disk subsystem is not meeting demand, correcting the problem may require additional disks, faster disks, or modifying the disk configuration.

**I/O Log Writes Average Latency**

Indicates the average time, in ms, to write a log buffer to the active log file. This count value should be 10 ms or less on production servers.

You can modify warning and critical thresholds and add notes.

Possible issues: Indication that the MSExchange Database\I/O Database Writes Average Latency is too high.
Resolution: If the disk subsystem is not meeting demand, correcting the problem may require additional disks, faster disks, or modifying the disk configuration.

Performance counters

This section provides performance counters included in the AppInsight for Exchange template.

Category: \MSExchange Store Interface(_Total)\n
- RPC Requests sent/sec
- RPC Slow requests latency average (msec)
- RPC Slow requests (%)
- ROP Requests Outstanding
- RPC Requests failed (%)
- RPC Requests outstanding
- RPC Latency average (msec)

Category: \MSExchange RpcClientAccess\n
- Connection Count
- Active User Count
- RPC Requests
- RPC Averaged Latency

Category: \MSExchange Database(Information Store)\n
- Database Cache Size (MB)
- Database Page Fault Stalls/sec
- Version buckets allocated
- Log Record Stalls/sec
- Log Threads Waiting

Category: \MSExchange Replication(_total)\n
- CopyQueueLength
- ReplayQueueLength
- Log Copy KB/sec
- Log Replay Rate (generations/sec)
- Log Replay is Not Keeping Up

Category: \MSExchange Calendar Attendant\n
- Average Calendar Attendant Processing Time
- Calendar Attendant Requests Failed
Category: \MSExchange Resource Booking

- Average Resource Booking Processing Time
- Resource Booking Requests Failed

Category: \MSExchange Database ==> Instances(information store/_Total)\n
- I/O Database Reads Average Latency
- I/O Database Writes Average Latency
- I/O Log Reads Average Latency
- I/O Log Writes Average Latency

**ApplInsight for IIS**

ApplInsight template for monitoring IIS instances. This Template helps you to monitor health of your whole IIS instance. For details on ApplInsight, see [ApplInsight for IIS](#).

**Prerequisites**

- WMI access to target server.

**Monitored Components**

For details on monitors, see [SAM Component Monitor Types](#).

**Application Pools**

Collects the status of all monitored application pools for the IIS application.

Due to dependencies, you can only add notes. Values cannot be modified.

**Sites**

Collects the status of all monitored sites for the IIS application.

Due to dependencies, you can only add notes. Values cannot be modified.

**Site Bindings Monitor**

Collects the data for site bindings, including the type of HTTP or HTTPS, IP address, and ports.

Due to dependencies, you can only add notes. Values cannot be modified.

**Worker Process Statistic Monitor**

Collects and provides data and status of the worker process activation service for an application pool. This information includes the number of processes running in the application pool, recent failures of the process in the pool, total pool recycles since the service was started, total ping failures, total shutdown failures, and total startup failures.

You can modify the thresholds for this monitor.
Log Parsing Monitor

Collects and displays log data for the AppInsight for IIS log.

You can modify the thresholds for this monitor.

Total Connection Attempts

The total number of connections to the Web or FTP service attempted since service startup. The count is the total for all Web sites or FTP sites combined, regardless of what you choose for Instance. This number does not include connection attempts that failed at the TCP (transport) or IP (network) layer.

You can modify the thresholds for this monitor.

Total Logon Attempts

The total number of successful logons to the Web or FTP service since the service started. Value does not include failed logon attempts.

You can modify the thresholds for this monitor.

Current Connections

Current Connections is the current number of connections established with the Web service. This is the sum of both non-anonymous (authenticated) and anonymous (unauthenticated) users.

You can modify the thresholds for this monitor.

Possible issues: If this number is at or near the maximum connections allowable, the Web service is at full capacity.

Resolution: If the value is too high for a particular IIS server, then load balancing or clustering technologies can be applied to lower the burden of the server in question. Also check the Web Site property page for maximum connection limit.

Current Anonymous users

Current Anonymous Users is the number of users who currently have an anonymous connection using the Web service. If anonymous connections are not permitted on the server, the value of all anonymous user counters is always zero.

You can modify the thresholds for this monitor.

Current NonAnonymous Users

Current NonAnonymous Users is the number of users who currently have a non-anonymous connection using the Web service. If authentication is not enabled on the server, and none of the applications that run on the server request or require authentication, then the value of all non-anonymous user counters is always zero.

You can modify the thresholds for this monitor.
**Total Connection Attempts**

The total number of connections to the Web or FTP service that have been attempted since service startup. The count is the total for all Web sites or FTP sites combined, regardless of what you choose for Instance. This number does not include connection attempts that failed at the TCP (transport) or IP (network) layer.

You can modify the thresholds for this monitor.

**Total Logon Attempts**

The total number of successful logons to the Web or FTP service since the service started. Value does not include failed logon attempts.

You can modify the thresholds for this monitor.

**Total Bytes Received**

The total bytes of data that have been received by the WWW service since the service started. This information can be used to determine network load on a specific Web site.

You can modify the thresholds for this monitor.

**Total Bytes Sent**

The number of data bytes that have been sent by the WWW service since the service started. This information can be used to determine network load on a specific Web site.

You can modify the thresholds for this monitor.

**Total Bytes Transferred**

The total number of bytes of data that have been sent and received by the WWW service since the service started. This information can be used to determine network load on a specific Web site.

You can modify the thresholds for this monitor.

**HTTP Bindings Monitor**

A performance counter, displays the response time for loading the HTTP Bindings and testing the web server's ability to accept incoming sessions and transmit the requested page.

You can modify all settings.

**HTTPS Bindings Monitor**

A performance counter, displays the response time for loading the HTTPS Bindings and testing the web server's ability to accept incoming sessions and transmit the requested page.

You can modify all settings.

**SSL Certificate Monitor**

This component monitor tests a web server’s ability to accept incoming sessions over a secure channel and then test the security certificate.

You can modify the thresholds for this monitor.
Site Directory Info Monitor

Provides site directory information for the Exchange server.
You can modify the thresholds for this monitor.

Site Log Directory Monitor

Provides site log directory information for the Exchange server.
You can modify the thresholds for this monitor.

Windows Process Activation Service

Collects data from the Windows process activation service.
You can modify the thresholds for this monitor.

World Wide Web Publishing Service

Collects data and status from the W3Svc service. This is used for Internet access.
You can modify the thresholds for this monitor.

Web Management Service

Collects data and status from the Web Management Service. This is used for authentication.
You can modify the thresholds for this monitor.

ASP.NET State Service

Collects and provides status data for all ASP.NET IIS application requests that contain all the websites for the current application.
You can modify all settings.

Application Host Helper Service

Collects and provides data from the Application Host Helper Service, which enables IIS configuration history and application pool SID (security identifier) mapping. It enables the configuration history functionality by saving the ApplicationHost.config file to separate configuration history subdirectories at set intervals.
You can modify all settings.

IIS Event Log Monitor

Collects and displays IIS events.
You can modify settings, but cannot disable this monitor.

Current File Cache Memory Usage

Current number of bytes used for the user-mode file cache.
You can modify the thresholds for this monitor.

Output Cache Current Memory Usage

Current memory usage by output cache.
You can modify the thresholds for this monitor.

**File Cache Hits %**

The ratio of user-mode file cache hits to the total number of cache requests since the service started.

This counter reflects how well the settings for the IIS file cache are working. A site with mostly static files should have a very high cache hit percentage (70%-85%). If the Kernel: Cache Hits % counter is low, this value should be high. Note that this counter does not include dynamic content, only static files. If your static files are not being cached, you might want to lengthen the activity period for this cache.

You can modify the thresholds for this monitor.

Possible issues: The value returned from Kernel: Cache Hits % is low.

Resolution: Examine your file set and determine why your files are not being cached.

**Kernel: URI Cache Hits %**

The ratio of kernel URI cache hits to the total number of cache requests since the service started.

You can modify the thresholds for this monitor.

**Metadata Cache Hits %**

The ratio of user-mode metadata cache hits to total number of cache request since the service started.

You can modify the thresholds for this monitor.

**Output Cache Current Hits %**

Output cache current hit ratio. The ratio is calculated as \( \frac{H}{H+M} \), where \( H \) and \( M \) represent Hits and Misses in previous sample intervals, respectively.

You can modify the thresholds for this monitor.

**URI Cache Hits %**

The ratio of user-mode URI Cache Hits to the total number of cache requests since the service started.

If content cannot be cached in the HTTP.sys response cache, the value of this counter should be as high as possible. If your content can be stored in the HTTP.sys response cache, the value of this counter should be low.

You can modify the thresholds for this monitor.

**Active Requests**

Current number of requests being processed by the worker process.

You can modify the thresholds for this monitor.

**Requests / Sec**

HTTP requests/sec being processed by the worker process.
You can modify the thresholds for this monitor.

**Active Threads Count**
Number of threads actively processing requests in the worker process.
You can modify the thresholds for this monitor.

**Current Worker Processes**
The current number of worker processes that are running in the application pool.
You can modify the thresholds for this monitor.

**Recent Worker Process Failures**
The number of times that the worker process for the application pool failed during the rapid-fail protection interval. Value should be count as difference with threshold greater than 0.
You can modify the thresholds for this monitor.

**Total Application Pool Recycles**
The number of times that the application pool has been recycled since Windows Process Activation Service (WAS) started. Value should be count as difference with threshold greater than 0.
You can modify the thresholds for this monitor.

**Total Worker Process Failures**
The number of times that worker processes have crashed since the application pool was started.
Value should be count as difference with threshold greater than 0.
You can modify the thresholds for this monitor.

**Total Worker Process Ping Failures**
The number of times that Windows Process Activation Service (WAS) did not receive a response to ping messages sent to a worker process. Value should be count as difference with threshold greater than 0.
You can modify the thresholds for this monitor.

**Total Worker Process Shutdown Failures**
The number of times that Windows Process Activation Service (WAS) failed to shut down a worker process. Value should be count as difference with threshold greater than 0.
You can modify the thresholds for this monitor.

**Total Worker Process Startup Failures**
The number of times that Windows Process Activation Service (WAS) failed to start a worker process.
Value should be count as difference with threshold greater than 0.
You can modify the thresholds for this monitor.
Maximum File Cache Memory Usage

Maximum number of bytes used by the user-mode file cache since service startup. The value of this counter and the value of Web Service Cache\Current File Cache Memory Usage should be the same.

You can modify the thresholds for this monitor.

Possible issues: If the numbers are different, the cache was flushed. If this counter is significantly higher than Web Service Cache\Current File Cache Memory Usage, you might consider recycling the worker process because the application might have a memory leak.

File Cache Hits

Total number of successful lookups in the user-mode file cache since service startup. Value depends on content. If the content files cannot be cached by HTTP.sys, a high value is good.

You can modify the thresholds for this monitor.

File Cache Misses

Total number of unsuccessful lookups in the user-mode file cache since service startup. A file cache miss means the request for the file must go to the hard disk.

You can modify the thresholds for this monitor.

Possible issues: File cache misses negatively impact performance and scalability. This value should be as low as possible. Also note that kernel cache hits will cause this value to be low.

Metadata Cache Hits

Total number of successful lookups in the user-mode metadata cache since service startup.

You can modify the thresholds for this monitor.

Metadata Cache Misses

Total number of unsuccessful lookups in the user-mode metadata cache since service startup. Value should be as low as possible.

You can modify the thresholds for this monitor.

Output Cache Total Hits

Total number of successful lookups in the output cache since service startup.

You can modify the thresholds for this monitor.

Output Cache Total Misses

Total number of unsuccessful lookups in the output cache since service startup.

You can modify the thresholds for this monitor.
**URI Cache Hits**

Total number of successful lookups in the user-mode URI cache since service startup. Value depends on content. If content cannot be cached in the `HTTP.sys` response cache, the value of this counter should be as high as possible. If your content can be stored in the `HTTP.sys` response cache, the value of this counter should be low.

You can modify the thresholds for this monitor.

**URI Cache Misses**

Total number of unsuccessful lookups in the user-mode URI cache since service startup.

Low is better. The value of this counter increases when IIS cannot locate requested content in either the `HTTP.sys` response cache or the IIS file cache, and must locate the requested content on the hard disk.

You can modify the thresholds for this monitor.

Possible issues: If the value of this counter is high, IIS locate requested content on hard disk which could slow overall performance.

**Total Method Requests**

The number of HTTP requests that have been made since the WWW service started.

You can modify the thresholds for this monitor.

**Delete Requests**

The number of HTTP requests that have used the DELETE method since the WWW service started.

You can modify the thresholds for this monitor.

**Get Requests**

The number of HTTP requests that have used the GET method since the WWW service started. GET requests are generally used for basic file retrievals or image maps, though they can be used with forms.

You can modify the thresholds for this monitor.

Resolution: If the value is too high for a particular IIS server, then load balancing or clustering technologies can be applied to lower the burden of the server in question.

**Head Requests**

The number of HTTP requests that have used the HEAD method since the WWW service started. HEAD requests typically indicate that a client is querying the state of a document they already have to see if it needs to be refreshed.

You can modify the thresholds for this monitor.
CGI Requests

The number of all CGI requests that have been made since the WWW service started. CGI requests are custom gateway executable (.exe files) the administrator can install to add forms processing or other dynamic data sources. CGI requests spawn a process on the server which can be a large drain on server resources.

You can modify the thresholds for this monitor.

ISAPI Extension Requests

The number of ISAPI extension requests that have been made since the WWW service started. ISAPI Extension Requests are custom gateway DLLs, which the administrator can install to add forms processing or other dynamic data sources.

You can modify the thresholds for this monitor.

Put Requests

The number of HTTP requests that have used the PUT method since the WWW service started.

You can modify the thresholds for this monitor.

Post Requests

The number of HTTP requests that have used the POST method since the WWW service started. Post requests are generally used for forms or gateway requests.

You can modify the thresholds for this monitor.

Resolution: If the value is too high for a particular IIS server, then load balancing or clustering technologies can be applied to lower the burden of the server in question.

Files Received

The number of files that have been received by the WWW service since the service started.

You can modify the thresholds for this monitor.

Files Sent

The number of user-mode files that have been sent by the WWW service since the service started. This counter does not include cache hits. Note that this counter does not increment when files are being served from the kernel-mode cache.

You can modify the thresholds for this monitor.

Files Transferred

The sum of Total Files Sent and Total Files Received by the WWW service since the service started. Note that this counter does not increment when files are being served from the kernel-mode cache.

You can modify the thresholds for this monitor.
Locked Errors

The number of requests that have been made since the service started that could not be satisfied by the server because the requested document was locked. This is usually reported as HTTP error 423. Baseline required.

You can modify the thresholds for this monitor.

Not Found Errors

The number of requests that have been made since the service started that were not satisfied by the server because the requested document was not found. This is usually reported as HTTP error 404.

You can modify the thresholds for this monitor.

Request Execution Time

This displays the number of milliseconds that it took to execute the most recent request.

The execution time begins when the HttpContext for the request is created, and stops before the response is sent to IIS. Assuming that user code does not call HttpResponse.Flush, this implies that execution time stops before sending any bytes to IIS, or to the client. When the process model is enabled, the request execution time includes the time required to write the response to the client, and therefore depends upon the bandwidth of the client's connection. There is no threshold for this counter. The value of this counter should be stable. Experience will help you set a threshold for a particular site.

You can modify the thresholds and enabled/disabled status for this monitor.

Request Wait Time

This displays the number of milliseconds that the most recent request was waiting in the queue. This does not include any time spent waiting in application queues. The threshold for this counter is 1,000. The average request should spend 0 milliseconds waiting in the queue.

You can modify the thresholds and enabled/disabled status for this monitor.

Possible issues: If this indicator is greater than 1,000 ms, the performance of the IIS server is suffering.

Requests Queued

This displays the number of requests waiting to be processed.

The Aspnet_wp process queue is a named pipe through which the request is sent from one process to the other. The number of requests in this queue increases if there is a shortage of available I/O threads in the Aspnet_wp process. When the limit specified by <processModel requestQueueLimit=/> is exceeded, requests will be rejected with a 503 error (Service Unavailable). Note that if a request is rejected for this reason, it will never reach managed code and error handlers will not be notified. Normally this only occurs when the server is under a very heavy load. Virtual directory queues maintain the availability of worker and I/O threads. The number of requests in these queues increases if the number of available worker threads or available I/O threads falls below the limit specified by <httpRuntime minFreeThreads=/>. When the limit specified by <httpRuntime appRequestQueueLimit=/> is exceeded, the request is rejected with a 503 error and the client is sent an HTTP exception with the message, Service Unavailable.
You can modify the thresholds and enabled/disabled status for this monitor.

Possible issues: When this value starts to increment linearly with increased client load, the web server computer has reached the limit of concurrent requests that it can process.

Resolution: The default maximum value for this counter is 5,000. You can change this setting in the Machine.config file.

Requests Rejected
This displays the number of requests rejected because the request queue was full.
Requests are rejected when one of the queue limits is exceeded. Back-end latency, such as that caused by a slow computer running SQL Server, is often preceded by a sudden increase in the number of pipeline instances and a decrease in % Processor Time and Requests/second. A server might be overwhelmed during times of heavy load due to processor or memory constraints that ultimately result in the rejection of requests.

You can modify the thresholds and enabled/disabled status for this monitor.

Possible issues: The value of this counter should be 0. Values greater than 0 should be investigated.

AppInsight for SQL
AppInsight template for monitoring SQL server instances. This Template helps you to monitor health of your whole SQL server instance.

Prerequisites
WMI and SQL access to target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

All Databases
Collects data for all monitored databases on the SQL instance.

Top Tables for Database
Performance counter that collects data to provide metrics for top table resources per database details view.

Top Indexes for Database
Performance counter that collects data to provide data for clustered and non-clustered index resources per database details view.

Database Files
Performance counter that collects data to provide metrics for file size resource per database details view.
Top Active Sessions with Statistics
Collects data for the top active sessions by duration active. Each session includes statistics including duration, idle time, and bytes transferred.

Top Expensive Queries
Collects data for the most expensive queries by CPU usage.

SQL Agent Job Info
Collects and provides stats and details data for administrative jobs run by the SQL Agent service.

SQL Server Events
Collects and provides data on SQL server events.

SQL Active Directory Helper Service

SQL Server
Collects and provides status on SQL server counters of statistics and values. Each statistic is consumed and displayed by other process monitors.

SQL Server Agent
Collects and provides data, status, and metrics for the SQL Server Agent process.

SQL Server Browser
Collects and provides data, status, and metrics for the SQL Server Browser process.

SQL Server VSS Writer
Collects and provides data, status, and metrics for the SQL VSS Writer process.

SQL Event Log Monitor
Collects and provides event log data for a database instance. These events are consumed by other process monitors.

Buffer Cache Hit Ratio
Indicates the percentage of pages found in the buffer cache without having to read from disk. The ratio is the total number of cache hits divided by the total number of cache lookups over the last few thousand page accesses.

After a long period of time, the ratio moves very little. Because reading from the cache is much less expensive than reading from disk, you want this ratio to be high. Generally, you can increase the buffer cache hit ratio by increasing the amount of memory available to SQL Server. The higher this ratio, the less often SQL Server has to go to the hard disk to fetch data, and performance is boosted overall. This counter averages the Buffer Cache Hit Ratio from the time the last instance of SQL Server was restarted. This counter is not a real-time measurement, but an average of all the days since SQL Server was last restarted. In OLAP (http://en.wikipedia.org/wiki/Online_analytical_processing) applications, the ratio could be much lower because of the nature of how OLAP works.
Possible issues: If the returned value is low, this could indicate that your SQL server may not have enough memory to function at peak performance.

Resolution: Check your SQL server and verify its memory is being used efficiently. Applications other than SQL may be using a great deal of memory. Try and recover memory by closing unnecessary applications. Installing additional memory may also help.

Cache Used/Min

This displays the number of times the cache object has been looked up.

This is not incremented when parameterized (http://technet.microsoft.com/en-us/library/ms175037.aspx) queries find a plan in the cache. However, this can be incremented multiple times when using Showplan. Good plan reuse is one sign of a healthy system. Compiling a query plan can be a CPU-intensive operation, especially with complex queries, so reuse is encouraged.

Possible issues: If the returned value is low, this can indicate ineffective reusing of plan cache which could cause a CPU spike. Conversely, if the returned value is high for a large number of plans, this could indicate that your cache space is being taken up with plans that were compiled and used once to execute an ad hoc query, then never used again.

Resolution: A database setting that can be helpful to plan reuse is forced parameterizaton. (You can set this using the following command: ALTER DATABASE <databaseName> SET PARAMETERIZATION FORCED). Normally, the query optimizer is very conservative when deciding what queries can be parameterized, but this setting makes the optimizer be more liberal in choosing parameters.

Page Splits/Batch Request

This performance counter displays the number of page splits per second that occur as the result of overflowing index pages. The returned value needs to be low as possible.

Possible issues: High values could mean poor table or index design.

Resolution: If the number of page splits is high, consider increasing the Fill Factor (http://msdn.microsoft.com/en-us/library/aa933139.aspx) of your indexes. An increased Fill Factor helps to reduce page splits because there is more room in data pages before it fills up and a page split has to occur. Note that this counter also includes the new page allocations as well and does not necessarily pose a problem. The other place we can confirm the page splits that involve data or index rows moves are the fragmented indexes on page splits.

Lazy Writers/sec

The lazy writer is a system process that flushes out buffers that contain changes that must be written back to disk before the buffer can be reused for a different page and makes them available to user processes.

This performance counter tracks how many times per second that the Lazy Writer process is moving dirty pages from the buffer to disk to free up buffer space. The Lazy Writer eliminates the need to perform frequent checkpoints to create available buffers. This should not be a high value, for example more than 20 per second. Ideally, it should be close to zero. If it is zero, this indicates that your SQL Server's buffer cache is large and your SQL Server does not need to free up dirty pages.
Possible issues: If the returned value is high, this can indicate that your SQL Server's buffer cache is small and that your SQL Server needs to free up dirty pages.

Resolution: Check your SQL server and verify its memory is being used efficiently. Applications other than SQL may be using a great deal of memory. Try and recover memory by closing unnecessary applications. Installing additional memory may also help.

**Free list stalls/sec**

Indicates the number of requests per second that had to wait for a free page. This displays the frequency with which requests for available database pages are suspended because no buffers are available.

Possible issues: If the returned value is high, this indicates that not enough memory is available for the SQL Server.

Resolution: Check your SQL server and verify its memory is being used efficiently. Applications other than SQL may be using a great deal of memory. Try and recover memory by closing unnecessary applications. Installing additional memory may also help.

**User Connections**

The User Connections performance counter identifies the number of different users that are connected to your SQL Server at the time the sample was taken.

You need to watch this counter over time to understand your baseline user connection numbers. Since each user connection consumes some memory space, a high number of user connections can impact throughput and cause a performance slow-down. Once you have an idea of your high and low thresholds during normal usage of your system, you can then look for times when this counter exceeds these high and low marks.

Possible issues: If the returned value of this counter goes down and the load on the system remains stable, you might have a bottleneck that is not allowing your server to handle the normal load. Keep in mind that this counter value might go down just because less people are using your SQL Server instance. If you see this number jump by 500% from your baseline, you may be seeing a slowdown of your server activity.

Resolution: You may want to boost the SQL Server configuration setting, Maximum Worker Threads to a figure higher than the default setting of 255. The setting for Maximum Worker Threads should be higher than the maximum number of user connections your server ever reaches.

**Active Sessions**

A current connection that is actively processing. To find information about an active session, Use Sp_Who2 Active or Sys.Dm_Exec_Sessions (Available in SQL 2005 or greater).

Possible issues: Blocking session.

Resolution: Wait until blocking clears or kill the session. If killed, the process would roll back changes. If there are many changes, it could take a while to roll-back.

**Inactive Sessions**

A current connection that is not currently processing. To find information about an inactive sessions, use Sp_Who2.
Possible issues: Blocking session.

Resolution: Kill the session if blocking a process needs to finish. If killed, the process would roll back changes. If there are many changes, it could take a while to roll-back.

**System Sessions**

A System initiated connection. Normally these numbers are less than 50.

Possible issues: Blocking session.

Resolution: Do not kill system sessions.

**User Sessions**

A user initiated connection. Normally these numbers are greater than 50.

Possible issues: Blocking session.

Resolution: Kill the session if blocking a process needs to finish. If killed, the process would roll back changes. If there are many changes, it could take a while to roll-back.

**Logins/sec**

This performance counter returns the total number of logins started, per second, and does not include pooled connections. Opening and closing connections is an expensive process. A pooled connection is one which is kept open by an application for other requests to re-use.

Possible issues: If the returned value is high, this can indicate that the application is not correctly using connection pooling.


**Logout/sec**

This performance counter returns the total number of logout operations started, per second. Opening and closing connections is an expensive process. When applications do not use a connection pool, each request needs to establish its own connection before the query can be executed. It then has to close it. A pooled connection is one which is kept open by an application for other requests to re-use.

Possible issues: If the returned value is high, this can indicate that the application is not correctly using connection pooling.

Lock Requests/sec

This performance counter returns the number of requests for a type of lock, per second. Blocking is an unavoidable characteristic of any relational database management system (RDBMS) with lock-based concurrency. On SQL Server, blocking occurs when one Server Process ID (SPID) holds a lock on a specific resource and a second SPID attempts to acquire a conflicting lock type on the same resource. Typically, the time frame for which the first SPID locks the resource is very small. When it releases the lock, the second connection is free to acquire its own lock on the resource and continue processing. This is normal behavior and may happen many times throughout the course of a day with no noticeable effect on system performance. For thresholds to be tuned to your environment, thresholds for this performance counter should be set using the Baseline Calculator.

Possible issues: If the returned value is high, this can indicate that the queries are accessing large numbers of rows. If you notice a high Average Wait time, it may indicate a SQL Server blocking issue.

Resolution: Review High Read queries. The simple way to fix locking is just kill the connection that is causing the lock. Fixing locking, blocking, and deadlocking issues is often a matter of redesign. You should examine either the schema of your database and/or the way the application is designed. One of the most efficient ways to deal with locking is to ensure that the design of your system does not have to deal with excessive locks. The best way to do this is to normalize your tables, using more atomic structures that allow the query to get in and get out faster. Another method is to code with the locks in mind. If the design requires less normalization, you will have to evaluate the programs to ensure that they have the right isolation levels.

Lock Waits/sec

This performance counter reports the number of times users waited to acquire a lock over the past second. This counter only gets incremented only when you “wake up” after waiting on the lock. For thresholds to be tuned to your environment, thresholds for this performance counter should be set using the Baseline Calculator.

Possible issues: Non-zero values indicate that there is at least some level of SQL Server blocking occurring. If you combine this with the Lock Wait Time counter, you can get some idea of how long the blocking lasted. A zero value for this counter can definitively rule out blocking as a potential cause.

Resolution: High Read queries should be reviewed.

Lock Timeouts/sev

This performance counter returns the number of lock requests per second that have timed out, including internal requests for NoWait (http://msdn.microsoft.com/en-us/library/c8bys6hz.aspx) locks.

The timeout_period is the number of milliseconds that will pass before Microsoft SQL Server returns a locking error. A value of -1 (default) indicates no time-out period (that is, wait forever). When a wait for a lock exceeds the time-out value, an error is returned. A value of 0 means to not wait at all and return a message as soon as a lock is encountered. For thresholds to be tuned to your environment, thresholds for this performance counter should be set using the Baseline Calculator.

Possible issues: If you see a value above 0 for this counter, your users will experience problems as their queries are not completing.
Resolution: You should review your queries to determine which queries are causing this situation.

**Average Latch Wait Time**

This performance counter reports the average latch wait time, in milliseconds, for latch requests that had to wait.

SQL Server two lightweight mutual exclusion solutions—Latches and Spinlocks—which are less robust than locks but are less resource-intensive. The value of this counter should generally correlate to Latch Waits/sec and move up or down with it accordingly.

Possible issues: If you see this number jump above 300, you may have contention for your server's resources. High values for this counter could potentially block other users.

Resolution: You should examine tasks currently waiting using the following command: sys.dm_os_waiting_tasks DMV.

**Average Lock Wait Time**

This performance counter reports the average amount of Wait time, in milliseconds, for each lock request that resulted in a wait. The lower the value, the better. This value should correlate to the Lock Waits/sec counter and move up or down with it accordingly.

Possible issues: An average wait time longer than 500ms may indicate excessive SQL Server blocking.

Resolution: You should determine which queries are generating locks to identify where the blocking is originating.

**Deadlocks/sec**

The number of lock requests that resulted in a deadlock. Since only a COMMIT, ROLLBACK, or deadlock can terminate a transaction (excluding failures or errors), this is an important value to track.

Possible issues: When returning value is above zero users and applications will experience problems. Their queries will abort and the applications may fail.

Resolution: You should trace deadlocks and examine trace output in SQL Server log. Deadlocks can be prevented by one or more of the following methods:

- Adding missing indexes to support faster queries
- Dropping unnecessary indexes which may slow down INSERTs for example
- Redesigning indexes to be "thinner", for example, removing columns from composite indexes or making table columns "thinner"
- Adding index hints to queries
- Redesigning tables with "thinner" columns like smalldatetime vs. datetime or smallint vs. int
- Modifying the stored procedures to access tables in a similar pattern
- Keeping transactions as short and quick as possible: "mean & lean"
- Removing unnecessary extra activity from the transactions like triggers
- Removing JOINs to Linked Server (remote) tables
- Implementing regular index maintenance; usually weekend schedule suffices; use FILLFACTOR
= 80 for dynamic tables

- Setting MAXDOP=1 solves deadlocking in some cases

**Lock Wait Time**

This performance counter displays the total time spent waiting across all transactions, in milliseconds, to acquire a lock in the last second. This counts how many milliseconds SQL Server is waiting on locks during the last second. This counter starts recording at the end of locking event. Peaks most likely represent one large locking event.

Possible issues: If the returned value is greater than 60 seconds (60,000ms) then there may be extended blocking which could be an issue.

Resolution: Thoroughly analyze the blocking script output. Some applications are written for timing out after 60 seconds. Because SQL Server records a lock at the end of a locking event, remember that an application with large transactions may have inflated lock wait times while still performing as expected. For example, an application that issues multi-million record updates might have very long lock wait times while performing exactly as it was designed.

**Total Server Memory**

This performance counter measures the current amount of memory that SQL Server is using.

If the value of this counter continues to grow larger, the server has not yet reached its steady state and is still trying to populate the cache and get pages loaded into memory. Performance will likely be somewhat slower if this value continually grows larger since more disk I/O is required. This behavior is normal. Eventually Total Server Memory should approximate Target Server Memory.

Possible issues: If the Total Server Memory counter is greater than or equal to the Target Server Memory counter, this can indicate that your SQL Server may be under memory pressure.

Resolution: Installing additional memory into your SQL server should resolve the problem.

**Target Server Memory**

This performance counter measures the total amount of dynamic memory the server can consume. This performance counter tells you how much memory SQL Server would like to use to operate efficiently. Compare with Total Server Memory.

Possible issues: If the Total Server Memory counter is greater than or equal to the Target Server Memory counter, this could indicate that your SQL Server may be under memory pressure.

Resolution: Installing additional memory into your SQL server should resolve the problem.

**SQL Cache Memory**

This performance counter measures the total amount of dynamic memory the server is using for the Dynamic SQL cache ([http://www.sommarskog.se/dynamic_sql.html](http://www.sommarskog.se/dynamic_sql.html)).
Most memory used by SQL Server is allocated to the Buffer Pool, which is used to store data pages. SQL Server steals a proportion of this memory for use in caching query plans. The overall amount of memory available to SQL Server depends upon the amount of memory installed on the server, the architecture of the server, the version and edition of SQL Server and the amount of memory pressure being experienced by SQL Server. This pressure can be internal (SQL Server resources need memory) or external (operating system needs memory). SQL Server is designed to respond to memory pressure when necessary.

Possible issues: Memory contention with the buffer pool.

Resolution: Increase memory available to SQL server.

**Lock Memory**

This performance counter returns the total amount of dynamic memory the server is using for locks.

Lock pages in memory is used to prevent older versions of Windows and SQL from allowing Windows operating system page out of the buffer pool.

Possible issues: Lock pages in memory determines which accounts can use a process to keep data in physical memory, which prevents the system from paging the data to virtual memory on disk. Exercising this privilege could significantly affect system performance by decreasing the amount of available random access memory (RAM).

Resolution: Upgrade to Windows 2008 R2 or greater and SQL 2008 or greater.

**Optimizer Memory**

This performance counter returns the total amount of dynamic memory the server is using for query optimization. There are no thresholds associated with this performance counter.

**Connection Memory**

This performance counter returns the total amount of dynamic memory the server is using for maintaining connections.

SQL Server sets aside three packet buffers for every connection made from a client. Each buffer is sized according to the default network packet size specified by the `sp_configure` stored procedure. If the default network packet size is less than 8KB, the memory for these packets comes from SQL Server's buffer pool. If it is 8KB or larger, the memory is allocated from SQL Server's `MemToLeave` region. It is worth noting that the default network packet size for the .NET Framework Data Provider for SQL Server is 8KB, so the buffers associated with managed code client connections typically come from SQL Server's `MemToLeave` region. This contrasts with classic ADO applications, where the default packet size is 4KB, and the buffers are allocated form the SQL Server buffer pool.

**Memory Grants Pending**

This performance counter returns the total number of processes waiting for a workspace memory grant (http://msdn.microsoft.com/en-us/library/ms190924.aspx).

Memory resources are required for each user request. If sufficient memory is not available, the user waits until there is adequate memory for the query to run.

Possible issues: Returned values greater than zero for a sustained period of time is a very strong indicator of memory pressure.
Resolution: You should first examine the database design, queries, and indexes to ensure the system is properly tuned before installing additional RAM. There may be query inefficiencies in the instance that is causing excessive memory grant requirements. For example, large Sorts (http://msdn.microsoft.com/en-us/library/ms188723.aspx) or Hashes (http://technet.microsoft.com/en-us/library/ms189313.aspx) that can be resolved by tuning the indexing or queries being executed.

Compare with Memory Grants Outstanding. If the number of pending grants increases, try the following:

- Add more memory to SQL Server
- Add more physical memory to the server.
- Check for memory pressure. See and correct indexing if you experience “Out of memory” conditions.

Workfiles Created/sec

This is the number of work files created per second. For example, work files could be used to store temporary results for hash joins and hash aggregates. The returned value should be less than 20. Tempdb work files are used in processing hash operations when the amount of data being processed is too large to fit into the available memory.

Possible issues: High values can indicate thrash in the tempdb file as well as poorly coded queries.

Resolution: It is possible to reduce the value this monitor returns by making queries more efficient by adding/changing indexes. Adding additional memory will also help.

Worktables Created/sec

This performance counter displays the number of work tables created per second. For example, work tables could be used to store temporary results for query spool, lob variables, XML variables, and cursors. The returned value should be less than 20. Worktables are used for queries that use various spools (table spool, index spool, and so on).

Possible issues: High values could cause general slowdown.

Resolution: Remediation requires rewriting your procedures.

Cache Hit Ratio

This metric is the ratio between Cache Hits and Lookups. Cache Hit Ratio measures how much the plan cache (http://msdn.microsoft.com/en-us/library/ee343986.aspx) is being used.

A high percentage here means that your SQL Server is not building a new plan for every query it is executing and is working effectively and efficiently. A low percentage here means that, for some reason, the SQL Server is doing more work than it needs to. This metric needs to be considered alongside the plan cache reuse metric which looks at the spread of plan reuse through your cache.
Plan cache is memory used to store objects such as stored procedures, ad hoc and prepared Transact-SQL (http://msdn.microsoft.com/en-us/library/bb510741.aspx) statements, and triggers. The plan cache is the component of SQL memory that stores query plans for re-use. When a query is issued against SQL, the optimizer will attempt to re-use a cached plan if the traits of the query permit - but can only do so if that plan resides in cache, otherwise it needs to compile a new plan. This is not to say that every plan that is cached is re-used. Changes in schema, a query running parallel that may have run serially before, or changes in parameters may require a new plan to be compiled even if a similar plan exists in cache. Plan compilations are expensive though. Ideally this counter should be near 100%.

Possible issues: The value of this counter should never fall below 90%. Low cache hit ratio (<20%) along with a sustained query execution rate (Batch Requests/sec) indicates that compiled plans are not being re-used. It should be noted that the hit ratio counter may be skewed by internal lookups performed.

Resolution: The amount of caching should be reduced by examining the workload to see if queries have been parameterized (http://technet.microsoft.com/en-us/library/ms175037.aspx), or can be rewritten with stored procedures.

Page Reads/sec

This performance counter returns the number of physical database page reads issued. 80 – 90 physical database page reads per second is normal.

Possible issues: Returned values that are high could indicate indexing or memory constraint.

Resolution: Attempt to tune the application so that fewer I/O operations are required. For example, perhaps I/O operations would be reduced if there were the appropriate indexes, or if the database design were de-normalized. If the applications cannot be tuned, you will need to acquire disk devices with more capacity. Because physical I/O operations are expensive, you may be able to minimize the cost either by using a larger data cache, intelligent indexes, more efficient queries, or by changing the database design.

Page Writes/sec

This performance counter returns the number of physical database page writes issued. 80 – 90 physical database page writes per second is normal.

Possible issues: If the returned values are high, you should check the Lazy Writer/sec monitor. This can indicate that your SQL Server's buffer cache is small and that your SQL Server needs to free up dirty pages.

Resolution: Check your SQL server and verify its memory is being used efficiently. Applications other than SQL may be using a great deal of memory. Try and recover memory by closing unnecessary applications. Installing additional memory may also help.

Page Splits/sec

This performance counter returns the number of page splits per second. The returned value for this monitor should be as low as possible.
Possible issues: Returned values that are high can indicate the overflowing of index pages. A high value for this counter is not bad in situations where many new pages are being created, since it includes new page allocations.

Resolution: To avoid Page Splits (http://careerride.com/SQL-Server-what-is-page-splits.aspx), review the table and index design so as to reduce non-sequential inserts. You can also implement Fillfactor (http://msdn.microsoft.com/en-us/library/ms177459.aspx) and Pad_Index (http://stackoverflow.com/questions/6857007/what-is-the-purpose-of-pad-index-in-this-sql-server-constraint) to leave more empty space per page.

Page Life Expectancy

This performance counter returns the number of seconds a page will stay in the buffer pool (http://msdn.microsoft.com/en-us/library/aa337525.aspx) without references. This performance monitor reports, on average, how long data pages are staying in the buffer.

Possible issues: If this value gets below 300 seconds, this is a potential indication that your SQL Server could use more memory to boost performance. Consistently having pages that stay in memory for less than that amount of time may indicate the need for more memory.

Resolution: Add additional memory to your SQL server.

Free pages

This performance counter displays the total number of pages on all free lists. This is not a main indicator of memory problems and could only used as signal of possible memory pressure. For thresholds to be tuned to your environment, thresholds for this performance counter should be set using the Baseline Calculator.

Possible issues: If this counter is critical and other memory counters are good, it is possible that there are no problems with memory.

Resolution: Check other memory counters. If they have critical values, you may try to install additional memory into SQL server.

Free Memory

The amount of memory available for SQL Server to use.

When SQL Server is using memory dynamically, it queries the system periodically to determine the amount of free memory. Maintaining this free memory prevents the operating system (OS) from paging. If less memory is free, SQL Server releases memory to the OS. If more memory is free, SQL Server may allocate more memory. SQL Server adds memory only when its workload requires more memory; a server at rest does not increase the size of its virtual address space. The returned value should be as high as possible.

Possible issues: If Resource Semaphore does not find enough free memory, then it puts the current query into the waiting queue.

Resolution:
- Increase RAM
- Increase SQL Server's Max Server Memory
- Consider OS requirements and other instances
Total Pages

This performance counter returns the number of pages in the buffer pool. The returned value includes database, free, and stolen pages.

ℹ️ This counter is not available in SQL 2012.

SQL Compilation/sec

This performance counter returns the number of times per second that SQL Server compilations have occurred. This value should be as low as possible.

Possible issues: If you see a high value, say above 100, then this can be an indication that there are a great deal of ad hoc queries that are running which may cause increased CPU usage.

Resolution: Re-write the running ad hoc queries as stored procedures or use the following command: `sp_executeSQL`.

Full Scans/sec

This performance counter returns the number of Full Scans on base tables or indexes. This is the number of unrestricted full scans per second. These can be either base-table or full-index scans. For thresholds to be tuned to your environment, thresholds for this performance counter should be set using the Baseline Calculator.

Possible issues: Values greater than 1 or 2 indicate table/Index page scans are occurring. If the CPU is running high, you should investigate the cause as related to this counter measurement. You can rule this out as a problem if the full scans are on small tables.

Resolution: Following are the main causes of high Full Scans/sec values:

- Missing indexes
- Too many rows requested; Queries with missing indexes or too many rows requested will have a large number of logical reads and an increased CPU time.
- Scans are IO-intensive and should run within your databases minimally. Identify the tables that have a large number of scans against them. Review the fill factor you have set up on your indexes and minimize it where appropriate.

Batch Requests/sec

This performance counter returns the number of Batch Requests ([http://sqlserverplanet.com/dba/understanding-batch-requests-sec](http://sqlserverplanet.com/dba/understanding-batch-requests-sec)) that SQL Server receives per second. The values this monitor returns generally follows in step as to how busy your server's CPUs are. From a network bottleneck approach, a typical 100Mbs network card is only able to handle about 3,000 batch requests per second.

Possible issues: Generally speaking, over 1,000 batch requests per second indicates a very busy SQL Server. If this is the case, you may soon experience a CPU bottleneck, if you are not already. Of course, this is a relative number, and the more powerful your hardware, the more batch requests per second your SQL Server can handle.
Sometimes low Batch Requests/Sec can be misleading. If there were a SQL Statements/sec counter, this would be a more accurate measure of the amount of SQL Server activity. For example, an application may call only three stored procedures, yet each stored procedure does a great deal of work. In this case, we will see a low number for Batch Requests/sec, but each stored procedure (one batch) will execute many SQL statements that drive up CPU and other resources. As a result, many counter thresholds based on the number of Batch Requests/sec will seem to identify issues because the batch requests on such a server are unusually low for the level of activity on the server.

Resolution: Check your SQL server and verify system resources are being used efficiently. Applications other than SQL may be using unnecessary system resources. Try and recover memory by closing unnecessary applications. Installing additional memory and upgrading your hardware should solve this problem.

Data File(s) Sizer

This performance counter shows the cumulative size (in kilobytes) of all the data files in the database including any automatic growth. Monitoring this counter is useful for determining the correct size of tempdb. The value returned from this monitor reports the size of your database (not including the Transaction log). Information about distinct primary data files and secondary data files is shown under the Files section of the Database Overview page in SQL Server Management Studio.

Having a file size increase on demand is expensive and will degrade performance significantly. Autogrowth should only be used to let a database increase in size if you are running out of disk space. Autogrowth should not be used to manage your MDF (http://msdn.microsoft.com/en-us/library/ms190209.aspx) size increases. Data files should be sized properly when they are initially created to meet the expected growth. This also helps avoid fragmentation. This also leads to better database performance.

Possible issues: Be wary of large and unusual increases to the size of your data files. Generally speaking, your database should be sized to minimize Autogrowth (http://msdn.microsoft.com/en-us/library/ee308850.aspx). An increase in size is expensive concerning I/O. Additionally, this will fragment your data and log files. If the returned value occasionally drops to zero, this can indicate a problem with the following file: sys.master_files. This file is what the SQL Monitor uses to collect data.

Resolution:

- Ensure that Full Recovery Mode (http://msdn.microsoft.com/en-us/library/ms189275.aspx) is used for your databases and that you regularly backup everything, including the transaction log.
- Manually add space as data increases in size. It is recommended that you have approximately one year of space available for data growth. If this is not possible, move the database to a higher capacity drive or simply upgrade the drive.

Compressing files causes fragmentation and is therefore not recommended.
Log File(s) Size

This performance counter shows the cumulative size (in kilobytes) of all the transaction log files in the database. Every transaction in the database is logged to the Transaction log. This is useful during recovery in the event of data loss. Information about the log file is shown under the Files section of the Database Overview page in SQL Server Management Studio.

The size of this file is based on the logging level set for the database. By default, a new database uses Full Recovery Mode (http://msdn.microsoft.com/en-us/library/ms189275.aspx) or the recovery mode that the model database is set up as. Transactions in the log file are only removed when a complete backup or transaction log backup is initiated. This enables pinpoint recovery for critical applications. Be aware that if the transaction log is not backed up on a regular basis, the log will grow until your disk is completely full. The transaction log should be adjusted to a reasonable size. This will depend on the number of transactions you expect, and how often you perform backups.

Set the correct Autogrowth (http://msdn.microsoft.com/en-us/library/ee308850.aspx) properties: The default of 10% Autogrowth for data and log files should be enough for low use databases. Conversely, a 500 MB Autogrowth rate may be better suited for a busy database, preventing a large I/O impact caused by normal Autogrowth operations.

Possible issues: If the returned value occasionally drops to zero, this can indicate a problem with the following file: sys.master_files. This file is what the SQL Monitor uses to collect data.


Resolution:

- If you are performing a insert operation, you should consider switching the recovery model to Bulk Logged for the insert.
- If you do not need pinpoint recovery, it is recommended you switch to Simple Recovery model.
- If your database is configured with the Full or Bulk Logged recovery model, back up the log on a regular basis so it can be truncated to free up log space.

| This action removes inactive virtual log files, but does not reduce the file size. |

Total Size

This performance counter returns the total size of the database including white space.

Possible issues: Running out of storage space.

Resolution: Shrink the database if free space is running low.

**Total Size: Percent Change 24 Hrs**

This value is the same as the value returned by the performance counter, Total Size but calculated as a percentage of change over the last 24 hours. This metric allows users to be alerted when the database experiences sudden growth.

Possible issues: A database that suddenly changes in size by a high percentage could be indicative of a problem that should be investigated.
Active Transactions

This performance counter returns the number of active transactions for the database. During an active transaction, no other transaction can modify the data held by the active transaction. While you are modifying data, an exclusive lock is held on that data. Conversely, you cannot read data held by another transaction because another transaction holds an exclusive lock on the data that prevents it from being read. The returned value for this monitor should be less than 200.

Possible issues: A high number of active transactions can indicate that certain transactions are never completing.

Resolution: Keeping a low level of active transactions assists in keeping requested data accessible.

Transactions/sec

This performance counter returns the number of transactions started for the database, per second. Transaction rate is affected by general system performance and resource constraints, such as I/O, number of users, cache size, and the complexity of requests.

Possible issues: A high rate of transactions can indicate that some transactions are not completing.

Resolution: Using stored procedures in transactions speeds transaction processing because SQL code in stored procedures runs locally on the server. The transactions can finish much faster without the network traffic required by the transactions.

Log Cache Hit Ratio

This performance counter returns the percentage of Log cache reads satisfied from the Log cache. The log cache is used to hold information that will be written to the transaction log. There are no thresholds associated with this performance counter.

Log Cache Reads/sec

This performance counter returns the amount of Reads performed per second through the Log Manager cache.

Log Byutes Flushed/sec

This performance counter shows the average log bytes flushed per second for the current database since the last data point. The value returned helps identify trends of the transaction log. A log flush happens when data is written from the log cache to the transaction log on disk, each time a transaction happens.

This is not available in SQL 2012.

Possible issues: The rate at which log records are written to the disk. This is the log generation rate of the application. It plays a very important role in determining database mirroring performance. This counter is in the Databases performance object.

Log Bytes Flushed/sec can indicate many small transactions leading to high mechanical disk activity.
Resolution: Look at the statements associated with the log flush and determine if the number of log flushes can be reduced. When a single transaction is used, the log records for the transaction can be bundled and a single, larger write can be used to flush the gathered log records. The mechanical intervention is significantly reduced. It is not recommended that you increase your transaction scope. Long-running transactions can lead to excessive and unwanted blocking as well as increased overhead.

**Log Flush Wait Time**

This performance counter returns the total wait time (in milliseconds) to flush the log to the transaction log file. On an AlwaysOn secondary database, this value indicates the wait time for log records to be hardened to disk.

**Log Flush Waits/sec**

This performance counter returns the number of commits, per second, waiting for the log flush. This value should be as low as possible.

Possible issues: A high number of Log Flush Waits can indicate that it is taking longer than normal to flush the transaction log cache. This will slow the performance of your SQL Server.

Resolution: Check the value of the Disk avg. Write time monitor. If the returned value is greater than 5ms, then this can indicate that there is an I/O bottleneck. Move your transaction log file to a disk drive separate from your data files. This should increase performance since there is no access competition on the same disk. Consider upgrading to RAID 10 for transaction log storage. Also, adding spindles to your RAID array should increase performance.

**Log Flushes/sec**

This performance counter returns the number of log flushes per second, averaged since the last collection time. A log flush happens when a transaction is committed and data is written from the log cache to the transaction log file. The log cache is a location in memory where SQL Server stores data to be written to the log file. This is used to roll back a transaction before it is committed. Once complete, the log cache is flushed to the physical log file on the disk. Generally speaking, log flushes per second should parallel the number of transactions per second.

Possible issues: If the returned value is higher than expected, check your use of explicit transactions in your queries.

Resolution: Explicitly define the start and end of your transactions. This should reduce the number of log flushes, and reduce the impact on I/O. Also check the Log Bytes Flushed/Sec monitor.

**Percent Log Used**

This performance counter returns the percentage of space in the log that is in use. This is the size of the transaction log that actively contains data in relation to the total physical size on disk of the log file.

Possible issues: If the log file is 100% used, it will attempt to increase its size. If there is not sufficient disk space to accommodate the growth, the database will stop functioning.

Resolution: Perform a transaction log backup to truncate the log.
**Average Disk sec/Write**

This performance counter shows the average time, in seconds, of a write of data to the disk. The returned value indicates the average time of write data from the disk. 4-8ms is ideal. The returned value is considered acceptable up to 20ms. Any higher value needs further investigation. For thresholds to be tuned to your environment, thresholds for this performance counter should be set using the Baseline Calculator.

Possible issues: Values greater than 15-20ms may indicate disk bottlenecks.

Resolution: Increase the number of hard disks.

**Average Disk sec/Read**

This performance counter shows the average time, in seconds, of a read of data from the disk. The returned value indicates the average time of read data from the disk. 4-8ms is ideal. The returned value is considered acceptable up to 20ms. Any higher value needs further investigation. For thresholds to be tuned to your environment, thresholds for this performance counter should be set using the Baseline Calculator.

Possible issues: If a value greater than 15-20ms is reported, this may indicate disk bottlenecks.

Resolution: Increase the number of hard disks.

**Physical Disk sec/Write**

This performance counter returns the ratio of elapsed time when the disk drive was busy with read or write requests. This counter is deceptive because it makes no accommodation for multiple spindles. Thus, the more spindles (i.e. physical hard disks) you have, the higher the percentile values can go. Conversely, if these spindles are shared across LUNs or other services, you may have high numbers on this counter without any correlation to SQL Server activity. The value for this counter should be below 50%. For thresholds to be tuned to your environment, thresholds for this performance counter should be set using the Baseline Calculator.

Possible issues: If this counter sustains an average above 70%, you may have contention with your drive or RAM.

Resolution: You increase number of hard drives used by SQL server.

**Average Disk sec/Read**

This performance counter returns the average number of pages faulted (http://blogs.technet.com/b/askperf/archive/2008/06/10/the-basics-of-page-faults.aspx) per second. This counter gives an idea of how many times information being requested is not where the application expects it to be. The information must either be retrieved from another location in memory or from the pagefile. While a sustained value may indicate trouble, you should be more concerned with hard page faults that represent actual reads or writes to the disk. Disk access is much slower than RAM.

Possible issues: Any measurement higher than zero delays response time and probably indicates that more RAM is needed.

Resolution: Add additional memory to your SQL server.
Physical Disk Time

This is the rate at which pages are read from or written to disk to resolve hard page faults. This is a primary indicator of the kinds of faults that cause system-wide delays. This should be close to zero on a dedicated SQL Server. You will see spikes during backups and restores, but this is normal. For thresholds to be tuned to your environment, thresholds for this performance counter should be set using the Baseline Calculator.

Possible issues: High values causes hard page faults, which can cause SQL Server to use the page, as opposed to RAM.

Resolution: You may want to add additional RAM to stop the paging.

Page Faults/sec

This is the amount of available physical memory on the server. An acceptable output for this may vary widely based on how much physical memory is in the machine. If you have 2 GB of RAM installed on the machine, it is common to see SQL Server use 1.7 GB. If no other processes are running on your SQL Server, ensure you have at least 80 MB available for Windows at any given time. For thresholds to be tuned to your environment, thresholds for this performance counter should be set using the Baseline Calculator.

Possible issues: Low values show that SQL server has lack of memory.

Resolution: Install additional memory.

Pages/sec

This is the rate at which pages are read from or written to disk to resolve hard page faults. This is a primary indicator of the kinds of faults that cause system-wide delays. This should be close to zero on a dedicated SQL Server. You will see spikes during backups and restores, but this is normal. For thresholds to be tuned to your environment, thresholds for this performance counter should be set using the Baseline Calculator.

Possible issues: High values causes hard page faults, which can cause SQL Server to use the page, as opposed to RAM.

Resolution: You may want to add additional RAM to stop the paging.

Available MBytes

This is the amount of available physical memory on the server. An acceptable output for this may vary widely based on how much physical memory is in the machine. If you have 2GB of RAM installed on the machine, it is common to see SQL Server use 1.7GB of RAM. If no other processes are running on your SQL Server, ensure you have at least 80MB available for Windows at any given time. In order for thresholds to be tuned to your environment, thresholds for this performance counter should be set using the Baseline Calculator.

Possible issues: Low values show that SQL server has lack of memory.

Resolution: Install additional memory.
Page Usage

This shows the percentage of the page file that is being utilized. A Page File is simply a file on the hard drive that handles situations where the system wants to move or “page out” sections of memory. There are several situations that cause this, but the one you should be most concerned about is when the system is out of physical memory. In order for thresholds to be tuned to your environment, thresholds for this performance counter should be set using the Baseline Calculator.

Possible issues: Values greater than 70 percent indicate paging and lack of memory. If the system runs out of memory it can “borrow” some storage from the hard drive to release some memory until it needs that data again. The reason that this is bad is because hard drives are amazingly slow in comparison with solid-state memory access. Using the page file slows SQL Server a great deal.

Resolution: Install additional memory.

Database Pages

This metric tells you have many database pages are currently being occupied in the data cache. The higher the buffer manager Database Pages is, the less room there is for SQL Server to cache more data pages. This means that SQL Server may have to free up data cache pages order to make room for pages being moved in from disk to the data cache, which can increase disk IO and hurt performance. There are no specific thresholds for this counter as each server is different. Instead, watch baseline values and look for sudden changes in the baseline value.

Possible issues: If the value for this counter increases above its typical baseline value, this may indicate memory pressure for the SQL Server instance.

Resolution: Investigate buffer management and disk I/O.

Longest Transaction Running Time

The length of time, in seconds, the transaction that has been running the longest, has been active. Transactions that run longer than others use more resources. They can be used to track down procedures and calls that are taking longer than expected by identifying the specific transaction(s).

Possible issues: Long running transactions can prevent truncation of transaction logs. This can cause the transaction log files to grow until they consume all available physical disk space shutting down access to the database.

Resolution: Check the functionality of the query and/or redesign the long running transaction.

Granted Workspace Memory


This performance counter tells you how much memory has currently been granted to running queries. If there is memory pressure because of workspace memory, this value should be at least 25% of the virtual memory available to SQL Server.
Possible issues: If the memory pressure is severe, the server might return errors such as 701 or 8645.

Resolution: If this is the case, this might be a good reason to consider using SQL Server 64-bit.

Prove Scans/sec

This performance counter returns the number of Probe Scans, per second, that are used to find at most, one single qualified row in an index or base table directly.

Range Scans/sec

This performance counter returns the number of Qualified Range Scans through indexes per second. This monitor returns the number of qualified range scans through indexes per second.

Auto-Param Attempts/sec

This performance counter returns the number of auto-parameterization

The total for this monitor should be the sum of the failed, safe, and unsafe auto-parameterizations. Auto-parameterization occurs when an instance of SQL Server tries to parameterize a Transact-SQL request by replacing some literals with parameters so that reuse of the resulting cached execution plan across multiple similar-looking requests is possible. Note that auto-parameterizations are also known as simple parameterizations in newer versions of SQL Server. This counter does not include forced parameterizations (http://technet.microsoft.com/en-us/library/ms175037.aspx).

Possible issues: Bad T-SQL coding practices can increase recompilation frequency and adversely affect SQL Server's performance. Such situations can be debugged and corrected in many cases.

Failed Auto-Params/sec

This performance counter returns the number of failed auto-parameterization

The value returned by this monitor should be low. Auto-parameterizations are also known as simple parameterizations in later versions of SQL Server. Preferred values should be near zero. In order for thresholds to be tuned to your environment, thresholds for this performance counter should be set using the Baseline Calculator.

Possible issues: Bad T-SQL coding practices can increase recompilation frequency and adversely affect SQL Server's performance. Such situations can be debugged and corrected in many cases.

Cache Object Counts

This performance counter returns the number of cache objects in the cache.

The Plan Cache object provides counters to monitor how SQL Server uses memory to store objects such as stored procedures, ad hoc and prepared Transact-SQL statements, and triggers. Multiple instances of the Plan Cache object can be monitored at the same time, with each instance representing a different type of plan to monitor.

Possible issues: High numbers of total cached objects use portions of the physical memory available to a SQL instance on a per database basis. This can result in one database cache impacting the performance of other local databases due to memory contention.
Resolution: Increase the memory available to SQL services, reduce the number of databases on this instance of SQL, or examine the volume of ad hoc queries running against the server.

**Cache Objects in Use**

This performance counter returns number of cache objects in use. The Plan Cache object provides counters to monitor how SQL Server uses memory to store objects such as stored procedures, ad hoc and prepared Transact-SQL statements, and triggers. Multiple instances of the Plan Cache object can be monitored at the same time, with each instance representing a different type of plan to monitor.

Possible issues: High numbers of cached objects in use consume the memory available to a SQL server at a higher rate than non-active objects on a per database basis. This can result in one database cache impacting the performance of other local databases due to memory contention.

Resolution: Increase the memory available to SQL server, reduce the number of active objects, consolidate stored procedures, consolidate and convert ad hoc queries to stored procedures where possible, or reduce the number of databases on the server.

**Memory Grants Outstanding**

This performance counter returns the total number of processes that have successfully acquired a workspace memory grant (http://msdn.microsoft.com/en-us/library/ms190924.aspx).

Look at Memory Grants Outstanding and Memory Grants Pending. If you see a long queue of pending grants as compared to outstanding grants, there is likely memory pressure because of query workspace memory. You can confirm this by checking the Granted Workspace Memory (KB) performance counter that tells you how much memory has currently been granted to running queries.

Possible issues: A returned value that is high can indicate peak user activity. If there is memory pressure because of workspace memory, this value should be at least 25% of the virtual memory available to SQL Server. If the memory pressure is severe, the server might even return errors such as 701 or 8645.

Resolution: If severe, and using 32-bit, consider using SQL Server 64-bit. See Memory Grants Pending.

**Repl. Trans. Rate**

This performance counter returns the number of transactions read out of the transaction log and sent to the distribution database.

SQL Server Overall Replication Performance Analysis provides a graph of several SQL Server overall replication performance counters for the specified server during the specified time period. Performance counter data is averaged by the hour. The graph displays the following replication performance counters:

- SQLServer:Databases / Replication Pending Xacts (SQL Server; Scale=1\100)
- SQLServer:Databases / Replication Transaction Rate (SQL Server; Scale=1\100)
- SQLServer Replication Published DB / Replicated Transactions Per Second
**Bulk Copy Rows/sec**

This performance counter returns the number of rows bulk copied per second. Measure the number of rows coming into the database. Optimization yields a higher number. See The Data Loading Performance Guide (http://technet.microsoft.com/en-us/library/dd425070.aspx)

Possible issues: BCP to bulk load data over the network, having the correct throughput configured is crucial.

**Bulk Copy Throughput/sec**

This performance counter returns the amount of data bulk copied (in kilobytes) per second.

Possible issues: Overall throughput will mostly be limited by your I/O subsystem.

**Backup/Restore Throughput/sec**

This performance counter shows the Read/Write throughput for backup and restore operations of a database per second.

You can measure how the performance of the database backup operation changes when more backup devices are used in parallel, or when faster devices are used. Throughput of a database backup or restore operation allows you to determine the progress and performance of your backup and restore operations. There are no thresholds associated with this performance counter.

**Shrink Space**

This is essentially the white space in the database that can be reclaimed by compacting/shrinking the database. Shrinking data files recovers space by moving pages of data from the end of the file to unoccupied space closer to the front of the file. When enough free space is created at the end of the file, data pages at end of the file can de-allocated and returned to the file system.

Possible issues: Data that is moved to shrink a file can be scattered to any available location in the file. This causes index fragmentation and can slow the performance of queries that search a range of the index.

Resolution: To eliminate the fragmentation, consider rebuilding the indexes on the file after shrinking.

**Average Read Latency**

This performance counter indicates the response time of the disk – how long it takes for a read request to get acknowledged by the disk. The average read latency should be less than 20ms for database files.

**Average Write Latency**

Avg. Disk sec/Write is the average time, in seconds, to write data to the disk. This analysis determines if any of the physical disks are responding slowly.

Possible issues: If the response times are greater than .015 (15 milliseconds), then the disk subsystem is keeping up with demand, but does not have much overhead left. If the response times are greater than .025 (25 milliseconds), then noticeable slow-downs and performance issues affecting users may be occurring.
Average Bytes/Read

Perfmon captures the total number of bytes sent to the disk (write) and retrieved from the disk (read) over a period of one second. The Disk Read Bytes/sec and the Disk Write Bytes/sec performance counters break down the results displaying only read bytes or only write bytes, respectively.

Average Bytes/Write

Perfmon captures the total number of bytes sent to the disk (write) and retrieved from the disk (read) over a period of one second. The Disk Read Bytes/sec and the Disk Write Bytes/sec performance counters break down the results displaying only read bytes or only write bytes, respectively.

Number of Reads/sec

This performance counter returns the number of physical database page reads issued per second. This statistic displays the total number of physical page reads across all databases. 80 to 90 per second is normal. Anything that is above 90 indicates indexing or memory constraint.

Possible issues: Because physical I/O is expensive, you may be able to minimize the cost, either by using a larger data cache, intelligent indexes, and more efficient queries, or by changing the database design.

Resolution: Attempt to tune the application so that fewer I/O operations are required. For example, perhaps I/O would be reduced if there were appropriate indexes or if the database design were denormalized. If the applications cannot be tuned, you will need to acquire disk devices with more capacity.

Compare to the Memory: Pages/sec performance counter to see if there is paging while the SQL Server:Buffer Manager\Page reads/sec is high.

Before adjusting the fill factor, at a database level, compare the SQL Server:Buffer Manager\Page reads/sec performance counter to the SQL Server:Buffer Manager\Page writes/sec counter, and use the fill factor option only if writes are a substantial fraction of reads (greater than 30 percent).

Numbers of Writers/sec

This performance counter returns the number of data pages written per second. Page writes per second are the total number of physical writes, including checkpoint writes, lazy writer writes, and large block writes done during index creation or bulk copy operations.

Possible issues: If Page Writes/sec is high, this might indicate a SQL Server performance issue.

Resolution: If these values are high, you can try to reduce the values by tuning your application or database to reduce I/O operations such as index coverage, better indexes, normalization, increasing the I/O capacity of the hardware, or by adding memory.

Page Lookups/Batch Request

This performance counter displays the number of page splits per second that occur as the result of overflowing index pages. \((\text{Page lookups/sec}) \div (\text{Batch Requests/sec}) > 100.\) In order for thresholds to be tuned to your environment, thresholds for this performance counter should be set using the Baseline Calculator.
Possible issues: When the ratio of page lookups to batch requests is much greater than 100, this is an indication that while query plans are looking up data in the buffer pool, these plans are inefficient.

Resolution: Identify queries with the highest amount of logical I/O's and tune them.

**Compilations/Recompliations/Sec**

Monitoring the number of query compilations and recompliations and the number of batches received by an instance of SQL Server gives you an indication of how quickly SQL Server is processing user queries and how effectively the query optimizer is processing the queries. Compilation is a significant part of a query's turnaround time. To save the compilation cost, the Database Engine saves the compiled query plan in a query cache. The objective of the cache is to reduce compilation by storing compiled queries for later reuse, therefore ending the requirement to recompile queries when later executed. However, each unique query must be compiled at least one time.

Compilations/sec divided by 10 minus recompliations/sec. In order for thresholds to be tuned to your environment, thresholds for this performance counter should be set using the Baseline Calculator.

Possible issues: Query recompliations can be caused by the following factors:

- Schema changes, including base schema changes such as adding columns or indexes to a table, or statistics schema changes such as inserting or deleting a significant number of rows from a table.
- Environment (Set statement) changes. Changes in session settings such as Ansi_Padding or Ansi_Nulls can cause a query to be recompiled.

**Plan Re-Use**

A query plan is used to execute a query. Plan re-use is desirable for OLTP workloads because recreating the same plan (for similar or identical transactions) is a waste of CPU resources. In order for thresholds to be tuned to your environment, thresholds for this performance counter should be set using the Baseline Calculator.

Possible issues: Zero cost plans will not be cached (not re-used) in SQL 2005 SP2. Applications that use zero cost plans will have a lower plan re-use but this is not a performance issue.

Resolution: Review your plan re-use design. Tune your plan re-use design as it is described in the following article (http://sqlmag.com/sql-server/fine-tuning-plan-reuse).

**Forwarded Records/Batch Requests**

This performance counter identifies the use of a pointer which has been created when variable length columns have caused a row to move to a new page in a heap (http://msdn.microsoft.com/en-us/library/ms188270.aspx).

Possible issues: Rows with Varchar (http://msdn.microsoft.com/en-us/library/ms176089.aspx) columns can experience expansion when Varchar values are updated with a longer string. In the case where the row cannot fit in the existing page, the row migrates and access to the row will traverse a pointer. This only happens on heaps (tables without clustered indexes).
Resolution: Evaluate clustered indexes for heap tables. In cases where clustered indexes cannot be used, drop non-clustered indexes, build a clustered index to Reorg (http://technet.microsoft.com/en-us/library/ms189858.aspx) pages and rows, drop the clustered index, then recreate non-clustered indexes.

**Total Latch Wait Time/Latch Waits**

This monitor returns the ratio of Total Latch Wait Time, in milliseconds, for latch requests in the last second to amount of latches, in a one second period that had to wait. Latches are lightweight means of holding a very transient server resource, such as an address in memory.

This ratio should be less than 10. Monitoring the latches to determine user activity and resource usage can help you to identify performance bottlenecks. In order for thresholds to be tuned to your environment, thresholds for this performance counter should be set using the Baseline Calculator.

Possible issues: If the returned value is high, it is likely there is an I/O or memory bottleneck.

Resolution: Check your SQL server and verify its memory is being used efficiently. Applications other than SQL may be using a great deal of memory. Try and recover memory by closing unnecessary applications. Installing additional memory may also help.

**Recompilations/Compilation**

This performance counter shows the ratio of SQL Recompilations to SQL Compilations. SQL Recompilations should be less than 10% of SQL Compilations. In order for thresholds to be tuned to your environment, thresholds for this performance counter should be set using the Baseline Calculator.

Possible issues: Returned values that are high can indicate more temporary tables in use.

Resolution: Change stored procedures to not change schemas, Use table variables instead of temporary tables

**Target - Total Server Memory**

This performance counter shows the difference between the total amount of dynamic memory the server can consume and the current amount of memory that SQL Server is using.

Possible issues: If you have evidence of memory pressure and this counter is not close to zero, it may indicate that the buffer pool cannot expand. Examples of memory pressure include: (1) Memory Grants Pending metric stays above zero for any significant time. (2) Queries with a significant portion of wait time spent in the **RESOURCE_SEMAPHORE** wait type.

Resolution: Installing additional memory into SQL server may resolve the problem or you may need to identify queries with high demands on memory.
Barracuda Spam and Virus Firewall

This template assesses the overall performance of Barracuda Spam and Virus Firewall by using SNMP protocol.

Prerequisites

SNMP enabled on the Barracuda Spam and Virus Firewall server.

Credentials

None (uses the SNMP public string assigned to the node).

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Inbound Queue

This monitor returns the number of messages waiting to be processed by the Barracuda Spam & Virus Firewall.

Outbound Queue

This monitor returns the number of messages waiting to be sent to the mail server. Note that alerts and notifications are queued separately from outbound email.

Deferred Queue

This monitor returns the number of messages deferred because they could not be processed, and will be requeued for processing.

Average Email Latency

This monitor returns the difference between the time a message was received by the Barracuda Spam & Virus Firewall and the time it is sent to the mail server.

Notification Queue

This monitor returns number of messages in the notification queue.

Inbound: Blocked

This monitor returns the total number of inbound messages blocked since last system reset.

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.
Inbound: Blocked (Viruses)

This monitor returns the total number of inbound messages blocked due to viruses since last system reset.

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

Inbound: Deferred (Rate Control)

This monitor returns the total number of inbound messages deferred due to Rate Control since last system reset.

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

Inbound: Quarantined

This monitor returns the total number of inbound messages quarantined since last system reset.

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

Inbound: Tagged

This monitor returns the total number of inbound messages tagged since last system reset.

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

Inbound: Allowed

This monitor returns the total number of allowed inbound messages.

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

Outbound: Blocked (Policy)

This monitor returns the total number of outbound messages blocked due to policy since last system reset.

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

Outbound: Blocked (Spam)

This monitor returns the total number of outbound messages blocked due to spam since last system reset.
This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

**Outbound: Blocked (Viruses)**

This monitor returns the total number of outbound messages blocked due to viruses since last system reset.

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

**Outbound: Deferred (Rate Control)**

This monitor returns the total number of outbound messages deferred due to Rate Control since last system reset.

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

**Outbound: Quarantined**

This monitor returns the total number of outbound messages quarantined since last system reset.

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

**Encrypted**

This monitor returns the number of messages sent to the Barracuda Message Center for encryption and delivery since last system reset.

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

**Redirected**

This monitor returns the number of messages redirected to another mail server since last system reset.

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

**Delivered**

This monitor returns the number of outbound messages delivered to the intended recipient, without modification, since last system reset.

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.
Bind

The following templates are available:

- **Bind (Linux - v9.5 and earlier)**
- **Bind (Linux - v9.6 and higher)**
Bind (Linux - v9.5 and earlier)

This template assesses the performance of a Bind service on Linux machines. It uses Perl scripts for monitoring the performance of queries.

Prerequisites

SSH and Perl installed on the target server. SNMP installed on the target server and permission to monitor named processes.

If Perl is installed in a location different from /usr/bin/perl, you should correct all components in the first line of the Script Body field (#!/usr/bin/perl), or you can create a symbolic link to Perl (refer to documentation for the ln command).

You can find where Perl is installed by using the following command: which perl

Credentials

Root credentials on the target server.

Tested on CentOS 5.5 and Bind 9.3.6 version.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

You need to set thresholds for counters according to your environment. It is recommended to monitor counters for some period of time to understand potential value ranges and then set the thresholds accordingly. For more information, see "Using the Orion APM MIN/MAX Average Statistic Data historical charts for creating threshold settings based on 95th percentile line".

Queries Rate per Sec

This monitor returns rates per second of different queries. All rates are calculated as the number of specific queries for 20 seconds and then divided by 20. (Note: It is possible that scripts will return non-integer values. If this monitor is unavailable, it may be that this service is not running.) Returned values:

- Success - This component returns the number of successful queries per second that the name server handled. Successful queries are those that did not result in referrals or errors.
- Referral - This component returns the number of queries per second that the name server handled and resulted in referrals.
- Nxrrset - This component returns the number of queries per second that the name server handled and resulted in responses saying that the type of record the client requested did not exist for the domain name it specified.
- Nxdomain - This component returns the number of queries per second that the name server handled that resulted in responses saying that the domain name specified did not exist.
• Recursion - This component returns the number of queries that the name server received that required recursive processing to answer.
• Failure - This component returns the number of queries the name server received that resulted in errors other than those covered by nxrrset and nxdomain.
• Total - This component returns the total number of queries per second.

**SNMP Process Monitor: Named**

This component returns CPU and memory usage of the named daemon. If these counters are unavailable, there may be problems with SNMP configuration or the named service has stopped.
Bind (Linux - v9.6 and higher)

This template assesses the performance of a Bind service, version 9.6 and later, on Linux machines. It uses Perl scripts for monitoring the performance of queries.

Prerequisites

SSH and Perl installed on the target server. SNMP installed on the target server and permission to monitor named processes.

If Perl is installed in a location different from `/usr/bin/perl`, you should correct all components in the first line of the Script Body field (`#!/usr/bin/perl`), or you can create a symbolic link to Perl (refer to the documentation for the `ln` command).

You can find where Perl is installed by using the following command: `which perl`

Credentials

Root credentials on the target server.

Tested on CentOS 5.5 and Bind 9.9.2 version.

All monitors except SNMP Process Monitor: Named, has the Count statistic as difference option enabled and will show the statistical difference from the last SAM polling cycle.

All monitors except SNMP Process Monitor: Named, require the following arguments:

```
perl ${SCRIPT} path_to_rndc path_to_named.stats
```

where

- `path_to_rndc` - This is full path to the `rndc` command. By default: `/usr/local/sbin/rndc`.
- `path_to_named.stats` - This is full path to named.stat file, which is generated by the “rndc stats” command.

Below is an example using the Scripts Arguments field:

```
perl ${SCRIPT} /usr/local/sbin/rndc /var/named/named.stats
```

Monitored Components

For details on monitors, see [SAM Component Monitor Types](#).

You need to set thresholds for counters according to your environment. It is recommended to monitor counters for some period of time to understand potential value ranges and then set the thresholds accordingly. For more information, see "Using the Orion APM Min/Max/Average statistics data for creating threshold settings" in the [SolarWinds Success Center](#).

SNMP Process Monitor: Named

This component returns CPU and memory usage of the named daemon.
If these counters are unavailable, there may be problems with SNMP configuration or the named service has stopped.

Incoming Queries

This monitor returns the number of incoming queries for several RR type. You should provide correct arguments. If this monitor is unavailable, it may be that this service is not running. Returned values:

- **A** – This component returns the number of incoming A queries. This record is a 32-bit IP address.
- **NS** – This component returns the number of incoming NS queries. This record is the authoritative name server for the domain.
- **CNAME** – This component returns the number of incoming CNAME queries. This record identifies the canonical name of an alias.
- **SOA** – This component returns the number of incoming SOA queries. This record identifies the start of a zone of authority.
- **PTR** – This component returns the number of incoming PTR queries. This record is a pointer to another part of the domain name space.
- **MX** – This component returns the number of incoming MX queries. This record identifies a mail exchange for the domain with a 16-bit preference value (lower is better) followed by the host name of the mail exchange.
- **AAAA** – This component returns the number of incoming AAAA queries. This record is an IPv6 address.
- **SRV** – This component returns the number of incoming SRV queries. This record have information about well-known network services (replaces WKS).
- **A6** – This component returns the number of incoming A6 queries. This record is an IPv6 address. This can be a partial address (a suffix) and an indirection to the name where the rest of the address (the prefix) can be found.
- **Total** – This component returns the total number of all incoming queries.

Outgoing Queries

This monitor returns the number of outgoing queries for several RR type sent from the internal resolver. You should provide the correct arguments. If this monitor is unavailable, it may be that this service is not running. Returned values:

- **A** – This component returns the number of outgoing A queries. This record is a 32-bit IP address.
- **NS** – This component returns the number of outgoing NS queries. This record is the authoritative name server for the domain.
- **CNAME** – This component returns the number of outgoing CNAME queries. This record identifies the canonical name of an alias.
- **SOA** – This component returns the number of outgoing SOA queries. This record identifies the start of a zone of authority.
- **PTR** – This component returns the number of outgoing PTR queries. This record is a pointer to another part of the domain name space.
• **MX** – This component returns the number of outgoing MX queries. This record identifies a mail exchange for the domain with a 16-bit preference value (lower is better) followed by the host name of the mail exchange.

• **AAAA** – This component returns the number of outgoing AAAA queries. This record is an IPv6 address.

• **SRV** – This component returns the number of outgoing SRV queries. This record has information about well-known network services (replaces WKS).

• **A6** – This component returns the number of outgoing A6 queries. This record is IPv6 address. This can be a partial address (a suffix) and an indirection to the name where the rest of the address (the prefix) can be found.

• **Total** – This component returns the total number of all outgoing queries.

**Name Server Statistics 1**

This monitor returns the statistics counters about incoming request processing. You should provide correct arguments. If this monitor is unavailable, it may be that this service is not running. Returned values:

• **IPv4 requests received** – This component returns the number of IPv4 requests received. This also counts non query requests.

• **IPv6 requests received** – This component returns the number of IPv6 requests received. This also counts non query requests.

• **queries resulted in successful answer** – This component returns the number of queries resulted in a successful answer. This means the query which returns a NOERROR response with at least one answer RR.

• **queries resulted in authoritative answer** – This component returns the number of queries resulted in authoritative answer.

• **queries resulted in non authoritative answer** – This component returns the number of queries resulted in non authoritative answer.

• **queries resulted in nxrrset** – This component returns the number of queries resulted in NOERROR responses with no data.

• **queries resulted in SERVFAIL** – This component returns the number of queries resulted in SERVFAIL.

• **queries resulted in NXDOMAIN** – This component returns the number of queries resulted in NXDOMAIN.

• **queries resulted in referral answer** – This component returns the number of queries resulted in referral answer.

• **duplicate queries received** – This component returns the queries which the server attempted to recurse but discovered an existing query with the SAMe IP address, port, query ID, name, type and class already being processed.

**Name Server Statistics 2**

This monitor returns the statistics counters about incoming requests processing. You should provide the correct arguments. If this monitor is unavailable, it may be that this service is not running. Returned values:
• TCP requests received – This component returns the number of TCP requests received.
• auth queries rejected – This component returns the number of authoritative (non recursive) queries rejected.
• recursive queries rejected – This component returns the number of recursive queries rejected.
• update requests rejected – This component returns the number of dynamic update requests rejected.
• responses sent – This component returns the number of responses sent.
• queries dropped – This component returns the number of recursive queries for which the server discovered an excessive number of existing recursive queries for the same name, type, and class and were subsequently dropped.
• other query failures – This component returns the number of other query failures.
• queries caused recursion – This component returns the number of queries which caused the server to perform recursion to find the final answer.
• requests with EDNS(0) received – This component returns the number of requests with EDNS(0) received. Extension mechanisms for DNS (EDNS) is a specification for expanding the size of several parameters of the Domain Name System (DNS) protocol which had size restrictions that the Internet engineering community deemed too limited for increasing functionality of the protocol.
• responses with EDNS(0) sent – This component returns the number of responses with EDNS (0) sent. Extension mechanisms for DNS (EDNS) is a specification for expanding the size of several parameters of the Domain Name System (DNS) protocol which had size restrictions that the Internet engineering community deemed too limited for increasing functionality of the protocol.

Zone Maintenance Statistics

This monitor returns the statistics counters regarding zone maintenance operations such as zone transfers. You should provide the correct arguments. If this monitor is unavailable, it may be that this service is not running. Returned values:

• IPv4 notifies sent – This component returns the number of IPv4 notifies sent.
• IPv6 notifies sent – This component returns the number of IPv6 notifies sent.
• IPv4 notifies received – This component returns the number of IPv4 notifies received.
• IPv6 notifies received – This component returns the number of IPv6 notifies received.
• transfer requests succeeded – This component returns the number of zone transfer requests succeeded.
• transfer requests failed – This component returns the number of zone transfer requests failed.
• notifies rejected – This component returns the number of incoming notifies rejected.

Resolver Statistics 1

This monitor returns the statistics counters about name resolution performed in the internal resolver. You should provide correct arguments. If this monitor is unavailable, it may be that this service is not running. Returning values:
• **IPv4 queries sent** – This component returns the number of IPv4 queries sent.
• **IPv6 queries sent** – This component returns the number of IPv6 queries sent.
• **IPv4 responses received** – This component returns the number of IPv4 responses received.
• **IPv6 responses received** – This component returns the number of IPv6 responses received.
• **queries with RTT less than 10ms** – This component returns the number of queries with round trip times (RTTs) less than 10 ms.
• **queries with RTT 10 to 100ms** – This component returns the number of queries with round trip times (RTTs) between 10 and 100 ms.
• **queries with RTT 100 to 500ms** – This component returns the number of queries with round trip times (RTTs) between 100 and 500 ms.
• **queries with RTT 500 to 800ms** – This component returns the number of queries with round trip times (RTTs) between 500 and 800 ms.
• **queries with RTT 800 to 1600ms** – This component returns the number of queries with round trip times (RTTs) between 800 and 1600 ms.
• **queries with RTT more than 1600ms** – This component returns the number of queries with round trip times (RTTs) more than 1600 ms.

**Resolver Statistics 2**

This monitor returns the statistics counters about name resolution performed in the internal resolver. You should provide the correct arguments. If this monitor is unavailable, it may be that this service is not running. Returned values:

• **NXDOMAIN received** – This component returns the number of NXDOMAIN received.
• **SERVFAIL received** – This component returns the number of SERVFAIL received.
• **FORMERR received** – This component returns the number of FORMERR received.
• **other errors received** – This component returns the number of other errors received.
• **EDNS(0) query failures** – This component returns the number of EDNS(0) query failures.
• **query retries** – This component returns the number of query retries performed.
• **query timeouts** – This component returns the number of query timeouts.
• **lame delegations received** – This component returns the number of lame delegations received.
• **IPv4 NS address fetches** – This component returns the number of IPv4 NS address fetches invoked.
• **IPv4 NS address fetch failed** – This component returns the number of IPv4 NS address fetch failed.

**Socket I/O Statistics (IPv4)**

This monitor returns the statistics counters about network related events for IPv4. You should provide the correct arguments. If this monitor is unavailable, it may be that this service is not running. Returned values:

• **UDP/IPv4 sockets opened** – This component returns the number of sockets opened successfully.
• **UDP/IPv4 sockets closed** – This component returns the number of sockets closed.
- **UDP/IPV4 socket bind failures** – This component returns the number of failures of binding sockets.
- **UDP/IPV4 connections established** – This component returns the number of connections established successfully.
- **TCP/IPV4 sockets opened** – This component returns the number of sockets opened successfully.
- **TCP/IPV4 sockets closed** – This component returns the number of sockets closed.
- **TCP/IPV4 socket connect failures** – This component returns the number of failures of connecting sockets.
- **TCP/IPV4 connections established** – This component returns the number of connections established successfully.
- **TCP/IPV4 send errors** – This component returns the number of errors in socket send operations.
- **TCP/IPV4 recv errors** – This component returns the number of errors in socket receive operations.

**Socket I/O Statistics (IPv6)**

This monitor returns the statistics counters about network related events for IPv6. You should provide the correct arguments. By default, this monitor is disabled. If this monitor is unavailable, it may be that this service is not running. Returned values:

- **UDP/IPV6 sockets opened** – This component returns the number of sockets opened successfully.
- **UDP/IPV6 sockets closed** – This component returns the number of sockets closed.
- **UDP/IPV6 socket bind failures** – This component returns the number of failures of binding sockets.
- **UDP/IPV6 connections established** – This component returns the number of connections established successfully.
- **TCP/IPV6 sockets opened** – This component returns the number of sockets opened successfully.
- **TCP/IPV6 sockets closed** – This component returns the number of sockets closed.
- **TCP/IPV6 socket connect failures** – This component returns the number of failures of connecting sockets.
- **TCP/IPV6 connections established** – This component returns the number of connections established successfully.
- **TCP/IPV6 send errors** – This component returns the number of errors in socket send operations.
- **TCP/IPV6 recv errors** – This component returns the number of errors in socket receive operations.
BizTalk

The following templates are available:

- BizTalk Server 2010-2013 Adapters Performance Counters
- BizTalk Server 2010-2013 Availability Status
- BizTalk Server 2010-2013 Host Throttling Performance Counters
- BizTalk Server 2010-2013 Message Box and Orchestrations Performance Counters

BizTalk Server 2010-2013 Adapters Performance Counters

This template assesses the status and overall of performance of BizTalk adapters of default Microsoft BizTalk Server 2010 or 2013 installation. It monitors next adapters: Microsoft Message Queue (MSMQ), files from file system (FILE), FTP, HTTP, POP3, SMTP, SOAP and SQL.

Prerequisites

RPC access to the target server.

Credentials

Windows Administrator on the target server.

For monitoring a SharePoint server, you can also use “Internet Information Service (IIS) Services and Counters”, “Windows Server 2003-2008 Services and Counters” and “SQL Server 2005-2008 Performance” templates.

Monitored Components

For details on monitors, see [SAM Component Monitor Types](#).

**FILE Receive Adapter: Bytes received/Sec**

This component monitor returns the number of bytes received by the file receive adapter per second. The counter applies only to messages that have been completely read by the file adapter from the file system.

**FILE Receive Adapter: Lock failures/sec**

This component monitor returns the number of times the file receive adapter failed to lock the file per second.

**FILE Receive Adapter: Messages received/Sec**

This component monitor returns the number of messages received by the file receive adapter per second. The counter applies only to messages that have been completely read by the file receive adapter from the file system.
**FILE Receive Adapter: Time to build batch**

This component monitor returns the average time taken by file receive adapter to build a batch.

**FILE Send Adapter: Bytes sent/Sec**

This component monitor returns the number of bytes sent by the file send adapter per second. The counter applies only to messages that have been completely written to file system.

**FILE Send Adapter: Messages sent/Sec**

This component monitor returns the number of messages sent by the file send adapter per second. The counter applies only to messages that have been completely written to file system.

**FTP Receive Adapter: Bytes received/Sec**

This component monitor returns the number of bytes received by the FTP receive adapter per second. The counter applies only to messages that have been completely read by the FTP receive adapter from the FTP server.

**FTP Receive Adapter: Messages received/Sec**

This component monitor returns the number of messages received by the FTP receive adapter per second. The counter applies only to messages that have been completely read by the FTP receive adapter from the FTP server.

**FTP Send Adapter: Bytes sent/Sec**

This component monitor returns the number of bytes sent by the FTP send adapter per second. The counter applies only to messages that have been written to the destination FTP server.

**FTP Send Adapter: Messages sent/Sec**

This component monitor returns the number of messages sent by the FTP send adapter per second. The counter applies only to messages that have been written to destination FTP server.

**HTTP Receive Adapter: Memory queue size**

This component monitor returns the number of incoming messages in the HTTP receive adapter's internal memory queue.

**HTTP Receive Adapter: Messages received/Sec**

This component monitor returns the number of HTTP requests received by the HTTP receive adapter per second. The counter applies only to request messages that have been completely read by the HTTP receive adapter from the HTTP client.

**HTTP Receive Adapter: Messages sent/Sec**

This component monitor returns the number of HTTP responses sent by the HTTP receive adapter per second. The counter applies only to response messages that have been successfully sent to HTTP clients.

**HTTP Receive Adapter: Time to build batch**

This component monitor returns the average time taken by the HTTP receive adapter to build a message batch.
HTTP Send Adapter: Memory queue size
This component monitor returns the number of outgoing messages in the HTTP send adapter's internal memory queue.

HTTP Send Adapter: Messages received/Sec
This component monitor returns the number of HTTP responses received by the HTTP send adapter per second. The counter applies only to response messages that have been completely read by the HTTP send adapter from HTTP servers.

HTTP Send Adapter: Messages sent/Sec
This component monitor returns the number of HTTP requests sent by the HTTP send adapter per second. The counter applies only to request messages that have reached the destination URL.

MSMQ Receive Adapter: Bytes received/Sec
This component monitor returns the number of bytes received by the MSMQ receive adapter per second. The counter applies only to messages that have been completely read by the MSMQ receive adapter from the source queue.

MSMQ Receive Adapter: Messages received/Sec
This component monitor returns the number of messages received by the MSMQ receive adapter per second. The counter applies only to messages that have been completely read by the MSMQ receive adapter from the source queue.

MSMQ Send Adapter: Bytes sent/Sec
This component monitor returns the number of bytes sent by the MSMQ send adapter per second. The counter applies only to messages that have reached the destination queue.

MSMQ Send Adapter: Messages sent/Sec
This component monitor returns the number of messages sent by the MSMQ send adapter per second. The counter applies only to messages that have reached the destination queue.

POP3 Receive Adapter: Active sessions
This component monitor returns the number of open POP3 connections the POP3 adapter is managing at a time.

POP3 Receive Adapter: Bytes received/Sec
This component monitor returns the number of bytes downloaded by the POP3 adapter from a mail server per second.

POP3 Receive Adapter: Messages received/Sec
This component monitor returns the number of email messages downloaded by the POP3 adapter from mail server per second.

SMTP Send Adapter: Messages sent/Sec
This component monitor returns the number of messages sent by the SMTP adapter per second. The counter applies only to messages that have been transmitted to the SMTP server.
SOAP Receive Adapter: Messages received/Sec
This component monitor returns the number of messages received by the SOAP receive adapter per second. The counter applies only to request messages that have been completely read by the adapter from the SOAP client.

SOAP Send Adapter: Messages sent/Sec
This component monitor returns the number of messages sent by the SOAP send adapter per second. The counter applies only to messages that have reached the destination URL.

SQL Receive Adapter: Messages received/Sec
This component monitor returns the number of messages read by the SQL receive adapter from a SQL server per second.

SQL Send Adapter: Messages sent/Sec
This component monitor returns the number of messages sent by the SQL send adapter per second. The counter applies only to messages that have been written to the destination SQL table.

BizTalk Server 2010-2013 Availability Status
This template allows you to check the status of BizTalk statistics: Host Instances, Orchestrations, Send Ports and Send Port Group by using WMI queries.

Prerequisites
WMI access on target server.

Credentials
Administrator on target server.

Before using this template you should provide the correct names of instances/ports/orchestrations in the Query field. See notes for each particular monitor.

If BizTalk and SQL Server are on different servers, this template may not work due to a “double hop” issue, which causes the SQL database used by BizTalk to deny access to the WMI call being made to run the required query for monitoring.

Monitored Components
For details on monitors, see SAM Component Monitor Types.

Host Instance State
This component monitor returns the specific Host Instance service status.
Possible values:
- 1 – Stopped.
- 2 – Start pending.
- 3 – Stop pending.
- 4 – Running.
- 5 – Continue pending.
- 6 – Pause pending.
- 7 – Paused.
- 8 – Unknown.

You should set the correct Host Instance name in the Query field in: "Microsoft BizTalk Server HOSTNAME SERVER"

The Host Instance name begins with the phrase “Microsoft BizTalk Server”. Following that comes the Hostname of the BizTalk host to which this BizTalk host instance belongs (HOSTNAME). The last one is the BizTalk server name (SERVER).

Example: HOSTNAME=client1, SERVER=bizserver. The result of the Query field should be:
Select ServiceState From MSBTS_HostInstance where Name = "Microsoft BizTalk Server client1 bizserver"

**Orchestration Status**

This component monitor returns the specific Orchestration status.

Possible values:
- 1 – Unbound.
- 2 – Bound.
- 3 – Stopped.
- 4 – Started.

By default, this monitor is disabled.

You should set correct Orchestration name in the Query field.

Example: ORCHESTRATION_NAME=orch1. The result of the Query field should be:
Select OrchestrationStatus From MSBTS_Orchestration Where Name = "orch1"

**Send Port Status**

This component monitor returns the specific Send Port status.

Possible values:
- 1 – Bound - default state.
- 2 – Started - indicates the send port is started, and subscriptions are activated.
- 3 – Stopped - indicates the send port is enlisted, and subscriptions are created but they are deactivated.

⚠️ You should set correct Send Port name in the Query field.
Example: SEND_PORT_NAME=SendPort1. The result of the Query field should be: Select Status From MSBTS_SendPort Where Name = "SendPort1"

Send Port Status

This component monitor returns the specific Send Port Group status.

Possible values:

- 1 – Bound - default state.
- 2 – Started - indicates the send port group is started, and subscriptions are activated.
- 3 – Stopped - indicates the send port group is enlisted, and subscriptions are created but they are deactivated.

You should set the correct Send Port Group name in the Query field.

Example: SEND_PORT_GROUP_NAME=SendPortGroup1. The result of the Query field should be: Select Status From MSBTS_SendPortGroup Where Name = "SendPortGroup1"

BizTalk Server 2010-2013 Host Throttling Performance Counters

This template assesses the status and overall of performance of host throttling of default Microsoft BizTalk Server 2010 or 2013 installation.

Prerequisites

RPC access to the target server.

Credentials

Windows Administrator on the target server.

For monitoring a SharePoint server, you can also use “Internet Information Service (IIS) Services and Counters”, “Windows Server 2003-2008 Services and Counters” and “SQL Server 2005-2008 Performance” templates.

Monitored Components

The BizTalk:MessageAgent performance counters are provided for the explicit purpose of analyzing the throttling behavior of a host and therefore will not capture data unless the specified host is actively processing documents. This behavior is by design to prevent consuming system threads with performance monitor when throttling activities are not occurring.

Active instance count

This component monitor returns number of service instances active in memory. For the orchestration engine, a service instance refers to each running instance of an orchestration schedule. For the End Point Manager, a service instance may either correspond to a single stateless message, or to a collection of stateful messages.

Stateful instances are those that maintain certain state information about the messages associated with the instance. Messages belonging to a stateful instance are co-related in some form or the other. For example an ordered send port that maintains information about the ordering are considered stateful instances. Most messaging scenarios involve stateless instances where messages are processed completely independent of each other. Each such stateless instance corresponds to a single message within the EPM.

Database size

This component monitor returns number of messages in the database queues that this process has published. This value is measured by the number of items in the queue tables for all hosts and the number of items in the spool and tracking tables. If a process is publishing to multiple queues, this counter reflects the weighted average of all the queues.

If the host is restarted, statistics held in memory are lost. Since there is some overhead involved, BizTalk Server will resume gathering statistics only when there are at least 100 publishes with 5% of the total publishes within the restarted host process.

Database session

This component monitor returns number of concurrent MessageBox database connections being used.

High database session

This component monitor returns a flag indicating whether the number of currently opened database sessions exceeds the threshold.

Possible values:

- 0 – Normal
- 1 – Database session count exceeds threshold.

Threshold value is controlled by the “Database connection per CPU” value in the BizTalk Host Throttling settings. “Database connection per CPU” is the maximum number of concurrent database sessions (per CPU) allowed before throttling begins.

High database size

This component monitor returns a flag indicating whether the destination queue depth of all message box databases exceeds the threshold. If the host publishes to multiple queues, the weighted average across all destination queues is computed (based on recent publish statistics) and compared with the threshold.

Possible values:
Database size has grown beyond threshold

By default the host message count in database throttling threshold is set to a value of 50,000, which will trigger a throttling condition under the following circumstances:

- The total number of messages published by the host instance to the work, state, and suspended queues of the subscribing hosts exceeds 50,000.
- The number of messages in the spool table or the tracking table exceeds 500,000 messages.

If this occurs, then consider a course of action that will reduce the number of messages in the database. For example, ensure the SQL Server jobs in BizTalk Server are running without error and use the Group Hub page in the BizTalk Server Administration console to determine whether message build up is caused by large numbers of suspended messages.

**High in-process message count**

This component monitor returns a flag indicating whether the number of in-process messages exceeds the threshold.

Possible values:

- 0 – Normal
- 1 – In-process message count exceeds limit

If throttling is occurring, consider adjusting the “In-Process messages per CPU” setting. This parameter only affects outbound message throttling. Enter a value of 0 in the “In-Process messages per CPU” setting to disable throttling based on the number of in-process messages per CPU. The default value for the “In-Process messages per CPU” setting is 1,000. Note that modifying this value can also have an impact on low latency of messages and/or the efficiency of BizTalk resources.

**High message delivery rate**

This component monitor returns a flag indicating whether the message delivery rate is higher than the message processing rate.

Possible values:

- 0 – Normal
- 1 – Message delivery rate exceeds the message processing rate

High message delivery rates can be caused by high processing complexity, slow outbound adapters, or a momentary shortage of system resources.

**High message publishing rate**

This component monitor returns a flag indicating whether the message publishing request rate is higher than the message publishing completion rate.

Possible values:

- 0 – Normal
- 1 – Publishing request rate exceeds completion rate
If this occurs, then the database cannot keep up with the publishing rate of messages to the BizTalk MessageBox database.

**High process memory**

This component monitor returns a flag indicating whether the process memory consumption exceeds the threshold.

Possible values:

- 0 – Normal
- 1 – Process memory exceeds threshold.

The BizTalk Process Memory usage throttling threshold setting is the percentage of memory used compared to the sum of the working set size and total available virtual memory for the process if a value from 1 through 100 is entered. When a percentage value is specified the process memory threshold is recalculated at regular intervals.

**High system memory**

This component monitor returns a flag indicating whether the system-wide physical memory consumption exceeds the threshold.

Possible values

- 0 – Normal
- 1 – System memory exceeds threshold

The BizTalk Physical Memory usage throttling threshold setting is the percentage of memory consumption compared to the total amount of available physical memory if a value from 1 through 100 is entered. This setting can also be the total amount of available physical memory in megabytes if a value greater than 100 is entered. The default value is 0.

**High thread count**

This component monitor returns a flag indicating whether the thread count exceeds the threshold.

Possible values:

- 0 – Normal
- 1 – Thread count exceeds threshold

“Threads Per CPU” is the total number of threads in the host process including threads used by adapters. If this threshold is exceeded, BizTalk Server will try to reduce the size of the EPM thread pool and message agent thread pool. Thread based throttling should be enabled in scenarios where high load can lead to the creation of a large number of threads. This parameter affects both inbound and outbound throttling. Thread based throttling is disabled by default.

**Message delivery incoming rate**

This component monitor returns number of messages per second that are being delivered to the Orchestration engine or the Messaging engine in the given sample interval.

High message delivery rates can be caused by high processing complexity, slow outbound adapters, or a momentary shortage of system resources.
Message delivery outgoing rate

This component monitor returns number of messages per second that are being processed by the Orchestration engine or the Messaging engine in the given sample interval.

High message delivery rates can be caused by high processing complexity, slow outbound adapters, or a momentary shortage of system resources.

Message delivery throttling state

This component monitor returns a flag indicating whether the system is throttling message delivery (affecting XLANG message processing and outbound transports).

Possible values:

- 0 - Not throttling
- 1 - Throttling due to imbalanced message delivery rate (input rate exceeds output rate)
- 3 - Throttling due to high in-process message count
- 4 - Throttling due to process memory pressure
- 5 - Throttling due to system memory pressure
- 9 - Throttling due to high thread count
- 10 - Throttling due to user override on delivery

Message delivery delay (ms)

This component monitor returns the current delay in ms imposed on each message delivery batch (applicable if the message delivery is being throttled).

In regards to throttling, a delay is applied in the publishing or processing of the message, depending on whether the message is inbound or outbound. The delay period is proportional to the severity of the throttling condition. Higher severity throttling conditions will initiate a longer throttling period than lower severity throttling conditions. This delay period is adjusted up and down within certain ranges by the throttling mechanism as conditions change. Long message delivery delays may indicate heavy throttling due to high load. This counter should be less than 5000 ms.

Message delivery throttling state duration

This component monitor returns the number of seconds since the system entered this state. If the host is throttling, how long it has been throttling; if it is not throttling, how long since throttling was applied.

Message publishing incoming rate

This component monitor returns the number of messages per second that are being sent to the database for publishing in the given sample interval.

Message publishing outgoing rate

This component monitor returns the number of messages per second that are published in the database in the given sample interval.
**Message publishing throttling state**

This component monitor returns a flag indicating whether the system is throttling message publishing (affecting XLANG message processing and inbound transports).

Possible values:

- 0 - Not throttling
- 2 - Throttling due to imbalanced message publishing rate (input rate exceeds output rate)
- 4 - Throttling due to process memory pressure
- 5 - Throttling due to system memory pressure
- 6 - Throttling due to database growth
- 8 - Throttling due to high session count
- 9 - Throttling due to high thread count
- 11 - Throttling due to user override on publishing

**Message publishing delay (ms)**

This component monitor returns the current delay in ms imposed on each message publishing batch (applicable if the message publishing is being throttled and if the batch is not exempted from throttling).

In regards to throttling, a delay is applied in the publishing or processing of the message, depending on whether the message is inbound or outbound. The delay period is proportional to the severity of the throttling condition. Higher severity throttling conditions will initiate a longer throttling period than lower severity throttling conditions. This delay period is adjusted up and down within certain ranges by the throttling mechanism as conditions change. Long message delivery delays may indicate heavy throttling due to high load. This counter should be less than 5000 ms.

**Message publishing throttling state duration**

This component monitor returns the number of seconds since the system entered this state. If the host is throttling, how long it has been throttling; if it is not throttling, how long since throttling was applied.

**Process memory usage (MB)**

This component monitor returns the process memory consumption in MB. This is the maximum of the process's working set size and the total space allocated for the page file for the process.

BizTalk process memory throttling can occur if the batch to be published has steep memory requirements, or if too many threads are processing messages.

**Thread count**

This component monitor returns the number of threads being used within the process.
BizTalk Server 2010-2013 Message Box and Orchestrations Performance Counters

This template assesses the status and overall of performance of Message Box and Orchestrations of default Microsoft BizTalk Server 2010 or 2013 installation.

Prerequisites

RPC access to the target server.

Credentials

Windows Administrator on the target server.


Monitored Components

For details on monitors, see SAM Component Monitor Types.

Service: BizTalk Server Application

This component monitor shows the status of the BizTalk Server Service.

If this service is stopped, all performance counters related with BizTalk become unavailable.

Message Box (General): Instances - Total Number

This component monitor tracks the sum of all the instances of each host which exist within a particular Message Box.

The instance field is installation-specific. Open windows perfmon utility, find BizTalk:Message Box:General Counters category and check what instance this counter uses (for example: biztalkmsgboxdb:emily).

Message Box (General): Spool Size

This component monitor tracks the size of the spool on a particular message box on a particular server.

The instance field is installation-specific. Open windows perfmon utility, find BizTalk:Message Box:General Counters category and check what instance this counter uses (for example: biztalkmsgboxdb:emily).
Message Box (General): Tracking data size

This component monitor tracks the size of the tracking data table on a particular message box on a particular server.

The instance field is installation-specific. Open windows perfmon utility, find BizTalk:Message Box:General Counters category and check what instance this counter uses (for example: biztalkmsgboxdb:emily).

Message Box (Host Queue): Instance State Msg Refs – Length

This component monitor tracks the number of message references in the Instance State Queue for this particular host.

The instance field is installation-specific. Open windows perfmon utility, find BizTalk:Message Box:General Counters category and check what instance this counter uses (for example: biztalkmsgboxdb:emily).

Message Box (Host Queue): Length

This component monitor tracks the total number of messages in the particular host queue.

The instance field is installation-specific. Open windows perfmon utility, find BizTalk:Message Box:General Counters category and check what instance this counter uses (for example: biztalkmsgboxdb:emily).

This counter can be useful in determining if a specific host is bottlenecked. Assuming unique hosts are used for each transport, this can be helpful in determining potential transport bottlenecks. Host Queue Length is a weighted Queue length by aggregating the record count of all the Queues (Work Q, State Q, Suspended Q) of the target host. This counter should be near zero.

Message Box (Host Queue): Number of Instances

This component monitor tracks the number of instances of this particular host.

The instance field is installation-specific. Open windows perfmon utility, find BizTalk:Message Box:General Counters category and check what instance this counter uses (for example: biztalkmsgboxdb:emily).

Message Box (Host Queue): Suspended Msgs – Length

This component monitor tracks the total number of suspended messages for the particular host.

The instance field is installation-specific. Open windows perfmon utility, find BizTalk:Message Box:General Counters category and check what instance this counter uses (for example: biztalkmsgboxdb:emily).

The suspended message queue is a queue that contains work items for which an error or failure was encountered during processing. A suspended queue stores the messages until they can be corrected and reprocessed, or deleted. An increasing trend could indicate severe processing errors.
**Orchestrations: Average batch factor**

This component monitor returns the current ratio between the number of persistence points committed and underlying database transactions committed.

This metric is beneficial where the Orchestration engine merges multiple atomic transactions into a single transaction. Assuming that a "persistence point" is really a segment boundary, this metric provides some substantial facts about the effect of batching atomic transactions. The greater the number, the greater the effect of "transaction batching" (that is, the less underlying transactions are being created).

**Orchestrations: Database transactions**

This component monitor returns number of underlying database transactions used to commit orchestrations work.

**Orchestrations: Database transactions/sec**

This component monitor returns number of underlying database transactions used per second.

**Orchestrations: Dehydrating orchestrations**

This component monitor returns total number of dehydratable orchestrations which are currently in the process of dehydrating.

When many long-running business processes are running at the same time, memory and performance issues are possible. The orchestration engine addresses these issues by "dehydrating" and "rehydrating" orchestration instances. Dehydration is used to minimize the use of system resources by reducing the number of orchestrations that have to be instantiated in memory at one time. Therefore, dehydrations save memory consumption, but are relatively expensive operations to perform. If so, BizTalk Server may be running out of memory (either virtual or physical), a high number of orchestrations are waiting on messages, or the dehydration settings are not set properly. This counter should be less than 10.

**Orchestrations: Dehydration cycles**

This component monitor returns number of dehydration cycles completed.

**Orchestrations: Megabytes allocated private memory**

This component monitor returns megabytes of allocated private memory for the host instance.

Private Bytes is the current size, in bytes, of memory that a process has allocated that cannot be shared with other processes. A host instance consuming large portions of memory is fine as long as it returns the memory to the system. Look for increasing trends in the chart. An increasing trend over a long period of time could indicate a memory leak.

**Orchestrations: Megabytes allocated virtual memory**

This component monitor returns megabytes reserved for virtual memory for the host instance.

A host instance consuming large portions of memory is fine as long as it returns the memory to the system. Look for increasing trends in the chart. An increasing trend over a long period of time could indicate a memory leak.
**Orchestrations: MessageBox databases connection failures**

This component monitor returns number of attempted database connections that failed since the host instance started.

If the SQL Server service hosting the BizTalk databases becomes unavailable for any reason, the database cluster transfers resources from the active computer to the passive computer. During this failover process, the BizTalk Server service instances experience database connection failures and automatically restart to reconnect to the databases. The functioning database computer (previously the passive computer) begins processing the database connections after assuming the resources during failover.

**Orchestrations: Online MessageBox databases**

This component monitor returns number of MessageBox databases currently available to the application.

**Orchestrations: Orchestrations completed/sec**

This component monitor returns number of orchestrations completed per second.

This is a good indicator as to how much throughput BizTalk is processing.

**Orchestrations: Orchestrations created/sec**

This component monitor returns number of orchestrations created per second.

**Orchestrations: Orchestrations dehydrated/sec**

This component monitor returns number of orchestrations dehydrated per second.

**Orchestrations: Orchestrations discarded/sec**

This component monitor returns number of orchestrations discarded per second.

An orchestration can be discarded if the engine fails to persist its state. This counter should be always zero.

**Orchestrations: Orchestrations suspended/sec**

This component monitor returns number of orchestrations suspended per second.

Generally, suspended instances caused by system errors are resumable upon resolution of the system issue. Often, suspended instances due to a message problem are not resumable, and the message itself must be fixed and resubmitted to the BizTalk Server system. This counter should be always zero.

**Orchestrations: Pending work items**

This component monitor returns number of basic code blocks that are scheduled for to run.

**Orchestrations: Running orchestrations**

This component monitor returns number of orchestration instances currently executing.
Blackberry

The following templates are available:

- Blackberry Delivery Confirmation
- Blackberry Enterprise Server
- Blackberry Enterprise Server 10 Services (Windows)
- Blackberry Enterprise Server 10 Statistic (SNMP)
- Blackberry Enterprise Server 12 Services (Windows)
- Blackberry Enterprise Server 12 Statistics (SNMP)
Blackberry Delivery Confirmation

This template tests the ability of a Blackberry handheld device to receive messages using the built-in delivery confirmation function. The script in this template sends a specially formed test email to the blackberry device, and then the script checks an email account for the confirmation reply from the Blackberry device.

The script in this template requires you to customize variables before it can be run.

Prerequisites

Access to an SMTP Server, MAPI access to a Microsoft Exchange server, MAPI Client and CDO Objects installed on the SAM server.

Credentials

Windows credential valid on both the SAM server and the Microsoft Exchange server.

Customizing Script Variables

You must substitute your own values for many of the following variables in the script body:

```javascript
const SenderMailbox = "SAM.test"
Replace SAM.test with the Exchange mailbox for sending and receiving the delivery confirmation messages.

const SenderEmailAddress = sam.test@example.com
Replace sam.test@example.com with the email address for sending and receiving the test and the confirmation messages.

const BlackberryAddress = test.blackberry@example.com
Replace test.blackberry@example.com with the email address of the user with the Blackberry handheld device.

const ExchangeServer = "exchange.example.com"
Replace exchange.example.com with the Microsoft Exchange server hosting the Exchange mailbox.

const SenderSmtpServer = "smtp.example.com"
Replace smtp.example.com with the SMTP Server for sending the test email.

const SenderSmtpPort = 25
The script uses port 25 on the SMTP server for sending the test email. If the SMTP server uses a different port, change to match your port configuration.
```
const MaxInboxScans = 300

The script will scan for the confirmation message on the Exchange mailbox 300 times. Modify this value as you need, higher or lower.

const MaxMessagesPerScan = 100

The script will scan the most recent 100 messages in the Exchange mailbox for the confirmation message. Modify this value as you need, higher or lower.

const MillisecondsBetweenScans = 1000

The script will wait 1000 milliseconds between Exchange mailbox scans. Modify this value as you need, higher or lower.

Monitored Components

For details on monitors, see [SAM Component Monitor Types](#).

**BlackBerry Delivery Confirmation**

This monitor returns confirmation of delivered messages to the Blackberry handheld device.
Blackberry Enterprise Server

This template monitors the status of services and server statistics related to the operation of Blackberry Enterprise Servers.

Prerequisites

WMI access to target server.

Credentials

Windows Administrator on target server.

Monitored Components

For details on monitors, see [SAM Component Monitor Types](#).

Blackberry Router Service

Net Service Name: Blackberry Router

Blackberry Alert Service

Net Service Name: Blackberry Alert

Blackberry Attachment Service

Net Service Name: Blackberry Attachment Service

Blackberry Collaboration Service

Net Service Name: Blackberry Collaboration Service

Blackberry Controller Service

Net Service Name: Blackberry Controller

Blackberry MDS Connection Service

Net Service Name: Blackberry MDS Connection Service

Blackberry Policy Service

Net Service Name: Blackberry Policy Service

Blackberry Synchronization Service

Net Service Name: Blackberry Synchronization Service

Blackberry Convert Process

Process name: BBConvert.exe

Connection State

0 is disconnected, 1 is connected.
Messages Expired

The total number of expired messages.

Messages Queued for Delivery

The number of pending messages queued for handheld device delivery.

Messages Received per Minute

The average number of messages per minute received by handheld device.

Messages Sent per Minute

The average number of messages per minute sent by handheld device.

Blackberry Enterprise Server 10 Services (Windows)

This template assesses the status and overall of services and performance of a BlackBerry Enterprise Server 10 installed on Windows machine.

Prerequisites

WMI access to the target server.

Credentials

Windows Administrator on the target server.

Monitored Components

For details on monitors, see [SAM Component Monitor Types](#).

**Service: Administration Console**

An administration console that permits you to manage iOS devices and Android devices.

**Service: BlackBerry Administration Service - Application Server**

This is the Application Server of the BlackBerry Administration Service.

**Service: BlackBerry Administration Service - Native Code Container**

This is the Native Code Container of the BlackBerry Administration Service.

**Service: BlackBerry Controller**

Monitors components and restarts them if they stop responding.

**Service: BlackBerry Dispatcher**

Performs data encryption and compression services for data that BlackBerry devices send or receive through the BlackBerry Infrastructure.
Service: BlackBerry Licensing Service
If registered as the active licensing server, stores the licenses for use.

Service: BlackBerry Management Studio
An administration console that permits you to manage BlackBerry devices, iOS devices, and Android devices.

Service: BlackBerry MDS Connection Service
Provides a communication channel for BlackBerry devices to access application servers and content servers on your organization’s intranet or on the Internet.

Service: BlackBerry Secure Connect Service
Maintains a connection through the BlackBerry Infrastructure with the BES10 Client on iOS devices and Android devices.

Service: BlackBerry Web Services
An add-on to the Universal Device Service that contains administrative APIs that are exposed as web services.

Service: BlackBerry Work Connect Notification Service
Sends notifications to iOS devices when new email messages and calendar entries are available in the Work Connect app.

Service: Enterprise Management Web Service
Sends profiles, applications, IT policies, and IT administration commands to BlackBerry devices.

TCP Port: Admin Service (HTTP)
This component monitor tests the ability of a BES Admin service to accept incoming sessions by HTTP. By default it monitors TCP port 38180.

TCP Port: Admin Service (HTTPS)
This component monitor tests the ability of a BES Admin service to accept incoming sessions by HTTPS. By default it monitors TCP port 38443.

TCP Port: Licensing Server
This component monitor tests the ability of a BES Licensing service to accept incoming sessions by HTTPS. By default it monitors TCP port 3333.

TCP Port: Universal Device Service
This component monitor tests the ability of a BES Universal Device service to accept incoming sessions by HTTPS. By default it monitors TCP port 6443.

TCP Port: BlackBerry Management Studio
This component monitor tests the ability of a BES Management Studio to accept incoming sessions by HTTPS. By default it monitors TCP port 7443.
Error and Warning Events: BlackBerry MDS Connection Service
This monitor returns the number of error and warning events generated by BlackBerry MDS Connection Service. This monitor should be as low as possible. If returning value is more than zero you should investigate application log for details.

Error and Warning Events: BES10 - BlackBerry Controller
This monitor returns the number of error and warning events generated by BlackBerry Controller. This monitor should be as low as possible. If returning value is more than zero you should investigate application log for details.

APN Gateway: Pokes Failed Per Second
This monitor returns the number of failed APNs pokes per second.

APN Gateway: Pokes Per Second
This monitor returns the number of successful APNs pokes per second.

Core Client: Exceptions Per Second
This monitor returns the number of exceptions during requests to core per sec.

Core Client: Requests Per Second
This monitor returns the number of requests sent to core per sec.

Core Client: Timeout Exceptions Per Second
This monitor returns the number of timeout exceptions during requests to core per sec.

Core: Non Scheduled Poke Requests Per Second
This monitor returns the number of non-scheduled (non-polling) poke requests per second.

Core: Scheduled Poke Requests Per Second
This monitor returns the number of scheduled (polling) poke requests per second.

Data Provider: SQL Requests Failed Per Second
This monitor returns the number of failed SQL requests per second.

Data Provider: SQL Requests Per Second
This monitor returns the number of performed SQL requests per second.

EAS Sync Service: Devices to EAS Sync Current
This monitor returns the number of devices that are in the process of being EAS synched.

EAS Sync Service: Request Failed
This monitor returns the number of failed requests from EAS sync plug-in.

EAS Sync Service: Users to EAS Sync Current
This monitor returns the number of users that are in the process of being EAS whitelist synched.
**iOS: Active Communications**

This monitor returns the number of iOS device active communications.

**iOS: Idle Commands Received Per Second**

This monitor returns the number of iOS device received Idle command per second.

**Nagging Service: Devices to Nag Current**

This monitor returns the number of devices that are in the process of being nagged.

**Poke Service: Devices to Poke Current**

This monitor returns the number of devices that are in the process of being poked.

**SWSM: Connections Failed Per Second**

This monitor returns the number of failed requests to Secure Work Space Manager performed per second.

**SWSM: Connections Per Second**

This monitor returns the number of requests to Secure Work Space Manager performed per second.

---

**Blackberry Enterprise Server 10 Statistic (SNMP)**

This template assesses the status and overall performance of a BlackBerry Enterprise Server (BES) 10 by using SNMP protocol. You can use the Orion agent for Linux or SNMP agentless to monitor.

**Prerequisites for Orion agent for Linux**

If using Orion agent for Linux for monitoring, you may need to complete additional configurations. If using SNMP v2, the Orion agent for Linux automatically configures SNMP. If using SNMP v3, see [SNMP for agents](#).

**Prerequisites**

WMI access to the target server.

**Credentials**

Windows Administrator on the target server.

**Monitored Components**

For details on monitors, see [SAM Component Monitor Types](#).

**Dispatcher: Threads Number**

This monitor returns the number of threads that are running in the BlackBerry Enterprise Server environment.

OID: .1.3.6.1.4.1.3530.7.7.15.20.5.1.2.1.3
Dispatcher: Pending Transactions

This monitor returns the number of transactions pending in the processing queue.

OID: .1.3.6.1.4.1.3530.7.7.15.20.5.1.4.1.3

Dispatcher: Proxy Messages Sent to Devices

This monitor returns the number of IP proxy messages sent to all BlackBerry devices.

OID: .1.3.6.1.4.1.3530.7.7.15.30.29.1.2.1.3

- This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

Dispatcher: Proxy Messages Sent from Devices

This monitor returns the number of IP proxy messages sent from all BlackBerry devices.

OID: .1.3.6.1.4.1.3530.7.7.15.30.30.1.2.1.3

- This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

Dispatcher: Total Messages Sent to Devices

This monitor returns the total number of messages sent to all BlackBerry devices.

OID: .1.3.6.1.4.1.3530.7.7.15.30.33.1.2.1.3

- This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

Dispatcher: Total Messages Sent from Devices

This monitor returns the total number of messages sent from all BlackBerry devices.

OID: .1.3.6.1.4.1.3530.7.7.15.30.34.1.2.1.3

- This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

MDS Connection Service: Threads Number

This monitor returns the number of threads that are running in the BlackBerry Enterprise Server environment.

OID: .1.3.6.1.4.1.3530.7.7.40.20.5.1.2.1.13

MDS Connection Service: Pending Transactions in Queue

This monitor returns the number of transactions pending in the processing queue.

OID: .1.3.6.1.4.1.3530.7.7.40.20.5.1.4.1.13
**MDS Connection Service: Users with Enabled MDS Connection Service on Devices**

This monitor returns the number of users that have the BlackBerry MDS Connection Service enabled on their BlackBerry devices.

OID: .1.3.6.1.4.1.3530.7.7.40.20.5.1.6.1.13

**MDS Connection Service: Total Size of Received from Devices Packets (kB)**

This monitor returns the total size of the data packets received from all BlackBerry devices on connections initiated by BlackBerry devices, in kB.

OID: .1.3.6.1.4.1.3530.7.7.40.40.10.1.2.1.13

ℹ️ This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

**MDS Connection Service: Total Size of Sent to Devices Packets (kB)**

This monitor returns the total size of the data packets sent to BlackBerry devices on connections initiated by BlackBerry devices, in kB.

OID: .1.3.6.1.4.1.3530.7.7.40.40.10.1.4.1.13

ℹ️ This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

**MDS Connection Service: Total Number of Received from Devices Packets**

This monitor returns the total number of data packets received from all BlackBerry devices on connections initiated by BlackBerry devices.

OID: .1.3.6.1.4.1.3530.7.7.40.40.10.1.6.1.13

ℹ️ This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

**MDS Connection Service: Total Number of Sent to Devices Packets**

This monitor returns the total number of the data packets sent to BlackBerry devices on connections initiated by BlackBerry devices.

OID: .1.3.6.1.4.1.3530.7.7.40.40.10.1.10.1.13

ℹ️ This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

**MDS Connection Service: Total Number of Push Connections**

This monitor returns the total number of push connections initiated by BlackBerry devices.

OID: .1.3.6.1.4.1.3530.7.7.40.40.10.1.12.1.13

ℹ️ This component has Count statistic as difference enabled. It will return the difference
MDS Connection Service: Number of Packets Declined

This monitor returns the number of packets that the BlackBerry Dispatcher declined.

OID: .1.3.6.1.4.1.3530.7.7.40.40.15.1.6.1.13

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

MDS Connection Service: Number of Invalid Sent Packets

This monitor returns the number of invalid packets sent to the BlackBerry Dispatcher.

OID: .1.3.6.1.4.1.3530.7.7.40.40.15.1.8.1.13

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

MDS Connection Service: Number of Truncated Connections

This monitor returns the number of truncated connections.

OID: .1.3.6.1.4.1.3530.7.7.40.40.15.1.10.1.13

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

MDS Connection Service: Not Delivered Push Connections

This monitor returns the number of push connections that could not be delivered within the default timeout. This is reported only for push messages that do not have a specified delivery timeout.

OID: .1.3.6.1.4.1.3530.7.7.40.40.15.1.14.1.13

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

MDS Connection Service: Successful SRP Connections

This monitor returns the number of successful SRP connections to the BlackBerry Dispatcher.

OID: .1.3.6.1.4.1.3530.7.7.40.40.15.1.16.1.13

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

MDS Connection Service: Failed SRP Connections

This monitor returns the number of failed SRP connections to the BlackBerry Dispatcher.

OID: .1.3.6.1.4.1.3530.7.7.40.40.15.1.18.1.13
Blackberry Enterprise Server 12 Services (Windows)

This template assesses the status and overall of services and performance of a Blackberry Enterprise Server 12 installed on Windows machines.

For the SNMP version, see Blackberry Enterprise Server 12 Statistics (SNMP).

Prerequisites

WMI access to the target server.

Credentials

Windows Administrator on the target server.

Portions of this document were compiled from the information found at http://us.blackberry.com/enterprise/products/bes12.html

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Service: Blackberry Core

This monitor provides authentication and authorization services for BES. Is responsible for scheduling and sending commands, IT policies and profiles to devices, and logging, monitoring, reporting, and managing functions.

Service: Blackberry Affinity Manager

Maintains an active SRP connection to the Blackberry Infrastructure and manages changes in device relationships in a BES domain.

The Manager assigns Blackberry devices to a BES instance, monitors enterprise connectivity for each instance, and moves Blackberry users if there are issues with enterprise connectivity.

Service: Blackberry Dispatcher

This monitor maintains an active SRP connection to the Blackberry Infrastructure and manages changes in device relationships in a BES domain.

The Manager assigns Blackberry devices to a BES instance, monitors enterprise connectivity for each instance, and moves Blackberry users if there are issues with enterprise connectivity.

Service: Blackberry Gatekeeping Service

This monitor adds devices to the Exchange ActiveSync list of devices that are allowed to connect to the mail server. The Service assures that only devices managed by BES12 can access work email and other work information on the device.
Service: BlackBerry MDS Connection Service

This monitor provides a secure connection between BlackBerry devices and intranet network when the device is not connected to your work Wi-Fi network or using a VPN connection. It also provides enterprise data push services for BlackBerry devices.

Service: BlackBerry Secure Connect Plus

This monitor provides a secure IP tunnel between work applications on devices and the intranet. One tunnel that supports standard IPv4 (TCP and UDP) data is established for each device through the BlackBerry Infrastructure.

Service: BlackBerry Work Connection Notification Service

Sends new and changed email and organizer notifications to iOS devices that are using Secure Work Space.

Service: BlackBerry Management console

Web-based interface used to complete post-installation configuration settings. View and manage users, devices, policies, profiles, applications, system settings, and move IT policies, profiles, groups, and users to BES12.

Provides access to BES12 Self-Service and allows iOS device users to manage apps using the Work Apps icon.

Blackberry Affinity Manager RCP Listener

The port that the active BlackBerry Affinity Manager listens on for RCP connections from the BlackBerry Dispatcher.

BlackBerry Dispatcher BIPPe Listener

The port that the BlackBerry Dispatcher listens on for BIPPe connections from the BlackBerry MDS Connection Service.

Self-Service Portal

The ports that BES12 Self-Service and the management console listen on for HTTPS connections.

Management Console

The ports that BES12 Self-Service and the management console listen on for HTTPS connections.

BlackBerry Affinity Manager ReST Listener

The port that the active BlackBerry Affinity Manager listens on for REST notifications.

Work Connect Notification Service Listener

The secure SSL port that the BlackBerry Work Connect Notification Service listens on.

BlackBerry Core Listener

The port that the administration console uses to connect to the BES12 Core.

BlackBerry Secure Connect Plus Listener

The port that the BES12 Core uses to check the status of BlackBerry Secure Connect Plus.
BlackBerry Internal Communication Listener

The port that is used for internal communication between the BES12 Core and the management console and BES12 Self-Service.

Device Management Requests Listener

The port that BES12 uses to receive management requests for BlackBerry 10 devices. The connection uses mutual authentication with ECC certificates.

BlackBerry Device Enrollment Requests Listener

The port that BES12 uses to receive enrollment requests for BlackBerry 10 devices.

iOS/Android/Windows Phone Device Enrollment Requests Receiver

The port that BES12 uses to receive enrollment requests for iOS, Android, and Windows phone devices.

iOS/Android/Windows Phone Device Management Requests Receiver

The port that BES12 uses to receive management requests for iOS, Android, and Windows phone devices. The connection uses mutual authentication with RSA certificates.

iOS Management Requests Receiver

An additional port that BES12 uses to receive management requests for iOS devices. The connection uses mutual authentication with RSA certificates.

Authenticated Connection Status Check Listener

The port that BES12 uses for authenticated connections to check the status of BES12 instances.

BlackBerry Secure Connect Plus SCEP Requests Receiver

The port that the BES12 Core uses to handle SCEP requests for BlackBerry Secure Connect Plus (the BES12 Core acts as the CA).

BlackBerry Gatekeeping Service Listener

The secure SSL port that the BlackBerry Gatekeeping Service listens on.

BlackBerry MDS Connection Service Listener

The HTTP port that the BlackBerry MDS Connection Service listens on for enterprise push data.

BlackBerry Secure Connect Plus Listener

The port that BlackBerry Secure Connect Plus uses to listen for signaling requests from the BlackBerry infrastructure.

BlackBerry Web Service Listener

The port that applications can use to send data to the BlackBerry Web Services.

BlackBerry Core iOS Email Notification Listener

The port that the BES12 Core listens on to route email notification traffic through the BlackBerry infrastructure to the APNs for iOS devices.
**BlackBerry Core Migration Listener**

The port that the BES12 Core listens on for migration requests when you move devices from BES10 to BES12.

**iOS/Android Secure Work Space Listener**

The port that supports Secure Work Space traffic from iOS and Android devices through the BES12 Core and BlackBerry Infrastructure to connect to work resources.

**BlackBerry Router Listener**

The port that your organization's TCP proxy server or the BlackBerry Router listens on for data that BES12 sends to the APNs.

**Error and Warning Events: BlackBerry MDS Connection Service**

This monitor returns the number of error and warning events generated by BlackBerry MDS Connection Service. This monitor should be as low as possible. If the returned value is greater than zero, you should investigate the application log for details.

---

**Blackberry Enterprise Server 12 Statistics (SNMP)**

This template assesses the status and overall performance of a BlackBerry Enterprise Server (BES) 12 by using SNMP protocol. You can use the Orion agent for Linux or SNMP agentless to monitor.

For the Windows version, see [Blackberry Enterprise Server 12 Services (Windows)](https://www.solarwinds.com/products/blackberry-enterprise-server-12-services).

**Prerequisites for Orion agent for Linux**

If using Orion agent for Linux for monitoring, you may need to complete additional configurations. If using SNMP v2, the Orion agent for Linux automatically configures SNMP. If using SNMP v3, see [SNMP for agents](https://www.solarwinds.com/products/blackberry-enterprise-server-12-services).

**Prerequisites**

WMI access to the target server.

**Credentials**

Windows Administrator on the target server.

**Notification Queues monitors**

All notification queue monitors require additional configuration in the BlackBerry Enterprise Server administration page. To enable SNMP monitor for BES12 Core service, use port 1610.

**Monitored Components**

For details on monitors, see [SAM Component Monitor Types](https://www.solarwinds.com/products/blackberry-enterprise-server-12-services).
Dispatcher: Pending Transactions

BlackBerry uses internal queues for transactions' handling process. This monitor returns the number of transactions pending in the processing queue.

OID: .1.3.6.1.4.1.3530.8.7.15.20.5.1.4.1.6

Dispatcher: Users

This monitor returns the number of users assigned to the service.

OID: .1.3.6.1.4.1.3530.8.7.15.20.5.1.6.1.6

Dispatcher: Work Requests Packets

This monitor returns the number of work request packets in the BlackBerry interprocess protocol engine queue.

OID: .1.3.6.1.4.1.3530.8.7.15.20.5.1.8.1.6

Dispatcher: Messages Sent to Devices

This monitor returns the number of messages sent to all BlackBerry devices connected to this dispatcher.

OID: .1.3.6.1.4.1.3530.8.7.15.30.33.1.2.1.6

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

Dispatcher: Messages Sent from Devices

This monitor returns the total number of messages sent from all BlackBerry devices connected to this dispatcher.

OID: .1.3.6.1.4.1.3530.8.7.15.30.34.1.2.1.6

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

MDS Connection Service: Pending Transactions in Queue

BlackBerry uses internal queues for transactions' handling process. This monitor returns the number of transactions pending in the processing queue.

OID: .1.3.6.1.4.1.3530.8.7.40.20.5.1.4.1.1

MDS Connection Service: Number of Packets Declined

This monitor returns the number of packets that the BlackBerry Dispatcher declined.

OID: .1.3.6.1.4.1.3530.8.7.40.40.15.1.6.1.1

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.
MDS Connection Service: Number of Invalid Sent Packets

This monitor returns the number of invalid packets sent to the BlackBerry Dispatcher.

OID: .1.3.6.1.4.1.3530.8.7.40.40.15.1.8.1.1

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

MDS Connection Service: Number of Expired IPPP Packets

This monitor returns the number of expired IPPP packets.

OID: .1.3.6.1.4.1.3530.8.7.40.40.15.1.9.1.1

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

MDS Connection Service: Number of Timeout Push Connections

This monitor returns the number of push connections that could not be delivered within the default timeout. The monitor reported only for push messages that do not have a specified delivery timeout.

OID: .1.3.6.1.4.1.3530.8.7.40.40.15.1.14.1.1

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

MDS Connection Service: Number of Declined IPPP Connections

This monitor returns the number of declined IPPP connections.

OID: .1.3.6.1.4.1.3530.8.7.40.40.15.1.15.1.1

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

MDS Connection Service: Successful SRP Connections

This monitor returns the number of successful Server Routing Protocol (SRP) connections to the BlackBerry Dispatcher.

OID: .1.3.6.1.4.1.3530.8.7.40.40.15.1.16.1.1

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

MDS Connection Service: Failed SRP Connections

This monitor returns the number of failed Server Routing Protocol (SRP) connections to the BlackBerry Dispatcher.

OID: .1.3.6.1.4.1.3530.8.7.40.40.15.1.18.1.1
This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

**MDS Connection Service: Failed Outbound TCP Socket Connections**
This monitor returns the number of outbound TCP socket connections that failed to open.
OID: .1.3.6.1.4.1.3530.8.7.40.70.5.1.34.1.1

**MDS Connection Service: Active Outbound TCP Socket Connections**
This monitor returns the number of outbound TCP socket connections that were open/active.
OID: .1.3.6.1.4.1.3530.8.7.40.70.5.1.36.1.1

**MDS Connection Service: Opened Outbound TCP Socket Connections**
This monitor returns the number of outbound TCP socket connections that were successfully opened.
OID: .1.3.6.1.4.1.3530.8.7.40.70.5.1.38.1.1

**MDS Connection Service: Closed Outbound TCP Socket Connections**
This monitor returns the number of outbound TCP socket connections that were successfully closed.
OID: .1.3.6.1.4.1.3530.8.7.40.70.5.1.40.1.1

**MDS Connection Service: Number of Packets Sent to External Servers**
This monitor returns the number of the data packets sent over outbound TCP socket connections to external servers.
OID: .1.3.6.1.4.1.3530.8.7.40.70.5.1.42.1.1

**MDS Connection Service: Number of Packets Received from External Servers**
This monitor returns the number of data packets received over outbound TCP socket connections from external servers.
OID: .1.3.6.1.4.1.3530.8.7.40.70.5.1.44.1.1

**MDS Connection Service: Number of Active IPPP/TCP Connections**
This monitor returns the number of active IPPP/TCP connections.
OID: .1.3.6.1.4.1.3530.8.7.40.80.5.1.2.1.1

**MDS Connection Service: Size of Packets Received over TCP connections (kB)**
This monitor returns the size of the data packets received over TCP connections, in kB.
OID: .1.3.6.1.4.1.3530.8.7.40.80.5.1.4.1.1
MDS Connection Service: Size of Packets Sent over TCP connections (kB)

This monitor returns the size of the data packets sent over TCP connections, in kB.

OID: .1.3.6.1.4.1.3530.8.7.40.80.5.1.6.1.1

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

MDS Connection Service: Number of Socket Connection Errors

This monitor returns the number of socket connection errors.

OID: .1.3.6.1.4.1.3530.8.7.40.80.5.1.8.1.1

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

Affinity Manager: Number of Bytes Received over RCP connections

This monitor returns the number of bytes received over RCP connections.

OID: .1.3.6.1.4.1.3530.8.7.145.15.5.1.4.1.0

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

Affinity Manager: Number of Bytes Sent over RCP connections

This monitor returns the number of bytes sent over RCP connections.

OID: .1.3.6.1.4.1.3530.8.7.145.15.5.1.6.1.0

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

Affinity Manager: Number of Received Operations over RCP connections

This monitor returns the number of received operations over RCP connections.

OID: .1.3.6.1.4.1.3530.8.7.145.15.5.1.8.1.0

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

Affinity Manager: Number of Sent Operations over RCP connections

This monitor returns the number of sent operations over RCP connections.

OID: .1.3.6.1.4.1.3530.8.7.145.15.5.1.10.1.0

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.
**Affinity Manager: Number of External RCP connections**

This monitor returns the number of external RCP connections.

OID: .1.3.6.1.4.1.3530.8.7.145.15.5.1.12.1.0

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

**Affinity Manager: Number of Internal Server connections**

This monitor returns the number of internal server connections.

OID: .1.3.6.1.4.1.3530.8.7.145.15.5.1.14.1.0

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

**Reconciliation Process: Number of Requests**

This monitor returns the number of reconciliation requests.

OID: .1.3.6.1.4.1.3530.8.1.1.2.1.1.0

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

**Reconciliation Process: Time Taken by the Last Process**

This monitor returns the time taken by the last reconciliation process.

OID: .1.3.6.1.4.1.3530.8.1.1.2.1.4.0

**Reconciliation Process: Time Taken by All Processes**

This monitor returns the time taken by all reconciliation processes.

OID: .1.3.6.1.4.1.3530.8.1.1.2.1.5.0

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

**Core: Number Of Connections to BlackBerry Infrastructure**

This monitor returns the number of connections between BES12 Core and the BlackBerry Infrastructure.

OID: .1.3.6.1.4.1.3530.8.1.1.2.100.1.0

**Core: Number Of Failed Connections to BlackBerry Infrastructure**

This monitor returns the number of failed connections between BES12 Core and the BlackBerry Infrastructure.

OID: .1.3.6.1.4.1.3530.8.1.1.2.100.2.0
Core: Bytes Received from the BlackBerry Infrastructure

This monitor returns bytes received from the BlackBerry Infrastructure.

OID: .1.3.6.1.4.1.3530.8.1.1.2.100.4.0

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

Core: Bytes Sent to the BlackBerry Infrastructure

This monitor returns bytes sent to the BlackBerry Infrastructure.

OID: .1.3.6.1.4.1.3530.8.1.1.2.100.5.0

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

Android Notification Queue: New Notifications

BES internally uses a queue to notify Android devices. This monitor returns the number of new notifications added to the Android notification queue.

OID: .1.3.6.1.4.1.3530.8.1.1.3.1.1.0

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

Android Notification Queue: Size

BES internally uses a queue to notify Android devices. This monitor returns the size of Android notification queue.

OID: .1.3.6.1.4.1.3530.8.1.1.3.1.2.0

Android Notification Queue: Handled Notifications

BES internally uses a queue to notify Android devices. This monitor returns the number of notifications taken from the Android notification queue.

OID: .1.3.6.1.4.1.3530.8.1.1.3.1.3.0

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

Apple Notification Queue: New Notifications

BES internally uses a queue to notify Apple devices. This monitor returns the number of new notifications added to the Apple notification queue.

OID: .1.3.6.1.4.1.3530.8.1.1.3.2.1.0

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.
Apple Notification Queue: Size

BES internally uses a queue to notify Apple devices. This monitor returns the size of Apple notification queue.

OID: .1.3.6.1.4.1.3530.8.1.3.2.2.0

Apple Notification Queue: Handled Notifications

BES internally uses a queue to notify Apple devices. This monitor returns the number of notifications taken from the Apple notification queue.

OID: .1.3.6.1.4.1.3530.8.1.3.2.3.0

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

BlackBerry Notification Queue: New Notifications

BES internally uses a queue to notify BlackBerry devices. This monitor returns the number of new notifications added to the BlackBerry notification queue.

OID: .1.3.6.1.4.1.3530.8.1.3.4.1.0

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

BlackBerry Notification Queue: Size

BES internally uses a queue to notify BlackBerry devices. This monitor returns the size of BlackBerry notification queue.

OID: .1.3.6.1.4.1.3530.8.1.3.4.2.0

BlackBerry Notification Queue: Handled Notifications

BES internally uses a queue to notify BlackBerry devices. This monitor returns the number of notifications taken from the BlackBerry notification queue.

OID: .1.3.6.1.4.1.3530.8.1.3.4.3.0

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

Device REST Notification Queue: New Notifications

BES internally uses a queue to notify other types of devices (e.g. Windows). This monitor returns the number of new notifications added to the Device REST notification queue.

OID: .1.3.6.1.4.1.3530.8.1.3.7.1.0

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.
Device REST Notification Queue: Size

BES internally uses a queue to notify other types of devices (e.g. Windows). This monitor returns the size of Device REST notification queue.

OID: .1.3.6.1.4.1.3530.8.1.1.3.7.2.0

Device REST Notification Queue: Handler Notifications

BES internally uses a queue to notify other types of devices (e.g. Windows). This monitor returns the number of notifications taken from the Device REST notification queue.

OID: .1.3.6.1.4.1.3530.8.1.1.3.7.3.0

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

Download REST Notification Queue: New Notifications

BES internally uses a Download REST queue. This monitor returns the number of new notifications added to the queue.

OID: .1.3.6.1.4.1.3530.8.1.1.3.9.1.0

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

Download REST Notification Queue: Size

BES internally uses a Download REST queue. This monitor returns the size of the queue.

OID: .1.3.6.1.4.1.3530.8.1.1.3.9.2.0

Download REST Notification Queue: Handler Notifications

BES internally uses a Download REST queue. This monitor returns the number of notifications taken from the queue.

OID: .1.3.6.1.4.1.3530.8.1.1.3.9.3.0

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.
Cisco

The following templates are available:

- Cisco CallManager
- CiscoSecure ACS (via SNMP)
- CiscoWorks LAN Management Solution
Cisco CallManager

This template monitors critical events generated by Cisco CallManager indicating possible service outages or configuration problems. Alerts are set to display the descriptions of events and the host name.

Prerequisites

SNMP access to target server.

Credentials

None

Monitored Components

For details on monitors, see SAM Component Monitor Types.

CallManager Status

The current status of the CallManager. Status 1 is unknown, 2 is up, 3 is down.

Registered Phones

The number of phones registered with the local call manager.

Unregistered Phones

The number of phones not registered with the local call manager.

Rejected Phones

The number of phones refused registration by the local call manager.

Registered Gateways

The number of gateways registered with the local call manager.

Unregistered Gateways

The number of gateways not registered with the local call manager.

Rejected Gateways

The number of gateways refused registration by the local call manager.

Registered Media Devices

The number of media devices registered with the local call manager.

Unregistered Media Devices

The number of media devices not registered with the local call manager.

Rejected Media Devices

The number of media devices refused registration by the local call manager.
Registered CTI Devices
The number of CTI devices registered with the local call manager.

Unregistered CTI Devices
The number of CTI devices not registered with the local call manager.

Rejected CTI Devices
The number of CTI devices refused registration by the local call manager.

Registered Voice Messaging Devices
The number of voice messaging devices registered with the local call manager.

Unregistered Voice Messaging Devices
The number of voice messaging devices not registered with the local call manager.

Rejected Voice Messaging Devices
The number of voice messaging devices refused registration by the local call manager.

Citrix Licensing
Net Service Name: lmgrd
CiscoSecure ACS (via SNMP)

This template assesses the overall performance of a CiscoSecure ACS server by monitoring its key processes.

Prerequisites

SNMP access to target server.

Credentials

None.

Monitored Components

For details on monitors, see [SAM Component Monitor Types](#).

**CS Admin - SNMP**

Process Name: CSAdmin.exe

**CS Auth - SNMP**

Process Name: CSAuth.exe

**CS Tacacs - SNMP**

Process Name: CSTacacs.exe

**CS Radius - SNMP**

Process Name: CSRadius.exe

**CS DBSync - SNMP**

Process Name: CSDBSync.exe

**CS Log - SNMP**

Process Name: CSLog.exe

**CS Mon - SNMP**

Process Name: CSMon.exe
CiscoWorks LAN Management Solution

This template assesses the status and overall performance of a CiscoWorks LAN Management Solution.

This template was tested on CiscoWorks LAN Management Solution 4.

Prerequisites

- WMI access to the target server.

Credentials

- Windows Administrator on the target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Service: CiscoWorks ANI database engine

This monitor returns the CPU and memory usage of CiscoWorks ANI database engine. This service performs Data Collection for purposes of build a layer 2 network topology. Also handles all Network Topology, Layer 2 Services and User Tracking client requests.

Service: CiscoWorks Daemon Manager

This monitor returns the CPU and memory usage of CiscoWorks Daemon Manager. This is administrative service for CiscoWorks processes.

Service: CiscoWorks RME NG database engine

This monitor returns the CPU and memory usage of CiscoWorks RME NG database engine. This service stores all Inventory and Configuration data pertaining to inventory and Syslog messages, but only references config files and software images stored outside of the database.

Service: CiscoWorks Tomcat Servlet Engine

This monitor returns the CPU and memory usage of CiscoWorks Tomcat Servlet Engine. This is the main application engine for CiscoWorks running Java servlets, and compiling and serving Java Server Pages.

Service: CiscoWorks Web Server

This monitor returns the CPU and memory usage of CiscoWorks Web Server (Apache).

Service: CWCS Cmf database engine

This monitor returns the CPU and memory usage of CiscoWorks Cmf database engine. This service stores job data, DCR data, and OGS data for Common Services, Fault Management, and Network Topology, Layer 2 Services and User Tracking. Reinitializing this database will remove all devices from all applications.
Service: CWCS rsh/rcp service
This monitor returns the CPU and memory usage of CiscoWorks rsh/rcp service. This service is responsible for using Remote Copy Protocol and Remote Shell.

Service: CWCS syslog service
This monitor returns the CPU and memory usage of CiscoWorks Syslog service.

Service: CWCS tftp service
This monitor returns the CPU and memory usage of CiscoWorks tftp service. This service is responsible for accepting tftp connections.

Service: DFM dfmEpm database engine
This monitor returns the CPU and memory usage of DFM dfmEpm database engine. This service serves database connections for storing and retrieving Fault Management alerts and events.

Service: DFM dfmFh database engine
This monitor returns the CPU and memory usage of DFM dfmFh database engine. This service stores archived Fault Management alerts and events for 31 days..

Service: DFM dfmInv database engine
This monitor returns the CPU and memory usage of DFM dfmInv database engine. This service stores CiscoWorks copy of Fault Management inventory.

Port: SSH
This component monitor tests the ability of a Cisco Secure Shell (SSH) to accept incoming sessions. By default, it monitors TCP port 22.

Port: Remote Copy Protocol
This component monitor tests the ability of a Remote Copy Protocol (RCP) to accept incoming sessions. RCP is a protocol that allows users to copy files to and from a file system residing on a remote host or server on the network. By default, it monitors TCP port 514.

Port: HTTP server in SSL mode
This component monitor tests the ability of a CiscoWorks HTTP server in SSL mode to accept incoming sessions. By default, it monitors TCP port 443.

Port: HTTP Protocol
This component monitor tests the ability of a CiscoWorks HTTP Protocol to accept incoming sessions. By default, it monitors TCP port 1741.

Port: OSAGENT
This component monitor tests the ability of an OSAGENT to accept incoming sessions. This is one of the base components needed for certain inter-process communication functions. By default, it monitors TCP port 42342.
Port: Log Server

This component monitor tests the ability of a Log Server to accept incoming sessions. By default, it monitors TCP port 8898.

Port: DynamID authentication (DFM Broker)

This component monitor tests the ability of a Device Fault Manager (DFM) broker service to accept incoming sessions. By default, it monitors TCP port 9002.

Port: Ajp13 connector used by Tomcat

This component monitor tests the ability of an Ajp13 connector used by Tomcat to accept incoming sessions. By default, it monitors TCP port 9009.

Port: ANIServer

This component monitor tests the ability of an ANIServer to accept incoming sessions. ANI service performs Data Collection for purposes of build a layer 2 network topology. Also handles all Network Topology, Layer 2 Services and User Tracking client requests. By default, it monitors TCP port 43242.

Port: Event Services Software (ESS) Listening

This component monitor tests the ability of an Event Services Software (ESS) to accept incoming sessions. Event Services Software (ESS) is an asynchronous messaging service that provides a messaging infrastructure based on a publish-and-subscribe paradigm. It enables distributed, loosely coupled interprocess communications. By default, it monitors TCP port 43450.

Port: CMF Database

This component monitor tests the ability of a CMF database to accept incoming sessions. CMF database stores job data, DCR data, and OGS data for Common Services, Fault Management, and Network Topology, Layer 2 Services and User Tracking. By default, it monitors TCP port 43441.

Port: RME Database

This component monitor tests the ability of a RME database to accept incoming sessions. RME database stores all Inventory and Configuration data pertaining to inventory and Syslog messages. By default, it monitors TCP port 43455.

Port: ANIDbEngine

This component monitor tests the ability of a ANI database engine to accept incoming sessions. By default, it monitors TCP port 43443.

Port: Fault History Database

This component monitor tests the ability of a Fault History Database to accept incoming sessions. This database stores the history of DFM events and alerts from the past 31 days. By default, it monitors TCP port 43445.

Port: Inventory Service Database

This component monitor tests the ability of an Inventory Service Database to accept incoming sessions. This database stores all inventory information. By default, it monitors TCP port 43446.
Port: HUM Database

This component monitor tests the ability of a HUM database to accept incoming sessions. This database stores information about network elements (such as CPU, memory, interfaces/ports, and links) and provides historical reporting. By default, it monitors TCP port 43800.

Port: IPM Database

This component monitor tests the ability of a CiscoWorks Internetwork Performance Monitor (IPM) database to accept incoming sessions. This database stores network response time and availability of network devices. By default, it monitors TCP port 43820.

Port: Event Promulgation Module Database

This component monitor tests the ability of an Event Promulgation Module Database to accept incoming sessions. This database stores Fault Management alerts and events. By default, it monitors TCP port 43447.

Port: SOAPMonitor

This component monitor tests the ability of a SOAP monitor to accept incoming sessions. Cisco SOAP-Performance Monitoring APIs service allows you to use performance monitoring counters for various applications through SOAP APIs. By default, it monitors TCP port 50001.

Events: CRM log events

This component returns the number of warning and error log messages of CRM log service.

- Source name: crmlog
- Log file: Application

This monitor should be zero at all times. If not, you should investigate this in the Windows Event Viewer.

Events: CRM tftp events

This component returns the number of warning and error log messages of CRM tftp service.

- Source name: crmtftp
- Log file: Application

This monitor should be zero at all times. If not, you should investigate this in the Windows Event Viewer.

Events: CRM rsh events

This component returns the number of warning and error log messages of CRM rsh service.

- Source name: crmrsh
- Log file: Application

This monitor should be zero at all times. If not, you should investigate this in the Windows Event Viewer.
Events: CRM Daemon Management events

This component returns the number of warning and error log messages of CRM Daemon Management service.

- Source name: CRMdmgtd
- Log file: Application

This value should be zero at all times. If not, you should investigate this in the Windows Event Viewer.
Citrix templates

The following templates are available:

- Citrix XenApp 5.0 Core WMI Counters
- Citrix XenApp 5.0 ICA WMI Session Counters
- Citrix XenApp 5.0 Presentation Server WMI Counters
- Citrix XenApp 5.0 Services
- Citrix XenApp 6.0 Core Counters
- Citrix XenApp 6.0 ICA Session
- Citrix XenApp 6.0 Presentation Server
- Citrix XenApp 6.0 Services
- Citrix XenApp and Xen Desktop 7.x (Advanced)
- Citrix XenApp and Xen Desktop 7.x (Events)
- Citrix XenApp and Xen Desktop 7.x (Performance Counters)
- Citrix XenApp and Xen Desktop 7.x (Services)
Citrix XenApp 5.0 Core WMI Counters

This template monitors critical events generated by Citrix XenApp 5.0 which may indicate possible service outages or configuration problems. Alerts are set to display descriptions of events as well as the host name.

Prerequisites

RPC access to the target server.

Credentials

Windows Administrator on target server.

Monitored Components

The following component monitors reads Windows Performance Counter data using Remote Procedure Calls (RPC) instead of Windows Management Instrumentation (WMI).

Citrix CPU Utilization Mgmt: CPU Entitlement

This component monitor returns the percentage of CPU availability for the Citrix CPU Utilization Management feature.

When this resource is fully utilized, the Citrix CPU Utilization Mgmt feature uses the share/reservation assignment and recent CPU consumption of each user to determine the CPU entitlement of that user. On multi-processor machines, the maximum value of the counter is 100% multiplied by the number of logical processors.

Citrix CPU Utilization Mgmt: CPU Reservation

This component monitor returns the percentage of the CPU that is reserved for users using the Citrix CPU Utilization Management feature, if needed.

A value in the range 1-99 indicates that a CPU reservation is applied. A value of zero indicates that no CPU reservation is being used. When the CPU resource is fully utilized, Citrix CPU Utilization Mgmt uses the reservation when calculating the CPU entitlement of a user.

Citrix CPU Utilization Mgmt: CPU Shares

This component monitor returns the percentage of the CPU assigned to a user.

A value of zero indicates that no CPU shares value is being used. When the CPU resource is fully utilized, Citrix CPU Utilization Mgmt uses the shares value when calculating the CPU entitlement of a user.
**Citrix CPU Utilization Mgmt: CPU Usage**

This component monitor returns the percentage of the CPU being used by a user, averaged over a short period of time. This may be used to identify users who consume significant amounts of CPU resources and to provide CPU usage accounting data. On multi-processor machines, the maximum value of the counter is 100% multiplied by the number of logical processors.

**Citrix CPU Utilization Mgmt: Long-term CPU Usage**

This component monitor returns the percentage of the CPU used by a user averaged over a long period of time. On multi-processor machines, the maximum value of the counter is 100% multiplied by the number of logical processors.

**Citrix IMA Networking: Bytes Received/sec**

This component monitor returns the data rate of incoming IMA network traffic.

**Citrix IMA Networking: Bytes Sent/sec**

This component monitor returns the data rate of outgoing IMA network traffic.

**Citrix IMA Networking: Network Connections**

This component monitor returns the number of active network IMA connections to IMA servers.

**Citrix Licensing: Average License Check-In Response Time (ms)**

This component monitor returns the average response time for a license check-in operation.

**Citrix Licensing: Average License Check-Out Response Time (ms)**

This component monitor returns the average response time for a license check-out operation.

**Citrix Licensing: Last Recorded License Check-In Response Time (ms)**

This component monitor returns the last response time for a license check-in operation.

**Citrix Licensing: Last Recorded License Check-Out Response Time (ms)**

This component monitor returns the last response time for a license check-out operation.

**Citrix Licensing: License Server Connection Failure**

This component monitor returns the time, in minutes, that the Citrix XenApp server has been without a connection to the license server. The time returned should be less than 30 minutes. Ideally, the returned time should be zero.

**Citrix Licensing: Maximum License Check-In Response Time (ms)**

This component monitor returns the maximum response time for a license check-in operation.

**Citrix Licensing: Maximum License Check-Out Response Time (ms)**

This component monitor returns the maximum response time for a license check-out operation.
Secure Ticket Authority: STA Bad Data Request Count
This component monitor returns the number of unsuccessful ticket validation and data requests over the lifetime of the STA.

Secure Ticket Authority: STA Bad Refresh Request Count
This component monitor returns the number of unsuccessful ticket refresh requests over the lifetime of the STA.

Secure Ticket Authority: STA Bad Ticket Request Count
This component monitor returns the number of unsuccessful ticket creation requests over the lifetime of the STA.

Secure Ticket Authority: STA Count of Active Tickets
This component monitor returns the number of tickets currently in the STA.

Secure Ticket Authority: STA Good Data Request Count
This component monitor returns the number of successful ticket validation and data requests over the lifetime of the STA.

Secure Ticket Authority: STA Good Refresh Request Count
This component monitor returns the number of successful ticket refresh requests over the lifetime of the STA.

Secure Ticket Authority: STA Good Ticket Request Count
This component monitor returns the number of successful ticket creation requests over the lifetime of the STA.

Secure Ticket Authority: STA Peak All Request Rate
This component monitor returns the highest activities per second recorded for all activities over the lifetime of the STA.

Secure Ticket Authority: STA Peak Data Request Rate
This component monitor returns the highest data requests per second recorded over the lifetime of the STA.

Secure Ticket Authority: STA Peak Ticket Refresh Rate
This component monitor returns the highest ticket refresh requests per second recorded over the lifetime of the STA.

Secure Ticket Authority: STA Peak Ticket Request Rate
This component monitor returns the highest ticket creation requests per second recorded over the lifetime of the STA.
Secure Ticket Authority: STA Ticket Timeout Count

This component monitor returns the number of ticket request timeouts recorded over the lifetime of the STA.
Citrix XenApp 5.0 ICA WMI Session Counters

This template monitors critical events generated by Citrix XenApp 5.0 which may indicate possible service outages or configuration problems. Alerts are set to display the descriptions of events as well as the host name.

Prerequisites

RPC access to the target server.

Credentials

Windows Administrator on target server.

The following component monitors reads Windows Performance Counter data using Remote Procedure Calls (RPC) instead of Windows Management Instrumentation (WMI).

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Input Audio Bandwidth

This component monitor returns the client-to-server bandwidth used for audio in ICA sessions in bits per second.

Input Clipboard Bandwidth

This component monitor returns the bandwidth used for clipboard operations between ICA sessions and local windows in bits per second.

Input COM 1 Bandwidth

This component monitor returns the bandwidth used for printing to the client port, COM 1, through an ICA session without print spooler support. The bandwidth reported is in bits per second.

Input COM 2 Bandwidth

This component monitor returns the bandwidth used for printing to the client port, COM 2, through an ICA session without print spooler support. The bandwidth reported is in bits per second.

Input COM Bandwidth

This component monitor returns the client-to-server bandwidth used in receiving data from the client COM port in bits per second.

Input Control Channel Bandwidth

This component monitor returns the client-to-server bandwidth used to execute the LongCommandLine parameters of published applications. The bandwidth reported is in bits per second.
Input Drive Bandwidth
This component monitor returns the client-to-server bandwidth used to perform file operations during ICA sessions in bits per second.

Input Font Data Bandwidth
This component monitor returns the bandwidth used to initiate the font changes in ICA sessions with SpeedScreen in bits per second.

Input Licensing Bandwidth
This component monitor returns the bandwidth used to negotiate session licensing in bits per second. This counter normally does not contain any data.

Input LPT1 Bandwidth
This component monitor returns the virtual channel bandwidth used for printing to the client port, LPT1, through an ICA session without print spooler support. The bandwidth reported is in bits per second.

Input LPT2 Bandwidth
This component monitor returns the virtual channel bandwidth used for printing to the client port, LPT2, through an ICA session without print spooler support. The bandwidth reported is in bits per second.

Input Management Bandwidth
This component monitor returns the bandwidth used to perform management tasks in bits per second.

Input PN Bandwidth
This component monitor returns the Program Neighborhood bandwidth used to obtain details about application sets. The bandwidth reported is in bits per second.

Input Printer Bandwidth
This component monitor returns the bandwidth used for printing to a client printer through a client with print spooler support. The bandwidth reported is in bits per second.

Input Seamless Bandwidth
This component monitor returns the bandwidth used for published applications not embedded in a session window. The bandwidth reported is in bits per second.

Input Session Bandwidth
This component monitor returns the client-to-server bandwidth used for a session. The bandwidth reported is in bits per second.

Input Session Compression
This component monitor returns the client-to-server compression ratio used for a session.
**Input Session Line Speed**

This component monitor returns the client-to-server line speed for a session. The bandwidth reported is in bits per second.

**Input SpeedScreen Data Channel Bandwidth**

This component monitor returns the client-to-server bandwidth used for data channel traffic. The bandwidth reported is in bits per second.

**Input Text Echo Bandwidth**

This component monitor returns the client-to-server bandwidth used for text echo. The bandwidth reported is in bits per second.

**Input ThinWire Bandwidth**

This component monitor returns the client-to-server bandwidth used for ThinWire traffic. The bandwidth reported is in bits per second.

**Input VideoFrame Bandwidth**

This component monitor returns the client-to-server bandwidth used for traffic over virtual channels. The bandwidth reported is in bits per second.

**Latency - Last Recorded**

This component monitor returns the last recorded latency value of the session.

**Latency - Session Average**

This component monitor returns the average latency over the session lifetime. This value should be as low as possible.

**Latency - Session Deviation**

This component monitor returns the difference between the minimum and the maximum session latency values. This value should be as low as possible.

**Output Audio Bandwidth**

This component monitor returns the server-to-client bandwidth used for audio in ICA sessions. The bandwidth reported is in bits per second.

**Output Clipboard Bandwidth**

This component monitor returns the bandwidth used for clipboard operations between ICA sessions and local windows. The bandwidth reported is in bits per second.

**Output COM 1 Bandwidth**

This component monitor returns the bandwidth used for printing to the client port, COM 1, through an ICA session without print spooler support. The bandwidth reported is in bits per second.
Output COM 2 Bandwidth

This component monitor returns the bandwidth used for printing to the client port, COM 2, through an ICA session without print spooler support. The bandwidth reported is in bits per second.

Output COM Bandwidth

This component monitor returns the server-to-client bandwidth used receiving data from the client COM port. The bandwidth reported is in bits per second.

Output Control Channel Bandwidth

This component monitor returns the server-to-client bandwidth used to execute the LongCommandLine parameters of published applications. The bandwidth reported is in bits per second.

Output Drive Bandwidth

This component monitor returns the server-to-client bandwidth used to perform file operations during ICA sessions. The bandwidth reported is in bits per second.

Output Font Data Bandwidth

This component monitor returns the bandwidth used to initiate the font changes in ICA sessions with SpeedScreen. The bandwidth reported is in bits per second.

Output Licensing Bandwidth

This component monitor returns the bandwidth used to negotiate session licensing. The bandwidth reported is in bits per second. Normally, this contains no data.

Output LPT1 Bandwidth

This component monitor returns the bandwidth used for printing to the client port, LPT1, through an ICA session without print spooler support. The bandwidth reported is in bits per second.

Output LPT2 Bandwidth

This component monitor returns the bandwidth used for printing to the client port, LPT2, through an ICA session without print spooler support. The bandwidth reported is in bits per second.

Output Management Bandwidth

This component monitor returns the bandwidth used to perform management tasks. The bandwidth reported is in bits per second.

Output PN Bandwidth

This component monitor returns the Program Neighborhood bandwidth used to obtain details about application sets. The bandwidth reported is in bits per second.

Output Printer Bandwidth

This component monitor returns the bandwidth used for printing to a client printer through a client with print spooler support. The bandwidth reported is in bits per second.
Output Seamless Bandwidth
This component monitor returns the bandwidth used for published applications not embedded in a session window. The bandwidth reported is in bits per second.

Output Session Bandwidth
This component monitor returns the server-to-client bandwidth used for a session. The bandwidth reported is in bits per second.

Output Session Compression
This component monitor returns the server-to-client compression ratio used for a session.

Output Session Line speed
This component monitor returns the server-to-client line speed used for a session. The bandwidth reported is in bits per second.

Output SpeedScreen Data Channel Bandwidth
This component monitor returns the server-to-client bandwidth used for data channel traffic. The bandwidth reported is in bits per second.

Output Text Echo Bandwidth
This component monitor returns the bandwidth used for text echo. The bandwidth reported is in bits per second.

Output ThinWire Bandwidth
This component monitor returns the server-to-client bandwidth used for ThinWire traffic. The bandwidth reported is in bits per second.

Output VideoFrame Bandwidth
This component monitor returns the server-to-client bandwidth used for traffic on virtual channels. The bandwidth reported is in bits per second.
Citrix XenApp 5.0 Presentation Server WMI Counters

This template monitors critical events generated by Citrix XenApp 5.0 which may indicate possible service outages or configuration problems. Alerts are set to display the descriptions of events and the host name.

Prerequisites

RPC access to the target server.

Credentials

Windows Administrator on target server.

The following component monitors reads Windows Performance Counter data using Remote Procedure Calls (RPC) instead of Windows Management Instrumentation (WMI).

Monitored Components

For details on monitors, see SAM Component Monitor Types.

**Application Enumeration/sec**
This component monitor returns the number of non-XML-based enumerations (requests for application lists) per second.

**Application Resolution Time (ms)**
This component monitor measures the time required to resolve the Least-Loaded Server during an application in milliseconds.

A baseline would be needed to establish increases during peak logon times before an accurate threshold can be defined.

**Application Resolutions Failed/sec**
This component monitor returns the number of application resolutions failed per second. This value should be zero at all times.

**Application Resolutions/sec**
This component monitor returns the number of resolutions (application launch requests) per second.

**DataStore Connection Failure**
This component monitor returns the number of minutes that the XenApp server has been disconnected from the data store. This value should be zero at all times.

**DataStore bytes read**
This component monitor returns the number of bytes read from the data store.
DataStore bytes read/sec
This component monitor returns the number of bytes read from the data store per second.

DataStore bytes written/sec
This component monitor returns the number of bytes written to the data store per second.

DataStore reads
This component monitor returns the number of times data was read from the data store.

DataStore reads/sec
This component monitor returns the number of times data was read from the data store per second.

DataStore writes/sec
This component monitor returns the number of times data was written to the data store per second.

DynamicStore bytes read/sec
This component monitor returns the number of dynamic data store bytes read per second.

DynamicStore bytes written/sec
This component monitor returns the number of dynamic data store bytes written per second.

DynamicStore Gateway Update Count
This component monitor returns the number of dynamic store update packets sent to remote data collectors.

DynamicStore Gateway Update Bytes Sent
This component monitor returns the number of bytes of data sent across gateways to remote data collectors.

DynamicStore Query Count
This component monitor returns the number of performed dynamic store queries.

DynamicStore Query Request Bytes Received
This component monitor returns the number of bytes of data received in dynamic store query request packets.

DynamicStore Query Response Bytes Sent
This component monitor returns the number of bytes of data sent in response to dynamic store queries.

DynamicStore reads/sec
This component monitor returns the number of times data was read from the dynamic store per second.
DynamicStore Update Bytes Received
This component monitor returns the number of bytes of data received in dynamic store update packets.

DynamicStore Update Packets Received
This component monitor returns the number of update packets received by the dynamic store.

DynamicStore Update Response Bytes Sent
This component monitor returns the number of bytes of data sent in response to dynamic store update packets.

DynamicStore writes/sec
This component monitor returns the number of times data was written to the dynamic store per second.

Filtered Application Enumerations/sec
This component monitor returns the number of XML-based enumerations (requests for application lists) per second.

LocalHostCache bytes read/sec
This component monitor returns the number of bytes of IMA local host cache data read per second.

LocalHostCache bytes written/sec
This component monitor returns the number of bytes of IMA local host cache data written per second.

LocalHostCache reads/sec
This component monitor returns the number of times data was read from the IMA local host cache per second.

LocalHostCache writes/sec
This component monitor returns the number of times data was written to the IMA local host cache per second.

Maximum number of XML threads
This component monitor returns the maximum number of threads allocated to service Web-based sessions since the server last restarted.

Number of busy XML threads
This component monitor returns the number of XML requests that are currently being processed.
This value should be less than 12. The maximum number of requests that the XML service can process at any one time is 16.

Number of XML threads
This component monitor returns the number of threads allocated to service web-based sessions.
Resolution WorkItem Queue Executing Count

This component monitor returns the number of work items (related to application launches) that are waiting to be processed by IMA.

Resolution WorkItem Queue Ready Count

This component monitor returns the number of resolution work items that are ready to be executed. This value should be zero at all times.

WorkItem Queue Executing Count

This component monitor returns the number of work items that are currently being executed.

WorkItem Queue Pending Count

This component monitor returns the number of work items that are not yet ready to be executed.

WorkItem Queue Ready Count

This component monitor returns the number of work items that are ready and waiting to be processed by IMA. This value should be zero at all times.

Zone Elections

This component monitor returns the number of zone elections that occurred. This value starts at zero each time the IMA Service starts and is incremented each time a zone election takes place.

Zone Elections Won

This component monitor returns the number of times the server won a zone election.
Citrix XenApp 5.0 Services

This template monitors critical events generated by Citrix XenApp 5.0 which may indicate possible service outages or configuration problems. Alerts are set to display the descriptions of events and the host name.

Prerequisites

- RPC access to the target server.

Credentials

- Windows Administrator on target server.

The following component monitors use WMI or RPC communication to test if a specified Windows service is running and reports the CPU, virtual memory, and physical memory used by the service.

Monitored Components

For details on monitors, see [SAM Component Monitor Types](#).

Citrix ActiveSync Service

This component monitor supports ActiveSync in ICA sessions.

Citrix ADF Installer Service

This component monitor is used by Installation Manager in the Enterprise and Platinum versions to install packages onto Presentation Servers.

Citrix Client Network

This component monitor handles the mapping of client drives and peripherals within ICA sessions.

Citrix CPU Utilization Mgmt/CPU Rebalancer (requires multiple CPUs)

This component monitor enhances resource management across multiple CPUs.

Citrix CPU Utilization Mgmt/Resource Mgmt

This component monitor is used in the Enterprise and Platinum versions to manage resource consumption.

Citrix CPU Utilization Mgmt/User-Session Sync

This component monitor is used in the Enterprise version to synchronize user IDs of processes with their respective owner.

Citrix Diagnostic Facility COM Server

This component monitor manages Diagnostic Facility tracing when used to diagnose problems with the Citrix Server.
**Citrix Encryption Service**
This component monitor handles encryption between the client device and the Citrix Server.

**Citrix Health Monitoring and Recovery**
This component monitor provides health monitoring and recovery services if event problems occur.

**Citrix Independent Management Architecture**
This component monitor provides management services within the Citrix farm.

**Citrix License Management Console (License server only)**
This component monitor provides the web-based interface for licensing administration.

**Citrix Licensing WMI (License server only)**
This component monitor provides information and notification regarding licensing events on the license server.

**Citrix MFCOM Service (MetaFrame COM Server)**
This component monitor provides COM services which allow remote connections of the management consoles.

**Citrix Print Manager Service**
This component monitor handles the creation of printers and driver usage within Citrix sessions.

**Citrix Resource Manager Mail**
This component monitor is used in the Enterprise and Platinum versions to send email alerts when thresholds in the server farm have been met or exceeded.

**Citrix Services Manager**
This component monitor allows the components of the presentation server to interface with the operating system.

**Citrix SMA Service**
This component monitor watches the event log and Citrix WMI to raise alerts in the Access Suite Console or Access Management Console.

**Citrix Streaming Service**
This component monitor is used in the Enterprise and Platinum versions to manage the Citrix Streaming Client when streaming applications.

**Citrix Virtual Memory Optimization**
This component monitor is used in the Enterprise and Platinum versions to release .dlls to free up server memory.
Citrix WMI Service
This component monitor is used by the Citrix WMI classes for information and management purposes.

Citrix XTE Server
This component monitor handles SSL Relay and Session Reliability functionality.

Citrix Licensing (License server only)
This component monitor handles allocation of licenses on the license server.

Citrix End User Experiencing Monitoring
This component monitor handles the Net Service Name: Citrix EUEM.
Citrix XenApp 6.0 Core Counters

This template monitors critical events generated by Citrix XenApp 6.0 which may indicate possible service outages or configuration problems. Alerts are set to display descriptions of events as well as the host name.

Prerequisites

WMI access to the target server.

Credentials

Windows Administrator on target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

You need to set thresholds for counters according to your environment. It is recommended to monitor counters for some period of time to understand potential value ranges and then set the thresholds accordingly. For more information, see "Using the Orion APM MIN/MAX Average Statistic Data historical charts for creating threshold settings based on 95th percentile line."

Citrix IMA Networking: Bytes Received/sec

This component monitor returns the data rate of incoming IMA network traffic.

Citrix IMA Networking: Bytes Sent/sec

This component monitor returns the data rate of outgoing IMA network traffic.

Citrix IMA Networking: Network Connections

This component monitor returns the number of active network IMA connections to IMA servers.

Citrix Licensing: Average License Check-In Response Time (ms)

This component monitor returns the average response time for a license check-in operation.

Citrix Licensing: Average License Check-Out Response Time (ms)

This component monitor returns the average response time for a license check-out operation.

Citrix Licensing: Last Recorded License Check-In Response Time (ms)

This component monitor returns the last response time for a license check-in operation.

Citrix Licensing: Last Recorded License Check-Out Response Time (ms)

This component monitor returns the last response time for a license check-out operation.
Citrix Licensing: License Server Connection Failure

This component monitor returns the time, in minutes, that the Citrix XenApp server has been without a connection to the license server. The time returned should be less than 30 minutes. Ideally, the returned time should be zero.

Citrix Licensing: Maximum License Check-In Response Time (ms)

This component monitor returns the maximum response time for a license check-in operation.

Citrix Licensing: Maximum License Check-Out Response Time (ms)

This component monitor returns the maximum response time for a license check-out operation.

Secure Ticket Authority: STA Bad Data Request Count

This component monitor returns the number of unsuccessful ticket validation and data requests over the lifetime of the STA.

Secure Ticket Authority: STA Bad Refresh Request Count

This component monitor returns the number of unsuccessful ticket refresh requests over the lifetime of the STA.

Secure Ticket Authority: STA Bad Ticket Request Count

This component monitor returns the number of unsuccessful ticket creation requests over the lifetime of the STA.

Secure Ticket Authority: STA Count of Active Tickets

This component monitor returns the number of tickets currently in the STA.

Secure Ticket Authority: STA Good Data Request Count

This component monitor returns the number of successful ticket validation and data requests over the lifetime of the STA.

Secure Ticket Authority: STA Good Refresh Request Count

This component monitor returns the number of successful ticket refresh requests over the lifetime of the STA.

Secure Ticket Authority: STA Good Ticket Request Count

This component monitor returns the number of successful ticket creation requests over the lifetime of the STA.

Secure Ticket Authority: STA Peak All Request Rate

This component monitor returns the highest activities per second recorded for all activities over the lifetime of the STA.

Secure Ticket Authority: STA Peak Data Request Rate

This component monitor returns the highest data requests per second recorded over the lifetime of the STA.
Secure Ticket Authority: STA Peak Ticket Refresh Rate

This component monitor returns the highest ticket refresh requests per second recorded over the lifetime of the STA.

Secure Ticket Authority: STA Peak Ticket Request Rate

This component monitor returns the highest ticket creation requests per second recorded over the lifetime of the STA.

Secure Ticket Authority: STA Ticket Timeout Count

This component monitor returns the number of ticket request timeouts recorded over the lifetime of the STA.
Citrix XenApp 6.0 ICA Session

This template monitors critical events generated by Citrix XenApp 6.0 which may indicate possible service outages or configuration problems. Alerts are set to display the descriptions of events as well as the host name.

Prerequisites

WMI access to target server.

Credentials

Windows Administrator on target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

You need to set thresholds for counters according to your environment. It is recommended to monitor counters for some period of time to understand potential value ranges and then set the thresholds accordingly.

Input Audio Bandwidth

This component monitor returns the client-to-server bandwidth used for audio in ICA sessions in bits per second.

Input COM 1 Bandwidth

This component monitor returns the bandwidth used for printing to the client port, COM 1, through an ICA session without print spooler support. The bandwidth reported is in bits per second.

Input COM 2 Bandwidth

This component monitor returns the bandwidth used for printing to the client port, COM 2, through an ICA session without print spooler support. The bandwidth reported is in bits per second.

Input COM Bandwidth

This component monitor returns the client-to-server bandwidth used in receiving data from the client COM port in bits per second.

Input Control Channel Bandwidth

This component monitor returns the client-to-server bandwidth used to execute the LongCommandLine parameters of published applications. The bandwidth reported is in bits per second.
Input Drive Bandwidth

This component monitor returns the client-to-server bandwidth used to perform file operations during ICA sessions in bits per second.

Input Font Data Bandwidth

This component monitor returns the bandwidth used to initiate the font changes in ICA sessions with SpeedScreen in bits per second.

Input Licensing Bandwidth

This component monitor returns the bandwidth used to negotiate session licensing in bits per second. This counter normally does not contain any data.

Input LPT1 Bandwidth

This component monitor returns the virtual channel bandwidth used for printing to the client port, LPT1, through an ICA session without print spooler support. The bandwidth reported is in bits per second.

Input LPT2 Bandwidth

This component monitor returns the virtual channel bandwidth used for printing to the client port, LPT2, through an ICA session without print spooler support. The bandwidth reported is in bits per second.

Input PN Bandwidth

This component monitor returns the Program Neighborhood bandwidth used to obtain details about application sets. The bandwidth reported is in bits per second.

Input Printer Bandwidth

This component monitor returns the bandwidth used for printing to a client printer through a client with print spooler support. The bandwidth reported is in bits per second.

Input Seamless Bandwidth

This component monitor returns the bandwidth used for published applications not embedded in a session window. The bandwidth reported is in bits per second.

Input Session Bandwidth

This component monitor returns the client-to-server bandwidth used for a session. The bandwidth reported is in bits per second.

Input Session Compression

This component monitor returns the client-to-server compression ratio used for a session.

Input Session Line Speed

This component monitor returns the client-to-server line speed for a session. The bandwidth reported is in bits per second.
Input SpeedScreen Data Channel Bandwidth

This component monitor returns the client-to-server bandwidth used for data channel traffic. The bandwidth reported is in bits per second.

Input Text Echo Bandwidth

This component monitor returns the client-to-server bandwidth used for text echo. The bandwidth reported is in bits per second.

Input ThinWire Bandwidth

This component monitor returns the client-to-server bandwidth used for ThinWire traffic. The bandwidth reported is in bits per second.

Latency - Last Recorded

This component monitor returns the last recorded latency value of the session.

Latency - Session Average

This component monitor returns the average latency over the session lifetime. This value should be as low as possible.

Latency - Session Deviation

This component monitor returns the difference between the minimum and the maximum session latency values. This value should be as low as possible.

Output Audio Bandwidth

This component monitor returns the server-to-client bandwidth used for audio in ICA sessions. The bandwidth reported is in bits per second.

Output Clipboard Bandwidth

This component monitor returns the bandwidth used for clipboard operations between ICA sessions and local windows. The bandwidth reported is in bits per second.

Output COM 1 Bandwidth

This component monitor returns the bandwidth used for printing to the client port, COM 1, through an ICA session without print spooler support. The bandwidth reported is in bits per second.

Output COM 2 Bandwidth

This component monitor returns the bandwidth used for printing to the client port, COM 2, through an ICA session without print spooler support. The bandwidth reported is in bits per second.

Output COM Bandwidth

This component monitor returns the server-to-client bandwidth used receiving data from the client COM port. The bandwidth reported is in bits per second.
Output Control Channel Bandwidth
This component monitor returns the server-to-client bandwidth used to execute the 
LongCommandLine parameters of published applications. The bandwidth reported is in bits per 
second.

Output Drive Bandwidth
This component monitor returns the server-to-client bandwidth used to perform file operations 
during ICA sessions. The bandwidth reported is in bits per second.

Output Font Data Bandwidth
This component monitor returns the bandwidth used to initiate the font changes in ICA sessions 
with SpeedScreen. The bandwidth reported is in bits per second.

Output Licensing Bandwidth
This component monitor returns the bandwidth used to negotiate session licensing. The bandwidth 
reported is in bits per second. Normally, this contains no data.

Output LPT1 Bandwidth
This component monitor returns the bandwidth used for printing to the client port, LPT1, through an 
ICA session without print spooler support. The bandwidth reported is in bits per second.

Output LPT2 Bandwidth
This component monitor returns the bandwidth used for printing to the client port, LPT2, through an 
ICA session without print spooler support. The bandwidth reported is in bits per second.

Output PN Bandwidth
This component monitor returns the Program Neighborhood bandwidth used to obtain details about 
application sets. The bandwidth reported is in bits per second.

Output Printer Bandwidth
This component monitor returns the bandwidth used for printing to a client printer through a client 
with print spooler support. The bandwidth reported is in bits per second.

Output Seamless Bandwidth
This component monitor returns the bandwidth used for published applications not embedded in a 
session window. The bandwidth reported is in bits per second.

Output Session Bandwidth
This component monitor returns the server-to-client bandwidth used for a session. The bandwidth 
reported is in bits per second.

Output Session Compression
This component monitor returns the server-to-client compression ratio used for a session.
Output Session Line speed

This component monitor returns the server-to-client line speed used for a session. The bandwidth reported is in bits per second.

Output SpeedScreen Data Channel Bandwidth

This component monitor returns the server-to-client bandwidth used for data channel traffic. The bandwidth reported is in bits per second.

Output Text Echo Bandwidth

This component monitor returns the bandwidth used for text echo. The bandwidth reported is in bits per second.

Output ThinWire Bandwidth

This component monitor returns the server-to-client bandwidth used for ThinWire traffic. The bandwidth reported is in bits per second.

Output VideoFrame Bandwidth

This component monitor returns the server-to-client bandwidth used for traffic on virtual channels. The bandwidth reported is in bits per second.
Citrix XenApp 6.0 Presentation Server

This template monitors critical events generated by Citrix XenApp 6.0 which may indicate possible service outages or configuration problems. Alerts are set to display the descriptions of events and the host name.

Prerequisites

RPC access to the target server.

Credentials

Windows Administrator on target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

You need to set thresholds for counters according to your environment. It is recommended to monitor counters for some period of time to understand the potential value ranges and then set the thresholds accordingly.

Application Enumeration/sec

This component monitor returns the number of non-XML-based enumerations (requests for application lists) per second.

Application Resolution Time (ms)

This component monitor measures the time required to resolve the Least-Loaded Server during an application in milliseconds.

A baseline would be needed to establish increases during peak logon times before an accurate threshold can be defined.

Application Resolutions Failed/sec

This component monitor returns the number of application resolutions failed per second. This value should be zero at all times.

Application Resolutions/sec

This component monitor returns the number of resolutions (application launch requests) per second.

DataStore Connection Failure

This component monitor returns the number of minutes that have elapsed since the XenApp server has been disconnected from the data store. This value should be zero at all times.

DataStore bytes read

This component monitor returns the number of bytes read from the data store.
DataStore bytes read/sec
This component monitor returns the number of bytes read from the data store per second.

DataStore bytes written/sec
This component monitor returns the number of bytes written to the data store per second.

DataStore reads
This component monitor returns the number of times data was read from the data store.

DataStore reads/sec
This component monitor returns the number of times data was read from the data store per second.

DataStore writes/sec
This component monitor returns the number of times data was written to the data store per second.

DynamicStore bytes read/sec
This component monitor returns the number of dynamic data store bytes read per second.

DynamicStore bytes written/sec
This component monitor returns the number of dynamic data store bytes written per second.

DynamicStore Gateway Update Count
This component monitor returns the number of dynamic store update packets sent to remote data collectors.

DynamicStore Gateway Update Bytes Sent
This component monitor returns the number of bytes of data sent across gateways to remote data collectors.

DynamicStore Query Count
This component monitor returns the number of dynamic store queries performed.

DynamicStore Query Request Bytes Received
This component monitor returns the number of bytes of data received in dynamic store query request packets.

DynamicStore Query Response Bytes Sent
This component monitor returns the number of bytes of data sent in response to dynamic store queries.

DynamicStore reads/sec
This component monitor returns the number of times data was read from the dynamic store per second.

DynamicStore Update Bytes Received
This component monitor returns the number of bytes of data received in dynamic store update packets.

**DynamicStore Update Packets Received**

This component monitor returns the number of update packets received by the dynamic store.

**DynamicStore Update Response Bytes Sent**

This component monitor returns the number of bytes of data sent in response to dynamic store update packets.

**DynamicStore writes/sec**

This component monitor returns the number of times data was written to the dynamic store per second.

**Filtered Application Enumerations/sec**

This component monitor returns the number of XML-based enumerations (requests for application lists) per second.

**LocalHostCache bytes read/sec**

This component monitor returns the number of bytes of IMA local host cache data read per second.

**LocalHostCache bytes written/sec**

This component monitor returns the number of bytes of IMA local host cache data written per second.

**LocalHostCache reads/sec**

This component monitor returns the number of times data was read from the IMA local host cache per second.

**LocalHostCache writes/sec**

This component monitor returns the number of times data was written to the IMA local host cache per second.

**Maximum number of XML threads**

This component monitor returns the maximum number of threads allocated to service Web-based sessions since the server last restarted.

**Number of busy XML threads**

This component monitor returns the number of XML requests that are currently being processed.

This value should be less than 12. The maximum number of requests that the XML service can process at any one time is 16.

**Number of XML threads**

This component monitor returns the number of threads allocated to service web-based sessions.

**Resolution WorkItem Queue Executing Count**
This component monitor returns the number of work items (related to application launches) that are waiting to be processed by IMA.

Resolution WorkItem Queue Ready Count
This component monitor returns the number of resolution work items that are ready to be executed. This value should be zero at all times.

WorkItem Queue Executing Count
This component monitor returns the number of work items that are currently being executed.

WorkItem Queue Pending Count
This component monitor returns the number of work items that are not yet ready to be executed.

WorkItem Queue Ready Count
This component monitor returns the number of work items that are ready and waiting to be processed by IMA. This value should be zero at all times.

Zone Elections
This component monitor returns the number of zone elections that occurred. This value starts at zero each time the IMA service starts and is incremented each time a zone election takes place.

Zone Elections Won
This component monitor returns the number of times the server won a zone election.

Number of Active Sessions
This component monitor returns the number of currently active connections to the Citrix server.

Number ofDisconnected Sessions
This component monitor returns the number of currently disconnected connections to the Citrix server.
Citrix XenApp 6.0 Services

This template monitors critical events generated by Citrix XenApp 6.0 which may indicate possible service outages or configuration problems. Alerts are set to display the descriptions of events and the host name.

Prerequisites

WMI access to the target server.

Credentials

Windows Administrator on target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Citrix Diagnostic Facility COM Server

This component monitors the service which manages and controls Citrix diagnostic trace sessions on the system.

Citrix Encryption Service

This component monitors the service which enables secure communication with RC5 128-bit encryption between Citrix Delivery Clients and this Citrix XenApp server.

Citrix Health Monitoring and Recovery

This component monitors the service which provides Health Monitoring and Recovery services for Citrix XenApp Server.

Citrix Independent Management Architecture

This component monitors the service which provides management services for Citrix products.

Citrix Licensing WMI (License server only)

This component monitors the service which enables Citrix Licensing using WMI.

Citrix MFCOM Service (MetaFrame COM Server)

This component monitors the service which provides COM access to a Citrix farm.

Citrix Print Manager Service

This component monitors the service which supports the Citrix Advanced Universal Printing Architecture.

Citrix Services Manager

This component monitors the service which provides a Citrix Presentation Server with an interface to the operating system.
Citrix Streaming Service
This component monitors the service which manages the Citrix offline plug-in.

Citrix Virtual Memory Optimization
This component monitors the service which dynamically optimizes applications running on this machine.

Citrix WMI Service
This component monitors the service which provides the Citrix WMI classes.

Citrix XTE Server
This component monitors the service which requests for session reliability and SSL from Citrix components.

Citrix Licensing (License server only)
This component monitors the service which provides licensing services for Citrix products.

Citrix End User Experiencing Monitoring
This component monitors the service which collects and collates end user experience measurements.

Citrix Audio Redirection Service
This component monitors the service which provides audio redirection between the endpoint device and the virtual desktop.

Citrix Group Policy Engine
This component monitors the service which is responsible for applying settings configured by Citrix administrators for the computer and users through the Group Policy component.

Citrix HDX MediaStream for Flash Service
This component monitors the service which provides the HDX MediaStream for the Flash feature to published applications and virtual desktops. HDX MediaStream for Flash allows the Adobe Flash Player to run on the client user device instead of within the server session.

Citrix Licensing Support Service
This component monitors the service which allow controls reading the license files and updating strings with license trailers (data dictionary functionality).

Citrix Smart Card Service
This component monitors the service which provides Smart Card redirection between the endpoint device and the virtual desktop.

Citrix Streaming Helper Service
This component monitors the service which manages the Citrix offline plug-in.
Citrix XenApp and Xen Desktop 7.x (Advanced)

This template assesses the status and overall health of the Citrix XenApp and XenDesktop 7.x installed on Windows by using PowerShell scripts.

For PowerShell requirements, see Use PowerShell in SAM.

Prerequisites

WMI access to the target server.

Credentials

Windows Administrator on target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Controllers

This monitor returns the status of controllers running broker services in the site.

Desktop Groups

This monitor returns broker desktop status.

Machines

This monitor returns machine status.

Sessions

This monitor returns session status.

Broker Service Status)

This monitor determines the current state of the Broker Service on the controller.

Specific Desktop Catalog State)

This monitor returns specific desktop catalog state.

Specific Machine State

This monitor returns specific machine status.

Citrix XenApp and Xen Desktop 7.x (Events)

This template assesses the status and overall health of the Citrix XenApp and XenDesktop 7.x installed on Windows by looking for XenApp and XenDesktop events.

All monitors in this template look for events in the Application log file.
Prerequisites

WMI access to the target server.

Credentials

Windows Administrator on target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

AG Service

This monitor returns Warning and Error events.

Authentication Events

This monitor returns Warning and Error events.

Broker Service

This monitor returns Warning and Error events.

Configuration Events

This monitor returns Warning and Error events.

Default Log

This monitor returns Warning and Error events.

Delegated Events

This monitor returns Warning and Error events.

Delivery Service Events

This monitor returns Warning and Error events.

Desktop Appliance

This monitor returns Warning and Error events.

Director Service

This monitor returns Warning and Error events.

Domain Service

This monitor returns Warning and Error events.

Environment Test Service

This monitor returns Warning and Error events.

Host Service

This monitor returns Warning and Error events.
Legacy Support
This monitor returns Warning and Error events.

Machine Creation Service
This monitor returns Warning and Error events.

Monitor Service
This monitor returns Warning and Error events.

Peer Resolution Service
This monitor returns Warning and Error events.

Receiver for Web
This monitor returns Warning and Error events.

Roaming Service
This monitor returns Warning and Error events.

Store Service
This monitor returns Warning and Error events.

Storefront Service
This monitor returns Warning and Error events.

Licensing Service
This monitor returns Warning and Error events.

**Citrix XenApp and Xen Desktop 7.x (Performance Counters)**

This template assesses the status and overall health of the Citrix XenApp and XenDesktop 7.x installed on Windows by retrieving data from performance counters.

**Prerequisites**
- WMI access to the target server.

**Credentials**
- Windows Administrator on target server.

**Monitored Components**

For details on monitors, see [SAM Component Monitor Types](#).

You need to set thresholds for counters according to your environment. It is recommended to monitor counters for some period of time to understand the potential value ranges and then set the thresholds accordingly.
**Broker: Brokered Sessions**
Brokered Sessions is the number of virtual desktop sessions brokered by the Citrix Broker Service.

**Broker: Database Avg. Transaction Time**
Database Avg. Transaction Time is the time on average, in seconds, taken to execute a database transaction from Citrix Broker Service. A baseline needs to be established in the environment to accurately establish threshold values. In case the reported values exceed the baseline response time constantly, a potential performance issue needs to be investigated at the SQL server level.

**Broker: Database Connected**
Database Connected indicates whether the Citrix Broker Service is in contact with its database (1 is connected; 0 is not connected.)

**Broker: Database Transaction Errors/sec**
Database Transactions/sec is the rate at which database transactions are failing, when executed from Citrix Broker Service. Should be 0 all the time. High values may indicate connectivity issues of the XenDesktop Broker service with the XenDesktop database. In case issues are reported, SQL server and network availability needs to be verified.

**Broker: Database Transactions/sec**
Database Transactions/sec is the rate at which database transactions are being executed from the Citrix Broker Service.

**Broker: Expired Launches/sec**
Expired Launches/sec is the rate at which virtual desktops timeout waiting on clients to connect to them, as detected by the Citrix Broker Service.

**Broker: Expired Registrations/sec**
Expired Registrations/sec is the rate at which virtual desktop registrations with the Citrix Broker Service expire through inactive communication.

**Broker: Hard Registrations/sec**
Hard Registrations/sec is the rate at which virtual desktop agents hard-register with the Citrix Broker Service.

**Broker: Registration Avg. Request Time**
Registration Avg. Request Time is the time on average, in seconds, taken to process a virtual desktop registration request in the Citrix Broker Service.

**Broker: Registration Rejects/sec**
Registration Rejects/sec is the rate at which Citrix Broker Service rejects registration requests from virtual desktops.

**Broker: Registration Requests/sec**
Registration Requests/sec is the rate at which Citrix Broker Service receives registration requests from virtual desktops.
Broker: Soft Registrations/sec
Soft Registrations/sec is the rate at which virtual desktop agents soft-register with the Citrix Broker Service.

AD Identity: Database Connected
Database Connected indicates whether this service is in contact with its database (1 is connected; 0 is not connected.)

AD Identity: Database Transaction Errors/sec
Database Transactions Errors/sec is the rate at which database transactions are failing when executed from this service.

Configuration Logging: Database Connected
Database Connected indicates whether this service is in contact with its database (1 is connected; 0 is not connected.)

Configuration Logging: Database Transaction Errors/sec
Database Transactions Errors/sec is the rate at which database transactions are failing when executed from this service.

Configuration Service: Database Connected
Database Connected indicates whether this service is in contact with its database (1 is connected; 0 is not connected.)

Configuration Service: Database Transaction Errors/sec
Database Transactions Errors/sec is the rate at which database transactions are failing when executed from this service.

Delegated Admin: Database Connected
Database Connected indicates whether this service is in contact with its database (1 is connected; 0 is not connected.)

Delegated Admin: Database Transaction Errors/sec
Database Transactions Errors/sec is the rate at which database transactions are failing when executed from this service.

Environment Test: Database Connected
Database Connected indicates whether this service is in contact with its database (1 is connected; 0 is not connected.)

Environment Test: Database Transaction Errors/sec
Database Transactions Errors/sec is the rate at which database transactions are failing when executed from this service.

Host Service: Database Connected
Database Connected indicates whether this service is in contact with its database (1 is connected; 0 is not connected.)
Host Service: Database Transaction Errors/sec

Database Transactions Errors/sec is the rate at which database transactions are failing when executed from this service.

Machine Creation Service: Database Connected

Database Connected indicates whether this service is in contact with its database (1 is connected; 0 is not connected.)

Machine Creation Service: Database Transaction Errors/sec

Database Transactions Errors/sec is the rate at which database transactions are failing when executed from this service.

Monitor: Database Connected

Database Connected indicates whether this service is in contact with its database (1 is connected; 0 is not connected.)

Monitor: Database Transaction Errors/sec

Database Transactions Errors/sec is the rate at which database transactions are failing when executed from this service.

Storefront: Database Connected

Database Connected indicates whether this service is in contact with its database (1 is connected; 0 is not connected.)

Storefront: Database Transaction Errors/sec

Database Transactions Errors/sec is the rate at which database transactions are failing when executed from this service.

Citrix XenApp and Xen Desktop 7.x (Services)

This template assesses the status and overall health of the Citrix XenApp and XenDesktop 7.x services and TCP ports installed on Windows.

Prerequisites

WMI access to the target server.

Credentials

Windows Administrator on target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.
Citrix AD Identity Service

This monitor returns CPU and memory usage of the Citrix AD Identity Service. It manages Active Directory Computer Accounts.

Citrix Broker Service

This monitor returns CPU and memory usage of the Citrix Broker Service. It provides configuration and allows brokering of connections to desktops and applications.

Citrix Configuration Logging Service

This monitor returns CPU and memory usage of the Citrix Configuration Logging Service. It logs Administrator activity and configuration changes in a XenDesktop deployment.

Citrix Configuration Replication

This monitor returns CPU and memory usage of the Citrix Configuration Replication. It provides access to Delivery Services Replication configuration information.

Citrix Configuration Service

This monitor returns CPU and memory usage of the Citrix Configuration Service. It stores Service configuration information.

Citrix Credential Wallet

This monitor returns CPU and memory usage of the Citrix Credential Wallet Service. It provides a secure store for Credentials.

Citrix Default Domain Services

This monitor returns CPU and memory usage of the Citrix Default Domain Services. It provides authentication, change password and other domain services.

Citrix Delegated Administration Service

This monitor returns CPU and memory usage of the Citrix Delegated Administration Service. It manages configuration of delegated administration permissions.

Citrix Diagnostic Facility COM Server

This monitor returns CPU and memory usage of the Citrix Diagnostic Facility COM Server. It manages and controls Citrix diagnostic trace sessions on the system.

Citrix Environment Test Service

This monitor returns CPU and memory usage of the Citrix Environment Test Service. It manages tests for evaluating the state of a XenDesktop Site

Citrix Host Service

This monitor returns CPU and memory usage of the Citrix Host Service. It manages Hosts, and Hypervisor Connections
Citrix Licensing

This monitor returns CPU and memory usage of Citrix Licensing. It provides licensing services for Citrix products.

Citrix Licensing Support Service

This monitor returns CPU and memory usage of the Citrix Licensing Support Service. This account controls reading the license files and updating strings with license trailers (data dictionary functionality).

Citrix Machine Creation Service

This monitor returns CPU and memory usage of the Citrix Machine Creation Service. It creates new Virtual Machines.

Citrix Monitor Service

This monitor returns CPU and memory usage of the Citrix Monitor Service. It monitors the FlexCast system.

Citrix Peer Resolution Service

This monitor returns CPU and memory usage of the Citrix Peer Resolution Service. It resolves peer names within peer-to-peer meshes.

Citrix Storefront Privileged Administration Service

This monitor returns CPU and memory usage of the Citrix Storefront Privileged Administration Service. It manages privileged operations on Storefront.

Citrix Storefront Service

This monitor returns CPU and memory usage of the Citrix Storefront Service. It manages deployment of Storefront.

Citrix Subscriptions Store

This monitor returns CPU and memory usage of the Citrix Subscriptions Store. It provides a store and replication of user subscriptions.

Citrix Web Services for Licensing

This monitor returns CPU and memory usage of Citrix Web Services for Licensing. It automates the allocation and installation of licenses on the Citrix License Server.

TCP Port: Web Site (HTTP)

This component monitor tests the ability of the Delivery Controller, Director, and Storefront services to accept incoming sessions by using HTTP protocol. By default it monitors TCP port 80.

TCP Port: Web Site (HTTPS)

This component monitor tests the ability of the Delivery Controller, Director, and Storefront services to accept incoming sessions by using HTTPS protocol. By default it monitors TCP port 443.
TCP Port: License Server (7279)

This component monitor tests the ability of a License service to accept incoming sessions. By default it monitors TCP port 7279.

TCP Port: License Server (27000)

This component monitor tests the ability of a License service to accept incoming sessions. By default it monitors TCP port 27000.

TCP Port: License Server (8083)

This component monitor tests the ability of a License service to accept incoming sessions. By default it monitors TCP port 8083.

TCP Port: License Server (8082)

This component monitor tests the ability of a License service to accept incoming sessions. By default it monitors TCP port 8082.
Clam AV

This template assesses the status and performance of a CUPS service installed on a Linux/Unix system. Perl scripts are used for retrieving performance data.

Prerequisites

SSH and Perl installed on the target server. SNMP installed on the target server and permission to monitor clamd processes.

Credentials

Root credentials on the target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Process: clamd

This monitor returns the CPU and memory usage of clamd process.

TCP Port: clamd

This component monitor tests the ability of a ClamAV service to accept incoming sessions. It monitors TCP port 3310.

By default, this monitor is disabled.

Antivirus Database Status

This monitor compares local antivirus database file (daily.cvd) version to the version advertised from the ClamAV site.

This script requires Net::DNS perl module. You can install this module by running the following command on ClamAV server:

```
perl -MCPAN -e 'install Net::DNS'
```

Before using this monitor you should provide full path to clamd command. For example:

```
/usr/local/sbin/clamd
```
CUPS

This template assesses the status and performance of a CUPS service installed on a Linux/Unix system. Perl scripts are used for retrieving performance data.

Works with the Orion Agent for Linux.

Prerequisites

SSH and Perl installed on the target server.

The user account used to monitor CUPS must have read access (generally restricted to root access) to the following files:

- /var/log/cups/page_log
- /var/log/cups/error_log

Credentials

Root credentials on the target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Daemon CUPS status

This monitor returns the status of a Linux/Unix print server daemon.

Possible values:

- 0 - CUPS daemon is stopped.
- 1 - CUPS daemon is running.

Print queue

This monitor returns the current length of the default print queue.

Total pages printed

This monitor returns the number of printed pages by retrieving data from the CUPS page_log file.

New emergency messages in CUPS error log

This monitor returns the number of new emergency messages by retrieving data from the CUPS error_log file. All emergency events begin with the “X” symbol.

This monitor should be zero all times. If it is not, you should manually examine this log file.
New warning messages in CUPS error log

This monitor returns the number of new warning messages by retrieving data from the CUPS error_log file. All emergency events begin with the “W” symbol.

This monitor should be zero all times. If it is not, you should manually examine this log file.

New alert messages in CUPS error log

This monitor returns the number of new alert messages by retrieving data from the CUPS error_log file. All emergency events begin with the “A” symbol.

This monitor should be zero all times. If it is not, you should manually examine this log file.

New critical error messages in CUPS error log

This monitor returns the number of new critical error messages by retrieving data from the CUPS error_log file. All emergency events begin with the “C” symbol.

This monitor should be zero all times. If it is not, you should manually examine this log file.

CUPS listening TCP port

This component monitor tests the ability of a CUPS service to accept incoming sessions.

By default, it monitors the TCP port 631. If your CUPS server listens on another port, you should manually change it.
DHCP User Experience Monitor

This template tests the availability of DHCP services for end users by performing typical DHCP request operations and measuring how long it takes to complete these operations.

**Prerequisites**

None.

**Credentials**

None.

**Monitored Components**

For details on monitors, see [SAM Component Monitor Types](#).

**DHCP User Experience Monitor**

This component monitor measures how long it takes to get a lease from a DHCP server. The monitor verifies that the DHCP responds with an IP address, but neither confirms nor accepts the lease. For details, see [DHCP User Experience Monitor](#).
Directory Size

This template determines the disk space used by files in a directory.

Prerequisites

WMI access on the target server.

Credentials

Administrator on the target server.

Monitored Components

Directory Size Monitor

This component monitor determines the disk space used by the files in a directory. By default, it monitors the Documents and Settings folder situated on the target server on the C drive. To change the target folder, you should provide the correct UNC path to that folder.

For example: `\${IP}\c$\Documents and Settings\`

By default, this monitor calculates the size of the directory, including its subdirectories. If you do not want to include subdirectories, uncheck the Include Subdirectories option.

By default, the File Extensions Filter option is set to the wildcard, `[*]`. This means the monitor will calculate the size of all the files. If you need to calculate the size of a certain type of file, add the proper extension, as in the following example:

For example: For only ZIP archives, you should set the filter option to "zip".

More information, see Directory Size monitor.
Distributed File System (DFS)

This template assesses the status and overall performance of a Microsoft Distributed File System (DFS) service. This template uses Windows Performance Counters, WMI Monitors and Windows DFS Replication Event Log.

**Prerequisites**

WMI access to the target server.

**Credentials**

Windows Administrator on the target server.

**Monitored Components**

You need to set thresholds for counters according to your environment. It is recommended to monitor counters for some period of time to understand potential value ranges and then set the thresholds accordingly. All Windows Event Log monitors (beginning with Warning or Error) should return zero values. Returned values other than zero indicate an abnormality. Examining the Windows DFS Replication log file should provide information pertaining to the issue.

**Service: DFS Namespace**

This counter monitors DFS Namespace service which enables you to group shared folders located on different servers into one or more logically structured namespaces. Each namespace appears to users as a single shared folder with a series of subfolders.

**Service: DFS Replication**

This counter monitors DFS Replication service which enables you to synchronize folders on multiple servers across local or wide area network connections. This service uses the Remote Differential Compression (RDC) protocol to update only the portions of files that have changed since the last replication.

**Replication Folders: Conflict Space In Use (B)**

This counter returns the total size (in bytes) of the conflict loser files and folders currently in the Conflict and Deleted folder used by the DFS Replication service. The DFS Replication service automatically detects and resolves conflicts encountered in replicated folders and moves the losing version to the Conflict and Deleted folder. The service automatically cleans up the Conflict and Deleted folder when it exceeds a pre-configured threshold of the quota.

The instance field is installation-specific. Open perfmon find the DFS Replicated Folders object. After that, choose any counter in this object and you will see available instances (for example: test-\{79E95064-B701-449D-9B3C-32FS8932B96B\}).
Replication Folders: Deleted Space In Use (B)

This counter returns the total size (in bytes) of the deleted files and folders currently in the Conflict and Deleted folder used by the DFS Replication service. The DFS Replication service detects remote deletes from its sending partner and moves the file or folder to the Conflict and Deleted folder. The service automatically cleans up the Conflict and Deleted folder when it exceeds a pre-configured threshold of the quota.

1. The instance field is installation-specific. Open perfmon and find the DFS Replicated Folders object. After that, choose any counter in this object and you will see available instances (for example: test-{79E95064-B701-449D-9B3C-32F58932B96B}).

Replication Folders: Staging Space In Use (B)

This counter returns the total size (in bytes) of the files and folders currently in the staging folder used by the DFS Replication service. This counter will fluctuate as staging space is reclaimed. The DFS Replication service stages files and folders in the staging folder before they are replicated, and automatically cleans up the staging folder when it exceeds a pre-configured threshold of the quota.

1. The instance field is installation-specific. Open perfmon and find the DFS Replicated Folders object. After that, choose any counter in this object and you will see available instances (for example: test-{79E95064-B701-449D-9B3C-32F58932B96B}).

Replication Folders: Updates Dropped

This counter returns the number of redundant file replication update records that were ignored by the DFS Replication service because they did not change the replicated file or folder. For example, dropped updates can occur when access control lists (ACLs) are overwitten with identical ACLs on a file or folder.

1. The instance field is installation-specific. Open perfmon and find the DFS Replicated Folders object. After that, choose any counter in this object and you will see available instances (for example: test-{79E95064-B701-449D-9B3C-32F58932B96B}).

Replication Folders: File Installs Retried

This counter returns the number of file installs that are being retried due to sharing violations or other errors encountered when installing the files. The DFS Replication service replicates staged files into the staging folder, decompresses them in the installing folder and renames them to the target location. The second and third steps of this process are known as installing the file.

This returned value should be as low as possible.

1. The instance field is installation-specific. Open perfmon and find the DFS Replicated Folders object. After that, choose any counter in this object and you will see available instances (for example: test-{79E95064-B701-449D-9B3C-32F58932B96B}).

DFS Replication State

This counter shows the current state of DFS Replication service.
Possible values:
- 0 - Service Starting
- 1 - Service Running
- 2 - Service Degraded
- 3 - Service Shutting Down

DFS Volume State
This counter shows the current DFS volume state.
Possible values:
- 0 - Initialized
- 1 - Shutting Down
- 2 - In Error
- 3 - Auto Recovery

Warning: Failed to Contact Configuration on DC
This monitor returns the number of events when the DFS Replication service failed to contact the domain controller to access configuration information.

Type of event: Warning. Event ID: 1204.
You should check your network connection.

Warning: Staging Space above High Watermark
This monitor returns the number of events when the DFS Replication service detected that the staging space usage exceeds the staging quota for the replicated folder. The service might fail to replicate some large files and the replicated folder might get out of sync. The service will attempt to clean up the staging space automatically.

Type of event: Warning. Event ID: 4202.
Staging files might be purged prematurely because the replicated folder contains files that are larger than the configured staging quota, or because the configured maximum staging size has been exceeded. This purging can cause excessive hard drive activity and CPU usage.

To avoid this error, increase the quota of the staging folder.

Warning: Failed to Clean Old Staging Data
This monitor returns the number of events when the DFS Replication service failed to clean up old staging files for the replicated folder at the local path. The service might fail to replicate some large files and the replicated folder might get out of sync. The service will automatically retry staging space cleanup in 30 minute intervals. The service may start cleanup earlier if it detects some staging files have been unlocked.

Type of event: Warning. Event ID: 4206.
It is recommended to increase the quota of the staging folder.
Warning: Staging Space above Staging Quota

This monitor returns the number of events when the DFS Replication service detected that the staging space usage is above the staging quota for the replicated folder at the local path. The service might fail to replicate some large files and the replicated folder might get out of sync. The service will attempt to clean up the staging space automatically.

Type of event: Warning. Event ID: 4208.

It is recommended to increase the quota of the staging folder.

Warning: File Prevented from Replication

This monitor returns the number of events when the DFS Replication service has been repeatedly prevented from replicating a file due to consistent sharing violations encountered on the file.

Type of events: Warning. Event ID: 4302 or 4304.

Event 4302: A local sharing violation occurs when the service cannot receive and update the file because the local file is being used. This occurs on the "receive" side of the file change. The file is already replicated. However, it cannot be moved from the installing directory to the final destination.

Event 4304: The service cannot stage a file for replication because of a sharing violation. This occurs on the "send" side of the file change. DFSR wants to stage or copy the file for replication; however, an exclusive lock prevents this.

Warning: No Configured Connections for Replication Folder

This monitor returns the number of events when the DFS Replication service has detected that no connections are configured for replication group. No data is being replicated for this replication group.

Type of event: Warning. Event ID: 6804.

If the data replicates through DFS Replication without any issues, ignore this event. If problems with replication exist, you should closely look at the replication folder configuration.

Error: Failed to Contact DC

This monitor returns the number of events when the DFS Replication service failed to contact the domain controller to access configuration information. Replication is stopped. The service will try again during the next configuration polling cycle.

Type of event: Error. Event ID: 1202.

The DFS Replication service could not contact the domain controller to obtain new configuration information. If replication was previously working and this error is reported, the service will use cached configuration, stored locally, but will not respond to any configuration changes until the issue is resolved.

This event can be caused by TCP/IP connectivity, firewall, Active Directory®, or DNS errors or misconfigurations.
Error: Replication Stopped

This monitor returns the number of events when the DFS Replication service stopped replication on the replicated folder on the local path.

Type of event: Error. Event ID: 4004.

When the DFS Replication service initializes the replicated folders for the replication process, it traverses all related paths to check whether the replicated folders are reparse points that act as symbolic links or that act as mount points.

The DFS Replication service expects to open synchronous handles to access these paths. However, it uses the asynchronous handles incorrectly. The DFS Replication service cannot handle the I/O requests that are held by a filter driver. Therefore, the DFS Replication service stops responding.

If the DFS Replication service stops responding, you may need to install the following HotFix: http://support.microsoft.com/kb/977381/EN-US. © 2018 Microsoft Corp., available at http://support.microsoft.com, obtained on October 31, 2018

Error: File Changed on Multiple Servers

This monitor returns the number of events when the DFS Replication service detected that a file was changed on multiple servers. A conflict resolution algorithm was used to determine the winning file. The losing file was moved to the Conflict and Deleted folder.

Type of event: Error. Event ID: 4412.

Error: Communication with Partner

This monitor returns the number of events when the DFS Replication service encountered an error communicating with a partner for the listed replication group.

Type of event: Error. Event ID: 5002.

This error usually appears when the DFS Replication service is unable to set up a Remote Procedure Call (RPC) binding to communicate with the partner. It may also be caused by RPC blocking at a firewall between partners, or a DNS error. Finally, this error may appear when the two partner computers are running different versions of Dfsr.exe.

Verify that normal communication between the two computers is working. Ensure that the same version of Dfsr.exe is running on both partner computers. The file is located at %system32%\DFSR.exe. You might need to install service packs, downloads or hotfixes on one or both computers to run matching versions of the service.

Error: Host Unreachable

This monitor returns the number of events when the DFS Replication service failed to communicate with a partner for the replication group. This error can occur if the host is unreachable or if the DFS Replication service is not running on the server.

Type of event: Error. Event ID: 5008.

Check network connectivity.
Error: Partner Didn’t Recognize the Connection

This monitor returns the number of events when the DFS Replication service failed to communicate with a partner for the replication group. The partner did not recognize the connection or the replication group configuration.

**Type of event:** Error. Event ID: 5012.

This error usually occurs when one partner attempts to establish an RPC connection with another member, but is unable to. The problem may be intermittent and resolve itself automatically. If the two members obtain configuration data from different domain controllers, they may have mismatched configuration data due to Active Directory replication reaching one domain controller before the other.

The service will retry the connection periodically. If this problem persists, please verify that Active Directory replication is working and that the service is able to reach a domain controller.

Error: Connection with Partner Removed or Disabled

This monitor returns the number of events when the DFS Replication service detected that the connection with a partner for the replication group has been removed or disabled.

**Type of event:** Error. Event ID: 5016.

Check network connectivity.

Error: Invalid Local Path to Replication Folder

This monitor returns the number of events when the replicated folder has an invalid local path.

**Type of event:** Error. Event ID: 6404.

DFS Replication cannot replicate the replicated folder because the configured local path is not the fully qualified path name of an existing, accessible local folder. This replicated folder is not replicating to or from this server.

Fix this problem by configuring the replicated folder with a valid local path using the DFS Management snap-in or the Dfsradmin.exe command-line tool.

Warning: No Free Space for Replication

This monitor returns the number of events when DFS Replication service encountered errors replicating one or more files because adequate free space was not available on volume. This volume contains the replicated folder, the staging folder, or both. The service will retry replication periodically.

**Type of event:** Error. Event ID: 4502.

Please make sure that enough free space is available on this volume for replication to proceed.
DNS User Experience

This template tests the ability of a DNS server to respond to a record query, and measures its responsiveness.

**Prerequisites**

None.

**Credentials**

None.

**Monitored Components**

For details on monitors, see [SAM Component Monitor Types](#).

**DNS User Experience Monitor**

This component monitor tests a DNS server’s ability to respond to a record query, compares the query response against a list of IP addresses, and measures the response time. The component monitor passes if the DNS response matches the expected IP addresses.

The DNS Monitor measures the time it takes the DNS “get” for the record query referenced in the component monitor to load. This response time is measured in milliseconds.

For details, see [DNS User Experience monitor](#)
Download Speed Monitor

This template tests the available bandwidth between the SAM server and another node on the network.

**Prerequisites**

A character generator service running on target server.

**Credentials**

None.

**Installing the Microsoft Windows Character Generator Service**

The Character Generator service is part of the Microsoft Windows Simple TCP/IP Services component.

To install the Simple TCP/IP Services component on Windows 2003 computers:

1. Log in to target server with an administrator-level account.
2. Open Add or Remove Programs in the Control Panel.
3. Click Add/Remove Windows Components.
4. Click Networking Services.
5. Click Details.
7. Click Ok, Next, and then click Finish to complete the wizard.

To install the Simple TCP/IP Services component on Windows 2008 (including R2) computers:

1. Log in to target server with an administrator-level account.
2. Open Server Manager by clicking Start > Server Manager.
3. In the left panel of the Server Manager, click Features.
4. In the right panel of the Server Manager, click Add Features.
5. In the Add Features Wizard, check the box for Simple TCP/IP Services.
6. Click Next, and then click Install.
7. When installation is finished, click Close.
8. The Simple TCP/IP Services will be started when the system is rebooted.
9. If you want to start the services immediately, click Start > Administrative Tools > Services.
10. Right-click Simple TCP/IP Services, and then select Start from the context menu.
Enabling the Unix/Linux Character Generator Service

The character generator service chargen is built into the standard Unix/Linux inetd daemon. If the service is not enabled, add the following lines to the /etc/inetd.conf configuration file, and then restart inetd.

```
chargen stream tcp nowait root internal chargen dgram udp wait root internal
```

Monitored Components

For details on monitors, see [SAM Component Monitor Types](#).

**Download Speed Monitor**

This component monitor measures the time it takes to download data from the target node, and reports the speed in KB/s (1024 bytes per second). The target node must be running a Character Generator service. For details, see [Download Speed Monitor](#).
Errors in Application Event Log

This template sets the state of the application to Down if there are any errors in the last five minutes of the Windows Application event log.

Prerequisites

WMI access to target server.

Credentials

Windows Administrator on target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Windows Event Log Monitor.

This component monitor can use both WMI and RPC communication to scan Windows Event Logs for recent events matching your defined criteria. Events are considered recent based on the age of the event as compared to the application polling frequency. If a matching event is found, the component monitor changes status.

The component monitor eventually returns to its original status as time passes so you may not notice a matching event unless you create an alert to email you when the component goes down.

This component monitor uses the following ports:

- TCP/135
- RPC/named pipes (NP) TCP 139
- RPC/NP TCP 445
- RPC/NP UDP 137
- RPC/NP UDP 138
Files

The following templates are available:

- File Age Monitor
- File Change Monitor
- File Count Script
- File Count
- File Existence Monitor
- File Size Monitor
File Age Monitor

This component monitor determines when a file was last modified.

**Statistic**

The statistic is the number of elapsed hours since the file modification date.

**Agent-less or Orion agent for Windows requirements**

Windows credentials with read access to the network share and file.

Implementation of these components relies either on WMI or Windows file share access to the target machine.

**Orion agent for Linux requirements**

Python implementation leverages native file system access directly from the python script that runs locally on the target agent machine.

To leverage this monitor against a Linux based system, the Orion Agent for Linux is required. This means that the Linux machine you plan to monitor must have the Linux agent installed, and that the node is managed using the agent within the Orion Platform.

Monitored Components

For details on monitors, see [SAM Component Monitor Types](#).

**File Age Monitor**

This component monitor determines when a file was last modified. The statistic is the number of elapsed hours since the file modification date. This component monitor uses TCP/445 and UDP/445 ports.
File Change Monitor

This template tests if a file was modified. The component monitor performs an MD5 checksum comparison on the file to verify it was not modified.

**Prerequisites**

If monitoring a Windows machine, you'll need Windows credentials with read access to the network share and file.

**Statistic**

The statistic is the number of hours since the file modification.

**Credentials**

Windows credential with read access to the network share and file.

**Agent-less or Orion agent for Windows requirements**

Implementation of these components relies either on WMI or Windows file share access to the target machine.

**Orion agent for Linux requirements**

Python implementation leverages native filesystem access directly from the python script running locally on the target agent machine. Due to the configuration settings, switching between agent-less and Orion agent for Linux will not establish a correct connection as the file path in UNC format will not work on a Linux-based computer. For details, see [Linux/Unix system configurations for component monitors](#).

**Monitored Components**

For details on monitors, see [SAM Component Monitor Types](#).

**File Change Monitor**

This component monitor tests if a file has been modified and then reports the time in hours since the file was modified as a statistic. The component monitor performs an MD5 checksum comparison on the file to verify it was not modified. If SolarWinds SAM detects the monitored file was modified, the component monitor will remain in a Down state until you recalculate the checksum. This component monitor uses TCP/445 and UDP/445 ports.
**File Count**

This component monitor determines the number of files within a directory.

**Prerequisites**

WMI access on target server.

**Credentials**

Administrator on target server.

**Monitored Components**

For details on monitors, see [SAM Component Monitor Types](#).

**File Count Monitor**

This component monitor determines the number of files within a directory. By default, it monitors the Documents and Settings folder situated on the target server the C:\ drive. To change target folder, you should provide the correct UNC path to the folder.

For example: `\${IP}\c$\Documents and Settings\`

By default, this monitor counts the number of files, including subdirectories. If you do not need the subdirectories included, you should uncheck the Include Subdirectories option.

By default, the File Extensions Filter option is set to the wildcard [\*] so that the monitor will count all files.

For example: If you need to count only ZIP archives, you should set this option to zip.
File Count Script

This template monitors the number of files in a directory. Specify the path as the script argument. The statistic is the number of files in the directory.

Prerequisites

None.

Credentials

Windows credentials valid on both the SAM and target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

File Count

This component monitor counts the number of files in a directory, optionally including its subdirectories. Files that do not match the file extension or file attribute type are ignored.

This monitor may fail if you attempt to count more than 20,000 files in a directory using the wildcard * filter extension. To get an accurate count of the files in such large directories, you must instead create a Windows Script monitor that runs the File Count script located in the script examples folder C:\Program Files\SolarWinds\Orion\APM\SampleScriptMonitors\WindowsScripts.
**File Existence Monitor**

This template tests if a file exists at the given file path.

**Prerequisites**

None.

**Credentials**

Windows credentials with read access to the network share.

**Agent-less or Orion agent for Windows requirements**

Implementation of these components relies either on WMI or windows file share access to the target machine.

**Orion agent for Linux requirements**

Python implementation leverages native file system access directly from the python script running locally on the target agent machine. Due to the configuration settings, switching between agent-less and Orion agent for Linux will not establish a correct connection as the file path in UNC format will not work on a Linux-based computer. For details, see [Linux/Unix system configurations for component monitors](#).

**Monitored components**

For details on monitors, see [SAM Component Monitor Types](#).

**File Existence Monitor**

This component monitor tests if a file exists at the given file path and uses ports TCP/445 and UDP/445.
File Size Monitor

This template measures the size of a file at the given file path. The statistic is the file size in bytes.

Prerequisites

None.

Credentials

Windows credential with read access to the network share.

Agent-less or Orion agent for Windows requirements

Implementation of these components relies either on WMI or windows file share access to the target machine.

Orion agent for Linux requirements

Python implementation leverages native filesystem access directly from the python script running locally on the target agent machine. Due to the configuration settings, switching between agent-less and Orion agent for Linux will not establish a correct connection as the file path in UNC format will not work on a Linux-based computer. For details, see [Linux/Unix system configurations for component monitors](#).

Monitored Components

For details on monitors, see [SAM Component Monitor Types](#).

File Size Monitor

This component monitor measures the size of a file at the given file path and then reports the file size in bytes as a statistic. This component monitor uses TCP/445 and UDP/445 ports.

This monitor cannot monitor files larger than 2 gigabytes in size.
FTP User Experience

This template tests the ability of an FTP server to accept incoming sessions, process user logins, and then transmit the requested file. The component monitor performs an SHA1 checksum comparison on the downloaded file to verify content integrity.

Prerequisites

None.

Credentials

FTP account with read permissions on target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

FTP User Experience Monitor

This component monitor tests the ability of an FTP server to accept an incoming session, process the user login, and then transmit the specified file to the Orion server. After receiving the file, SolarWinds SAM performs a file integrity test comparing the SHA1 checksum of the downloaded file against a previously generated checksum. If the checksums match, the component monitor reports its status as up.

The FTP Monitor measures the time it takes the FTP “get” for the reference in the component monitor to load. This response time is measured in milliseconds.
GlassFish (JMX)

This template monitors GlassFish server statistics by using the JMX protocol. You can use the Orion agent for Linux or SNMP agentless to monitor.

Works with the Orion Agent for Linux.

Prerequisites

Target server configured to allow JMX queries.

This template is configured to send JMX requests on port 8686.

Credentials

Dependent on the JMX configuration.

JMX Configurations for Orion agent for Linux

For JMX configurations, install and configure WebSphere per your Linux/Unix distribution. See the IBM Knowledge Center for details. The overall steps include:

1. Install WebSphere and note the following details:
   - You may need to create an administrator account and a new package group.
   - During installation, turn off the secure storage option as this is not needed.
   - Make sure to select the Application Server during installation.

2. Start and stop the WebSphere AppServer.

3. Use a browser to access the WebSphere AppServer console at http://websphere-host:9060/ibm/console
   - You may need to open a port to 9060 on the Websphere host.
   - Use the credentials for the account created during installation.

4. In the console, expose the JMX platform mbeans in the WebSphere AppServer by:
   a. Clicking Servers > Server Types > WebSphere application servers.
   b. Selecting the listed application server.

5. Locate the Java and Process Management > Process definition. In the Generic JVM arguments dialog box, enter the following code:

   ```
   Djavax.management.builder.initial=
   # Note: There is nothing after the = sign.
   Dcom.sun.management.jmxremote=true
   Dcom.sun.management.jmxremote.port=8686
   Dcom.sun.management.jmxremote.ssl=false
   ```
6. Restart the AppServer.

**Monitored Components**

All components may vary in a running environment. You can add your own threshold limits as needed.

**Classes Loaded Count**

This monitor returns the number of classes that are currently loaded in the Java virtual machine.

**Classes Total Loaded Count**

This monitor returns the total number of classes that have been loaded since the Java virtual machine has started execution.

**Classes Unloaded Count**

This monitor returns the total number of classes unloaded since the Java virtual machine has started execution.

**Memory Pending Final Count**

This monitor returns the approximate number of objects for which finalization is pending.

**Memory Heap Init Size (B)**

This monitor returns the initial amount of memory in bytes that the Java virtual machine allocates; or -1 if undefined.

**Memory Heap Used (B)**

This monitor returns the amount of used memory in bytes. The amount of used memory in the returned memory usage is the amount of memory occupied by both live objects and garbage objects that have not been collected, if any.

**Memory Heap Committed (B)**

This monitor returns the amount of committed memory in bytes.

**Memory Heap Max Size (B)**

This monitor returns the maximum amount of memory in bytes that can be used; or -1 if undefined.

**Memory Non Heap Init Size (B)**

This monitor returns the initial amount of memory in bytes that the Java virtual machine allocates; or -1 if undefined.

**Memory Non Heap Used (B)**

This monitor returns the amount of used memory in bytes.
**Memory Non Heap Committed (B)**

This monitor returns the amount of committed memory in bytes.

**Memory Non Heap Max Size (B)**

This monitor returns the maximum amount of memory in bytes that can be used; or -1 if undefined.

**Memory Garbage Collections Count**

This monitor returns the total number of collections that have occurred.

**Memory Garbage Collection Time (ms)**

This monitor returns the approximate accumulated collection elapsed time in milliseconds.

**Memory Pool Init Size (B)**

This monitor returns the initial amount of memory (in bytes) that the Java virtual machine requests from the operating system for memory management during startup. The Java virtual machine may request additional memory from the operating system and may also release memory to the system over time. The value of init may be undefined.

**Memory Pool Used (B)**

This monitor returns the amount of memory currently used (in bytes).

**Memory Pool Committed Size (B)**

This monitor returns the amount of memory (in bytes) that is guaranteed to be available for use by the Java virtual machine. The amount of committed memory may change over time (increase or decrease). The Java virtual machine may release memory to the system and committed could be less than init. committed will always be greater than or equal to used.

**Memory Pool Max Size (B)**

This monitor returns the maximum amount of memory (in bytes) that can be used for memory management. Its value may be undefined. The maximum amount of memory may change over time if defined. The amount of used and committed memory will always be less than or equal to max if max is defined. A memory allocation may fail if it attempts to increase the used memory such that used > committed even if used <= max would still be true (for example, when the system is low on virtual memory).

**Memory Pool Peak Used (B)**

This monitor returns the peak amount of memory currently used (in bytes).

**Memory Pool Peak Committed (B)**

This monitor returns the peak amount of memory (in bytes) that is guaranteed to be available for use by the Java virtual machine. The amount of committed memory may change over time (increase or decrease). The Java virtual machine may release memory to the system and committed could be less than init. committed will always be greater than or equal to used.
Memory Pool Peak Max Size (B)

This monitor returns the maximum peak amount of memory (in bytes) that can be used for memory management. Its value may be undefined. The maximum amount of memory may change over time if defined. The amount of used and committed memory will always be less than or equal to max if max is defined. A memory allocation may fail if it attempts to increase the used memory such that used > committed even if used <= max would still be true (for example, when the system is low on virtual memory).

Threads Total Started Count

This monitor returns the total number of threads created and also started since the Java virtual machine started.

Current Thread Count

This monitor returns the current number of live threads including both daemon and non-daemon threads.

Current Thread Cpu Time

This monitor returns the total CPU time for the current thread in nanoseconds.

Current Thread User Time

This monitor returns the CPU time that the current thread has executed in user mode in nanoseconds.

Runtime Uptime (ms)

This monitor returns the uptime of the Java virtual machine in milliseconds.

Compiler Time (ms)

This monitor returns the approximate accumulated elapsed time (in milliseconds) spent in compilation.
GoodLink Server for Microsoft Exchange

This template assesses the status and overall performance of a GoodLink Messaging Server integrated in Microsoft Exchange server. This template uses Windows System Event Log, Windows Service and PowerShell monitors.

Prerequisites

- GoodLink Server Command Line Tools should be installed on the target server. These tools can be found on GoodLink Server installation media in archive like this gmc-cli_1.3.5.235.zip. You need to unpack these tools somewhere, for example: C:\gmc-cli_1.3.5.235.
- Java installed on the target server;
- WinRM should be properly configured on the target server.

Credentials

GoodLink administrator (domain\user) on the target server. Also this user should be in the administrators group on the target server.

Monitored Components

For details on monitors, see [SAM Component Monitor Types](#).

Statistic for All Handhelds

This monitor returns statistics for all handhelds added in the GoodLink Server by running the GMExportStats.bat tool from GoodLink Server Command Line Tools. Returned values are as follows:

- **Email messages sent** – This component returns the total number of email messages sent to all handhelds from the Good Messaging Server.
- **Email messages received** – This component returns the total number of email messages received from all handhelds by the Good Messaging Server.
- **Filtered email** – This component returns the number of messages not sent to handhelds due to filters set on handhelds (using the Blocked Senders email option).
- **Calendar messages sent** – This component returns the number of calendar messages sent to all handhelds from the Good Messaging Server.
- **Calendar messages received** – This component returns the number of calendar messages received from all handhelds by the Good Messaging Server.
- **Task messages sent** – This component returns the number of total task messages sent to all handhelds by the Good Messaging Server.
- **Task messages received** – This component returns the number of total task messages received from all handhelds by the Good Messaging Server.
- **Messages sent** – This component returns the number of Total Email, Calendar, Contact, Note, and Task messages sent to all handhelds by the Good Messaging Server. (Includes control messages.)
- **Messages received** – This component returns the number of Total Email, Calendar, Contact, Note, and Task messages received from all handhelds by the Good Messaging Server. (Includes control messages.)

This monitor uses the following arguments:

```plaintext
path_to_GMExportStats,URL_to_GoodLink_Server,GoodLink_Server_hostname
where
path_to_GMExportStats - Full path to GMExportStats command;
URL_to_GoodLink_Server - URL to GoogLink server in format https://localhost:port;
GoodLink_Server_hostname - Hostname of GoodLink Server.
```

Example:

```plaintext
C:\gmc-cli_1.3.5.235\GMExportStats.bat,https://localhost:19005,ifrit
```

1. By default, this monitor has the Count statistic as difference box checked. It will show the statistic since the last polling period.

**Statistic for Specific Handheld**

This monitor returns statistics for a specific handheld added in the GoodLink Server by running the GMExportStats.bat tool from GoodLink Server Command Line Tools. Returned values are as follows:

- **Email messages sent** – This component returns the total number of email messages sent to a specific handheld from the Good Messaging Server.
- **Email messages received** – This component returns the total number of email messages received from specific handheld by the Good Messaging Server.
- **Filtered email** – This component returns the number of messages not sent to specific handheld due to filters set on handhelds (using the Blocked Senders email option).
- **Calendar messages sent** – This component returns the number of calendar messages sent to a specific handheld from the Good Messaging Server.
- **Calendar messages received** – This component returns the number of calendar messages received from a specific handheld by the Good Messaging Server.
- **Task messages sent** – This component returns the number of total task messages sent to a specific handheld by the Good Messaging Server.
- **Task messages received** – This component returns the number of total task messages received from a specific handheld by the Good Messaging Server.
- **Messages sent** – This component returns the number of Total Email, Calendar, Contact, Note, and Task messages sent to a specific handheld by the Good Messaging Server (includes control messages).
- **Messages received** – This component returns the number of Total Email, Calendar, Contact, Note, and Task messages received from a specific handheld by the Good Messaging Server (includes control messages).

This monitor uses the following arguments:

```plaintext
path_to_GMExportStats,URL_to_GoodLink_Server,GoodLink_Server_hostname,handheld
where
```
path_to_GMExportStats – Full path to GMExportStats command;
URL_to_GoodLink_Server – URL to GoogLink server in format
https://localhost:port;
GoodLink_Server_hostname – Hostname of GoodLink Server;
handheld – Handheld name which should be monitor.

Example:
C:\gmc-cli_
1.3.5.235\GMExportStats.bat,https://localhost:19005,ifrit,administrator

ℹ️ By default, this monitor has the Count statistic as difference box checked. It will show
statistic since the last polling period.

**Service: GoodLink Server**

This monitor returns CPU and memory usage of the GoodLink Server. Good Mobile Messaging Server
service which provides enterprise wireless email, calendar, contacts, and more.

**GoodLink Server TCP port**

This component monitor tests the ability of a GoodLink Server to accept incoming sessions. By
default it monitors TCP port 19005.
Group Policy Object (System and Application Logs)

This template assesses the status and overall performance of a Windows Group Policy Object by checking Windows logs for critical events. This template sets the state of the application to Down if there are any errors or warnings related with the Group Policy Object within the last five minutes. In Windows Server 2003, the Group Policy Object writes events to the application log. In Windows Server 2008, the Group Policy Object writes events to the system log.

Prerequisites

- WMI access to the target server.

Credentials

- Windows Administrator on the target server.

This template is based on the following information:

Group Policy troubleshooting tips can be found here:

Monitored Components

For details on monitors, see SAM Component Monitor Types.

All monitors should return zero values. Returned values other than zero indicate an abnormality. Examining the Windows system and application log files should provide information pertaining to the issue.

Failed Allocation

This monitor returns the number of memory allocation fails.

Type of event: Error. Event ID: 1002.

DS Bind Failure

This monitor returns the number of failed authentication attempts of the Active Directory.

Type of event: Error. Event ID: 1006.

Site Query Failure

This monitor returns the number of failed attempts to query the Active Directory Site using the credentials of the user or computer.

Type of event: Error. Event ID: 1007.
GPO Query Failure
This monitor returns the number of failed attempts to query Group Policy Objects.
Type of event: Error. Event ID: 1030.

Computer Role Failure
This monitor returns the number of failed attempts to determine the role of the computer, (i.e.: workgroup, domain member, or domain controller).
Type of event: Error. Event ID: 1052.

User Name Resolution Failure
This monitor returns the number of failed attempts to resolve a user name.
Type of event: Error. Event ID: 1053.

DC Resolution Failure
This monitor returns the number of failed attempts to obtain the name of a domain controller.
Type of event: Error. Event ID: 1054.

Computer Name Resolution Failure
This monitor returns the number of failed attempts to resolve a computer name.
Type of event: Error. Event ID: 1055.

Policy Read Failure
This monitor returns the number of failed attempts to read the GPT.INI of a Group Policy Object.
Type of event: Error. Event ID: 1058.

WMI Evaluation Failure
This monitor returns the number of failed attempts to evaluate a WMI filter.
Type of event: Error. Event ID: 1065.

GPO Search Failure
This monitor returns the number of failed attempts to obtain a list of Group Policy Objects.
Type of event: Error. Event ID: 1079.

OU Search Failure
This monitor returns the number of failed attempts to search the Active Directory Organizational Unit hierarchy.
Type of event: Error. Event ID: 1080.

CSE Failure Warning
This monitor returns the number of events when the Group Policy client side extension fails.
Type of event: Warning. Event ID: 1085.
Excessive GPO Failure

This monitor returns the number of events for when the scope of Group Policy Objects, for a computer or user, exceeds 999.

Type of event: Error. Event ID: 1088.

RSOP Session Failure

This monitor returns the number of events when a Resultant Set of Policy session fails.

Type of event: Warning. Event ID: 1089.

WMI Failure

This monitor returns the number of events the Group Policy service encounters caused by errors with the WMI service.

Type of event: Warning. Event ID: 1090.

RSOP CSE Failure

This monitor returns the number of events the Group Policy client side extension has due to failed attempts to record Resultant Set of Policy information.

Type of event: warning. Event ID: 1091.

RSOP Failure

This monitor returns the number of errors that occur while recording Resultant Set of Policy information.

Type of event: warning. Event ID: 1095.

The Group Policy service logs this event when an error occurs while recording Resultant Set of Policy information.

Registry.pol Failure

This monitor returns the number of failed attempts to read registry.pol.

Type of event: Error. Event ID: 1096.

Computer Token Failure

This monitor returns the number of failed attempts to read the computer's authentication token.

Type of event: Error. Event ID: 1097.

Object Not Found Failure

This monitor returns the number of failed attempts to locate an Active Directory object.

Type of event: Error. Event ID: 1101.

WMI Filter Not Found Warning

This monitor returns the number of failed attempts to locate an associated WMI filter.

Type of event: Warning. Event ID: 1104.
**Cross Forest Discovery Failure**

This monitor returns the number of failed attempts to determine if the user and computer belong to the same forest.

Type of event: Error. Event ID: 1110.

**CSE Synchronous Warning**

This monitor returns the number of events when a Group Policy client side extension requires synchronous policy processing to apply one or more policy settings.

Type of event: warning. Event ID: 1112.

**Time Skew Failure**

This monitor returns the number of events that indicate the time on the local computer is not synchronized with the time on the domain controller.

Type of event: Error. Event ID: 1126.

**DC Connectivity Failure**

This monitor returns the number of events when there is an absence of authenticated connectivity from the computer to the domain controller.

Type of event: error. Event ID: 1129.

**Script Failure**

This monitor returns the number of failed attempts to run a script.

Type of event: Error. Event ID: 1130.
Helix

The following templates are available:

- Helix Universal Media Server (Linux/Unix)
- Helix Universal Media Server (Windows)
Helix Universal Media Server (Linux/Unix)

This template assesses the performance of the Real Helix Universal Media Server on Linux/Unix machines. It uses Perl scripts to get statistics from RSS log files and an SNMP process monitor for monitoring Universal Media Server process.

Prerequisites

SSH and Perl installed on the target server. SNMP installed on the target server and permission to monitor rmserver processes.

Credentials

Root credentials on the target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

You need to set thresholds for counters according to your environment. It is recommended to monitor counters for some period of time to understand potential value ranges and then set the thresholds accordingly. For more information, see "Using the Orion APM Min/Max/Average statistics data for creating threshold settings" in the SolarWinds Success Center.

All Linux/Unix monitors retrieve statistical information from RSS log files which can be found here:

<Path_To_Helix_Folder>/Logs/rss/.

Each RSS configuration varies as to how many log files will be stored and how often this statistic will be updated. By default, the RSS interval is set to one minute in the following folder.

(rmsserver.cfg file, “RSS Logging” section)

Before using this template, the correct arguments should be set to all Linux/Unix monitors. Following is an example using the arguments field:

perl ${SCRIPT} “/usr/Helix/Logs/rss/rsslogs.*”

rsslogs.* should be put at the end of the RSS folder path. The entire argument should be within in double brackets. The script in monitors automatically determine which log file is the most recent and will retrieve statistical information from it.

CPU usage

This component monitor returns the overall use of system processor time. For machines with up to 4 CPUs, these statistics provide an accurate guide to the server processing load. For machines with more processors, the number may fall short in representing the actual server load. Returned values are as follows:
• **User** – This monitor returns the percentage of time used by the server itself, not counting operating system time and kernel time.

• **Kernel** – This monitor returns the percentage of time used by the operating system kernel on behalf of the server.

• **System** – This monitor returns the total system CPU load, including CPU used by other applications. This includes both user and kernel time.

**Memory Statistic and Allocations**

This component monitor returns statistics about actual server memory usage, memory allocation according to the operating system, and allocated memory, in Kilobytes, divided by the number of currently connected media players at the time the RSS report was written. Returned values are as follows:

• **Used** – This monitor returns the amount of memory, in units defined by a script, in use by the server when the RSS report was written. This may be less than the amount of application memory reported by the operating system. The difference represents memory that the server has reserved for use, but that is currently idle.

• **Cache_Hit_Ratio** – This monitor returns the percentage of memory operations during this RSS period that were carried out using the server’s memory cache. (This cache is internal to the server and unrelated to L1/L2 system memory cache.) Because these operations occur faster with less resource contention than non-cached memory functions, a higher percentage indicates greater server efficiency.

• **Used_High_Watermark** – This monitor returns the high-water mark for the amount of memory used, in units defined by a script. This should be close to the amount of application memory in use as reported by the operating system. This number, which may have been reached in a preceding RSS period, never falls until the server is restarted. The maximum value is set by the -m command option.

• **Pages** – This monitor returns the high-water mark for the amount of memory used, in pages.

• **Memory_Mapped_IO** – This monitor returns the amount of memory, in units defined by a script, used for memory-mapped I/O when this report was written. This memory is not included in the application memory allocation. It is not limited by the -m option.

• **Memory_Per_Player** – This monitor returns the allocated memory, in kB, divided by the number of currently connected media players. Keep in mind that this is only an average and the amount of memory allocated to each player can vary widely depending on the type of player and the type of media streamed.

**Players statistic**

This component monitor returns general statistics about how many new players are connected or disconnected. Returned values are as follows:

• **Total** – This monitor returns the total number of players connected when the RSS report was written.

• **New** – This monitor returns the number of new player connections since the start of this RSS interval.

• **Leaving** – This monitor returns the number of players disconnected since the start of this RSS interval.
Players by Protocol

This component monitor returns the percentage of media players using each of the supported control protocols in their streaming sessions. This breakdown includes the total number of players connected when the RSS report was generated. Returned values are as follows:

- **RTSP** – This monitor returns the percentage of players connected through RTSP and RTSP cloaked as HTTP.
- **RTMP** – This monitor returns the percentage of players connected through RTMP and RTMP cloaked as HTTP.
- **MMS** – This monitor returns the percentage of players connected through MMS and MMS cloaked as HTTP.
- **HTTP** – This monitor returns the percentage of players using HTTP as the control protocol. This does not include players using RTSP or MMS cloaked as HTTP.

Players by Transport

This component monitor returns the percentage of media players using each of the supported transports in their streaming sessions. This breakdown includes the total number of players that have connected since the start of this RSS interval. The total number of players connected in a scalable multicast is unknown during the broadcast. Players may report connection statistics to a Web server after the broadcast ends. Returned values are as follows:

- **TCP** – This monitor returns the percentage of players receiving data by TCP.
- **UDP** – This monitor returns the percentage of players receiving data by UDP.
- **Multicast** – This monitor returns the percentage of players connected through a back-channel multicast.

HTTP Connections

This component monitor returns the percentage of persistent, secure and cloaked, connections to the server. Returned values are as follows:

- **Persistent** – This monitor returns the percentage of persistent HTTP connections.
- **Secure** – This monitor returns the percentage of secure HTTP connections.
- **Cloaked** – This monitor returns the percentage of cloaked HTTP connections.

Bandwidth Statistic

This component monitor provides a guide to how well the server fulfills the requirements for streaming rates of requested media. These statistics can help you determine if the server’s outgoing bandwidth is sufficient to meet your streaming media needs. Returned values are as follows:

- **Output** – This monitor returns the average amount of bandwidth, in units defined by a script, that the server delivered to the network over the RSS period.
- **Bandwidth_Per_Player** – This monitor returns the average amount of bandwidth per media player during the RSS period, in units defined by a script. This is equal to the Output value divided by the number of players connected when the RSS report was written.
Subscribed – This monitor returns the percentage value that indicates the total output bandwidth divided by the cumulative bandwidth for all media player Subscribe requests. An RTSP Subscribe request indicates the encoded rate of a clip or broadcast requested by the media player.

For example: To receive a 512 Kbps encoding of a SureStream clip, a player sends a Subscribe request for the 512 Kbps stream. The returned value should be as high as possible. This monitor can return values greater than 100%. If the returned value is less than 100%, it may indicate that the server is not meeting the player's stream requests.

Nominal – This monitor returns the percentage value that equals the total outgoing bandwidth divided by the delivery bandwidth that media players have requested using the RTSP SetDeliveryBandwidth directive. This directive indicates the rate at which the player wants to receive the stream, regardless of the stream’s encoded rate.

For example: Upon requesting a stream, a player may set an initial high delivery rate to fill its buffer quickly. The returned value should be as high as possible. This monitor can return values greater than 100%. If the returned value is less than 100%, it may indicate that the server is not meeting the player’s stream requests.

Network Recent Statistic

This component monitor returns miscellaneous network statistics. Returned values are as follows:

- **Written Packets** – This monitor returns the number of packets written to the network in this RSS period.
- **Overload** – This monitor returns the number of packets that were late being scheduled.
- **No Buffer Errors** – This monitor returns the number of ENOBUFS errors returned from UDP socket network write calls. An ENOBUFS error indicates that the output queue for a network interface was full. This generally means that the interface has stopped sending, which may be caused by transient congestion. A consistent, high number of these errors across many RSS periods indicate a consistently congested network.
- **Other_UDP_Errors** – This monitor returns the number of general UDP write errors encountered. A consistent, high number of these errors may indicate technical problems with your network connection.
- **Behind** – This monitor returns the number of packets that were written to the network late. These packets may or may not arrive too late to be of use to a media player. A large number of late packets may cause increased media player resend requests.
- **Resend** – This monitor returns the number of packet resend requests made by media players that the server honored.
- **Aggregated_Packets** – This monitor returns the number of aggregated packets written. Aggregated packets are packets from 200 to 1,350 bytes in size that the server writes when it determines that the large size is an efficient delivery means given the current server load and network state. Aggregating packets reduces CPU load and helps the server run more efficiently. As server load increases, the server tries to write more, and larger, aggregated packets. Packets are aggregated for streams using the UDP transport and the RealNetworks proprietary RDT packet format. Packets for streams using the TCP transport or the standards-based RTP format are not aggregated.
- **WouldBlocks** – This monitor returns the number of packet write attempts during this RSS interval that were blocked by the network (i.e. EWOULDBLOCK errors). When a write attempt is blocked, the server queues the blocked packet, attempting to deliver it later. In many cases, a successful delivery may occur within milliseconds of the blocked attempt, allowing the packet to reach the media player on time. A positive value for WouldBlocks typically reflects temporary network congestion. However, a consistently high number of blocked writes across several RSS periods may indicate persistent network problems. If you notice a frequent, high number for WouldBlocks, check for increases in the Behind and Resend values on the preceding lines of the RSS report to determine if the WouldBlocks events affected packet delivery.

- **Accepts** – This monitor returns the number of incoming socket connections accepted since the last RSS interval. The number is typically close to the New players number, as most Accepts indicate a request from a new media player or another resource, such as a proxy or a transmitter. If the returned value is far greater than the New players number, this may indicate an external security issue, such as a denial-of-service attack.

### Mutex Collisions, Scheduler and Network Items

This component monitor returns the statistic concerning Mutex Collisions, the activity of the server’s internal Scheduler, and network items such as reads and writes. Returned values are as follows:

- **Mutex_Collisions** – This monitor returns the average number of collisions per second, as measured across this RSS period. A Mutex collision occurs when one server process must wait for another process to release a lock on a shared server resource. Mutex collisions are normal, and the number to expect can vary greatly depending on server tasks and load, as well as the machine architecture. A consistently high number, such as 100,000 or more collisions per second, may indicate a server problem.

- **CPU_Spinning** – This monitor returns a rough measure of Mutex collisions as related to average CPU usage. Ideally, this value should be near zero. A number greater than a fraction of a percent (such as 2.000%) indicates a great deal of Mutex contention.

- **Memory_Ops** – This monitor returns the approximate percentage of Mutex collisions caused by non-mainlock locks. These are primarily memory-related locks, but also include registry locks and other types of locks. This value should be as low as possible.

- **Scheduled_Items_With_Mutex** – This monitor returns the number of non-threadsafes actions that were scheduled to occur at a specific time that were triggered. These items cause greater Mutex contention, as well as reduced scalability and performance relative to the Without Mutex items.

- **Scheduled_Items_Without_Mutex** – This monitor returns the number of threadsafe actions that were scheduled to occur at a specific time that were triggered. A higher value relative to the With Mutex value indicates better server performance.

- **Network_Read_Items** – This monitor returns the number of reads to network sockets that were completed in this RSS interval.

- **Network_Write_Items** – This monitor returns the number of writes to network sockets that were completed in this RSS interval.

### Miscellaneous Statistic

This component monitor returns information about the internal server state. Returned values are as follows:
**File_Objects** – This monitor returns the number of internal file objects currently in use. When a server plug-in generates streaming packets for a clip, it opens one or more file objects. The number of open file objects may therefore be twice or more the number of connected media players.

**Idle_Streams** – This monitor returns the number of streams that are currently idle. (PPM refers to the server's standard packet delivery system.) Each stream using PPM periodically enters a state where it is ready to send more data to the player, but does not yet have any packets to send. That stream then goes idle, temporarily.

**Forced_Selects** – This monitor returns the number of times the server had to service a timer-triggered event without having data to read or write.

**Aggregation_Support** – This monitor returns the number of PPM streams that support packet aggregation.

**Total_Crash_Avoidances** – This monitor returns the total number of crash avoidances (CAs) since the last server restart. A CA occurs when the server uses fault-tolerance features to compensate for a problem. For example, if the server encounters corrupt packets in a media file, it attempts to compensate by dropping the corrupt packets and continuing the stream past the corruption point. If it can compensate without terminating the stream, it logs the event as a CA. A small number of CA's is to be expected, and does not indicate a significant problem. A consistently high number of CA's across several RSS periods may indicate serious system problems.

**Current_Crash_Avoidances** – This monitor returns the number of crash avoidances (CAs) have occurred within the current, four-hour window. If it reaches 1,000, the server automatically restarts in an attempt to reset into a more stable state. A CA occurs when the server uses fault-tolerance features to compensate for a problem. For example, if the server encounters corrupt packets in a media file, it attempts to compensate by dropping the corrupt packets and continuing the stream past the corruption point. If it can compensate without terminating the stream, it logs the event as a CA. A small number of CA's is to be expected, and does not indicate a significant problem. A consistently high number of CA's across several RSS periods may indicate serious system problems.

**Net_Devices** – This monitor returns the number of network connections to the server, other than media player requests, at the time the RSS report was written. This number includes proxy accounting connections, as well as connections to other Helix Servers for content distribution, live stream splitting, and so on.

**Broadcast Reception Statistic**

This component monitor provides statistics about incoming broadcast streams. Returned values are as follows:

- **Feeds** – This monitor returns the number of live feeds coming into the server from encoders or other Helix Server transmitters when the RSS report was written.
- **Total_Bandwidth** – This monitor returns the total amount of bandwidth, in units defined by a script, coming into the server as live streams.
- **Packets** – This monitor returns the total number of live stream packets arriving at the server during this RSS period.
- **Lost** – This monitor returns the total number of packets lost in transit to this server during this RSS period.
- **Lost_Upstream** – This monitor returns the number of live packets reported as lost by upstream transmitters. These packets were lost before the live stream was sent through the network to this receiver.
- **Resends** – This monitor returns the total number of packet resends this receiver requested from encoders or upstream transmitters. The receiver requests a resend of a lost packet only if it determines the packet will arrive in time to be of use in its broadcast stream. In general, the lower the amount of receiver buffering, the fewer resends the receiver requests.
- **Out_of_Order** – This monitor returns the total number of packets for live streams received out of order during this RSS interval.
- **Duplicate** – This monitor returns the total number of duplicate packets received for all live streams during this RSS interval.
- **Late** – This monitor returns the total number of late packets for all live streams received during this RSS interval. The packets may or may not have been too late to be of use in the broadcast.

**Broadcast Distribution Statistic**

This component monitor provides statistics about streams being split to downstream receivers. This information applies only to downstream Helix Server receivers. Returned values are as follows:

- **Feeds** – This monitor returns the total number of split feeds (both push and pull) being transmitted by this server when the RSS report was published.
- **Push** – This monitor returns the total number of push-split feeds being transmitted by this server. With a push feed, the server sends the stream to a downstream receiver once the stream is available.
- **Pull** – This monitor returns the total number of pull-split feeds being transmitted by this server. With a pull feed, the server does not send the stream to a downstream receiver until the receiver requests it.
- **Data_Transmitted** – This monitor returns the amount of data transmitted by all feeds, in units defined by a script.
- **Packets** – This monitor returns the total number of packets transmitted for the live feeds during this RSS interval.
- **Resends** – This monitor returns the number of resend requests processed by this transmitter. The transmitter will not honor the resend request if the packet was lost upstream, or if it determines that the packet will arrive at the receiver too late to be of use.
- **Requested** – this component returns the number of resends requested by downstream receivers.
- **Lost_Upstream** – This monitor returns the number of live packets lost by upstream transmitters. A value greater than 0 is reported only if this server is not the origin transmitter for the stream.
- **Dropped** – This monitor returns the number of packets dropped by this transmitter. This typically occurs if the packet arrives late from the encoder or upstream transmitter, and the server determines that the packet will subsequently arrive at downstream receivers too late to be of use.
Broadcast Core Statistic

This component monitor provides statistics about streams being split to downstream receivers. This information applies only to downstream Helix Server receivers. Returned values are as follows:

- **Dropped Packets** – This monitor returns the number of live stream packets dropped in this RSS period by the broadcast core. These packets were queued for another process or thread, but were dropped when the queue for that process or thread overflowed. A significant number of dropped packets indicate a general system overload.

- **Client Overflows** – This monitor returns the number of live stream packets dropped in this RSS period because the outgoing connection to the receiving client was blocked. Although the server buffers packets to compensate for temporary blockages, it drops the packets if the network blockage does not clear quickly enough.

Main Loop Iterations

This component monitor provides statistics about streams being split to downstream receivers. This information applies only to downstream Helix Server receivers. Returned values are as follows:

- **Main Loop Iterations** – This monitor returns the average number of loop iterations for all server processes per second during this RSS period.

- **Load State** – This monitor returns the server's current load state: 0–Normal, 1–High, 2–Extreme. The server gauges its internal state using several measurements, including the number of packets written late to the network. During high load states, the server attempts to write large aggregate packets to conserve CPU usage.

Process: rmserver

This component monitor returns the CPU and memory usage of Real Helix Universal Media Server process (rmserver).
Helix Universal Media Server (Windows)

This template assesses the performance of the Real Helix Universal Media Server on Windows machines. It uses PowerShell scripts to get statistics from RSS log files and WMI process monitors for monitoring Universal Media Server process.

Prerequisites

WinRM must be installed and properly configured on the target server. APM and Helix servers should be in the same domain.

Credentials

Domain administrator credentials on the target server (WinRM requirement).

Monitored Components

- For details on monitors, see SAM Component Monitor Types.
- You need to set thresholds for counters according to your environment. It is recommended to monitor counters for some period of time to understand potential value ranges and then set the thresholds accordingly. For more information, see "Using the Orion APM Min/Max/Average statistics data for creating threshold settings" in the SolarWinds Success Center.

All PowerShell monitors retrieve statistical information from RSS log files which can be found here:

```<Path_To_Helix_Folder> \Logs\rss>```

Each RSS configuration varies as to how many log files will be stored and how often this statistic will be updated. By default, the RSS interval is set to one minute in the following folder.

`(rmserver.cfg file, “RSS Logging” section)`

Before using this template, the correct arguments should be set to all PowerShell monitors. Following is an example using the arguments field:

```C:\Program Files\Real\Helix Server\Logs\rss```

The entire argument should be within in double brackets. The script in monitors automatically determine which log file is the most recent and will retrieve statistical information from it.

CPU usage

This component monitor returns the overall use of system processor time. For machines with up to 4 CPUs, these statistics provide an accurate guide to the server processing load. For machines with more processors, the number may fall short in representing the actual server load. Returned values are as follows:
- **User** – This monitor returns the percentage of time used by the server itself, not counting operating system time and kernel time.

- **Kernel** – This monitor returns the percentage of time used by the operating system kernel on behalf of the server.

- **System** – This monitor returns the total system CPU load, including CPU used by other applications. This includes both user and kernel time.

**Memory Statistic and Allocations**

This component monitor returns statistics about actual server memory usage, memory allocation according to the operating system, and allocated memory, in Kilobytes, divided by the number of currently connected media players at the time the RSS report was written. Returned values are as follows:

- **Used** – This monitor returns the amount of memory, in units defined by a script, in use by the server when the RSS report was written. This may be less than the amount of application memory reported by the operating system. The difference represents memory that the server has reserved for use, but that is currently idle.

- **Cache_Hit_Ratio** – This monitor returns the percentage of memory operations during this RSS period that were carried out using the server’s memory cache. (This cache is internal to the server and unrelated to L1/L2 system memory cache.) Because these operations occur faster with less resource contention than non-cached memory functions, a higher percentage indicates greater server efficiency.

- **Used_High_Watermark** – This monitor returns the high-water mark for the amount of memory used, in units defined by a script. This should be close to the amount of application memory in use as reported by the operating system. This number, which may have been reached in a preceding RSS period, never falls until the server is restarted. The maximum value is set by the -m command option.

- **Pages** – This monitor returns the high-water mark for the amount of memory used, in pages.

- **Memory_Mapped_IO** – This monitor returns the amount of memory, in units defined by a script, used for memory-mapped I/O when this report was written. This memory is not included in the application memory allocation. It is not limited by the -m option.

- **Memory_Per_Player** – This monitor returns the allocated memory, in kB, divided by the number of currently connected media players. Keep in mind that this is only an average and the amount of memory allocated to each player can vary widely depending on the type of player and the type of media streamed.

**Players statistic**

This component monitor returns general statistics about how many new players are connected or disconnected. Returned values are as follows:

- **Total** – This monitor returns the total number of players connected when the RSS report was written.

- **New** – This monitor returns the number of new player connections since the start of this RSS interval.

- **Leaving** – This monitor returns the number of players disconnected since the start of this RSS interval.
Players by Protocol

This component monitor returns the percentage of media players using each of the supported control protocols in their streaming sessions. This breakdown includes the total number of players connected when the RSS report was generated. Returned values are as follows:

- **RTSP** – This monitor returns the percentage of players connected through RTSP and RTSP cloaked as HTTP.
- **RTMP** – This monitor returns the percentage of players connected through RTMP and RTMP cloaked as HTTP.
- **MMS** – This monitor returns the percentage of players connected through MMS and MMS cloaked as HTTP.
- **HTTP** – This monitor returns the percentage of players using HTTP as the control protocol. This does not include players using RTSP or MMS cloaked as HTTP.

Players by Transport

This component monitor returns the percentage of media players using each of the supported transports in their streaming sessions. This breakdown includes the total number of players that have connected since the start of this RSS interval. The total number of players connected in a scalable multicast is unknown during the broadcast. Players may report connection statistics to a Web server after the broadcast ends. Returned values are as follows:

- **TCP** – This monitor returns the percentage of players receiving data by TCP.
- **UDP** – This monitor returns the percentage of players receiving data by UDP.
- **Multicast** – This monitor returns the percentage of players connected through a back-channel multicast.

HTTP Connections

This component monitor returns the percentage of persistent, secure and cloaked, connections to the server. Returned values are as follows:

- **Persistent** – This monitor returns the percentage of persistent HTTP connections.
- **Secure** – This monitor returns the percentage of secure HTTP connections.
- **Cloaked** – This monitor returns the percentage of cloaked HTTP connections.

Bandwidth Statistic

This component monitor provides a guide to how well the server fulfills the requirements for streaming rates of requested media. These statistics can help you determine if the server’s outgoing bandwidth is sufficient to meet your streaming media needs. Returned values are as follows:

- **Output** – This monitor returns the average amount of bandwidth, in units defined by a script, that the server delivered to the network over the RSS period.
- **Bandwidth_Per_Player** – This monitor returns the average amount of bandwidth per media player during the RSS period, in units defined by a script. This is equal to the Output value divided by the number of players connected when the RSS report was written.
- **Subscribed** – This monitor returns the percentage value that indicates the total output bandwidth divided by the cumulative bandwidth for all media player Subscribe requests. An RTSP Subscribe request indicates the encoded rate of a clip or broadcast requested by the media player.

- **For example:** To receive a 512 Kbps encoding of a SureStream clip, a player sends a Subscribe request for the 512 Kbps stream. The returned value should be as high as possible. This monitor can return values greater than 100%. If the returned value is less than 100%, it may indicate that the server is not meeting the player’s stream requests.

- **Nominal** – This monitor returns the percentage value that equals the total outgoing bandwidth divided by the delivery bandwidth that media players have requested using the RTSP SetDeliveryBandwidth directive. This directive indicates the rate at which the player wants to receive the stream, regardless of the stream’s encoded rate.

For example: Upon requesting a stream, a player may set an initial high delivery rate to fill its buffer quickly. The returned value should be as high as possible. This monitor can return values greater than 100%. If the returned value is less than 100%, it may indicate that the server is not meeting the player’s stream requests.

**Network Recent Statistic**

This component monitor returns miscellaneous network statistics. Returned values are as follows:

- **Written_Packets** – This monitor returns the number of packets written to the network in this RSS period.

- **Overload** – This monitor returns the number of packets that were late being scheduled.

- **No_Buffer_Errors** – This monitor returns the number of ENOBUFS errors returned from UDP socket network write calls. An ENOBUFS error indicates that the output queue for a network interface was full. This generally means that the interface has stopped sending, which may be caused by transient congestion. A consistent, high number of these errors across many RSS periods indicate a consistently congested network.

- **Other_UDP_Errors** – This monitor returns the number of general UDP write errors encountered. A consistent, high number of these errors may indicate technical problems with your network connection.

- **Behind** – This monitor returns the number of packets that were written to the network late. These packets may or may not arrive too late to be of use to a media player. A large number of late packets may cause increased media player resend requests.

- **Resend** – This monitor returns the number of packet resend requests made by media players that the server honored.

- **Aggregated_Packets** – This monitor returns the number of aggregated packets written. Aggregated packets are packets from 200 to 1,350 bytes in size that the server writes when it determines that the large size is an efficient delivery means given the current server load and network state. Aggregating packets reduces CPU load and helps the server run more efficiently. As server load increases, the server tries to write more, and larger, aggregated packets. Packets are aggregated for streams using the UDP transport and the RealNetworks proprietary RDT packet format. Packets for streams using the TCP transport or the standards-based RTP format are not aggregated.
• **WouldBlocks** – This monitor returns the number of packet write attempts during this RSS interval that were blocked by the network (i.e. EWOULDBLOCK errors). When a write attempt is blocked, the server queues the blocked packet, attempting to deliver it later. In many cases, a successful delivery may occur within milliseconds of the blocked attempt, allowing the packet to reach the media player on time. A positive value for WouldBlocks typically reflects temporary network congestion. However, a consistently high number of blocked writes across several RSS periods may indicate persistent network problems. If you notice a frequent, high number for WouldBlocks, check for increases in the Behind and Resend values on the preceding lines of the RSS report to determine if the WouldBlocks events affected packet delivery.

• **Accepts** – This monitor returns the number of incoming socket connections accepted since the last RSS interval. The number is typically close to the New players number, as most Accepts indicate a request from a new media player or another resource, such as a proxy or a transmitter. If the returned value is far greater than the New players number, this may indicate an external security issue, such as a denial-of-service attack.

**Mutex Collisions, Scheduler and Network Items**

This component monitor returns the statistic concerning Mutex Collisions, the activity of the server's internal Scheduler, and network items such as reads and writes. Returned values are as follows:

• **Mutex_Collisions** – This monitor returns the average number of collisions per second, as measured across this RSS period. A Mutex collision occurs when one server process must wait for another process to release a lock on a shared server resource. Mutex collisions are normal, and the number to expect can vary greatly depending on server tasks and load, as well as the machine architecture. A consistently high number, such as 100,000 or more collisions per second, may indicate a server problem.

• **CPU_Spinning** – This monitor returns a rough measure of Mutex collisions as related to average CPU usage. Ideally, this value should be near zero. A number greater than a fraction of a percent (such as 2.000%) indicates a great deal of Mutex contention.

• **Memory_Ops** – This monitor returns the approximate percentage of Mutex collisions caused by non-mainlock locks. These are primarily memory-related locks, but also include registry locks and other types of locks. This value should be as low as possible.

• **Scheduled_Items_With_Mutex** – This monitor returns the number of non-threadsafe actions that were scheduled to occur at a specific time that were triggered. These items cause greater Mutex contention, as well as reduced scalability and performance relative to the Without Mutex items.

• **Scheduled_Items_Without_Mutex** – This monitor returns the number of threadsafe actions that were scheduled to occur at a specific time that were triggered. A higher value relative to the With Mutex value indicates better server performance.

• **Network_Read_Items** – This monitor returns the number of reads to network sockets that were completed in this RSS interval.

• **Network_Write_Items** – This monitor returns the number of writes to network sockets that were completed in this RSS interval.

**Miscellaneous Statistic**

This component monitor returns information about the internal server state. Returned values are as follows:
- **File_Objects** – This monitor returns the number of internal file objects currently in use. When a server plug-in generates streaming packets for a clip, it opens one or more file objects. The number of open file objects may therefore be twice or more the number of connected media players.

- **Idle(Streams)** – This monitor returns the number of streams that are currently idle. (PPM refers to the server's standard packet delivery system.) Each stream using PPM periodically enters a state where it is ready to send more data to the player, but does not yet have any packets to send. That stream then goes idle, temporarily.

- **Forced_Selects** – This monitor returns the number of times the server had to service a timer-triggered event without having data to read or write.

- **Aggregation_Support** – This monitor returns the number of PPM streams that support packet aggregation.

- **Total(Crash_Avoidances)** – This monitor returns the total number of crash avoidances (CAs) since the last server restart. A CA occurs when the server uses fault-tolerance features to compensate for a problem. For example, if the server encounters corrupt packets in a media file, it attempts to compensate by dropping the corrupt packets and continuing the stream past the corruption point. If it can compensate without terminating the stream, it logs the event as a CA. A small number of CA's is to be expected, and does not indicate a significant problem. A consistently high number of CA's across several RSS periods may indicate serious system problems.

- **Current(Crash_Avoidances)** – This monitor returns the number of crash avoidances (CAs) that have occurred within the current, four-hour window. If it reaches 1,000, the server automatically restarts in an attempt to reset into a more stable state. A CA occurs when the server uses fault-tolerance features to compensate for a problem. For example, if the server encounters corrupt packets in a media file, it attempts to compensate by dropping the corrupt packets and continuing the stream past the corruption point. If it can compensate without terminating the stream, it logs the event as a CA. A small number of CA's is to be expected, and does not indicate a significant problem. A consistently high number of CA's across several RSS periods may indicate serious system problems.

- **Net_Devices** – This monitor returns the number of network connections to the server, other than media player requests, at the time the RSS report was written. This number includes proxy accounting connections, as well as connections to other Helix Servers for content distribution, live stream splitting, and so on.

**Broadcast Reception Statistic**

This component monitor provides statistics about incoming broadcast streams. Returned values are as follows:

- **Feeds** – This monitor returns the number of live feeds coming into the server from encoders or other Helix Server transmitters when the RSS report was written.

- **Total_Bandwidth** – This monitor returns the total amount of bandwidth, in units defined by a script, coming into the server as live streams.

- **Packets** – This monitor returns the total number of live stream packets arriving at the server during this RSS period.
Lost - This monitor returns the total number of packets lost in transit to this server during this RSS period.

Lost_Upstream - This monitor returns the number of live packets reported as lost by upstream transmitters. These packets were lost before the live stream was sent through the network to this receiver.

Resends - This monitor returns the total number of packet resends this receiver requested from encoders or upstream transmitters. The receiver requests a resend of a lost packet only if it determines the packet will arrive in time to be of use in its broadcast stream. In general, the lower the amount of receiver buffering, the fewer resends the receiver requests.

Out_of_Order - This monitor returns the total number of packets for live streams received out of order during this RSS interval.

Duplicate - This monitor returns the total number of duplicate packets received for all live streams during this RSS interval.

Late - This monitor returns the total number of late packets for all live streams received during this RSS interval. The packets may or may not have been too late to be of use in the broadcast.

Broadcast Distribution Statistic

This component monitor provides statistics about streams being split to downstream receivers. This information applies only to downstream Helix Server receivers. Returned values are as follows:

Feeds - This monitor returns the total number of split feeds (both push and pull) being transmitted by this server when the RSS report was published.

Push - This monitor returns the total number of push-split feeds being transmitted by this server. With a push feed, the server sends the stream to a downstream receiver once the stream is available.

Pull - This monitor returns the total number of pull-split feeds being transmitted by this server. With a pull feed, the server does not send the stream to a downstream receiver until the receiver requests it.

Data_Transmitted - This monitor returns the amount of data transmitted by all feeds, in units defined by a script.

Packets - This monitor returns the total number of packets transmitted for the live feeds during this RSS interval.

Resends - This monitor returns the number of resend requests processed by this transmitter. The transmitter will not honor the resend request if the packet was lost upstream, or if it determines that the packet will arrive at the receiver too late to be of use.

Requested - this component returns the number of resends requested by downstream receivers.

Lost_Upstream - This monitor returns the number of live packets lost by upstream transmitters. A value greater than 0 is reported only if this server is not the origin transmitter for the stream.

Dropped - This monitor returns the number of packets dropped by this transmitter. This typically occurs if the packet arrives late from the encoder or upstream transmitter, and the server determines that the packet will subsequently arrive at downstream receivers too late to be of use.
Broadcast Core Statistic

This component monitor provides statistics about streams being split to downstream receivers. This information applies only to downstream Helix Server receivers. Returned values are as follows:

- **Dropped_Packets** – This monitor returns the number of live stream packets dropped in this RSS period by the broadcast core. These packets were queued for another process or thread, but were dropped when the queue for that process or thread overflowed. A significant number of dropped packets indicate a general system overload.

- **Client_Overflows** – This monitor returns the number of live stream packets dropped in this RSS period because the outgoing connection to the receiving client was blocked. Although the server buffers packets to compensate for temporary blockages, it drops the packets if the network blockage does not clear quickly enough.

Main Loop Iterations

This component monitor provides statistics about streams being split to downstream receivers. This information applies only to downstream Helix Server receivers. Returned values are as follows:

- **Main_Loop_Iterations** – This monitor returns the average number of loop iterations for all server processes per second during this RSS period.

- **Load_State** – This monitor returns the server’s current load state: 0–Normal, 1–High, 2–Extreme. The server gauges its internal state using several measurements, including the number of packets written late to the network. During high load states, the server attempts to write large aggregate packets to conserve CPU usage.

Process: rmserver

This component monitor returns the CPU and memory usage of Real Helix Universal Media Server process (rmserver).
**HP-UX**

This template assesses the performance of the HP-UX operating system installed on the target server. Perl scripts are used for monitoring the performance of queries.

The template supports all versions of HP-UX. SolarWinds recommends installing and using the NET-SNMP to monitor. Download and install the NET-SNMP agent on the HP-UX server.

This template was tested on HP-UX B.11.23.

**Prerequisites**

SSH and Perl installed on the target server.

**Credentials**

Root credentials on the target server.

**Port**

Use port 1161 for the template.

**Monitored Components**

- For details on monitors, see [SAM Component Monitor Types](#).

- You need to set thresholds for counters according to your environment. It is recommended to monitor counters for some period of time to understand potential value ranges and then set the thresholds accordingly.

If you have the wrong set of terminal characteristics, you will receive errors that resemble the following:

  Can't modify constant item in scalar assignment at /tmp/APM_1933032963.pl line 1, near ");"
  syntax error at /tmp/APM_1933032963.pl line 4, near "++) "
  syntax error at /tmp/APM_1933032963.pl line 7, near "++) "
  syntax error at /tmp/APM_1933032963.pl line 10, near "}"

  Execution of /tmp/APM_1933032963.pl aborted due to compilation errors.

To resolve this you should add the following line into /etc/profile:

```
stty erase "^H" kill "^U" intr "^C" eof "^D"
```

**CPU statistic (%)**

This monitor returns the percentage of CPU time used. The returned values are as follows:

- **User** – This component returns the percentage of CPU time spent running non-kernel code (user time). This represents the time spent executing user code. This statistic depends on the
programs that the user is running. It is recommended to use the lowest threshold possible.

- **System** – This component returns the percentage of CPU time spent running the system kernel code (system time). It is recommended to use the lowest threshold possible.
- **Idle** – This component returns the percentage of CPU time spent idle. It is recommended to use the highest threshold possible at all times.

System faults statistic/sec

This monitor returns the rate of system faults, per second. The returned values are as follows:

- **Interrupts** – This component returns the number of interrupts per second. The threshold for this component depends on the processor. For modern CPUs, a threshold of 1,500 interrupts/sec is a acceptable. A dramatic increase in this value, without a corresponding increase in system activity, indicates a hardware problem.
- **System Calls** – This component returns the number of system calls per second. This is a measure of how busy the system is handling applications and services. High System Calls/sec indicates high utilization caused by software. With today's faster CPUs, 20,000 would represent a reasonable threshold.
- **Context Switches** – This component returns the number of context switches per second. High activity rates can result from inefficient hardware or poorly designed applications. The normal amount of Context Switches/Sec depends on your servers and applications. The threshold for Context Switches/sec is cumulative for all processors, so you need a minimum of 14,000 per processor (single=14,000, dual=28,000, quad=56,000, and so forth).

Processes statistic

This monitor returns the number of processes in different states. The returned values are as follows:

- **In_Run_Queue** – This component returns the average number of runnable kernel threads over the sampling interval. This should be as low as possible. If the run queue is constantly growing, it may indicate the need for a more powerful CPU or more CPUs. Set the thresholds appropriately for your environment.
- **Waiting_For_resources** – This component returns the average number of kernel threads placed in the VMM wait queue (awaiting resource, awaiting input/output) over the sampling interval. This should be as low as possible. Set the thresholds appropriately for your environment.
- **Swapped** – This component returns the number of runnable or short sleeper (< 20 secs) but swapped processes.

Memory and Swap statistic (MB)

This monitor returns the memory and swap statistic in MB. The returned values are as follows:

- **Free_Memory** – This component returns the amount of available memory in MB. Use the highest threshold possible at all times. Set the thresholds appropriately for your environment.
- **Used_Memory** – This component returns the amount of used memory in MB. Use the lowest threshold possible.
- **Free_Swap** – This component returns the amount of available swap in MB. Use the highest threshold possible at all times. Set the thresholds appropriately for your environment.
• **Used Swap** – This component returns the amount of used swap in MB. Use the lowest threshold possible.

**Paging statistic/sec**

This monitor returns the different paging statistics. The returned values are as follows:

- **Address_Translation_Faults** – This component shows the number of page address translation faults per second (valid page not in memory). Use the lowest threshold possible.
- **Paged_In** – This component returns the rate of pages "paged in" from paging space in kB, per second. The operation of reading one inactive page or a cluster of inactive memory pages from the disk is called a "page in." Use the lowest threshold possible.
- **Paged_Out** – This component returns the rate of pages "paged out" from paging space in kB, per second. The operation of writing one inactive page or a cluster of inactive memory pages to the disk is called a "page out." Use the lowest threshold possible. Values above 20 pages (80 kB), or so, indicate a significant performance problem. In this situation, more memory should be installed.

**Processes in different states**

This monitor returns the different paging statistics. The returned values are as follows:

- **Sleeping** – This component returns the number of processes that are waiting for an event to complete.
- **Runnable** – This component returns the number of processes that are on run queue.
- **Zombie** – This component returns the number of processes that are terminated and where the parent is not waiting. This should always be zero. If it is not zero, you should manually kill zombie processes. Use the following commands to see these zombie processes: `ps -el | grep "Z"`
- **Stopped** – This component returns the amount of processes that are stopped, either by a job control signal or because it is being traced.

**Space on root (/) partition (MB)**

This monitor returns the available and used space of the root (/) partition in MB. The returned values are as follows:

- **Available_Space** – This component returns the available space on the root (/) partition in MB. Use the highest threshold possible at all times.
- **Used_Space** – This component returns the used space on the root (/) partition in MB.

**Using percentage of active system devices**

This monitor returns the name of the active system device and the percentage of time the device was busy servicing a transfer request.

**Disk operations/sec of active system devices**

This monitor returns the name of the active system device and its read/write transfers to or from the device.
**Top 10 active processes**

This monitor returns the top 10 active processes and share of CPU usage in percent.
HTTP

The following templates are available:

- HTTP template
- HTTP Form Login template
- HTTPS Monitor template
HTTP template

This template tests the ability of a web server to respond to HTTP requests.

**Prerequisites**

None.

**Credentials**

None.

Monitored Components

For details on monitors, see [SAM Component Monitor Types](#).

**HTTP Monitor**

This component monitor tests a web server's ability to accept incoming sessions and transmit the requested page. The component monitor can optionally search the delivered page for specific text strings and pass or fail the test based on that search.

The HTTP Monitor measures the time it takes the HTTP “get” for the page referenced in the component monitor to load. This response time is measured in milliseconds.

If a web page redirects to another page, the response time measures the entire time from the original request until the last redirected page is loaded.

This monitor supports the following additional macros:

- `${Node.SysName}`
- `${Node.Caption}`
- `${Node.DNS}`
- `${Node.ID}`
**HTTPS Monitor template**

This template tests a web server's ability to accept incoming sessions over a secure channel and then transmit the requested page.

**Prerequisites**

WMI access on target server.

**Credentials**

Administrator on target server.

**Monitored Components**

[Information] For details on monitors, see [SAM Component Monitor Types](#).

**Directory Size Monitor**

This component monitor tests a web server's ability to accept incoming sessions over a secure channel and then transmit the requested page. The component monitor can also test the security certificate.

Before using this template, you must provide the correct Url and Port Number options. By default, the SolarWinds SAM variables contained in the default value for the Url field attempt to monitor a web site at the IP address of the assigned node \${IP} and on the port specified in the Port Number field \${PORT}. By default, the Port Number is set to 443. If you are using a proxy, you must put the correct proxy information in for this monitor.
HTTP Form Login template

This template tests the ability of a web server to serve web pages secured behind a forms-based login page.

Prerequisites

None.

Credentials

A valid user name and password for the forms-based login page.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

HTTP Form Login Monitor

This component monitor tests the ability of a web server to serve web pages secured behind a forms-based login page. The test is performed by using the credential as the user name and password for the login form, retrieving the page behind the login form, and then searching the retrieved page for keywords that indicate either a successful or a failed login attempt.

The HTTP Form Login Monitor does not work on any login screens that are pop up.
IBM

The following templates are available:

- IBM DB2
- IBM DB2 HADR Health
- IBM Informix
- IBM WebSphere (JMX)
IBM DB2

This template assesses the performance of an IBM DB2 database by retrieving performance data from the built-in SYSIBMADM tables.

This template is compatible with the Orion Agent for Linux.

Prerequisites

- IBM DB2 9.7 or later installed on the target server
- Install IBM DB2 ODBC Driver (© 2018 IBM Corp.; https://www-01.ibm.com; link acquired on August 2, 2018) on AIX devices
- Access to SYSIBMADM tables in the IBM DB2 database

Credentials

- Database user name and password.

Database preparation

To prepare the IBM DB2 database server for the template:

1. Execute the following commands in the Command Editor before using this template:
   
   ```
   UPDATE DBM CFG USING DFT_MON_BUFPOOL ON
   UPDATE DBM CFG USING DFT_MON_LOCK ON
   UPDATE DBM CFG USING DFT_MON_STMT ON
   UPDATE DBM CFG USING DFT_MON_UOW on
   ```

2. Use the GRANT EXECUTE ON FUNCTION statement to grant privileges for the SYSPROC.MON_GET_TABLE function to `user`, where `user` is the username that SAM will utilize to monitor the IBM DB2 database, as shown in this example:

   ```
   GRANT EXECUTE ON FUNCTION SYSPROC.MON_GET_TABLE TO user
   ```

3. Restart the database server.

Configuration for Orion agent for Linux monitoring

Here are prerequisites for the following steps:

- IBM DB2 is installed on a Linux-based computer.
- A user account exists on the server and in the IBM DB2 database.

To run commands, you will need the instance users for the database. The instance user connects to the DB and should have the sqlib directory set up.

1. Log into the Linux-based computer with administrator privileges.
2. Use the following command to install the unixODBC package:
yum -y install unixODBC

3. **Update the ODBC config files by adding the following settings to /etc/odbcinst.ini:**

   [DB2]
   Description = DB2 Driver
   Driver = /opt/ibm/db2/V10.5/lib64/libdb2.so
   FileUsage = 1
   DontDLClose = 1

   ![i] Verify that libdb2.so has the correct file path.

4. **Add the following settings to /etc/odbc.ini:**

   [dbname]
   Driver = DB2

   ![i] The drivers should match in both files.

5. **Connect locally to the database with the instance user credentials. For example:**

   isql -v dbname db2inst1 Password1

6. **Log into the DB2 database with the instance user credentials and open the DB2 command line tool.**

7. **Enable the required following setting used by the SAM IBM DB2 template:**

   UPDATE DBM CFG USING DFT_MON_BUFPOOL ON
   UPDATE DBM CFG USING DFT_MON_LOCK ON
   UPDATE DBM CFG USING DFT_MON_STMT ON
   UPDATE DBM CFG USING DFT_MON_UOW on

8. **Use the GRANT EXECUTE ON FUNCTION statement to grant privileges for the SYSPROC.MON_GET_TABLE function to user, where user is the username that SAM as shown in this example:**

   GRANT EXECUTE ON FUNCTION SYSPROC.MON_GET_TABLE TO user
Configure DB2 on AIX devices

Prerequisites

Important: Do not install the 64-bit ODBC drivers; use the 32-bit drivers instead to support Python distributed on the Orion agent.

- Install IBM DB2 ODBC Driver (© 2018 IBM Corp.; https://www-01.ibm.com; link acquired on August 2, 2018) on AIX devices. The commands use the following driver bundle: v11.1.1fp1_aix64_odbc_cli_32.tar.gz.
- Install the ODBC driver manager package and its dependencies from www.perzl.org/aix (Obtained from www.perzl.org/aix, on February 1, 2018). Dependencies include:
  - info-6.4-1.aix5.1.ppc.rpm
  - libiconv-1.15-1.aix5.1.ppc.rpm
  - libtool-ltdl-1.5.26-2.aix5.1.ppc.rpm
  - readline-7.0-3.aix5.1.ppc.rpm
  - libffi-3.1.1.aix5.1.ppc.rpm (not a direct dependency, but needed by the SAM monitor plugin)
- The gunzip utility, which is part of the AIX 5L™ default installation setup. You can also download gzip for AIX 5L from http://www.ibm.com/servers/aix/products/aixos/linux/rpmgroups.html (© 2018 IBM Corp.; https://www-01.ibm.com; link acquired on August 2, 2018)
- Verify that the IBM rpm.rte package exists in the /usr/bin/rpm directory

Configure ODBC for AIX

1. Log into the AIX-based computer with administrator privileges.
2. Install the RPM packages.
   
   Run the following command as root: rpm -ivh unixODBC-2.3.4-1.aix5.1.ppc.rpm

   ! To install all dependencies, run the following command that expects the dependencies are in the same directory:.
   
   rpm -ivh *.rpm

3. Install the DB2 ODBC driver. The example code creates a directory odbc_cli_32 in the /opt directory.
   
   gunzip v11.1.1fp1_aix64_odbc_cli_32.tar.gz
   tar -x -f v11.1.1fp1_aix64_odbc_cli_32.tar -C /opt

4. Add the following lines to /opt/freeware/etc/odbcinst.ini:
   
   [DB2]
   Description = DB2 Driver
   Driver = /opt/odbc_cli_32/clidriver/lib/libdb2.so
   FileUsage = 1
DontDLClose = 1

Verify libdb2 has the correct file path.

5. Add the following settings to /opt/freeware/etc/odbc.ini:

   [dbname]
   Description = IBM DB2 ODBC data source
   Driver = DB2
   DMEnvAttr = SQL_ATTR_UNIXODBC_ENVATTR="/opt/odbc_cli_32/clidriver"

   • In [dbname], enter the name of the database to be monitored.
   • DMEnvAttr value depends on the installation directory for the DB2 ODBC CLI driver.

6. Run the following command as root. It allows the unixODBC manager driver to find the DB2 ODBC file.

   ar -X32 x libdb2.a shr.o
   mv shr.o libdb2.so

7. Verify that the SAM python plugin can connect to the DB2 database to monitor it. Save the following script as verifyodbc.py. The script is written for Orion agents in the default location /opt/SolarWinds/Agent.

   **Important:** If you are not using the default port, add server hostname and port number to the connection string.

   ```python
   import sys
   sys.path.insert(0, "/opt/SolarWinds/Agent/bin/Plugins/SharedPythonLibs")
   import pypyodbc

   # Set Database, Uid, and Pwd to the database name, username, and user's password to access said database respectively.
   # In this example, database name, username, and the user's password are TEST, db2inst1, and Password1 respectively.

   conn_str = 'Driver=
{DB2};Database=TEST;Uid=db2inst1;Pwd=Password1;'

   You can also use the following script to verify that the SAM python plugin can connect to the DB2 database:
conn = pypyodbc.connect(conn_str, ansi=True)
        conn.close()
    except Exception, ex:
        print ex
        print "Failure"

8. Run the script using the following command:
   /opt/SolarWinds/Agent/bin/python2 verifyodbc.py

9. SolarWinds recommends that you configure the utilities bundled in the DB2 ODBC CLI bundle. Create the db2cli.ini configuration file in /opt/odbc_cli_32/clidriver/cfg/db2cli.ini:

   **Replace TEST with your database name.**

   ```
   TEST
   Database=TEST
dbalias=TEST
   Protocol=TCPIP
   Hostname=127.0.0.1
   ServiceName=50000
   ```

   Configure and assign the SAM IBM DB2 template to your Linux/Unix-based computer with the instance user credentials.

   1. In the Orion Web Console, click Settings > All Settings > SAM Settings > Manage Templates.
   2. Search for a IBM DB2 template. SolarWinds recommends creating a copy of the template. Select a template based on version and click Copy.
   3. Modify the settings of the template and component monitors based on the metrics you want to monitor.
   4. To enter credentials, select the component monitor check boxes and click Assign Credentials.
   5. Enter the credentials for the instance user account and click OK.
   6. Modify the connection strings for monitors to match your DB. Use one of the following methods:
      - Specify the actual DB and driver:
        ```
        Driver={DB2};Database=TESTDB;Hostname=${IP};Port=50000;Protocol=TCPIP;
        Uid=${USER};Pwd=${PASSWORD};
        ```
      - Specify the existing data source in odbc.ini:
        ```
        DSN=testdb;Uid=${USER};Pwd=${PASSWORD};
        ```

**Monitored Components**

   For details on monitors, see [SAM Component Monitor Types](#).
Components without predetermined threshold values provide guidance such as "Use the lowest threshold possible" or "Use the highest threshold possible" to help you find a threshold appropriate for your application.

**Database Used Space (MB)**

This component monitor returns the used space, in MB, of the current database.

By default, this monitor returns a value for the database named, SAMPLE. To change the database, find the following parameter in the ODBC driver string and replace SAMPLE with your database name:

```
Database=SAMPLE;
```

**Log File Used Space in Specified Database (MB)**

This component monitor returns the used space, in MB, of the log file in the specified database.

By default, this monitor returns a value for the database named, SAMPLE. To change the database, replace SAMPLE with your database name in the following SQL query:

```
WHERE DB_NAME = 'SAMPLE'
```

**Log File Free Space in Specified Database (MB)**

This component monitor returns the free space, in MB, of the log file in the specified database.

By default, this monitor returns the value for the database named, SAMPLE. To change the database, replace SAMPLE with your database name in the following SQL query:

```
WHERE DB_NAME = 'SAMPLE'
```

**Average Buffer Total Hit Ratio (%)**

This component monitor returns the average Total Hit Ratio (index, XDA, and data reads) for all buffers. To see the Hit Ratio for all buffers, you should manually execute the following SQL command:

```
SELECT * FROM SYSIBMADM.BP_HITRATIO
```

If you want to see the Hit Ratio for a specific buffer, you can use the following SQL construction:

```
SELECT REAL(AVG(TOTAL_HIT_RATIO_PERCENT))
FROM SYSIBMADM.BP_HITRATIO
WHERE BP_NAME = 'IBMDEFAULTBP'
```

The returned value should be as high as possible.
Average Data Hit Ratio (%)

This component monitor returns the average Data Hit Ratio for all buffers. To see the Hit Ratio for all buffers, you should manually execute the following SQL command:

```
SELECT * FROM SYSIBMADM.BP_HITRATIO
```

If you want to see the Hit Ratio for a specific buffer, you can use the following SQL construction:

```
SELECT REAL(AVG(DATA_HIT_RATIO_PERCENT))
FROM SYSIBMADM.BP_HITRATIO
WHERE BP_NAME = 'IBMDEFAULTBP'
```

The returned value should be as high as possible.

Average Index Hit Ratio (%)

This component monitor returns the average Index Hit Ratio for all buffers. To see the Hit Ratio for all buffers, you should manually execute the following SQL command:

```
SELECT * FROM SYSIBMADM.BP_HITRATIO
```

If you want to see the Hit Ratio for a specific buffer, you can use the following SQL construction:

```
SELECT REAL(AVG(INDEX_HIT_RATIO_PERCENT))
FROM SYSIBMADM.BP_HITRATIO
WHERE BP_NAME = 'IBMDEFAULTBP'
```

The returned value should be as high as possible.

Number of Locks Held in Specified Database

This component monitor returns the number of Locks currently held in the specified database.

By default, this monitor returns the value for the database named, SAMPLE. To change the database, replace SAMPLE with your database name in the following SQL query:

```
WHERE DB_NAME = 'SAMPLE'
```

The returned value should be as low as possible.

Average Read Time (ms)

This component monitor returns the average read time from the database in milliseconds. The returned value should be as low as possible.

Connected applications to Specified Database

This component monitor returns the number of connected applications to the specified database.

By default, this monitor returns the value for the database named, SAMPLE. To change the database, replace SAMPLE with your database name in the following SQL query:

```
WHERE DB_NAME = 'SAMPLE'
```
**Number of Long Running Queries**

This component monitor returns the number of Long Running Queries. You should set the threshold according to your environment.

**Number of Table Scans**

This component monitor returns the number of table scans currently in progress in the specified database.

**Table with the Biggest Table Scans Value**

This component monitor returns the table name with the Biggest Value of Table Scans and the value itself.

**Used Space of the Biggest Table (MB)**

This component monitor returns the name of the Biggest Table and its size, in MB.
IBM DB2 HADR Health

This template assesses the performance of an IBM DB2 HADR health by retrieving data from the built-in SNAPHADR view.

This template was tested on IBM DB2 v 9.7.

Prerequisites

IBM DB2 installed on the target server. IBM DB2 ODBC Driver. This driver can be found on the IBM DB2 installation media.

You should give SELECT or CONTROL privileges to the user on the SNAPHADR administrative view and the EXECUTE privilege on the SNAP_GET_HADR table function.

Credentials

Database user name and password.

Configuration for Orion agent for Linux monitoring

Here are prerequisites for the following steps:

- IBM DB2 is installed on a Linux-based computer.
- A user account exists on the server and in the IBM DB2 database.

To run commands, you will need the instance users for the database. The instance user connects to the DB and should have the sqllib directory set up.

1. Log into the Linux-based computer with administrator privileges.
2. Use the following command to install the unixODBC package:
   ```
   yum -y install unixODBC
   ```
3. Update the ODBC config files by adding the following settings to /etc/odbcinst.ini:
   ```
   [DB2]
   Description = DB2 Driver
   Driver = /opt/ibm/db2/V10.5/lib64/libdb2.so
   FileUsage = 1
   DontDLClose = 1
   ```
   - Verify that libdb2.so has the correct file path.
4. Add the following settings to /etc/odbc.ini:
   ```
   [dbname]
   Driver = DB2
   ```
   - The drivers should match in both files.
5. Connect locally to the database with the instance user credentials. For example:
   ```
   isql -v dbname db2inst1 Password1
   ```
6. Log into the DB2 database with the instance user credentials and open the DB2 command line tool.

7. Enable the required following setting used by the SAM IBM DB2 template:
   
   ```sql
   UPDATE DBM CFG USING DFT_MON_BUFPOOL ON
   UPDATE DBM CFG USING DFT_MON_LOCK ON
   UPDATE DBM CFG USING DFT_MON_STMT ON
   UPDATE DBM CFG USING DFT_MON_UOW on
   ```

8. Use the GRANT EXECUTE ON FUNCTION statement to grant privileges for the SYSPROC.MON_GET_TABLE function to user, where user is the username that SAM as shown in this example:
   
   ```sql
   GRANT EXECUTE ON FUNCTION SYSPROC.MON_GET_TABLE TO user
   ```
Configure DB2 on AIX devices

Prerequisites

Important: Do not install the 64-bit ODBC drivers; use the 32-bit drivers instead to support Python distributed on the Orion agent.

- Install IBM DB2 ODBC Driver (© 2018 IBM Corp.; https://www-01.ibm.com; link acquired on August 2, 2018) on AIX devices. The commands use the following driver bundle: v11.1.1fp1_aix64_odbc_cli_32.tar.gz.
- Install the ODBC driver manager package and its dependencies from www.perzl.org/aix (Obtained from www.perzl.org/aix, on February 1, 2018). Dependencies include:
  - info-6.4-1.aix5.1.ppc.rpm
  - libiconv-1.15-1.aix5.1.ppc.rpm
  - libtool-ltdl-1.5.26-2.aix5.1.ppc.rpm
  - readline-7.0-3.aix5.1.ppc.rpm
  - libffi-3.1.1.aix5.1.ppc.rpm (not a direct dependency, but needed by the SAM monitor plugin)
- The gunzip utility, which is part of the AIX 5L™ default installation setup. You can also download gzip for AIX 5L from http://www.ibm.com/servers/aix/products/aixos/linux/rpmgroups.html (© 2018 IBM Corp.; https://www-01.ibm.com; link acquired on August 2, 2018)
- Verify that the IBM rpm.rte package exists in the /usr/bin/rpm directory

Configure ODBC for AIX

1. Log into the AIX-based computer with administrator privileges.
2. Install the RPM packages.
   Run the following command as root: rpm -ivh unixODBC-2.3.4-1.aix5.1.ppc.rpm

   To install all dependencies, run the following command that expects the dependencies are in the same directory:
   rpm -ivh *.rpm

3. Install the DB2 ODBC driver. The example code creates a directory odbc_cli_32 in the /opt directory.
   gunzip v11.1.1fp1_aix64_odbc_cli_32.tar.gz
   tar -x -f v11.1.1fp1_aix64_odbc_cli_32.tar -C /opt

4. Add the following lines to /opt/freeware/etc/odbcinst.ini:
   [DB2]
   Description = DB2 Driver
   Driver = /opt/odbc_cli_32/clidriver/lib/libdb2.so
   FileUsage = 1
DontDLClose = 1

Verify libdb2 has the correct file path.

5. **Add the following settings to** `/opt/freeware/etc/odbc.ini`:

   ```ini
   [dbname]
   Description = IBM DB2 ODBC data source
   Driver = DB2
   DMEnvAttr = SQL_ATTR_UNIXODBC_ENVATTR=/opt/odbc_cli_32/clidriver
   ```

   - In [dbname], enter the name of the database to be monitored.
   - DMEnvAttr value depends on the installation directory for the DB2 ODBC CLI driver.

6. Run the following command as root. It allows the unixODBC manager driver to find the DB2 ODBC file.

   ```bash
   ar -X32 x libdb2.a shr.o
   mv shr.o libdb2.so
   ```

7. **Verify that the SAM python plugin can connect to the DB2 database to monitor it. Save the following script as verifyodbc.py. The script is written for Orion agents in the default location `/opt/SolarWinds/Agent`.**

   **Important:** If you are not using the default port, add server hostname and port number to the connection string.

   ```python
   import sys
   sys.path.insert(0, "/opt/SolarWinds/Agent/bin/Plugins/SharedPythonLibs")
   import pypyodbc
   
   # Set Database, Uid, and Pwd to the database name, username, and user's password to access said database respectively.
   # In this example, database name, username, and the user's password are TEST, db2inst1, and Password1 respectively.

   conn_str = 'Driver= {DB2};Database=TEST;Uid=db2inst1;Pwd=Password1;'
   ```

   You can also use the following script to verify that the SAM python plugin can connect to the DB2 database:
conn = pypyodbc.connect(conn_str, ansi=True)
conn.close()
except Exception, ex:
    print ex
    print "Failure"

8. Run the script using the following command:
   /opt/SolarWinds/Agent/bin/python2 verifyodbc.py

9. SolarWinds recommends that you configure the utilities bundled in the DB2 ODBC CLI bundle. Create the db2cli.ini configuration file in /opt/odbc_cli_32/clidriver/cfg/db2cli.ini:

   Replace TEST with your database name.

   TEST
   Database=TEST
dbalias=TEST
   Protocol=TCPIP
   Hostname=127.0.0.1
   ServiceName=50000

Configure and assign the SAM IBM DB2 template to your Linux/Unix-based computer with the instance user credentials.

1. In the Orion Web Console, click Settings > All Settings > SAM Settings > Manage Templates.
2. Search for a IBM DB2 template. SolarWinds recommends creating a copy of the template. Select a template based on version and click Copy.
3. Modify the settings of the template and component monitors based on the metrics you want to monitor.
4. To enter credentials, select the component monitor check boxes and click Assign Credentials.
5. Enter the credentials for the instance user account and click OK.
6. Modify the connection strings for monitors to match your DB. Use one of the following methods:
   - Specify the actual DB and driver:
     Driver={DB2};Database=TESTDB;Hostname=${IP};Port=50000;Protocol=TCPIP
     ;Uid=${USER};Pwd=${PASSWORD};
   - Specify the existing data source in odbc.ini:
     DSN=testdb;Uid=${USER};Pwd=${PASSWORD};

Monitored Components

For details on monitors, see SAM Component Monitor Types.
Components without predetermined threshold values provide guidance such as "Use the lowest threshold possible" or "Use the highest threshold possible" to help you find a threshold appropriate for your application.

If some or all components return nothing, it may indicate that the database is currently unavailable or it is not an HADR database. You should check your database configuration.

**HADR Role**

This component monitor returns the current HADR role of the target database.

Possible values:

- 1 – Database is not an HADR database.
- 2 – Database is the primary HADR database.
- 3 – Database is the standby HADR database.

By default, this monitor returns a value for the database named, TEST2. To change the database, replace TEST2 with your database name in the following SQL query: `WHERE DB_NAME = 'TEST2'`

**HADR Connect Status**

This component monitor returns the current HADR connect status of the target database.

Possible values:

- 1 – The database is connected to its partner node.
- 2 – The database is connected to its partner node, but the connection is congested. A connection is congested when the TCP/IP socket connection between the primary-standby pair is still alive, but one end cannot send to the other end.
- 3 – The database is not connected to its partner node.

By default, this monitor returns a value for the database named, TEST2. To change the database, replace TEST2 with your database name in the following SQL query: `WHERE DB_NAME = 'TEST2'`

**HADR Heartbeat**

This component monitor returns the number of missed heartbeats on the HADR connection. If the database is in HADR primary or standby role, this element indicates the health of the HADR connection. A heartbeat is a message sent from the other HADR database at regular intervals. If the value for this element is zero, no heartbeats have been missed and the connection is healthy. The higher the value, the worse the condition of the connection.

By default, this monitor returns a value for the database named, TEST2. To change the database, replace TEST2 with your database name in the following SQL query: `WHERE DB_NAME = 'TEST2'`
HADR Log Gap

This component monitor returns the running average of the gap between the primary Log sequence number (LSN) and the standby log LSN. The gap is measured in number of bytes. When a log file is truncated, the LSN in the next log file starts as if the last file were not truncated. This LSN hole does not contain any log data. Such holes can cause the log gap not to reflect the actual log difference between the primary and the standby.

By default, this monitor returns a value for the database named, TEST2. To change the database, replace TEST2 with your database name in the following SQL query: WHERE DB_NAME = 'TEST2'

HADR State

This component monitor returns the current HADR state of the target database.

Possible values:

- 1 – The primary and standby databases are connected and are in peer state.
- 2 – The database is doing local catch-up.
- 3 – The database is doing remote catch-up.
- 4 – The database is waiting to connect to its partner to do remote catch-up.
- 5 and 6 – The database is not connected to its partner database.

By default, this monitor returns a value for the database named, TEST2. To change the database, replace TEST2 with your database name in the following SQL query: WHERE DB_NAME = 'TEST2'

HADR Sync Mode

This component monitor returns the current HADR sync mode of the target database.

Possible values:

- 1 – The databases uses sync mode.
- 2 – The databases uses near sync mode.
- 3 – The databases uses async mode.
- 4 – The databases uses super async mode.

More information about sync modes can be found here:

By default, this monitor returns a value for the database named, TEST2. To change the database, replace TEST2 with your database name in the following SQL query: WHERE DB_NAME = 'TEST2'
**IBM Informix**

This template assesses the performance of an IBM Informix database by retrieving performance data from the built-in system monitoring interface (SMI) tables located in the sysmaster database.

**Prerequisites**

IBM Informix 11.70 installed on the target server. IBM Informix ODBC driver installed on the APM server. The driver can be found in the IBM Informix Client SDK on the IBM site. Your database should be accessible by using the olsoctcp protocol.

By default, all components use the following ODBC connection string:

```
>Driver={IBM INFORMIX ODBC DRIVER};Host=${IP};Server=ol_informix1170;Service=ol_informix1170;Protocol=olsoctcp;Database=sysmaster;Uid=${USER};Pwd=${PASSWORD};
```

Adjust this string to suit your environment by updating the Server and Service fields.

**Credentials**

Database user name and password.

**Minimum Permissions**

You should create an OS user (for example: monuser) and add this user into “Informix” group. This is default Informix installation user group. The following highlighted instructions can be found at: [http://pic.dhe.ibm.com/infocenter/idshelp/v115/index.jsp?topic=%2Fcom.ibm.igul.doc%2Fids_in_005x.htm](http://pic.dhe.ibm.com/infocenter/idshelp/v115/index.jsp?topic=%2Fcom.ibm.igul.doc%2Fids_in_005x.htm).

Creating the group informix and user informix

Typically the installation application creates these required objects, but you may need to create them before installing. The Mac OS X installation application automatically creates group and user informix in all circumstances, so this task does not apply to Mac computers.

You need to create the objects before you run the installation application in the following situations:

- You want to specify a particular identifier (ID) number.
- The group informix exists on the system; however, the user informix does not. In this case, you need to create the user only.

If you plan to install IBM® Informix® products using RPM Package Manager (RPM) and user informix and group informix do not exist on the target computer, you must create these objects on the operating system before performing the RPM-based installation.

To create the group informix and user informix:
1. Create the group informix by using the `groupadd` utility followed by the name of the group, in this format: `groupadd n informix` where `n` is an unused identifier (ID) greater than 100. On AIX®, use the `mkgroup` command instead of `groupadd`.

2. Create the user informix by using the `useradd` utility followed by the group (informix) and user name (informix) in this format: `useradd -u n -g informix informix` where `n` is an unused identifier (ID) greater than 100.

   **Important:** Only add users to the group informix if the users need administrative access to the database server.

3. Create a password for user informix by running the `passwd` utility.

4. Once complete, you should login as a DBA (informix user) to “sysmaster” database on your Informix instance (For example: `ol_informix1170`).

5. Under DBA user, you should create stored procedures described in the “For IBM Informix installed on Linux” section below and grant execute permissions on these procedures to the “monuser” by using the following SQL query: `GRANT EXECUTE ON procedure_name TO monuser;`

6. Edit `/etc/sqlhosts` and `/etc/services`. This step is described in the “For IBM Informix installed on Linux” below.

7. Correct the Server and Service properties in the ODBC connection string. Adjust the “Platform to run polling job on” option as needed.

**For IBM Informix installed on Windows**

The following commands should be executed on the IBM Informix server before using this template. These commands will create all the necessary stored procedures for monitoring your server from SAM:

```
--Page Reads /sec
CREATE PROCEDURE APM_P_READS ()
RETURNING DECIMAL(8,2);
DEFINE x,y,res DECIMAL(8,2);
SELECT value INTO x FROM sysprofile WHERE name = 'pagreads';
SYSTEM "timeout 10";
SELECT value INTO y FROM sysprofile WHERE name = 'pagreads';
LET res = (y - x) / 10;
RETURN res;
END PROCEDURE;

--Page Writes /sec
CREATE PROCEDURE APM_P_WRITES ()
RETURNING DECIMAL(8,2);
DEFINE x,y,res DECIMAL(8,2);
SELECT value INTO x FROM sysprofile WHERE name = 'pagwrites';
SYSTEM "timeout 10";
```
SELECT value INTO y FROM sysprofile WHERE name = 'pagwrites';
LET res = (y - x) / 10;
RETURN res;
END PROCEDURE;

--Committed Transactions /sec
CREATE PROCEDURE APM_TR_COM ()
RETURNING DECIMAL(8,2);
DEFINE x,y,res DECIMAL(8,2);
SELECT value INTO x FROM sysprofile WHERE name = 'iscommits';
SYSTEM "timeout 10";
SELECT value INTO y FROM sysprofile WHERE name = 'iscommits';
LET res = (y - x) / 10;
RETURN res;
END PROCEDURE;

--Rolled back Transactions /sec
CREATE PROCEDURE APM_TR_ROL ()
RETURNING DECIMAL(8,2);
DEFINE x,y,res DECIMAL(8,2);
SELECT value INTO x FROM sysprofile WHERE name = 'isrollbacks';
SYSTEM "timeout 10";
SELECT value INTO y FROM sysprofile WHERE name = 'isrollbacks';
LET res = (y - x) / 10;
RETURN res;
END PROCEDURE;

--Latch Request Waits /sec
CREATE PROCEDURE APM_LATCH_WAIT ()
RETURNING DECIMAL(8,2);
DEFINE x,y,res DECIMAL(8,2);
SELECT value INTO x FROM sysprofile WHERE name = 'latchwts';
SYSTEM "timeout 10";
SELECT value INTO y FROM sysprofile WHERE name = 'latchwts';
LET res = (y - x) / 10;
RETURN res;
END PROCEDURE;

--Lock Requests /sec
CREATE PROCEDURE APM_L_REQ ()
RETURNING DECIMAL(8,2);
DEFINE x,y,res DECIMAL(8,2);
SELECT value INTO x FROM sysprofile WHERE name = 'lockreqs';
SYSTEM "timeout 10";
SELECT value INTO y FROM sysprofile WHERE name = 'lockreqs';
LET res = (y - x) / 10;
RETURN res;
END PROCEDURE;

--Lock Waits /sec
CREATE PROCEDURE APM_L_WAIT ()
RETURNING DECIMAL(8,2);
DEFINE x,y, res DECIMAL(8,2);
SELECT value INTO x FROM sysprofile WHERE name = 'lockwts';
SYSTEM "timeout 10";
SELECT value INTO y FROM sysprofile WHERE name = 'lockwts';
LET res = (y - x) / 10;
RETURN res;
END PROCEDURE;

--Deadlocks /sec
CREATE PROCEDURE APM_DEADL ()
RETURNING DECIMAL(8,2);
DEFINE x,y, res DECIMAL(8,2);
SELECT value INTO x FROM sysprofile WHERE name = 'deadlks';
SYSTEM "timeout 10";
SELECT value INTO y FROM sysprofile WHERE name = 'deadlks';
LET res = (y - x) / 10;
RETURN res;
END PROCEDURE;

--Sequential Scans /sec
CREATE PROCEDURE APM_SEQ_S ()
RETURNING DECIMAL(8,2);
DEFINE x,y, res DECIMAL(8,2);
SELECT value INTO x FROM sysprofile WHERE name = 'seqscans';
SYSTEM "timeout 10";
SELECT value INTO y FROM sysprofile WHERE name = 'seqscans';
LET res = (y - x) / 10;
RETURN res;
END PROCEDURE;

--Sorts /sec
CREATE PROCEDURE APM_SORTS ()
RETURNING DECIMAL(8,2);
DEFINE x,y, res DECIMAL(8,2);
SELECT value INTO x FROM sysprofile WHERE name = 'totalsorts';
SYSTEM "timeout 10";
SELECT value INTO y FROM sysprofile WHERE name = 'totalsorts';
LET res = (y - x) / 10;
RETURN res;
END PROCEDURE;

--Number of Network Connections /sec
CREATE PROCEDURE APM_CONNECT ()
RETURNING DECIMAL(8,2);
DEFINE x,y,res DECIMAL(8,2);
SELECT ng_connects INTO x FROM sysnetglobal;
SYSTEM "timeout 10";
SELECT ng_connects INTO y FROM sysnetglobal;
LET res = (y - x) / 10;
RETURN res;
END PROCEDURE;

1. On the IBM Informix server, open the setnet32 utility found in the IBM Informix folder. Select the Host Information tab and add the following:
   - Current Host: APM-server
   - User Name: your_username (e.g.: Informix)
   - Password Option: Password
   - Password: username_password

2. Open C:\Windows\System32\drivers\etc\services and add the following line: service_name 1528/tcp #INFORMIX where service_name is name of your Informix instance (for example: ol_informix1170).

3. Add a firewall rule for tcp port 1528.

For IBM Informix installed on Linux

Execute the following SQL commands:

```
--Page Reads /sec
CREATE PROCEDURE APM_P_READS ()
RETURNING DECIMAL(8,2);
DEFINE x,y,res DECIMAL(8,2);
SELECT value INTO x FROM sysprofile WHERE name = 'pagreads';
SYSTEM "sleep 10";
SELECT value INTO y FROM sysprofile WHERE name = 'pagreads';
LET res = (y - x) / 10;
RETURN res;
END PROCEDURE;
```

The only difference between the prior SQL commands and the following SQL commands is that the string SYSTEM "timeout 10"; has been changed to SYSTEM "sleep 10"; multiple times throughout.
-- Page Writes /sec
CREATE PROCEDURE APM_P_WRITES ()
RETURNING DECIMAL(8,2);
DEFINE x,y,res DECIMAL(8,2);
SELECT value INTO x FROM sysprofile WHERE name = 'pagwrites';
SYSTEM "sleep 10";
SELECT value INTO y FROM sysprofile WHERE name = 'pagwrites';
LET res = (y - x) / 10;
RETURN res;
END PROCEDURE;

-- Committed Transactions /sec
CREATE PROCEDURE APM_TR_COM ()
RETURNING DECIMAL(8,2);
DEFINE x,y,res DECIMAL(8,2);
SELECT value INTO x FROM sysprofile WHERE name = 'iscommits';
SYSTEM "sleep 10";
SELECT value INTO y FROM sysprofile WHERE name = 'iscommits';
LET res = (y - x) / 10;
RETURN res;
END PROCEDURE;

-- Rolled back Transactions /sec
CREATE PROCEDURE APM_TR_ROL ()
RETURNING DECIMAL(8,2);
DEFINE x,y,res DECIMAL(8,2);
SELECT value INTO x FROM sysprofile WHERE name = 'isrollbacks';
SYSTEM "sleep 10";
SELECT value INTO y FROM sysprofile WHERE name = 'isrollbacks';
LET res = (y - x) / 10;
RETURN res;
END PROCEDURE;

-- Latch Request Waits /sec
CREATE PROCEDURE APM_LATCH_WAIT ()
RETURNING DECIMAL(8,2);
DEFINE x,y,res DECIMAL(8,2);
SELECT value INTO x FROM sysprofile WHERE name = 'latchwts';
SYSTEM "sleep 10";
SELECT value INTO y FROM sysprofile WHERE name = 'latchwts';
LET res = (y - x) / 10;
RETURN res;
END PROCEDURE;

-- Lock Requests /sec
CREATE PROCEDURE APM_L_REQ()
RETURNING DECIMAL(8,2);
DEFINE x,y,res DECIMAL(8,2);
SELECT value INTO x FROM sysprofile WHERE name = 'lockreqs';
SYSTEM "sleep 10";
SELECT value INTO y FROM sysprofile WHERE name = 'lockreqs';
LET res = (y - x) / 10;
RETURN res;
END Procedure;

--Lock Waits /sec
CREATE PROCEDURE APM_L_WAIT()
RETURNING DECIMAL(8,2);
DEFINE x,y,res DECIMAL(8,2);
SELECT value INTO x FROM sysprofile WHERE name = 'lockwts';
SYSTEM "sleep 10";
SELECT value INTO y FROM sysprofile WHERE name = 'lockwts';
LET res = (y - x) / 10;
RETURN res;
END Procedure;

--Deadlocks /sec
CREATE PROCEDURE APM_DEADL()
RETURNING DECIMAL(8,2);
DEFINE x,y,res DECIMAL(8,2);
SELECT value INTO x FROM sysprofile WHERE name = 'deadlks';
SYSTEM "sleep 10";
SELECT value INTO y FROM sysprofile WHERE name = 'deadlks';
LET res = (y - x) / 10;
RETURN res;
END Procedure;

--Sequential Scans /sec
CREATE PROCEDURE APM_SEQ_S()
RETURNING DECIMAL(8,2);
DEFINE x,y,res DECIMAL(8,2);
SELECT value INTO x FROM sysprofile WHERE name = 'seqscans';
SYSTEM "sleep 10";
SELECT value INTO y FROM sysprofile WHERE name = 'seqscans';
LET res = (y - x) / 10;
RETURN res;
END Procedure;

--Sorts /sec
CREATE PROCEDURE APM_SORTS()
RETURNING DECIMAL(8,2);
DEFINE x,y,res DECIMAL(8,2);
SELECT value INTO x FROM sysprofile WHERE name = 'totalsorts';
SYSTEM "sleep 10";
SELECT value INTO y FROM sysprofile WHERE name = 'totalsorts';
LET res = (y - x) / 10;
RETURN res;
END PROCEDURE;

-- Number of Network Connections / sec
CREATE PROCEDURE APM_CONNECT ()
RETURNING DECIMAL(8,2);
DEFINE x,y,res DECIMAL(8,2);
SELECT ng_connects INTO x FROM sysnetglobal;
SYSTEM "sleep 10";
SELECT ng_connects INTO y FROM sysnetglobal;
LET res = (y - x) / 10;
RETURN res;
END PROCEDURE;

Open the /etc/sqlhost:

Database servername Protocol APM-server Service_name where:

- Database servername is the database name
- Protocol is the protocol used to connect to the database (put olsoctcp)
- APM-server is the hostname of your SAM server
- Service_name is the name of your Informix instance

For example:

```
ol_informix1170 olsoctcp myAPM ol_informix1170
```

Open the /etc/services file and add the following line:

```
service_name 1528/tcp #INFORMIX
```

where service_name is the name of your Informix instance (for example: ol_informix1170).

Add a firewall rule for TCP port 1528.

Monitored Components:

For details on monitors, see [SAM Component Monitor Types](#).

Components without predetermined threshold values provide guidance such as "Use the lowest threshold possible" or "Use the highest threshold possible" to help you find a threshold appropriate for your application.
Read Cache Hit %

This monitor returns the percentage of the read cache rate. The read and write cache rates can vary dramatically depending upon the applications and the type and size of the data being operated on. In general, both the read cache rate and write cache rate should be in the 80 to 90th percentile. If these rates are consistently lower than 80%, you should consider increasing the value of the Buffers parameter in your Informix configuration file to achieve higher read and write cache rates. Low read and write cache rates indicate IDS is doing a lot more disk reads and writes than it should, which will greatly slow down overall database engine performance.

Write Cache Hit %

This monitor returns the percentage of write cache rate. The read and write cache rates can vary dramatically depending upon the applications and the type and size of the data being operated on. In general, both the read cache rate and write cache rate should be in the 80 to 90th percentile. If these rates are consistently lower than 80%, you should consider increasing the value of the Buffers parameter in your Informix configuration file to achieve higher read and write cache rates. Low read and write cache rates indicate IDS is doing a lot more disk reads and writes than it should, which will greatly slow down overall database engine performance.

Page Reads /sec

This monitor returns the number of physical database page reads issued. This value should be as low as possible. Higher values may indicate indexing or memory constraints.

Page Writes /sec

This monitor returns the number of physical database page writes issued. This value should be as low as possible. Higher values may indicate indexing or memory constraints.

Committed Transactions/sec

This monitor returns the number of committed transactions rate, per second.

Rolled Back Transactions/sec

This monitor returns the number of rolled back transactions rate, per second.

Latch Request Waits/sec

A latch was the first method that was used in Informix products to protect shared memory resources from being accessed by multiple users at one time. This monitor returns the number of events, per second, when a thread had to wait for a latch.

Buffer Waits Ratio

This monitor returns the buffer waits ratio using the following formula: BR = (bufwaits/ (pagreads + bufwrits)) * 100.

If this value is below seven, everything is considered fine. If this value is between seven and ten, you can expect some sluggishness in response times. If this value is greater than ten, it is
likely that system responses are very slow.

Suggested resolutions:

- Increase the value of the Buffers parameter if the number of unused buffers is zero, and/or if viewing onstat -P over time, you see a small number of partnums trading large percentages of the buffer cache back and forth.
- Increase the value of the LRUS and Cleaners parameters significantly. (The Cleaners parameter should always be greater than or equal to the value of the LRUS parameter for the best LRU flush performance.

Avoid 32 & 64. A known bug may still remain with Informix that causes very poor LRU contention at those values.

**Lock Requests/sec**

A lock is used to reserve access to a database object. This monitor returns the rate of events, per second, that sessions requested a lock.

**Lock Waits /sec**

A lock is used to reserve access to a database object. This monitor returns the rate of events, per second, when sessions had to wait for a lock.

**Deadlocks/sec**

A deadlock occurs when two users hold locks and each user wants to acquire a lock that the other user owns. Informix uses the lock table to detect deadlocks automatically and stop them before they occur. This monitor returns the deadlocks rate, per second. This value should be as low as possible.

**Sequential Scans/sec**

This monitor returns the sequential scans rate, per second. This value should be as low as possible. If the value of this monitor is constantly high and continues to increase, it may indicate some performance problems, especially if your system is in an OLTP environment. You should investigate further to determine the root cause of excessive sequential scans.

Sequential access to a table is sometimes harmful to performance since the database engine needs to scan the entire table to pick up the rows that satisfy the query's conditions.

If tables are small, say a couple of hundred rows, this is acceptable because the database engine initially scans tables that will reside in memory. The next time the database engine scans, all of the data in that table can be retrieved directly from memory.

This is actually an efficient way of using sequential scans. However, if the tables are large, say tables with more than 100,000 rows, repeated sequential scans are deadly to performance.

If you have tables with a large number of sequential scans, it is recommended that you add indexes to this table or use program directives to force the internal query optimizer to choose indexes for accessing data in this table, rather than sequential scans.
Sorts/sec
This monitor returns the sorts rate, per second.

Number of Databases
This monitor returns the number of databases presented in this instance.

Number of DBspaces
This monitor returns the number of database spaces presented in this instance.

Number of Network Connections/sec
This monitor returns the cutwork connections rate, per second.

Locks Overflow
This monitor returns the number of times IDS attempted to exceed the maximum number of locks. If this number is non-zero, you may need to increase the value of the Locks parameter in the configuration file.

Datadbs available space (MB)
This monitor returns the available space, in MB, for database space - datadbs. This value should be as high as possible. You can change which dbspace to monitor by correcting the name in this line of your SQL query: `and name = 'datadbs'`
IBM WebSphere (JMX)

This template monitors IBM WebSphere server statistics by using the JMX protocol. You can use the Orion agent for Linux or SNMP agentless to monitor.

Works with the Orion Agent for Linux.

Prerequisites

Target server configured to allow JMX queries.

This template is configured to send JMX requests on port 8686.

Credentials

Dependent on the JMX configuration.

Configuring WebSphere for Orion agent for Linux

For JMX configurations, install and configure WebSphere per your Linux/Unix distribution. See the IBM Knowledge Center for details. The overall steps include:

1. Install WebSphere and note the following details:
   - You may need to create an administrator account and a new package group.
   - During installation, turn off the secure storage option as this is not needed.
   - Make sure to select the Application Server during installation.

2. Start and stop the WebSphere AppServer.

3. Use a browser to access the WebSphere AppServer console at http://websphere-host:9060/ibm/console
   - You may need to open a port to 9060 on the Websphere host.
   - Use the credentials for the account created during installation.

4. In the console, expose the JMX platform mbeans in the WebSphere AppServer by:
   a. Clicking Servers > Server Types > WebSphere application servers.
   b. Selecting the listed application server.

5. Locate the Java and Process Management > Process definition. In the Generic JVM arguments dialog box, enter the following code:

   ```
   Djavax.management.builder.initial=
   
   Note: There is nothing after the = sign.
   
   Dcom.sun.management.jmxremote=true
   Dcom.sun.management.jmxremote.port=8686
   Dcom.sun.management.jmxremote.ssl=false
   Dcom.sun.management.jmxremote.authenticate=false
   ```
6. Restart the AppServer.

For more information, see Configuring Java Application Servers for JMX.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

All components may vary from a running environment. You can add your own threshold limits as necessary.

**Classes Loaded Count**

This monitor returns the number of classes that are currently loaded in the Java virtual machine.

**Classes Total Loaded Count**

This monitor returns the total number of classes that have been loaded since the Java virtual machine has started execution.

**Classes Unloaded Count**

This monitor returns the total number of classes unloaded since the Java virtual machine has started execution.

**Memory Pending Final Count**

This monitor returns the approximate number of objects for which finalization is pending.

**Memory Heap Init Size (B)**

This monitor returns the initial amount of memory in bytes that the Java virtual machine allocates; or -1 if undefined.

**Memory Heap Used (B)**

This monitor returns the amount of used memory in bytes. The amount of used memory in the returned memory usage is the amount of memory occupied by both live objects and garbage objects that have not been collected, if any.

**Memory Heap Committed (B)**

This monitor returns the amount of committed memory in bytes.

**Memory Heap Max Size (B)**

This monitor returns the maximum amount of memory in bytes that can be used; or -1 if undefined.

**Memory Non Heap Init Size (B)**

This monitor returns the initial amount of memory in bytes that the Java virtual machine allocates; or -1 if undefined.
Memory Non Heap Used (B)
This monitor returns the amount of used memory in bytes.

Memory Non Heap Committed (B)
This monitor returns the amount of committed memory in bytes.

Memory Non Heap Max Size (B)
This monitor returns the maximum amount of memory in bytes that can be used; or -1 if undefined.

Memory Garbage Collections Count
This monitor returns the total number of collections that have occurred.

Memory Garbage Collection Time (ms)
This monitor returns the approximate accumulated collection elapsed time in milliseconds.

Threads Total Started Count
This monitor returns the total number of threads created and also started since the Java virtual machine started.

Current Thread Count
This monitor returns the current number of live threads including both daemon and non-daemon threads.

Current Thread Cpu Time
This monitor returns the total CPU time for the current thread in nanoseconds.

Current Thread User Time
This monitor returns the CPU time that the current thread has executed in user mode in nanoseconds.

Runtime Uptime (ms)
This monitor returns the uptime of the Java virtual machine in milliseconds.

Compiler Time (ms)
This monitor returns the approximate accumulated elapsed time (in milliseconds) spent in compilation.
**IMAP4 Round Trip Email**

This template simulates an email round trip to test the ability of your SMTP server to receive and distribute email, and the ability of your users to retrieve messages from IMAP4-enabled email clients.

**Prerequisites**

None.

**Credentials**

Windows credential valid on both the SAM server and the Microsoft Exchange server.

**Monitored Components**

For details on monitors, see [SAM Component Monitor Types](#).

**IMAP 4 User Experience Monitor**

This component monitor tests an email round trip from your SMTP mail server to your IMAP4 server and measures the time it takes to complete the trip. This response time is measured in milliseconds.

This component monitor uses the following ports when used with a Microsoft Exchange mail server:

- 143 and 993 - IMAP4
- 25 - SMTP
ISC DHCP Server (Linux)

This template assesses the performance of the ISC DHCP service on Linux machines. It uses Perl script and an SNMP process monitor for monitoring the performance of queries.

Prerequisites

SSH and Perl installed on the target server. SNMP installed on the target server and permission to monitor dhcpd processes.

If Perl is installed in a location different from /usr/bin/perl, you should correct all components in the first line of the Script Body field (#!/usr/bin/perl), or you can create a symbolic link to Perl (refer to your documentation for the ln command).

You can find where Perl is installed by using the following command: which perl

Credentials

Root credentials on the target server.

Tested on CentOS 5.5 and ISC DHCP 3.0.5 version.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

You need to set thresholds for counters according to your environment. It is recommended to monitor counters for some length of time to understand potential value ranges and then set the thresholds accordingly.

Queries Rate per Sec

This monitor returns the rates per second of different queries. All rates are calculated as the number of specific queries for 20 seconds and then divided by 20. Information about DHCP queries are taken from the /var/log/messages file. It is possible that scripts will return non-integer values. Returned values are as follows:

- **Discovery** – This component returns the number of queries, which the client broadcasts to locate available servers.
- **Offer** – This component returns the number of DHCP server responses to Discovery queries offering, with configuration information.
- **Request** – This component returns the number of clients' responses to the server Offer packets, containing the following:
  - Requesting offered parameters from one server and implicitly declining offers from all others
  - Confirming correctness of previously allocated address after, (e.g., system reboot)
  - Extending the lease on a particular network address
- **Ack** – This component returns the server’s response to the client Request queries containing configuration parameters, including committed network address.

- **Nak** – This component returns the server’s response to the client Request queries indicating the client's notion of the network address is incorrect (e.g., client has moved to new subnet) or client's lease has expired.

- **Decline** – This component returns the number of clients’ queries indicating network address is already in use.

- **Release** – This component returns the number of clients’ queries relinquishing network address and cancelling the remaining lease.

- **Inform** – This component returns the number of clients’ queries where the client is asking only for local configuration parameters (client already has externally configured network address).

**SNMP Process Monitor: Dhcpd**

This component returns CPU and memory usage of the Dhcpd daemon.

If this counter is unavailable, there may be problems with SNMP configuration or the Dhcpd service has stopped.
Java Application Server (SNMP)

This template assesses the overall performance of Java Application Servers by using SNMP protocol. The following application servers are supported: Apache Tomcat, JBoss, GlassFish, IBM WebSphere and Oracle WebLogic. You can use the Orion agent for Linux or SNMP agentless to monitor.

Prerequisites for Orion agent for Linux

If using Orion agent for Linux for monitoring, you may need to complete additional configurations. If using SNMP v2, the Orion agent for Linux automatically configures SNMP. If using SNMP v3, see SNMP for agents.

Prerequisites

SNMP enabled on the operating system. Target JVM configured to allow SNMP queries.

This template is configured to send SNMP requests on port 1161.

Credentials

None. The template uses the SNMP public string assigned to the node.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Some components may not have preset warning or critical threshold values. You can add your own threshold limits as necessary.

Classes Loaded Count

Indicates the number of classes currently loaded in the JVM.

For more information, reference the following Java method:
java.lang.management.ClassLoadingMXBean.getLoadedClassCount()

Classes Total Loaded Count

Indicates the number of classes that have been loaded since the JVM was started.

For more information, reference the following Java methods:
java.lang.management.ClassLoadingMXBean and getTotalLoadedClassCount()

Classes Unloaded Count

Indicates the number of classes that have been unloaded since the JVM was started.

For more information, reference the following Java method:
java.lang.management.ClassLoadingMXBean.getUnloadedClassCount()
Memory Pending Final Count

The approximate number of objects that are pending finalization. This should be as low as possible.

For more information, reference the following Java methods:
java.lang.management.MemoryMXBean. and getObjectPendingFinalizationCount()

Memory Heap Init Size (B)

The amount of memory (in bytes) that the JVM initially requests from the operating system for memory management used for heap memory pools.

For more information, reference the following Java method: java.lang.management.MemoryMXBean.getHeapMemoryUsage() and getInit()

Memory Heap Used (B)

The amount of used memory (in bytes) from heap memory pools. This should be as low as possible.

For more information, reference the following Java method:
java.lang.management.MemoryMXBean.getHeapMemoryUsage() and getUsed()

Memory Heap Committed (B)

The amount of memory (in bytes) committed by heap memory pools.

For more information, reference the following Java methods:
java.lang.management.MemoryMXBean.getHeapMemoryUsage() and getCommitted()

Memory Heap Max Size (B)

The maximum amount of memory (in bytes) for all heap memory pools.

For more information, reference the following Java method: java.lang.management.MemoryMXBean.getHeapMemoryUsage() and getMax()

Memory Non-heap Init Size (B)

The amount of memory (in bytes) that the JVM initially requests from the operating system for memory management for non-heap memory pools.

For more information, reference the following Java method:
java.lang.management.MemoryMXBean.getNonHeapMemoryUsage() and getInit()

Memory Non-heap Used (B)

The amount of used memory (in bytes) from non-heap memory pools. This should be as low as possible.

For more information, reference the following Java method:
java.lang.management.MemoryMXBean.getNonHeapMemoryUsage() and getUsed()

Memory Non-heap Committed (B)

The amount of memory (in bytes) committed by non-heap memory pools.
For more information, reference the following Java methods:
java.lang.management.MemoryMXBean and getNonHeapMemoryUsage() and getCommitted()

Memory Non-heap Max Size (B)

The maximum size of memory (in bytes) for all non-heap memory pools.

For more information, reference the following Java method:
java.lang.management.MemoryMXBean.getNonHeapMemoryUsage() and getMax()

Memory Garbage Collections Count

The number of collections that have occurred, as returned by
GarbageCollectorMXBean.getCollectionCount()

If garbage collection statistics are not available, this object is set to 0.

For more information, reference the following Java method:
java.lang.management.GarbageCollectorMXBean.getCollectionCount()

Memory Garbage Collection Time (ms)

The approximate accumulated collection elapsed time (in milliseconds) since the Java virtual machine has started. This object is set to 0 if the collection elapsed time is undefined for this collector.

For more information, reference the following Java method:
java.lang.management.GarbageCollectorMXBean.getCollectionTime()

Memory Pool Init Size (B)

The initial size of the memory pool. This counter shows statistics for the first memory pool. If another pool needs monitoring, change the last digit of the OID.

For more information, reference the following Java method:
java.lang.management.MemoryPoolMXBean.getUsage() and getInit()

Memory Pool Used (B)

The amount of used memory in the memory pool. This counter shows statistics for the first memory pool. If another pool needs monitoring, change the last digit of the OID. This should be as low as possible.

For more information, reference the following Java method: java.lang.management.MemoryPoolMXBean.getUsage() and getUsed()

Memory Pool Committed (B)

The amount of committed memory in the memory pool. This counter shows statistics for the first memory pool. If another pool needs monitoring, change the last digit of the OID.

For more information, reference the following Java method:
java.lang.management.MemoryPoolMXBean.getUsage() getCommitted()
Memory Pool Max Size (B)

The maximum size of the memory pool. This counter shows statistics for the first memory pool. If another pool needs monitoring, change the last digit of the OID.

For more information, reference the following Java method:
java.lang.management.MemoryPoolMXBean.getUsage() and getMax()

Memory Pool Peak Used (B)

The amount of used memory in the memory pool at the peak usage point. This counter shows statistics for the first memory pool. If another pool needs monitoring, change the last digit of the OID.

For more information, reference the following Java method: java.lang.management. and MemoryPoolMXBean.getPeakUsage() and getUsed()

Memory Pool Peak Committed (B)

The amount of used memory in the memory pool at the peak usage point. This counter shows statistics for the first memory pool. If another pool needs monitoring, change the last digit of the OID.

For more information, reference the following Java method:
java.lang.management.MemoryPoolMXBean.getPeakUsage() and getCommitted()

Memory Pool Peak Max Size (B)

The maximum size of the memory pool at the peak usage point. This counter shows statistics for the first memory pool. If another pool needs monitoring, change the last digit of the OID.

For more information, reference the following Java method: java.lang.management. and MemoryPoolMXBean.getPeakUsage() and getMax()

Threads Total Started Count

The number of threads created and started since the Java Virtual Machine started. This counter shows statistics for the first thread. If another thread needs monitoring, change the last digit of the OID.

For more information, reference the following Java method:
java.lang.management.ThreadMXBean.getTotalStartedThreadCount()

Thread Instant Blocked Count

The number of times that this thread has blocked the “to enter” or “re-enter” monitor. This counter shows statistics for the first thread. If another thread needs monitoring, change the last digit of the OID.

For more information, reference the following Java methods:
java.lang.management.ThreadMXBean.getThreadInfo (long,boolean) And getBlockedCount()
Thread Instant Blocked Time (ms)

The approximate accumulated elapsed time (in milliseconds) that a thread has blocked the “to enter” or “re-enter” monitor since it has started, or since thread contention monitoring was enabled.

This object is always set to 0 if thread contention monitoring is disabled or not supported. This counter shows statistics for the first thread. If another thread needs monitoring, change the last digit of the OID. This should be as low as possible.

For more information, reference the following Java method: `java.lang.management.ThreadMXBean.getThreadInfo(long,boolean)` and `getBlockedTime()`

Thread Instant Wait Count

This counter shows the number of times that this thread waited for notification. It also shows statistics for the first thread. If another thread needs monitoring, change the last digit of the OID.

For more information, reference the following Java methods:

`java.lang.management.ThreadMXBean.getThreadInfo(long,boolean)` and `getWaitedCount()`

Thread Instant Wait Time (ms)

The approximate accumulated elapsed time (in milliseconds) that a thread has waited for a monitor through a “java.lang.Object.wait” method since it has started, or since thread contention monitoring was enabled.

This object is always set to 0 if thread contention monitoring is disabled or not supported. It also shows statistics for first thread. If another thread needs monitoring, change the last digit of the OID. This should be as low as possible.

For more information, reference the following Java methods:

`java.lang.management.ThreadMXBean.getThreadInfo(long,boolean)` and `getWaitedTime()`

Runtime Input Arguments Count

This is the number of input arguments passed to the Java Virtual Machine.

For more information, reference the following Java method:

`java.lang.management.RuntimeMXBean.getInputArguments()`

Runtime Uptime (ms)

This is the uptime of the Java virtual machine (in milliseconds). This is equivalent to `(System.currentTimeMillis() - jvmStartTimeMs)`. 

For more information, reference the following Java methods:

`jvmRTStartTimeMs:java.lang.management.RuntimeMXBean.getUptime()`
Compiler Time (ms)

This gets the approximate accumulated elapsed time (in milliseconds) spent in compilation since the Java virtual machine has started. If multiple threads are used for compilation, this value is the summation of the approximate time that each thread spent in compilation. If compiler time monitoring is not supported, then this object remains set at 0.

For more information, reference the following Java method:
java.lang.management.CompilationMXBean.getTotalCompilationTime()
JBoss (JMX)

This template monitors JBoss server statistics by using the JMX protocol. You can use the Orion agent for Linux or SNMP agentless to monitor.

**Important:** JMX polling is not supported using an Orion Agent for Windows. However, you can configure an application to poll agentlessly by editing the assigned application, expanding the Advanced' section, and change the Preferred Polling Method from Agent to Agentless.

**Prerequisites**

Target server configured to allow JMX queries. See Configuring Java Application Servers for JMX for details.

**Template configuration changes**

The following settings in the component monitors should be changed from defaults:

- The template is configured to send JMX requests on port 8686. For this template, you should change the port to 9999.
- The URL is set to /jmxrmi by default. For this template, you should change the URL to `service:jmx:remoting-jmx://${IP}:${PORT}`.

**Credentials**

Dependent on the JMX configuration.

**JMX Configurations for Orion agent for Linux**

For JMX configurations, install and configure WebSphere per your Linux/Unix distribution. See the IBM Knowledge Center for details. The overall steps include:

1. Install WebSphere and note the following details:
   - You may need to create an administrator account and a new package group.
   - During installation, turn off the secure storage option as this is not needed.
   - Make sure to select the Application Server during installation.

2. Start and stop the WebSphere AppServer.

3. Use a browser to access the WebSphere AppServer console at `http://websphere-host:9060/ibm/console`
   - You may need to open a port to 9060 on the Websphere host.
   - Use the credentials for the account created during installation.

4. In the console, expose the JMX platform mbeans in the WebSphere AppServer by:
   a. Clicking Servers > Server Types > WebSphere application servers.
   b. Selecting the listed application server.
5. Locate the Java and Process Management > Process definition. In the Generic JVM arguments dialog box, enter the following code:

```java
Djavax.management.builder.initial=
Dcom.sun.management.jmxremote=true
Dcom.sun.management.jmxremote.port=8686
Dcom.sun.management.jmxremote.ssl=false
Dcom.sun.management.jmxremote.authenticate=false
Djava.rmi.server.hostname=localhost
```

Note: There is nothing after the = sign.

6. Restart the AppServer.

**Monitored Components**

For details on monitors, see [SAM Component Monitor Types](#).

All components may vary in a running environment. You can add your own threshold limits as needed.

**Classes Loaded Count**

This monitor returns the number of classes that are currently loaded in the Java virtual machine.

**Classes Total Loaded Count**

This monitor returns the total number of classes that have been loaded since the Java virtual machine has started execution.

**Classes Unloaded Count**

This monitor returns the total number of classes unloaded since the Java virtual machine has started execution.

**Memory Pending Final Count**

This monitor returns the approximate number of objects for which finalization is pending.

**Memory Heap Init Size (B)**

This monitor returns the initial amount of memory in bytes that the Java virtual machine allocates; or -1 if undefined.

**Memory Heap Used (B)**

This monitor returns the amount of used memory in bytes. The amount of used memory in the returned memory usage is the amount of memory occupied by both live objects and garbage objects that have not been collected, if any.

**Memory Heap Committed (B)**

This monitor returns the amount of committed memory in bytes.
Memory Heap Max Size (B)

This monitor returns the maximum amount of memory in bytes that can be used; or -1 if undefined.

Memory Non Heap Init Size (B)

This monitor returns the initial amount of memory in bytes that the Java virtual machine allocates; or -1 if undefined.

Memory Non Heap Used (B)

This monitor returns the amount of used memory in bytes.

Memory Non Heap Committed (B)

This monitor returns the amount of committed memory in bytes.

Memory Non Heap Max Size (B)

This monitor returns the maximum amount of memory in bytes that can be used; or -1 if undefined.

Memory Garbage Collections Count

This monitor returns the approximate accumulated collection elapsed time in milliseconds.

You should set the correct Object Name. You can see which names are available by running the Find Processes, Services, and Performance Counters wizard. In the wizard, expand java.lang, and GarbageCollector and check which names are available. By default, this counter uses: name=Copy.

Memory Garbage Collection Time (ms)

This monitor returns the approximate accumulated collection elapsed time in milliseconds.

You should set the correct Object Name. You can see which names are available by running the Find Processes, Services, and Performance Counters wizard. In the wizard, expand java.lang, and GarbageCollector and check which names are available. By default, this counter uses: name=Copy.

Memory Pool Init Size (B)

This monitor returns the initial amount of memory (in bytes) that the Java virtual machine requests from the operating system for memory management during startup. The Java virtual machine may request additional memory from the operating system and may also release memory to the system over time. The value of init may be undefined.

You should set the correct Object Name. You can see which names are available by running the Find Processes, Services, and Performance Counters wizard. In the wizard, expand java.lang and MemoryPool and check which names are available. By default, this counter uses: name=Code Cache.

Memory Pool Used (B)

This monitor returns the amount of memory currently used (in bytes).
Memory Pool Committed Size (B)

This monitor returns the amount of memory (in bytes) that is guaranteed to be available for use by the Java virtual machine. The amount of committed memory may change over time (increase or decrease). The Java virtual machine may release memory to the system and committed could be less than init. committed will always be greater than or equal to used.

Memory Pool Max Size (B)

This monitor returns the maximum amount of memory (in bytes) that can be used for memory management. Its value may be undefined. The maximum amount of memory may change over time if defined. The amount of used and committed memory will always be less than or equal to max if max is defined. A memory allocation may fail if it attempts to increase the used memory such that used > committed even if used <= max would still be true (for example, when the system is low on virtual memory).

Memory Pool Peak Used (B)

This monitor returns the peak amount of memory currently used (in bytes).
Memory Pool Peak Committed (B)

This monitor returns the peak amount of memory (in bytes) that is guaranteed to be available for use by the Java virtual machine. The amount of committed memory may change over time (increase or decrease). The Java virtual machine may release memory to the system and committed could be less than init. committed will always be greater than or equal to used.

You should set the correct Object Name. You can see which names are available by running the Find Processes, Services, and Performance Counters wizard. In the wizard, expand java.lang and MemoryPool and check which names are available. By default, this counter uses: name=Code Cache.

Memory Pool Peak Max Size (B)

This monitor returns the maximum peak amount of memory (in bytes) that can be used for memory management. Its value may be undefined. The maximum amount of memory may change over time if defined. The amount of used and committed memory will always be less than or equal to max if max is defined. A memory allocation may fail if it attempts to increase the used memory such that used > committed even if used <= max would still be true (for example, when the system is low on virtual memory).

You should set the correct Object Name. You can see which names are available by running the Find Processes, Services, and Performance Counters wizard. In the wizard, expand java.lang and MemoryPool and check which names are available. By default, this counter uses: name=Code Cache.

Threads Total Started Count

This monitor returns the total number of threads created and also started since the Java virtual machine started.

Current Thread Count

This monitor returns the current number of live threads including both daemon and non-daemon threads.

Current Thread Cpu Time

This monitor returns the total CPU time for the current thread in nanoseconds.

Current Thread User Time

This monitor returns the CPU time that the current thread has executed in user mode in nanoseconds.

Runtime Uptime (ms)

This monitor returns the uptime of the Java virtual machine in milliseconds.

Compiler Time (ms)

This monitor returns the approximate accumulated elapsed time (in milliseconds) spent in compilation.
Active Thread Count
This monitor returns the number of active threads in the JVM.

Active Thread Group Count
This monitor returns the number of active thread groups in the JVM.

Free Memory
This monitor returns the amount of free memory for the JVM this app server instance is running on. This counter should be as high as possible.

Available Processors
This monitor returns the number of available processors.

Total Memory
This monitor returns the total memory for the JVM this app server instance is running on.

Configuring Java Application Servers for JMX

A Java Management Extension (JMX) allows remote clients to connect to a Java Virtual Machine (JVM). The SAM JMX template allows you to monitor vital statistics from JVM. Before assigning the template to a node with a JVM, configure the target JVM to accept remote JMX queries.

This section describes how to configure JVM servers for JMX monitoring including servers embedded with JBoss, Glassfish, IBM Websphere, and Oracle Weblogic. Configuration instructions are given for both Linux and Microsoft Windows operating systems.

- Java arguments
- Configuring a Standalone Java Virtual Machine
- Configuring JBoss (tested on versions 6.1)
- Configuring GlassFish (tested on version 3.1)
- Configuring IBM WebSphere (tested on version 8.0)
- Configuring Oracle WebLogic (tested on version 12)

Java Arguments
To enable remote JMX monitoring, use the following Java arguments:

-Djava.rmi.server.hostname=192.168.0.236
This line indicates the IP address the RMI server will use. Type your server IP address here.

-Dcom.sun.management.jmxremote
This line enables remote JMX monitoring.

-Dcom.sun.management.jmxremote.port=8686
This line indicates which port the JMX module will use to accept JMX connections.
Dcom.sun.management.jmxremote.ssl=false

This line indicates if SSL is used.

Dcom.sun.management.jmxremote.authenticate=true

This line indicates if authentication is used. Use of authentication is recommended. If you do not want to use authentication, you should change the value to false.

Dcom.sun.management.jmxremote.password.file=c:\jmxremote.password

This line indicates where the passwords file is stored. Do not add this line if you are not using authentication.

Dcom.sun.management.jmxremote.access.file=c:\jmxremote.access

This line indicates where the access file is stored. Do not add this line if you are not using authentication.

More information can be found at the following website: http://docs.oracle.com/en/.

Configuring a Standalone Java Virtual Machine

Windows

1. Download the JDK from the Oracle website: http://www.oracle.com/technetwork/java/javase/downloads/index.html (tested on JDK 1.7.0, update version 3).
2. Install the JDK.
3. On the license agreement page, read and accept the license, and then click Next.
4. Click Change to change the installation directory to C:\Program Files\Java\jdk1.7.0_3, and then click OK.
5. Click Next.
6. Click Finish to exit the installer.
7. Add a variable to the system with its path pointing to the JDK installation folder.

For example:

- **Variable name:** JAVA_HOME
- **Variable value:** C:\Program Files\Java\jdk1.7.0_3

If you want to run Java commands from the command line, you should add the JDK installation path to the PATH variable.

If you plan to use JMX authentication:
1. Navigate to the %JAVA_HOME%\jre\lib\management folder.

2. Rename the jmx.remote.password.template file to jmxremote.password. Edit jmxremote.password by replacing/adding its content with the following: samuser somepasswd where samuser is the user for the JVM monitored from SAM and somepasswd is the password.

3. Edit jmxremote.access by replacing/adding its content with the following: samuser readonly where samuser is user for the JVM monitored and readonly gives this read only permissions.

4. Copy jmxremote.access and jmxremote.password to a folder, for example c:\jmxremote\.

5. Grant access to the jmxremote.password file only for the Administrator. To grant access only for the Administrator, refer to this topic at the following location: http://download.oracle.com/javase/6/docs/technotes/guides/security-windows.html

---

**Linux**

---


2. Unpack and run the JDK. In this case, the JDK was installed into the /usr/java/jdk1.7.0_3 folder.

3. Move this folder to /usr/local.

4. In the /usr/local directory, create a symbolic link to jdk1.7.0_3 named Java. Now the JDK is installed in /usr/local/jdk1.7.0_3 and linked to /usr/local/java.

5. Add the /usr/local/java/bin folder to the system path. (If it is only for your account, add it in .bash_profile file in your home directory). In Slackware, it should be in the .profile file. To make it a system wide environment, add it in the /etc/profile.

6. Edit a line in .bash_profile to be similar to:

   PATH=$PATH:$HOME/bin:/usr/local/java/bin. The path will be automatically set at boot time. To set the path immediately, use the following command: $ export
   PATH=$PATH:/usr/local/java/bin

7. Add a variable to the system with the path pointing to the JDK installation folder.

8. Add the following lines to the /etc/profile file. Syntax dependencies may be different in various Linux distributions. This example is shown for the CentOS system:

   ```
   export JAVA_HOME=/usr/java/jdk1.7.0_3
   export PATH=$PATH:/usr/java/jdk1.7.0_3
   ```

To set this immediately, run the export commands in your shell, or logout then log back in to your system.

---

If you use JMX authentication:

1. Go to the $JAVA_HOME/jre/lib/management folder and rename the jmxremote.password.template file to jmxremote.password.

2. Edit jmxremote.password by replacing/adding the content with the following:

   ```
   samuser somepasswd
   ```

   where samuser is the user for the JVM monitored from SAM and somepasswd is the password.
3. Edit `jmxremote.access` by replacing/adding the content with the following:
   ```
   samuser readonly
   where samuser is user for the JVM monitored and readonly - gives this read only permissions.
   ```
4. Copy `jmxremote.access` and `jmxremote.password` to a folder, for example `/jmxremote/`.
5. Grant access to the `jmxremote.password` file only for the root user. Run the following commands as the root user in your shell:
   ```
   # chown root.root $JAVA_HOME/jre/lib/management/jmxremote.password
   # chmod 600 $JAVA_HOME/jre/lib/management/jmxremote.password
   ```

**Testing a Standalone JVM**

You can test that your JVM can respond to JMX queries by adding the following to the `java` command line. This will enable JMX on port 8686 using authentication:

```
```

For example:

```
```

In a separate window/shell, run the following command to test JMX and the JDK configurations:

```
%JAVA_HOME%\jdk1.7.0_3\bin\jconsole
```

In the `jconsole` window, select Remote Process, type `127.0.0.1:8686` and provide Username: `sam` and Password: `somepasswd`. After a successful connection, you will be able to see different monitoring statistics.

**Configuring JBoss (tested on version 6.1)**

**Windows Command Line:**

Edit `%JBoss_HOME%\bin\run.bat` by adding the following lines where `%JBoss_HOME%` is the path to your JBoss installation and where `192.168.0.236` is the IP address of the JBoss server:

```
set "JAVA_OPTS=%JAVA_OPTS% -Djavax.management.builder.initial=org.jboss.system.server.jmx.MBeanServerBuilderImpl"
set "JAVA_OPTS=%JAVA_OPTS% -Djboss.platform.mbeanserver"
```

---

*SAM TEMPLATE REFERENCE: SERVER & APPLICATION MONITOR*
The above lines should go before the following section:

```
set "JAVA_OPTS=%JAVA_OPTS% -Djava.rmi.server.hostname=192.168.0.236"
set "JAVA_OPTS=%JAVA_OPTS% -Dcom.sun.management.jmxremote.port=8686"
set "JAVA_OPTS=%JAVA_OPTS% -Dcom.sun.management.jmxremote.ssl=false"
set "JAVA_OPTS=%JAVA_OPTS% -Dcom.sun.management.jmxremote.authenticate=true"
set "JAVA_OPTS=%JAVA_OPTS% -Dcom.sun.management.jmxremote.password.file="c:\jmxremote\jmxremote.password"
set "JAVA_OPTS=%JAVA_OPTS% -Dcom.sun.management.jmxremote.access.file="c:\jmxremote\jmxremote.access"
```

Start JBoss by running `%JBoss_HOME%\bin\run.bat`.

Linux

Edit `$JBoss_HOME/bin/run.sh` by adding the following lines where `$JBoss_HOME` is the path to your JBoss installation and where `192.168.0.236` is the IP address of JBoss server:

```
JAVA_OPTS="$JAVA_OPTS -Djavax.management.builder.initial=org.jboss.system.server.jmx.MBeanServerBuilderImpl"
JAVA_OPTS="$JAVA_OPTS -Djboss.platform.mbeanserver"
JAVA_OPTS="$JAVA_OPTS -Djava.rmi.server.hostname=192.168.0.236"
JAVA_OPTS="$JAVA_OPTS -Dcom.sun.management.jmxremote.port=8686"
JAVA_OPTS="$JAVA_OPTS -Dcom.sun.management.jmxremote.ssl=false"
JAVA_OPTS="$JAVA_OPTS -Dcom.sun.management.jmxremote.authenticate=true"
JAVA_OPTS="$JAVA_OPTS -Dcom.sun.management.jmxremote.password.file="/jmxremote/jmxremote.password"
JAVA_OPTS="$JAVA_OPTS -Dcom.sun.management.jmxremote.access.file="/jmxremote/jmxremote.access"
```
The above lines should go before the following section:

```
# Display our environment
echo
"========================================================================="
echo ""
echo " JBoss Bootstrap Environment"
echo ""
echo " JBOSS_HOME: $JBOSS_HOME"
echo ""
echo " JAVA: $JAVA"
echo ""
echo " JAVA_OPTS: $JAVA_OPTS"
echo ""
echo " CLASSPATH: $JBOSS_CLASSPATH"
echo ""
echo "=========================================================================
```

Run JBoss by running `$JBOSS_HOME/bin/run.sh`.

### Configuring GlassFish (tested on version 3.1)

1. Run the GlassFish Application Server.
2. Open a web browser and then navigate to: `http://hostname:4848` where `hostname` which is the name of your GlassFish server.
3. In the left panel, click Configurations: server-config.
4. In the main window, click JVM settings.
5. Click the JVM Options tab.
6. Click Add JVM Option and then type: `Dcom.sun.management.jmxremote` in the blank field.
7. Click Add JVM Option and then type: `Djava.rmi.server.hostname=192.168.0.236` in the blank field, where `192.168.0.236` is IP address of GlassFish server.
8. Click Add JVM Option and then type: `Dcom.sun.management.jmxremote.port=8686` in the blank field.
9. Click Add JVM Option and then type: `Dcom.sun.management.jmxremote.ssl=false` in the blank field.
10. Click Add JVM Option and then type: `Dcom.sun.management.jmxremote.authenticate=true` in the blank field.
11. Click Add JVM Option and then type:
    
    `Dcom.sun.management.jmxremote.password.file="c:/jmxremote/jmxremote.password"` in the blank field.
12. Click Add JVM Option and then type: 
   `Dcom.sun.management.jmxremote.access.file=c:/jmxremote/jmxremote.access` in the blank field.

13. Click Save.

14. Restart the GlassFish server.

### Configuring IBM WebSphere (tested on version 8.0)

1. Run the IBM WebSphere Application Server.
2. Open a web browser and then navigate to: `https://hostname:9043` where `hostname` is the name of the IBM WebSphere server.
3. In the left panel, click Expand Servers and Server types.
4. Click WebSphere Application Servers.
5. In the main window, click your server.
7. Click Process Definition.
8. In the Additional Properties section, click Java Virtual Machine.
9. In Generic JVM Arguments, add the following:

   ```
   This will enable JMX without authentication
   
   -Djavax.management.builder.initial= -
   Djava.rmi.server.hostname=192.168.0.236 -Dcom.sun.management.jmxremote -
   Dcom.sun.management.jmxremote.port=8686 -
   Dcom.sun.management.jmxremote.ssl=false -
   Dcom.sun.management.jmxremote.authenticate=false
   ```

10. Click OK.
11. Click Save and then click OK.
12. Click Save.
13. Restart the IBM WebSphere Application Server.

If you have errors after these configuration changes, you can manually change/restore the configuration. 
These changes are stored in the following file:

```
%WEBSPHERE_HOME%\profiles\your_profile\config\cells\your_cell\nodes\your_node\servers\your_server\server.xml
```
Configuring Oracle WebLogic (tested on version 12)

Windows

Edit the following file:
%MIDDLEWARE_HOME%\user_projects\domains\<your_domain>\bin\startWebLogic.cmd

where %MIDDLEWARE_HOME% is the path to your WebLogic installation, by adding the following lines:

```bash
set "JAVA_OPTIONS=%JAVA_OPTIONS% -Djavax.management.builder.initial=weblogic.management.jmx.mbeanserver.WLSMBeanServerBuilder"
set "JAVA_OPTIONS=%JAVA_OPTIONS% -Dcom.sun.management.jmxremote"
set "JAVA_OPTIONS=%JAVA_OPTIONS% -Dcom.sun.management.jmxremote.port=8686"
set "JAVA_OPTIONS=%JAVA_OPTIONS% -Dcom.sun.management.jmxremote.ssl=false"
set "JAVA_OPTIONS=%JAVA_OPTIONS% -Dcom.sun.management.jmxremote.authenticate=true"
set "JAVA_OPTIONS=%JAVA_OPTIONS% -Dcom.sun.management.jmxremote.password.file="c:\jmxremote\jmxremote.password"
set "JAVA_OPTIONS=%JAVA_OPTIONS% -Dcom.sun.management.jmxremote.access.file="c:\jmxremote\jmxremote.access"
```

The result should resemble:

```bash
... call "%DOMAIN_HOME%\bin\setDomainEnv.cmd" %*
set "JAVA_OPTIONS=%JAVA_OPTIONS% -Djavax.management.builder.initial=weblogic.management.jmx.mbeanserver.WLSMBeanServerBuilder"
set "JAVA_OPTIONS=%JAVA_OPTIONS% -Dcom.sun.management.jmxremote"
set "JAVA_OPTIONS=%JAVA_OPTIONS% -Dcom.sun.management.jmxremote.port=8686"
set "JAVA_OPTIONS=%JAVA_OPTIONS% -Dcom.sun.management.jmxremote.ssl=false"
set "JAVA_OPTIONS=%JAVA_OPTIONS% -Dcom.sun.management.jmxremote.authenticate=true"
set "JAVA_OPTIONS=%JAVA_OPTIONS% -Dcom.sun.management.jmxremote.password.file="c:\jmxremote\jmxremote.password"
set "JAVA_OPTIONS=%JAVA_OPTIONS% -Dcom.sun.management.jmxremote.access.file="c:\jmxremote\jmxremote.access"
set SAVE_JAVA_OPTIONS=%JAVA_OPTIONS%
...```

⚠️ This file is created by the Configuration Wizard. Your changes to this script will be lost the next time you use the configuration wizard.
Restart the WebLogic Server.

**Linux**

Edit the following file:

```bash
$MIDDLEWARE_HOME/user_projects/domains/<your_domain>/bin/startWebLogic.sh
```

where `$MIDDLEWARE_HOME` is the path to your WebLogic installation, by adding the following lines:

```bash
JAVA_OPTIONS="$JAVA_OPTIONS-
Djavax.management.builder.initial=weblogic.management.jmx.mbeanserver.WLSMBeanServerBuilder"
JAVA_OPTIONS="$JAVA_OPTIONS -Dcom.sun.management.jmxremote"
JAVA_OPTIONS="$JAVA_OPTIONS-Dcom.sun.management.jmxremote.port=8686"
JAVA_OPTIONS="$JAVA_OPTIONS-Dcom.sun.management.jmxremote.ssl=false"
JAVA_OPTIONS="$JAVA_OPTIONS-Dcom.sun.management.jmxremote.authenticate=true"
JAVA_OPTIONS="$JAVA_OPTIONS-Dcom.sun.management.jmxremote.password.file="/jmxremote/jmxremote.password"
JAVA_OPTIONS="$JAVA_OPTIONS-Dcom.sun.management.jmxremote.access.file="/jmxremote/jmxremote.access"
```

The result should resemble:

```bash
...
. ${DOMAIN_HOME}/bin/setDomainEnv.sh $*
JAVA_OPTIONS="$JAVA_OPTIONS-
Djavax.management.builder.initial=weblogic.management.jmx.mbeanserver.WLSMBeanServerBuilder"
JAVA_OPTIONS="$JAVA_OPTIONS-Dcom.sun.management.jmxremote"
JAVA_OPTIONS="$JAVA_OPTIONS-Dcom.sun.management.jmxremote.port=8686"
JAVA_OPTIONS="$JAVA_OPTIONS-Dcom.sun.management.jmxremote.ssl=false"
JAVA_OPTIONS="$JAVA_OPTIONS-Dcom.sun.management.jmxremote.authenticate=true"
JAVA_OPTIONS="$JAVA_OPTIONS-Dcom.sun.management.jmxremote.password.file="/jmxremote/jmxremote.password"
JAVA_OPTIONS="$JAVA_OPTIONS-Dcom.sun.management.jmxremote.access.file="/jmxremote/jmxremote.access"
SAVE_JAVA_OPTIONS="${JAVA_OPTIONS}"
...
```

⚠️ This file is created by the Configuration Wizard. Your changes to this script will be lost the next time you use the configuration wizard.

Restart the WebLogic Server.
Java Application Server (JMX)

This template assesses the overall performance of Java Application Servers by using JMX protocol. The following application servers are supported: Apache Tomcat, JBoss, GlassFish, IBM WebSphere and Oracle WebLogic.

Prerequisites: Target JVM configured to allow JMX queries.

This template is configured to send JMX requests on port 8686.

Credentials: Dependent on the JMX configuration.

All monitoring information is taken from: http://docs.oracle.com/javase/1.5.0/docs/guide/management/overview.html.

Monitored Components

All components may vary from a running environment. You can add your own threshold limits as necessary. For more information, see "Using the Orion APM Min/Max/Average statistics data for creating threshold settings" in the SolarWinds Success Center.

Classes Loaded Count

This monitor returns the number of classes that are currently loaded in the Java virtual machine.

Classes Total Loaded Count

This monitor returns the total number of classes that have been loaded since the Java virtual machine has started execution.

Classes Unloaded Count

This monitor returns the total number of classes unloaded since the Java virtual machine has started execution.

Memory Pending Final Count

This monitor returns the approximate number of objects for which finalization is pending.

Memory Heap Init Size (B)

This monitor returns the initial amount of memory in bytes that the Java virtual machine allocates; or -1 if undefined.

Memory Heap Used (B)

This monitor returns the amount of used memory in bytes. The amount of used memory in the returned memory usage is the amount of memory occupied by both live objects and garbage objects that have not been collected, if any.

Memory Heap Committed (B)

This monitor returns the amount of committed memory in bytes.
**Memory Heap Max Size (B)**

This monitor returns the maximum amount of memory in bytes that can be used; or -1 if undefined.

**Memory Non Heap Init Size (B)**

This monitor returns the initial amount of memory in bytes that the Java virtual machine allocates; or -1 if undefined.

**Memory Non Heap Used (B)**

This monitor returns the amount of used memory in bytes.

**Memory Non Heap Committed (B)**

This monitor returns the amount of committed memory in bytes.

**Memory Non Heap Max Size (B)**

This monitor returns the maximum amount of memory in bytes that can be used; or -1 if undefined.

**Memory Garbage Collections Count**

This monitor returns the approximate accumulated collection elapsed time in milliseconds.

> You should set the correct Object Name. You can see which names are available by running the Find Processes, Services, and Performance Counters wizard. In the wizard, expand java.lang, and GarbageCollector and check which names are available. By default, this counter uses: name=Copy.

**Memory Garbage Collection Time (ms)**

This monitor returns the approximate accumulated collection elapsed time in milliseconds.

You should set the correct Object Name. You can see which names are available by running the Find Processes, Services, and Performance Counters wizard. In the wizard, expand java.lang, and GarbageCollector and check which names are available. By default, this counter uses: name=Copy.

**Memory Pool Init Size (B)**

This monitor returns the initial amount of memory (in bytes) that the Java virtual machine requests from the operating system for memory management during startup. The Java virtual machine may request additional memory from the operating system and may also release memory to the system over time. The value of init may be undefined.

> You should set the correct Object Name. You can see which names are available by running the Find Processes, Services, and Performance Counters wizard. In the wizard, expand java.lang, and MemoryPool and check which names are available. By default, this counter uses: name=Code Cache.

For IBM WebSphere, this counter is unavailable and you should disable it.

**Memory Pool Used (B)**
This monitor returns the amount of memory currently used (in bytes).

You should set the correct Object Name. You can see which names are available by running the Find Processes, Services, and Performance Counters wizard. In the wizard, expand java.lang and MemoryPool and check which names are available. By default, this counter uses: name=Code Cache.

For IBM WebSphere, this counter is unavailable and you should disable it.

Memory Pool Committed Size (B)

This monitor returns the amount of memory (in bytes) that is guaranteed to be available for use by the Java virtual machine. The amount of committed memory may change over time (increase or decrease). The Java virtual machine may release memory to the system and committed could be less than init. committed will always be greater than or equal to used.

You should set the correct Object Name. You can see which names are available by running the Find Processes, Services, and Performance Counters wizard. In the wizard, expand java.lang and MemoryPool and check which names are available. By default, this counter uses: name=Code Cache.

For IBM WebSphere, this counter is unavailable and you should disable it.

Memory Pool Max Size (B)

This monitor returns the maximum amount of memory (in bytes) that can be used for memory management. Its value may be undefined. The maximum amount of memory may change over time if defined. The amount of used and committed memory will always be less than or equal to max if max is defined. A memory allocation may fail if it attempts to increase the used memory such that used > committed even if used <= max would still be true (for example, when the system is low on virtual memory).

You should set the correct Object Name. You can see which names are available by running the Find Processes, Services, and Performance Counters wizard. In the wizard, expand java.lang and MemoryPool and check which names are available. By default, this counter uses: name=Code Cache.

For IBM WebSphere, this counter is unavailable and you should disable it.

Memory Pool Peak Used (B)

This monitor returns the peak amount of memory currently used (in bytes).

You should set the correct Object Name. You can see which names are available by running the Find Processes, Services, and Performance Counters wizard. In the wizard, expand java.lang and MemoryPool and check which names are available. By default, this counter uses: name=Code Cache.
For IBM WebSphere, this counter is unavailable and you should disable it.

Memory Pool Peak Committed (B)

This monitor returns the peak amount of memory (in bytes) that is guaranteed to be available for use by the Java virtual machine. The amount of committed memory may change over time (increase or decrease). The Java virtual machine may release memory to the system and committed could be less than init. committed will always be greater than or equal to used.

You should set the correct Object Name. You can see which names are available by running the Find Processes, Services, and Performance Counters wizard. In the wizard, expand java.lang and MemoryPool and check which names are available. By default, this counter uses: name=Code Cache.

For IBM WebSphere, this counter is unavailable and you should disable it.

Memory Pool Peak Max Size (B)

This monitor returns the maximum peak amount of memory (in bytes) that can be used for memory management. Its value may be undefined. The maximum amount of memory may change over time if defined. The amount of used and committed memory will always be less than or equal to max if max is defined. A memory allocation may fail if it attempts to increase the used memory such that used > committed even if used <= max would still be true (for example, when the system is low on virtual memory).

You should set the correct Object Name. You can see which names are available by running the Find Processes, Services, and Performance Counters wizard. In the wizard, expand java.lang and MemoryPool and check which names are available. By default, this counter uses: name=Code Cache.

For IBM WebSphere, this counter is unavailable and you should disable it.

Threads Total Started Count

This monitor returns the total number of threads created and also started since the Java virtual machine started.

Current Thread Count

This monitor returns the current number of live threads including both daemon and non-daemon threads.

Current Thread CPU Time

This monitor returns the total CPU time for the current thread in nanoseconds.

Current Thread User Time

This monitor returns the CPU time that the current thread has executed in user mode in nanoseconds.

Runtime Uptime (ms)
This monitor returns the uptime of the Java virtual machine in milliseconds.

**Compiler Time (ms)**

This monitor returns the approximate accumulated elapsed time (in milliseconds) spent in compilation.
JD Edwards EnterpriseOne Server Manager (Windows)

This template allows you to check health of JD Edwards EnterpriseOne Server Manager by checking for critical events in the agent log file and monitoring critical processes and TCP ports. This template should be assigned on the server where JD Edwards EnterpriseOne Server Manager is installed.

Prerequisites

WinRM must be installed and properly configured on the target server.

Credentials

Administrator on target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Server Manager Agent Log File

This monitor returns new server manager events from the last polling period. The server manager agent log contains events related to: registering/installing E1 managed instances; registering and managing IBM WebSphere and Oracle Application Server; managing the configuration file(s) for E1 managed instances; starting/stopping E1 servers and the J2EE servers; performing tools release upgrades/downgrades for E1 servers; discovering and sending log files to the management console for viewing. The returned values are as follows:

- **SEVERE** – This component returns the number of SEVERE messages. SEVERE messages occur when a critical error has occurred from the perspective of the agent. Critical errors are non-recoverable errors and require immediate attention. An example would be a critical problem with initializing the agent that would prevent it from starting or functioning properly. In the message fields, this monitor also returns the SEVERE message.

- **WARNING** – This component returns the number of WARNING messages. WARNING messages denote an abnormal or unexpected result occurred that is recoverable, from the perspective of the agent. An example would include a failure while changing the tools release of an E1 server. It is a significant problem; however, the agent will recover so this is considered a warning. In the message fields, this monitor also returns the SEVERE message.

- **INFO** – This component returns the number of INFO messages. INFO message denotes informative messages providing contextual information as to what the agent is doing. An E1 server that is started using SM would have a log message indicating this at the INFO level.

- **CONFIG** – This component returns the number of CONFIG messages. CONFIG messages are not commonly used in SM. A message at the configuration level is simply a means for logging information particular to that installation, such as the platform of the server.
- **FINE** – This component returns the number of FINE messages. FINE messages are a lower level message still intended as human readable that provides insight into what the agent is doing. This can be thought of as a standard “debug” message.

- **FINER** – This component returns the number of FINER messages. FINER message is an even lower level trace of the debug message. Messages are classified at this level rather than FINE if they are very frequently occurring and less likely to be of interest.

This monitor uses the following arguments:
```
path_to_agent_log_file,agent_name
```
where
```
path_to_agent_log_file - Full path to server manager log file;
agent_name - Agent name. This argument takes part only in generating temporary files.
```
Change this if you monitor several agents on the same target host.

Example:
```
c:\jre_home\logs\elagent_0.log,agent1
```

**Management Console HTTP Port**

This component monitor tests the ability of a Management HTTP Console to accept incoming sessions. By default it monitors TCP port 8999.

**Management Server JMX Port**

This component monitor tests the ability of a Management Server JMX to accept incoming sessions. By default, it monitors TCP port 14501. This port can be changed in the Server Manager HTTP Console in the Management Agents section.

**Management Agent Port**

This component monitor tests the ability of a Remote Management Agent to accept incoming sessions. By default, it monitors TCP port 14502. This port can be changed in the Server Manager HTTP Console in the Management Agents section.

**Management Agent Process**

This monitor returns the CPU and memory usage of the Management Agent process *(steagent.exe).*
Kaspersky Security Center Antivirus

This template assesses the status and overall performance of a Kaspersky Security Center Antivirus.

**Prerequisites**

WMI access to the target server.

**Credentials:**

Windows Administrator on the target server.

**Monitored Components**

For details on monitors, see [SAM Component Monitor Types](#).

**Service: Kaspersky Activation Proxy**

This monitor returns CPU and memory usage of Kaspersky Activation Proxy. This service that gives Network Agent access to activation servers on which you can activate installed applications.

**Service: Kaspersky Lab Administration Server**

This monitor returns CPU and memory usage of Kaspersky Lab Administration Server. Administration Server manages Kaspersky Lab applications installed throughout an enterprise network.

**Service: Kaspersky Lab Network Agent**

This monitor returns CPU and memory usage of Kaspersky Lab Network Agent. Network Agent coordinates the interaction between the Administration Server and Kaspersky Lab applications installed on client computers.

**Service: Kaspersky Lab Web Server**

This monitor returns CPU and memory usage of Kaspersky Lab Web Server.

**TCP Port: Administration server (13000)**

This component monitor tests the ability of Administration Server to accept incoming sessions. By default it monitors TCP port 13000. This TCP port is required for gathering the data from client hosts, connecting Update agents and connecting slave Administration servers. Uses secure SSL connection.

**TCP Port: Administration server (14000)**

This component monitor tests the ability of Administration Server to accept incoming sessions. By default it monitors TCP port 14000. This TCP port is required for gathering the data from
client hosts, connecting Update agents and connecting slave Administration servers. Uses secure SSL connection.

**TCP Port: Kaspersky Security Center Web-Console (HTTP)**

This component monitor tests the ability of Kaspersky Security Center Web-Console (HTTP) to accept incoming sessions. By default, it monitors TCP port 8060. This TCP port is required for connecting to the web server to manage Kaspersky Security Center Web-Console and to organize inner corporate portal.

**TCP Port: Kaspersky Security Center Web-Console (HTTPS)**

This component monitor tests the ability of Kaspersky Security Center Web-Console (HTTPS) to accept incoming sessions. By default, it monitors TCP port 8061. This TCP port is required for connecting to the web server to manage Kaspersky Security Center Web-Console and to organize inner corporate portal. Encryption is used upon connection.

**TCP Port: Activation Proxy Server**

This component monitor tests the ability of Activation Proxy Server to accept incoming sessions. By default, it monitors TCP port 17000. This TCP port is required for connecting to an activation proxy server. Uses secure SSL connection.

**TCP Port: Web Console**

This component monitor tests the ability of Activation Proxy Server to accept incoming sessions. By default, it monitors TCP port 13291. Used for a secure SSL connection between Web Console and Administration Server.

> This monitor is disabled by default.

**Warning and Errors Events: Network Agent**

This monitor returns warning and error events of Kaspersky Network Agent.

- **Source name:** klnagent
- **Event log:** Kaspersky Event Log

**Warning and Errors Events: Administration Server**

This monitor returns warning and error events of Kaspersky Administration Server.

- **Source name:** kladminserver
- **Event log:** Kaspersky Event Log

**Warning and Errors Events: Web Server**

This monitor returns warning and error events of Kaspersky Web Server.

- **Source name:** klwebsrv
- **Event log:** Kaspersky Event Log

**Warning and Errors Events: Activation Proxy**

This monitor returns warning and error events of Kaspersky Activation Proxy.
Source name: klactprx
Event log: Kaspersky Event Log
LDAP User Experience Monitor

This template tests the capabilities of a LightWeight Directory Access Protocol (LDAP) server, and measures the time it takes to perform LDAP search-and-compare operations.

Prerequisites

WMI access on target server.

Credentials

Administrator on target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

LDAP User Experience Monitor

This component monitor tests the capabilities of a Lightweight Directory Access Protocol (LDAP) server and measures the time it takes to perform an LDAP query. This monitor returns the number of entries returned by the LDAP query. By default, it queries the Administrator user.

Before using this monitor you must provide the correct values in the Realm (user domain) and LDAP Search Root fields. In the Realm (user domain) fields, you must provide the realm to use for LDAP authentication. In the LDAP Search Root field, you must specify the LDAP root or suffix to use for the search.

By default, this monitor queries the Administrator in the somedomain.test domain.
Linux templates

The following templates are available:

- Linux CPU Monitoring Perl
- Linux Disk Monitoring Perl
- Linux Memory Monitoring Perl
- Linux Sendmail Monitoring Perl
Linux CPU Monitoring Perl

This template assesses the CPU performance of a Linux computer. It uses Perl scripts for monitoring performance.

Works with the Orion Agent for Linux.

Prerequisites:

SSH and Perl installed on the target server.

If Perl is installed in a location different from /usr/bin/perl, you should correct all components in the first line of the field "script body" (#!/usr/bin/perl), or you can create a symbolic link to Perl (refer to the documentation for the ln command).

You can find where Perl is installed by using the following command: which perl

Operating Systems:

The following operating system versions may cause issues with certain counters in this template:

- Red Hat Enterprise Linux 3

Credentials:

Root credentials on the target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Components without predetermined threshold values have guidance such as "Use the lowest threshold possible" or "use the highest threshold possible" to help you find a threshold appropriate for your application.

CPU User Time

Time, in percentages, spent running non-kernel code (user time, including nice time). This represents the time spent executing user code. It depends on the programs that the user uses.

Use the lowest threshold possible.

CPU System Time

Time, in percentages, spent running system kernel code (system time).

Use the lowest threshold possible.

Wait IO

Time, in percentages, spent waiting for input/output (IO) operations.
Use the lowest threshold possible.

If CPU waits IO is high, there may be problems with hard disk or problems with accessing NFS shares (if you use NFS).

**CPU Idle Time**

Time, in percentages, spent idle (this includes IO-wait time).

Use the highest threshold possible at all times.

**Run queue**

The number of processes waiting for run time.

This should be as low as possible, but not more than 4 per processor. If the run queue is constantly growing, it may indicate the need for a more powerful CPU or more CPUs.

Set the thresholds appropriately for your environment.

**Interrupts per second**

The number of interrupts per second, including the clock.

This depends on the processor. For current CPUs, use a threshold of 1500 interrupts per second. A dramatic increase in this counter value without a corresponding increase in system activity indicates a hardware problem. Identify the network adapter or disk controller card causing the interrupts. You may need to install an additional adapter or controller card.

Set the thresholds appropriately for your environment.

**Context switches per second**

The number of context switches per second.

High activity rates can result from inefficient hardware or poorly designed applications. The normal amount of Context Switches/Sec depends on your servers and applications. To set the threshold, you really need to baseline the server. The threshold for Context Switches/sec is cumulative for all processors, so you need a minimum of 14000 per processor (single=14000, dual=28000, quad=56000 and so forth).

Set the thresholds appropriately for your environment.

**Total amount of interrupts after boot**

The total number of interrupts after boot.

**Total amount of CPU context switches after boot**

The total number of CPU context switches after boot.
Linux Disk Monitoring Perl

This template assesses the disk performance of a Linux computer. This template uses Perl scripts for monitoring performance.

ℹ️ Works with the Orion Agent for Linux.

Prerequisites

SSH and Perl installed on the target server.

If Perl is installed in a location different from /usr/bin/perl, you should correct all components in the first line of the field "script body" (#!/usr/bin/perl), or you can create a symbolic link to Perl (refer to the documentation for the ln command).

You can find where Perl is installed by using the following command: which perl

Operating Systems

The following operating system versions may cause issues with certain counters in this template:

- Fedora 14

Credentials

The component monitors Timing cached reads and Timing buffered disk reads require root credentials on the target server. These component monitors require access to vmstat and df utilities.

All other component monitors can use any user account.

Monitored Components

ℹ️ For details on monitors, see SAM Component Monitor Types.

ℹ️ Components without predetermined threshold values have guidance such as "use the lowest threshold possible" or "use the highest threshold possible" to help you find a threshold appropriate for your application.

Timing cached reads (MB/sec)

Perform timings of cache reads for benchmark and comparison purposes. This displays the speed of reading directly from the Linux buffer cache without disk access. This measurement is essentially an indication of the throughput of the processor, cache, and memory of the system under test.

ℹ️ Use the highest threshold possible. You should monitor this counter for some time and then set thresholds appropriately for your environment.
Troubleshooting: There is a bug in the component script. It tests only the first hard drive (SATA or IDE). If you have a first SATA or a first IDE (but only one hard drive), the script works well. But if you have SATA first hard drive and IDE first hard drive (both hard drives), the result will be only for the SATA first hard drive.

If you need to monitor a second or third IDE hard drive, you should find and change the lines “/dev/hda” to “/dev/hdb” (for the second IDE) or to “/dev/hdc” (for the third IDE hard drive).

If you need to monitor a second or third SATA hard drive, you should find and change the lines “/dev/sda” to “/dev/sdb” (for second SATA) or to “/dev/sdc” (for third SATA hard drive).

This component requires root credentials on the target server.

Timing buffered disk reads (MB/sec)

Perform timings of device reads for benchmark and comparison purposes. This displays the speed of reading through the buffer cache to the disk without any prior caching of data. This measurement is an indication of how fast the drive can sustain sequential data reads under Linux, without any file system overhead.

Use the highest threshold possible. You should monitor this counter for some time and then set thresholds appropriately for your environment.

Troubleshooting: There is a bug in the component script. It tests only the first hard drive (SATA or IDE). If you have a first SATA or a first IDE (but only one hard drive), the script works well. But if you have SATA first hard drive and IDE first hard drive (both hard drives), the result will be only for the SATA first hard drive.

If you need to monitor a second or third IDE hard drive, you should find and change the lines “/dev/hda” to “/dev/hdb” (for the second IDE) or to “/dev/hdc” (for the third IDE hard drive).

If you need to monitor a second or third SATA hard drive, you should find and change the lines “/dev/sda” to “/dev/sdb” (for second SATA) or to “/dev/sdc” (for third SATA hard drive).

This component requires root credentials on the target server.

Blocks received from block device (blocks/sec)

This shows the number of blocks read from the disk in the previous interval. All Linux blocks are currently 1024 bytes. Old kernels may report blocks as 512 bytes, 2048 bytes, or 4096 bytes.

Blocks sent to a block device (blocks/sec)

This indicates the total number of blocks written to disk in the previous interval. All Linux blocks are currently 1024 bytes. Old kernels may report blocks as 512 bytes, 2048 bytes, or 4096 bytes.

Available space on / partition (MB)

This shows the available space on the root (/) partition in MB.

You should set this threshold according to your Linux installation and your
requirements. In the worst case, it should be more than 512 MB.
Linux Memory Monitoring Perl

This template assesses the memory performance of a Linux computer. This template uses Perl scripts for monitoring performance.

Works with the Orion Agent for Linux.

Prerequisites

SSH and Perl installed on the target server.

If Perl is installed in a location different from /usr/bin/perl, you should correct all components in the first line of the field “script body” (#!/usr/bin/perl), or you can create a symbolic link to Perl (refer to the documentation for the ln command).

You can find where Perl is installed by using the following command: which perl

Operating Systems

The following operating system versions may cause issues with certain counters in this template:

- Red Hat Enterprise Linux 3, 4
- SUSE Linux Enterprise Server 9

Credentials

Root credentials on the target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Components without predetermined threshold values have guidance such as "use the lowest threshold possible" or "use the highest threshold possible" to help you find a threshold appropriate for your application.

Total memory (kB)

This shows the amount of total usable RAM in kB.

Used memory (kB)

This shows the amount of used memory in kB.

This should be as low as possible.

Free memory (kB)

This shows the amount of available memory in kB.
This should be more than 100000 kB at all times or paging will occur.

**Total swap (kB)**

This shows the amount of total swap space in kB.

**Used swap (kB)**

This shows the amount of used swap space in kB. Paging is one of the memory-management schemes by which a computer can store and retrieve data from secondary storage for use in main memory. Paging is an important part of virtual memory implementation in most contemporary general-purpose operating systems, allowing them to use disk storage for data that does not fit into physical random-access memory (RAM).

This should be as low as possible. Ideally it should be near zero. If the value is large, it may indicate that there is no free memory left.

**Free swap (kB)**

This shows amount of available swap space in kB.

It should be near the “total swap” value. If paging occurs in the system, the value should be as high as possible.

**Buffers (kB)**

RAM that is allocated to disk write operations.

**Cache (kB)**

RAM that is allocated to disk read operations.

**Dirty Pages (kB)**

The total amount of memory, in kilobytes, waiting to be written back to the disk.

This should be as low as possible.

You should monitor this counter for some time and then set thresholds appropriately for your environment.

**Anonymous Pages (kB)**

Anonymous memory is memory that is managed by segvn but is not really directly associated with a file. It is used for things like process stacks, heap, or COW (copy on write) pages. A good example of this is if you fork a process. All the addresses in the second process actually map back to the same bits of physical memory (the same pages). However if your child process was then to do something different with the memory (for example the child went off and manipulated an array in memory), the VM subsystem would copy those pages and change the mappings in the child process to point to the new pages. This new memory would be anonymous memory, and the child process would merrily make the changes to the array, unaware it now had new "physical" memory it was addressing.

This should be as low as possible. You should monitor this counter for some time and then set thresholds appropriately for your environment.
Amount of zombie processes

This show the number of “zombie” processes. A “zombie” or defunct process is a process that has completed execution, but still has an entry in the process table. This entry is still needed to allow the process that started the (now zombie) process to read its exit status. When a process finishes execution, it will have an exit status to report to its parent process. Because of this last little bit of information, the process will remain in the operating system's process table as a zombie process, indicating that it is not to be scheduled for further execution, but that it cannot be completely removed (and its process ID cannot be reused) until it has been determined that the exit status is no longer needed.

This should always be zero (0). If it is not zero, you should manually kill zombie processes. Use the following command to show these zombie processes (and look for a Z in the STAT column): ps aux

To kill zombie processes:

- The first option is to wait. It is possible that the parent process is intentionally leaving the process in a zombie state to ensure that future children it may create will not receive the same pid. Or perhaps the parent is occupied, and will reap the child process momentarily.
- The second option is to send a SIGCHLD signal to the parent (kill -s SIGCHLD <ppid>). This will cause well-behaving parents to reap their zombie children.
- The third option is to kill the parent process of the zombie. At that point, all of the parent's children will be adopted by the init process (pid 1), which periodically runs wait() to reap any zombie children.
Linux Sendmail Monitoring Perl

This template assesses the Linux sendmail status and performance. This template uses Perl scripts for monitoring performance.

Prerequisites

SSH and Perl installed on the target server.

Perl should be found in: /usr/bin/perl. You can find where Perl is installed by using the following command: which perl

If Perl is installed in another location, you should correct all components in the first line of the field "script body" (#!/usr/bin/perl), or you can create a symbolic link to Perl (refer to the documentation for the ln command).

Operating Systems

The following operating system versions may cause issues with certain counters in this template:

- SUSE Linux Enterprise Server 9, 10, 11
- OpenSUSE 11.3
- Ubuntu Server 10.10

Credentials

Root credentials on the target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Components without predetermined threshold values have guidance such as "use the lowest threshold possible" or "use the highest threshold possible" to help you find a threshold appropriate for your application.

Sendmail instances running

This shows how many instances of sendmail daemon are currently started.

- 0 – Sendmail is stopped. Run sendmail manually.
- >1 – Sendmail is up and running.

Daemon: syslogd

This shows the status of syslogd daemon (Syslog is a standard for logging program messages).

- 0 – Syslog daemon is stopped. Run syslogd manually.
- 1 – Syslog daemon is up and running.
Disk space usage (kB) of mail folder

This shows the disk space in kB used by the user mailboxes in /var/mail.

- Set thresholds according to your requirements.

Disk space usage (kB) of mail queue folder

This shows the disk space in kB used by queued mail in /var/spool/mqueue.

- Set thresholds according to your requirements.

Mail queue length

This shows the mail queue length (how many items are in the queue for delivery).

This should be as low as possible. If the mail queue value is constantly rising, it may indicate problems with delivering messages.

- Set thresholds according to your requirements.

Available space on partition with /var/spool (MB)

This shows the available space on the partition with /var/spool folder in MB.

By default it checks available space on the root (/) partition. If you have created a separate partition /var or /var/spool you need change it in the script (grep "/\$"). You can investigate what partitions you have by using the following command: df

For the /var partition, you should make the following change: change grep "/\$" to grep "/var\$"

For the /var/spool partition, you should make the following change: change grep "/\$" to grep "/var/spool\$"

- Set thresholds according to your requirements.
Log Parser

The following templates are available:

- Log Parser (Perl)
- Log Parser (PowerShell)
Log Parser (PowerShell)

The Log Parser template allows you to check a specified log file and determine the total number of lines that match your search criteria.

Prerequisites

WinRM must be installed and properly configured on the target server.

Credentials

Administrator on target server.

You must specify the correct arguments for each monitored component in the Script Arguments field. If you fail to do this, the monitor will return with a status error of Undefined.

Configuring Windows Remote Management (WinRM)

1. If necessary, install PowerShell 2.0 or later and WinRM on the SAM and target servers. (For installation details, see Microsoft's documentation website (https://docs.microsoft.com/en-us/powershell/).

2. On the SAM server, open a command prompt as an Administrator. Go to the Start menu and right-click the cmd.exe and then select Run as Administrator.

3. Enter the following in the command prompt:
   winrm quickconfig -qwinrm set winrm/config/client @{TrustedHosts="*"}

4. On the target server, open a command prompt as an Administrator and enter the following:
   winrm quickconfigwinrm set winrm/config/client @{TrustedHosts="IP_ADDRESS"}
where IP address is the IP address of your SAM server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Total number of strings found

This monitor shows the total number of strings that match the search criteria. Additionally in the message field, this monitor returns all strings that match the search criteria. In the returning message, this component returns all lines that match the search criteria divided by ";"

This monitor uses the following arguments:

- LogFilePath, RegularExpression  where LogFilePath - This is the path of the target log file on the target server. The path cannot contain any spaces.
- RegularExpression - This is used for regular expression searches to find a desired string in the log file. Searches are not case sensitive; however, a search cannot contain spaces.
Below is an example using the Scripts Arguments field to search the number of strings that match the word "error" in the powertest.log file:

*d:\powertest.log,^error*

**Number of newly found strings**

This monitor shows the number of newly found strings. Additionally, in the message field, this monitor returns all new strings that match search criteria.

This monitor uses the following arguments:

- **LogFilePath,RegularExpression** where LogFilePath - This is the path of the target log file on the target server. The path cannot contain any spaces.
- **RegularExpression** - This is used for regular expression searches to find a desired string in the log file. Searches are not case sensitive; however, a search cannot contain spaces.

Below is an example using the Scripts Arguments field to search for the number of newly found strings since the last script execution. In this case, just the new instances of the searched word, "error" is returned. In the returning message, this component returns all lines that match the search criteria divided by ";:

*d:\powertest.log,^error*

**Found String in # Position**

This monitor shows the number position of the string found from the end that matches the search criteria, as well as the string itself. By default, this counter also shows the last string.

This monitor uses the following arguments:

- **LogFilePath,RegularExpression,Position** where LogFilePath - This is the path of the target log file on the target server. The path cannot contain any spaces.
- **RegularExpression** - This is used for regular expression searches to find a desired string in the log file. Searches are not case sensitive; however, a search cannot contain spaces.
- **Position** - This value determines the position from the last string of the log file. By default, a value of 1 will return the last string found.

For example using the Scripts Arguments field which searches for the position of the word, "error" in relation to the end of the log file: *d:\powertest.log,^error,1*
Log Parser (Perl)

The Log Parser template allows you to check a specified log file and determine the total number of lines that match your search criteria.

Prerequisites

Perl must be installed on the target server.

Credentials

Root on target server.

Component Arguments and Syntax

These three arguments are used in the following order: perl ${SCRIPT} "LogFilePath" "RegularExpression" "Position"

1. Log file path – This is the path of the log file on the target server. The path can contain spaces, as opposed to the PowerShell template, which cannot.

2. Regular Expression – This is used for regular expression searches to find a desired string in the log file. Searches are case sensitive and can contain spaces, as opposed to the PowerShell template, which cannot.

3. Position – This value determines the position from the last string of the log file in the Found String in # Position monitor. For other monitors, this takes part in generating temp files.

For the Total Number of Strings Found and Number of Newly Found Strings monitors: If you monitor the same file but different search strings, use random values in the Position argument to generate different temp files.

Below is an example using the Command Line field used in the Number of Newly found strings component monitor. This example returns the number of newly found strings that match word init from the /etc/inittab file.

perl ${SCRIPT} "/etc/inittab" "init"

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Total Number of Strings Found

This monitor shows the total number of strings that match the search criteria in the entire log file. Additionally, in the message field, this monitor returns all strings that match search criteria.

Below is an example using the Command Line field:

perl ${SCRIPT} "/etc/inittab" "init" "0"
Number of Newly Found Strings

This monitor shows the number of newly found strings after the last script execution. Additionally in message field this monitor returns all strings that matches search criteria.

Below is an example using the Command Line field:
perl ${SCRIPT} "/etc/inittab" "init" "0"

Found String in # Position

This monitor shows the number position of the string found from the end that matches the search criteria, as well as the string itself. By default, this counter also shows the last string.

Below is an example using the Command Line field. The Position argument is employed as “1”.
perl ${SCRIPT} "/etc/inittab" "init" "1"
Lotus templates

The following templates are available:

- Lotus Domino Server Processes and Network Ports (Linux)
- Lotus Domino Server Processes and Network Ports (Windows)
- Lotus Domino Server Statistics
Lotus Domino Server Processes and Network Ports (Windows)

This template assesses the overall performance of Lotus Domino Server on Windows processes by using SNMP protocol.

**Prerequisites**

SNMP enabled on the operating system.

**Credentials**

None. The SNMP public string assigned to the node is used.

**Monitored Components**

For details on monitors, see [SAM Component Monitor Types](#).

Some components may not have preset warning or critical threshold values. You can add your own threshold limits as necessary.

**Process: Administrative Process**

This monitor returns CPU and memory usage of the Lotus Domino Administrative process, which performs many of the tedious and multi-step maintenance tasks in a Domino Domain (environment).

**Process: Agent Manager**

This monitor returns CPU and memory usage of the Lotus Domino Agent Manager process, which runs scheduled agents – usually multiple instances. The number of namgr tasks depends on the day vs. night settings in the server document.

**Process: Calendar Connector**

This monitor returns CPU and memory usage of the Lotus Domino Calendar Connector process. This process handles free-time requests from users/other servers for calendaring functionality for PIM functionality for user calendaring and reservations.

**Process: Event Monitor**

This monitor returns CPU and memory usage of the Lotus Domino Event Monitor process, which monitors the system for events to handle.

**Process: IMAP Server**

This monitor returns CPU and memory usage of the Lotus Domino IMAP Server process. This process provides the mail IMAP server for Domino that handles mail clients that use the IMAP format.
Process: LDAP Server
This monitor returns CPU and memory usage of the Lotus Domino LDAP server process. This process runs the Domino LDAP server on the administrative server for the Lotus Domain. This process is not usually run on other Domino servers.

Process: POP3 Server
This monitor returns CPU and memory usage of the Lotus Domino POP3 server process. This process provides the mail POP3 server for Domino that handles mail clients that use the POP3 format.

Process: Replicator
This monitor returns CPU and memory usage of the Lotus Domino Replicator process. This process replicates/syncs changes within the same applications between Domino servers. This process is needed if you have more than one Domino server.

Process: Router
This monitor returns CPU and memory usage of the Lotus Domino Router process used for sending NRPC mail.

Process: Schedule Manager
This monitor returns CPU and memory usage of the Lotus Domino Schedule Manager. This process performs schedule lookups for PIM (Personal Information Management) for user calendaring and reservations.

Process: Database Server
This monitor returns CPU and memory usage of the Lotus Domino Database Server process. This process provides core database services. There will be multiple threads handling this process and user/server connections.

Process: SMTP Server
This monitor returns CPU and memory usage of the Lotus Domino SMTP server process, which is used for Domino servers receiving SMTP mail from the Internet.

Process: Indexer
This monitor returns CPU and memory usage of the Lotus Domino Indexer process, which provides view index updates on the server.

Lotus Domino Server TCP port
This component monitor tests the ability of a Lotus Domino Server to accept incoming sessions. This port used for replication of Lotus Notes servers. Also, the Lotus Notes Client uses this port by default to communicate with the Lotus Notes server. By default, TCP port 1352 is used.

IMAP4 User Experience Monitor
This component monitor tests an email round trip from your SMTP mail server to your IMAP4 server and measures the time it takes to complete the trip.
POP3 User Experience Monitor

This component monitor tests an email round trip from your SMTP mail server to your POP3 mail server and measures the time it takes to complete the trip.

By default, this component is disabled. To use this component, you should enable it and properly configure it.
Lotus Domino Server Processes and Network Ports (Linux)

This template assesses the overall performance of a Lotus Domino Server on Linux processes by using the SNMP protocol.

**Prerequisites**

SNMP enabled on the operating system and permissions to monitor the following processes: nadminp, namgr, ncalconn, nevent, nimap, nldap, npop3, nreplica, nrouter, nrouter, nserver, nsmtp, nupdate.

**Credentials**

None. The SNMP public string assigned to the node is used.

**Monitored Components**

For details on monitors, see [SAM Component Monitor Types](#).

Some components may not have preset warning or critical threshold values. You can add your own threshold limits as necessary.

**Process: Administrative Process**

This monitor returns CPU and memory usage of the Lotus Domino Administrative process, which performs many of the tedious and multi-step maintenance tasks in a Domino Domain (environment).

**Process: Agent Manager**

This monitor returns CPU and memory usage of the Lotus Domino Agent Manager process, which runs scheduled agents, (usually multiple instances). The number of namgr tasks depends on the day vs. night settings in the server document.

**Process: Calendar Connector**

This monitor returns CPU and memory usage of the Lotus Domino Calendar Connector process. This process handles free-time requests from users/other servers used for calendaring functionality for PIM functionality for user calendaring and reservations.

**Process: Event Monitor**

This monitor returns CPU and memory usage of the Lotus Domino Event Monitor process, which monitors the system for events to handle.

**Process: IMAP Server**

This monitor returns CPU and memory usage of the Lotus Domino IMAP server process. This process provides the mail IMAP server for Domino that handles mail clients that use the IMAP format.
Process: LDAP Server

This monitor returns CPU and memory usage of the Lotus Domino LDAP server process. This process runs the Domino LDAP server on the administrative server for the Lotus Domain. This is not usually run on other Domino servers.

Process: POP3 Server

This monitor returns CPU and memory usage of the Lotus Domino POP3 server process. This process provides the mail POP3 server for Domino that handles mail clients that use the POP3 format.

Process: Replicator

This monitor returns CPU and memory usage of the Lotus Domino Replicator process. This process replicates/syncs changes within the same applications between Domino servers. This is needed if you have more than one Domino server.

Process: Router

This monitor returns CPU and memory usage of the Lotus Domino Router process used for sending NRPC mail.

Process: Schedule Manager

This monitor returns CPU and memory usage of the Lotus Domino Schedule Manager, which performs schedule lookups for PIM (Personal Information Management) for user calendaring and reservations.

Process: Database Server

This monitor returns CPU and memory usage of the Lotus Domino Database Server process, which provides core database services. There will be multiple threads handling this process and user/server connections.

Process: SMTP Server

This monitor returns CPU and memory usage of the Lotus Domino SMTP server process, which is used for Domino servers receiving SMTP mail from Internet.

Process: Indexer

This monitor returns CPU and memory usage of the Lotus Domino Indexer process, which provides view index updates on the server.

Lotus Domino Server TCP port

This component monitor tests the ability of a Lotus Domino Server to accept incoming sessions. This port used for the replication of Lotus Notes servers. Also, the Lotus Notes Client uses this port by default to communicate with the Lotus Notes server. By default, TCP port 1352 is used.

IMAP4 User Experience Monitor

This component monitor tests an email round trip from your SMTP mail server to your IMAP4 server and measures the time it takes to complete the trip.
By default, this component is disabled. To use this component, you should enable it and properly configure it.

**POP3 User Experience Monitor**

This component monitor tests an email round trip from your SMTP mail server to your POP3 mail server and measures the time it takes to complete the trip.

By default, this component is disabled. To use this component, you should enable it and properly configure it.
Lotus Domino Server Statistics

This template assesses the overall performance of a Lotus Domino Server by using the SNMP protocol.

Prerequisites

SNMP enabled on the operating system. SNMP adapter enabled on Lotus Domino.

Credentials

None. The SNMP public string assigned to the node is used.

To enable the SNMP adapter on Lotus Domino, navigate here:

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Some components may not have preset warning or critical threshold values. You can add your own threshold limits as necessary.

Available Resources (%)

This monitor returns the current percentage index of a server's availability. The value range is 0-100. Zero (0) indicates no available resources. A value of 100 indicates that the server is completely available.

OID: 1.3.6.1.4.1.334.72.1.1.6.3.19.0

Open User Sessions

This monitor returns the number of users with sessions open on the server.

OID: 1.3.6.1.4.1.334.72.1.1.6.3.6.0

Peak Open User Sessions

This monitor returns the peak number of concurrent users with open sessions since the server was started.

OID: 1.3.6.1.4.1.334.72.1.1.6.3.11.0

Dropped Session Count

This monitor returns the number of dropped sessions.

OID: 1.3.6.1.4.1.334.72.1.1.6.3.1.0
**DB Cache Rejection Count**

This monitor returns the number of times a database is not placed into the cache when it is closed because InDBCacheCurrentEntries equals or exceeds InDBCacheMaxEntries*1.5. This number should stay low. If this number begins to rise, you should increase the NSF_DbCache_Maxentries settings.

OID: 1.3.6.1.4.1.334.72.1.1.10.21.0

**LDAP Tasks Running**

This monitor returns the number of LDAP server tasks currently running.

OID: 1.3.6.1.4.1.334.72.1.1.21.10.0

**Peak Transactions per Minute**

This monitor returns the peak number of transactions that took place in any given minute since the server was started.

OID: 1.3.6.1.4.1.334.72.1.1.6.3.3.0

**Max Mail Delivery Time (sec)**

This monitor returns the maximum time for mail delivery in seconds.

OID: 1.3.6.1.4.1.334.72.1.1.4.12.0

Note: If the counter returns with the error “No such name,” you should send a test email. The counter should be accessible at this point.

**Pending Mail Messages**

This monitor returns the number of mail messages pending.

OID: 1.3.6.1.4.1.334.72.1.1.4.31.0

Note: If the counter returns with the error “No such name,” you should send a test email. The counter should be accessible at this point.

**Server Transactions per Minute**

This monitor returns the average number of transactions per minute since the server was started.

OID: 1.3.6.1.4.1.334.72.1.1.6.3.2.0

**Number of Undeliverable Messages**

This monitor returns the number of dead (undeliverable) mail messages.

OID: 1.3.6.1.4.1.334.72.1.1.4.1.0

**Total Mail Failures**

This monitor returns the total number of routing failures since the server started.

OID: 1.3.6.1.4.1.334.72.1.1.4.3.0
Note: If the counter returns with the error “No such name,” you should send a test email. The counter should be accessible at this point.

**Number of Waiting Messages**

This monitor returns the number of mail messages waiting to be routed.

OID: 1.3.6.1.4.1.334.72.1.1.4.6.0

**Number of Messages on Hold**

This monitor returns the number of mail messages in message queue on hold.

OID: 1.3.6.1.4.1.334.72.1.1.4.21.0

**Database Cache Hit**

This monitor returns the number of times an lnDBCacheInitialDbOpen is satisfied by finding a database in the cache. A high “hits-to-opens” ratio indicates the database cache is working effectively, since most users are opening databases in the cache without having to wait for the usual time required by an initial (non-cache) open. If the ratio is low, the administrator can increase the NSF_DBCACHE_MAXENTRIES settings.

OID: 1.3.6.1.4.1.334.72.1.1.10.17.0

**Database Initial Opens**

This monitor returns the number of times a user/server opened a database that was not already being used by another user/server. By comparing this number to lnDBCacheHits, administrators can gauge the effectiveness of the cache.

OID: 1.3.6.1.4.1.334.72.1.1.10.18.0

**Access Denial of Agent Manager**

This monitor returns the number of times the agent manager failed to execute a given task, probably due to ACL restrictions.

OID: 1.3.6.1.4.1.334.72.1.1.11.1.0

---

If the counter returns with the error “No such name,” you should send a test email. The counter should be accessible at this point.

---

**Unsuccessful Runs of Agent Manager**

This monitor returns the number of tasks the agent manager has unsuccessfully run during the course of the day.

OID: 1.3.6.1.4.1.334.72.1.1.11.4.0

---

If the counter returns with the error “No such name,” you should send a test email. The counter should be accessible at this point.
MAPI Round Trip Email

This template simulates an email round trip to test the ability of your SMTP server to receive and distribute email, and the ability of your users to retrieve messages from MAPI-enabled email clients.

MAPI Profiles created manually or automatically are created in the context of the user whose credentials have been defined as part of the component monitor.

For example: If you have assigned the "John Doe" credentials to this MAPI User Experience Monitor, then John Doe must be able to log in locally to the SAM server so a MAPI profile can be created.

Prerequisites

MAPI access to a Microsoft Exchange server. MAPI Client and CDO Objects installed on the SAM server.

Credentials

Windows credential valid on both the SAM server and the Microsoft Exchange server.

You cannot monitor POP3-based Google Gmail accounts with this template. Use the template instead.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

MAPI User Experience Monitor

This component monitor sends an email from your SMTP mail server to your Microsoft Exchange Server Mailbox and measures the time it takes to complete the trip. You can use this component monitor to monitor the performance of Outlook. This response time is measured in milliseconds.

The Exchange Server computer uses port 135 for client connections to the RPC endpoint mapper service. After a client connects to a socket, the Exchange Server computer allocates the client two random ports to use to communicate with the directory and the information store.

It is recommended that you log into the SAM server console locally as the user whose credentials you have assigned to the MAPI User Experience Monitor. From here, use MFCMapi.exe (http://mfcmapi.codeplex.com/) to verify the profile defined in the monitor actually exists. If it does not, you can either manually create the MAPI profile under this users context, or delete all existing MAPI profiles and MAPI UX monitors and recreate the monitor, which should then automatically create the profile.
Memcached

This template allows you to monitor the performance of Memcached installed on a Linux machine by using Perl scripts.

This template was created on Memcached version 1.4.13.

Prerequisites

SSH and Perl installed on the target server. SNMP installed on the target server and permission to monitor the memcached process.

Credentials

User under which Memcached was installed.

Each Linux/Unix monitor uses the same argument structure. For example: perl ${SCRIPT} 11211

where:

11211 – TCP port used by memcached.

- You must specify the correct arguments for each monitored component in the Script Arguments field. If you fail to do this, the monitor will return with a status error of "Undefined."
- On some Linux distributions, there is no "nc" command. The "netcat" command is used instead. This can result in a situation where all the components except "Memcached TCP Port Monitor" and "Process: memcached" show "Fail" with the following error: "nc not found." In some cases, you may need to change "nc" to "netcat" to avoid this error.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

General statistic

This monitor returns general statistics. The returned values are as follows:

- **Used threads** – This component returns the number of worker threads requested.
- **Current connections** – This component returns the number of opened connections.
- **Total connections** – This component returns the total number of connections opened since the server started running.
- **Connection structures** – This component returns the number of internal connection handles currently held by the server. Compare this monitor to Current connections. Memcached should have about 10% more Connection structures than Current connections.
- **Current items** – This component returns the current number of items currently stored.
- **Total items** – This component returns the total number of items stored since the server started.
- **Used for caching MB** – This component returns the current number of MB to store items.
- **Evictions** – This component returns the number of valid items removed from the cache to free memory for new items. This value should be zero at all times.
- **Denied connections** – This component returns the number of denied connection attempts because Memcached reached its configured connection limit. This monitor should zero at all times.
- **Memcache cache usage ratio %** – This component returns the cache usage ratio. It is calculated by the following formula: used_for_caching*(limit_maxbytes/100.0). This value should be as low as possible.

**Requests**

This monitor returns the requests statistic. The returned value are as follows:

- **Retrieval requests** – This component returns the cumulative number of retrieval requests.
- **Storage requests** – This component returns the cumulative number of storage requests.
- **Flush requests** – This component returns the cumulative number of flush requests.
- **Touch requests** – This component returns the cumulative number of touch requests.

1. By default, this monitor has the Count statistic as difference box checked. It will show the total number of requests in the Message field while the Statistic field will only show the new number of requests since the last polling period.

**Operations statistic**

This monitor returns the operations statistic. The returned values are as follows:

- **Get hits** – This component returns the number of keys that have been requested and found to be present.
- **Get misses** – This component returns the number of items that have been requested and not found to be present.
- **Delete hits** – This component returns the number of deletion requests resulting in an item being removed.
- **Delete misses** – This component returns the number of deletion requests for missing keys.
- **Incremental hits** – This component returns the number of successful incremental requests. Incremental is a replace adding one to the stored value and failing if no value is stored.
- **Incremental misses** – This component returns the number of incremental requests against missing keys. Incremental is a replace adding one to the stored value and failing if no value is stored.
- **Decremental hits** – This component returns the number of successful decremental requests. The decremental command decreases a stored (integer) value by one.
- **Decremental misses** – This component returns the number of decremental requests against missing keys. The decremental command decreases a stored (integer) value by one.
- **CAS hits** – This component returns the number of successful CAS requests. The CAS command is Memcached’s anti-locking command.
• **CAS misses** – This component returns the number of CAS requests against missing keys. The CAS command is Memcached’s anti-locking command.

By default, this monitor has the **Count statistic as difference box** checked. It will show the total number of requests in the Message field while the Statistic field will show only new number of requests since the last polling period.

**Operations ratio**

This monitor returns the operations ratio statistic. The returned values are as follows:

- **Get hit ratio %** – This component returns the get hit ratio. It is calculated by the following formula: \( \text{get\_hits}/(\text{get\_hits}+\text{get\_misses}) \times 100.0 \). This value should be as high as possible.

- **Delete hit ratio %** – This component returns the delete hit ratio. It is calculated by the following formula: \( \text{delete\_hits}/(\text{delete\_hits}+\text{delete\_misses}) \times 100.0 \). This value should be as high as possible.

- **Incremental hit ratio %** – This component returns the incremental hit ratio. Incremental is a replace adding one to the stored value and failing if no value is stored. It is calculated by the following formula: \( \text{incr\_hits}/(\text{incr\_hits}+\text{incr\_misses}) \times 100.0 \). This value should be as high as possible.

- **Decremental hit ratio %** – This component returns the decremental hit ratio. The decremental command decreases a stored (integer) value by one. It is calculated by the following formula: \( \text{decr\_hits}/(\text{decr\_hits}+\text{decr\_misses}) \times 100.0 \). This value should be as high as possible.

- **CAS hit ratio %** – This component returns the CAS hit ratio. The CAS command is Memcached’s anti-locking command. It is calculated by the following formula: \( \text{cas\_hits}/(\text{cas\_hits}+\text{cas\_misses}) \times 100.0 \). This value should be as high as possible.

**Network statistic**

This monitor returns network statistics. The returned values are as follows:

- **Received kB** – This component returns the total number of kBs received from the network by this server.

- **Sent kB** – This component returns the total number of kBs sent to the network by this server.

By default, this monitor has the Count statistic as difference box checked. It will show the total number of kB in the Message field while the Statistic field will show only new number of kBs since the last polling period.

**Slabs statistic**

This monitor returns slabs statistics. The returned values are as follows:

- **Active slab classes** – This component returns the total number of slab classes allocated.

- **Allocated memory to slab pages** – This component returns the total amount of memory allocated to slab pages.
Memcached TCP Port Monitor

This component monitor tests the ability of a memcached service to accept incoming sessions. By default, it monitors TCP port 11211.

Process: memcached

This monitor returns CPU and memory usage of the memcached server process.
Active Directory

The following templates are available:

- Active Directory 2003-2008 Services and Counters
- Active Directory 2008 R2-2012 Services and Counters
- Active Directory 2016 Domain Controller Security
- Active Directory 2016 Services and Counters

See also AppInsight for Active Directory.

Periodically, SolarWinds releases SAM templates to support the latest product versions such as Microsoft Server 2016. You can continue using templates for older product versions, but updating to the latest template is recommended.
Active Directory 2003-2008 Services and Counters

This template assesses the overall health of Active Directory 2003—2008 services and counters on a domain controller. It is recommended to use this template in conjunction with the Windows Server 2003—2008 Services and Counters template.

Prerequisites

RPC and WMI access to the domain controller.

Credentials

Windows Administrator on the domain controller.

Periodically, SolarWinds releases SAM templates to support the latest product versions such as Microsoft Server 2016. You can continue using templates for older product versions, but updating to the latest template is recommended.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Components without predetermined threshold values have guidance such as "use the lowest threshold possible" or "use the highest threshold possible" to help you find a threshold appropriate for your application.

Service: Distributed File System

Enables you to group shared folders located on different servers into one or more logically structured namespaces. Each namespace appears to users as a single shared folder with a series of subfolders.

Service: DNS Server

Enables DNS clients to resolve DNS names by answering DNS queries and dynamic DNS update requests. If this service is stopped, DNS updates will not occur. If this service is disabled, any services that explicitly depend on it will fail to start.

Service: File Replication

Synchronizes folders with file servers that use File Replication Service (FRS) instead of the newer DFS Replication technology.

Service: Intersite Messaging

Enables messages to be exchanged between computers running Windows Server sites. If this service is stopped, messages will not be exchanged, nor will site routing information be calculated for other services. If this service is disabled, any services that explicitly depend on it will fail to start.
Service: Kerberos Key Distribution Center

On domain controllers, this service enables users to log on to the network using the Kerberos authentication protocol. If this service is stopped on a domain controller, users will be unable to log on to the network. If this service is disabled, any services that explicitly depend on it will fail to start.

Service: Windows Time

Maintains date and time synchronization on all clients and servers in the network. If this service is stopped, date and time synchronization will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

Service: DNS Client

The DNS Client service (dnscache) caches Domain Name System (DNS) names and registers the full computer name for this computer. If the service is stopped, DNS names will continue to be resolved. However, the results of DNS name queries will not be cached and the computer's name will not be registered. If the service is disabled, any services that explicitly depend on it will fail to start.

Service: Security Accounts Manager

The startup of this service signals other services that the Security Accounts Manager (SAM) is ready to accept requests. Disabling this service will prevent other services in the system from being notified when the SAM is ready, which may in turn cause those services to fail to start correctly. This service should not be disabled.

Service: Server

Supports file, print, and named-pipe sharing over the network for this computer. If this service is stopped, these functions will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

Service: Workstation

Creates and maintains client network connections to remote servers using the SMB protocol. If this service is stopped, these connections will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

Service: Remote Procedure Call (RPC)

The RPCSS service is the Service Control Manager for COM and DCOM servers. It performs object activation requests, object exporter resolutions, and distributed garbage collection for COM and DCOM servers. If this service is stopped or disabled, programs using COM or DCOM will not function properly. It is strongly recommended that you have the RPCSS service running.

Service: Net Logon

Maintains a secure channel between this computer and the domain controller for authenticating users and services. If this service is stopped, the computer may not authenticate users and services, and the domain controller cannot register DNS records. If this service is disabled, any services that explicitly depend on it will fail to start.

LDAP Active Threads

The current number of threads in use by the LDAP subsystem of the local directory service.
You can provide a value for the warning and critical thresholds based on your current environment and your requirements.

**LDAP Bind Time**

The time (in milliseconds) required for the completion of the last successful LDAP binding. This counter should be as low as possible. If it is not, it usually indicates that hardware or network-related problems are occurring.

**LDAP Client Sessions**

The number of currently connected LDAP client sessions. This counter should show activity over time. If it does not, it usually indicates that network-related problems are occurring.

You can provide a value for the warning and critical thresholds based on your current environment and your requirements.

**Directory Service Threads in Use**

The current number of threads in use by the directory service. This counter should show activity over time. If it does not, it usually indicates that network problems are hindering client requests.

You can provide a value for the warning and critical thresholds based on your current environment and your requirements.

**Address Book Client Sessions**

The number of connected Address Book client sessions.

**Directory Service Notify Queue Size**

The number of pending update notifications that are queued, but not yet transmitted to clients.

This counter should be as low as possible.

**DRA Inbound Full Sync Objects Remaining**

The number of objects remaining until the full synchronization is completed (while replication is done).

This counter should be as low as possible.

**DRA Inbound Values (DNs only)/sec**

The number of object property values received from inbound replication partners that are distinguished names (DNs) that reference other objects. DN values, such as group or distribution list memberships, are generally more expensive to apply than other types of values.
DRA Outbound Values (DNs only)/sec
- The number of object property values containing DNs sent to outbound replication partners. DN values, such as group or distribution list memberships, are generally more expensive to read than other kinds of values.

LDAP Successful Binds/sec
- The number of LDAP bindings (per second) that occurred successfully.
- This counter should show activity over time. If it does not, it usually indicates that network-related problems are occurring.

LDAP Searches/sec
- The number of search operations per second performed by LDAP clients.
- This counter should show activity over time. If it does not, it usually indicates that network problems are hindering client requests.

DS Directory Reads/sec
- The number of directory reads per second.

DS Directory Writes/sec
- The number of directory writes per second.

DRA Pending Replication Synchronizations
- The number of directory synchronizations that are queued for this server but not yet processed.

Replication: Change Orders Received
- The number of change orders received. In an idle state this counter should be zero.

Replication: Change Orders Sent
- The number of change orders sent. In an idle state this counter should be zero.

Replication: Usn Records Accepted
- The number of USN records accepted. Replication is triggered by entries to the NTFS USN journal. A high value on this counter, such as one every five seconds, indicates heavy replication traffic and may result in replication latency.

System: Context Switches/sec
- Used to determine whether or not the processor must handle too many applications.
Interpret the data cautiously. A thread that is heavily using the processor lowers the rate of context switches, because it does not allow much processor time for other processes' threads. A high rate of context switching means that the processor is being shared repeatedly—for example, by many threads of equal priority. It is a good practice to minimize the context switching rate by reducing the number of active threads on the system. The use of thread pooling, I/O completion ports, and asynchronous I/O can reduce the number of active threads. Consult your in-house developers or application vendors to determine if the applications you are running provide tuning features that include limiting the number of threads.

A context switching rate of 300 per second per processor is a moderate amount; a rate of 1000 per second or more is high. Values at this high level may be a problem.

You can provide a value for the warning and critical thresholds based on your current environment and your requirements.

**System: Processor Queue Length**

Indicates if the system is able to handle processing requests.

This counter is a rough indicator of the number of threads each processor is servicing. The processor queue length, sometimes called processor queue depth, reported by this counter is an instantaneous value that is representative only of a current snapshot of the processor, so it is necessary to observe this counter over a long period of time. Also this counter is reporting a total queue length for all processors, not a length per processor. For additional information on how to monitor this counter, refer to the following article: [http://technet.microsoft.com/en-us/library/cc938643.aspx](http://technet.microsoft.com/en-us/library/cc938643.aspx).
Active Directory 2008 R2-2012 Services and Counters

This template assesses the overall health of Active Directory 2008 R2 - 2012 services and counters on a domain controller. It is recommended to use this template in conjunction with the Windows Server 2003 - 2012 Services and Counters template.

Prerequisites

RPC and WMI access to the domain controller.

Credentials

Windows Administrator on the domain controller.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Components without predetermined threshold values provide guidance such as "use the lowest threshold possible" or "use the highest threshold possible" to help you find a threshold appropriate for your application.

Service: Distributed File System

Enables you to group shared folders located on different servers into one or more logically structured namespaces. Each namespace appears to users as a single shared folder with a series of subfolders.

Service: DNS Server

Enables DNS clients to resolve DNS names by answering DNS queries and dynamic DNS update requests. If this service is stopped, DNS updates will not occur. If this service is disabled, any services that explicitly depend on it will fail to start.

Service: DFS Replication

Enables you to synchronize folders on multiple servers across local or wide area network (WAN) network connections. This service uses the Remote Differential Compression (RDC) protocol to update only the portions of files that have changed since the last replication.

Service: Intersite Messaging

Enables messages to be exchanged between computers running Windows Server sites. If this service is stopped, messages will not be exchanged, nor will site routing information be calculated for other services. If this service is disabled, any services that explicitly depend on it will fail to start.
**Service: Kerberos Key Distribution Center**

On domain controllers, this service enables users to log on to the network using the Kerberos authentication protocol. If this service is stopped on a domain controller, users will be unable to log on to the network. If this service is disabled, any services that explicitly depend on it will fail to start.

**Service: Windows Time**

Maintains date and time synchronization on all clients and servers in the network. If this service is stopped, date and time synchronization will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

**Service: DNS Client**

The DNS Client service (dnscache) caches Domain Name System (DNS) names and registers the full computer name for this computer. If the service is stopped, DNS names will continue to be resolved. However, the results of DNS name queries will not be cached and the computer's name will not be registered. If the service is disabled, any services that explicitly depend on it will fail to start.

**Service: Security Accounts Manager**

The startup of this service signals other services that the Security Accounts Manager (SAM) is ready to accept requests. Disabling this service will prevent other services in the system from being notified when the SAM is ready, which may in turn cause those services to fail to start correctly. This service should not be disabled.

**Service: Server**

Supports file, print, and named-pipe sharing over the network for this computer. If this service is stopped, these functions will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

**Service: Workstation**

Creates and maintains client network connections to remote servers using the SMB protocol. If this service is stopped, these connections will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

**Service: Remote Procedure Call (RPC)**

The RPCSS service is the Service Control Manager for COM and DCOM servers. It performs object activation requests, object exporter resolutions, and distributed garbage collection for COM and DCOM servers. If this service is stopped or disabled, programs using COM or DCOM will not function properly. It is strongly recommended that you have the RPCSS service running.

**Service: Net Logon**

Maintains a secure channel between this computer and the domain controller for authenticating users and services. If this service is stopped, the computer may not authenticate users and services, and the domain controller cannot register DNS records. If this service is disabled, any services that explicitly depend on it will fail to start.

**LDAP Active Threads**

The current number of threads in use by the LDAP subsystem of the local directory service.
You can provide a value for the warning and critical thresholds based on your current environment and your requirements.

**LDAP Bind Time**

The time (in milliseconds) required for the completion of the last successful LDAP binding.

This counter should be as low as possible. If it is not, it usually indicates that hardware or network-related problems are occurring.

**LDAP Client Sessions**

The number of currently connected LDAP client sessions.

This counter should show activity over time. If it does not, it usually indicates that network-related problems are occurring.

You can provide a value for the warning and critical thresholds based on your current environment and your requirements.

**Directory Service Threads in Use**

The current number of threads in use by the directory service.

This counter should show activity over time. If it does not, it usually indicates that network problems are hindering client requests.

You can provide a value for the warning and critical thresholds based on your current environment and your requirements.

**Address Book Client Sessions**

The number of connected Address Book client sessions.

**Directory Service Notify Queue Size**

The number of pending update notifications that are queued, but not yet transmitted to clients.

This counter should be as low as possible.

**DRA Inbound Full Sync Objects Remaining**

The number of objects remaining until the full synchronization is completed (while replication is done).

This counter should be as low as possible.

**DRA Inbound Values (DNs only)/sec**

The number of object property values received from inbound replication partners that are distinguished names (DNs) that reference other objects. DN values, such as group or distribution list memberships, are generally more expensive to apply than other types of values.
DRA Outbound Values (DNs only)/sec

The number of object property values containing DNs sent to outbound replication partners. DN values, such as group or distribution list memberships, are generally more expensive to read than other kinds of values.

DS Threads in Use

Indicates the current number of threads in use by the directory service.

LDAP Successful Binds/sec

The number of LDAP bindings (per second) that occurred successfully. This counter should show activity over time. If it does not, it usually indicates that network-related problems are occurring.

LDAP Searches/sec

The number of search operations per second performed by LDAP clients. This counter should show activity over time. If it does not, it usually indicates that network problems are hindering client requests.

DS Directory Reads/sec

The number of directory reads per second.

DS Directory Writes/sec

The number of directory writes per second.

DRA Pending Replication Synchronizations

The number of directory synchronizations that are queued for this server but not yet processed.

System: Context Switches/sec

Used to determine whether or not the processor must handle an excessive amount of applications. Interpret this data cautiously. A thread that is heavily using the processor lowers the rate of context switches because it does not allow much processor time for other process threads. A high rate of context switching means that the processor is being shared repeatedly—for example, by many threads of equal priority. It is a good practice to minimize the context switching rate by reducing the number of active threads on the system. The use of thread pooling, I/O completion ports, and asynchronous I/O can reduce the number of active threads. Consult your in-house developers or application vendors to determine if the applications you are running provide tuning features that include limiting the number of threads.

A context switching rate of 300 per second per processor is a moderate amount; a rate of 1000 per second or more is high. Values at this high level may be a problem.

You can provide a value for the warning and critical thresholds based on your current environment and your requirements.
System: Processor Queue Length

Indicates if the system is able to handle processing requests.

This counter is a rough indicator of the number of threads each processor is servicing. The processor queue length, sometimes called processor queue depth, reported by this counter is an instantaneous value that is representative only of a current snapshot of the processor, so it is necessary to observe this counter over a long period of time. Also this counter is reporting a total queue length for all processors, not a length per processor. For additional information on how to monitor this counter, refer to the following article: http://technet.microsoft.com/en-us/library/cc938643.aspx.

Service: Active Directory Domain Services

This is a core AD DS Domain Controller service. If this service is stopped, users will be unable to log on to the network. If this service is disabled, any services that explicitly depend on it will fail to start.

Service: Active Directory Web Services

This service provides a Web Service interface to instances of the directory service (AD DS and AD LDS) that are running locally on this server. If this service is stopped or disabled, client applications, such as Active Directory PowerShell, will not be able to access or manage any directory service instances that are running locally on this server.

Active Directory 2016 Domain Controller Security

Use this template to check locked, disabled users, and events from Windows security log related to Windows 2016 Domain Controller security.

Prerequisites

WinRM must be installed and properly configured on the target server

WMI access to the target server

Enable audit on domain controller (success and failure) for Account Management, Logon Events, Policy Changes, and System Events

Credentials

Windows Administrator on the target server

All monitors (except “Locked out users” and “Disabled users”) should return zero values. Returned values other than zero may indicate an abnormality, but not always. Examine the Windows security log file for details.

For a list of Component Monitors included in this template, select the template on the Manage Templates page and click Edit.
Periodically, SolarWinds releases SAM templates to support the latest product versions such as Microsoft Server 2016. You can continue using templates for older product versions, but updating to the latest template is recommended.

Active Directory 2016 Services and Counters

This template assesses the overall health of Active Directory 2016 services and counters on a domain controller. It is recommended to use this template in conjunction with the Windows Server 2016 Services and Counters template.

Prerequisites

RPC and WMI access to the domain controller.

Credentials

Windows Administrator on the domain controller.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Components without predetermined threshold values have guidance such as "use the lowest threshold possible" or "use the highest threshold possible" to help you find a threshold appropriate for your application.

Service: Distributed File System

Enables you to group shared folders located on different servers into one or more logically structured namespaces. Each namespace appears to users as a single shared folder with a series of subfolders.

Service: DNS Server

Enables DNS clients to resolve DNS names by answering DNS queries and dynamic DNS update requests. If this service is stopped, DNS updates will not occur. If this service is disabled, any services that explicitly depend on it will fail to start.

Service: DFS Replication

Synchronizes folders with file servers that use Distributed File System (DFS) technology.
Service: Intersite Messaging

Enables messages to be exchanged between computers running Windows Server sites. If this service is stopped, messages will not be exchanged, nor will site routing information be calculated for other services. If this service is disabled, any services that explicitly depend on it will fail to start.

Service: Kerberos Key Distribution Center

On domain controllers, this service enables users to log on to the network using the Kerberos authentication protocol. If this service is stopped on a domain controller, users will be unable to log on to the network. If this service is disabled, any services that explicitly depend on it will fail to start.

Service: Windows Time

Maintains date and time synchronization on all clients and servers in the network. If this service is stopped, date and time synchronization will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

Service: DNS Client

The DNS Client service (dnscache) caches Domain Name System (DNS) names and registers the full computer name for this computer. If the service is stopped, DNS names will continue to be resolved. However, the results of DNS name queries will not be cached and the computer’s name will not be registered. If the service is disabled, any services that explicitly depend on it will fail to start.

Service: Security Accounts Manager

The startup of this service signals other services that the Security Accounts Manager (SAM) is ready to accept requests. Disabling this service will prevent other services in the system from being notified when the SAM is ready, which may in turn cause those services to fail to start correctly. This service should not be disabled.

Service: Server

Supports file, print, and named-pipe sharing over the network for this computer. If this service is stopped, these functions will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

Service: Workstation

Creates and maintains client network connections to remote servers using the SMB protocol. If this service is stopped, these connections will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

Service: Remote Procedure Call (RPC)

The RPCSS service is the Service Control Manager for COM and DCOM servers. It performs object activation requests, object exporter resolutions, and distributed garbage collection for COM and DCOM servers. If this service is stopped or disabled, programs using COM or DCOM will not function properly. It is strongly recommended that you have the RPCSS service running.
Service: Net Logon

Maintains a secure channel between this computer and the domain controller for authenticating users and services. If this service is stopped, the computer may not authenticate users and services, and the domain controller cannot register DNS records. If this service is disabled, any services that explicitly depend on it will fail to start.

LDAP Active Threads

The current number of threads in use by the LDAP subsystem of the local directory service.

ℹ️ You can provide a value for the warning and critical thresholds based on your current environment and your requirements.

LDAP Bind Time

The time (in milliseconds) required for the completion of the last successful LDAP binding.

This counter should be as low as possible. If it is not, it usually indicates that hardware or network-related problems are occurring.

LDAP Client Sessions

The number of currently connected LDAP client sessions.

This counter should show activity over time. If it does not, it usually indicates that network-related problems are occurring.

ℹ️ You can provide a value for the warning and critical thresholds based on your current environment and your requirements.

Directory Service Threads in Use

The current number of threads in use by the directory service.

This counter should show activity over time. If it does not, it usually indicates that network problems are hindering client requests.

ℹ️ You can provide a value for the warning and critical thresholds based on your current environment and your requirements.

Address Book Client Sessions

The number of connected Address Book client sessions.

Directory Service Notify Queue Size

The number of pending update notifications that are queued, but not yet transmitted to clients.

ℹ️ This counter should be as low as possible.

DRA Inbound Full Sync Objects Remaining

The number of objects remaining until the full synchronization is completed (while replication is done).
This counter should be as low as possible.

**DRA Inbound Values (DNs only)/sec**

The number of object property values received from inbound replication partners that are distinguished names (DNs) that reference other objects. DN values, such as group or distribution list memberships, are generally more expensive to apply than other types of values.

**DRA Outbound Values (DNs only)/sec**

The number of object property values containing DN values sent to outbound replication partners. DN values, such as group or distribution list memberships, are generally more expensive to read than other kinds of values.

**LDAP Successful Binds/sec**

The number of LDAP bindings (per second) that occurred successfully.

This counter should show activity over time. If it does not, it usually indicates that network-related problems are occurring.

**LDAP Searches/sec**

The number of search operations per second performed by LDAP clients.

This counter should show activity over time. If it does not, it usually indicates that network problems are hindering client requests.

**DS Directory Reads/sec**

The number of directory reads per second.

**DS Directory Writes/sec**

The number of directory writes per second.

**DRA Pending Replication Synchronizations**

The number of directory synchronizations that are queued for this server but not yet processed.

**System: Context Switches/sec**

Used to determine whether or not the processor must handle too many applications.

Interpret the data cautiously. A thread that is heavily using the processor lowers the rate of context switches, because it does not allow much processor time for other processes' threads. A high rate of context switching means that the processor is being shared repeatedly-for example, by many threads of equal priority. It is a good practice to minimize the context switching rate by reducing the number of active threads on the system. The use of thread pooling, I/O completion ports, and asynchronous I/O can reduce the number of active threads. Consult your in-house developers or application vendors to determine if the applications you are running provide tuning features that include limiting the number of threads.

A context switching rate of 300 per second per processor is a moderate amount; a rate of 1000 per second or more is high. Values at this high level may be a problem.
System: Processor Queue Length

Indicates if the system is able to handle processing requests.

This counter is a rough indicator of the number of threads each processor is servicing. The processor queue length, sometimes called processor queue depth, reported by this counter is an instantaneous value that is representative only of a current snapshot of the processor, so it is necessary to observe this counter over a long period of time. Also this counter is reporting a total queue length for all processors, not a length per processor. For additional information on how to monitor this counter, refer to the following article: http://technet.microsoft.com/en-us/library/cc938643.aspx.

Service: Active Directory Domain Services

This is a core AD DS Domain Controller service. If this service stops, users cannot log on to the network. If this service is disabled, any services that explicitly depend on it will fail to start.

Service: Active Directory Web Servers

This service provides a Web Service interface to instances of the directory service (AD DS and AD LDS) that run locally on this server. If this service is stopped or disabled, client applications, such as Active Directory PowerShell, cannot access or manage any directory service instances running locally on this server.

Events: Machine Account Authentication Failure

This monitor returns the number of events that indicate a machine account failed to authenticate, which is usually caused by either multiple instances of the same computer name, or the computer name was not replicated to every domain controller.

If you do not find multiple instances of the computer name, verify that replication is functioning for the domain that contains the computer account.

Events: Replicate Duplicate Object Found

This monitor returns the number of events that indicate a duplicate object is present in the Active Directory of the replication partner of the local domain controller, so updating it is impossible.

Events: Failed Replication

This monitor returns the number of events that indicate replication failed for the reason stated in the message text.

Use Repadmin.exe to further identify the problem, and use Table x.x to determine the appropriate action to take for the message generated by Repadmin.exe. If the event message indicates that the target account name is incorrect, troubleshoot GUID discrepancies. If the event message indicates a time difference between the client and server, synchronize replication from the PDC emulator.
Events: Replication Configuration Does Not Reflect Topology

This monitor returns the number of events that occur when the replication configuration information in Active Directory Sites and Services does not accurately reflect the physical topology of the network.

Events: Lingering Objects Disconnection Error

This monitor returns the number of events usually generated by a lingering object which resulted from disconnecting a domain controller for too long.

If the domain controller does not also function as a global catalog server, see "Remove Lingering Objects from an Outdated Writable Domain Controller" on http://technet.microsoft.com. If the domain controller also functions as a global catalog server, see "Remove Lingering Objects from a Global Catalog Server."

Events: Replication Link GUID Mismatch

This monitor returns the number of events that occur over an existing replication link when the GUID of the NTDS Settings object of a replication partner does not match the GUID defined in the Service Principal Name (SPN) attributes of the computer object of this replication partner. Troubleshoot GUID discrepancies as necessary.

Events: User Account Cannot Be Resolved

This monitor returns the number of events that indicate a user account in one or more Group Policy objects (GPOs) cannot be resolved to a security identifier (SID). This error is possibly caused by a mistyped or deleted user account referenced in either the User Rights Assignment or Restricted Groups branch of a GPO.
Microsoft Direct Access

The following templates are available:

- Microsoft DirectAccess 2008 R2
- Microsoft DirectAccess 2012
- Microsoft DirectAccess 2012 R2
- Microsoft DirectAccess 2012 (Health with PowerShell)

Periodically, SolarWinds releases SAM templates to support the latest product versions such as Microsoft Server 2016. You can continue using templates for older product versions, but updating to the latest template is recommended.

Microsoft DirectAccess 2008 R2

This template assesses the overall health of the Microsoft DirectAccess server installed on Windows 2008 R2.

Prerequisites

RPC and WMI access to the domain controller.

Credentials

Windows Administrator on the domain controller.

Monitored Components

For details on monitors, see [SAM Component Monitor Types](#).

Components without predetermined threshold values provide guidance such as "use the lowest threshold possible" or "use the highest threshold possible" to help you find a threshold appropriate for your application.

**Teredo Relay: In - Error Packets**

This monitor returns the total number of error packets received by the Teredo relay.

By default, this monitor has the Count statistic as difference box checked. It will show the statistic since the last polling period.

**Teredo Relay: In - Success Packets**

This monitor returns the total number of success packets received by the Teredo relay.

By default, this monitor has the Count statistic as difference box checked. It will show
the statistic since the last polling period.

**Teredo Relay: In - Error and Success Packets**  
This monitor returns the rate of total packets received by the Teredo relay.

**Teredo Relay: Out - Error Packets**  
This monitor returns the total number of packets failed to be sent by the Teredo relay.

By default, this monitor has the Count statistic as difference box checked. It will show the statistic since the last polling period.

**Teredo Relay: Out - Error and Success Packets**  
This monitor returns the rate of total packets sent by the Teredo relay.

**Network Interface (6TO4 Adapter): Packets Received Errors**  
This monitor returns the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

By default, this monitor has the Count statistic as difference box checked. It will show the statistic since the last polling period.

**Network Interface (6TO4 Adapter): Packets Received/sec**  
This monitor returns the rate at which packets are received on the network interface.

**Network Interface (6TO4 Adapter): Packets Sent Non-Unicast/sec**  
This monitor returns the rate at which packets are requested to be transmitted to non-unicast (subnet broadcast or subnet multicast) addresses by higher-level protocols. The rate includes the packets that were discarded or not sent.

**Network Interface (6TO4 Adapter): Packets Sent Unicast/sec**  
This monitor returns the rate at which packets are requested to be transmitted to subnet-unicast addresses by higher-level protocols. The rate includes the packets that were discarded or not sent.

**Network Interface (6TO4 Adapter): Packets Sent/sec**  
This monitor returns the rate at which packets are sent on the network interface.

**Network Interface (6TO4 Adapter): Packets/sec**  
This monitor returns the rate at which packets are sent and received on the network interface.

**IPHTTPS Global: Authentication Errors**  
This monitor returns the total number of authentication errors.

By default, this monitor has the Count statistic as difference box checked. It will show the statistic since the last polling period.
IPHTTPS Global: Receive Errors on the Server

This monitor returns the total number of Receive errors on the server.

By default, this monitor has the Count statistic as difference box checked. It will show the statistic since the last polling period.

IPHTTPS Global: Transmit Errors on the Server

This monitor returns the total number of Transmit errors on the server.

By default, this monitor has the Count statistic as difference box checked. It will show the statistic since the last polling period.

IPHTTPS Global: Bytes Received

This monitor returns the total number of bytes received on the IPHTTPS server.

By default, this monitor has the Count statistic as difference box checked. It will show the statistic since the last polling period.

IPHTTPS Global: Packets Received

This monitor returns the total number of packets received on the server.

By default, this monitor has the Count statistic as difference box checked. It will show the statistic since the last polling period.

IPHTTPS Global: Bytes Sent

This monitor returns the total number of bytes sent on the IPHTTPS server.

By default, this monitor has the Count statistic as difference box checked. It will show the statistic since the last polling period.

IPHTTPS Global: Packets Sent

This monitor returns the total number of packets sent from the server.

By default, this monitor has the Count statistic as difference box checked. It will show the statistic since the last polling period.

IPHTTPS Global: Sessions

This monitor returns the total number of sessions on the server.

By default, this monitor has the Count statistic as difference box checked. It will show the statistic since the last polling period.

Network Interface (isatap): Packets Received Errors

This monitor returns the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
By default, this monitor has the Count statistic as difference box checked. It will show the statistic since the last polling period.

Before using this monitor, you should provide the correct instance field. For example, the instance should resemble the following:

`isatap.<DOMAIN> where <DOMAIN> FQDN is the name of your domain.

Example: isatap.example.com`

**Network Interface (isatap): Packets Received/sec**

This monitor returns the rate at which packets are received on the network interface.

Before using this monitor, you should provide the correct instance field. For example, the instance should resemble the following:

`isatap.<DOMAIN> where <DOMAIN> FQDN is the name of your domain.

Example: isatap.example.com`

**Network Interface (isatap): Packets Sent Non-Unicast/sec**

This monitor returns the rate at which packets are requested to be transmitted to non-unicast (subnet broadcast or subnet multicast) addresses by higher-level protocols. The rate includes the packets that were discarded or not sent.

Before using this monitor, you should provide the correct instance field. For example, the instance should resemble the following:

`isatap.<DOMAIN> where <DOMAIN> FQDN is the name of your domain.

Example: isatap.example.com`

**Network Interface (isatap): Packets Sent Unicast/sec**

This monitor returns the rate at which packets are requested to be transmitted to subnet-unicast addresses by higher-level protocols. The rate includes the packets that were discarded or not sent.

Before using this monitor, you should provide the correct instance field. For example, the instance should resemble the following:

`isatap.<DOMAIN> where <DOMAIN> FQDN is the name of your domain.

Example: isatap.example.com`

**Network Interface (isatap): Packets Sent/sec**

This monitor returns the rate at which packets are sent on the network interface.
Before using this monitor, you should provide the correct instance field. For example, the instance should resemble the following:

```
isatap.<DOMAIN> where <DOMAIN> FQDN is the name of your domain.
```

Example: `isatap.example.com`

**Network Interface (isatap): Packets/sec**

This monitor returns the rate at which packets are sent and received on the network interface.

Before using this monitor, you should provide the correct instance field. For example, the instance should resemble the following:

```
isatap.<DOMAIN> where <DOMAIN> FQDN is the name of your domain.
```

Example: `isatap.example.com`

**IPsec AuthIP IPv4: Active Extended Mode SAs**

This monitor returns the number of currently active extended mode security associations.

**IPsec AuthIP IPv4: Active Main Mode SAs**

This monitor returns the number of currently active main mode security associations.

**IPsec AuthIP IPv4: Active Quick Mode SAs**

This monitor returns the number of currently active quick mode security associations.

**IPsec AuthIP IPv4: Failed Extended Mode Negotiations/sec**

This monitor returns the rate of failed extended mode negotiations.

**IPsec AuthIP IPv4: Failed Main Mode Negotiations/sec**

This monitor returns the rate of failed main mode negotiations.

**IPsec AuthIP IPv4: Failed Quick Mode Negotiations/sec**

This monitor returns the rate of failed quick mode negotiations.

**IPsec AuthIP IPv4: Pending Extended Mode Negotiations**

This monitor returns the number of pending extended mode negotiations.

**IPsec AuthIP IPv4: Pending Main Mode Negotiations**

This monitor returns the number of pending main mode negotiations.

**IPsec AuthIP IPv4: Pending Quick Mode Negotiations**

This monitor returns the number of pending quick mode negotiations.

**IPsec AuthIP IPv6: Active Extended Mode SAs**

This monitor returns the number of currently active extended mode security associations.
IPsec AuthIP IPv6: Active Main Mode SAs
This monitor returns the number of currently active main mode security associations.

IPsec AuthIP IPv6: Active Quick Mode SAs
This monitor returns the number of currently active quick mode security associations.

IPsec AuthIP IPv6: Failed Extended Mode Negotiations/sec
This monitor returns the rate of failed extended mode negotiations.

IPsec AuthIP IPv6: Failed Main Mode Negotiations/sec
This monitor returns the rate of failed main mode negotiations.

IPsec AuthIP IPv6: Failed Quick Mode Negotiations/sec
This monitor returns the rate of failed quick mode negotiations.

IPsec AuthIP IPv6: Pending Extended Mode Negotiations
This monitor returns the number of pending extended mode negotiations.

IPsec AuthIP IPv6: Pending Main Mode Negotiations
This monitor returns the number of pending main mode negotiations.

IPsec AuthIP IPv6: Pending Quick Mode Negotiations
This monitor returns the number of pending quick mode negotiations.

IPsec DoS Protection: Current State Entries
This monitor returns the number of state entries in the table. A state entry is a pair of IPv6 addresses that is authorized to pass through from a public to an internal interface.

IPsec DoS Protection: Per IP Rate Limit Queues
This monitor returns the current number of per internal IP address rate limit queues for unauthenticated IKEv1, IKEv2, AuthIP, or ESP IPv6 packets. An unauthenticated packet is an IPsec packet without an associated state entry. A state entry is a pair of IPv6 addresses that is authorized to pass through from a public to an internal interface. Unauthenticated packets are placed in a separate queue for each destination IP address that is available on the internal interface.

IPsec DoS Protection: State Entries/sec
This monitor returns the rate at which state entries are created by the IPsec Denial of Service Protection component. A state entry is a pair of IPv6 addresses that is authorized to pass through from a public to an internal interface.

IPsec Driver: Bytes Received in Tunnel Mode/sec
This monitor returns the rate of bytes received using tunnel mode.
Service: Remote Access Connection Manager

This service manages dial-up and virtual private network (VPN) connections from this computer to the Internet or other remote networks. If this service is disabled, any services that explicitly depend on it will fail to start.

TCP Port: Direct Access

This monitor tests the ability of a DirectAccess service to accept incoming sessions. The Forefront UAG DirectAccess server is listening on TCP port 443 for traffic from IP-HTTPS-based DirectAccess clients.

Configuring Windows Remote Management (WinRM)

1. If not already done so, install PowerShell 2.0 or later and WinRM on the SAM and target servers. (For installation details, see Microsoft's documentation website (https://docs.microsoft.com/en-us/powershell/).
2. On the SAM server, open a command prompt as an Administrator. To do this, go to the Start menu and right-click the cmd.exe and then select Run as Administrator.
3. Enter the following in the command prompt:
   ```bash
   winrm quickconfig
   winrm set winrm/config/client @{TrustedHosts="*"}
   ```
4. On the target server, open a command prompt as an Administrator and enter the following:
   ```bash
   winrm quickconfig
   winrm set winrm/config/client @{TrustedHosts="IP_ADDRESS"}
   ```
   where IP address is the IP address of your SAM server.

Microsoft DirectAccess 2012

This template assesses the overall health of Microsoft DirectAccess server installed on Windows 2012.

Prerequisites

RPC and WMI access to the domain controller.

Credentials

Windows Administrator on the domain controller.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Components without predetermined threshold values provide guidance such as "use the lowest threshold possible" or "use the highest threshold possible" to help you find a threshold appropriate for your application.
Teredo Relay: In - Error Packets

This monitor returns the total number of error packets received by the Teredo relay.

- By default, this monitor has the Count statistic as difference box checked. It will show the statistic since the last polling period.

Teredo Relay: In - Success Packets

This monitor returns the total number of error packets received by the Teredo relay.

- By default, this monitor has the Count statistic as difference box checked. It will show the statistic since the last polling period.

Teredo Relay: In - Error and Success Packets

This monitor returns the rate of total packets received by the Teredo relay.

Teredo Relay: Out - Error Packets

This monitor returns the total number of packets failed to be sent by the Teredo relay.

- By default, this monitor has the Count statistic as difference box checked. It will show the statistic since the last polling period.

Teredo Relay: Out - Error and Success Packets

This monitor returns the rate of total packets sent by the Teredo relay.

Network Interface (6TO4 Adapter): Packets Received Errors

This monitor returns the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

- By default, this monitor has the Count statistic as difference box checked. It will show the statistic since the last polling period.

Network Interface (6TO4 Adapter): Packets Received/sec

This monitor returns the rate at which packets are received on the network interface.

Network Interface (6TO4 Adapter): Packets Sent Non-Unicast/sec

This monitor returns the rate at which packets are requested to be transmitted to non-unicast (subnet broadcast or subnet multicast) addresses by higher-level protocols. The rate includes the packets that were discarded or not sent.

Network Interface (6TO4 Adapter): Packets Sent Unicast/sec

This monitor returns the rate at which packets are requested to be transmitted to subnet-unicast addresses by higher-level protocols. The rate includes the packets that were discarded or not sent.

Network Interface (6TO4 Adapter): Packets Sent/sec

This monitor returns the rate at which packets are sent on the network interface.
Network Interface (6TO4 Adapter): Packets/sec

This monitor returns the rate at which packets are sent and received on the network interface.

IPHTTPS Global: Authentication Errors

This monitor returns the total authentication errors.

- By default, this monitor has the Count statistic as difference box checked. It will show the statistic since the last polling period.

IPHTTPS Global: Receive Errors on the Server

This monitor returns the total receive errors on the server.

- By default, this monitor has the Count statistic as difference box checked. It will show the statistic since the last polling period.

IPHTTPS Global: Transmit Errors on the Server

This monitor returns the total transmit errors on the server.

- By default, this monitor has the Count statistic as difference box checked. It will show the statistic since the last polling period.

IPHTTPS Global: Bytes Received

This monitor returns the total bytes received on the IPHTTPS server.

- By default, this monitor has the Count statistic as difference box checked. It will show the statistic since the last polling period.

IPHTTPS Global: Packets Received

This monitor returns the total packets received on the server.

- By default, this monitor has the Count statistic as difference box checked. It will show the statistic since the last polling period.

IPHTTPS Global: Bytes Sent

This monitor returns the total bytes sent on the IPHTTPS server.

- By default, this monitor has the Count statistic as difference box checked. It will show the statistic since the last polling period.

IPHTTPS Global: Packets Sent

This monitor returns the total packets sent from the server.

- By default, this monitor has the Count statistic as difference box checked. It will show the statistic since the last polling period.
IPHTTPS Global: Sessions

This monitor returns the total number of sessions on the server.

1. By default, this monitor has the Count statistic as difference box checked. It will show the statistic since the last polling period.

Network Interface (isatap): Packets Received Errors

This monitor returns the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

1. By default, this monitor has the Count statistic as difference box checked. It will show the statistic since the last polling period.

Before using this monitor, you should provide the correct instance field. For example, the instance should resemble the following:

isatap.<DOMAIN> where <DOMAIN> FQDN is the name of your domain.

Example: isatap.example.com

Network Interface (isatap): Packets Received/sec

This monitor returns the rate at which packets are received on the network interface.

Before using this monitor, you should provide the correct instance field. For example, the instance should resemble the following:

isatap.<DOMAIN> where <DOMAIN> FQDN is the name of your domain.

Example: isatap.example.com

Network Interface (isatap): Packets Sent Non-Unicast/sec

This monitor returns the rate at which packets are requested to be transmitted to non-unicast (subnet broadcast or subnet multicast) addresses by higher-level protocols. The rate includes the packets that were discarded or not sent.

Before using this monitor, you should provide the correct instance field. For example, the instance should resemble the following:

isatap.<DOMAIN> where <DOMAIN> FQDN is the name of your domain.

Example: isatap.example.com

Network Interface (isatap): Packets Sent Unicast/sec

This monitor returns the rate at which packets are requested to be transmitted to subnet-unicast addresses by higher-level protocols. The rate includes the packets that were discarded or not sent.
Before using this monitor, you should provide the correct instance field. For example, the instance should resemble the following:

\texttt{isatap.<\texttt{DOMAIN}> where <\texttt{DOMAIN}> FQDN is the name of your domain.}

\textbf{Example: isatap.example.com}

\textbf{Network Interface (isatap): Packets Sent/sec}
This monitor returns the rate at which packets are sent on the network interface.

Before using this monitor, you should provide the correct instance field. For example, the instance should resemble the following:

\texttt{isatap.<\texttt{DOMAIN}> where <\texttt{DOMAIN}> FQDN is the name of your domain.}

\textbf{Example: isatap.example.com}

\textbf{Network Interface (isatap): Packets/sec}
This monitor returns the rate at which packets are sent and received on the network interface.

Before using this monitor, you should provide the correct instance field. For example, the instance should resemble the following:

\texttt{isatap.<\texttt{DOMAIN}> where <\texttt{DOMAIN}> FQDN is the name of your domain.}

\textbf{Example: isatap.example.com}

\textbf{IPsec AuthIP IPv4: Active Extended Mode SAs}
This monitor returns the number of currently active extended mode security associations.

\textbf{IPsec AuthIP IPv4: Active Main Mode SAs}
This monitor returns the number of currently active main mode security associations.

\textbf{IPsec AuthIP IPv4: Active Quick Mode SAs}
This monitor returns the number of currently active quick mode security associations.

\textbf{IPsec AuthIP IPv4: Failed Extended Mode Negotiations/sec}
This monitor returns the rate of failed extended mode negotiations.

\textbf{IPsec AuthIP IPv4: Failed Main Mode Negotiations/sec}
This monitor returns the rate of failed main mode negotiations.

\textbf{IPsec AuthIP IPv4: Failed Quick Mode Negotiations/sec}
This monitor returns the rate of failed quick mode negotiations.

\textbf{IPsec AuthIP IPv4: Pending Extended Mode Negotiations}
This monitor returns the number of pending extended mode negotiations.
IPsec AuthIP IPv4: Pending Main Mode Negotiations
This monitor returns the number of pending main mode negotiations.

IPsec AuthIP IPv4: Pending Quick Mode Negotiations
This monitor returns the number of pending quick mode negotiations.

IPsec AuthIP IPv6: Active Extended Mode SAs
This monitor returns the number of currently active extended mode security associations.

IPsec AuthIP IPv6: Active Main Mode SAs
This monitor returns the number of currently active main mode security associations.

IPsec AuthIP IPv6: Active Quick Mode SAs
This monitor returns the number of currently active quick mode security associations.

IPsec AuthIP IPv6: Failed Extended Mode Negotiations/sec
This monitor returns the rate of failed extended mode negotiations.

IPsec AuthIP IPv6: Failed Main Mode Negotiations/sec
This monitor returns the rate of failed main mode negotiations.

IPsec AuthIP IPv6: Failed Quick Mode Negotiations/sec
This monitor returns the rate of failed quick mode negotiations.

IPsec AuthIP IPv6: Pending Extended Mode Negotiations
This monitor returns the number of pending extended mode negotiations.

IPsec AuthIP IPv6: Pending Main Mode Negotiations
This monitor returns the number of pending main mode negotiations.

IPsec AuthIP IPv6: Pending Quick Mode Negotiations
This monitor returns the number of pending quick mode negotiations.

IPsec DoS Protection: Current State Entries
This monitor returns the number of state entries in the table. A state entry is a pair of IPv6 addresses that is authorized to pass through from a public to an internal interface.

IPsec DoS Protection: Per IP Rate Limit Queues
This monitor returns the current number of per internal IP address rate limit queues for unauthenticated IKEv1, IKEv2, AuthIP, or ESP IPv6 packets. An unauthenticated packet is an IPsec packet without an associated state entry. A state entry is a pair of IPv6 addresses that is authorized to pass through from a public to an internal interface. Unauthenticated packets are placed in a separate queue for each destination IP address that is available on the internal interface.
**IPsec DoS Protection: State Entries/sec**

This monitor returns the rate at which state entries are created by the IPsec Denial of Service Protection component. A state entry is a pair of IPv6 addresses that is authorized to pass through from a public to an internal interface.

**IPsec Driver: Bytes Received in Tunnel Mode/sec**

This monitor returns the rate of bytes received using tunnel mode.

**Service: Remote Access Connection Manager**

This service manages dial-up and virtual private network (VPN) connections from this computer to the Internet or other remote networks. If this service is disabled, any services that explicitly depend on it will fail to start.

**Service: Remote Access Management service**

This service logs, monitors, and manages DirectAccess and VPN connections to the server.

**Remote Access Warning and Error Events**

This service monitors Warning and Error events.

**TCP Port: Direct Access**

This monitor tests the ability of a DirectAccess service to accept incoming sessions. The Forefront UAG DirectAccess server is listening on TCP port 443 for traffic from IP-HTTPS-based DirectAccess clients.

---

**Configuring Windows Remote Management (WinRM)**

1. If not already done so, install PowerShell 2.0 or later and WinRM on the SAM and target servers. (For installation details, see Microsoft's documentation website [https://docs.microsoft.com/en-us/powershell/](https://docs.microsoft.com/en-us/powershell/).

2. On the SAM server, open a command prompt as an Administrator. To do this, go to the Start menu and right-click the cmd.exe and then select Run as Administrator.

3. Enter the following in the command prompt:
   ```
   winrm quickconfig
   winrm set winrm/config/client @{TrustedHosts="*"}
   ```

4. On the target server, open a command prompt as an Administrator and enter the following:
   ```
   winrm quickconfig
   winrm set winrm/config/client @{TrustedHosts="IP_ADDRESS"}
   ```
   where IP address is the IP address of your SAM server.

---

**Microsoft DirectAccess 2012 R2**

This template assesses the overall health of Microsoft DirectAccess server installed on Windows 2012 R2.
Prerequisites

RPC and WMI access to the domain controller.

Credentials

Windows Administrator on the domain controller.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Components without predetermined threshold values provide guidance such as "use the lowest threshold possible" or "use the highest threshold possible" to help you find a threshold appropriate for your application.

Teredo Relay: In - Error Packets

This monitor returns the total number of error packets received by the Teredo relay.

By default, this monitor has the Count statistic as difference box checked. It will show the statistic since the last polling period.

Teredo Relay: In - Success Packets

This monitor returns the total number of error packets received by the Teredo relay.

By default, this monitor has the Count statistic as difference box checked. It will show the statistic since the last polling period.

Teredo Relay: In - Error and Success Packets

This monitor returns the rate of total packets received by the Teredo relay.

Teredo Relay: Out - Error Packets

This monitor returns the total number of packets failed to be sent by the Teredo relay.

By default, this monitor has the Count statistic as difference box checked. It will show the statistic since the last polling period.

Teredo Relay: Out - Error and Success Packets

This monitor returns the rate of total packets sent by the Teredo relay.

Network Interface (6TO4 Adapter): Packets Received Errors

This monitor returns the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

By default, this monitor has the Count statistic as difference box checked. It will show the statistic since the last polling period.
Network Interface (6TO4 Adapter): Packets Received/sec

This monitor returns the rate at which packets are received on the network interface.

Network Interface (6TO4 Adapter): Packets Sent Non-Unicast/sec

This monitor returns the rate at which packets are requested to be transmitted to non-unicast (subnet broadcast or subnet multicast) addresses by higher-level protocols. The rate includes the packets that were discarded or not sent.

Network Interface (6TO4 Adapter): Packets Sent Unicast/sec

This monitor returns the rate at which packets are requested to be transmitted to subnet-unicast addresses by higher-level protocols. The rate includes the packets that were discarded or not sent.

Network Interface (6TO4 Adapter): Packets Sent/sec

This monitor returns the rate at which packets are sent on the network interface.

Network Interface (6TO4 Adapter): Packets/sec

This monitor returns the rate at which packets are sent and received on the network interface.

IPHTTPS Global: Authentication Errors

This monitor returns the total authentication errors.

By default, this monitor has the Count statistic as difference box checked. It will show the statistic since the last polling period.

IPHTTPS Global: Receive Errors on the Server

This monitor returns the total receive errors on the server.

By default, this monitor has the Count statistic as difference box checked. It will show the statistic since the last polling period.

IPHTTPS Global: Transmit Errors on the Server

This monitor returns the total transmit errors on the server.

By default, this monitor has the Count statistic as difference box checked. It will show the statistic since the last polling period.

IPHTTPS Global: Bytes Received

This monitor returns the total bytes received on the IPHTTPS server.

By default, this monitor has the Count statistic as difference box checked. It will show the statistic since the last polling period.

IPHTTPS Global: Packets Received

This monitor returns the total packets received on the server.
By default, this monitor has the Count statistic as difference box checked. It will show the statistic since the last polling period.

**IPHTTPS Global: Bytes Sent**

This monitor returns the total bytes sent on the IPHTTPS server.

By default, this monitor has the Count statistic as difference box checked. It will show the statistic since the last polling period.

**IPHTTPS Global: Packets Sent**

This monitor returns the total packets sent from the server.

By default, this monitor has the Count statistic as difference box checked. It will show the statistic since the last polling period.

**IPHTTPS Global: Sessions**

This monitor returns the total number of sessions on the server.

By default, this monitor has the Count statistic as difference box checked. It will show the statistic since the last polling period.

**Network Interface (isatap): Packets Received Errors**

This monitor returns the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

By default, this monitor has the Count statistic as difference box checked. It will show the statistic since the last polling period.

Before using this monitor, you should provide the correct instance field. For example, the instance should resemble the following:

**isatap.<DOMAIN>** where **<DOMAIN>** FQDN is the name of your domain.

Example: **isatap.example.com**

**Network Interface (isatap): Packets Received/sec**

This monitor returns the rate at which packets are received on the network interface.

Before using this monitor, you should provide the correct instance field. For example, the instance should resemble the following:

**isatap.<DOMAIN>** where **<DOMAIN>** FQDN is the name of your domain.

Example: **isatap.example.com**
Network Interface (isatap): Packets Sent Non-Unicast/sec

This monitor returns the rate at which packets are requested to be transmitted to non-unicast (subnet broadcast or subnet multicast) addresses by higher-level protocols. The rate includes the packets that were discarded or not sent.

Before using this monitor, you should provide the correct instance field. For example, the instance should resemble the following:

isatap.<DOMAIN> where <DOMAIN> FQDN is the name of your domain.

Example: isatap.example.com

Network Interface (isatap): Packets Sent Unicast/sec

This monitor returns the rate at which packets are requested to be transmitted to subnet-unicast addresses by higher-level protocols. The rate includes the packets that were discarded or not sent.

Before using this monitor, you should provide the correct instance field. For example, the instance should resemble the following:

isatap.<DOMAIN> where <DOMAIN> FQDN is the name of your domain.

Example: isatap.example.com

Network Interface (isatap): Packets Sent/sec

This monitor returns the rate at which packets are sent on the network interface.

Before using this monitor, you should provide the correct instance field. For example, the instance should resemble the following:

isatap.<DOMAIN> where <DOMAIN> FQDN is the name of your domain.

Example: isatap.example.com

Network Interface (isatap): Packets/sec

This monitor returns the rate at which packets are sent and received on the network interface.

Before using this monitor, you should provide the correct instance field. For example, the instance should resemble the following:

isatap.<DOMAIN> where <DOMAIN> FQDN is the name of your domain.

Example: isatap.example.com

IPsec AuthIP IPv4: Active Extended Mode SAs

This monitor returns the number of currently active extended mode security associations.

IPsec AuthIP IPv4: Active Main Mode SAs

This monitor returns the number of currently active main mode security associations.
IPsec AuthIP IPv4: Active Quick Mode SAs
This monitor returns the number of currently active quick mode security associations.

IPsec AuthIP IPv4: Failed Extended Mode Negotiations/sec
This monitor returns the rate of failed extended mode negotiations.

IPsec AuthIP IPv4: Failed Main Mode Negotiations/sec
This monitor returns the rate of failed main mode negotiations.

IPsec AuthIP IPv4: Failed Quick Mode Negotiations/sec
This monitor returns the rate of failed quick mode negotiations.

IPsec AuthIP IPv4: Pending Extended Mode Negotiations
This monitor returns the number of pending extended mode negotiations.

IPsec AuthIP IPv4: Pending Main Mode Negotiations
This monitor returns the number of pending main mode negotiations.

IPsec AuthIP IPv4: Pending Quick Mode Negotiations
This monitor returns the number of pending quick mode negotiations.

IPsec AuthIP IPv6: Active Extended Mode SAs
This monitor returns the number of currently active extended mode security associations.

IPsec AuthIP IPv6: Active Main Mode SAs
This monitor returns the number of currently active main mode security associations.

IPsec AuthIP IPv6: Active Quick Mode SAs
This monitor returns the number of currently active quick mode security associations.

IPsec AuthIP IPv6: Failed Extended Mode Negotiations/sec
This monitor returns the rate of failed extended mode negotiations.

IPsec AuthIP IPv6: Failed Main Mode Negotiations/sec
This monitor returns the rate of failed main mode negotiations.

IPsec AuthIP IPv6: Failed Quick Mode Negotiations/sec
This monitor returns the rate of failed quick mode negotiations.

IPsec AuthIP IPv6: Pending Extended Mode Negotiations
This monitor returns the number of pending extended mode negotiations.

IPsec AuthIP IPv6: Pending Main Mode Negotiations
This monitor returns the number of pending main mode negotiations.
IPsec AuthIP IPv6: Pending Quick Mode Negotiations

This monitor returns the number of pending quick mode negotiations.

IPsec DoS Protection: Current State Entries

This monitor returns the number of state entries in the table. A state entry is a pair of IPv6 addresses that is authorized to pass through from a public to an internal interface.

IPsec DoS Protection: Per IP Rate Limit Queues

This monitor returns the current number of per internal IP address rate limit queues for unauthenticated IKEv1, IKEv2, AuthIP, or ESP IPv6 packets. An unauthenticated packet is an IPsec packet without an associated state entry. A state entry is a pair of IPv6 addresses that is authorized to pass through from a public to an internal interface. Unauthenticated packets are placed in a separate queue for each destination IP address that is available on the internal interface.

IPsec DoS Protection: State Entries/sec

This monitor returns the rate at which state entries are created by the IPsec Denial of Service Protection component. A state entry is a pair of IPv6 addresses that is authorized to pass through from a public to an internal interface.

IPsec Driver: Bytes Received in Tunnel Mode/sec

This monitor returns the rate of bytes received using tunnel mode.

Service: Remote Access Connection Manager

This service manages dial-up and virtual private network (VPN) connections from this computer to the Internet or other remote networks. If this service is disabled, any services that explicitly depend on it will fail to start.

Service: Remote Access Management service

This service logs, monitors, and manages DirectAccess and VPN connections to the server.

Remote Access Warning and Error Events

This service monitors Warning and Error events.

TCP Port: Direct Access

This monitor tests the ability of a DirectAccess service to accept incoming sessions. The Forefront UAG DirectAccess server is listening on TCP port 443 for traffic from IP-HTTPS-based DirectAccess clients.

Configuring Windows Remote Management (WinRM)

1. If you have not already done so, install PowerShell 2.0 or later and WinRM on the SAM and target servers. (For installation details, see Microsoft's documentation website [https://docs.microsoft.com/en-us/powershell/].)

2. On the SAM server, open a command prompt as an Administrator. To do this, go to the Start menu and right-click the cmd.exe and then select Run as Administrator.
3. Enter the following in the command prompt:
   ```powershell
   winrm quickconfig
   winrm set winrm/config/client @{TrustedHosts="*"}
   ```

4. On the target server, open a command prompt as an Administrator and enter the following:
   ```powershell
   winrm quickconfig
   winrm set winrm/config/client @{TrustedHosts="IP_ADDRESS"}
   ```
   *where IP address is the IP address of your SAM server.*

**Microsoft DirectAccess 2012 (Health with PowerShell)**

This template assesses the overall health of Microsoft DirectAccess server installed on Windows 2012 by using PowerShell scripts.

**Prerequisites**

RPC and WMI access to the domain controller.

**Credentials**

Windows Administrator on the domain controller.

**Monitored Components**

For details on monitors, see [SAM Component Monitor Types](#).

**Remote Access Health 1**

This monitor returns the current health of a DirectAccess deployment. It returns a status (OK, Disabled, Unknown, Warning, Error) for the following components:

- Server
- 6to4
- DNS
- DNS64
- Domain Controller
- IP-HTTPS
- IPsec
- Kerberos
- NAT64
- Network Adapters

**Remote Access Health 2**

This monitor returns the current health of DirectAccess deployment. It returns a status (OK, Disabled, Unknown, Warning, Error) for the following components:
- Network Location Server
- Network Security
- Services
- Management Servers
- Otp
- High Availability
- Isatap
- Teredo
- Vpn Addressing
- Vpn Connectivity
Microsoft Dynamics

The following templates are available:

- Microsoft Dynamics AX 2012
- Microsoft Dynamics CRM 2011 Events
- Microsoft Dynamics CRM 2011 Statistics
- Microsoft Dynamics CRM 4.0 Events
- Microsoft Dynamics CRM 4.0 Statistics

Microsoft Dynamics AX 2012

This template assesses the status and overall performance of a Microsoft Dynamics AX 2012 server by monitoring critical errors in the Windows Application Log file.

Prerequisites

- WMI access to the target server.

Credentials

- Windows Administrator on the target server.

Performance Monitor Counters

Server: Processor Time

This monitor returns the total CPU percentage used by all Worker processes.

Server: User Time

This monitor returns the User CPU percentage used by all Worker processes.

Server: Active Sessions

The monitor returns the number of currently active server sessions

Server: Number of Bytes Received by Server

The monitor returns the number of bytes received by the AOS instance since it started. This component has “Count statistic as difference” enabled. It will return the difference between two polling intervals.

Server: Number of Bytes Sent by Server

The monitor returns the number of bytes that the AOS instance has sent since it started. This component has “Count statistic as difference” enabled. It will return the difference between two polling intervals.
Server: Number of Client Requests

The monitor returns the number of client-to-server requests since the AOS instance started. This component has “Count statistic as difference” enabled. It will return the difference between two polling intervals.

Server: Number of Client Requests per Second

The monitor returns the number of client-to-server requests that the AOS instance processes per second.

Server: Number of Server Requests

The monitor returns the number of server-to-client requests that have been processed since the AOS instance started. This component has “Count statistic as difference” enabled. It will return the difference between two polling intervals.

Server: Total Sessions

The monitor returns the total number of active sessions since the AOS instance started. This component has “Count statistic as difference” enabled. It will return the difference between two polling intervals.

Server: Total Number of Clears

The monitor returns the total number of times the cache was cleared of all contents. This component has “Count statistic as difference” enabled. It will return the difference between two polling intervals.

Server: Total Number of Hits

The monitor returns the total number of times a record was found successfully in the cache. This component has “Count statistic as difference” enabled. It will return the difference between two polling intervals.

Server: Total Number of Misses

The monitor returns the total number of times a record was not found in the cache. This component has “Count statistic as difference” enabled. It will return the difference between two polling intervals.

Server: Total Number of Remove Oldest

The monitor returns the total number of times the cache was flushed due to size. This component has “Count statistic as difference” enabled. It will return the difference between two polling intervals.

Client: Remote Calls #

The monitor returns the number of remote calls made. This component has “Count statistic as difference” enabled. It will return the difference between two polling intervals.
Client: AOD Cache Cleanups #

The monitor returns the number of times the AOD cache cleaned up older items. This component has “Count statistic as difference” enabled. It will return the difference between two polling intervals.

Client: AOD Cache Count #

The monitor returns the number of AOD items currently cached.

Client: X++ Cache Cleanups #

The monitor returns the number of times the X++ cache cleaned up older items. This component has “Count statistic as difference” enabled. It will return the difference between two polling intervals.

Client: X++ Cache Count #

The monitor returns the number of X++ methods currently cached.

Events: Microsoft Dynamics AX Errors

The monitor returns the number of all Error Windows Events from the Microsoft Dynamics AX.

Events: Microsoft Dynamics AX Warnings

The monitor returns the number of all Warning Windows Events from the Microsoft Dynamics AX.

Portions of this document were originally created by and are excerpted from the following sources:

Microsoft Corporation, Copyright © 2015 Microsoft Corporation. All rights reserved. Available at https://technet.microsoft.com/en-us/library/aa834416.aspx

Last updated: 2/05/2016
Microsoft Dynamics CRM 2011 Statistics

This template assesses the status and overall performance of a Microsoft Dynamics CRM 2011 server by retrieving statistics from performance counters.

Prerequisites

- WMI access to the target server.

Credentials

- Windows Administrator on the target server.

Monitored Components

For details on monitors, see [SAM Component Monitor Types](#).

Server: Failed CrmService Requests

This component returns the number of requests to the Microsoft Dynamics CRM Web service (part of the Microsoft Dynamics CRM SDK) that failed because of a time-out error or other SOAP failure.

- This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

Server: Failed InProcess CrmService Requests

This component returns the number of failed web service requests made by applications to the InProcess CrmService. The InProcess CrmService is a part of the Microsoft Dynamics CRM SDK used internally at Microsoft.

- This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

Server: Failed MetadataService Requests

This component returns the number of requests made to the MetadataService that failed because of a time-out or other SOAP failure.

- This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

Server: Failed Report Render Requests

This component returns the number of requests made to render Microsoft SQL Server Reporting Services reports that failed because of a time-out or error.

- This component has Count statistic as difference enabled. It will return the difference between two polling intervals.
Server: Script Error Reports

This component returns the total number of error reports generated by the web client as well as Microsoft Dynamics CRM for the Outlook client. This counter is reset weekly to zero.

This counter is an indicator of high script error frequency. If a large number of error reports are received in a short time, the Operations team should investigate to determine which pages are producing errors.

It is recommend that you set a monitoring alert to notify you if there are more than 500 error reports in a 10-minute period.

Auth: DB Authentication Failures in the Last Minute

This component returns the number of unsuccessful authentication requests per minute that are processed by using the Active Directory authentication credentials. This counter measures the entire Microsoft Dynamics CRM deployment including all organizations.

A high count may indicate that the system is possibly under a Denial of Service attack, or there may be a problem with the Authentication service configuration.

Auth: CRM Authentication Failures in the Last Minute

This component returns the number of unsuccessful authentication requests per minute that are processed by using the Microsoft Dynamics CRM authentication credentials. This counter measures the entire deployment including all organizations.

A high count may indicate that the system is possibly under a Denial of Service attack, or there may be a problem with the Authentication service configuration.

Auth: Windows Live ID Authentication Failures in the Last Minute

This component returns the number of failed authentication requests per minute that are processed by using the Windows Live ID authentication credentials. This counter measures the entire Microsoft Dynamics CRM deployment including all organizations.

A high count may indicate that the system is possibly under a Denial of Service attack, or there may be a problem with the Authentication service configuration.

Auth: Windows Authentication Failures in the Last Minute

This component returns the total number of authentication requests that are processed per minute. This counter includes successful and unsuccessful authentication attempts, and measures the entire Microsoft Dynamics CRM deployment including all organizations.
This counter is useful to show the authentication engine throughput of requests that use Active Directory authentication credentials and are requests for access to a specific organization. Together with the Processor and Memory counters, this counter can indicate whether the Microsoft Dynamics CRM server is overloaded with authentication requests and may require load balancing.

Outlook Sync: Total ABP Sync Requests

This component returns the total number of Address Book Provider (ABP) synchronization requests made from Microsoft Dynamics CRM for Outlook clients to a Microsoft Dynamics CRM Server.

This counter is useful to indicate the client load on the Asynchronous Processing Service. A high count indicates a high client load on that service.

You should set thresholds according to your environment.

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

Outlook Sync: Total Offline Sync Requests

This component returns the total number of offline synchronization requests made from Microsoft Dynamics CRM for Outlook clients to a Microsoft Dynamics CRM Server.

This counter is useful to indicate the client load on the Asynchronous Processing service. A high count indicates a high client load on the service.

You should set thresholds according to your environment.

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

Outlook Sync: Total Outlook Sync Requests

This component returns the total number of ABP Sync Requests and the Offline Sync Requests.

This counter is useful to indicate the client load on the Asynchronous Processing Service. A high count indicates a high client load on that service.

You should set thresholds according to your environment.

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

Outlook Sync: Total Succeeded Offline Sync Requests

This component returns the number of successful offline synchronization requests made from Microsoft Dynamics CRM for Outlook clients to a Microsoft Dynamics CRM Server.

A count that is much lower than the total number of offline synchronization requests may indicate a problem with clients that try to synchronize with the server.

You should set thresholds according to your environment.
This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

**Discovery: Failed Discovery Service Requests**

This component returns the number of requests to the Microsoft Dynamics CRM Discovery service that are unsuccessful for any reason. For example, a request may fail because the requesting party is not recognized as user in the requested organization.

A high count may indicate that the system is possibly under a Denial of Service attack, or there is some problem with the Discovery service configuration.

**Locator: Failed Cache Flush Requests**

This component returns the number of LocatorService cache flush requests that were unsuccessful for any reason. For example, a request may fail because it was for an invalid cache entry, or the cache may not flush because of an incorrect cache state.

A high count may indicate a problem with the LocatorService cache, or a problem with the connection to CONFIG_DB. For information about the cause, review the event log for errors.

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

**Locator: Total Cache Flush Requests**

This component returns the total number of LocatorService flush requests that have been received. This includes successful and unsuccessful requests.

A high count may indicate that the caching algorithm is not optimized, or that the data is changing too frequently.

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

**Platform: Average time of import request**

This component returns the average time that is required to process Microsoft Dynamics CRM data import requests.

Import requests are resource-intensive SQL operations. If the average time is too high and the number of concurrent imports is high, some organizations may have to be moved to a different server. Also, you may want to consider processing import jobs during a maintenance window to reduce the performance effect on users.

You should set thresholds according to your environment.

**Async Service: Active Organizations**

This component returns the total number of organizations in the Microsoft Dynamics CRM deployment that are actively being polled by the Microsoft CRM Asynchronous Processing Service.
Async Service: Total Operations Failed

This component returns the total number of asynchronous operations that failed for all organizations in the deployment.

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

Microsoft CRM Asynchronous Processing Service

This component returns the CPU and memory usage of Microsoft CRM Asynchronous Processing service. This service handles the processing of queued Asynchronous Events.

Dynamics CRM TCP Port

This component monitor tests the ability of a Dynamics CRM service to accept incoming sessions.

By default, TCP port 80 is monitored.
Microsoft Dynamics CRM 2011 Events

This template assesses the status and overall performance of a Microsoft Dynamics CRM 2011 server by monitoring critical errors in the Windows Application Log file.

Prerequisites

WMI access to the target server.

Credentials

Windows Administrator on the target server.

Monitored Components

For details on monitors, see [SAM Component Monitor Types](#).

All monitors should return values of zero. Returned values other than zero may indicate an abnormality. If you believe an abnormality exists, you should examine the Windows Application log for details.

Events: Audit Operations Errors

This monitor returns the number of audit operations errors, such as:

- Async Job Failed;
- Failed To Drop Partition On AuditBase;
- Async operation has been suspended;
- Failed To Create New Partition On AuditBase;
- Failure while monitoring async operations queue;
- Failure while starting monitoring for async operations queue.

Event ID: 17424, 24322, 17425, 24321, 17411, 17410.

**Async Job failure** can be caused by a number of different issues including a SQL deadlock or database error. Check the event log for more information about this error.

**Failed To Drop Partition On AuditBase**: The clustered indexes on the AuditBase table have been changed. Change the clustered indexes on the AuditBase table to be consistent with those defined in the stored procedure `p_deletesingleauditpartition.sql`.

**Async operation has been suspended** could be caused by SQL exceptions (timeouts, webstore cache expiry, and so on). Analyze the event logs and trace logs to identify the issue.

**Failed To Create New Partition On AuditBase**: A new partition could not be created on AuditBase because the Alter Partition Function failed.

The last two events generally means there is a problem contacting the configuration database (MSCRM_CONFIG) or there is a configuration issue for the server. Check for connectivity issues from the server to the SQL servers. Check the event logs for errors other than from Windows services.
**Events: Database Errors**

This monitor returns the number of database errors such as:

- Database error while updating operation status;
- Error while backing up database for organization;
- Error while backing up database transaction log for organization.

Event ID: 14414, 17422, 17423.

**Database error while updating operation status:** This error occurs when the host could not recover from a database error while updating status for an operation for organization. Analyze the event logs and trace logs to identify issue.

**Error while backing up database for organization** and **Error while backing up database transaction log for organization** occur when the backup log share could not be reached. This is specific to Microsoft Dynamics CRM Online. Check the configuration of the backup log share, and check permissions.

**Events: E-mail Router Service Errors**

This monitor returns the number of audit operations errors, such as:

- CRM Server Version is Not Compatible with E-mail Router;
- E-mail Router Service Cannot Connect to CRM Server;
- E-mail Router Service Could Not Run Service Background Thread;
- E-mail Router Version is Not Compatible with CRM Server;
- E-mail Router Work Item Aborted.

Event ID: 40215, 6188, 16192, 36673, 14494.

**CRM Server Version is Not Compatible with E-mail Router:** When Microsoft Dynamics CRM Server is not compatible with the E-mail Router, verify that the version of the E-mail Router is the same as that of the Microsoft Dynamics CRM server.

**E-mail Router Service Cannot Connect to CRM Server:** This is likely due to an issue with the E-Mail Router service account or network connectivity. Verify that the account that is used to run the E-mail Router service has sufficient permission to access the Microsoft Dynamics CRM server and that there are no connectivity problems.

**E-mail Router Service Could Not Run Service Background Thread:** Check the event logs for more details and restart the E-mail Router service.

**For E-mail Router Version is Not Compatible with CRM Server:** Verify that the version of the E-mail Router is the same as that of the Microsoft Dynamics CRM server.

**E-mail Router Work Item Aborted:** This occurs when there is a problem with the network or because the e-mail server is busy. Verify that you can log on to the e-mail server by using an e-mail application that uses the account specified for the e-mail router.

**Events: E-mail Connection Errors**

This monitor returns the number of audit operations errors, such as:
- Error Occurred While Checking Connection to CRM Server;
- Error Occurred While Checking Connection to E-mail Server;
- Error Occurred While Checking for Outgoing E-Mail;
- Error Occurred While Opening Mailbox;
- Error Occurred While Processing Outgoing E-mail.

Event ID: 5689, 9663, 61346, 26090, 61042.

**Error Occurred While Checking Connection to CRM Server** is likely due to an issue with credentials. Verify that the credentials to connect to CRM specified in the Deployments tab in the E-mail Router Configuration Manager are correct.

**Error Occurred While Checking Connection to E-mail Server** is likely due to an issue with credentials. Verify the credentials specified in the E-mail Router Configuration Manager are correct.

**Error Occurred While Checking for Outgoing E-Mail** is caused by outbound e-mail configuration possibly being incorrect. Check the outbound e-mail configuration in the e-mail router for the CRM users or queues.

**Error Occurred While Opening Mailbox** is caused because the mailbox may not exist or the credentials to connect may be insufficient or incorrect. Check if the mailbox exists and that the credentials specified to connect to the mailbox are correct.

**Error Occurred While Processing Outgoing E-mail** is caused because the outbound e-mail configuration may be incorrect. Verify the outbound e-mail configuration in the e-mail router.

**Events: E-mail Authentication Errors**

This monitor returns the number of audit operations errors, such as:

- Insufficient Privileges to Access Mailbox;
- Insufficient Privileges to Send E-Mail;
- Missing Credentials for Queue;
- Missing Credentials for User;
- NLTM Authentication is Not Supported;
- Service Account Cannot be Authenticated;
- Service Account Has Insufficient Permissions;
- SSL Authentication Failed.

Event ID: 39182, 41230, 30413, 29287, 8168, 51242, 61018, 6822.

**Insufficient Privileges to Access Mailbox:** Verify the credentials specified in the E-mail Router Configuration Manager are correct.

**Insufficient Privileges to Send E-Mail:** Verify that the credentials to connect to CRM specified in the Deployments tab in the E-mail Router Configuration Manager are correct.

**Missing Credentials for Queue:** Verify the credentials specified in the E-mail Router Configuration Manager are correct.
**Missing Credentials for User:** Verify the credentials specified in the E-mail Router Configuration Manager are correct.

**NLTM Authentication is Not Supported:** Verify the authentication type for the POP3 e-mail server.

**Service Account Cannot be Authenticated:** Verify that the credentials to connect to CRM specified in the Deployments tab in the E-mail Router Configuration Manager are correct.

**Service Account Has Insufficient Permissions:** Verify that the credentials to connect to CRM specified in the Deployments tab in the E-mail Router Configuration Manager are correct.

**SSL Authentication Failed:** Verify that the certificates on the e-mail router machine have been installed correctly.

**Events: Service Errors**

This monitor returns the number of audit operations errors such as:

- Incorrect Exchange Web Services URL;
- Invalid CRM Discovery Service URL.

Event ID: 15250, 14849.

**Incorrect Exchange Web Services URL:** Verify that you specified the correct Exchange Web Services URL.

**Invalid CRM Discovery Service URL:** Select the Deployments tab in the E-mail Router Configuration Manager and specify the correct CRM URL.

**Events: Web Service Errors**

This monitor returns the number of audit operations errors, such as:

- Customization uninstall failed;
- Language provisioning failed;
- Language translations labels import failed;
- Solution import failed.

Event ID: 19459, 19458, 19456, 19457.

**Customization uninstall failed** due to dependencies that prevent the solution from being uninstalled, or a timeout occurred, or other errors. To resolve this, uninstall the components or solutions with errors and then reinstall the solution. You can also try the operation again, or follow the resolution suggested in the error message.

**Language provisioning failed** is caused by a timeout occurring. Try the operation again.

**Language translations labels import failed** is caused because a translations file is malformed, or other possible errors. To resolve this, fix the contents of the translations file, and then reimport the translations. If this does not work, follow the resolution suggested in the error message.
Solution import failed occurs because the solution contains dependencies on components not present on the system, or the contents of the solution package are malformed, or a timeout occurred. To resolve this, install or create the missing components and then reinstall the solution. You can also try to fix the contents of the solution package and reinstalling the solution, or retry the operation. Splitting the solution into multiple smaller solutions may work as well.

Events: Deletion Service Errors

This monitor returns the number of audit operations errors, such as:

- Deletion Service failed to retrieve list of tables for cleanup;
- Deletion Service failed to successfully perform cleanup.

Event ID: 16394, 16387.

Deletion Service failed to retrieve list of tables for cleanup: When users delete a record, the record is marked for deletion, but is still present in the Microsoft Dynamics CRM Organization database. The Microsoft Dynamics CRM Deletion service periodically retrieves a list of records that have been marked for deletion from the Microsoft Dynamics CRM Organization database; then it scans and deletes records based on the deletion list. The retrieval likely failed due to a database error or SQL deadlock. The Deletion service will periodically retry to retrieve the list of tables for cleanup from the database. Wait for the Deletion service to run again. If there are numerous retry attempts, check the event logs and trace logs for more details.

Deletion Service failed to successfully perform cleanup: This problem can occur if the SQL Server Agent service is not running. Restart the SQL Server Agent service. If the problem persists, install the most recent cumulative update rollup for Microsoft Dynamics CRM 2011.

Event: Failed to Load Authentication Pipeline

This monitor returns the number of Failed to Load Authentication Pipeline errors.

Event ID: 17205.

The configuration database AuthenticationPipeline tables may be corrupt. Reinstall the configuration database or restore from a backup. There is no user-configurable information in these tables.

Events: Report Errors

This monitor returns the number of audit operations errors, such as:

- Report Render Failure;
- Report Server Web Service Failure;
- Report Server Web Service SOAP Failure.

Event ID: 19714, 19712, 19713.

Report Render Failure: This could be an issue with the installation or configuration of the Microsoft Dynamics CRM Reporting Extensions or that the reporting service account does not have sufficient privileges to the organization databases. Review the following articles in the Microsoft Knowledge Base: 946289 and 946585.

Event: Trace File Failure Alert

This monitor returns the number of trace file failure errors.

Event ID: 17156.

If this event occurs frequently, the tracing service might not be able to log traces to the trace file. Verify the access rights for the account under which CRM Platform Service is running to the trace file path name. Also, free disk space in the tracing file path name needs to be checked.

Microsoft Dynamics CRM 4.0 Events

This template assesses the status and overall performance of a Microsoft Dynamics CRM 4.0 server by monitoring critical errors in the Windows Application Log file.

**Prerequisites**

WMI access to the target server.

**Credentials**

Windows Administrator on the target server.

**Monitored Components**

For details on monitors, see SAM Component Monitor Types.

All monitors should return values of zero. Returned values other than zero may indicate an abnormality. If you believe an abnormality exists, you should examine the Windows Application log for details.

**Events: Audit Operations Errors**

This monitor returns the number of audit operations errors, such as:

- Async Job Failed;
- Failed To Drop Partition On AuditBase;
- Async operation has been suspended;
- Failed To Create New Partition On AuditBase;
- Failure while monitoring async operations queue;
- Failure while starting monitoring for async operations queue.

Event ID: 17424, 24322, 17425, 24321, 17411, 17410.

**Async Job failure** can be caused by a number of different issues including a SQL deadlock or database error. Check the event log for more information about this error.

**Failed To Drop Partition On AuditBase:** The clustered indexes on the AuditBase table have been changed. Change the clustered indexes on the AuditBase table to be consistent with those defined in the stored procedure p_deletesingleauditpartition.sql.
Async operation has been suspended could be caused by SQL exceptions (timeouts, webstore cache expiry, and so on). Analyze the event logs and trace logs to identify the issue.

Failed To Create New Partition On AuditBase: A new partition could not be created on AuditBase because the Alter Partition Function failed.

The last two events generally means there is a problem contacting the configuration database (MSCRM_CONFIG) or there is a configuration issue for the server. Check for connectivity issues from the server to the SQL servers. Check the event logs for errors other than from Windows services.

Events: Database Errors

This monitor returns the number of database errors such as:

- Database error while updating operation status;
- Error while backing up database for organization;
- Error while backing up database transaction log for organization.

Event ID: 14414, 17422, 17423.

Database error while updating operation status: This error occurs when the host could not recover from a database error while updating status for an operation for organization. Analyze the event logs and trace logs to identify issue.

Error while backing up database for organization and Error while backing up database transaction log for organization occur when the backup log share could not be reached. This is specific to Microsoft Dynamics CRM Online. Check the configuration of the backup log share, and check permissions.

Events: E-mail Router Service Errors

This monitor returns the number of audit operations errors, such as:

- CRM Server Version is Not Compatible with E-mail Router;
- E-mail Router Service Cannot Connect to CRM Server;
- E-mail Router Service Could Not Run Service Background Thread;
- E-mail Router Version is Not Compatible with CRM Server;
- E-mail Router Work Item Aborted.

Event ID: 40215, 6188, 16192, 36673, 14494.

CRM Server Version is Not Compatible with E-mail Router: When Microsoft Dynamics CRM Server is not compatible with the E-mail Router, verify that the version of the E-mail Router is the same as that of the Microsoft Dynamics CRM server.

E-mail Router Service Cannot Connect to CRM Server: This is likely due to an issue with the E-Mail Router service account or network connectivity. Verify that the account that is used to run the E-mail Router service has sufficient permission to access the Microsoft Dynamics CRM server and that there are no connectivity problems.

E-mail Router Service Could Not Run Service Background Thread: Check the event logs for more details and restart the E-mail Router service.
For E-mail Router Version is Not Compatible with CRM Server: Verify that the version of the E-mail Router is the same as that of the Microsoft Dynamics CRM server.

E-mail Router Work Item Aborted: This occurs when there is a problem with the network or because the e-mail server is busy. Verify that you can log on to the e-mail server by using an e-mail application that uses the account specified for the e-mail router.

Events: E-mail Connection Errors

This monitor returns the number of audit operations errors, such as:

- Error Occurred While Checking Connection to CRM Server;
- Error Occurred While Checking Connection to E-mail Server;
- Error Occurred While Checking for Outgoing E-Mail;
- Error Occurred While Opening Mailbox;
- Error Occurred While Processing Outgoing E-mail.

Event ID: 5689, 9663, 61346, 26090, 61042.

Error Occurred While Checking Connection to CRM Server is likely due to an issue with credentials. Verify that the credentials to connect to CRM specified in the Deployments tab in the E-mail Router Configuration Manager are correct.

Error Occurred While Checking Connection to E-mail Server is likely due to an issue with credentials. Verify the credentials specified in the E-mail Router Configuration Manager are correct.

Error Occurred While Checking for Outgoing E-Mail is caused by outbound e-mail configuration possibly being incorrect. Check the outbound e-mail configuration in the e-mail router for the CRM users or queues.

Error Occurred While Opening Mailbox is caused because the mailbox may not exist or the credentials to connect may be insufficient or incorrect. Check if the mailbox exists and that the credentials specified to connect to the mailbox are correct.

Error Occurred While Processing Outgoing E-mail is caused because the outbound e-mail configuration may be incorrect. Verify the outbound e-mail configuration in the e-mail router.

Events: E-mail Authentication Errors

This monitor returns the number of audit operations errors, such as:

- Insufficient Privileges to Access Mailbox;
- Insufficient Privileges to Send E-Mail;
- Missing Credentials for Queue;
- Missing Credentials for User;
- NLTM Authentication is Not Supported;
- Service Account Cannot be Authenticated;
- Service Account Has Insufficient Permissions;
- SSL Authentication Failed.

Event ID: 39182, 41230, 30413, 29287, 8168, 51242, 61018, 6822.
Insufficient Privileges to Access Mailbox: Verify the credentials specified in the E-mail Router Configuration Manager are correct.

Insufficient Privileges to Send E-Mail: Verify that the credentials to connect to CRM specified in the Deployments tab in the E-mail Router Configuration Manager are correct.

Missing Credentials for Queue: Verify the credentials specified in the E-mail Router Configuration Manager are correct.

Missing Credentials for User: Verify the credentials specified in the E-mail Router Configuration Manager are correct.

NLTM Authentication is Not Supported: Verify the authentication type for the POP3 e-mail server.

Service Account Cannot be Authenticated: Verify that the credentials to connect to CRM specified in the Deployments tab in the E-mail Router Configuration Manager are correct.

Service Account Has Insufficient Permissions: Verify that the credentials to connect to CRM specified in the Deployments tab in the E-mail Router Configuration Manager are correct.

SSL Authentication Failed: Verify that the certificates on the e-mail router machine have been installed correctly.

Events: Service Errors

This monitor returns the number of audit operations errors such as:

- Incorrect Exchange Web Services URL;
- Invalid CRM Discovery Service URL.

Event ID: 15250, 14849.

Incorrect Exchange Web Services URL: Verify that you specified the correct Exchange Web Services URL.

Invalid CRM Discovery Service URL: Select the Deployments tab in the E-mail Router Configuration Manager and specify the correct CRM URL.

Events: Web Service Errors

This monitor returns the number of audit operations errors, such as:

- Customization uninstall failed;
- Language provisioning failed;
- Language translations labels import failed;
- Solution import failed.

Event ID: 19459, 19458, 19456, 19457.

Customization uninstall failed due to dependencies that prevent the solution from being uninstalled, or a timeout occurred, or other errors. To resolve this, uninstall the components or solutions with errors and then reinstall the solution. You can also try the operation again, or follow the resolution suggested in the error message.

Language provisioning failed is caused by a timeout occurring. Try the operation again.
Language translations labels import failed is caused because a translations file is malformed, or other possible errors. To resolve this, fix the contents of the translations file, and then reimport the translations. If this does not work, follow the resolution suggested in the error message.

Solution import failed occurs because the solution contains dependencies on components not present on the system, or the contents of the solution package are malformed, or a timeout occurred. To resolve this, install or create the missing components and then reinstall the solution. You can also try to fix the contents of the solution package and reinstalling the solution, or retry the operation. Splitting the solution into multiple smaller solutions may work as well.

Events: Deletion Service Errors

This monitor returns the number of audit operations errors, such as:

- Deletion Service failed to retrieve list of tables for cleanup;
- Deletion Service failed to successfully perform cleanup.

Event ID: 16394, 16387.

Deletion Service failed to retrieve list of tables for cleanup: When users delete a record, the record is marked for deletion, but is still present in the Microsoft Dynamics CRM Organization database. The Microsoft Dynamics CRM Deletion service periodically retrieves a list of records that have been marked for deletion from the Microsoft Dynamics CRM Organization database; then it scans and deletes records based on the deletion list. The retrieval likely failed due to a database error or SQL deadlock. The Deletion service will periodically retry to retrieve the list of tables for cleanup from the database. Wait for the Deletion service to run again. If there are numerous retry attempts, check the event logs and trace logs for more details.

Deletion Service failed to successfully perform cleanup: This problem can occur if the SQL Server Agent service is not running. Restart the SQL Server Agent service. If the problem persists, install the most recent cumulative update rollup for Microsoft Dynamics CRM 2011.

Event: Failed to Load Authentication Pipeline

This monitor returns the number of Failed to Load Authentication Pipeline errors.

Event ID: 17205.

The configuration database AuthenticationPipeline tables may be corrupt. Reinstall the configuration database or restore from a backup. There is no user-configurable information in these tables.

Events: Report Errors

This monitor returns the number of audit operations errors, such as:

- Report Render Failure;
- Report Server Web Service Failure;
- Report Server Web Service SOAP Failure.

Event ID: 19714, 19712, 19713.
Report Render Failure: This could be an issue with the installation or configuration of the Microsoft Dynamics CRM Reporting Extensions or that the reporting service account does not have sufficient privileges to the organization databases. Review the following articles in the Microsoft Knowledge Base: 946289 and 946585.


Event: Trace File Failure Alert

This monitor returns the number of trace file failure errors.

Event ID: 17156.

If this event occurs frequently, the tracing service might not be able to log traces to the trace file. Verify the access rights for the account under which CRM Platform Service is running to the trace file path name. Also, free disk space in the tracing file path name needs to be checked.

Microsoft Dynamics CRM 4.0 Statistics

This template assesses the status and overall performance of a Microsoft Dynamics CRM 4.0 server by retrieving statistics from performance counters.

Prerequisites

WMI access to the target server.

Credentials

Windows Administrator on the target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Server: Failed CrmService Requests

This component returns the number of requests to the Microsoft Dynamics CRM Web service (part of the Microsoft Dynamics CRM SDK) that failed because of a time-out error or other SOAP failure.

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

Server: Failed InProcess CrmService Requests

This component returns the number of failed web service requests made by applications to the InProcess CrmService. The InProcess CrmService is a part of the Microsoft Dynamics CRM SDK used internally at Microsoft.

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.
Server: Failed MetadataService Requests

This component returns the number of requests made to the MetadataService that failed because of a time-out or other SOAP failure.

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

Server: Failed Report Render Requests

This component returns the number of requests made to render Microsoft SQL Server Reporting Services reports that failed because of a time-out or error.

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

Server: Script Error Reports

This component returns the total number of error reports generated by the web client as well as Microsoft Dynamics CRM for the Outlook client. This counter is reset weekly to zero.

This counter is an indicator of high script error frequency. If a large number of error reports are received in a short time, the Operations team should investigate to determine which pages are producing errors.

It is recommend that you set a monitoring alert to notify you if there are more than 500 error reports in a 10-minute period.

Auth: DB Authentication Failures in the Last Minute

This component returns the number of unsuccessful authentication requests per minute that are processed by using the Active Directory authentication credentials. This counter measures the entire Microsoft Dynamics CRM deployment including all organizations.

A high count may indicate that the system is possibly under a Denial of Service attack, or there may be a problem with the Authentication service configuration.

Auth: CRM Authentication Failures in the Last Minute

This component returns the number of unsuccessful authentication requests per minute that are processed by using the Microsoft Dynamics CRM authentication credentials. This counter measures the entire deployment including all organizations.

A high count may indicate that the system is possibly under a Denial of Service attack, or there may be a problem with the Authentication service configuration.

Auth: Windows Live ID Authentication Failures in the Last Minute

This component returns the number of failed authentication requests per minute that are processed by using the Windows Live ID authentication credentials. This counter measures the entire Microsoft Dynamics CRM deployment including all organizations.
A high count may indicate that the system is possibly under a Denial of Service attack, or there may be a problem with the Authentication service configuration.

**Auth: Windows Authentication Failures in the Last Minute**

This component returns the total number of authentication requests that are processed per minute. This counter includes successful and unsuccessful authentication attempts, and measures the entire Microsoft Dynamics CRM deployment including all organizations.

This counter is useful to show the authentication engine throughput of requests that use Active Directory authentication credentials and are requests for access to a specific organization. Together with the Processor and Memory counters, this counter can indicate whether the Microsoft Dynamics CRM server is overloaded with authentication requests and may require load balancing.

**Outlook Sync: Total ABP Sync Requests**

This component returns the total number of Address Book Provider (ABP) synchronization requests made from Microsoft Dynamics CRM for Outlook clients to a Microsoft Dynamics CRM Server.

This counter is useful to indicate the client load on the Asynchronous Processing Service. A high count indicates a high client load on that service.

You should set thresholds according to your environment.

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

**Outlook Sync: Total Offline Sync Requests**

This component returns the total number of offline synchronization requests made from Microsoft Dynamics CRM for Outlook clients to a Microsoft Dynamics CRM Server.

This counter is useful to indicate the client load on the Asynchronous Processing service. A high count indicates a high client load on the service.

You should set thresholds according to your environment.

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

**Outlook Sync: Total Outlook Sync Requests**

This component returns the total number of ABP Sync Requests and the Offline Sync Requests.

This counter is useful to indicate the client load on the Asynchronous Processing Service. A high count indicates a high client load on that service.

You should set thresholds according to your environment.

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.
**Outlook Sync: Total Succeeded Offline Sync Requests**

This component returns the number of successful offline synchronization requests made from Microsoft Dynamics CRM for Outlook clients to a Microsoft Dynamics CRM Server. A count that is much lower than the total number of offline synchronization requests may indicate a problem with clients that try to synchronize with the server.

You should set thresholds according to your environment.

1. This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

**Discovery: Failed Discovery Service Requests**

This component returns the number of requests to the Microsoft Dynamics CRM Discovery service that are unsuccessful for any reason. For example, a request may fail because the requesting party is not recognized as user in the requested organization.

A high count may indicate that the system is possibly under a Denial of Service attack, or there is some problem with the Discovery service configuration.

**Locator: Failed Cache Flush Requests**

This component returns the number of LocatorService cache flush requests that were unsuccessful for any reason. For example, a request may fail because it was for an invalid cache entry, or the cache may not flush because of an incorrect cache state.

A high count may indicate a problem with the LocatorService cache, or a problem with the connection to CONFIG_DB. For information about the cause, review the event log for errors.

1. This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

**Locator: Total Cache Flush Requests**

This component returns the total number of LocatorService flush requests that have been received. This includes successful and unsuccessful requests.

A high count may indicate that the caching algorithm is not optimized, or that the data is changing too frequently.

1. This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

**Platform: Average time of import request**

This component returns the average time that is required to process Microsoft Dynamics CRM data import requests.

Import requests are resource-intensive SQL operations. If the average time is too high and the number of concurrent imports is high, some organizations may have to be moved to a different server. Also, you may want to consider processing import jobs during a maintenance window to reduce the performance effect on users.
You should set thresholds according to your environment.

Async Service: Active Organizations

This component returns the total number of organizations in the Microsoft Dynamics CRM deployment that are actively being polled by the Microsoft CRM Asynchronous Processing Service.

Async Service: Total Operations Failed

This component returns the total number of asynchronous operations that failed for all organizations in the deployment.

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

Microsoft CRM Asynchronous Processing Service

This component returns the CPU and memory usage of Microsoft CRM Asynchronous Processing service. This service handles the processing of queued Asynchronous Events.

Dynamics CRM TCP Port

This component monitor tests the ability of a Dynamics CRM service to accept incoming sessions.

By default, TCP port 80 is monitored.
Exchange templates

These templates allow you to monitor counters and services for Microsoft Exchange.

See also AppInsight for Exchange.

Periodically, SolarWinds releases SAM templates to support the latest product versions such as Microsoft Server 2016. You can continue using templates for older product versions, but updating to the latest template is recommended.

- **Exchange 2007 Client Access Role Counters (Advanced)**
- **Exchange 2007 Edge Transport Role Counters (Advanced)**
- **Exchange 2007 Hub Transport Role Counters (Advanced)**
- **Exchange 2007 Mailbox Role Counters (Advanced)**
- **Exchange 2007 Outlook Web Access (OWA) Form Login**
- **Exchange 2007 Unified Messaging Role Counters (Advanced)**
- **Exchange 2007 — 2010 Client Access Role Services and Counters (Basic)**
- **Exchange 2007 — 2010 Common Performance Counters**
- **Exchange 2007 — 2010 Edge Transport Role Services and Counters (Basic)**
- **Exchange 2007 — 2010 Hub Transport Role Services and Counters (Basic)**
- **Exchange 2007 — 2010 Unified Messaging Role Services and Counters (Basic)**
- **Exchange 2010 Client Access Role Counters (Advanced)**
- **Exchange 2010 Edge Transport Role Counters (Advanced)**
- **Exchange 2010 Hub Transport Role Counters (Advanced)**
- **Exchange 2010 OWA Form Login (PowerShell)**
- **Exchange 2016 Unified Messaging Role Counters (Advanced)**
- **Exchange 2013 Client Access Role Counters (Advanced)**
- **Exchange 2013 Client Access Role Services and Counters (Basic)**
- **Exchange 2016 Client Access Role Services and Counters (Basic)**
- **Exchange 2016 Client Access Role Services and Counters (Advanced)**
- **Exchange 2016 Hub Transport Role Counters (Advanced)**
- **Exchange 2016 Hub Transport Role Services and Counters (Basic)**
- **Exchange Active Sync Connectivity**
- **Exchange Server 2000 and 2003**
- **Exchange Web Services User Experience monitor**

### Basic versus Advanced templates

These templates are divided into two categories:
- Basic Services and Performance Counters
- Advanced

The templates in the Basic Services and Performance Counters category contain templates with basic counters and services for monitoring 2007, 2010, and 2016 versions of Exchange. These templates should work out of the box. Counters in this category have well documented thresholds and do not require any additional configuration.

The templates in the Advanced category contain other performance and statistics counters. You can use these templates in addition to the basic templates if the information from the basic templates is not sufficient to monitor the server. The advanced templates are provided for a specific Exchange version, as indicated by the template name. For example, the Exchange 2007 — 2010 Mailbox Role Counters (Advanced) template applies to Exchange 2007 — 2010 only. Some of the counters will require manual configuration, such as specific instances, correcting thresholds for your environment, and so forth.

There is also an Exchange 2016 Common Performance Counters template. This template contains general counters (CPU usage, available memory, LDAP times, and so forth) that can be used in all server roles. This template will require manual configuration similar to that required by the advanced templates.

**Typical usage scenario**

Assume that you need to monitor an Exchange 2007 installation with Mailbox Role.

First apply the Exchange 2007 — 2010 Mailbox Role Services and Counters (Basic) template. As a result, you will have the statuses for critical Exchange services (up or down) and information from general performance counters for this role. If you need system level general performance counters (CPU usage, available memory, and so forth) you can also apply the Exchange 2007 — 2010 Common Performance Counters template, but you will need to correct some counters manually according to your environment.

If the information provided by the basic template is not enough, you need to additionally apply the Exchange 2007 — 2010 Mailbox Role Counters (Advanced) template. After applying this template, you may need to modify some thresholds and instances according to your environment. Then you should receive full performance and statistics information for this Exchange role.
Exchange 2007 Client Access Role Counters (Advanced)

This template contains advanced performance and statistics counters for monitoring Exchange 2007 Client Access Role. Some of counters may require manual configuration, such as setting up installation-specific instances, correcting thresholds for the client's environment, and so forth. Use this template in addition to the 2007-2010 Client Access Role Services and Counters (Basic) template.

**Prerequisites**

RPC and WMI access to the Exchange server.

**Credentials**

Windows Administrator on the target server.

**Monitored Components**


These performance counters are based on the following information:


**Availability Requests (sec)**

Shows the number of requests serviced per second. The request can be only for free/busy or include suggestions. One request may contain multiple mailboxes.

Determines the rate at which Availability service requests are occurring.

**Average Request Time (Active Sync)**

Shows the average time that elapsed while waiting for a request to complete. Includes Ping Request Time, which can increase the general response time of this counter. Adding ping counters helps clarify where performance is being impacted.

Determines the rate at which Availability service requests are occurring.

**Requests/sec (Active Sync)**

Shows the number of HTTP requests that are received from the client via ASP.NET per second.

Determines the current Exchange ActiveSync request rate.

**OWA: Requests/sec**

Shows the number of requests handled by Outlook Web Access per second.

Determines current user load.

**Current Connections**

Shows the current number of connections established with the Web service.
Determines current user load.

**ASP.NET: Requests Current**

Shows the current number of requests, including those that are queued, currently executing, or waiting to be written to the client. Under the ASP.NET process model, when this counter exceeds the requestQueueLimit defined in the processModel configuration section, ASP.NET will begin rejecting requests.

Should be less than 5,000 at all times.

The maximum value is 5,000. The server will return a 503 error if this value is exceeded. This value can be increased in the `machine.config` file to allow for Client Access server scalability.

**ASP.NET: Request Wait Time**

Shows the number of milliseconds the most recent request was waiting in the queue.

Should be less than 1,000 milliseconds (ms) at all times.

**Disk Reads/sec**

Indicates that a paging situation may exist because data was read from disk instead of memory.

Should be less than 50 at all times.

**Disk Writes/sec**

Indicates that a paging situation may exist because data was written to disk instead of being stored in memory.

Should be less than 50 at all times.

**Average Response Time**

Shows the average time (in milliseconds) that elapsed between the beginning and end of an OEH or ASPX request.

Should be less than 100 ms at all times.

Used to determine the latency that a client is experiencing. Higher values may indicate high user load or higher than normal CPU time.
Exchange 2007 Edge Transport Role Counters (Advanced)

This template contains advanced performance and statistics counters for monitoring Exchange 2007 Edge Transport Role. Some of the counters may require manual configuration, such as setting up installation-specific instances, correcting thresholds for the client's environment, and so forth. Use this template in addition to the Exchange 2007-2010 Edge Transport Role Services and Counters (Basic) template.

Prerequisites

RPC and WMI access to the Exchange server.

Credentials

Windows Administrator on target server.

Monitored Components:

For details on monitors, see SAM Component Monitor Types.

These performance counters are based on the following information:


Dumpster Size

Shows the total size (in bytes) of mail items currently in the transport dumpster on this server.

Dumpster Inserts/sec

Shows the rate at which items are inserted into the transport dumpster on this server. Determines the current rate of transport dumpster inserts.

Dumpster Item Count

Shows the total number of mail items currently in the transport dumpster on this server. Shows the current number of items being held in the transport dumpster.

Dumpster Deletes/sec

Shows the rate at which items are deleted from the transport dumpster on this server. Determines the current rate of transport dumpster deletions.

I/O Log Writes/sec (database)

Shows the rate of log file write operations completed. Determines the current load. Compare values to historical baselines.

I/O Log Reads/sec (database)

Shows the rate of log file read operations completed. Determines the current load. Compare values to historical baselines.
Log Generation Checkpoint Depth (database)

Represents the amount of work (in count of log files) that needs to be redone or undone to the database files if the process fails.

Should be less than 1,000 at all times.

I/O Database Reads/sec (database)

Shows the rate of database read operations completed. Determines the current load. Compare values to historical baselines.

I/O Database Writes/sec

Shows the rate of database write operations completed. Determines the current load. Compare values to historical baselines.

Messages Submitted Per Second

Shows the number of messages queued in the Submission queue per second. Determines the current load. Compare values to historical baselines.

Messages Received/sec

Shows the number of messages received by the SMTP server each second. Determines the current load. Compare values to historical baselines.

Messages Queued for Delivery Per Second

Shows the number of messages queued for delivery per second. Determines the current load. Compare values to historical baselines.

Messages Completed Delivery Per Second

Shows the number of messages delivered per second. Determines the current load. Compare values to historical baselines.

Avg. Disk sec/Read (Physical Disk)

Shows the average time, in seconds, of a read of data from the disk.

Should be less than 20 milliseconds (ms) on average. Spikes (maximum values) should not be higher than 50 ms.

When looking at hard disks using perfmon.exe, an understanding of the underlying hard disk subsystem is required to determine which counters (physical disk or logical disk) to look at.

Avg. Disk sec/Write (Physical Disk)

Shows the average time, in seconds, of a write of data to the disk.

Should be less than 20 milliseconds (ms) on average. Spikes (maximum values) should not be higher than 50 ms.

When looking at hard disks using perfmon.exe, an understanding of the underlying
hard disk subsystem is required to determine which counters (physical disk or logical disk) to look at.

**Avg. Disk sec/Read (Logical Disk)**

Shows the average time, in seconds, of a read of data from the disk.

Should be less than 20 milliseconds (ms) on average. Spikes (maximum values) should not be higher than 50 ms.

When looking at hard disks using perfmon.exe, an understanding of the underlying hard disk subsystem is required to determine which counters (physical disk or logical disk) to look at.

**Avg. Disk sec/Write (Logical Disk)**

Shows the average time, in seconds, of a write of data to the disk.

Should be less than 20 milliseconds (ms) on average. Spikes (maximum values) should not be higher than 50 ms.

When looking at hard disks using perfmon.exe, an understanding of the underlying hard disk subsystem is required to determine which counters (physical disk or logical disk) to look at.

**Retry Non-Smtp Delivery Queue Length**

Shows the number of messages in a retry state in the non-SMTP gateway delivery queues.

Should not exceed 100.

**Largest Delivery Queue Length**

Shows the number of messages in the largest delivery queues.

Should be less than 200 for the Edge Transport and Hub Transport server roles.

**Version buckets allocated (database)**

Total number of version buckets allocated. Shows the default backpressure values as listed in the edgetransport.exe.config file.

Should be less than 200 at all times.

**Log Record Stalls/sec (database)**

Shows the number of log records that cannot be added to the log buffers per second because they are full. If this counter is nonzero most of the time, the log buffer size may be a bottleneck.

Should be less than 10 per second on average. Spikes (maximum values) should not be greater than 100 per second.
Log Threads Waiting (database)

Shows the number of threads waiting for their data to be written to the log to complete an update of the database. If this number is too high, the log may be a bottleneck.

Should be less than 10 threads waiting on average.
Exchange 2007 Hub Transport Role Counters (Advanced)

This template contains advanced performance and statistics counters for monitoring Exchange 2007 Hub Transport Role. Some of the counters may require manual configuration, such as setting up installation-specific instances, correcting thresholds for the client's environment, and so forth. Use this template in addition to the Exchange 2007 Hub Transport Role Services and Counters (Basic) template.

Prerequisites

RPC and WMI access to the Exchange server.

Credentials

Windows Administrator on the target server.

Monitored Components

These performance counters are based on the following information:


Dumpster Size

Shows the total size (in bytes) of mail items currently in the transport dumpster on this server.

Dumpster Inserts/sec

Shows the rate at which items are inserted into the transport dumpster on this server. Determines the current rate of transport dumpster inserts.

Dumpster Item Count

Shows the total number of mail items currently in the transport dumpster on this server. Shows the current number of items being held in the transport dumpster.

Dumpster Deletes/sec

Shows the rate at which items are deleted from the transport dumpster on this server. Determines the current rate of transport dumpster deletions.

I/O Log Writes/sec (database)

Shows the rate of log file write operations completed. Determines the current load. Compare values to historical baselines.

I/O Log Reads/sec (database)

Shows the rate of log file read operations completed. Determines the current load. Compare values to historical baselines.
Log Generation Checkpoint Depth (database)

Represents the amount of work (in count of log files) that needs to be redone or undone to the database files if the process fails.

Should be less than 1,000 at all times.

I/O Database Reads/sec (database)

Shows the rate of database read operations completed. Determines the current load. Compare values to historical baselines.

I/O Database Writes/sec

Shows the rate of database write operations completed. Determines the current load. Compare values to historical baselines.

Messages Submitted Per Second

Shows the number of messages queued in the Submission queue per second. Determines the current load. Compare values to historical baselines.

Messages Received/sec

Shows the number of messages received by the SMTP server each second. Determines the current load. Compare values to historical baselines.

Messages Sent/sec

Shows the number of messages sent by the SMTP send connector each second. Determines the current load. Compare values to historical baselines.

Messages Queued for Delivery Per Second

Shows the number of messages queued for delivery per second. Determines the current load. Compare values to historical baselines.

Messages Completed Delivery Per Second

Shows the number of messages delivered per second. Determines the current load. Compare values to historical baselines.

Avg. Disk sec/Read (Physical Disk)

Shows the average time, in seconds, of a read of data from the disk.

Should be less than 20 milliseconds (ms) on average. Spikes (maximum values) should not be higher than 50 ms.

When looking at hard disks using perfmon.exe, an understanding of the underlying hard disk subsystem is required to determine which counters (physical disk or logical disk) to look at.

Avg. Disk sec/Write (Physical Disk)

Shows the average time, in seconds, of a write of data to the disk.
Should be less than 20 milliseconds (ms) on average. Spikes (maximum values) should not be higher than 50 ms.

When looking at hard disks using \texttt{Perfmon.exe}, an understanding of the underlying hard disk subsystem is required to determine which counters (physical disk or logical disk) to look at.

\textbf{Avg. Disk sec/Read (Logical Disk)}

Shows the average time, in seconds, of a read of data from the disk.

Should be less than 20 milliseconds (ms) on average. Spikes (maximum values) should not be higher than 50 ms.

When looking at hard disks using \texttt{Perfmon.exe}, an understanding of the underlying hard disk subsystem is required to determine which counters (physical disk or logical disk) to look at.

\textbf{Avg. Disk sec/Write (Logical Disk)}

Shows the average time, in seconds, of a write of data to the disk.

Should be less than 20 milliseconds (ms) on average. Spikes (maximum values) should not be higher than 50 ms.

When looking at hard disks using \texttt{Perfmon.exe}, an understanding of the underlying hard disk subsystem is required to determine which counters (physical disk or logical disk) to look at.

\textbf{Retry Non-Smtp Delivery Queue Length}

Shows the number of messages in a retry state in the non-SMTP gateway delivery queues.

Should not exceed 100.

\textbf{Largest Delivery Queue Length}

Shows the number of messages in the largest delivery queues.

Should be less than 200 for the Edge Transport and Hub Transport server roles.

\textbf{Version buckets allocated (database)}

Total number of version buckets allocated. Shows the default backpressure values as listed in the \texttt{edgetransport.exe.config} file.

Should be less than 200 at all times.

\textbf{Log Record Stalls/sec (database)}

Shows the number of log records that cannot be added to the log buffers per second because they are full. If this counter is nonzero most of the time, the log buffer size may be a bottleneck.
Should be less than 10 per second on average. Spikes (maximum values) should not be greater than 100 per second.

**Log Threads Waiting (database)**

Shows the number of threads waiting for their data to be written to the log to complete an update of the database. If this number is too high, the log may be a bottleneck.

Should be less than 10 threads waiting on average.
Exchange 2007 Mailbox Role Counters (Advanced)

This template contains advanced performance and statistics counters for monitoring Exchange 2007 Mailbox Role. Some of the counters may require manual configuration, such as setting up installation-specific instances, correcting thresholds for the client's environment, and so forth. Use this template in addition to the Exchange 2007 Mailbox Role Services and Counters (Basic) template.

**Prerequisites**

RPC and WMI access to the Exchange server.

**Credentials**

Windows Administrator on the target server.

**Monitored Components**


These performance counters are based on the following information:

Monitoring Mailbox Servers: Exchange 2007 Help, "Microsoft TechNet":


**Messages Sent/sec**

Shows the rate that messages are sent to transport.

Used to determine current messages sent to transport.

**Directory Access: LDAP Reads/sec**

Shows the current rate that the Lightweight Directory Access Protocol (LDAP) reads occur while processing requests for the client.

Used to determine the current LDAP read rate per protocol.

**Directory Access: LDAP Searches/sec**

Shows the current rate that the LDAP searches occur while processing requests for the client.

Used to determine the current LDAP search rate per protocol.

**User Count (Information Store)**

Shows the number of users connected to the information store.

Used to determine current user load.

**% Processor time (Exchange Search)**

Shows the amount of processor time that is currently being consumed by the Exchange Search service.
Should be less than 1% of overall CPU typically and not sustained above 5%.

% Processor Time (msftefd)

Shows the amount of processor time that is being consumed to update content indexing within the store process.

Should be less than 10% of what the store process is during steady state.

Full crawls will increase overall processing time, but should never exceed overall store CPU capacity. Check throttling counters to determine if throttling is occurring due to server performance bottlenecks.

Throttling Delay Value

Shows the total time, in milliseconds, a worker thread sleeps before it retrieves a document from the Microsoft Exchange Information Store service. This is set by the throttling monitor thread.

Indicates the current throttling delay value. If this value is nonzero, this indicates a potential server bottleneck causing delay values to be introduced to throttle the rate at which indexing is occurring.

In the instance field, you can specify your own mailbox database or use the default value. Use perfmon.exe to determine the name of the instance. Default value: instance=_total.

% Processor Time (Mailbox Assistants)

Shows the amount of processor time that is being consumed by mailbox assistants.

Should be less than 5% of overall CPU capacity.

Average Event Processing Time in Seconds

Shows the average processing time of the events chosen.

Should be less than 2 at all times.

In the instance field, you can specify your own mailbox database or use the default value. Use perfmon.exe to determine the name of the instance. Default value: instance=msexchangemailboxassistants-total.

Average Resource Booking Processing Time

Shows the average time to process an event in the Resource Booking Attendant.

Should be a low value at all times. High values may indicate a performance bottleneck.

Requests Failed (resource booking)

Shows the total number of failures that occurred while the Resource Booking Attendant was processing events.

Should be 0 at all times.

Average Calendar Attendant Processing time

Shows the average time to process an event in the Calendar Attendant.
Should be a low value at all times. High values may indicate a performance bottleneck.

**Requests Failed (calendar attendant)**

Shows the total number of failures that occurred while the Calendar Attendant was processing events.

Should be 0 at all times.

**Information Store: RPC Requests**

Indicates the overall RPC requests that are currently executing within the information store process.

Should be below 70 at all times.

The maximum value in Exchange 2007 is 500 RPC requests that can execute at any designated time before the information store starts rejecting any new connections from clients.

**Information Store: RPC Averaged Latency**

Indicates the RPC latency, in milliseconds, averaged for all operations in the last 1,024 packets. For information about how clients are affected when overall server RPC averaged latencies increase, see "Understanding Client Throttling" at: [http://go.microsoft.com/fwlink/?LinkId=116695](http://go.microsoft.com/fwlink/?LinkId=116695).

Should not be higher than 25 ms on average.

To determine if certain protocols are causing overall RPC latencies, monitor MSExchangeIS Client (\RPC Average Latency to separate latencies based on client protocol. Cross-reference MSExchangeIS\RPC Client Backoff/sec to ensure higher latencies are not causing client throttling.

**Information Store: RPC Client Backoff/sec**

Shows the rate that the server notifies the client to back off. Indicates the rate at which client backoffs are occurring. Higher values may indicate that the server may be incurring a higher load resulting in an increase in overall averaged RPC latencies, causing client throttling to occur. This can also occur when certain client user actions are being performed. Depending on what the client is doing and the rate at which RPC operations are occurring, it may be normal to see backoffs occurring.

**Database: Database Page Fault Stalls/sec**

Shows the rate that database file page requests require of the database cache manager to allocate a new page from the database cache.

This should be 0 at all times.

If this value is nonzero, this indicates that the database is not able to flush dirty pages to the database file fast enough to make pages free for new page allocations.

**Database: Log Record Stalls/sec**

Shows the number of log records that cannot be added to the log buffers per second because the log buffers are full. If this counter is nonzero most of the time, the log buffer size may be a bottleneck.

The average value should be below 10 per second.
Spikes (maximum values) should not be higher than 100 per second.

**Database: Version buckets allocated**

Shows the total number of version buckets allocated.

Should be less than 12,000 at all times.

The maximum default version is 16,384. If version buckets reach 70 percent of maximum, the server is at risk of running out of the version store.

**Database Cache Size (MB)**

Shows the amount of system memory, in megabytes, used by the database cache manager to hold commonly used information from the database files to prevent file operations. If the database cache size seems too small for optimal performance and there is little available memory on the system (check the value of Memory/Available Bytes), adding more memory to the system may increase performance. If there is ample memory on the system and the database cache size is not growing beyond a certain point, the database cache size may be capped at an artificially low limit. Increasing this limit may increase performance.

Maximum value is RAM-2GB (RAM-3GB for servers with sync replication enabled). This and Database Cache Hit % are extremely useful counters for gauging whether a server’s performance problems might be resolved by adding more physical memory.

Use this counter along with store private bytes to determine if there are store memory leaks.

Note: Set the thresholds as appropriate for your environment.

**Average Document Indexing Time**

Shows the average, in milliseconds, of how long it takes to index documents.

Should be less than 30 seconds at all time.

Note: In the instance field, you can specify your own mailbox database or use the default value. Use perfmon.exe to determine the name of the instance. Default value: instance=_total.

**Events in queue**

Shows the number of events in the in-memory queue waiting to be processed by the assistants.

Should be a low value at all times. High values may indicate a performance bottleneck.

Note: In the instance field, you can specify your own mailbox database or use the default value. Use perfmon.exe to determine the name of the instance. Default value: instance=msexchangemailboxassistants_total.

**RPC Latency average (msec)**

Shows the average latency, in milliseconds, of RPC requests. The average is calculated over all RPCs since exrpc32 was loaded.

Should be less than 100 ms at all times.
Failed Submissions Per Second

Shows the number of failed submissions per second.
Should be 0 at all times.
Exchange 2007 Outlook Web Access (OWA) Form Login

This template helps you check the availability of the OWA service for end-users by performing the user login procedure. The template collects response times for login procedure.

Prerequisites

A functioning Exchange OWA server.

Credentials

Valid Exchange OWA user name and password.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

HTTP Form Login Monitor

Performs a user login procedure and returns the length of time it takes to log in.
Exchange 2007 Unified Messaging Role Counters (Advanced)

This template contains advanced performance and statistics counters for monitoring Exchange 2007 Unified Messaging Role. Some of the counters may require manual configuration, such as setting up installation-specific instances, correcting thresholds for the client's environment, and so forth. Use this template in addition to the Exchange 2007 Unified Messaging Role Service and Counters (Basic) template.

Prerequisites

RPC and WMI access to the Exchange server.

Credentials

Windows Administrator on the target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

These performance counters are based on the following information:


**Queued OCS User Event Notifications**

Shows the number of notifications that have been created and not yet submitted for delivery.

Should be 0 at all times.

Represents the number of missed call notifications that have been generated in the Office Communications Server environment and have not been submitted for delivery.

**Unhandled Exceptions/sec**

Shows the number of calls that were disconnected after an internal system error occurred in the last second.

Should be 0 at all times.

**Mailbox Server Access Failures**

Shows the number of times the system did not access a Mailbox server.

Should be 0 at all times.

A non-zero value indicates that Unified Messaging is having problems with MAPI connectivity to mbx servers.

**Call Answer Queued Messages**

Shows the number of messages created and not yet submitted for delivery.
Should be less than 50 at all times.

**Hub Transport Access Failures**

Shows the number of times that attempts to access a Hub Transport server failed. This number is only incremented if all Hub Transport servers were unavailable.

Should be 0 at all times.
Exchange 2007 — 2010 Client Access Role Services and Counters (Basic)

This template contains basic performance counters and services for monitoring the Exchange 2007 and 2010 Client Access Role. This template is designed to work out of the box and does not require any additional configuration. If you need more detailed monitoring, you should use it in combination with the Exchange 2007 and 2010 Client Access Role Counters (Advanced) template.

**Prerequisites**

- RPC and WMI access to the Exchange server.

**Credentials**

- Windows Administrator on target server.

**Monitored Components**

For details on monitors, see [SAM Component Monitor Types](#).

These performance counters and services are based on the following information:


**Service: Exchange Active Directory Topology**

- Provides Active Directory topology information to Exchange services. If this service is stopped, most Exchange services are unable to start. This service has no dependencies.

**Service: Exchange File Distribution Service**

- Distributes offline address book (OAB) and custom Unified Messaging prompts. This service is dependent on the Microsoft Exchange Active Directory Topology and Workstation services.

**Service: Exchange IMAP4**

- Provides IMAP4 service to clients. If this service is stopped, clients will not be able to connect to this computer using the IMAP4 protocol. This service is dependent upon the Microsoft Exchange Active Directory Topology service.

**Service: Exchange Monitoring**

- Allows applications to call the Exchange diagnostic cmdlets. This service has no dependencies.
**Service: Exchange POP3**

Provides POP3 service to clients. If this service is stopped, clients cannot connect to this computer using the POP3 protocol. This service is dependent on the Microsoft Exchange Active Directory Topology service.

**Service: Exchange Service Host**

Provides a host for several Exchange services. On internal server roles, this service is dependent on the Microsoft Exchange Active Directory Topology service. On Edge Transport servers, this service is dependent upon the Microsoft Exchange ADAM service.

**Average Search Time**

Shows the average time that elapsed while waiting for a search to complete.

Should be less than 5,000 milliseconds (ms) at all times.

**Average Time to Process a Free Busy Request**

Shows the average time to process a free/busy request in seconds. One request may contain multiple mailboxes. Free/busy responses do not have meeting suggestions.

Should always be less than 5.

**Requests Queued**

Shows the number of HTTP requests waiting to be assigned to a thread.

Average of 50-100.

**Download Task Queued**

Shows the number of OAB download tasks queued since the File Distribution service started.

Should be 0 at all times.

Values greater than 0 indicate a failure to copy OAB data files from Mailbox servers.
Exchange 2007 — 2010 Common Performance Counters

This template contains common Exchange and OS performance counters (CPU usage, available memory, LDAP times, etc.) that can be monitored for all Exchange 2007 — 2010 roles. This template requires additional configuration, and can be used together with other Exchange 2007 — 2010 templates.

Prerequisites

RPC and WMI access to the Exchange server.

Credentials

Windows Administrator on target server.

Monitored Components

For details on monitors, see [SAM Component Monitor Types](#).

These performance counters are based on the following information:

Monitoring Common Counters: Exchange 2007 Help, "Microsoft TechNet":

Common Counters: Exchange 2010 Help, "Microsoft TechNet":

**% Processor Time**

Shows the percentage of time that the processor is executing application or operating system processes. This is when the processor is not idle.

Should be less than 75% on average.

**Available Mbytes (memory)**

Shows the amount of physical memory, in MBs, immediately available for allocation to a process or for system use. It is equal to the sum of memory assigned to the standby (cached), free, and zero page lists. For a full explanation of the memory manager, refer to Microsoft Developer Network (MSDN) or System Performance and Troubleshooting Guide in the Windows Server 2003 Resource Kit.

Should remain above 100 MB at all times.

**.NET CLR Memory: % Time in GC**

Shows when garbage collection has occurred. When the counter exceeds the threshold, it indicates that the CPU is cleaning up and is not being used efficiently for load. Adding memory to the server would improve this situation.

Should be below 10% on average.
If this counter increases to a high value, there might be some objects that are surviving Gen 1 garbage collections and being promoted to Gen 2. Gen 2 collections require a full global catalog for clean up. Add other .NET Framework memory counters to determine if this is the case.

**.NET CLR Exceptions: # of Excepts Thrown / sec**

Displays the number of exceptions thrown per second. These include both .NET Framework exceptions and unmanaged exceptions that get converted into .NET Framework exceptions. For example, the null pointer reference exception in unmanaged code would get thrown again in managed code as a .NET Framework System.NullReferenceException. This counter includes both handled and unhandled exceptions.

Should be less than 5% of total requests per second

Exceptions should only occur in rare situations and not in the normal control flow of the program. This counter was designed as an indicator of potential performance problems due to a large (greater than 100 sec) rate of exceptions thrown. This counter is not an average over time. It displays the difference between the values observed in the last two samples divided by the duration of the sample interval.

**LDAP Search Time**

Shows the time (in ms) to send an LDAP search request and receive a response.

Should be below 50 ms on average. Spikes (maximum values) should not be higher than 100 ms.

Note: The instance field is installation-specific. You need to specify the full DNS name of the Domain Controller (for example: `dc.example.com`).

**LDAP Read Time**

Shows the time in milliseconds (ms) to send an LDAP read request to the specified domain controller and receive a response.

Should be below 50 ms on average. Spikes (maximum values) should not be higher than 100 ms.

Note: The instance field is installation-specific. You need to specify the full DNS name of the Domain Controller (for example: `dc.example.com`).

**LDAP Searches timed out per minute**

Shows the number of LDAP searches that returned LDAP_Timeout during the last minute.

Should be below 10 at all times for all roles.

Higher values may indicate issues with Active Directory resources.

Note: The instance field is installation-specific. You need to specify the full DNS name of the Domain Controller (for example: `dc.example.com`).

**Long running LDAP operations/Min**

Shows the number of LDAP operations on this domain controller that took longer than the specified threshold per minute. (Default threshold is 15 seconds.)

Should be less than 50 at all times.
Higher values may indicate issues with Active Directory resources.

Note: The instance field is installation-specific. You need to specify the full DNS name of the Domain Controller (for example: dc.example.com).

**Page Reads/sec (memory)**

Indicates data must be read from the disk instead of memory. Indicates there is not enough memory and paging is beginning. A value of more than 30 per second means the server is no longer keeping up with the load.

Should be less than 100 on average.
Exchange 2007 – 2010 Edge Transport Role Services and Counters (Basic)

This template contains basic performance counters and services for monitoring Exchange 2007 and 2010 Edge Transport Role. This template is designed to work out of the box and does not require any additional configuration. If you need more detailed monitoring, you should use it in combination with the Exchange 2007 (2010) Edge Transport Role Counters (Advanced) template.

Prerequisites

RPC and WMI access to the Exchange server.

Credentials

Windows Administrator on target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

These performance counters and services are based on the following information:


Transport Server Counters: Exchange 2010 Help, "Microsoft TechNet":

Service: Exchange ADAM

Stores configuration data and recipient data on the Edge Transport server. This service represents the named instance of Active Directory Lightweight Directory Service (AD LDS) that is automatically created by Setup during Edge Transport server installation. This service is dependent on the COM+ Event System service.

Service: Exchange Anti-spam Update

Provides the Microsoft Forefront Protection 2010 for Exchange Server anti-spam update service. On Hub Transport servers, this service is dependent on the Microsoft Exchange Active Directory Topology service. On Edge Transport servers, this service is dependent on the Microsoft Exchange ADAM service.

Service: Exchange Monitoring

Allows applications to call the Exchange diagnostic cmdlets. This service has no dependencies.
Service: Exchange Transport

Provides SMTP server and transport stack. On Hub Transport servers, this service is dependent on the Microsoft Exchange Active Directory Topology service. On Edge Transport servers, this service is dependent on the Microsoft Exchange ADAM service.

Service: Exchange Transport Log Search

Provides remote search capability for Microsoft Exchange Transport log files. On Hub Transport servers, this service is dependent on the Microsoft Exchange Active Directory Topology service. On Edge Transport servers, this service is dependent on the Microsoft Exchange ADAM service.

Aggregate Delivery Queue Length (All Queues)

Shows the number of messages queued for delivery in all queues.

Should be less than 3,000 and not more than 5,000.

Active Remote Delivery Queue Length

Shows the number of messages in the active remote delivery queues.

Should be less than 250 at all times.

Active Mailbox Delivery Queue Length

Shows the number of messages in the active mailbox queues.

Should be less than 250 at all times.

Submission Queue Length

Shows the number of messages in the submission queue.

Should not exceed 100.

If sustained high values are occurring, investigate Active Directory and Mailbox servers for bottlenecks or performance-related issues.

Active Non-Smtp Delivery Queue Length

Shows the number of messages in the drop directory used by a Foreign connector.

Should be less than 250 at all times.

Retry Mailbox Delivery Queue Length

Shows the number of messages in a retry state attempting to deliver a message to a remote mailbox.

Should be less than 100 at all times.

Retry Remote Delivery Queue Length

Shows the number of messages in a retry state in the remote delivery queues.

Should not exceed 100.

We recommend that you check the next hop to determine the causes for queuing.
Unreachable Queue Length

Shows the number of messages in the Unreachable queue.
Should not exceed 100.

Poison Queue Length

Shows the number of messages in the poison message queue.
Should be 0 at all times.

Exchange 2007 — 2010 Hub Transport Role Services and Counters (Basic)

This template contains basic performance counters and services for monitoring Exchange 2007 — 2010 Hub Transport Role. This template is designed to work out of the box and does not require any additional configuration. If you need more detailed monitoring, you should use it in combination with the Exchange 2007 — 2010 Hub Transport Role Counters (Advanced) template.

Prerequisites: RPC and WMI access to the Exchange server.

Credentials: Windows Administrator on target server.

Monitored Components:

These performance counters and services are based on the following information:


Service: Exchange Active Directory Topology

Provides Active Directory topology information to Exchange services. If this service is stopped, most Exchange services are unable to start. This service has no dependencies.

Service: Exchange EdgeSync

Connects to an AD LDS instance on subscribed Edge Transport servers over a secure LDAP channel to synchronize data between a Hub Transport server and an Edge Transport server. This service is dependent on the Microsoft Exchange Active Directory Topology service. If Edge Subscription is not configured, this service can be disabled.

Service: Exchange Anti-spam Update

Provides the Microsoft Forefront Protection 2010 for Exchange Server anti-spam update service. On Hub Transport servers, this service is dependent on the Microsoft Exchange Active Directory Topology service. On Edge Transport servers, this service is dependent on the Microsoft Exchange ADAM service.
Service: Exchange Monitoring

Allows applications to call the Exchange diagnostic cmdlets. This service has no dependencies.

Service: Exchange Transport

Provides SMTP server and transport stack. On Hub Transport servers, this service is dependent on the Microsoft Exchange Active Directory Topology service. On Edge Transport servers, this service is dependent on the Microsoft Exchange ADAM service.

Service: Exchange Transport Log Search

Provides remote search capability for Microsoft Exchange Transport log files. On Hub Transport servers, this service is dependent on the Microsoft Exchange Active Directory Topology service. On Edge Transport servers, this service is dependent on the Microsoft Exchange ADAM service.

Aggregate Delivery Queue Length (All Queues)

Shows the number of messages queued for delivery in all queues.

Should be less than 3,000 and not more than 5,000.

Active Remote Delivery Queue Length

Shows the number of messages in the active remote delivery queues.

Should be less than 250 at all times.

Active Mailbox Delivery Queue Length

Shows the number of messages in the active mailbox queues.

Should be less than 250 at all times.

Submission Queue Length

Shows the number of messages in the submission queue.

Should not exceed 100.

If sustained high values are occurring, investigate Active Directory and Mailbox servers for bottlenecks or performance-related issues.

Active Non-Smtp Delivery Queue Length

Shows the number of messages in the drop directory used by a Foreign connector.

Should be less than 250 at all times.

Retry Mailbox Delivery Queue Length

Shows the number of messages in a retry state attempting to deliver a message to a remote mailbox.

Should be less than 100 at all times.

Retry Remote Delivery Queue Length

Shows the number of messages in a retry state in the remote delivery queues.

Should not exceed 100.
We recommend that you check the next hop to determine the causes for queuing.

**Unreachable Queue Length**

Shows the number of messages in the Unreachable queue.

Should not exceed 100.

**Poison Queue Length**

Shows the number of messages in the poison message queue.

Should be 0 at all times.
Exchange 2007 — 2010 Unified Messaging Role Services and Counters (Basic)

This template contains basic performance counters and services for monitoring Exchange 2007 and 2010 Unified Messaging Role. This template is designed to work out of the box and does not require any additional configuration. If you need more detailed monitoring, you should use it in combination with the Exchange 2007 (2010) Unified Messaging Role Counters (Advanced) template.

Prerequisites

RPC and WMI access to the Exchange server.

Credentials

Windows Administrator on target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

These performance counters and services are based on the following information:


Service: Exchange Active Directory Topology

Provides Active Directory topology information to Exchange services. If this service is stopped, most Exchange services are unable to start. This service has no dependencies.

Service: Exchange File Distribution Service

Distributes offline address book (OAB) and custom Unified Messaging prompts. This service is dependent on the Microsoft Exchange Active Directory Topology and Workstation services.

Service: Exchange Monitoring

Allows applications to call the Exchange diagnostic cmdlets. This service has no dependencies.

Service: Exchange Speech Engine

Provides speech processing services for Unified Messaging (UM). This service is dependent on the Windows Management Instrumentation (WMI) service.
Service: Exchange Unified Messaging

Enables Microsoft Exchange Unified Messaging features. This allows voice and fax messages to be stored in Exchange and gives users telephone access to e-mail, voice mail, calendar, contacts, or an auto attendant. If this service is stopped, Unified Messaging is not available. This service is dependent on the Microsoft Exchange Active Directory Topology and the Microsoft Exchange Speech Engine service.

Directory Access Failures

Shows the number of times that attempts to access Active Directory failed.

Should be 0 at all times.

Operations over Six Seconds

Shows the number of all UM operations that took more than six seconds to complete. This is the time during which a caller was waiting for UM to respond.

Should be 0 at all times.

CallsDisconnected by Callers During UM Audio Hourglass

Shows the number of calls during which the caller disconnected while Unified Messaging was playing the audio hourglass tones.

Should be 0 at all times.

A nonzero value suggests excessive latency between a Unified Messaging server and targeted domain controller.
Exchange 2010 Client Access Role Counters (Advanced)

This template contains advanced performance and statistics counters for monitoring the Exchange Client Access Role. Some counters may require manual configuration, such as setting up installation-specific instances and correcting thresholds for the client's environment. Use this template in addition to the Exchange 2007 — 2010 Client Access Role Services and Counters (Basic) template.

Prerequisites

RPC and WMI access to the Exchange server.

Credentials

Windows Administrator on target server.

Monitored Components

These performance counters are based on the following information:

Client Access Server Counters: Exchange 2010 Help, "Microsoft TechNet":

RPC Operations/sec

Shows the rate at which RPC operations occur, per second.

Referral RPC Requests Average Latency

This is Exchange 2010 address book service counter. Shows the average time, in ms, that referral requests took to complete during the sampling period.

Should be below 1,000 ms.

Requests - Average Response Time

Shows the average time (in ms) the Exchange Control Panel took to respond to a request during the sampling period.

The average should be under 6,000 ms.

ActiveSync: Requests/sec

Shows the number of HTTP requests received from the client via ASP.NET per second.

Determines the current Exchange ActiveSync request rate.

OWA: Current Unique Users

Shows the number of unique users currently logged on to Outlook Web App. This value monitors the number of unique active user sessions, so that users are only removed from this counter after they log off or their session times out.
Determines current user load.

**OWA: Requests/sec**

Shows the number of requests handled by Outlook Web App per second.

Determines current user load.

**Web Service: Current Connections**

Shows the current number of connections established with the Web service.

Determines current user load.

**Requests - Activations/sec**

Shows the number of requests activated per second in the Exchange Control Panel.

**Connection Count**

This is RPC Client Access load counter. Shows the total number of client connections maintained.

**NSPI Connections Current**

This is Exchange Address Book load counter. Shows the number of NSPI clients currently connected to the server.

**NSPI RPC Requests/sec**

This is Exchange Address Book load counter. Shows the rate at which NSPI requests occur each second.
Exchange 2010 Edge Transport Role Counters (Advanced)

This template contains advanced performance and statistics counters for monitoring Exchange 2010 Edge Transport Role. Some of the counters may require manual configuration, such as setting up installation-specific instances, correcting thresholds for the client's environment, and so forth. Use this template in addition to the Exchange 2007 — 2010 Edge Transport Role Services and Counters (Basic) template.

Prerequisites

RPC and WMI access to the Exchange server.

Credentials

Windows Administrator on the target server.

Monitored Components

For details on monitors, see [SAM Component Monitor Types](#).

These performance counters are based on the following information:

Transport Server Counters: Exchange 2010 Help, "Microsoft TechNet":

**Dumpster Size**

Shows the total size (in bytes) of mail items currently in the transport dumpster on this server.

**Dumpster Inserts/sec**

Shows the rate at which items are inserted into the transport dumpster on this server. Determines the current rate of transport dumpster inserts.

**Dumpster Item Count**

Shows the total number of mail items currently in the transport dumpster on this server. Shows the current number of items being held in the transport dumpster.

**Dumpster Deletes/sec**

Shows the rate at which items are deleted from the transport dumpster on this server. Determines the current rate of transport dumpster deletions.

**I/O Log Writes/sec (database)**

Shows the rate of log file write operations completed. Determines the current load. Compare values to historical baselines.

**I/O Log Reads/sec (database)**

Shows the rate of log file read operations completed. Determines the current load. Compare values to historical baselines.
Log Generation Checkpoint Depth (database)

Represents the amount of work (in count of log files) that needs to be redone or undone to the database files if the process fails.

Should be less than 1,000 at all times.

I/O Database Reads/sec (database)

Shows the rate of database read operations completed. Determines the current load. Compare values to historical baselines.

I/O Database Writes/sec

Shows the rate of database write operations completed. Determines the current load. Compare values to historical baselines.

Messages Submitted Per Second

Shows the number of messages queued in the Submission queue per second. Determines current load. Compare values to historical baselines.

Messages Received/sec

Shows the number of messages received by the SMTP server each second. Determines current load. Compare values to historical baselines.

Messages Queued for Delivery Per Second

Shows the number of messages queued for delivery per second. Determines current load. Compare values to historical baselines.

Messages Completed Delivery Per Second

Shows the number of messages delivered per second. Determines current load. Compare values to historical baselines.

Avg. Disk sec/Read (Physical Disk)

Shows the average time, in seconds, of a read of data from the disk.

Should be less than 20 milliseconds (ms) on average. Spikes (maximum values) should not be higher than 50 ms.

When looking at hard disks using perfmon.exe, an understanding of the underlying hard disk subsystem is required to determine which counters (physical disk or logical disk) to look at.

Avg. Disk sec/Write (Physical Disk)

Shows the average time, in seconds, of a write of data to the disk.

Should be less than 20 milliseconds (ms) on average. Spikes (maximum values) should not be higher than 50 ms.

When looking at hard disks using perfmon.exe, an understanding of the underlying
A hard disk subsystem is required to determine which counters (physical disk or logical disk) to look at.

**Avg. Disk sec/Read (Logical Disk)**

Shows the average time, in seconds, of a read of data from the disk.

Should be less than 20 milliseconds (ms) on average. Spikes (maximum values) shouldn't be higher than 50 ms.

When looking at hard disks using `perfmon.exe`, an understanding of the underlying hard disk subsystem is required to determine which counters (physical disk or logical disk) to look at.

**Avg. Disk sec/Write (Logical Disk)**

Shows the average time, in seconds, of a write of data to the disk.

Should be less than 20 milliseconds (ms) on average. Spikes (maximum values) shouldn't be higher than 50 ms.

When looking at hard disks using `perfmon.exe`, an understanding of the underlying hard disk subsystem is required to determine which counters (physical disk or logical disk) to look at.

**Retry Non-Smtp Delivery Queue Length**

Shows the number of messages in a retry state in the non-SMTP gateway delivery queues.

Should not exceed 100.

**Largest Delivery Queue Length**

Shows the number of messages in the largest delivery queues.

Should be less than 200 for the Edge Transport and Hub Transport server roles.

**Version buckets allocated (database)**

Total number of version buckets allocated. Shows the default backpressure values as listed in the `edgetransport.exe.config` file.

Should be less than 200 at all times.

**Log Record Stalls/sec (database)**

Shows the number of log records that cannot be added to the log buffers per second because they are full. If this counter is nonzero most of the time, the log buffer size may be a bottleneck.

Should be less than 10 per second on average. Spikes (maximum values) should not be greater than 100 per second.
Log Threads Waiting (database)

Shows the number of threads waiting for their data to be written to the log to complete an update of the database. If this number is too high, the log may be a bottleneck.

Should be less than 10 threads waiting on average.

Event: Resource Pressure Increased

Event ID: 15004

This monitor returns number of the following events: Resource pressure increased from Previous Utilization Level to Current Utilization Level. Examine details of the events for additional information.

Event: Resource Pressure Occurs

Event ID: 15002

This monitor returns number of the following events: Resource pressure that occurs and is constant. Examine details of the events for additional information.
Exchange 2010 Hub Transport Role Counters (Advanced)

This template contains advanced performance and statistics counters for monitoring Exchange 2010 Hub Transport Role. Some of the counters may require manual configuration, such as setting up installation-specific instances, correcting thresholds for the client's environment, and so forth. Use this template in addition to the Exchange 2010 Hub Transport Role Services and Counters (Basic) template.

Periodically, SolarWinds releases SAM templates to support the latest product versions such as Microsoft Server 2016. You can continue using templates for older product versions, but updating to the latest template is recommended.

Prerequisites
- RPC and WMI access to the Exchange server.

Credentials
- Windows Administrator on target server.

Monitored Components

For details on monitors, see [SAM Component Monitor Types](#).

These performance counters are based on the following information:

Transport Server Counters: Exchange 2010 Help, "Microsoft TechNet":

Dumpster Size
- Shows the total size (in bytes) of mail items currently in the transport dumpster on this server.

Dumpster Inserts/sec
- Shows the rate at which items are inserted into the transport dumpster on this server. Determines the current rate of transport dumpster inserts.

Dumpster Item Count
- Shows the total number of mail items currently in the transport dumpster on this server. Shows the current number of items being held in the transport dumpster.

Dumpster Deletes/sec
- Shows the rate at which items are deleted from the transport dumpster on this server. Determines the current rate of transport dumpster deletions.

I/O Log Writes/sec (database)
- Shows the rate of log file write operations completed. Determines the current load. Compare values to historical baselines.
I/O Log Reads/sec (database)

Shows the rate of log file read operations completed. Determines the current load. Compare values to historical baselines.

Log Generation Checkpoint Depth (database)

Represents the amount of work (in count of log files) that needs to be redone or undone to the database files if the process fails.

Should be less than 1,000 at all times.

I/O Database Reads/sec (database)

Shows the rate of database read operations completed. Determines the current load. Compare values to historical baselines.

I/O Database Writes/sec

Shows the rate of database write operations completed. Determines the current load. Compare values to historical baselines.

Messages Submitted Per Second

Shows the number of messages queued in the Submission queue per second. Determines current load. Compare values to historical baselines.

Messages Received/sec

Shows the number of messages received by the SMTP server each second. Determines current load. Compare values to historical baselines.

Messages Sent/sec

Shows the number of messages sent by the SMTP send connector each second. Determines current load. Compare values to historical baselines.

Messages Queued for Delivery Per Second

Shows the number of messages queued for delivery per second. Determines current load. Compare values to historical baselines.

Messages Completed Delivery Per Second

Shows the number of messages delivered per second. Determines current load. Compare values to historical baselines.

Avg. Disk sec/Read (Physical Disk)

Shows the average time, in seconds, of a read of data from the disk.

Should be less than 20 milliseconds (ms) on average. Spikes (maximum values) should not be higher than 50 ms.

When looking at hard disks using perfmon.exe, an understanding of the underlying hard disk subsystem is required to determine which counters (physical disk or logical
Avg. Disk sec/Write (Physical Disk)

Shows the average time, in seconds, of a write of data to the disk.

Should be less than 20 milliseconds (ms) on average. Spikes (maximum values) should not be higher than 50 ms.

When looking at hard disks using `perfmon.exe`, an understanding of the underlying hard disk subsystem is required to determine which counters (physical disk or logical disk) to look at.

Avg. Disk sec/Read (Logical Disk)

Shows the average time, in seconds, of a read of data from the disk.

Should be less than 20 milliseconds (ms) on average. Spikes (maximum values) should not be higher than 50 ms.

When looking at hard disks using `perfmon.exe`, an understanding of the underlying hard disk subsystem is required to determine which counters (physical disk or logical disk) to look at.

Avg. Disk sec/Write (Logical Disk)

Shows the average time, in seconds, of a write of data to the disk.

Should be less than 20 milliseconds (ms) on average. Spikes (maximum values) should not be higher than 50 ms.

When looking at hard disks using `perfmon.exe`, an understanding of the underlying hard disk subsystem is required to determine which counters (physical disk or logical disk) to look at.

Retry Non-Smtp Delivery Queue Length

Shows the number of messages in a retry state in the non-SMTP gateway delivery queues.

Should not exceed 100.

Largest Delivery Queue Length

Shows the number of messages in the largest delivery queues.

Should be less than 200 for the Edge Transport and Hub Transport server roles.

Version buckets allocated (database)

Total number of version buckets allocated. Shows the default backpressure values as listed in the `edgetransport.exe.config` file.

Should be less than 200 at all times.
Log Record Stalls/sec (database)

Shows the number of log records that cannot be added to the log buffers per second because they are full. If this counter is nonzero most of the time, the log buffer size may be a bottleneck.

Should be less than 10 per second on average. Spikes (maximum values) should not be greater than 100 per second.

Log Threads Waiting (database)

Shows the number of threads waiting for their data to be written to the log to complete an update of the database. If this number is too high, the log may be a bottleneck.

Should be less than 10 threads waiting on average.
Exchange 2010 OWA Form Login (PowerShell)

This template assesses the availability of the Outlook Web Access service for users by performing a user login procedure and returns the length of time it takes to log in.

ℹ️ This template is used for internal OWA. PowerShell is a requirement.

Monitored Components

ℹ️ For details on monitors, see SAM Component Monitor Types.

Exchange 2010 OWA Form Login Monitor

Performs a user login procedure and returns the length of time it takes to log in.
Exchange 2016 Unified Messaging Role Counters (Advanced)

This template contains advanced performance and statistics counters for monitoring Exchange 2016 Unified Messaging Role. Some of the counters may require manual configuration, such as setting up installation-specific instances, correcting thresholds for the client's environment, and so forth. Use this template in addition to the Exchange 2016 Unified Messaging Role Services and Counters (Basic) template.

Prerequisites

RPC and WMI access to the Exchange server.

Credentials

Windows Administrator on the target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

These performance counters are based on the following information:

Unified Messaging Server Counters: Exchange 2010 Help, "Microsoft TechNet":

Average Call Duration

Average Call Duration is the average duration, in seconds, of calls since the service was started.

Total Calls

Total Calls is the number of calls answered or placed since the service was started. Transfers are not included.

User Response Latency

User Response Latency is the average response time, in milliseconds, for the system to respond to a user request. This average is calculated over the last 25 calls. This counter is limited to calls that require significant processing.

Call Answering Calls

Call Answering Calls is the number of diverted calls that were answered on behalf of subscribers.

Percentage of Successful Valid Fax Calls

Percentage of Successful Valid Fax Calls is the percentage of successful valid fax call requests.

% of Failed Mailbox Connection Attempts Over the Last Hour

Shows the percentage of mailbox connection attempts that failed in the last hour.

Should be less than 5%.
% of Inbound Calls Rejected by the UM Service Over the Last Hour

Shows the percentage of inbound calls that were rejected by the Microsoft Exchange Unified Messaging (UM) service over the last hour.

Should be less than 5%.

% of Inbound Calls Rejected by the UM Worker Process Over the Last Hour

Shows the percentage of inbound calls that were rejected by the UM worker process over the last hour.

Should be less than 5%.

% of Messages Successfully Processed Over the Last Hour

Shows the percentage of messages that were successfully processed by the Microsoft Exchange Unified Messaging service over the last hour.

Should be greater than or equal to 95%.

% of Partner Voice Message Transcription Failures Over the Last Hour

Shows the percentage of voice messages for which transcription failed in the last hour.

Should be less than 5%.

Calls Disconnected on Irrecoverable Internal Error

Shows the number of calls disconnected after an internal system error occurred.

Should be 0 at all times.

Total Inbound Calls Rejected by the UM Service

Shows the total number of inbound calls that were rejected by the Microsoft Exchange Unified Messaging Service since the service was started.

Should be 0 at all times.

Exchange 2013 Client Access Role Counters (Advanced)

This template contains advanced performance and statistics counters for monitoring Exchange 2013 Client Access Role. Some of the counters may require manual configuration, such as correcting thresholds for the client's environment. Use this template in addition to the Exchange 2013 Client Access Role Services and Counters (Basic) template.

Prerequisites

RPC and WMI access to the Exchange server.

Credentials

Windows Administrator on target server.
Monitored Components

For details on monitors, see [SAM Component Monitor Types](#).

**ASP.NET: Application Restarts**

This monitor returns the number of times the application has been restarted during the Web server's lifetime. The returned value should be 0 at all times.

- This monitor has the Count statistic as difference option enabled. It will return only new values from the last poll.

**ASP.NET: Worker Process Restarts**

This monitor returns the number of times a worker process has restarted on the computer. The returned value should be 0 at all times.

- This monitor has the Count statistic as difference option enabled. It will return only new values from the last poll.

**ASP.NET: Request Wait Time**

This monitor returns the number of milliseconds the most recent request was waiting in the queue. The returned value should be 0 at all times. Values greater than 0 should be investigated.

**Address Book: NSPI RPC Browse Requests Average Latency**

This monitor returns the average time, in ms, that Name Service Provider Interface (NSPI) browse requests took to complete during the sampling period. The returned value should be below 1,000 ms.

**Address Book: NSPI RPC Requests Average Latency**

This monitor returns the average time, in ms, that NSPI requests took to complete during the sampling period. The returned value should be below 1,000 ms.

**Address Book: Referral RPC Requests Average Latency**

This monitor returns the average time, in ms, that referral requests took to complete during the sampling period. The returned value should be below 1,000 ms.

**Control Panel: Outbound Proxy Requests - Average Response Time**

This monitor returns the average time (in ms) that requests sent to a secondary Client Access server took to complete during the sampling period. The average returned value should be under 6,000 ms.

**Control Panel: Requests - Average Response Time**

This monitor returns the average time (in ms) the Exchange Control Panel took to respond to a request during the sampling period. The average returned value should be under 6,000 ms.
Active Sync: Requests/sec
This monitor returns the number of HTTP requests received from the client via ASP.NET per second. This determines the current Exchange ActiveSync request rate.

Active Sync: Ping Commands Pending
This monitor returns the number of ping commands currently pending on the server. Ping Commands Pending and Sync Commands Pending are the number of hanging requests which should be almost equal to the number of Direct Push and hanging sync users.

Active Sync: Sync Commands Pending
This monitor returns the number of sync commands currently pending on the server. Ping Commands Pending and Sync Commands Pending are the number of hanging requests which should be almost equal to the number of Direct Push and hanging sync users.

Active Sync: Current Requests
This monitor returns the number of HTTP requests waiting to be assigned to a thread. The average returned value should be between 50–100.

Availability Service: Availability Requests (sec)
This monitor returns the number of requests serviced per second. The request can be only for free/busy information, or may include suggestions. One request may contain multiple mailboxes. This helps determine the rate at which Availability service requests are occurring.

OWA: Current Unique Users
This monitor returns the number of unique users currently logged on to Outlook Web Application. This value monitors the number of unique active user sessions so that users are only removed from this counter after they log off or their session times out. This helps determine current user load.

OWA: Requests/sec
This monitor returns the number of requests handled by the Outlook Web Application per second. This helps determine current user load.

Autodiscover: Requests/sec
This monitor returns the number of Autodiscover service requests processed each second. This helps determine current user load.

Web Service: Requests/sec
This monitor returns the number of requests processed each second. This helps determine current user load.

Web Service: Current Connections
This monitor returns the current number of connections established with the Web service. This helps determine current user load.
Web Service: Connection Attempts/sec
This monitor returns the rate that connections to the Web service are being attempted. This helps determine current user load.

Rpc Client Access: Active User Count
This monitor returns the number of unique users that have shown some activity in the last two minutes.

Rpc Client Access: User Count
This monitor returns the number of users connected to the service.

Rpc Client Access: RPC Operations/sec
This monitor returns the rate at which RPC operations occur, per second.

UM Availability: % of Failed Mailbox Connection Attempts Over the Last Hour
This monitor returns the percentage of mailbox connection attempts that failed in the last hour. The returned value should be less than 5%.

UM Availability: % of Inbound Calls Rejected by the UM Service Over the Last Hour
This monitor returns the percentage of inbound calls that were rejected by the Microsoft Exchange Unified Messaging service over the last hour. The returned value should be less than 5%.

UM Availability: % of Inbound Calls Rejected by the UM Worker Process Over the Last Hour
This monitor returns the percentage of inbound calls that were rejected by the UM worker process over the last hour. The returned value should be less than 5%.

UM Availability: % of Messages Successfully Processed Over the Last Hour
This monitor shows the percentage of messages that were successfully processed by the Microsoft Exchange Unified Messaging service over the last hour. The returned value should be greater or equal to 95%.

UM Availability: % of Partner Voice Message Transcription Failures Over the Last Hour
This monitor returns the percentage of voice messages for which transcription failed in the last hour. The returned value should be less than 5%.

UM Availability: Calls Disconnected on Irrecoverable Internal Error
This monitor returns the number of calls disconnected after an internal system error occurred. The returned value should be 0 at all times.

UM General: Calls Disconnected by User Failure
This monitor returns the total number of calls disconnected after too many user entry failures.

UM General: Current Calls
This monitor returns the number of calls that are currently connected to the UM server.
UM General: Total Calls per Second
This monitor returns the number of new calls that have arrived in the last second.

UM General: User Response Latency
This monitor returns the average response time, in milliseconds, for the system to respond to a user request. This average is calculated over the last 25 calls. This counter is limited to calls that require significant processing.

UM Fax: Percentage of Successful Valid Fax Calls
This monitor returns percentage of Successful Valid Fax Calls is the percentage of successful valid fax call requests.

Exchange 2013 Client Access Role Services and Counters (Basic)
This template contains basic performance counters and services for monitoring the Exchange 2013 Client Access Role. This template is designed to work out of the box and does not require any additional configuration. If you need more detailed monitoring, you should use it in combination with the Exchange 2013 Client Access Role Counters (Advanced) template.

Prerequisites
RPC and WMI access to the Exchange server.

Credentials
Windows Administrator on target server.

Monitored Components
For details on monitors, see SAM Component Monitor Types.

Service: Microsoft Exchange Active Directory Topology
This service provides Active Directory topology information to Exchange services. If this service is stopped, most Exchange services will be unable to start.

Service: Microsoft Exchange Service Host
This service provides a host for several Microsoft Exchange services.

Service: Microsoft Exchange POP3
This service provides Post Office Protocol version 3 service to clients. If this service is stopped, clients cannot connect to this computer using the POP3 protocol.

This monitor is disabled by default.
Service: Microsoft Exchange IMAP4

This service provides Internet Message Access Protocol service to clients. If this service is stopped, clients will be unable to connect to this computer using the IMAP4 protocol.

ℹ️ This monitor is disabled by default.

Service: Microsoft Exchange Unified Messaging

This service enables Microsoft Exchange Unified Messaging features. This allows voice and fax messages to be stored in Microsoft Exchange and gives users telephone access to e-mail, voice mail, calendar, contacts, or an auto attendant. If this service is stopped, Unified Messaging will not be available.

OWA: Average Search Time

This monitor returns the average time that elapsed while waiting for a search to complete. The returned value should be less than 5,000 milliseconds (5 seconds) at all times.

ASP.NET Applications: Requests In Application Queue

This monitor returns the number of requests in the application request queue. The returned value should be 0 at all times. Values greater than 0 should be investigated.

Availability Service: Average Time to Process a Free Busy Request

This monitor returns the average time to process a free/busy request, in seconds. One request may contain multiple mailboxes. Free/busy responses do not have meeting suggestions. The returned value should always be less than 5.

Rpc Client Access: RPC Averaged Latency

This monitor returns the latency, in ms, averaged for the past 1,024 packets. The returned value should be below 250 ms.

Rpc Client Access: RPC Requests

This monitor returns the number of client requests currently being processed by the RPC Client Access service. This returned value should not be over 40.

UM Availability: Directory Access Failures

This monitor returns the number of times that attempts to access Active Directory failed. The returned value should be 0 at all times.

UM Availability: Total Inbound Calls Rejected by the UM Service

This monitor returns the total number of inbound calls that were rejected by the Microsoft Exchange Unified Messaging Service since the service was started. The returned value should be 0 at all times.

ℹ️ This monitor has the Count statistic as difference option enabled. It will only return new values from the last poll.
UM Availability: Total Inbound Calls Rejected by the UM Worker Process

This monitor returns the total number of inbound calls that were rejected by the UM Worker process since the service was started. The returned value should be 0 at all times.

- This monitor has the Count statistic as difference option enabled. It will only return new values from the last poll.

UM Performance: Operations over Six Seconds

This monitor returns the number of all UM operations that took more than 6 seconds to complete. This is the time during which a caller was waiting for Unified Messaging to respond. The returned value should be as low as possible.

Exchange 2016 Client Access Role Services and Counters (Basic)

This template contains basic performance counters and services for monitoring the Exchange 2016 Client Access Role. This template is designed to work out of the box and does not require any additional configuration. If you need more detailed monitoring, use this in conjunction with the Exchange 2016 Client Access Role Counters (Advanced) template.

- Periodically, SolarWinds releases SAM templates to support the latest product versions such as Microsoft Server 2016. You can continue using templates for older product versions, but updating to the latest template is recommended.

- To monitor Exchange Server 2016, PowerShell 2.0 or later must be installed and Administrator rights must be granted.

Prerequisites

RPC and WMI access to the Exchange server.

Credentials

Windows Administrator on target server.

Monitored Components

- For details on monitors, see [SAM Component Monitor Types](#).

Service: Microsoft Exchange Active Directory Topology

This service provides Active Directory topology information to Exchange services. If this service is stopped, most Exchange services will be unable to start.

Service: Microsoft Exchange Service Host

This service provides a host for several Microsoft Exchange services.
Service: Microsoft Exchange POP3

This service provides Post Office Protocol version 3 service to clients. If this service is stopped, clients cannot connect to this computer using the POP3 protocol.

This monitor is disabled by default.

Service: Microsoft Exchange IMAP4

This service provides Internet Message Access Protocol service to clients. If this service is stopped, clients will be unable to connect to this computer using the IMAP4 protocol.

This monitor is disabled by default.

Service: Microsoft Exchange Unified Messaging

This service enables Microsoft Exchange Unified Messaging features. This allows voice and fax messages to be stored in Microsoft Exchange and gives users telephone access to e-mail, voice mail, calendar, contacts, or an auto attendant. If this service is stopped, Unified Messaging will not be available.

OWA: Average Search Time

This monitor returns the average time that elapsed while waiting for a search to complete. The returned value should be less than 5,000 milliseconds (5 seconds) at all times.

ASP.NET Applications: Requests In Application Queue

This monitor returns the number of requests in the application request queue. The returned value should be 0 at all times. Values greater than 0 should be investigated.

Availability Service: Average Time to Process a Free Busy Request

This monitor returns the average time to process a free/busy request, in seconds. One request may contain multiple mailboxes. Free/busy responses do not have meeting suggestions. The returned value should always be less than 5.

Rpc Client Access: RPC Averaged Latency

This monitor returns the latency, in ms, averaged for the past 1,024 packets. The returned value should be below 250 ms.

Rpc Client Access: RPC Requests

This monitor returns the number of client requests currently being processed by the RPC Client Access service. This returned value should not be over 40.

UM Availability: Directory Access Failures

This monitor returns the number of times that attempts to access Active Directory failed. The returned value should be 0 at all times.

UM Availability: Total Inbound Calls Rejected by the UM Service

This monitor returns the total number of inbound calls that were rejected by the Microsoft Exchange Unified Messaging Service since the service was started. The returned value should be 0 at all times.
This monitor has the Count statistic as difference option enabled. It will only return new values from the last poll.

**UM Availability: Total Inbound Calls Rejected by the UM Worker Process**

This monitor returns the total number of inbound calls that were rejected by the UM Worker process since the service was started. The returned value should be 0 at all times.

This monitor has the Count statistic as difference option enabled. It will only return new values from the last poll.

**UM Performance: Operations over Six Seconds**

This monitor returns the number of all UM operations that took more than 6 seconds to complete. This is the time during which a caller was waiting for Unified Messaging to respond. The returned value should be as low as possible.

---

**Exchange 2016 Client Access Role Services and Counters (Advanced)**

This template contains advanced performance and statistics counters for monitoring Exchange 2016 Client Access Role. Some of the counters may require manual configuration, such as setting up installation-specific instances, correcting thresholds for the client's environment, and so forth. Use this template in addition to the Exchange 2016 Client Access Role Services and Counters (Basic) template.

Periodically, SolarWinds releases SAM templates to support the latest product versions such as Microsoft Server 2016. You can continue using templates for older product versions, but updating to the latest template is recommended.

To monitor Exchange Server 2016, PowerShell 2.0 or later must be installed and Administrator rights must be granted.

**Prerequisites**

RPC and WMI access to the Exchange server.

**Credentials**

Windows Administrator on target server.

**Monitored Components**

For details on monitors, see [SAM Component Monitor Types](#).

These performance counters are based on the following information:

Client Access Server Counters: Exchange 2010 Help, "Microsoft TechNet":
**RPC Operations/sec**

Shows the rate at which RPC operations occur, per second.

**Referral RPC Requests Average Latency**

This is Exchange 2010 address book service counter. Shows the average time, in ms, that referral requests took to complete during the sampling period.

Should be below 1,000 ms.

**Requests - Average Response Time**

Shows the average time (in ms) the Exchange Control Panel took to respond to a request during the sampling period.

The average should be under 6,000 ms.

**ActiveSync: Requests/sec**

Shows the number of HTTP requests received from the client via ASP.NET per second.

Determines the current Exchange ActiveSync request rate.

**OWA: Current Unique Users**

Shows the number of unique users currently logged on to Outlook Web App. This value monitors the number of unique active user sessions, so that users are only removed from this counter after they log off or their session times out.

Determines current user load.

**OWA: Requests/sec**

Shows the number of requests handled by Outlook Web App per second.

Determines current user load.

**Web Service: Current Connections**

Shows the current number of connections established with the Web service.

Determines current user load.

**Requests - Activations/sec**

Shows the number of requests activated per second in the Exchange Control Panel.

**Connection Count**

This is RPC Client Access load counter. Shows the total number of client connections maintained.

**NSPI Connections Current**

This is Exchange Address Book load counter. Shows the number of NSPI clients currently connected to the server.
NSPI RPC Requests/sec

This is Exchange Address Book load counter. Shows the rate at which NSPI requests occur each second.

Exchange 2016 Hub Transport Role Counters (Advanced)

This template contains advanced performance and statistics counters for monitoring Exchange 2016 Hub Transport Role. Some counters may require manual configuration, such as setting up installation-specific instances, correcting thresholds for the client's environment, and so forth. Use this template in addition to the Exchange 2016 Hub Transport Role Services and Counters (Basic) template.

Periodically, SolarWinds releases SAM templates to support the latest product versions such as Microsoft Server 2016. You can continue using templates for older product versions, but updating to the latest template is recommended.

To monitor Exchange Server 2016, PowerShell 2.0 or later must be installed and Administrator rights must be granted.

Prerequisites

RPC and WMI access to the Exchange server.

Credentials

Windows Administrator on target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

These performance counters are based on the following information:

Transport Server Counters: Exchange 2010 Help, "Microsoft TechNet":

Dumpster Size

Shows the total size (in bytes) of mail items currently in the transport dumpster on this server.

Dumpster Inserts/sec

Shows the rate at which items are inserted into the transport dumpster on this server. Determines the current rate of transport dumpster inserts.

Dumpster Item Count

Shows the total number of mail items currently in the transport dumpster on this server. Shows the current number of items being held in the transport dumpster.
Dumpster Deletes/sec

Shows the rate at which items are deleted from the transport dumpster on this server. Determines the current rate of transport dumpster deletions.

I/O Log Writes/sec (database)

Shows the rate of log file write operations completed. Determines the current load. Compare values to historical baselines.

I/O Log Reads/sec (database)

Shows the rate of log file read operations completed. Determines the current load. Compare values to historical baselines.

Log Generation Checkpoint Depth (database)

Represents the amount of work (in count of log files) that needs to be redone or undone to the database files if the process fails.

Should be less than 1,000 at all times.

I/O Database Reads/sec (database)

Shows the rate of database read operations completed. Determines the current load. Compare values to historical baselines.

I/O Database Writes/sec

Shows the rate of database write operations completed. Determines the current load. Compare values to historical baselines.

Messages Submitted Per Second

Shows the number of messages queued in the Submission queue per second. Determines current load. Compare values to historical baselines.

Messages Received/sec

Shows the number of messages received by the SMTP server each second. Determines current load. Compare values to historical baselines.

Messages Sent/sec

Shows the number of messages sent by the SMTP send connector each second. Determines current load. Compare values to historical baselines.

Messages Queued for Delivery Per Second

Shows the number of messages queued for delivery per second. Determines current load. Compare values to historical baselines.

Messages Completed Delivery Per Second

Shows the number of messages delivered per second. Determines current load. Compare values to historical baselines.
Avg. Disk sec/Read (Physical Disk)

Shows the average time, in seconds, of a read of data from the disk.

Should be less than 20 milliseconds (ms) on average. Spikes (maximum values) should not be higher than 50 ms.

When looking at hard disks using perfmon.exe, an understanding of the underlying hard disk subsystem is required to determine which counters (physical disk or logical disk) to look at.

Avg. Disk sec/Write (Physical Disk)

Shows the average time, in seconds, of a write of data to the disk.

Should be less than 20 milliseconds (ms) on average. Spikes (maximum values) should not be higher than 50 ms.

When looking at hard disks using perfmon.exe, an understanding of the underlying hard disk subsystem is required to determine which counters (physical disk or logical disk) to look at.

Avg. Disk sec/Read (Logical Disk)

Shows the average time, in seconds, of a read of data from the disk.

Should be less than 20 milliseconds (ms) on average. Spikes (maximum values) should not be higher than 50 ms.

When looking at hard disks using perfmon.exe, an understanding of the underlying hard disk subsystem is required to determine which counters (physical disk or logical disk) to look at.

Avg. Disk sec/Write (Logical Disk)

Shows the average time, in seconds, of a write of data to the disk.

Should be less than 20 milliseconds (ms) on average. Spikes (maximum values) shouldn't be higher than 50 ms.

When looking at hard disks using perfmon.exe, an understanding of the underlying hard disk subsystem is required to determine which counters (physical disk or logical disk) to look at.

Retry Non-Smtp Delivery Queue Length

Shows the number of messages in a retry state in the non-SMTP gateway delivery queues.

Should not exceed 100.

Largest Delivery Queue Length

Shows the number of messages in the largest delivery queues.

Should be less than 200 for the Edge Transport and Hub Transport server roles.
Version buckets allocated (database)

Total number of version buckets allocated. Shows the default backpressure values as listed in the edgetransport.exe.config file.

Should be less than 200 at all times.

Log Record Stalls/sec (database)

Shows the number of log records that cannot be added to the log buffers per second because they are full. If this counter is nonzero most of the time, the log buffer size may be a bottleneck.

Should be less than 10 per second on average. Spikes (maximum values) should not be greater than 100 per second.

Log Threads Waiting (database)

Shows the number of threads waiting for their data to be written to the log to complete an update of the database. If this number is too high, the log may be a bottleneck.

Should be less than 10 threads waiting on average.

Exchange 2016 Hub Transport Role Services and Counters (Basic)

This template contains basic performance counters and services for monitoring Exchange 20016 Hub Transport Role. This template is designed to work out of the box and does not require any additional configuration. For more detailed monitoring, use this template in conjunction with the Exchange 20016 Hub Transport Role Counters (Advanced) template.

Periodically, SolarWinds releases SAM templates to support the latest product versions such as Microsoft Server 2016. You can continue using templates for older product versions, but updating to the latest template is recommended.

To monitor Exchange Server 2016, PowerShell 2.0 or later must be installed and Administrator rights must be granted.

Prerequisites: RPC and WMI access to the Exchange server.

Credentials: Windows Administrator on target server.

Monitored Components:

These performance counters and services are based on the following information:


Transport Server Counters: Exchange 2010 Help, "Microsoft TechNet":
Service: Exchange Active Directory Topology

Provides Active Directory topology information to Exchange services. If this service is stopped, most Exchange services are unable to start. This service has no dependencies.

Service: Exchange EdgeSync

Connects to an AD LDS instance on subscribed Edge Transport servers over a secure LDAP channel to synchronize data between a Hub Transport server and an Edge Transport server. This service is dependent on the Microsoft Exchange Active Directory Topology service. If Edge Subscription is not configured, this service can be disabled.

Service: Exchange Anti-spam Update

Provides the Microsoft Forefront Protection 2010 for Exchange Server anti-spam update service. On Hub Transport servers, this service is dependent on the Microsoft Exchange Active Directory Topology service. On Edge Transport servers, this service is dependent on the Microsoft Exchange ADAM service.

Service: Exchange Monitoring

Allows applications to call the Exchange diagnostic cmdlets. This service has no dependencies.

Service: Exchange Transport

Provides SMTP server and transport stack. On Hub Transport servers, this service is dependent on the Microsoft Exchange Active Directory Topology service. On Edge Transport servers, this service is dependent on the Microsoft Exchange ADAM service.

Service: Exchange Transport Log Search

Provides remote search capability for Microsoft Exchange Transport log files. On Hub Transport servers, this service is dependent on the Microsoft Exchange Active Directory Topology service. On Edge Transport servers, this service is dependent on the Microsoft Exchange ADAM service.

Aggregate Delivery Queue Length (All Queues)

Shows the number of messages queued for delivery in all queues.

Should be less than 3,000 and not more than 5,000.

Active Remote Delivery Queue Length

Shows the number of messages in the active remote delivery queues.

Should be less than 250 at all times.

Active Mailbox Delivery Queue Length

Shows the number of messages in the active mailbox queues.

Should be less than 250 at all times.

Submission Queue Length

Shows the number of messages in the submission queue.

Should not exceed 100.
If sustained high values are occurring, investigate Active Directory and Mailbox servers for bottlenecks or performance-related issues.

**Active Non-Smtp Delivery Queue Length**
Shows the number of messages in the drop directory used by a Foreign connector.
Should be less than 250 at all times.

**Retry Mailbox Delivery Queue Length**
Shows the number of messages in a retry state attempting to deliver a message to a remote mailbox.
Should be less than 100 at all times.

**Retry Remote Delivery Queue Length**
Shows the number of messages in a retry state in the remote delivery queues.
Should not exceed 100.
We recommend that you check the next hop to determine the causes for queuing.

**Unreachable Queue Length**
Shows the number of messages in the Unreachable queue.
Should not exceed 100.

**Poison Queue Length**
Shows the number of messages in the poison message queue.
Should be 0 at all times.

**Exchange Active Sync Connectivity**
The components of this template test the configuration of Microsoft Exchange ActiveSync on Exchange 2010 and 2013 servers using a PowerShell script.

**Prerequisites**
- Exchange Management Tools installed on the target Exchange server.
- Enable Windows Authentication for PowerShell on the Exchange server. This can be configured in IIS
  `mmc: Start > Administrative Tools > Internet Information Services (IIS) Manager`.
  1. In the IIS console, expand Your Server, Sites, Default Web Site.
  2. Select the PowerShell application.
  3. On the central panel, open Authentication.
  4. Select Windows Authentication and enable it from the right panel
- Create an ActiveSync test user on the Mailbox Exchange server by running the following script:
  `<Installed_Exchange_Folder>\Scripts\new-TestCasConnectivityUser.ps1`

If you do not run the script, the following error displays:
Could not find or sign in with user <user>. If this task is being run without credentials, sign in as a Domain Administrator, and then run Scripts\new-TestCasConnectivityUser.ps1 to verify that the user exists on Mailbox server <server>

**Credentials**

The credentials must be that of an Exchange Administrator account (Organization Manager) with at least view-only permissions. Credentials should be provided with the domain part in the login field. For example: domain\user.

If you have trouble with template functionality, refer to [Troubleshooting](#).

**Monitored Components**

For details on monitors, see [SAM Component Monitor Types](#).

**Active Sync Connectivity Testing**

This component monitor performs ActiveSync tests and returns latency in milliseconds of the performed tests (if possible):

Possible returned values:

- -1 – Test failed. See message field for errors.
- 0 – Test is unavailable.
- 1 – Test successfully finished. Test latency is not available. (This occurs on Exchange 2013 servers).
- 2 and higher – Test latency in milliseconds.

This component returns the status of the following scenarios:

- Options – Issue an HTTP OPTIONS command to retrieve the Exchange ActiveSync protocol version.
- FolderSync – Issue a FolderSync command to retrieve the folder hierarchy.
- First Sync – Initialize the Sync partnership for the test folder and create a sync state on the server.
- GetItemEstimate – Issue a GetItemEstimate command to retrieve count of items waiting to sync.
- Sync Data – Sync all existing data in the test folder.
- Ping – Execute Ping command for testing DirectPush against a test folder. An item is created in the folder to trigger the Ping response.
- Sync Test Item – Sync the test item.

**Troubleshooting**

**ERROR:** Please check target server argument and credentials (should be domain\user). [192.168.1.206] Connecting to remote server failed with the following error message: Access is denied.
Resolution: This error could occur when you use the wrong credentials. Check the credentials and verify the credentials are in the following format: (domain\user). The user should be Exchange Organization Manager.

ERROR: The operation couldn't be performed because object 'Mailbox Database 10580933221\*' couldn't be found on 'xchg2010.apmteam.sw'.

Resolution: Provide the correct database name.

ERROR: [192.168.1.206] Connecting to remote server failed with the following error message : The WinRM client cannot process the request. The WinRM client tried to use Negotiate authentication mechanism, but the destination computer (192.168.1.206:443) returned an 'access denied' error. Change the configuration to allow Negotiate authentication mechanism to be used or specify one of the authentication mechanisms supported by the server. To use Kerberos, specify the local computer name as the remote destination. Also verify that the client computer and the destination computer are joined to a domain. To use Basic, specify the local computer name as the remote destination, specify Basic authentication and provide user name and password.

Resolution: This error indicates that Windows Authentication is not enabled for the PowerShell application on IIS on the Exchange server.

ERROR:[192.168.1.206] Connecting to remote server failed with the following error message : The WinRM client received an HTTP status code of 403 from the remote WS-Management service.

Resolution: If you get this error, you should check your SSL settings for the PowerShell application in IIS on the Exchange server. You should use one of the following configurations:

- Require SSL unchecked
- Require SSL checked and Client Certificates is set to Accept
- Require SSL checked and Client Certificates is set to Ignore

ERROR: Please check target server argument and credentials (should be domain\user). [xchg2010]
Connecting to remote server failed with the following error message : The WS-Management service cannot process the request. This user allowed a maximum number of 5 concurrent shells, which has been exceeded. Close existing shells or raise the quota for this user.

Resolution: This error could occur when you use more than five remote PowerShell sessions (set by default) at the same time. If you get this error, it is recommended that you increase the number of concurrent shells on the Exchange server.

Open a windows Command Line as Administrator and run the following command:

```
winrm set winrm/config/winrs @{MaxShellsPerUser="30"}
```

**Exchange Server 2000 and 2003**

This template assesses the status and the overall performance of Microsoft Exchange Server 2000 and 2003. The critical threshold values for the performance counters are values recommended by Microsoft.

**Prerequisites**

- WMI access to target server.
Credentials

Windows Administrator on target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

The following component monitors are used to test Exchange services:

- MS Exchange Event
- MS Exchange IMAP4
- MS Exchange Information Store
- MS Exchange Management
- MS Exchange MTA Stacks
- MS Exchange POP3
- MS Exchange Routing Engine
- MS Exchange Site Replication
- MS Exchange System Attendant
- MS SMTP Monitor
- MS POP3 Monitor
- MS IMAP4 Monitor
- Processor Queue Length
- Number of Processes
- Mailbox Receive Queue
- Public Receive Queue
- SMTP Local Queue
- SMTP Remote Queue
- SMTP Categorizer Queue
- Average RPC Latency
- Percent Free Space
- Disk Read Bytes Per Second
- Disk Write Bytes Per Second
- Mailbox Send Queue
- Public Send Queue
- Address List Queue Length

Exchange Web Services User Experience monitor

This component monitor simulates an email round trip to test the ability of your SMTP server to receive and distribute email, and the ability of your users to retrieve email through Exchange Web Services.
Credentials

Credentials used for this monitor should be the user for whom the mailbox will be monitored.

If you receive a server error while browsing Exchange Web Services, see the following Microsoft KB article: http://support.microsoft.com/kb/2020789. (© 2018 Microsoft Corp., available at http://support.microsoft.com, obtained on October 31, 2018)

Field Descriptions

Description

This field provides a default description of the monitor. You can override the default description by adding to or replacing the text, which will then be automatically saved. The variable to access this field is ${UserDescription}.

Enable Component

Determines whether the component is enabled. Disabling the component leaves it in the application in a deactivated state, not influencing SolarWinds SAM application availability or status.

Credential for Monitoring

Select a credential or use the <Inherit credential from node> option. If the credential you need is not in the credentials list, add it in the Credentials Library. See Understand the Credentials Library for details.

Send Email From

Enter the email address where you want an email to be sent from

Send Email To

Enter the email address where you want an email to be sent to

Exchange Web Service URL

This field allows you to specify the URL of your Exchange Web Server.

Ignore CA Errors

Select to ignore Certificate Authority errors.

Ignore CN Errors

Select to ignore Common Name errors.

SMTP Server

Enter your SMTP server address here.
SMTP Port

Enter your SMTP port number here.

Use Credentials for SMTP

Check this box if needed.

Credential for SMTP

If needed, select the proper credentials from the drop-down list.

SMTP Encryption

Choose the method of encryption from the drop-down list.

Response Time Threshold

Select the conditions from the drop-down lists for the Warning and Critical thresholds, then set the time, in seconds, for these conditions to be met.

User Notes

This field allows you to add notes for easy reference. You can access this field by using the variable, ${UserNotes}.
Microsoft Forefront

The following templates are available:

- Microsoft Forefront Threat Management Gateway 2010
- Microsoft Forefront Endpoint Protection 2010 (Client)
- Microsoft Forefront Endpoint Protection 2010 (Server)
Microsoft Forefront Endpoint Protection 2010 (Client)

This template allows you to monitor the status of Microsoft Forefront Endpoint Protection (FEP) 2010 client installed on a Windows machine by using PowerShell and Event monitors.

Prerequisites

WinRM must be installed and properly configured on the target server and WMI access to the target server.

Credentials

Windows Administrator on the target server.

Monitored Components

For details on monitors, see [SAM Component Monitor Types](#).

All event monitors should return values of zero. Returned values other than zero may indicate an abnormality. If you believe an abnormality exists, you should examine the Windows System log for details. Source name: Microsoft Antimalware.

Antimalware Health and Firewall Status

This monitor returns the antimalware health and firewall status of FEP client.

Returned values:

- 0 – Service is disabled.
- 1 – Service is enabled.
- 255 – Script cannot check the service status from WMI.

This component returns the status of the following services:

- **Antivirus Enabled** – This component returns the status of Antivirus component.
- **Antispyware Enabled** – This component returns the status of Antispyware component.
- **Protection Enabled** – This component returns the status of FEP protection technology.
- **Behavior Monitor Enabled** – This component returns the status of the behavior monitor.
- **NIS Enabled** – This component returns the status of the Network Inspection System (NIS).
- **Firewall Enabled** – This component returns the status of the Windows Firewall.
- **Firewall Service Running** – This component returns the status of the Windows Firewall service.

Antimalware Infection Status

This monitor returns antimalware infection status of FEP client.

Returned values:
- 0 – Action not required.
- 1 – Action required.
- 255 – Script cannot check the action status from WMI.

This component returns the status of the following services:

- **Pending Full Scan** – This component returns whether there is a need for a full scan due to a threat action.
- **Pending Manual Steps** – This component returns whether there is a need for manual steps due to a threat action.
- **Pending Offline Scan** – This component returns whether there is a need for an offline scan.
- **Pending Reboot** – This component returns whether there is a need for a reboot due to a threat action.

**Days passed from last definition update**

This component monitor returns the number of days that have passed from the last definition update of the antivirus and antispyware modules. In the message field, this component returns the date of the last installed update.

**Microsoft Antimalware Service**

This monitors returns the CPU and memory usage of the Microsoft Antimalware service. This service helps protect users from malware and other potentially unwanted software.

**Event: Scan encountered error and stopped**

This monitor returns the number of events when the Forefront Endpoint Protection client scan has encountered an error and stopped.

Event ID: 1005.

This error record includes the scan ID, type of scan (antivirus, antispyware, antimalware), scan parameters, the user that started the scan, the error code, and a description of the error. Try to run the scan again. If it fails in the same way, look up the error code.

**Event: Malware or other potentially unwanted soft detected**

This monitor returns the number of events when the Forefront Endpoint Protection has detected malware or other potentially unwanted software.

Event ID: 1116.

No user action is required. Forefront Endpoint Protection can suspend and take routine action on this threat. To remove the virus manually, in the Forefront Endpoint Protection interface, click Clean Computer.

**Events: Error when taking action on malware**

This monitor returns the number of events when the Forefront Endpoint Protection client has encountered a non-critical or critical error when taking action on malware or other potentially unwanted software.

Event ID: 1118, 1119.
Perform a signature update and then verify that the quarantine succeeded and that the user has permission to access the necessary resources.

**Events: Error during signature or engine updating**

This monitor returns the number of events when the Forefront Endpoint Protection client has encountered an error trying to update signatures or the engine.


If you are having problems updating definitions, the following steps can help:

- Ensure your configuration for definition updates is correct;
- Check your WSUS configuration settings.
- Try to update the definitions manually by downloading the full definitions files.

If you are having problems updating the engine, the following steps can help:

- Restart the computer and try again.
- Check the configuration of definition updates.
- Manually download the latest definitions from the Microsoft Malware Protection Center.

**Event: Error during signature reverting**

This monitor returns the number of events when the Forefront Endpoint Protection client has encountered an error trying to load signatures and will attempt reverting back to a known-good set of signatures.


This error can occur if the Forefront Endpoint Protection client has encountered an error while trying to load the definitions or if the file is corrupt. Forefront Endpoint Protection client will attempt to revert back to a known-good set of definitions. You should restart the computer and check the configuration of definition updates.

**Event: Error during using Dynamic Signature Service**

This monitor returns the number of events when the Forefront Endpoint Protection client has encountered an error trying to use the Dynamic Signature Service.

Event ID: 2012.

This error is likely caused by a network connectivity issue. Check your Internet connectivity settings.

**Event: Real-Time Protection feature error**

This monitor returns the number of events when the Endpoint Protection client Real-Time Protection feature has encountered an error and failed.

Event ID: 3002.

Try to restart the following two services: Antimalware engine and NIS engine.
Event: Client engine terminated due to error

This monitor returns the number of events when the Forefront Endpoint Protection client engine has been terminated due to an unexpected error.

Event ID: 5008.

Try to restart the following two services: Antimalware engine and NIS engine.
Microsoft Forefront Endpoint Protection 2010 (Server)

This template allows you to monitor the status of Microsoft Forefront Endpoint Protection (FEP) 2010 Server installed on a Windows machine by using PowerShell and Service monitors.

Prerequisites

WinRM must be installed and properly configured on the target server and WMI access to the target server.

Credentials

Administrator on target server.

Each PowerShell monitor uses the same argument.

For Example: S01  where S01 is the 3-character site code where FEP installed. This code you provide during installation of Microsoft System Center Configuration Manager (SCCM).

ℹ️ You must specify the correct arguments for each monitored component in the Script Arguments field. If you fail to do this, the monitor will return with a status error of "Undefined."

Monitored Components

ℹ️ For details on monitors, see [SAM Component Monitor Types](#).

Deployment Status

This monitor returns the deployment status of FEP. The returned values are as follows:

- **Deployment Succeeded** – This component returns the number of computers with FEP clients deployed. The value returned should be as high as possible. You should set thresholds according to your requirements.
- **Out of Date** – This component returns the number of computers for which the reported FEP version is older than the one installed at the server.
- **Deployment Failed** – This component returns the current number of operations queued and waiting on a read lock. The returned value should be as low as possible.
- **Deployment Pending** – This component returns the number of computers for which an active Configuration Manager software distribution advertisement is trying to install the FEP client.
- **Locally Removed** – This component returns the number of computers where the FEP client was locally removed either by a user with local administrator permission or by some other software (e.g. malware). The returned value should be as low as possible.
- **Not Targeted** – This component returns the number of computers in your organization to which the client software was not targeted. The returned value should be as low as possible.

Policy Distribution Status

This monitor returns FEP policy distribution status. The returned values are as follows:
**Distribution Failed** – This component returns the number of computers to which a policy could not be deployed. The returned value should be as low as possible.

**Distribution Pending** – This component returns the number of computers to which a policy is in the process of being deployed.

**Policy Distributed** – This component returns the number of computers to which a policy was successfully deployed.

**Definition Status**

This monitor returns the definition status of FEP. The returned values are as follows:

- **Up to Date** – This component returns the number of client computers with up-to-date definitions. The returned value should be as high as possible.
- **Up to 3 Days** – This component returns the number of client computers with definitions that are up to three days old. The returned value should be as low as possible.
- **Up to 7 Days** – This component returns the number of client computers with definitions that are up to seven days old. The returned value should be as low as possible.
- **Older Than 1 Week** – This component returns the number of client computers with definitions more than one week old. The returned value should be as low as possible.

**Malware Activity Status**

This monitor returns the malware activity status of FEP. The returned values are as follows:

- **Infected** – This component returns the number of computers on which the FEP client software has detected active malware. The returned value should be as low as possible.
- **Restart Required** – This component returns the number of computers running the FEP client software that require a restart to complete malware cleaning.
- **Full Scan Required** – This component returns the number of computers running the FEP client software that require a full scan.
- **Recent Malware Activity** – This component returns the number of computers on which the FEP client software detected and cleaned malware within the last 24 hours.

**Health Status**

This monitor returns the malware activity status of FEP. The returned values are as follows:

- **Protection Service Off** – This component returns the number of computers on which the FEP antimalware service is turned off. The returned value should be as low as possible.
- **Not Reporting** – This component returns the number of computers to which the FEP client has been deployed, but have not sent a status report back to the Configuration Manager server in the past 14 days. The returned value should be as low as possible.
- **Healthy** – This component returns the number of computers running the FEP client software and have sent a status report back to the Configuration Manager server in the past 14 days.

**Service: Forefront Endpoint Protection Monitoring**

This monitors returns the CPU and memory usage of the Forefront Endpoint Protection Monitoring service. This service monitors security events from computers that are protected by Microsoft Forefront Endpoint Protection.
Microsoft Forefront Threat Management Gateway 2010

This template assesses the status and overall performance of a Microsoft Forefront Threat Management Gateway 2010 by using performance counters and windows service monitors.

Prerequisites

WMI access to the target server. On the Forefront server in the Forefront TGM snap-in, you will need to allow monitoring performance counters and services from the SAM server with the following parameters in the Firewall Policy menu. Create the following access rule:

Rule: Allow;
From: Local Host, SAM server;
To: Local Host, SAM server;
For: All users;
Protocols: Microsoft CIFS (TCP), NetBios Datagram, NetBios Name Service, NetBios Session, RPC (all Interfaces), TCP-10003-OUT.

where:

- SAM server is the IP address of your SAM server
- TCP-10003-OUT is the manually configured protocol with the following parameters in your primary connections:
  - Protocol: TCP
  - Port range: From 10003 to 10003
  - Direction: Outbound.

Credentials

Windows Administrator on the target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Components without predetermined threshold values have guidance such as "use the lowest threshold possible" or "use the highest threshold possible" to help you find a threshold appropriate for your application.
Service: Microsoft Forefront TMG Control
This monitor returns the CPU and memory usage of the Microsoft Forefront TMG Control service. This service controls Forefront Threat Management Gateway services.

Service: Microsoft Forefront TMG Firewall
This monitor returns the CPU and memory usage of the Microsoft Forefront TMG Firewall service. This service provides Forefront TMG internet access protection services.

Service: Microsoft Forefront TMG Job Scheduler
This monitor returns the CPU and memory usage of the Microsoft Forefront TMG Job Scheduler service. This service runs Forefront Threat Management Gateway jobs according to specified job schedules.

Service: Microsoft Forefront TMG Managed Control
This monitor returns the CPU and memory usage of the Microsoft Forefront TMG Managed Control service. This service Controls Forefront Threat Management Gateway managed services.

Service: Microsoft Forefront TMG Storage
This monitor returns the CPU and memory usage of the Microsoft Forefront TMG Storage service. This service provides Forefront Threat Management Gateway configuration storage.

Service: AD-LDS (ISASTGCTRL)
This monitor returns the CPU and memory usage of the ISASTGCTRL service. This service provides the Active Directory LDS instance.

Firewall Packet Engine: Active Connections
This monitor shows the total number of active connections currently passing data. Use this counter to monitor general performance.

Firewall Packet Engine: Bytes/sec
This monitor shows the total throughput, in bytes per second, passing through the firewall. Each byte is counted twice; once when it enters the firewall, and once when it leaves the firewall. Use this counter to monitor general performance.

Firewall Packet Engine: Dropped Packets/sec
This monitor shows the number of packets that were denied each second. Use this to monitor general security threats. If numbers are large (more than 100), check for network configuration errors and attacks.

Firewall Packet Engine: Packets/sec
This monitor shows the number of allowed and denied packets, per second. Use this to monitor general security threats and performance. This directly impacts CPU utilization.
Firewall Packet Engine: Connections/sec

This monitor shows the number of TCP and UDP connections created, per second. Use this to monitor general security threats and performance. This directly impacts CPU utilization.

H.323 Filter: Active H.323 Calls

This monitor returns the number of H.323 calls that are currently active.

Cache: Disk Failure Rate (failures/sec)

This monitor shows the number of I/O failures, per second, since the firewall service started. An I/O failure occurs when TMG fails to read from or write to the disk cache. This value should be as low as possible.

Cache: Memory Usage Ratio Percent (%)

This monitor shows the amount of fetches from the memory cache in proportion to the total fetches from the cache.

Cache: URL Commit Rate (URL/sec)

This monitor shows the rate at which URLs are stored to the cache.

Firewall Service: DNS Cache Hits %

This monitor shows the percentage of DNS domain names serviced by the DNS cache from the total of all DNS entries that have been retrieved by the firewall service. This value should be as high as possible.

Firewall Service: Active Sessions

This monitor shows the number of active sessions for the firewall service. Use this counter to monitor general performance. By comparing this counter at both peak and off-peak times, you can construct a good picture of routine usage.

Firewall Service: Active TCP Connections

This monitor shows the number of active TCP connections currently passing data. Connections pending, or not yet established, are counted elsewhere.

Firewall Service: Active UDP Connections

This monitor shows the number of active User Datagram Protocol (UDP) connections.

Firewall Service: Available Worker Threads

This monitor shows the number of firewall service worker threads that are available or waiting in the completion port queue. Available worker threads should never remain near 0 for any length of time. If TMG keeps this at or near 0, you should scale out.

Firewall Service: Worker Threads

This monitor shows the total number of firewall service worker threads.
SOCKS Filter: Active Sessions

This monitor shows a single SOCKS session and includes the CONNECT and BIND commands for a single client.

SOCKS Filter: Pending DNS Resolutions

This monitor shows the number of pending Winsock getaddrinfo() requests. These requests resolve host DNS names and IP addresses for SOCKS connections. This monitor should be as low as possible.

Web Proxy: Active Web Sessions

This monitor indicates how many clients are currently being served by the Web Proxy filter. Monitoring this counter at both peak and off-peak times gives a good indication of server usage. The configuration setting for maximum web request connections influences this value. This counter may also be useful if you need to temporarily stop TMG services. When authentication does not take place, all of the clients from a single IP address are viewed as one session.

Web Proxy: Average Milliseconds/request

This monitor shows the average number of milliseconds required to service a Web Proxy client request, not including requests serviced by the Secure Sockets Layer (SSL) tunnel. This counter can be monitored at peak and off-peak times to get a comprehensive picture of the rate at which client requests are being serviced. A counter with a value that is too high might indicate that the TMG computer is having difficulty in handling all requests and that requests are being delayed. This value should be as low as possible.

Web Proxy: Cache Hit Ratio (%)

This monitor determines how many Web Proxy client requests have been served using cached data (Total Cache Fetches), as a percentage of the total number of successful Web Proxy client requests to the TMG computer (Total Successful Requests). Its value gives a good indication of the effectiveness of the cache. A high counter value indicates that a high level of requests is being serviced from the cache, meaning faster response times. A zero counter value indicates that caching is not enabled. A low counter value may indicate a configuration problem. The cache size may be too small, or requests may not be cacheable.

Web Proxy: Connect Errors

This monitor shows the total number of errors that occurred while connecting.

Web Proxy: Failing Requests/sec

This monitor shows the rate of Web Proxy client requests that have been completed with some type of error. This counter can be compared with the Requests/sec counter to give an indication of how well TMG is servicing incoming Web requests. A high failure rate, as compared with the rate of incoming requests, suggests that TMG is having difficulty in coping with all incoming requests. Connection settings for incoming Web requests may be incorrectly configured, or connection bandwidth may be insufficient. This monitor should be as low as possible.

Web Proxy: Requests/sec

This monitor shows the rate of incoming requests that have been made to Web proxy. A higher value means that more TMG resources will be required to service incoming requests.
Web Proxy: Thread Pool Active Sessions

This monitor shows the number of sessions being actively serviced by thread pools.

Web Proxy: Memory Pool for HTTP Requests (%)

This monitor returns the percentage of memory available for HTTP requests. When an HTTP request is made, TMG uses memory from a pre-allocated pool. You can use the ProxyVmemAlloc3pSize registry value in the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3Proxy\ parameters registry key to modify the size of this pool.

Web Proxy: Memory Pool for SSL Requests (%)

This monitor returns the percentage of memory available for SSL requests. When an SSL request is made, TMG uses memory from a pre-allocated pool. You can use the ProxyVmemAlloc1pSize registry value in the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3Proxy\ parameters registry key to modify the size of this pool.

Web Proxy: Compression - Current Compression Ratio

This monitor returns the average size reduction of the HTTP response body as a percentage of the uncompressed body size during the sample period for HTTP responses compressed by TMG.

Web Proxy: Compression - Responses Compressed: Accumulated Ratio

This monitor shows the percentage of HTTP responses compressed by TMG out of the total number of HTTP requests handled by TMG.
Microsoft IIS

The following templates are available:

- IIS templates versions 6 and 10
- Microsoft IIS SMTP Server template

See also ApplInsight for IIS.
IIS templates

SolarWinds SAM includes two Microsoft Internet Information Services (IIS) server templates — one for IIS 6 and one for IIS 10. The critical threshold values for the performance counters are those recommended by Microsoft.

Prerequisites

WMI access to the target server.

Credentials

Windows Administrator on the target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

You need to set thresholds for counters according to your environment. It is recommended to monitor counters for some period of time to understand potential value ranges and then set the thresholds accordingly.

Service: World Wide Web Publishing

Provides web connectivity and administration through the Internet Information Services Manager.

HTTP Port Monitor

Check the availability of standard http port (default is port 80).

You need change the port value if you are using another port.

URI Cache Flushes Counter

The number of URI cache flushes that have occurred since the server started.

URI Cache Hits Counter

The number of successful lookups in the URI cache.

URI Cache Hits Percent Counter

The ratio of URI Cache Hits to the total number of cache requests.

URI Cache Misses Counter

The number of unsuccessful lookups in the URI cache.

Web service: Bytes Received/sec Counter

Rate at which data bytes are received by the WWW service, per second.

If World Wide Web Publishing Service is stopped, ignore this counter.
Web service: Bytes Sent/sec Counter
Rate that data bytes are sent by the WWW service, per second.

1 If World Wide Web Publishing Service is stopped, ignore this counter.

Web service: Bytes Total/sec Counter
Sum of bytes sent/sec and bytes received/sec.

1 If World Wide Web Publishing Service is stopped, ignore this counter.

Web service: Connection Attempts/sec Counter
Rate of attempted connections to the WWW service since service startup, per second.

1 If World Wide Web Publishing Service is stopped, ignore this counter.

Web service: Current Connections Counter
Current number of active connections to the WWW service.

1 If World Wide Web Publishing Service is stopped, ignore this counter.

Web service: Get Requests/sec Counter
Rate at which HTTP requests using the GET method are made to the WWW service, per second.

1 If World Wide Web Publishing Service is stopped, ignore this counter.

System: System Calls/sec
This counter is a measure of the number of calls made to the system components, Kernel mode services. This is a measure of how busy the system is taking care of applications and services. Set the value as low as possible.

1 To learn about setting the counter as low as possible, see the following article “Using SAM Min/Max Average Statistic Data historical charts to create threshold settings based on 95th percentile line”.

Microsoft IIS SMTP Server template
This template assesses the status and overall performance of a Microsoft SMTP Server.

Prerequisites
WMI access to the target server.

Credentials
Windows Administrator on the target server.
Monitored Components

For details on monitors, see [SAM Component Monitor Types](#).

**Service: Simple Mail Transfer Protocol (SMTP)**

This monitor returns CPU and memory usage of SMTP service. This service is responsible for sending emails from one server to another.

**SMTP Monitor**

This component monitor tests the ability of an SMTP server to accept incoming connections and respond with the correct code.

**Recipients Local**

This monitor shows the percentage of recipients that will be delivered locally.

**Recipients Remote**

Shows the percentage of recipients that will be delivered remotely.

**Badmailed Messages (Bad Pickup File)**

This monitor shows the number of malformed pickup messages sent to the badmail directory (a default directory used for forwarding undeliverable messages). The value for this monitor should be as low as possible.

**Badmailed Messages (General Failure)**

This monitor shows the number of messages sent to badmail for reasons not associated with a specific counter. The value for this monitor should be as low as possible.

**Badmailed Messages (Hop Count Exceeded)**

This monitor shows the number of messages sent to badmail because they had exceeded the maximum hop count. The value for this monitor should be as low as possible.

**Badmailed Messages (NDR of DSN)**

This monitor shows the number of Delivery Status Notifications sent to badmail because they could not be delivered. If a message is undeliverable, it is returned to the sender with a non-delivery report (NDR). The value for this monitor should be as low as possible.

**Badmailed Messages (No Recipients)**

This monitor shows the number of messages sent to badmail because they had no recipients. The value for this monitor should be as low as possible.

**Badmailed Messages (Triggered via Event)**

This monitor shows the number of messages sent to badmail at the request of a server event sink. An event sink is mechanism for notifying clients when events occur. The value for this monitor should be as low as possible.
**Connection Errors/sec**
This monitor shows the number of connection errors occurring per second.

**Inbound Connections Current**
This monitor shows the total number of connections currently inbound.

**DNS Queries/sec**
This monitor shows the rate of DNS lookups.

**Local Queue Length**
This monitor shows the number of messages in the local queue.

**Local Retry Queue Length**
This monitor shows the number of messages in the local retry queue.

**Messages Pending Routing**
This monitor shows the number of messages that have been categorized but not routed.

**Messages Received/sec**
This monitor shows the rate that inbound messages are being received.

**Messages Delivered/sec**
This monitor shows the rate that messages are delivered to local mailboxes.

**Messages Sent/sec**
This monitor shows the rate that outbound messages are being sent.

**Outbound Connections Current**
This monitor shows the number of connections currently outbound.

**Remote Queue Length**
This monitor shows the number of messages in the remote queue.

**Remote Retry Queue Length**
This monitor shows the number of messages in the retry queue for remote delivery.

**Cat: Categorizations completed/sec**
This monitor shows the total number of messages submitted to categorizer that have finished categorization.

**Cat: Categorizations failed (DS connection failure)**
This monitor shows the number of categorizations that failed due to an Active Directory connection failure. The value for this monitor should be as low as possible.
Cat: Categorizations failed (DS logon failure)

This monitor shows the number of categorizations that failed due to an Active Directory logon failure. The value for this monitor should be as low as possible.

Cat: Categorizations failed (non-retryable error)

This monitor shows the number of categorizations that failed with a hard error (one which does not allow attempts to retry the operation). The value for this monitor should be as low as possible.

Cat: Categorizations failed (Out Of Memory)

This monitor shows the number of categorizations that failed due to lack of available memory. The value for this monitor should be as low as possible.

Cat: Categorizations failed (retryable error)

This monitor shows the number of categorizations that failed with an error which allowed an attempt to retry the operation. The value for this monitor should be as low as possible.

Cat: Categorizations failed (sink retryable error)

This monitor shows the number of categorizations that failed with a generic error which allowed an attempt to retry the operation. The value for this monitor should be as low as possible.

Cat: Categorizations in progress

This monitor shows the number of categorizations in progress.

Events: SMTP Warnings and Errors

This monitor returns SMTP related warnings and errors. The value for this monitor should be as low as possible. For any values above zero, you should look in event log for details.
Microsoft Lync

The following templates are available:

- Microsoft Lync Server (Edge Role)
- Microsoft Lync Server (Front-End Role)
- Microsoft Lync Server (Mediation Role)
- Microsoft Lync Server 2013 (Front-End Role)
- Microsoft Lync Server 2013 (Edge Role)
- Microsoft Lync Server 2013 (Mediation Role)
Microsoft Lync Server (Edge Role)

This template assesses the status and overall health of services as well as the performance of the Edge Microsoft Lync Server.

**Prerequisites**

WMI access to the target server.

**Credentials**

Windows Administrator on the target server.

**Monitored Components**

For details on monitors, see [SAM Component Monitor Types](#).

You need to set thresholds for these counters according to your environment. It is recommended to monitor these counters for some period of time to understand potential value ranges and then set the thresholds accordingly.

**Service: Lync Server Replica Replicator Agent**

This component monitor returns the CPU and memory usage of the Lync Server Replica Replicator Agent. This service is used by the File Transfer Agent for replication configuration settings.

**SIP Peers: Connections Active**

This component monitor returns the number of established connections that are currently active. A connection is considered established when peer credentials are verified (e.g. via MTLS), or the peer receives a 2xx response. You will need to baseline this counter by testing and monitoring the user load. This returned value should be less than 15,000 connections per Front-End.

**SIP Peers: TLS Connections Active**

This component monitor returns the number of established TLS connections that are currently active. A TLS connection is considered established when the peer certificate, and possibly the host name, are verified for a trust relationship. You will need to baseline this counter by testing and monitoring the user load.

**SIP Peers: Average Outgoing Queue Delay**

This component monitor returns the average time, in seconds, that messages have been delayed in outgoing queues. Check the Outgoing Queue Delay for delays in sending messages to other servers or clients that could be causing messages to be accumulated in the server. The server will drop client connections if it is in a throttle state and messages stay in the outgoing queue for more than 32 seconds.
SIP Peers: Incoming Requests/sec

This component monitor returns the rate of received requests, per second. You will need to baseline this counter by testing and monitoring the user load.

SIP Protocol: Incoming Messages/sec

This component monitor returns the rate of received messages, per second. You will need to baseline this counter by testing and monitoring the user load.

SIP Load Management: Average Holding Time For Incoming Messages

This component monitor returns the average time that the server held the incoming messages currently being processed. This should usually be less than one second, on average, but it is normal to see short spikes of up to three seconds. The server will throttle new incoming messages after going above the high benchmark and until the number of messages falls below the low benchmark. The server starts rejecting new connections when the average holding time is greater than overload time of 15 seconds.

SIP Access Edge Server: External Messages/sec With Internally Supported Domain

This component monitor returns the per-second rate of messages received at the external edge with an internally supported domain.

SIP Access Edge Server: External Messages/sec Received With Allowed Partner Server Domain

This component monitor returns the per-second rate of messages received at the external edge with an allowed partner server domain.

SIP Access Edge Server: External Messages/sec Received With a Configured Allowed Domain

This component monitor returns the per-second rate of messages received at the external edge with a configured allowed domain.

A/V Edge UDP: Active Relay Sessions – Authenticated

This component monitor returns the number of active relay sessions over UDP.

A/V Edge UDP: Active Relay Sessions – Allocated Port

This component monitor returns the number of active relay sessions with a UDP port allocation.

A/V Edge UDP: Active Relay Sessions – Data

This component monitor returns the number of active relay data sessions over UDP.

A/V Edge UDP: Allocated Port Pool Count

This component monitor returns the number of UDP ports available in the Allocated Port Pool. This monitor should be more than zero. If it reaches zero there is a resource issue.

A/V Edge UDP: Allocate Requests/sec

This component monitor returns the per-second rate of Allocate Requests over UDP. You will need to baseline this counter by testing and monitoring the user load.
A/V Edge UDP: Authentication Failures/sec

This component monitor returns the per-second rate of failed attempts to authenticate with the relay over UDP. The returned value should be as low as possible.

A/V Edge UDP: Allocate Requests Exceeding Port Limit

This component monitor returns the number of allocate requests over UDP that exceeded the port limit. If the value is greater than zero, this could indicate an attempt to misuse the port.

A/V Edge UDP: Packets Received/sec

This component monitor returns the number of packets, received per second, by the relay over UDP. You will need to baseline this counter by testing and monitoring the user load.

A/V Edge UDP: Packets Sent/sec

This component monitor returns the number of packets sent per second by the relay over UDP. You will need to baseline this counter by testing and monitoring the user load.

A/V Edge UDP: Average Data Packet Latency (milliseconds)

This component monitor returns the average latency for a valid data request over UDP in milliseconds. The returned value should be as low as possible.

A/V Edge UDP: Packets Dropped/sec

This component monitor returns the per-second rate of packets over UDP dropped by the relay. The returned value should be as low as possible.

This error occurs when an unexpectedly high rate of User Datagram Protocol (UDP) packets is received at the Media Relay (A/V Edge server) causing some packets to be discarded. This could be the result of system overload or an indication of an attempt to misuse the MR.

To resolve this, check that the profile of network traffic to the MR is in line with expected usage. If the traffic exceeds 250 Mbps per interface, increase the Receive and Transmit buffer size on the associated network adapter network adapters to three times the default values.

If the cause is a general system overload, increase the capacity of the deployed MR function. A network level trace can be used to determine if there is an unusual amount of traffic originating from a single source. If the situation persists, enable tracing to check the network source of sessions exceeding the bandwidth limits to allow further troubleshooting of the cause.

A/V Edge TCP: Active Relay Sessions – Authenticated

This component monitor returns the number of active relay sessions over TCP.

A/V Edge TCP: Active Relay Sessions – Allocated Port

This component monitor returns the number of active relay sessions with a TCP port allocation.

A/V Edge TCP: Active Relay Sessions – Data

This component monitor returns the number of active relay data sessions over TCP.
A/V Edge TCP: Allocated Port Pool Count

This component monitor returns the number of TCP ports available in the Allocated Port Pool. This monitor should be greater than zero. If zero is reached, a resource issue exists.

A/V Edge TCP: Allocate Requests/sec

This component monitor returns the per-second rate of Allocate Requests over TCP. You will need to baseline this counter by testing and monitoring the user load.

A/V Edge TCP: Authentication Failures/sec

This component monitor returns the per-second rate of failed attempts to authenticate with the relay over TCP. The returned value should be as low as possible.

A/V Edge TCP: Allocate Requests Exceeding Port Limit

This component monitor returns the number of allocate requests over TCP that exceeded the port limit. If the value is greater than zero, this could indicate an attempt to misuse the port.

A/V Edge TCP: Packets Received/sec

This component monitor returns the number of packets received per second by the relay over TCP. You will need to baseline this counter by testing and monitoring the user load.

A/V Edge TCP: Packets Sent/sec

This component monitor returns the number of packets sent per second by the relay over TCP. You will need to baseline this counter by testing and monitoring the user load.

A/V Edge TCP: Average Data Packet Latency (milliseconds)

This component monitor returns the average latency for a valid data request over TCP in milliseconds. The returned value should be as low as possible.

A/V Edge TCP: Packets Dropped/sec

This component monitor returns the per-second rate of packets over TCP dropped by the relay. The returned value should be as low as possible.

This error occurs when an unexpectedly high rate of User Datagram Protocol (UDP) packets is received at the Media Relay (A/V Edge server) causing some packets to be discarded. This could be the result of system overload or an indication of an attempt to misuse the MR.

To resolve this, check that the profile of network traffic to the MR is in line with expected usage. If the traffic exceeds 250 Mbps per interface, increase the Receive and Transmit buffer size on the associated network adapter network adapters to three times the default values.

If the cause is a general system overload, increase capacity of the deployed MR function. A network level trace can be used to determine if there is an unusual amount of traffic originating from a single source. If the situation persists, enable tracing to check the network source of sessions.
Microsoft Lync Server (Front-End Role)

This template assesses the status and overall health of services as well as the performance of the Front-End Microsoft Lync Server.

**Prerequisites**

WMI access to the target server.

**Credentials**

Windows Administrator on the target server.

**Monitored Components**

For details on monitors, see [SAM Component Monitor Types](#).

You need to set thresholds for these counters according to your environment. It is recommended to monitor these counters for some period of time to understand potential value ranges and then set the thresholds accordingly.

**Service: Lync Server Audio Test Service**

This component monitor returns the CPU and memory usage of the Lync Server Audio Test Service. This service offers users the ability to subjectively test the quality of a call before placing the call. The user checks the call quality by making a test call.

**Service: Lync Server File Transfer Agent**

This component monitor returns the CPU and memory usage of the Lync Server File Transfer Agent. The File Transfer Agent is responsible for replicating configuration settings with the Replica Replicator Agent that runs on every Lync Server.

**Service: Lync Server Front-End**

This component monitor returns the CPU and memory usage of the Front-End Lync Server. The Front-End Servers maintain transient information, such as logged-on state and control information for an IM, Web, or audio/video (A/V) conference.

**Service: Lync Server IM Conferencing**

This component monitor returns the CPU and memory usage of the Lync Server IM Conferencing. The IM Conferencing service is responsible for multiplexing the instant messages data feed from the leader to all participants in the session.

**Service: Lync Server Master Replicator Agent**

This component monitor returns the CPU and memory usage of the Lync Server Master Replicator Agent. This service is used by File Transfer Agent for replication configuration settings.
Service: Lync Server Replica Replicator Agent

This component monitor returns the CPU and memory usage of the Lync Server Replica Replicator Agent. This service is used by the File Transfer Agent for replication configuration settings.

SIP Peers: Connections Active

This component monitor returns the number of established connections that are currently active. A connection is considered established when peer credentials are verified (e.g. via MTLS), or the peer receives a 2xx response. You will need to baseline this counter by testing and monitoring the user load. This returned value should be less than 15,000 connections per Front-End.

SIP Peers: TLS Connections Active

This component monitor returns the number of established TLS connections that are currently active. A TLS connection is considered established when the peer certificate, and possibly the host name, are verified for a trust relationship. You will need to baseline this counter by testing and monitoring the user load.

SIP Peers: Sends Outstanding

This component monitor returns the number of messages that are currently present in the outgoing queues. If you receive error message 504, investigate the results from this counter. Doing so will indicate which servers are having problems. To do so, you will need to change the instance from _Total, to the server hostname. You can check this within perfmon.exe.

SIP Peers: Average Outgoing Queue Delay

This component monitor returns the average time, in seconds, that messages have been delayed in outgoing queues. Check the Outgoing Queue Delay for delays in sending messages to other servers or clients that could be causing messages to be accumulated in the server. The server will drop client connections if it is in a throttle state and messages stay in the outgoing queue for more than 32 seconds.

SIP Peers: Flow-controlled Connections Dropped

This component monitor returns the total number of connections dropped because of excessive flow-control. You will need to baseline this counter by testing and monitoring the server’s health. The returned value should be as low as possible.

SIP Peers: Average Flow-Control Delay

This component monitor returns the average delay, in seconds, in message processing when the socket is flow-controlled. You will need to baseline this counter by testing and monitoring the server’s health. The returned value should be as low as possible.

SIP Peers: Incoming Requests/sec

This component monitor returns the rate of received requests, per second. You will need to baseline this counter by testing and monitoring the user load.
SIP Protocol: Incoming Messages/sec

This component monitor returns the rate of received messages, per second. You will need to baseline this counter by testing and monitoring the user load.

SIP Protocol: Events In Processing

This component monitor returns the number of SIP transactions, or dialog state change events, that are currently being processed. You will need to baseline this counter by testing and monitoring the user load.

SIP Responses: Local 500 Responses/sec

This component monitor returns the rate of 500 responses generated by the server, per second. This can indicate that there is a server component that is not functioning correctly.

SIP Responses: Local 503 Responses/sec

This component monitor returns the rate of 503 responses generated by the server, per second. The 503 code corresponds to the server being unavailable. On a healthy server, you should not receive this code at a steady rate. However, during ramp up, after a server has been brought back online, there may be some 503 responses. Once all users get back in and the server returns to a stable state, there should no longer be any 503 responses returned.

SIP Responses: Local 504 Responses/sec

This component monitor returns the rate of 504 responses generated by the server, per second. A few 504 responses to clients (for clients disconnecting abruptly) is to be expected, but this counter mainly indicates connectivity issues with other servers. It can indicate connection failures or delays connecting to remote servers.

SIP Load Management: Average Holding Time For Incoming Messages

This component monitor returns the average time that the server held the incoming messages currently being processed. This should usually be less than one second, on average, but it is normal to see short spikes of up to three seconds. The server will throttle new incoming messages after going above the high watermark and until the number of messages falls below the low watermark. The server starts rejecting new connections when the average holding time is greater than overload time of 15 seconds.

SIP Load Management: Address space usage

This component monitor returns the percentage of available address space currently in use by the server process. The returned value should be as low as possible.

SIP Load Management: Page file usage

This component monitor returns the percentage of available page file space currently in use by the server process. The returned value should be as low as possible.

IM Conferences: Active Conferences

This component monitor returns the number of active conferences. You will need to baseline this counter by testing and monitoring the user load.
IM Conferences: Connected Users

This component monitor returns the number of connected users in all conferences. You will need to baseline this counter by testing and monitoring the user load.

IM Conferences: Throttled Sip Connections

This component monitor returns the number of throttled Sip connections. If the value is greater than ten, it could indicate that Peer is not processing requests in a timely fashion. This can happen if the peer machine is overloaded. Peer is defined as the connected servers, adjacent Front-End servers, or MCUs in the same EE Pool. The same set of counters apply.

IM MCU Health And Performance: MCU Health State

This component monitor returns the current health of the MCU. Possible values:

- 0 = Normal.
- 1 = Loaded.
- 2 = Full.
- 3 = Unavailable.

IM MCU Health And Performance: MCU Draining State

This component monitor returns the current draining status of the MCU. Possible values:

- 0 = Not requesting to drain.
- 1 = Requesting to drain.
- 2 = Draining.

When a server is drained, it stops taking new connections and calls. These new connections and calls are routed through other servers in the pool. A server being drained allows its sessions on existing connections to continue until they naturally end. When all existing sessions have ended, the server is ready to be taken offline.

User Services - DBStore: Queue Latency (msec)

This component monitor returns the average time, in milliseconds, that a request is held in the database queue. This counter represents the time that a request spends in the queue of the Back-End Database Server. If the topology is healthy, this counter averages less than 100 ms. Occasional spikes are acceptable. The value will be higher on Front-End Servers that are located at the site opposite the location of the Back-End Database Servers. This value can increase if the Back-End Database Server is having performance problems or if network latency is too high. If the returned value is high, check both network latency and the health of the Back-End Database Server. Server health decreases as latency increases to 12 seconds, when server throttling begins.
User Services - DBStore: Sproc Latency (msec)

This component monitor returns the average time, in milliseconds, it takes to execute a stored procedure call. A healthy state is considered to be less than 100 ms. Server health decreases as latency increases to 12 seconds, when server throttling begins.

User Services - Https Transport: Number of failed connection attempts / Sec

This component monitor returns the rate of connection attempt failures, per second. You will need to baseline this counter by testing and monitoring the server's health.
Microsoft Lync Server (Mediation Role)

This template assesses the status and overall health of services as well as the performance of the Mediation Microsoft Lync Server.

**Prerequisites**

- WMI access to the target server.

**Credentials**

- Windows Administrator on the target server.

**Monitored Components**

For details on monitors, see [SAM Component Monitor Types](#).

You need to set thresholds for these counters according to your environment. It is recommended to monitor these counters for some period of time to understand potential value ranges and then set the thresholds accordingly.

**Service: Lync Server Replica Replicator Agent**

This component monitor returns the CPU and memory usage of the Lync Server Replica Replicator Agent. This service is used by the File Transfer Agent for replication configuration settings.

**Outbound Calls: Current**

This component monitor returns the total number of active calls going through the Mediation Server.

**Outbound Calls: Active media bypass calls**

This component monitor returns the total number of active calls going through Mediation Server that are in Media Bypass mode. Calls using Media Bypass use significantly fewer Mediation Server resources because the media is not flowing through the Mediation Server.

**Inbound Calls: Current**

This component monitor returns the number of inbound calls in progress.

**Inbound Calls: Active media bypass calls**

This component monitor returns the number of media bypass calls in progress.

**Media Relay: Media Connectivity Check Failure**

This component monitor returns the number of calls where media connectivity between the Mediation Server and the remote endpoints could not be established. The returned value should be as low as possible.
Health Indices: Load Call Failure Index

This component monitor returns the scaled index between zero and 100 that is related to all call failures due to Global Health Index as a heavy load.

Global Counters: Current audio channels with PSM quality reporting

This component monitor returns the total number of active channels that are having Phase Shift Modulation (PSM) quality reported. Calculating PSM quality has a processing overhead so this should be taken into account when measuring performance.

Total failed calls caused by unexpected interaction from the Proxy

This component monitor returns the number of calls that failed because of an unexpected response from the Front End Server. The returned value should be as low as possible.

Total failed calls caused by unexpected interaction from a gateway

This component monitor returns the number of calls that failed because of an unexpected response.
Microsoft Lync Server 2013 (Front-End Role)

This template assesses the status and overall health of services as well as the performance of the Front-End Microsoft Lync Server 2013.

Prerequisites

- WMI access to the target server.

Credentials

- Windows Administrator on the target server.

Monitored Components


You need to set thresholds for these counters according to your environment. It is recommended to monitor these counters for some period of time to understand potential value ranges and then set the thresholds accordingly.


**Service: Lync Server Application Sharing**

This component monitor returns the CPU and memory usage of the Lync Server Application Sharing service.

**Service: Lync Server Audio Test Service**

This component monitor returns the CPU and memory usage of the Lync Server Audio Test Service. This service offers users the ability to subjectively test the quality of a call before placing the call. The user checks the call quality by making a test call.

**Service: Lync Server Audio/Video Conferencing**

This component monitor returns the CPU and memory usage of the Lync Server Audio/Video Conferencing service.

**Service: Lync Server File Transfer Agent**

This component monitor returns the CPU and memory usage of the Lync Server File Transfer Agent. The File Transfer Agent is responsible for replicating configuration settings with the Replica Replicator Agent that runs on every Lync Server.

**Service: Lync Server Front-End**

This component monitor returns the CPU and memory usage of the Front-End Lync Server. The Front-End Servers maintain transient information, such as logged-on state and control information for an IM, Web, or audio/video (A/V) conference.
Service: Lync Server IM Conferencing

This component monitor returns the CPU and memory usage of the Lync Server IM Conferencing. The IM Conferencing service is responsible for multiplexing the instant messages data feed from the leader to all participants in the session.

Service: Lync Server Master Replicator Agent

This component monitor returns the CPU and memory usage of the Lync Server Master Replicator Agent. This service is used by File Transfer Agent for replication configuration settings.

Service: Lync Server Replica Replicator Agent

This component monitor returns the CPU and memory usage of the Lync Server Replica Replicator Agent. This service is used by the File Transfer Agent for replication configuration settings.

Peers: Connections Active

This component monitor returns the number of established connections that are currently active. A connection is considered established when peer credentials are verified (e.g. via MTLS), or the peer receives a 2xx response. You will need to baseline this counter by testing and monitoring the user load. This returned value should be less than 15,000 connections per Front-End.

Peers: TLS Connections Active

This component monitor returns the number of established TLS connections that are currently active. A TLS connection is considered established when the peer certificate, and possibly the host name, are verified for a trust relationship. You will need to baseline this counter by testing and monitoring the user load.

Peers: Sends Outstanding

This component monitor returns the number of messages that are currently present in the outgoing queues. If you receive error message 504, investigate the results from this counter. Doing so will indicate which servers are having problems. To do so, you will need to change the instance from _Total, to the server hostname. You can check this within perfmon.exe

Peers: Average Outgoing Queue Delay

This component monitor returns the average time, in seconds, that messages have been delayed in outgoing queues. Check the Outgoing Queue Delay for delays in sending messages to other servers or clients that could be causing messages to be accumulated in the server. The server will drop client connections if it is in a throttle state and messages stay in the outgoing queue for more than 32 seconds.

Peers: Flow-controlled Connections

This component monitor returns the number of connections that are currently being flow-controlled (no socket receives are posted).
Peers: Average Flow-Control Delay

This component monitor returns the average delay, in seconds, in message processing when the socket is flow-controlled. You will need to baseline this counter by testing and monitoring the server's health. The returned value should be as low as possible.

Peers: Incoming Requests/sec

This component monitor returns the rate of received requests, per second. You will need to baseline this counter by testing and monitoring the user load.

Peers: Incoming Responses/sec

This component monitor returns the rate of received responses, per second.

Peers: Outgoing Requests/sec

The per-second rate of outgoing requests.

Peers: Outgoing Responses/sec

This component monitor returns the rate of outgoing responses, per second.

Protocol: Average Event Processing Time

This component monitor returns the average time (in seconds) it takes to process a SIP transaction or dialog state change event.

Protocol: Average Incoming Message Processing Time

This component monitor returns the average time (in seconds) it takes to process an incoming message.

Protocol: Average Local Message Processing Time

This component monitor returns the average time (in seconds) it takes to process a locally generated message.

Protocol: Average Number Of Active Worker Threads

This component monitor returns the average number of active SIP worker threads that process incoming messages.

Protocol: Events In Processing

This component monitor returns the number of SIP transactions, or dialog state change events, that are currently being processed. You will need to baseline this counter by testing and monitoring the user load.

Protocol: Events Processed/sec

This component monitor returns the rate of SIP transaction or dialog state change events that were delivered for processing, per second.
Protocol: Incoming Messages/sec
This component monitor returns the rate of received messages, per second. You will need to baseline this counter by testing and monitoring the user load.

Protocol: Messages In Server
This component monitor returns the number of messages currently being processed by the server.

Protocol: Outgoing Messages/sec
This component monitor returns the rate of sent messages, per second.

Responses: Local 500 Responses/sec
This component monitor returns the rate of 500 responses generated by the server, per second. This can indicate that there is a server component that is not functioning correctly.

Responses: Local 503 Responses/sec
This component monitor returns the rate of 503 responses generated by the server, per second. The 503 code corresponds to the server being unavailable. On a healthy server, you should not receive this code at a steady rate. However, during ramp up, after a server has been brought back online, there may be some 503 responses. Once all users get back in and the server returns to a stable state, there should no longer be any 503 responses returned.

Responses: Local 504 Responses/sec
This component monitor returns the rate of 504 responses generated by the server, per second. A few 504 responses to clients (for clients disconnecting abruptly) is to be expected, but this counter mainly indicates connectivity issues with other servers. It can indicate connection failures or delays connecting to remote servers.

Load Management: Address space usage
This component monitor returns the percentage of available address space currently in use by the server process. The returned value should be as low as possible.

Load Management: Average Holding Time For Incoming Messages
This component monitor returns the average time that the server held the incoming messages currently being processed. This should usually be less than one second, on average, but it is normal to see short spikes of up to three seconds. The server will throttle new incoming messages after going above the high watermark and until the number of messages falls below the low watermark. The server starts rejecting new connections when the average holding time is greater than overload time of 15 seconds.

Load Management: Page file usage
This component monitor returns the percentage of available page file space currently in use by the server process. The returned value should be as low as possible.
IMMcu Conferences: Active Conferences

This component monitor returns the number of active conferences. You will need to baseline this counter by testing and monitoring the user load.

IMMcu Conferences: Connected Users

This component monitor returns the number of connected users in all conferences. You will need to baseline this counter by testing and monitoring the user load.

IMMcu Conferences: Throttled Sip Connections

This component monitor returns the number of throttled Sip connections. If the value is greater than ten, it could indicate that Peer is not processing requests in a timely fashion. This can happen if the peer machine is overloaded. Peer is defined as the connected servers, adjacent Front-End servers, or MCUs in the same EE Pool. The same set of counters apply.

MCU Health And Performance: MCU Draining State

This component monitor returns the current draining status of the MCU.

Possible values:
- 0 = Not requesting to drain.
- 1 = Requesting to drain.
- 2 = Draining.

When a server is drained, it stops taking new connections and calls. These new connections and calls are routed through other servers in the pool. A server being drained allows its sessions on existing connections to continue until they naturally end. When all existing sessions have ended, the server is ready to be taken offline.

MCU Health And Performance: MCU Health State

This component monitor returns the current health of the MCU.

Possible values:
- 0 = Normal.
- 1 = Loaded.
- 2 = Full.
- 3 = Unavailable.

USrv - DBStore: Queue Latency (msec)

This component monitor returns the average time, in milliseconds, that a request is held in the database queue. This counter represents the time that a request spends in the queue of the Back-End Database Server. If the topology is healthy, this counter averages less than 100 ms. Occasional spikes are acceptable. The value will be higher on Front-End Servers that are located at the site opposite the location of the Back-End Database Servers. This value can increase if the Back-End Database Server is having performance problems or if network latency is too high. If the returned value is high, check both network latency and the health of the Back-End Database Server. Server health decreases as latency increases to 12 seconds, when server throttling begins.
USrv - DBStore: Sproc Latency (msec)

This component monitor returns the average time, in milliseconds, it takes to execute a stored procedure call. A healthy state is considered to be less than 100 ms. Server health decreases as latency increases to 12 seconds, when server throttling begins.

USrv - Https Transport: Active HTTPS connections

This component monitor returns the number of active HTTPS connections.

USrv - Https Transport: Number of failed connection attempts / Sec

This component monitor returns the rate of connection attempt failures, per second. You will need to baseline this counter by testing and monitoring the server’s health.
Microsoft Lync Server 2013 (Edge Role)

This template assesses the status and overall health of services as well as the performance of the Edge Microsoft Lync Server 2013.

Prerequisites

WMI access to the target server.

Credentials

Windows Administrator on the target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Note: You need to set thresholds for these counters according to your environment. It is recommended to monitor these counters for some period of time to understand potential value ranges and then set the thresholds accordingly.

Service: Lync Server Replica Replicator Agent

This component monitor returns the CPU and memory usage of the Lync Server Replica Replicator Agent. This service is used by the File Transfer Agent for replication configuration settings.

SIP Peers: Connections Active

This component monitor returns the number of established connections that are currently active. A connection is considered established when peer credentials are verified (e.g. via MTLS), or the peer receives a 2xx response. You will need to baseline this counter by testing and monitoring the user load. This returned value should be less than 15,000 connections per Front-End.

SIP Peers: TLS Connections Active

This component monitor returns the number of established TLS connections that are currently active. A TLS connection is considered established when the peer certificate, and possibly the host name, are verified for a trust relationship. You will need to baseline this counter by testing and monitoring the user load.

SIP Peers: Average Outgoing Queue Delay

This component monitor returns the average time, in seconds, that messages have been delayed in outgoing queues. Check the Outgoing Queue Delay for delays in sending messages to other servers or clients that could be causing messages to be accumulated in the server. The server will drop client connections if it is in a throttle state and messages stay in the outgoing queue for more than 32 seconds.
SIP Peers: Incoming Requests/sec

This component monitor returns the rate of received requests, per second. You will need to baseline this counter by testing and monitoring the user load.

SIP Protocol: Incoming Messages/sec

This component monitor returns the rate of received messages, per second. You will need to baseline this counter by testing and monitoring the user load.

SIP Load Management: Average Holding Time For Incoming Messages

This component monitor returns the average time that the server held the incoming messages currently being processed. This should usually be less than one second, on average, but it is normal to see short spikes of up to three seconds. The server will throttle new incoming messages after going above the high benchmark and until the number of messages falls below the low benchmark. The server starts rejecting new connections when the average holding time is greater than overload time of 15 seconds.

SIP Access Edge Server: External Messages/sec With Internally Supported Domain

This component monitor returns the per-second rate of messages received at the external edge with an internally supported domain.

SIP Access Edge Server: External Messages/sec Received With Allowed Partner Server Domain

This component monitor returns the per-second rate of messages received at the external edge with an allowed partner server domain.

SIP Access Edge Server: External Messages/sec Received With a Configured Allowed Domain

This component monitor returns the per-second rate of messages received at the external edge with a configured allowed domain.

A/V Edge UDP: Active Relay Sessions – Authenticated

This component monitor returns the number of active relay sessions over UDP.

A/V Edge UDP: Active Relay Sessions – Allocated Port

This component monitor returns the number of active relay sessions with a UDP port allocation.

A/V Edge UDP: Active Relay Sessions – Data

This component monitor returns the number of active relay data sessions over UDP.

A/V Edge UDP: Allocated Port Pool Count

This component monitor returns the number of UDP ports available in the Allocated Port Pool. This monitor should be more than zero. If it reaches zero there is a resource issue.

A/V Edge UDP: Allocate Requests/sec

This component monitor returns the per-second rate of Allocate Requests over UDP. You will need to baseline this counter by testing and monitoring the user load.
A/V Edge UDP: Authentication Failures/sec

This component monitor returns the per-second rate of failed attempts to authenticate with the relay over UDP. The returned value should be as low as possible.

A/V Edge UDP: Allocate Requests Exceeding Port Limit

This component monitor returns the number of allocate requests over UDP that exceeded the port limit. If the value is greater than zero, this could indicate an attempt to misuse the port.

A/V Edge UDP: Packets Received/sec

This component monitor returns the number of packets, received per second, by the relay over UDP. You will need to baseline this counter by testing and monitoring the user load.

A/V Edge UDP: Packets Sent/sec

This component monitor returns the number of packets sent per second by the relay over UDP. You will need to baseline this counter by testing and monitoring the user load.

A/V Edge UDP: Average Data Packet Latency (milliseconds)

This component monitor returns the average latency for a valid data request over UDP in milliseconds. The returned value should be as low as possible.

A/V Edge UDP: Packets Dropped/sec

This component monitor returns the per-second rate of packets over UDP dropped by the relay. The returned value should be as low as possible.

This error occurs when an unexpectedly high rate of User Datagram Protocol (UDP) packets is received at the Media Relay (A/V Edge server) causing some packets to be discarded. This could be the result of system overload or an indication of an attempt to misuse the MR.

To resolve this, check that the profile of network traffic to the MR is in line with expected usage. If the traffic exceeds 250 Mbps per interface, increase the Receive and Transmit buffer size on the associated network adapter network adapters to three times the default values.

If the cause is a general system overload, increase the capacity of the deployed MR function. A network level trace can be used to determine if there is an unusual amount of traffic originating from a single source. If the situation persists, enable tracing to check the network source of sessions exceeding the bandwidth limits to allow further troubleshooting of the cause.

A/V Edge TCP: Active Relay Sessions – Authenticated

This component monitor returns the number of active relay sessions over TCP.

A/V Edge TCP: Active Relay Sessions – Allocated Port

This component monitor returns the number of active relay sessions with a TCP port allocation.

A/V Edge TCP: Active Relay Sessions – Data

This component monitor returns the number of active relay data sessions over TCP.
A/V Edge TCP: Allocated Port Pool Count

This component monitor returns the number of TCP ports available in the Allocated Port Pool. This monitor should be greater than zero. If zero is reached, a resource issue exists.

A/V Edge TCP: Allocate Requests/sec

This component monitor returns the per-second rate of Allocate Requests over TCP. You will need to baseline this counter by testing and monitoring the user load.

A/V Edge TCP: Authentication Failures/sec

This component monitor returns the per-second rate of failed attempts to authenticate with the relay over TCP. The returned value should be as low as possible.

A/V Edge TCP: Allocate Requests Exceeding Port Limit

This component monitor returns the number of allocate requests over TCP that exceeded the port limit. If the value is greater than zero, this could indicate an attempt to misuse the port.

A/V Edge TCP: Packets Received/sec

This component monitor returns the number of packets received per second by the relay over TCP. You will need to baseline this counter by testing and monitoring the user load.

A/V Edge TCP: Packets Sent/sec

This component monitor returns the number of packets sent per second by the relay over TCP. You will need to baseline this counter by testing and monitoring the user load.

A/V Edge TCP: Average Data Packet Latency (milliseconds)

This component monitor returns the average latency for a valid data request over TCP in milliseconds. The returned value should be as low as possible.

A/V Edge TCP: Packets Dropped/sec

This component monitor returns the per-second rate of packets over TCP dropped by the relay. The returned value should be as low as possible.

This error occurs when an unexpectedly high rate of User Datagram Protocol (UDP) packets is received at the Media Relay (A/V Edge server) causing some packets to be discarded. This could be the result of system overload or an indication of an attempt to misuse the MR.

To resolve this, check that the profile of network traffic to the MR is in line with expected usage. If the traffic exceeds 250 Mbps per interface, increase the Receive and Transmit buffer size on the associated network adapter network adapters to three times the default values.

If the cause is a general system overload, increase capacity of the deployed MR function. A network level trace can be used to determine if there is an unusual amount of traffic originating from a single source. If the situation persists, enable tracing to check the network source of sessions.
Microsoft Lync Server 2013 (Mediation Role)

This template assesses the status and overall health of services as well as the performance of the Mediation Microsoft Lync Server 2013.

Prerequisites

WMI access to the target server.

Credentials

Windows Administrator on the target server.

Monitored Components

For details on monitors, see [SAM Component Monitor Types](#).

You need to set thresholds for these counters according to your environment. It is recommended to monitor these counters for some period of time to understand potential value ranges and then set the thresholds accordingly.

Service: Lync Server Mediation

This component monitor returns the CPU and memory usage of the Lync Server Mediation service. This is main service for Mediation role.

Service: Lync Server Replica Replicator Agent

This component monitor returns the CPU and memory usage of the Lync Server Replica Replicator Agent. This service is used by the File Transfer Agent for replication configuration settings.

Outbound Calls: Current

This component monitor returns the total number of active calls going through the Mediation Server.

Outbound Calls: Active media bypass calls

This component monitor returns the total number of active calls going through Mediation Server that are in Media Bypass mode. Calls using Media Bypass use significantly fewer Mediation Server resources because the media is not flowing through the Mediation Server.

Inbound Calls: Current

This component monitor returns the number of inbound calls in progress.

Inbound Calls: Active media bypass calls

This component monitor returns the number of media bypass calls in progress.
**Media Relay: Media Connectivity Check Failure**

This component monitor returns the number of calls where media connectivity between the Mediation Server and the remote endpoints could not be established. The returned value should be as low as possible.

**Health Indices: Load Call Failure Index**

This component monitor returns the scaled index between zero and 100 that is related to all call failures due to Global Health Index as a heavy load.

**Global Counters: Current audio channels with PSM quality reporting**

This component monitor returns the total number of active channels that are having Phase Shift Modulation (PSM) quality reported. Calculating PSM quality has a processing overhead so this should be taken into account when measuring performance.

**Total failed calls caused by unexpected interaction from the Proxy**

This component monitor returns the number of calls that failed because of an unexpected response from the Front End Server. The returned value should be as low as possible.

**Total failed calls caused by unexpected interaction from a gateway**

This component monitor returns the number of calls that failed because of an unexpected response from a gateway peer. The returned value should be as low as possible.
Microsoft Message Queuing

The following templates are available:

- [Microsoft Message Queuing Events](#)
- [Microsoft Message Queuing (Performance)](#)
Microsoft Message Queuing Events

This template assesses the status and overall performance of a Microsoft Message Queuing (MSMQ) server by monitoring critical errors in the Windows Application log file.

Prerequisites

WMI access to the target server.

Credentials

Windows Administrator on the target server.

Monitored Components

For details on monitors, see [SAM Component Monitor Types](http://technet.microsoft.com/en-us/library/cc773676(v=ws.10).aspx).

All monitors should return values of zero. Returned values other than zero may indicate an abnormality. If you believe an abnormality exists, you should examine the Windows Application log for details. Filter with the source name “MSMQ.” For more information about MSMQ events, refer to this article: [http://technet.microsoft.com/en-us/library/cc773676(v=ws.10).aspx](http://technet.microsoft.com/en-us/library/cc773676(v=ws.10).aspx).

Active Directory Integration Configuration

This monitor returns the following events:

- Message Queuing was unable to create the msmq (MSMQ Configuration) object in the Active Directory;
- The Message Queuing service was unable to obtain the properties of the msmq (MSMQ Configuration) object from the Active Directory.

Event ID: 2116, 2120.

The MSMQ configuration object cannot be created in Active Directory Domain Services (ADDS): This error might be caused by one of the following conditions:

- The user who is installing Message Queuing does not have the correct permissions to create child objects in ADDS.
- Replication delays are not configured properly.
- A corrupted computer object exists in ADDS.
- The Message Queuing service was unable to obtain the properties of the msmq (MSMQ Configuration) object from Active Directory: There is an issue with replication delays. This issue should be resolved after Active Directory Domain Services (ADDS) replicates itself.

Active Directory Operation

This monitor returns the following events:

- The Message Queuing service cannot start. The Active Directory interface cannot be
The list of Message Queuing servers with directory service functionality in the Windows registry is empty;

- This domain controller is not trusted for delegation. Therefore, the Message Queuing server cannot run;
- The Message Queuing server cannot determine if the local domain controller is trusted for delegation. This may indicate a serious problem;
- The sites where the computer resides cannot be resolved. Check that the subnets in your network are configured correctly in the Active Directory and that each site is configured with the appropriate subnet;
- The Message Queuing service cannot join the Windows NT 4.0 domain. The Active Directory Integration subcomponent was therefore removed;
- The local computer is a Message Queuing routing server that formerly belonged to the domain and is now operating in workgroup mode. Other Message Queuing clients still regard this computer as a routing server and will try to route messages through this computer.

Event ID: 2035, 2068, 2122, 2123, 2165, 2166, 2169.

**The Active Directory interface cannot be initialized:** There may be several reasons why the Active Directory interface cannot be initialized. Possible actions include the following:

- Configuring Message Queuing objects to be accessible in Active Directory Domain Services (ADDS).
- Making modifications so that Message Queuing can find and bind to the directory service.
- Resolving issues that are preventing Message Queuing from synchronizing with ADDS.

**The list of Message Queuing servers with directory service functionality in the Windows registry is empty:** You can confirm the presence of the Directory Service Integration feature by doing the following:

1. Verify the registry key setting.
2. Verify that the computer is joined to the correct domain.
3. Verify Active Directory operation.

**This domain controller is not trusted for delegation:** The domain controller must have the Active Directory option “Trust computer for delegation” enabled.

**The Message Queuing server cannot determine if the local domain controller is trusted for delegation:** The domain controller must have the Active Directory option “Trust computer for delegation” enabled.

**The sites where the computer resides cannot be resolved:** The subnets may not be configured correctly. Possible actions include the following:

- Reconfigure the Active Directory subnets in your network.
- Configure each site with the appropriate subnet.
The Message Queuing service cannot join the Windows NT 4.0 domain: The MSMQ Service does not support joining a Windows NT 4.0 domain. You must integrate Active Directory or Active Directory Domain Services (ADDS) with a Windows 2000, Windows Server 2003, or Windows Server 2008 domain.

The local computer is a Message Queuing routing server that formerly belonged to the domain and is now operating in workgroup mode: Stale computer objects can cause the MSMQ Service to not operate properly. Deleting stale computer objects may solve this problem. However, deleting a computer object in Active Directory Domain Services (ADDS) can cause problems on the client computer. Before you delete a computer object, make sure that no services running on the client computer will be affected. In this case, deleting the Message Queuing Active Directory object will delete public queues on the computer.

Clustering

This monitor returns the following events:

- The Message Queuing service resource cannot bind to the cluster IP address;
- The IP address specified in the registry value is not a valid IP address for this computer.

Event ID: 2168, 2220.

The Message Queuing service resource cannot bind to the cluster IP address: The MSMQ Service on the physical node must be cluster aware. If the service is not cluster aware, this prevents the Message Queuing resource from coming online on this node. This problem can occur if the MSMQ Service running on the physical node was started before the computer became a member of the server cluster. As a result, the MSMQ Service running on the physical node listens on all IP addresses of the computer and prevents the Message Queuing resource from listening on the cluster IP address.

The IP address specified in the registry value is not a valid IP address for this computer: The IP address is not configured properly in the registry. Either remove the registry value or set it to the IP address suggested in the event.

Network Configuration

This monitor returns the following events:

- The queue cannot listen/bind to the multicast address;
- Message Queuing failed to bind to port 1801. The port may already be bound to another process;
- Message Queuing cannot bind to UDP port 3527;
- Message Queuing failed to listen on the IPv6 protocol. Messages will not be accepted on IPv6;
- Message Queuing failed to listen on the IPv4 protocol. Messages will not be accepted on IPv4.
- Message Queuing Service failed to listen on both IPv4 and IPv6 protocol. Messages will not be accepted from the network through TCP/IP protocols.

Event ID: 2160, 2170, 2171, 2197, 2198, 2199.
The queue cannot listen/bind to the multicast address: The multicast address that is specified in the event is not valid. Enter a valid multicast address for the queue that is using this address. IP multicast addresses must consist of four bytes, and they must lie in the class D range from 224.0.0.0 to 239.255.255.255. However, only certain ranges of addresses in this range are available for sending multicast messages.

Message Queuing failed to bind to port 1801: Message Queuing must bind to port 1801 to function. Make sure that the port is free (that is, no other programs are trying to use it), and then try to start the MSMQ Service again after allowing time for the port to close. If this problem occurs during setup, you must free the port and run Setup again.

Message Queuing cannot bind to UDP port 3527: The Message Queuing internal ping mechanism uses User Datagram Protocol (UDP) port 3527 to establish network connections. Another process may be using this port. Message Queuing can continue to operate without using this port, but connection times will not be optimal. To optimize the establishment of connections, free port 3527, and then restart the MSMQ Service.

Message Queuing failed to listen on the IPv6 protocol: Message Queuing is not able to listen to messages on IP version 6 (IPv6) because the protocol may not be supported on this computer. Find out if IPv6 can be installed on this computer, because your hardware or software may not support IPv6.

Message Queuing failed to listen on the IPv4 protocol: Message Queuing is not able to listen to messages on IP version 4 (IPv4) because of some issue. IPv4 may not be enabled, or your hardware or software may not support it.

Message Queuing Service failed to listen on both IPv4 and IPv6 protocol: The TCP/IP communication protocols are not functioning as expected. Try to restart TCP/IP services or the computer.

Connectivity

This monitor returns the following events:

- The Message Queuing service cannot communicate with other computers, because the RPC interface cannot use the TCP/IP protocol;
- This server was unable to resolve the IP addresses of other routing servers;
- Message Queuing could not resolve the name to an IP address;
- A socket operation failed with an error;
- Message Queuing could not establish connection to, because connection was refused by the recipient computer;
- The Message Queuing service cannot communicate with other computers because the select API socket failed.

Event ID: 2059, 2140, 2184, 2185, 2187, 2194.

The RPC interface cannot use the TCP/IP protocol: Try to resolve TCP/IP and RPC issues.
This server was unable to resolve the IP addresses of other routing servers: IP addresses must be assigned to all routing servers, and they must be registered properly in Domain Name System (DNS). Assign IP addresses to all routing servers, and make sure that they are registered in DNS. If that does not work, check the routing server configuration to ensure that the routing settings (in/out server, service is running, and others) are correct.

Message Queuing could not resolve the name to an IP address: Confirm that the computer name that is specified in the event is a valid computer name on the network. If it is a valid computer name, confirm the recipient computer's Domain Name System (DNS) settings, and then use the ping command to contact the recipient computer by network name to confirm name resolution functionality.

A socket operation failed with error: The MSMQ Service failed to connect to the host that is referred to in the event description. Make sure that the host computer is online, and ensure that you have network connectivity to the host.

Connection was refused by the recipient computer: Confirm network connectivity to the host that is referred to in the event description. This error can also occur if there are no more Client Access Licenses (CALs) available on the host or if the connection limit for the host has been reached.

The select API for socket failed: The selected application programming interface (API) may have failed for several different reasons. The most common reason for this failure is socket connection time-out. Make sure that the computer has connectivity to the network.

Functioning in Domain

This monitor returns the following events:

- The Message Queuing service failed to join the computer's domain;
- Message Queuing objects cannot move automatically between domains;
- The computer object for this computer was not found in Active Directory;
- The Message Queuing service will not join the domain. An MSMQ Configuration (msmq) object exists in the new domain with an ID differing from the service ID;
- Message Queuing could not access Active Directory and failed to compute routing path for messages sent to queue.

Event ID: 2124, 2127, 2145, 2164, 2188.

The Message Queuing service failed to join the computer's domain: Message Queuing was not able to join the domain or MSMQ Routing failed because of domain connectivity issues. This error might be caused by one of the following conditions:

- Stale objects in Active Directory Domain Services (ADDS) are preventing Message Queuing from joining the domain.
- The computer does not have connectivity and cannot join a domain.
- Appropriate permissions are needed to create and access objects.

Message Queuing objects cannot move automatically between domains: If you were not trying to perform an interforrest migration, uninstall Message Queuing and then reinstall it in the new domain.
The computer object for this computer was not found in Active Directory: There is an issue with replication delays. This issue should be resolved after Active Directory Domain Services (ADDS) replicates itself.

An MSMQ Configuration (msq) object exists in the new domain with an ID differing from the service ID: Stale objects can prevent the MSMQ Service from operating properly. Deleting stale objects may solve this problem. However, deleting a computer object in Active Directory Domain Services (ADDS) can cause problems on the client computer. Before deleting the computer object, make sure that no services running on the client computer will be affected. In this case, deleting the Message Queuing Active Directory object will delete public queues on that computer.

Message Queuing could not access Active Directory and failed to compute routing path for messages sent to queue: Message Queuing was not able to join the domain or MSMQ Routing failed because of domain connectivity issues. This error might be caused by one of the following conditions:

- Stale objects in Active Directory Domain Services (ADDS) are preventing Message Queuing from joining the domain.
- The computer does not have connectivity and cannot join a domain.
- Appropriate permissions are needed to create and access objects.

Logging and Checkpoint

This monitor returns the following events:

- The Message Queuing service has insufficient privileges to create audit log messages;
- The incoming sequences checkpoint file failed to initialize;
- The transactions checkpoint file failed to initialize;
- The logger files cannot be initialized;
- The Message Queuing service cannot start. The checkpoint files cannot be recovered;
- The Message Queuing service cannot start. The log file cannot be recovered;
- The Message Queuing service cannot start. The message file and the log file cannot be reloaded.

Event ID: 2044, 2053, 2064, 2076, 2078, 2079, 2083.

The Message Queuing service has insufficient privileges to create audit log messages: The user that the MSMQ Service runs under must be able to set the SE_AUDIT_NAME privilege. This privilege is automatically granted to the Network Service. To resolve this issue, confirm that the MSMQ Service is running as a Network Service.

The incoming sequences checkpoint file failed to initialize: Checkpoint files must be available for Message Queuing to function properly. To resolve this issue, you must delete the incoming sequence checkpoint files, as well as the QMLog file in the Message Queuing storage directory. This can result in some messages being duplicated. However, this will get the service running as soon as possible and usually without data loss.
The transactions checkpoint file failed to initialize: Checkpoint files must be available for Message Queuing to function properly. To resolve this issue, you must delete the transaction checkpoint files, as well as the QMLog file in the Message Queuing storage directory. This can result in some messages being duplicated. However, this resolution will get the service running as soon as possible and usually without data loss.

The logger files cannot be initialized: The MSMQ Service needs access permissions on the checkpoint and log files. If the service has permissions and you receive this error, then the file is probably corrupt. To start the MSMQ Service without losing consistency, you must correct or recover corrupted checkpoint and log files.

The checkpoint files cannot be recovered: Checkpoint files must be available for Message Queuing to function properly. To resolve this issue, you must delete all the checkpoint files, as well as the QMLog file in the Message Queuing storage directory. This can result in some messages being duplicated. However, this resolution will get the service running as soon as possible and usually without data loss.

The log file cannot be recovered: The MSMQ Service needs access permissions on the checkpoint and log files. If the service has permissions and you receive this error, then the file is probably corrupt. To start the MSMQ Service without losing consistency, you must correct or recover corrupted checkpoint and log files.

The message file and the log file cannot be reloaded: The MSMQ Service needs access permissions on the checkpoint and log files. If the service has permissions and you receive this error, then the file is probably corrupt. To start the MSMQ Service without losing consistency, you must correct or recover corrupted checkpoint and log files.

Mapping Operation

This monitor returns the following events:

- The Message Queuing service stopped monitoring the mapping folder;
- The mapping file was ignored. Its content cannot be read;
- The mapping file was ignored because it was improperly formatted;
- The mapping of the URL to the queue was ignored. This URL is already mapped to another queue;
- The mapping of the URL to the queue is ignored. This queue name is not a valid URL-style queue name.

Event ID: 2155, 2156, 2158, 2157, 2161.

The Message Queuing service stopped monitoring the mapping folder: Verify that the MSMQ Service is installed and running. Also, verify the presence of the mapping directory.

The mapping file was ignored. Its content cannot be read: Verify that the MSMQ Service is installed and running. Also, verify the presence of the mapping directory.

The mapping file was ignored because it was improperly formatted: The mapping file that is referred to is not formatted properly. Confirm that the mapping file is a valid XML document with correct queue mappings.
The mapping of the URL to the queue was ignored. This URL is already mapped to another queue: Each alias can only be used once in a mapping file. If you have multiple mapping files in use, it is possible to have the same alias in different mapping files pointing to different queues, which also does not work.

The mapping of the URL to the queue is ignored. This queue name is not a valid URL-style queue name: The queue that is indicated in the event does not have a correctly formed URL-style queue name in an MSMQ SFD mapping file.

**MSDTC Service Operation**

This monitor returns the following events:

- The Message Queuing service cannot start. A connection with the Distributed Transaction Coordinator cannot be established;
- The Microsoft Distributed Transaction Coordinator (DTC) failed. The Message Queuing service cannot continue.

Event ID: 2047, 2143.

For these events, check if the Microsoft Distributed Transaction Coordinator service (MSDTC) is started.

**System Resources**

This monitor returns the following events:

- The message file cannot be created. There is insufficient disk space or memory;
- The Message Queuing folder cannot be created;
- The service cannot start due to insufficient disk space or memory;
- Machine MSMQ storage quota was exceeded or there is insufficient disk space;
- Message Queuing failed to send a message due to low memory;
- Message Queuing will not be able to accept messages temporarily because system paged pool is low;
- Message Queuing will not be able to accept messages temporarily because system commit is high;
- Storage quota exceeded for MSMQ queue.

Event ID: 2085, 2096, 2147, 2183, 2189, 2250, 2251, 2182.

**The message file cannot be created. There is insufficient disk space or memory:** Try identifying and closing other applications that may be consuming a large amount of memory. If it turns out that the MSMQ Service is the only program consuming a large amount of memory, try receiving the messages from the queues or increasing the rate of message processing.

**The Message Queuing folder cannot be created:** The Message Queuing access control list (ACL) needs appropriate permissions to the directory that it is trying to write to. Make sure that the MSMQ Service is running as an account that has permissions to create and modify directories to be used by the MSMQ Service. (By default, the MSMQ Service creates directories under the %windir%\System32\MSMQ directory.) You can do this by directly giving Modify, Read, and Write permissions to the account that the MSMQ Service runs under.
The service cannot start due to insufficient disk space or memory: The MSMQ Service needs adequate disk space and memory to function properly. Try freeing up disk space and memory and then restarting the MSMQ Service.

Machine MSMQ storage quota was exceeded or there is insufficient disk space: The Message Queuing machine quota has been reached. The sending application should request negative acknowledgements (NACK) from the computer to which it is sending messages. If a NACK is returned to the sending application and indicates that the quota for the destination queue or computer has been reached, the sending application can either stop sending messages or offload the messages to another destination.

Message Queuing failed to send a message due to low memory: Try identifying and closing other applications that may be consuming a large amount of memory. If it turns out that the MSMQ Service is the only program consuming a large amount of memory, try receiving the messages from the queues or increasing the rate of message processing.

Message Queuing will not be able to accept messages temporarily because system paged pool is low: Common system resources are almost fully consumed. Message Queuing will not operate properly until system resources are freed up.

Message Queuing will not be able to accept messages temporarily because system commit is high: Common system resources are almost fully consumed. Message Queuing will not operate properly until system resources are freed up.

Storage quota exceeded for MSMQ queue: A Message Queuing queue quota has been reached. To resolve this issue:

- Process existing messages in the queue to reduce the outstanding message count below the queue quota threshold. Confirm that messages are being processed at a higher rate than they are being queued. This may require additional hardware or changes to solution architecture.
- You may also increase the specific queue quota.

To avoid this problem in the future, the sending application should request negative acknowledgements (NACK) from the computer to which it is sending messages. If a NACK is returned to the sending application and it indicates that the quota for the destination queue or computer has been reached, the sending application can either stop sending messages or offload the messages to another destination. Nacks and Acks are requested programmatically by the sender.

Service Initializing

This monitor returns the following events:

- The Message Queuing service cannot start. The local RPC interface cannot be initialized;
- The Message Queuing service cannot start because a queue is in an inconsistent state;
- The service cannot start due to its failure to connect to its device driver;
- A multicast listener initialization failed. The file may be corrupted;
- The Message Queuing service stopped.

Event ID: 2061, 2084, 2148, 2154, 2163.
The local RPC interface cannot be initialized: The local remote procedure call (RPC) endpoint could not be initialized. Ensure that no other processes are using the RPC endpoint with the name "Qmsvc."

The Message Queuing service cannot start because a queue is in an inconsistent state: Verify that the MSMQ Service is installed and running.

The service cannot start due to its failure to connect to its device driver: There is a problem with the Mqcac.sys file. This file is located in the System32 folder under the Windows directory (usually C:\Windows). Make sure that the Mqcac.sys file is present in the System32 folder. If the file is there, try restarting the MSMQ Service by performing the following procedures.

A multicast listener initialization failed: Multicast listener failed on one or more files. This may indicate that the store is corrupt. Try deleting the queues (through the file system or the directory service) for which such errors are generated, and then restart Message Queuing. Before you delete a queue, make sure that the queue is empty and that Message Queuing is offline.

The Message Queuing service stopped: The MSMQ Service may have stopped for several reasons. Check your event logs for any earlier failures during service startup. Fix those issues, and then restart the MSMQ Service.

Message Events

This monitor returns the following events:

- Message Queuing could not authenticate a message sent to queue. The message was rejected because the queue only accepts authenticated messages;
- Message Queuing failed to verify digital signature of a message sent to queue. The message was rejected;
- The message could not be moved to deadletter queue. The message was moved to the system transactional deadletter queue;
- The message could not be moved to deadletter queue. The deadletter queue is authenticated and the authenticity of the message could not be verified;
- The message could not be moved to deadletter queue. Deadletter queues should not require privacy of messages;
- The message could not be moved to deadletter queue. The deadletter queue needs to be transactional.

Event ID: 2195, 2196, 2253, 2254, 2255, 2256.

Message Queuing could not authenticate a message sent to queue: Because the queue accepts only authenticated messages, messages that are sent to the queue must be authenticated and signed with a certificate, which is registered in Active Directory Domain Services (ADDS).

Message Queuing failed to verify digital signature of a message sent to queue: Confirm that the Message Queuing application is using a strong hash function and that it has a valid user certificate.

The message could not be moved to deadletter queue. The message was moved to the system transactional dead letter queue: A deadletter queue must exist. It also needs appropriate permissions.
The deadletter queue is authenticated and the authenticity of the message could not be verified: The deadletter queue that is mentioned in the error is authenticated, but the MSMQ Service could not confirm the authenticity of the message in the deadletter queue. To resolve this issue, do one of the following:

- Confirm that the computer that sent the message is properly signing its authenticated messages.
- Allow the deadletter queue to receive nonauthenticated messages.

Deadletter queues should not require privacy of messages: To allow messages to enter a deadletter queue, set the privacy level of the specified deadletter queue to None or Optional, or ensure that the messages that are being sent to the queue are encrypted.

The deadletter queue needs to be transactional: The deadletter queue that is specified in the event is nontransactional, but there are transactional messages trying to go there. To allow messages to go to the deadletter queue, recreate the deadletter queue as a transactional queue, or if you have control over the messages that are being sent to the queue, ensure that the messages are nontransactional. To recreate the deadletter queue as a transactional queue, create a new transactional queue with all the same properties as the original deadletter queue, but make the new queue transactional.

Queue Events

This monitor returns the following events:

- The Message Queuing service deleted the message. The message cannot be restored because the queue does not exist;
- The Message Queuing registry values cannot be read (the registry is probably corrupt);
- The properties of the queue cannot be set. Copying the queue file to the temporary file returned an error;
- The properties of the queue cannot be set. Replacing the queue file with the temporary file returned an error.

Event ID: 2043, 2097, 2141, 2142.

The Message Queuing service deleted message. The message cannot be restored because the queue does not exist: The event indicates that the message refers to a queue that no longer exists. This might be due to the message pointing to the wrong queue or the absence of the specified queue.

The Message Queuing registry values cannot be read: The MSMQ Service cannot read configuration information from the registry. This may indicate either that the registry is corrupted or that Message Queuing was not installed properly. Delete Message Queuing registry values and reinstall Message Queuing.

Copying the queue file to the temporary file returned error: Internally, the MSMQ Service tries to make a temporary copy of the queue file before changing the queue properties, or it tries to copy the new queue permissions file over the old permissions file. If creation of the temporary file fails, this might indicate insufficient disk space, permission problems, or file system errors. Make sure that the disk is not full and that the MSMQ Service can access the Message Queuing storage directory.
Replacing the queue file with the temporary file returned error: Internally, the MSMQ Service tries to make a temporary copy of the queue file before changing the queue properties, or it tries to copy the new queue permissions file over the old permissions file. If creation of the temporary file fails, this might indicate insufficient disk space, permission problems, or file system errors. Make sure that the disk is not full and that the MSMQ Service can access the Message Queuing storage directory.

Authorization Events

This monitor returns the following events:

- The Message Queuing service rejects incoming messages when it is unable to check whether the sender is allowed access to the queue for sending messages;
- Message Queuing could not complete SSL negotiation with the remote computer;
- Message Queuing could not validate server certificate in HTTPS scenario because the certificate was found in disallowed store;
- Message Queuing could not establish SSL connection with the recipient computer because a trust chain from the server certificate to a trusted Certificate Authority certificate could not be established;
- Message Queuing could not establish SSL connection with the recipient computer because the computer name specified in the HTTP queue format name does not match the name of the recipient server certificate.

Event ID: 2177, 2190, 2191, 2192, 2193.

The Message Queuing service rejects incoming messages when it is unable to check whether the sender is allowed access to the queue for sending messages: Add only the computer accounts that need access to the Windows Authorization Access Group.

Message Queuing could not complete SSL negotiation with the remote computer: This issue may have one of the following causes:

- The server certificate may not be installed properly.
- The remote computer may not be listening with HTTPS on port 443 (SSL). You can use the procedure "Determine if the computer is listening on port 443" to determine if this is the issue.
- The Windows Firewall may be blocking communication over port 443. You can use the procedure "Ensure that Windows Firewall is allowing communication over port 443" to determine if this is the issue.

Message Queuing could not validate server certificate in HTTPS scenario because the certificate was found in disallowed store: The certificate may have been revoked or otherwise disallowed. Therefore, it could not be trusted.

Message Queuing could not establish SSL connection with the recipient computer because a trust chain from the server certificate to a trusted Certificate Authority certificate could not be established: Reestablish the trust chain.
Message Queuing could not establish SSL connection with the recipient computer because the computer name specified in the HTTP queue format name does not match the name of the recipient server certificate: Although the certificate chain from the server was verified, the computer name that is specified in the queue format is different from the name of the recipient in the server certificate. Make sure that the computer name in the server certificate is correct.
Microsoft Message Queuing (Performance)

This template assesses the status and overall performance of a Microsoft Message Queuing server by retrieving statistics from performance counters and monitoring services.

Prerequisites

WMI access to the target server.

Credentials

Windows Administrator on the target server.

Monitored Components

You need to set thresholds for counters according to your environment. It is recommended to monitor counters for some period of time to understand potential value ranges and then set the thresholds accordingly.

Incoming Messages/sec

This component returns the rate at which incoming Message Queuing messages are placed in queues on the selected computer by the Message Queuing service.

Incoming Multicast Sessions

This component returns the number of open incoming multicast sessions involving the selected computer.

IP Sessions

This component returns the number of open IP sessions involving the selected computer.

MSMQ Incoming Messages

This component returns the total number of incoming Message Queuing messages placed in queues on the selected computer by the Message Queuing service.

Note: This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

MSMQ Outgoing Messages

This component returns the total number of outgoing Message Queuing messages sent from the selected computer by the Message Queuing service.

Note: This component has Count statistic as difference enabled. It will return the difference between two polling intervals.
**Outgoing HTTP Sessions**

This component returns the number of open outgoing HTTP sessions involving the selected computer.

**Outgoing Messages / sec**

This component returns the rate at which outgoing Message Queuing messages are sent from the selected computer by the Message Queuing service.

**Outgoing Multicast Sessions**

This component returns the number of open outgoing multicast sessions involving the selected computer.

**Sessions**

This component returns the total number of open network sessions involving the selected computer.

**Total bytes in all queues**

This component returns the total number of bytes in all Message Queuing messages residing in active queues on the selected computer.

**Total messages in all queues**

This component returns the total number of Message Queuing messages residing in active queues on the selected computer.

**Bytes in Journal Queue**

This component returns the total number of bytes in all Message Queuing messages that currently reside in the selected journal. For the Computer Queues instance, this counter represents the computer journal.

> The instance field is installation-specific. By default, the instance set to “Computer Queues.”

**Bytes in Queue**

This component returns the total number of bytes in all Message Queuing messages that currently reside in the selected queue. For the Computer Queues instance, this counter represents the deadletter queue.

> The instance field is installation-specific. By default, the instance set to “Computer Queues.”

**Messages in Journal Queue**

This component returns the total number of Message Queuing messages that currently reside in the selected journal. For the Computer Queues instance, this counter represents the computer journal.

> The instance field is installation-specific. By default, the instance set to “Computer Queues.”
Messages in Queue

This component returns the total number of Message Queuing messages that currently reside in the selected queue. For the Computer Queues instance, this counter represents the deadletter queue.

The instance field is installation-specific. By default, the instance set to “Computer Queues.”

Service: Message Queuing

This component returns the CPU and memory usage of the Message Queuing service. This service provides a messaging infrastructure and development tool for creating distributed messaging applications for Windows-based networks and programs.

Service: Message Queuing Triggers

This component returns the CPU and memory usage of Message Queuing Triggers service. This service provides rule-based monitoring of messages arriving in a Message Queuing queue and, when the conditions of a rule are satisfied, invokes a COM component or a stand-alone executable program to process the message.

By default, this component is disabled. If you use this service in your environment you should enable it.

Message Queuing RPC-based remote port (public queue)

This component monitor tests the ability of a Message Queuing server to accept incoming sessions. This port is used by Message Queuing independent clients and servers to listen for RPC-based remote reads of their public queues. The dependent client also uses this port to communicate with its server for send and for receive.

By default, TCP port 2103 is monitored.

Message Queuing RPC-based remote port (private queue)

This component monitor tests the ability of a Message Queuing server to accept incoming sessions. This port is used by Message Queuing independent clients and servers to listen for RPC-based remote reads of their private queues. The dependent client also uses this port to communicate with its server for send and for receive.

By default, TCP port 2103 is monitored.

Connection between Queue Managers port

This component monitor tests the ability of a Message Queuing server to accept incoming sessions. This port is used for Message Queuing (including HTTP messaging) message traffic and internal session management traffic between Queue Managers.

By default, TCP port 1801 is monitored.
Microsoft Network Policy

The following templates are available:

- Microsoft Network Policy Server Events
- Microsoft Network Policy Server RADIUS Proxy
- Microsoft Network Policy Server RADIUS Server
Microsoft Network Policy Server Events

This template assesses the status and overall performance of a Microsoft Network Policy Server (NPS). This template uses Windows System and Security Event Logs.

Prerequisites

WMI access to the target server.

Credentials

Windows Administrator on the target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

All Windows Event Log monitors should return zero values. Returned values other than zero indicate an abnormality. Examining the Windows System and Security log files should provide information pertaining to the issue.

Detailed information about all these events can be found here: http://technet.microsoft.com/en-us/library/cc732054(WS.10).aspx.

Warning: NPS discarded the request for a user

This monitor returns the number of events when the Network Policy Server discarded the request for a user.

Type of event: Warning. Event ID: 6274.

This condition occurs when the NPS discards accounting requests because the structure of the accounting request message that was sent by a RADIUS client does not comply with the RADIUS protocol. You should reconfigure, upgrade, or replace the RADIUS client.

Warning: Domain Controller is not responsive

This monitor returns the number of events when domain controller is not responsive.

Type of event: Warning. Event ID: 4401.

You should check your domain controller availability.

Warning: NPS denied access to a user

This monitor returns the number of events when the Network Policy Server denied access to a user.

Type of event: Warning. Event ID: 6273.

This error might be caused by one of the following conditions:

- The user does not have valid credentials;
• The connection method is not allowed by the network policy;
• The network access server is under attack;
• NPS does not have access to the user account database on the domain controller;
• NPS log files and/or the SQL Server database is not available.

Warning: Internal error

This monitor returns the number of events when an internal error occurred while processing a request.

Type of event: Warning. Event ID: 12.

This error is typically returned when an exception that is not identified by some other error occurs. This error can also be returned by Extensible Authentication Protocol (EAP) or Schannel.

Warning: NPS discarded the accounting request for a user

This monitor returns the number of events when Network Policy Server discarded the accounting request for a user.

Type of event: Warning. Event ID: 6275.

Network corruption, latency, or other network problems unrelated to NPS might produce this condition. Wait a short while to see if the condition still exists. This problem might resolve itself.

Warning: Remote RADIUS server has not responded

This monitor returns the number of events when the remote RADIUS server has not responded to consecutive requests.

Type of event: Warning. Event ID: 36.

You should manually check the availability of the remote RADIUS server.

Warning: Server communication problems

This monitor returns the number of events when NPS cannot communicate with RADIUS clients due to different errors in the RADIUS message.

Type of event: Warning. Event ID: 15,16,17,18,19.

This condition can occur if the server running NPS receives one of the following from a RADIUS client:

• A response of a malformed message;
• A response that contains an incorrect value in the Code field;
• An Access-Request message that does not contain a Message-Authenticator attribute;
• A response that contains a message authenticator that is not valid;
• An Access-Request message that contains an Extensible Authentication Protocol (EAP) message, but no Message-Authenticator attribute.

Network corruption, latency, or other network problems unrelated to NPS might produce this condition. Wait a short while to confirm that the condition still exists. This problem might resolve itself.
Warning: NPS could not send a response due to network problems

This monitor returns the number of events when NPS could not send a response due to a network error. The data is the error code generated by Windows Sockets.

Type of event: Warning. Event ID: 22.

Use Windows Sockets error messages and documentation to determine the Windows Sockets reason for failure and to help determine the steps for a resolution. For more information, see Windows Sockets Error Codes at http://go.microsoft.com/fwlink/?LinkId=95404.

Warning: RADIUS error occurred

This monitor returns the number of events when a RADIUS error occurred.

Type of event: Warning. Event ID: 23.

Use Windows Sockets error messages and documentation to determine the Windows Sockets reason for failure and to help determine the steps for a resolution. For more information, see Windows Sockets Error Codes at http://go.microsoft.com/fwlink/?LinkId=95404.

Warning: Message with invalid authenticator

This monitor returns the number of events when a RADIUS message was received from a RADIUS client with an invalid authenticator.

Type of event: Warning. Event ID: 14.

This is typically caused by mismatched shared secrets. Verify the configuration of the shared secret for the RADIUS client in the Network Policy Server snap-in and the configuration of the network access server.

Warning: Response to client exceeds maximum message length

This monitor returns the number of events when the response to a RADIUS client exceeds the maximum RADIUS message length of 4096 bytes.


This condition can occur under the following circumstances:

- The RADIUS client configuration is incorrect and NPS received a RADIUS message that contains an authenticator that is not valid
- The RADIUS client needs to be updated because the size of the RADIUS message received from the RADIUS client exceeds the message size specified in the RADIUS protocol.

Warning: Could not resolve the name of RADIUS client

This monitor returns the number of events when the name of the RADIUS client could not be resolved. The data returned is the error code generated by Windows Sockets.

Type of event: Warning. Event ID: 10.

This condition can occur under the following circumstances:
In the NPS Microsoft Management Console (MMC), a RADIUS client is configured by fully qualified domain name (FQDN) or NetBIOS name, rather than by IP address, and NPS has not received a DNS server response to the name resolution query. Without the IP address provided by the name resolution query, NPS cannot contact the RADIUS client;

- NPS is receiving communication from a RADIUS client that is not configured in the NPS MMC;
- In the NPS MMC, a RADIUS client is configured by either IPv4 or IPv6 address, but the format of the IP address is incorrect.

**Warning: Wrong RADIUS clients IP address**

This monitor returns the number of events when the IP address of the RADIUS client is not a valid IP address.

Type of event: Warning. Event ID: 11.

This condition can occur under the following circumstances:

- In the NPS Microsoft Management Console (MMC), a RADIUS client is configured by fully qualified domain name (FQDN) or NetBIOS name rather than by IP address, and NPS has not received a DNS server response to the name resolution query. Without the IP address provided by the name resolution query, NPS cannot contact the RADIUS client;
- NPS is receiving communication from a RADIUS client that is not configured in the NPS MMC;
- In the NPS MMC, a RADIUS client is configured by either IPv4 or IPv6 address, but the format of the IP address is incorrect.

**Warning: Message received from invalid RADIUS client IP**

This monitor returns the number of events when a RADIUS message was received from the invalid RADIUS client IP address.


This condition can occur under the following circumstances:

- In the NPS Microsoft Management Console (MMC), a RADIUS client is configured by fully qualified domain name (FQDN) or NetBIOS name rather than by IP address, and NPS has not received a DNS server response to the name resolution query. Without the IP address provided by the name resolution query, NPS cannot contact the RADIUS client;
- NPS is receiving communication from a RADIUS client that is not configured in the NPS MMC;
- In the NPS MMC, a RADIUS client is configured by either IPv4 or IPv6 address, but the format of the IP address is incorrect.

**Error: No available domain controllers**

This monitor returns the number of events that occur when there is no domain controller available for the domain.

Type of event: Error. Event ID: 4402.

You should check your domain controller availability.
Error: NPS license compliance

This monitor returns the number of events when this edition of Windows Server cannot support any of the following NPS configurations:

- More than 50 RADIUS clients;
- More than two RADIUS server groups;
- Client identification by subnet mask.

Type of event: Error. Event ID: 46.

To set up your server to support any of these configurations, install a Windows Server edition without these limitations.

Error: Disk is full

This monitor returns the number of events that occur when a disk is full. NPS could not delete older log files to create free space or could not find older an log file to delete and create free space.

Type of event: Error. Event ID: 43,44.

You should verify that there is free disk space.

Error: RADIUS proxy could not resolve the name of remote server

This monitor returns the number of events when the RADIUS Proxy could not resolve the name of remote RADIUS server in a remote RADIUS server group to an IP address.

Type of event: Error. Event ID: 24.

You should manually check DNS settings and the availability of the remote RADIUS server.

Error: Unable to forward request to remote server

This monitor returns the number of events that occur when the RADIUS Proxy was unable to forward a RADIUS request to a remote RADIUS server because of a network error.

Type of event: Error. Event ID: 33.

You should manually check network configuration.
Microsoft Network Policy Server RADIUS Proxy

This template assesses the status and overall performance of a Microsoft Network Policy Server (NPS) configured as RADIUS proxy.

ℹ️ Apply this template if you have NPS installed as a RADIUS proxy.

**Prerequisites**

- WMI access to the target server.

**Credentials**

- Windows Administrator on the target server.

**Monitored Components**

ℹ️ For details on monitors, see [SAM Component Monitor Types](#).

You need to set thresholds for counters according to your environment. It is recommended to monitor counters for some period of time to understand potential value ranges and then set the thresholds accordingly.

**Accounting: Accounting-Requests/sec**

This monitor returns the average number of RADIUS Accounting-Request packets sent per second to the accounting port.

**Accounting: Accounting-Responses/sec**

This monitor returns the average number of RADIUS Accounting-Response packets received per second on the accounting port.

**Authentication: Access-Accepts/sec**

This monitor returns the average number of RADIUS Access-Accept packets received per second from this server.

**Authentication: Access-Challenges/sec**

This monitor returns the average number of RADIUS Access-Challenge packets received per second from this server.

**Authentication: Access-Rejects/sec**

This monitor returns the average number of RADIUS Access-Reject packets received per second from this server.

**Authentication: Access-Requests/sec**

This monitor returns the average number of RADIUS Access-Request packets sent per second to this server.
Authentication: Bad Authenticators/sec
This monitor returns the average number of RADIUS packets that contain an invalid Message Authenticator attribute per second.

Authentication: Dropped Packets/sec
This monitor returns the average number of incoming packets per second that are silently discarded for a reason other than "malformed," "invalid Message Authenticator," or "unknown type."

Authentication: FullAccess-Decisions/sec
This monitor returns the average number of Full-Access decisions received per second from this server.

Authentication: Malformed Packets/sec
This monitor returns the average number of packets containing malformed data received per second.

Authentication: Probation-Decisions/sec
This monitor returns the average number of probation decisions received per second from this server.

Authentication: Quarantine-Decisions/sec
This monitor returns the average number of quarantine decisions received per second from this server.

Authentication: Unknown Type/sec
This monitor returns the average number of unknown type (non-RADIUS) packets received per second.

Authentication: Invalid Addresses/sec
This monitor returns the average number of packets received per second from unknown addresses.

Authentication: Pending Requests
This monitor returns the number of requests destined for this server that have not yet timed out or received a response.

Authentication: Request Timeouts/sec
This monitor returns the average number of request timeouts per second to this server.

Authentication: Retransmissions/sec
This monitor returns the average number of requests retransmitted per second to this server.

Policy Engine: Last Round-Trip Time
This monitor returns the interval (in hundredths of a second) between the most recent request to the policy engine and its response.
**Policy Engine: Matched Remote Access Policies/sec**

This monitor returns the average number of remote access policies that have been matched per second.

**Policy Engine: Pending Requests**

This monitor returns the number of requests that have entered the policy engine but have not yet completed the process.

**Service: Network Policy Server**

This monitor returns the CPU and memory usage of the Network Policy Server service. This service manages authentication, authorization, auditing and accounting for virtual private network (VPN), dial-up, 802.1x wireless or Ethernet switch connection attempts sent by access servers that are compatible with the IETF RADIUS protocol. If this service is stopped, users might be unable to obtain a VPN, dial-up, wireless, or Ethernet connection to the network. If this service is disabled, any services that explicitly depend on it will fail to start.
Microsoft Network Policy Server RADIUS Server

This template assesses the status and overall performance of a Microsoft Network Policy Server (NPS) configured as a RADIUS server.

Apply this template if you have NPS installed as a RADIUS server.

**Prerequisites**
- WMI access to the target server.

**Credentials**
- Windows Administrator on the target server.

**Monitored Components**

For details on monitors, see [SAM Component Monitor Types](#).

You need to set thresholds for counters according to your environment. It is recommended to monitor counters for some period of time to understand potential value ranges and then set the thresholds accordingly.

**Service: Network Policy Server**

This monitor returns the CPU and memory usage of the Network Policy Server service. This service manages authentication, authorization, auditing, and accounting for virtual private network (VPN), dial-up, 802.1x wireless or Ethernet switch connection attempts sent by access servers that are compatible with the IETF RADIUS protocol. If this service is stopped, users might be unable to obtain a VPN, dial-up, wireless, or Ethernet connection to the network. If this service is disabled, any services that explicitly depend on it will fail to start.

**Accounting: Accounting-Requests/sec**

This monitor returns the average number of RADIUS Accounting-Requests received on the accounting port, per second.

**Accounting: Accounting-Responses/sec**

This monitor returns the average number of RADIUS Accounting-Responses sent per second.

**Accounting: Server Reset Time**

This monitor returns the time elapsed (in hundredths of a second) since the configuration of this NPS server was reset because of a configuration change or because the service control manager sent a reset to the NPS service.

**Accounting: Server Up Time**

This monitor returns the time elapsed (in hundredths of a second) since the server process was started on this NPS server.
Authentication: Access-Accepts/sec
This monitor returns the average number of RADIUS Access-Accept packets sent per second.

Authentication: Access-Challenges/sec
This monitor returns the average number of RADIUS Access-Challenge packets sent per second.

Authentication: Access-Rejects/sec
This monitor returns the average number of RADIUS Access-Reject packets sent per second.

Authentication: Access-Requests/sec
This monitor returns the average number of packets received per second on the authentication port.

Authentication: Bad Authenticators/sec
This monitor returns the average number of RADIUS packets per second that contain an invalid Message Authenticator attribute.

Authentication: Dropped Packets/sec
This monitor returns the average number of incoming packets per second that are silently discarded for a reason other than "malformed," "invalid Message Authenticator," or "unknown type."

Authentication: FullAccess-Decisions/sec
This monitor returns the average number of Full-Access decisions sent per second to this client.

Authentication: Malformed Packets/sec
This monitor returns the average number of packets containing malformed data received per second.

Authentication: Probation-Decisions/sec
This monitor returns the average number of probation decisions sent per second to this client.

Authentication: Quarantine-Decisions/sec
This monitor returns the average number of quarantine decisions sent per second to this client.

Authentication: Unknown Type/sec
This monitor returns the average number of unknown type (non-RADIUS) packets received per second.

Authentication: Invalid Requests/sec
This monitor returns the average number of RADIUS packets from unknown clients or remote RADIUS servers received per second.

Policy Engine: Last Round-Trip Time
This monitor returns the interval (in hundredths of a second) between the most recent request to the policy engine and its response.
Policy Engine: Matched Remote Access Policies/sec

This monitor returns the average number of remote access policies that have been matched per second.

Policy Engine: Pending Requests

This monitor returns the number of requests that have entered the policy engine but have not yet completed the process.
Microsoft Office 365

The following templates are available for Microsoft Office 365:

- Microsoft Office 365 Exchange Mailboxes
- Microsoft Office 365 Exchange Mobile Device Statistics
- Microsoft Office 365 Exchange Online
- Microsoft Office 365 Group Statistics
- Microsoft Office 365 License Statistics
- Microsoft Office 365 Mail Traffic Statistics
- Microsoft Office 365 Mobile Device Management
- Microsoft Office 365 Portal
- Microsoft Office 365 Security Statistics
- Microsoft Office 365 Subscription
- Office 365 User Statistics with PowerShell

Microsoft Office 365 Exchange Mailboxes

This template shows information about Office 365 Exchange mailboxes and includes the following Component Monitors:

- Inactive Exchange Users
- Mailbox Sizes (largest mailboxes)
- Mailboxes over Quota
- Mailbox Sizes (Shared)
- Archived Mailboxes
- Forwarded Exchange Users

Prerequisites

WMI access to the target server


**Important:** The PowerShell script mentioned in the Microsoft article above should be run on the Orion server, not the target node.
Credentials

- An Orion account with SAM administrator permissions.
- An Office 365 account with global administrator privileges.
  - The account must be a member of an Office 365 admin role.
  - The account should be an all-in-one, inclusive account to support the monitoring of all mailboxes.

Important: Use UPN format (username@domain) — not domain\username format to enter credentials. Also, a service account for Exchange Web Services is recommended to avoid authentication issues when passwords are updated.

Microsoft Office 365 Exchange Mobile Device Statistics

This template shows information about Office 365 Exchange mobile devices and includes the following component monitors:

- Mobile Users (Users with mobile devices associated with them)
- Mobile Devices by OS
- Mobile Devices (Inactive)
- Mobile Devices by Access State (Allowed vs. Blocked)

Prerequisites

WMI access to the target server


Important: The PowerShell script mentioned in the Microsoft article above should be run on the Orion server, not the target node.

Credentials

- An Orion account with SAM administrator permissions.
- An Office 365 account with global administrator privileges.
  - The account must be a member of an Office 365 admin role.
  - The account should be an all-in-one, inclusive account to support the monitoring of all mailboxes.

Important: Use UPN format (username@domain) — not domain\username format to enter credentials. Also, a service account for Exchange Web Services is recommended to avoid authentication issues when passwords are updated.
Microsoft Office 365 Exchange Online

This template shows status of Office 365 Exchange feature availability and includes the following Component Monitors:

- Sign-In
- E-Mail and calendar access
- E-Mail timely delivery
- Management and Provisioning
- Voice mail

Prerequisites

WMI access to the target server


**Important:** The PowerShell script mentioned in the Microsoft article above should be run on the Orion server, not the target node.

Credentials

- An Orion account with SAM administrator permissions.
- An Office 365 account with global administrator privileges.
  - The account must be a member of an Office 365 admin role.
  - The account should be an all-in-one, inclusive account to support the monitoring of all mailboxes.

Use UPN format (username@domain) — not domain\username format to enter credentials. Also, a service account for Exchange Web Services is recommended to avoid authentication issues when passwords are updated.

Microsoft Office 365 Group Statistics

This template shows information about Office 365 Exchange group statistics and includes the following Component Monitors.

- Groups
- Empty Groups
- Groups Accepting External Mail

Prerequisites

WMI access to the target server

**Important:** The PowerShell script mentioned in the Microsoft article above should be run on the Orion server, not the target node.

**Credentials**

- An Orion account with SAM administrator permissions.
- An Office 365 account with global administrator privileges.
  - The account must be a member of an Office 365 admin role.
  - The account should be an all-in-one, inclusive account to support the monitoring of all mailboxes.

*Use UPN format (username@domain) — not domain\username format to enter credentials. Also, a service account for Exchange Web Services is recommended to avoid authentication issues when passwords are updated.*

**Microsoft Office 365 License Statistics**

This template shows information about Office 365 Subscription Statistics and includes the following Component Monitors:

- License Usage Over Time - Consumed license units based on part number (SKU)
- Subscription Overview - Number of active subscriptions in your environment
- License by User - users with more than the threshold limit of licenses associated with their account
- Users without License - users who have a license count of 0
- Subscriptions Assigned by User - number of subscriptions for each user
- Users with No Subscriptions - users with no subscriptions associated with them

**Prerequisites**

WMI access to the target server


**Important:** The PowerShell script mentioned in the Microsoft article above should be run on the Orion server, not the target node.

**Credentials**

- An Orion account with SAM administrator permissions.
- An Office 365 account with global administrator privileges.
  - The account must be a member of an Office 365 admin role.
  - The account should be an all-in-one, inclusive account to support the monitoring of all mailboxes.
Use UPN format (username@domain) — not domain\username format to enter credentials. Also, a service account for Exchange Web Services is recommended to avoid authentication issues when passwords are updated.

Microsoft Office 365 Mail Traffic Statistics

This template shows information about Office 365 Exchange traffic statistics. The information provided includes the top senders and receivers of email in your environment based on count.

Prerequisites

WMI access to the target server


Important: The PowerShell script mentioned in the Microsoft article above should be run on the Orion server, not the target node.

Credentials

• An Orion account with SAM administrator permissions.
• An Office 365 account with global administrator privileges.
  ▪ The account must be a member of an Office 365 admin role.
  ▪ The account should be an all-in-one, inclusive account to support the monitoring of all mailboxes.

Use UPN format (username@domain) — not domain\username format to enter credentials. Also, a service account for Exchange Web Services is recommended to avoid authentication issues when passwords are updated.

Microsoft Office 365 Mobile Device Management

This template returns a status code for mobile device management availability. The Component Type is Windows PowerShell Monitor.

Prerequisites

WMI access to the target server


Important: The PowerShell script mentioned in the Microsoft article above should be run on the Orion server, not the target node.
**Credentials**

- An Orion account with SAM administrator permissions.
- An Office 365 account with global administrator privileges.
  - The account must be a member of an Office 365 admin role.
  - The account should be an all-in-one, inclusive account to support the monitoring of all mailboxes.

> Use UPN format (username@domain) — not domain\username format to enter credentials. Also, a service account for Exchange Web Services is recommended to avoid authentication issues when passwords are updated.

**Microsoft Office 365 Portal**

This template shows status of features made available via Microsoft's O365 status page and includes the following Component Monitors:

- Licensing and Renewal
- Network Availability
- Office Professional Plus Download

**Prerequisites**

WMI access to the target server


> **Important:** The PowerShell script mentioned in the Microsoft article above should be run on the Orion server, not the target node.

**Microsoft Office 365 Subscription**

This template shows status of features made available via Microsoft's O365 status page and includes the following Component Monitors:
Prerequisites

WMI access to the target server


Important: The PowerShell script mentioned in the Microsoft article above should be run on the Orion server, not the target node.

Credentials

- An Orion account with SAM administrator permissions.
- An Office 365 account with global administrator privileges.
  - The account must be a member of an Office 365 admin role.
  - The account should be an all-in-one, inclusive account to support the monitoring of all mailboxes.

Use UPN format (username@domain) — not domain\username format to enter credentials. Also, a service account for Exchange Web Services is recommended to avoid authentication issues when passwords are updated.

Microsoft Office 365 Security Statistics

This template shows status of Office 365 Exchange mailbox security and includes the following Component Monitors:

- User Mailbox Security - Users that have access to more than 20 mailboxes
- Users by Retention Policy - Users assigned to retention policies and their respective names
- User Password Settings - Users based on password expiration settings
- Last Password Change - Number of users that have password changes more than 90 days ago
- Administrative Roles - Administrative roles and the number of users assigned to them
- Mailbox Auditing - Mailboxes that currently have audit enabled
- Multi-Factor Authentication - Users that have multi-factor authentication enabled

Prerequisites

WMI access to the target server


Important: The PowerShell script mentioned in the Microsoft article above should be run on the Orion server, not the target node.
Credentials

- An Orion account with SAM administrator permissions.
- An Office 365 account with global administrator privileges.
  - The account must be a member of an Office 365 admin role.
  - The account should be an all-in-one, inclusive account to support the monitoring of all mailboxes.

Use UPN format (username@domain) — not domain\username format to enter credentials. Also, a service account for Exchange Web Services is recommended to avoid authentication issues when passwords are updated.

Office 365 User Statistics with PowerShell

This template tracks the statistics of Exchange mailboxes of Exchange Online server using PowerShell scripts.

Prerequisites

See Use PowerShell in SAM for prerequisites.

Credentials

- An Orion account with SAM administrator permissions.
- An Office 365 account with global administrator privileges.
  - The account must be a member of an Office 365 admin role.
  - The account should be an all-in-one, inclusive account to support the monitoring of all mailboxes.

Use UPN format (username@domain) — not domain\username format to enter credentials. Also, a service account for Exchange Web Services is recommended to avoid authentication issues when passwords are updated.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Recipient Statistics Report

This component monitor returns recipient statistics report which include the following:

- Total Number Of Mailboxes;
- Total Number Of Active Mailboxes;
- Number Of Contacts;
- Number Of Distribution Lists.

Total Items Count
This component monitor returns the total number of emails on the server.

**Total Items Size (MB)**

This component monitor returns the total mail size on the server in MB.

**Specific User Items Count**

This component monitor returns the number of emails for the specified user.

You must specify the correct arguments in the Script Arguments field of the corresponding PowerShell Monitor. This monitor requires the following argument:

```
user_name
where:
user_name - target username;
```

Example: john

**Specific User Items Size (MB)**

This component monitor returns the mailbox size for the specified user in MB.

You must specify the correct arguments in the Script Arguments field of the corresponding PowerShell Monitor. This monitor requires the following argument:

```
user_name
where:
user_name - target username;
```

Example: john

**Test User MAPI Connectivity**

This component verifies that a specified mailbox can connect by using the MAPI protocol, which is used by Microsoft Office Outlook.

By default, this monitor is disabled.

Possible returned values:
- 0 – Test failed. See message field for errors.
- 1 – MAPI Test successfully finished.

You must specify the correct arguments in the Script Arguments field of the corresponding PowerShell Monitor. This monitor requires the following argument:

```
user_name
where:
user_name - target username;
```

Example: john
Microsoft Routing and Remote Access

The following templates are available:

- Microsoft Routing and Remote Access 2008-2012 R2
- Microsoft Routing and Remote Access 2008 - 2016 (Events)
- Microsoft Routing and Remote Access 2016 (Events)
- Microsoft Routing and Remote Access 2016

Periodically, SolarWinds releases SAM templates to support the latest product versions such as Microsoft Server 2016. You can continue using templates for older product versions, but updating to the latest template is recommended.

Microsoft Routing and Remote Access 2008-2012 R2


Prerequisites

- WMI access to the target server.

Credentials

- Windows Administrator on the target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Service: Routing and Remote Access

This monitor returns CPU and memory usage of the Routing and Remote Access service. It offers routing services to businesses in local area and wide area network environments.

All Protocols: Alignment Errors

This monitor returns the total number of Alignment Errors for this connection. Alignment Errors occur when a byte received is different from the byte expected.

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

All Protocols: Buffer Overrun Errors

This monitor returns the total number of Buffer Overrun Errors for this connection. Buffer
Overrun Errors occur when the software cannot handle the rate at which data is received.

- **All Protocols: Bytes Received/Sec**
  This monitor returns the number of bytes received per second.

- **All Protocols: Bytes Transmitted/Sec**
  This monitor returns the number of bytes transmitted per second.

- **All Protocols: CRC Errors**
  This monitor returns the total number of CRC Errors for this connection. CRC Errors occur when the frame received contains erroneous data.

- **All Protocols: Percent Compression In**
  This monitor returns the compression ratio for bytes being received.

- **All Protocols: Percent Compression Out**
  This monitor returns the compression ratio for bytes being transmitted.

- **All Protocols: Serial Overrun Errors**
  This monitor returns the total number of Serial Overrun Errors for this connection. Serial Overrun Errors occur when the hardware cannot handle the rate at which data is received.

- **All Protocols: Timeout Errors**
  This monitor returns the total number of Timeout Errors for this connection. Timeout Errors occur when an expected is not received in time.

- **All Protocols: Total Errors/Sec**
  This monitor returns the total number of CRC, Timeout, Serial Overrun, Alignment, and Buffer Overrun Errors per second.

- **RAS Port: Alignment Errors**
  This monitor returns the total number of Alignment Errors for this connection. Alignment Errors occur when a byte received is different from the byte expected.
- This component has Count statistic as difference enabled. It will return the difference between two polling intervals.
- By default, this monitor is disabled.
- The instance field is installation-specific. You need to specify RRAS protocol (for example: VPN0-0). You can see all available instances in perfmon by looking counters in “RAS Port” object.

**RAS Port: Buffer Overrun Errors**

This monitor returns the total number of Buffer Overrun Errors for this connection. Buffer Overrun Errors occur when the software cannot handle the rate at which data is received.

- This component has Count statistic as difference enabled. It will return the difference between two polling intervals.
- By default, this monitor is disabled.
- The instance field is installation-specific. You need to specify RRAS protocol (for example: VPN0-0). You can see all available instances in perfmon by looking counters in “RAS Port” object.

**RAS Port: Bytes Received/Sec**

This monitor returns the number of bytes received per second.

- By default, this monitor is disabled.
- The instance field is installation-specific. You need to specify RRAS protocol (for example: VPN0-0). You can see all available instances in perfmon by looking counters in “RAS Port” object.

**RAS Port: Bytes Transmitted/Sec**

This monitor returns the number of bytes transmitted per second.

- By default, this monitor is disabled.
- The instance field is installation-specific. You need to specify RRAS protocol (for example: VPN0-0). You can see all available instances in perfmon by looking counters in “RAS Port” object.

**RAS Port: CRC Errors**

This monitor returns the total number of CRC Errors for this connection. CRC Errors occur when the frame received contains erroneous data.

- This component has Count statistic as difference enabled. It will return the difference between two polling intervals.
- By default, this monitor is disabled.
- The instance field is installation-specific. You need to specify RRAS protocol (for example: VPN0-0). You can see all available instances in perfmon by looking counters in “RAS Port” object.

**RAS Port: Percent Compression In**

This monitor returns the compression ratio for bytes being received.
By default, this monitor is disabled.

The instance field is installation-specific. You need to specify RRAS protocol (for example: VPN0-0). You can see all available instances in perfmon by looking counters in “RAS Port” object.

RAS Port: Percent Compression Out

This monitor returns the compression ratio for bytes being transmitted.

By default, this monitor is disabled.

The instance field is installation-specific. You need to specify RRAS protocol (for example: VPN0-0). You can see all available instances in perfmon by looking counters in “RAS Port” object.

RAS Port: Serial Overrun Errors

This monitor returns the total number of Serial Overrun Errors for this connection. Serial Overrun Errors occur when the hardware cannot handle the rate at which data is received.

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

By default, this monitor is disabled.

The instance field is installation-specific. You need to specify RRAS protocol (for example: VPN0-0). You can see all available instances in perfmon by looking counters in “RAS Port” object.

RAS Port: Timeout Errors

This monitor returns the total number of Timeout Errors for this connection. Timeout Errors occur when an expected is not received in time.

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

By default, this monitor is disabled.

The instance field is installation-specific. You need to specify RRAS protocol (for example: VPN0-0). You can see all available instances in perfmon by looking counters in “RAS Port” object.

RAS Port: Total Errors/Sec

This monitor returns the total number of CRC, Timeout, Serial Overrun, Alignment, and Buffer Overrun Errors per second.

By default, this monitor is disabled.

The instance field is installation-specific. You need to specify RRAS protocol (for example: VPN0-0). You can see all available instances in perfmon by looking counters in “RAS Port” object.
Microsoft Routing and Remote Access 2008 - 2016 (Events)


Prerequisites

WMI access to the target server.

Credentials

Windows Administrator on the target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Warning and Errors: Remote Access

This monitor returns warning and error events of the Routing and Remote Access connections.

Source Name: RemoteAccess.
Log File: Application.

Warning and Errors: Secure Socket Tunneling Protocol

This monitor returns warning and error events of Secure Socket Tunneling Protocol (SSTP).

Source Name: RasSstp.
Log File: Application.

Warning and Errors: RAS Client

This monitor returns warning and error events of the Routing and Remote Access clients.

Source Name: RasClient.
Log File: Application.

Warning and Errors: RAS Connection Manager Service

This monitor returns warning and error events of the Routing and Remote Access Manager service.

Source Name: RasMan.
Log File: Application.

Warning and Errors: DHCPv6

This monitor returns warning and error events of the DHCPv6 Relay Agent.

Source Name: RasRoutingProtocols-dhcpv6r.
Log File: Application.

Warning and Errors: IGMPv2
This monitor returns warning and error events of the Internet Group Management Protocol (IGMP).

**Source Name:** RasRoutingProtocols-IGMPv2.
**Log File:** Application.

**Warning and Errors: RIP**

This monitor returns warning and error events of the Router Information Protocol (RIP).

**Source Name:** RasRoutingProtocols-IPRIP2.
**Log File:** Application.

**Warning and Errors: BOOTP Relay Agent**

This monitor returns warning and error events of the Bootstrap Protocol (BOOTP) relay agent.

**Source Name:** RasIpBootp.
**Log File:** Application.

**Warning and Errors: RAS Server**

This monitor returns warning and error events of the Routing and Remote Access service.

**Source Name:** RasServer.
**Log File:** Application.

---

**Microsoft Routing and Remote Access 2016**

This template assesses the status and overall performance of a Microsoft Routing and Remote Access on Windows 2016.

**Prerequisites**

- WMI access to the target server.

**Credentials**

- Windows Administrator on the target server.

**Monitored Components**

- **Service: Routing and Remote Access**
  - This monitor returns CPU and memory usage of the Routing and Remote Access service. It offers routing services to businesses in local area and wide area network environments.

- **All Protocols: Alignment Errors**
  - This monitor returns the total number of Alignment Errors for this connection. Alignment Errors occur when a byte received is different from the byte expected.
This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

All Protocols: Buffer Overrun Errors
This monitor returns the total number of Buffer Overrun Errors for this connection. Buffer Overrun Errors occur when the software cannot handle the rate at which data is received.

All Protocols: Bytes Received/Sec
This monitor returns the number of bytes received per second.

All Protocols: Bytes Transmitted/Sec
This monitor returns the number of bytes transmitted per second.

All Protocols: CRC Errors
This monitor returns the total number of CRC Errors for this connection. CRC Errors occur when the frame received contains erroneous data.

All Protocols: Percent Compression In
This monitor returns the compression ratio for bytes being received.

All Protocols: Percent Compression Out
This monitor returns the compression ratio for bytes being transmitted.

All Protocols: Serial Overrun Errors
This monitor returns the total number of Serial Overrun Errors for this connection. Serial Overrun Errors occur when the hardware cannot handle the rate at which data is received.

All Protocols: Timeout Errors
This monitor returns the total number of Timeout Errors for this connection. Timeout Errors occur when an expected is not received in time.

All Protocols: Total Errors/Sec
This monitor returns the total number of CRC, Timeout, Serial Overrun, Alignment, and Buffer...
Overrun Errors per second.

**RAS Port: Alignment Errors**

This monitor returns the total number of Alignment Errors for this connection. Alignment Errors occur when a byte received is different from the byte expected.

- This component has Count statistic as difference enabled. It will return the difference between two polling intervals.
- By default, this monitor is disabled.
- The instance field is installation-specific. You need to specify RRAS protocol (for example: VPN0-0). You can see all available instances in perfmon by looking counters in “RAS Port” object.

**RAS Port: Buffer Overrun Errors**

This monitor returns the total number of Buffer Overrun Errors for this connection. Buffer Overrun Errors occur when the software cannot handle the rate at which data is received.

- This component has Count statistic as difference enabled. It will return the difference between two polling intervals.
- By default, this monitor is disabled.
- The instance field is installation-specific. You need to specify RRAS protocol (for example: VPN0-0). You can see all available instances in perfmon by looking counters in “RAS Port” object.

**RAS Port: Bytes Received/Sec**

This monitor returns the number of bytes received per second.

- By default, this monitor is disabled.
- The instance field is installation-specific. You need to specify RRAS protocol (for example: VPN0-0). You can see all available instances in perfmon by looking counters in “RAS Port” object.

**RAS Port: Bytes Transmitted/Sec**

This monitor returns the number of bytes transmitted per second.

- By default, this monitor is disabled.
- The instance field is installation-specific. You need to specify RRAS protocol (for example: VPN0-0). You can see all available instances in perfmon by looking counters in “RAS Port” object.

**RAS Port: CRC Errors**

This monitor returns the total number of CRC Errors for this connection. CRC Errors occur when the frame received contains erroneous data.

- This component has Count statistic as difference enabled. It will return the difference between two polling intervals.
- By default, this monitor is disabled.
The instance field is installation-specific. You need to specify RRAS protocol (for example: VPN0-0). You can see all available instances in perfmon by looking counters in “RAS Port” object.

**RAS Port: Percent Compression In**

This monitor returns the compression ratio for bytes being received.

- By default, this monitor is disabled.
- The instance field is installation-specific. You need to specify RRAS protocol (for example: VPN0-0). You can see all available instances in perfmon by looking counters in “RAS Port” object.

**RAS Port: Percent Compression Out**

This monitor returns the compression ratio for bytes being transmitted.

- By default, this monitor is disabled.
- The instance field is installation-specific. You need to specify RRAS protocol (for example: VPN0-0). You can see all available instances in perfmon by looking counters in “RAS Port” object.

**RAS Port: Serial Overrun Errors**

This monitor returns the total number of Serial Overrun Errors for this connection. Serial Overrun Errors occur when the hardware cannot handle the rate at which data is received.

- This component has Count statistic as difference enabled. It will return the difference between two polling intervals.
- By default, this monitor is disabled.
- The instance field is installation-specific. You need to specify RRAS protocol (for example: VPN0-0). You can see all available instances in perfmon by looking counters in “RAS Port” object.

**RAS Port: Timeout Errors**

This monitor returns the total number of Timeout Errors for this connection. Timeout Errors occur when an expected is not received in time.

- This component has Count statistic as difference enabled. It will return the difference between two polling intervals.
- By default, this monitor is disabled.
- The instance field is installation-specific. You need to specify RRAS protocol (for example: VPN0-0). You can see all available instances in perfmon by looking counters in “RAS Port” object.

**RAS Port: Total Errors/Sec**

This monitor returns the total number of CRC, Timeout, Serial Overrun, Alignment, and Buffer Overrun Errors per second.
- By default, this monitor is disabled.
- The instance field is installation-specific. You need to specify RRAS protocol (for example: VPN0-0). You can see all available instances in perfmon by looking counters in “RAS Port” object.

Microsoft Routing and Remote Access 2016 (Events)

This template assesses the status and overall performance of a Microsoft Routing and Remote Access on Windows 2016 by checking specific events.

Prerequisites>

WMI access to the target server.

Credentials

Windows Administrator on the target server.

Monitored Components

For details on monitors, see [SAM Component Monitor Types](#).

**Warning and Errors: Remote Access**

This monitor returns warning and error events of the Routing and Remote Access connections.

**Source Name:** RemoteAccess.

**Log File:** Application.

**Warning and Errors: Secure Socket Tunneling Protocol**

This monitor returns warning and error events of Secure Socket Tunneling Protocol (SSTP).

**Source Name:** RasSstp.

**Log File:** Application.

**Warning and Errors: RAS Client**

This monitor returns warning and error events of the Routing and Remote Access clients.

**Source Name:** RasClient.

**Log File:** Application.

**Warning and Errors: RAS Connection Manager Service**

This monitor returns warning and error events of the Routing and Remote Access Manager service.

**Source Name:** RasMan.

**Log File:** Application.

**Warning and Errors: DHCPv6**

This monitor returns warning and error events of the DHCPv6 Relay Agent.
Source Name: RasRoutingProtocols-dhcpv6r.
Log File: Application.

Warning and Errors: IGMPv2
This monitor returns warning and error events of the Internet Group Management Protocol (IGMP).

Source Name: RasRoutingProtocols-IGMPv2.
Log File: Application.

Warning and Errors: RIP
This monitor returns warning and error events of the Router Information Protocol (RIP).

Source Name: RasRoutingProtocols-IPRIP2.
Log File: Application.

Warning and Errors: BOOTP Relay Agent
This monitor returns warning and error events of the Bootstrap Protocol (BOOTP) relay agent.

Source Name: RasIpBootp.
Log File: Application.

Warning and Errors: RAS Server
This monitor returns warning and error events of the Routing and Remote Access service.

Source Name: RasServer.
Log File: Application.
Microsoft SharePoint

The following templates are available:

- [Microsoft SharePoint Server 2016](#)
- [SharePoint Server (MOSS) 2007](#)
- [SharePoint Server 2010](#)
- [SharePoint Server 2013](#)
- [SharePoint Services (WSS) 3.0](#)
- [SharePoint Services (WSS) 6.0](#)

> Periodically, SolarWinds releases SAM templates to support the latest product versions such as Microsoft Server 2016. You can continue using templates for older product versions, but updating to the latest template is recommended.

Microsoft SharePoint Server 2016

This template assesses the overall health and performance of Microsoft Office SharePoint Server 2016.

Prerequisites

WMI access to the SharePoint server.

Credentials

Windows Administrator on the SharePoint server.


Monitored Components

> For details on monitors, see [SAM Component Monitor Types](#).

Components without predetermined threshold values provide guidance such as "Use the lowest threshold possible" or "Use the highest threshold possible" to help you find a threshold appropriate for your application.

Service: SharePoint Search Host Controller

This monitor returns CPU and memory usage of the SharePoint Search Host Controller service. This service performs host deployment and management for SharePoint search components.
Service: SharePoint Server Search 15

This monitor returns CPU and memory usage of the SharePoint Server Search 15 service. This service administers and crawls content from repositories.

Service: SharePoint Timer Service

This monitor returns CPU and memory usage of the SharePoint Timer service. This service sends notifications and performs scheduled tasks for SharePoint.

Service: SharePoint Tracing Service

This monitor returns CPU and memory usage of the SharePoint Tracing service. This service manages trace output.

Service: SharePoint User Code Host

This monitor returns CPU and memory usage of the SharePoint User Code Host service. This service executes user code in a sandbox.

Service: Document Conversions Launcher

This monitor returns CPU and memory usage of the Document Conversions Launcher service. This service schedules and initiates document conversions. When SharePoint Foundation passes a document conversion request to the document conversion launcher service, the service must call the appropriate document converter.

Service: Document Conversions Load Balancer

This monitor returns CPU and memory usage of the Document Conversions Load Balancer service. This service balances the document conversion requests from across the server farm. When it receives a converter request from SharePoint Foundation, the document conversion load balancer service must return a URI to the appropriate document conversion launcher service. SharePoint Foundation connects to the specified launcher via .NET remotely and requests the specified document be converted.

Current Requests

This component monitor returns the current number of requests, including those that are queued, currently executing, or waiting to be written to the client. Under the ASP.NET process model, when this counter exceeds the requestQueueLimit defined in the processModel configuration section, ASP.NET will begin rejecting requests.

Request Wait Time

This component monitor returns the time, in milliseconds, that the most recent request waited for processing. As the number of wait events increases, you may experience degraded page-rendering performance. This number should be as low as possible. If this value consistently grows, you should think about implementing additional web servers.
Requests Queued

This component monitor returns the number of requests waiting to be processed. SharePoint Foundation 2013 provides the building blocks for HTML pages that are rendered in the user browser over HTTP. This component monitor returns the number of requests waiting to be processed. If this counter shows hundreds or thousands of requests queued, you should implement additional web servers. The default maximum for this counter is 5,000. You can change this setting in the configuration file. This number should be as low as possible.

Requests Rejected

This component monitor returns the total number of requests not executed because of insufficient server resources. This represents the number of requests that return a 503 HTTP status code, indicating that the server is too busy. This value should be zero. If this value consistently grows, you should think about implementing additional web servers.

Worker Process Restarts

This component monitor returns the number of times a worker process has restarted. Restarts use a great deal of resources and therefore should be monitored closely. Restarts can be caused by various process settings, memory leaks, and access violations. It is recommended to closely monitor restarts to determine their cause, thus preventing them from occurring in the future. Any returned number above zero may indicate a problem.

Requests/Sec

This component monitor returns the number of requests executed per second. This represents the current throughput of the application. Under constant load, this number should remain within a certain range, barring other server work (such as garbage collection, cache cleanup thread, external server tools, and so on).

Cache API Trims

This component monitor returns the number of cache items that have been removed due to a memory limit being hit, (i.e. they were trimmed). Ideally, this number should be very low or zero. Too many trims may indicate that you need to revisit your caching strategy or manually configure your cache memory limits.

Cache API Hit Ratio

This component monitor returns the cache hit-to-miss ratio when accessed through the external cache APIs. This counter does not track any use of the cache internally by ASP.NET. For read-only sites, the ratio should be 1. For read-write sites, the ratio may be lower.

Potential causes of a low hit ratio include the following:

- You are using anonymous user caching and users are regularly requesting content that has not yet been cached.
- You are using ASP.NET output caching for authenticated users and they have edit permissions on the pages they are viewing.
- You have customized any of the VaryBy* parameters on a page or customized a cache profile.
You may have configured a parameter that prevents the pages in the site from being cached effectively.

**Sql Query Executing time**

This component monitor returns an average executing time of Sql queries. Returning value should be as low as possible.

**Executing Sql Queries**

This component monitor returns the number of current executing Sql queries.

**Responded Page Requests Rate**

This component monitor returns the number of requests responded in last second.

**Executing Time/Page Request**

This component monitor returns an average executing time (in ms) for responded requests in last seconds.

**Current Page Requests**

This component monitor returns the number of current requests in processing.

**Rejected Page Requests Rate**

This component monitor returns the number of rejecting requests in last second. Returning value should be as low as possible.

**Incoming Page Requests Rate**

This component monitor returns the number of incoming requests in last second.

**Active Threads**

This component monitor returns the number of threads currently executing in SharePoint code.
SharePoint Server (MOSS) 2007

This template assess the overall health and performance of Microsoft Office SharePoint Server 2007.

Prerequisites

WMI access to SharePoint server.

Credentials

Windows Administrator on SharePoint server.

Monitored Components

Components without predetermined threshold values provide guidance such as "Use the lowest threshold possible" or "Use the highest threshold possible" to help you find a threshold appropriate for your application.

Document Conversions Launcher

This service schedules and initiates document conversions. When SharePoint Foundation passes a document conversion request to the document conversion launcher service, the service must call the appropriate document converter.

Document Conversions Load Balancer

This service balances the document conversion requests from across the server farm. When it receives a converter request from SharePoint Foundation, the document conversion load balancer service must return a URI to the appropriate document conversion launcher service. SharePoint Foundation connects to the specified launcher via .NET remotely and requests the specified document be converted.

Single Sign-on

This component monitor provides the storage and mapping of credentials such as account names and passwords so that portal-based applications can retrieve information from third-party Enterprise Resource Planning (ERP) and Customer Relations Management (CRM) systems.

SharePoint Server Search

This is a server farm-wide service that responds to query requests from front-end Web servers or crawl items.

ASP.NET: Requests/sec

This component monitors the number of requests executed per second. This represents the current throughput of the application. Under constant load, this number should remain within a certain range, barring other server work (such as garbage collection, cache cleanup thread, external server tools, and so on). This value should be as low as possible.
ASP.NET: Worker Processes Restarts

This component monitor returns the number of times a worker process has restarted. Restarts use a great deal of resources and therefore should be monitored closely. Restarts can be caused by various process settings, memory leaks, and access violations. It is recommended to closely monitor restarts to determine their cause, thus preventing them from occurring in the future. Any returned number above zero may indicate a problem.

Search Indexer: Queries

This component monitor returns the number of search queries.

Search Gatherer: Crawls In Progress

This component monitor returns the number of crawls in progress. Unless an administrator has manually initiated a crawl, the value should match the number of content sources with crawls scheduled.

Search Gatherer: Document Add Rate

This component monitor returns the number of items indexed per second, per content source.

Search Gatherer: Error Rate

This component monitor returns the number of index errors per second and should be as low as possible.

Search Gatherer: Incremental Crawls

This component monitor returns the number of incremental crawls in progress. An incremental crawl indexes only items that have changed.

Search Gatherer: Processed Documents Rate

This component monitor returns the number of documents processed per second.

Search Gatherer: Retries

This component monitor returns the total number of times document access has been retried.

Search Gatherer: Waiting Documents

This component monitor returns the number of documents waiting to be processed.

Search Gatherer: Documents Filtered Rate

This component monitor returns the number of documents filtered per second.

Search Gatherer: Filtering Threads

This component monitor returns the number of threads that have retrieved content and are being filtered. If the number is high, it may indicate that resources on the index server are being bottlenecked. This number should be as low as possible.

Search Gatherer: Threads Accessing Network
This component monitor returns the number of threads in the gatherer process that have sent requests to a remote data store and are either waiting for a response or processing a response. High values returned may indicate either a network bottleneck or that slow hosts may be connected to the index server.

**Search Gatherer: Document Entries**

This component monitor returns the number of document entries currently in memory.
SharePoint Server 2010

This template assesses the overall health and performance of Microsoft SharePoint Server 2010.

**Prerequisites**

WMI access to SharePoint server.

**Credentials**

Windows Administrator on SharePoint server.

**Monitored Components**

Components without predetermined threshold values provide guidance such as "Use the lowest threshold possible" or "Use the highest threshold possible" to help you find a threshold appropriate for your application.

**Service: SharePoint 2010 Timer**

This component monitor sends notifications and performs scheduled tasks for SharePoint.

**Service: SharePoint 2010 Tracing**

This component monitor manages trace output.

**Service: SharePoint 2010 User Code Host**

This component monitor executes user code in a sandbox.

**Service: SharePoint Foundation Search V4**

This service provides full-text indexing and search to SharePoint user and help content.

**Service: SharePoint Server Search 14**

SharePoint Server Search 14 provides enhanced full-text indexing and search capabilities.

**Service: Document Conversions Launcher**

This component launches the Microsoft SharePoint Server 2010 Document Conversions Services. This service schedules and initiates document conversions. When SharePoint Foundation passes a document conversion request to the document conversion launcher service, the service must call the appropriate document converter.

**Service: Document Conversions Load Balancer**
This component launches the Microsoft SharePoint Server 2010 Document Conversions Services Load Balancer. This service balances the document conversion requests from across the server farm. When it receives a converter request from SharePoint Foundation, the document conversion load balancer service must return a URI to the appropriate document conversion launcher service. SharePoint Foundation connects to the specified launcher via .NET remotely and requests the specified document be converted.

**Cache API Trims**

This component monitor returns the number of cache items that have been removed due to a memory limit being hit, (i.e. they were trimmed). Ideally, this number should be very low or zero. Too many trims may indicate that you need to revisit your caching strategy or manually configure your cache memory limits.

**Cache API Hit Ratio**

This component monitor returns the cache hit-to-miss ratio when accessed through the external cache APIs. This counter does not track any use of the cache internally by ASP.NET. For read-only sites, the ratio should be 1. For read-write sites, the ratio may be lower.

Potential causes of a low hit ratio include the following:

- You are using anonymous user caching and users are regularly requesting content that has not yet been cached.
- You are using ASP.NET output caching for authenticated users and they have edit permissions on the pages they are viewing.
- You have customized any of the VaryBy* parameters on a page or customized a cache profile.
- You may have configured a parameter that prevents the pages in the site from being cached effectively.

**Requests Queued**

SharePoint Foundation 2010 provides the building blocks for HTML pages that are rendered in the user browser over HTTP. This component monitor returns the number of requests waiting to be processed. If this counter shows hundreds or thousands of requests queued, you should implement additional web servers. The default maximum for this counter is 5,000. You can change this setting in the configuration file. This number should be as low as possible.

**Request Wait Time**

This component monitor returns the time, in milliseconds, that the most recent request waited for processing. As the number of wait events increases, you may experience degraded page-rendering performance. This number should be as low as possible. If this value consistently grows, you should think about implementing additional web servers.

**Requests Rejected**

This component monitor returns the total number of requests not executed because of insufficient server resources. This represents the number of requests that return a 503 HTTP status code, indicating that the server is too busy. This value should be zero. If this value consistently grows, you should think about implementing additional web servers.
Worker Process Restarts

This component monitor returns the number of times a worker process has restarted. Restarts use a great deal of resources and therefore should be monitored closely. Restarts can be caused by various process settings, memory leaks, and access violations. It is recommended to closely monitor restarts to determine their cause, thus preventing them from occurring in the future. Any returned number above zero may indicate a problem.

Requests/Sec

This component monitor returns the number of requests executed per second. This represents the current throughput of the application. Under constant load, this number should remain within a certain range, barring other server work (such as garbage collection, cache cleanup).
SharePoint Server 2013

This template assesses the overall health and performance of Microsoft Office SharePoint Server 2013.

Prerequisites

- WMI access to the SharePoint server.

Credentials

- Windows Administrator on the SharePoint server.


Monitored Components

For details on monitors, see [SAM Component Monitor Types.](#)

Components without predetermined threshold values provide guidance such as "Use the lowest threshold possible" or "Use the highest threshold possible" to help you find a threshold appropriate for your application.

Service: SharePoint Search Host Controller

This monitor returns CPU and memory usage of the SharePoint Search Host Controller service. This service performs host deployment and management for SharePoint search components.

Service: SharePoint Server Search 15

This monitor returns CPU and memory usage of the SharePoint Server Search 15 service. This service administers and crawls content from repositories.

Service: SharePoint Timer Service

This monitor returns CPU and memory usage of the SharePoint Timer service. This service sends notifications and performs scheduled tasks for SharePoint.

Service: SharePoint Tracing Service

This monitor returns CPU and memory usage of the SharePoint Tracing service. This service manages trace output.

Service: SharePoint User Code Host

This monitor returns CPU and memory usage of the SharePoint User Code Host service. This service executes user code in a sandbox.
Service: Document Conversions Launcher

This monitor returns CPU and memory usage of the Document Conversions Launcher service. This service schedules and initiates document conversions. When SharePoint Foundation passes a document conversion request to the document conversion launcher service, the service must call the appropriate document converter.

Service: Document Conversions Load Balancer

This monitor returns CPU and memory usage of the Document Conversions Load Balancer service. This service balances the document conversion requests from across the server farm. When it receives a converter request from SharePoint Foundation, the document conversion load balancer service must return a URI to the appropriate document conversion launcher service. SharePoint Foundation connects to the specified launcher via .NET remotely and requests the specified document be converted.

Current Requests

This component monitor returns the current number of requests, including those that are queued, currently executing, or waiting to be written to the client. Under the ASP.NET process model, when this counter exceeds the requestQueueLimit defined in the processModel configuration section, ASP.NET will begin rejecting requests.

Request Wait Time

This component monitor returns the time, in milliseconds, that the most recent request waited for processing. As the number of wait events increases, you may experience degraded page-rendering performance. This number should be as low as possible. If this value consistently grows, you should think about implementing additional web servers.

Requests Queued

This component monitor returns the number of requests waiting to be processed. SharePoint Foundation 2013 provides the building blocks for HTML pages that are rendered in the user browser over HTTP. This component monitor returns the number of requests waiting to be processed. If this counter shows hundreds or thousands of requests queued, you should implement additional web servers. The default maximum for this counter is 5,000. You can change this setting in the configuration file. This number should be as low as possible.

Requests Rejected

This component monitor returns the total number of requests not executed because of insufficient server resources. This represents the number of requests that return a 503 HTTP status code, indicating that the server is too busy. This value should be zero. If this value consistently grows, you should think about implementing additional web servers.
Worker Process Restarts

This component monitor returns the number of times a worker process has restarted. Restarts use a great deal of resources and therefore should be monitored closely. Restarts can be caused by various process settings, memory leaks, and access violations. It is recommended to closely monitor restarts to determine their cause, thus preventing them from occurring in the future. Any returned number above zero may indicate a problem.

Requests/Sec

This component monitor returns the number of requests executed per second. This represents the current throughput of the application. Under constant load, this number should remain within a certain range, barring other server work (such as garbage collection, cache cleanup thread, external server tools, and so on).

Cache API Trims

This component monitor returns the number of cache items that have been removed due to a memory limit being hit, (i.e. they were trimmed). Ideally, this number should be very low or zero. Too many trims may indicate that you need to revisit your caching strategy or manually configure your cache memory limits.

Cache API Hit Ratio

This component monitor returns the cache hit-to-miss ratio when accessed through the external cache APIs. This counter does not track any use of the cache internally by ASP.NET. For read-only sites, the ratio should be 1. For read-write sites, the ratio may be lower.

Potential causes of a low hit ratio include the following:

- You are using anonymous user caching and users are regularly requesting content that has not yet been cached.
- You are using ASP.NET output caching for authenticated users and they have edit permissions on the pages they are viewing.
- You have customized any of the VaryBy* parameters on a page or customized a cache profile.
- You may have configured a parameter that prevents the pages in the site from being cached effectively.

Sql Query Executing time

This component monitor returns an average executing time of Sql queries. Returning value should be as low as possible.

Executing Sql Queries

This component monitor returns the number of current executing Sql queries.

Responded Page Requests Rate

This component monitor returns the number of requests responded in last second.
Executing Time/Page Request

This component monitor returns an average executing time (in ms) for responded requests in last seconds.

Current Page Requests

This component monitor returns the number of current requests in processing.

Rejected Page Requests Rate

This component monitor returns the number of rejecting requests in last second. Returning value should be as low as possible.

Incoming Page Requests Rate

This component monitor returns the number of incoming requests in last second.

Active Threads

This component monitor returns the number of threads currently executing in SharePoint code.
SharePoint Services (WSS) 3.0

This template assess the overall health and performance of Windows SharePoint Services 3.0.

**Prerequisites**

- WMI access to SharePoint server.

**Credentials**

\Windows Administrator on SharePoint server.

**Monitored Components**

Components without predetermined threshold values provide guidance such as "Use the lowest threshold possible" or "Use the highest threshold possible" to help you find a threshold appropriate for your application.

**Internet Information Services**

This component monitors only the service that provides Web connectivity through the Internet Information Services Manager.

**SharePoint Services Search**

This service provides support for constructing complex search queries through the SQL syntax. search in Windows SharePoint Services.

**SharePoint Services Timer**

This component monitor sends notifications and performs scheduled tasks for SharePoint.

**SharePoint Services Tracing**

This component monitor manages the trace output of the call stack. Administrators can specify the path used to store the trace log files. This log file may be used by applications that are built on top of Windows SharePoint Services 3.0.

**ISAPI Connection Count**

This component monitor returns the current number of extension requests that are simultaneously being processed by the web service.

**ISAPI Request/Sec**

This component monitor returns the rate at which ISAPI extension requests are simultaneously being processed by the web service.

**ASP.NET Worker Process Restarts**

This component monitor returns the number of times a worker process has restarted. Restarts use a great deal of resources and therefore should be monitored closely. Restarts can be caused by various process settings, memory leaks, and access violations. It is recommended to
closely monitor restarts to determine their cause, thus preventing them from occurring in the future. Any returned number above zero may indicate a problem.

**SharePoint Services (WSS) 6.0**

This template assess the overall health and performance of Windows SharePoint Services 6.0.

**Prerequisites**

WMI access to SharePoint server.

**Credentials**

\Windows Administrator on SharePoint server.

**Monitored Components**

Components without predetermined threshold values provide guidance such as "Use the lowest threshold possible" or "Use the highest threshold possible" to help you find a threshold appropriate for your application.

**Internet Information Services**

This component monitors only the service that provides Web connectivity through the Internet Information Services Manager.

**SharePoint Services Search 16**

This service provides support for constructing complex search queries through the SQL syntax. search in Windows SharePoint Services.

**SharePoint Services Timer**

This component monitor sends notifications and performs scheduled tasks for SharePoint.

**SharePoint Services Tracing**

This component monitor manages the trace output of the call stack. Administrators can specify the path used to store the trace log files. This log file may be used by applications that are built on top of Windows SharePoint Services 3.0.

**ISAPI Connection Count**

This component monitor returns the current number of extension requests that are simultaneously being processed by the web service.

**ISAPI Request/Sec**

This component monitor returns the rate at which ISAPI extension requests are simultaneously being processed by the web service.

**ASP.NET Worker Process Restarts**

This component monitor returns the number of times a worker process has restarted. Restarts
use a great deal of resources and therefore should be monitored closely. Restarts can be caused by various process settings, memory leaks, and access violations. It is recommended to closely monitor restarts to determine their cause, thus preventing them from occurring in the future. Any returned number above zero may indicate a problem.
Microsoft Skype for Business templates

The following templates are available:

- Skype for Business Server 2015 (Edge Role)
- Skype for Business Server 2015 (Front-End Role)
- Skype for Business Server 2015 (Mediation Role)

Periodically, SolarWinds releases SAM templates to support the latest product versions such as Microsoft Server 2016. You can continue using templates for older product versions, but updating to the latest template is recommended.

Skype for Business Server 2015 (Edge Role)

This template assesses the status and overall health of services as well as the performance of the Microsoft Skype for Business Server (Edge Role) 2015.

Prerequisites

WMI access to the SharePoint server.

Credentials

Windows Administrator on the SharePoint server.

Set thresholds for these counters according to your environment. SolarWinds recommends monitoring counters for some period of time to understand potential value ranges and then set the thresholds accordingly.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Components without predetermined threshold values provide guidance such as "Use the lowest threshold possible" or "Use the highest threshold possible" to help you find a threshold appropriate for your application.

Skype for Business Server Replica Replicator Agent

This component monitor returns the CPU and memory usage of the Skype for Business Server Replica Replicator Agent. This service is used by the File Transfer Agent for replication configuration settings.

SIP - Incoming Requests /Sec

This component monitor returns the rate of received requests, per second. You will need to baseline this counter by testing and monitoring the user load.
**SIP - Incoming Messages /Sec**

This component monitor returns the rate of received messages, per second. You will need to baseline this counter by testing and monitoring the user load.

**SIP Peers: Connections Active**

This component monitor returns the number of established connections that are currently active. A connection is considered established when peer credentials are verified (e.g. via MTLS), or the peer receives a 2xx response. You will need to baseline this counter by testing and monitoring the user load. This returned value should be less than 15,000 connections per Front-End.

**SIP Peers: Average Outgoing Queue Delay**

This component monitor returns the average time, in seconds, that messages have been delayed in outgoing queues. Check the Outgoing Queue Delay for delays in sending messages to other servers or clients that could be causing messages to be accumulated in the server. The server will drop client connections if it is in a throttle state and messages stay in the outgoing queue for more than 32 seconds.

**SIP Peers: Connections Active**

This component monitor returns the average time that the server held the incoming messages currently being processed. This should usually be less than one second, on average, but it is normal to see short spikes of up to three seconds. The server will throttle new incoming messages after going above the high benchmark and until the number of messages falls below the low benchmark. The server starts rejecting new connections when the average holding time is greater than overload time of 15 seconds.

---

This template also includes multiple A/V Edge UDP component monitors. For details, edit the template and expand each monitor to display its description.

---

**Skype for Business Server 2015 (Front-End Role)**

This template assesses the status and overall health of services as well as the performance of the Microsoft Skype for Business Server (Front-End Role) 2015.

**Prerequisites**

WMI access to the SharePoint server.

**Credentials**

Windows Administrator on the SharePoint server.

---

Set thresholds for these counters according to your environment. SolarWinds recommends monitoring counters for some period of time to understand potential value ranges and then set the thresholds accordingly.
Monitored Components

For details on monitors, see [SAM Component Monitor Types](#).

Components without predetermined threshold values provide guidance such as "Use the lowest threshold possible" or "Use the highest threshold possible" to help you find a threshold appropriate for your application.

This template includes multiple component monitors. For details, edit the template and expand each monitor to display its description.

---

**Skype for Business Server 2015 (Mediation Role)**

This template assesses the status and overall health of services as well as the performance of the Microsoft Skype for Business Server (Mediation Role) 2015.

**Prerequisites**

- WMI access to the SharePoint server.

**Credentials**

- Windows Administrator on the SharePoint server.

Set thresholds for these counters according to your environment. SolarWinds recommends monitoring counters for some period of time to understand potential value ranges and then set the thresholds accordingly.
Components without predetermined threshold values provide guidance such as "Use the lowest threshold possible" or "Use the highest threshold possible" to help you find a threshold appropriate for your application.

This template includes multiple component monitors. For details, edit the template and expand each monitor to display its description.

<table>
<thead>
<tr>
<th>Component Monitor Name</th>
<th>Component Type</th>
<th>Test Node</th>
<th>Monitoring Status</th>
<th>Order</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skype for Business Server Mediation</td>
<td>Windows Service Monitor</td>
<td>Test node not specified</td>
<td>Enabled</td>
<td>2</td>
</tr>
<tr>
<td>Skype for Business Server Replica</td>
<td>Windows Service Monitor</td>
<td>Test node not specified</td>
<td>Enabled</td>
<td>2</td>
</tr>
<tr>
<td>Outbound Calls: Current</td>
<td>Performance Counter Monitor</td>
<td>Test node not specified</td>
<td>Enabled</td>
<td>2</td>
</tr>
<tr>
<td>Outbound Calls: Active media bypass calls</td>
<td>Performance Counter Monitor</td>
<td>Test node not specified</td>
<td>Enabled</td>
<td>2</td>
</tr>
<tr>
<td>Inbound Calls: Current</td>
<td>Performance Counter Monitor</td>
<td>Test node not specified</td>
<td>Enabled</td>
<td>2</td>
</tr>
<tr>
<td>Inbound Calls: Active media bypass calls</td>
<td>Performance Counter Monitor</td>
<td>Test node not specified</td>
<td>Enabled</td>
<td>2</td>
</tr>
<tr>
<td>Media Relay: Media Connectivity Check Fail...</td>
<td>Performance Counter Monitor</td>
<td>Test node not specified</td>
<td>Enabled</td>
<td>2</td>
</tr>
<tr>
<td>Health Indices: Load Cell Failure Index</td>
<td>Performance Counter Monitor</td>
<td>Test node not specified</td>
<td>Enabled</td>
<td>2</td>
</tr>
<tr>
<td>Global Count: Current audio channels with...</td>
<td>Performance Counter Monitor</td>
<td>Test node not specified</td>
<td>Enabled</td>
<td>2</td>
</tr>
<tr>
<td>Total failed calls caused by unexpected inte...</td>
<td>Performance Counter Monitor</td>
<td>Test node not specified</td>
<td>Enabled</td>
<td>2</td>
</tr>
<tr>
<td>Total failed calls caused by unexpected inte...</td>
<td>Performance Counter Monitor</td>
<td>Test node not specified</td>
<td>Enabled</td>
<td>2</td>
</tr>
</tbody>
</table>
Microsoft SQL Server

The following templates are available:

- SQL Server 2005 Analysis Services
- SQL Server 2008 Analysis Services
- SQL Server 2008 Reporting Services
- SQL Server 2008 Reporting Services R2
- SQL Server 2008-2012 Reporting Services (Events)
- SQL Server 2012 Analysis Services
- SQL Server 2012 Reporting Services

See also ApplInsight for SQL.

SQL Server 2005 Analysis Services

This template uses Windows performance counters to assess the status and performance of Microsoft SQL Server 2005 Analysis Services.

Prerequisites: WMI access to the target server.

Credentials: Windows Administrator on the target server.

Monitored Components:

**Service: SQL Server Analysis Services**

This monitor returns CPU and memory usage of SQL Server Analysis Services. This service supplies online analytical processing (OLAP) and data mining functionality for business intelligence applications.

**Cache: Direct hits/sec**

This monitor returns the rate of cache direct hits. Queries were answered from an existing cache entry.

**Cache: Lookups/sec**

This monitor returns the rate of cache lookups.

**Cache: Direct hit ratio**

This monitor returns the ratio of cache direct hits to cache lookups, for the period between obtaining counter values.

**Cache: Current entries**

This monitor returns the current number of cache entries.
Cache: Current KB
This monitor returns the current memory used by the aggregation cache, in KB.

Cache: Inserts/sec
This monitor returns the rate of insertions into the cache. This is per partition per cube per database.

Cache: Evictions/sec
This monitor returns the rate of evictions from the cache. This is per partition per cube per database. Typically due to background cleaner.

Cache: Misses/sec
This monitor returns the rate of cache misses.

Connection: Current connections
This monitor returns the current number of client connections established.

Connection: Current user sessions
This monitor returns the current number of user sessions established. A connection is always tied to a session, but there could be sessions without active user connections.

Connection: Requests/sec
This monitor returns the rate of connection requests (arrivals).

Connection: Failures/sec
This monitor returns the rate of connection failures.

Connection: Successes/sec
This monitor returns the rate of successful connection completions.

Data Mining Prediction: Queries/sec
This monitor returns the rate of Data Mining queries.

Data Mining Prediction: Predictions/sec
This monitor returns the rate of Data Mining prediction queries.

Locks: Current latch waits
This monitor returns the current number of threads waiting for a latch. These are latch requests that could not be given immediate grants and are in a wait state.

Locks: Current lock waits
This monitor returns the current number of clients waiting for a lock.

Locks: Current locks
This monitor returns the current number of locked objects.
Locks: Lock waits/sec

This monitor returns the number of lock waits per second. These are lock requests that could not be given immediate lock grants and were put in a wait state.

Locks: Total deadlocks detected

This monitor returns the total number of deadlocks detected.

Note: This counter has the Count statistic as difference option enabled and will show the statistical difference from the last polling cycle.

MDX: Total NON EMPTY unoptimized

This monitor returns the total number of times unoptimized a non empty algorithm is used. Total non empty un-optimized is the number of Calculate Non Empty operations that are using an un-optimized algorithm. If this number continues to grow, there may be MDX queries that are running slowly for this reason and we might want to find them and optimize them.

Note: This counter has the Count statistic as difference option enabled and will show the statistical difference from the last polling cycle.

MDX: Total recomputes

This monitor returns the total number of cells recomputed due to error.

Note: This counter has the Count statistic as difference option enabled and will show the statistical difference from the last polling cycle.

MDX: Total Sonar subcubes

This monitor returns the total number of subcubes that query optimizer generated.

Note: This counter has the Count statistic as difference option enabled and will show the statistical difference from the last polling cycle.

Memory: Cleaner Memory shrinkable KB

This monitor returns the amount of memory, in KB, subject to purging by the background cleaner.

Memory: Cleaner Memory nonshrinkable KB

This monitor returns the amount of memory, in KB, not subject to purging by the background cleaner.

Memory: Cleaner Memory KB

This monitor returns the amount of memory, in KB, known to the background cleaner. (Cleaner memory shrinkable + Cleaner memory nonshrinkable.) Note that this counter is calculated from internal accounting information so there may be some small deviation from the memory reported by the operating system.
Memory: Cleaner Balance/sec
This monitor returns the rate of balance+shrink operations. Shows how many times the current memory usage is compared against the settings. Memory usage is checked every 500ms, so the counter will trend towards 2 with slight deviations when the system is under high stress. Preferred Value 2

Memory: Filestore KB
This monitor returns the current memory allocated to filestore (file cache), in KB.

Memory: Filestore Writes/sec
This monitor returns the rate of filestore written pages (asynchronous writes).

Memory: Filestore IO Errors/sec
This monitor returns the rate of filestore IO Errors.

Memory: Quota Blocked
This monitor returns the current number of quota requests that are blocked until other memory quotas are freed.

Memory: Filestore Reads/sec
This monitor returns the filestore pages read/sec.

Proactive Caching: Notifications/sec
This monitor returns the rate of notifications from relational database.

Proactive Caching: Processing Cancellations/sec
This monitor returns the rate of processing cancellations caused by notifications.

Proc Aggregations: Temp file bytes written/sec
This monitor returns the rate of writing bytes to a temporary file. Temporary files are written when aggregations exceed memory limits.

Processing: Rows read/sec
This monitor returns the rate of rows read from all relational databases.

Processing: Rows written/sec
This monitor returns the rate of rows written during processing.

Storage Engine Query: Queries from cache direct/sec
This monitor returns the rate of queries answered from cache directly.

Storage Engine Query: Queries from cache filtered/sec
This monitor returns the rate of queries answered by filtering existing cache entry.

Storage Engine Query: Queries from file/sec
This monitor returns the rate of queries answered from files.
Storage Engine Query: Avg time/query

This monitor returns the average time per query, in milliseconds. Response time based on queries answered since the last counter measurement.

Storage Engine Query: Measure group queries/sec

This monitor returns the rate of measure group queries

Storage Engine Query: Dimension queries/sec

This monitor returns the rate of dimension queries

Threads: Processing pool idle threads

This monitor returns the number of idle threads in the processing thread pool.

Threads: Processing pool busy threads

This monitor returns the number of busy threads in the processing thread pool.

Threads: Processing pool job queue length

This monitor returns the number of jobs in the queue of the processing thread pool.

Threads: Processing pool job rate

This monitor returns the rate of jobs through the processing thread pool.
SQL Server 2008 Analysis Services

This template uses Windows performance counters to assess the status and performance of Microsoft SQL Server 2005 Analysis Services.

Prerequisites

WMI access to the target server.

Credentials

Windows Administrator on the target server.

Monitored Components

For details on monitors, see [SAM Component Monitor Types](#).

Service: SQL Server Analysis Services

This monitor returns CPU and memory usage of SQL Server Analysis Services. This service supplies online analytical processing (OLAP) and data mining functionality for business intelligence applications.

Cache: Direct hits/sec

This monitor returns the rate of cache direct hits. Queries were answered from an existing cache entry.

Cache: Lookups/sec

This monitor returns the rate of cache lookups.

Cache: Direct hit ratio

This monitor returns the ratio of cache direct hits to cache lookups, for the period between obtaining counter values.

Cache: Current entries

This monitor returns the current number of cache entries.

Cache: Current KB

This monitor returns the current memory used by the aggregation cache, in KB.

Cache: Inserts/sec

This monitor returns the rate of insertions into the cache. This is per partition per cube per database.

Cache: Evictions/sec

This monitor returns the rate of evictions from the cache. This is per partition per cube per database. Typically due to background cleaner.
Cache: Misses/sec
This monitor returns the rate of cache misses.

Connection: Current connections
This monitor returns the current number of client connections established.

Connection: Current user sessions
This monitor returns the current number of user sessions established. A connection is always tied to a session, but there could be sessions without active user connections.

Connection: Requests/sec
This monitor returns the rate of connection requests (arrivals).

Connection: Failures/sec
This monitor returns the rate of connection failures.

Connection: Successes/sec
This monitor returns the rate of successful connection completions.

Data Mining Prediction: Queries/sec
This monitor returns the rate of Data Mining queries.

Data Mining Prediction: Predictions/sec
This monitor returns the rate of Data Mining prediction queries.

Locks: Current latch waits
This monitor returns the current number of threads waiting for a latch. These are latch requests that could not be given immediate grants and are in a wait state.

Locks: Current lock waits
This monitor returns the current number of clients waiting for a lock.

Locks: Current locks
This monitor returns the current number of locked objects.

Locks: Lock waits/sec
This monitor returns the number of lock waits per second. These are lock requests that could not be given immediate lock grants and were put in a wait state.

Locks: Total deadlocks detected
This monitor returns the total number of deadlocks detected.

ℹ️ This counter has the Count statistic as difference option enabled and will show the statistical difference from the last polling cycle.
MDX: Total NON EMPTY unoptimized

This monitor returns the total number of times unoptimized a non empty algorithm is used. Total non empty un-optimized is the number of Calculate Non Empty operations that are using an un-optimized algorithm. If this number continues to grow, there may be MDX queries that are running slowly for this reason and we might want to find them and optimize them.

This counter has the Count statistic as difference option enabled and will show the statistical difference from the last polling cycle.

MDX: Total recomputes

This monitor returns the total number of cells recomputed due to error

This counter has the Count statistic as difference option enabled and will show the statistical difference from the last polling cycle.

MDX: Total Sonar subcubes

This monitor returns the total number of subcubes that query optimizer generated

This counter has the Count statistic as difference option enabled and will show the statistical difference from the last polling cycle.

Memory: Cleaner Memory shrinkable KB

This monitor returns the amount of memory, in KB, subject to purging by the background cleaner.

Memory: Cleaner Memory nonshrinkable KB

This monitor returns the amount of memory, in KB, not subject to purging by the background cleaner.

Memory: Cleaner Memory KB

This monitor returns the amount of memory, in KB, known to the background cleaner. (Cleaner memory shrinkable + Cleaner memory nonshrinkable.) Note that this counter is calculated from internal accounting information so there may be some small deviation from the memory reported by the operating system.

Memory: Cleaner Balance/sec

This monitor returns the rate of balance+shrink operations. Shows how many times the current memory usage is compared against the settings. Memory usage is checked every 500ms, so the counter will trend towards 2 with slight deviations when the system is under high stress. Preferred Value 2

Memory: Filestore KB

This monitor returns the current memory allocated to filestore (file cache), in KB.

Memory: Filestore Writes/sec

This monitor returns the rate of filestore written pages (asynchronous writes).
Memory: Filestore IO Errors/sec
This monitor returns the rate of filestore IO Errors.

Memory: Quota Blocked
This monitor returns the current number of quota requests that are blocked until other memory quotas are freed.

Memory: Filestore Reads/sec
This monitor returns the filestore pages read/sec.

Proactive Caching: Notifications/sec
This monitor returns the rate of notifications from relational database.

Proactive Caching: Processing Cancellations/sec
This monitor returns the rate of processing cancellations caused by notifications.

Proc Aggregations: Temp file bytes written/sec
This monitor returns the rate of writing bytes to a temporary file. Temporary files are written when aggregations exceed memory limits.

Processing: Rows read/sec
This monitor returns the rate of rows read from all relational databases.

Processing: Rows written/sec
This monitor returns the rate of rows written during processing.

Storage Engine Query: Queries from cache direct/sec
This monitor returns the rate of queries answered from cache directly.

Storage Engine Query: Queries from cache filtered/sec
This monitor returns the rate of queries answered by filtering existing cache entry.

Storage Engine Query: Queries from file/sec
This monitor returns the rate of queries answered from files.

Storage Engine Query: Avg time/query
This monitor returns the average time per query, in milliseconds. Response time based on queries answered since the last counter measurement.

Storage Engine Query: Measure group queries/sec
This monitor returns the rate of measure group queries

Storage Engine Query: Dimension queries/sec
This monitor returns the rate of dimension queries
Threads: Processing pool idle threads
This monitor returns the number of idle threads in the processing thread pool.

Threads: Processing pool busy threads
This monitor returns the number of busy threads in the processing thread pool.

Threads: Processing pool job queue length
This monitor returns the number of jobs in the queue of the processing thread pool.

Threads: Processing pool job rate
This monitor returns the rate of jobs through the processing thread pool.

SQL Server 2008 Reporting Services
This template uses Windows performance counters to assess the status and performance of Microsoft SQL Server 2008 Reporting Services.

Prerequisites:
WMI access to the target server.

Credentials:
Windows Administrator on the target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

MSRS Windows Service: Active Sessions
This monitor returns number of active sessions. This counter provides a cumulative count of all browser sessions generated from report executions, whether they are still active or not. The counter is decremented as session records are removed. By default, sessions are removed after ten minutes of no activity.

MSRS Windows Service: Cache Flushes/Sec
This monitor returns number of cache flushes per second.

MSRS Windows Service: Cache Hits/Sec
This monitor returns number of requests per second for cached reports. These are requests for re-rendered reports, not requests for reports processed directly from the cache.

MSRS Windows Service: Cache Misses/Sec
This monitor returns the number of requests per second that failed to return a report from the cache. Use this counter to find out whether the resources used for caching (disk or memory)
are sufficient.

**MSRS Windows Service: Delivers/Sec**

This monitor returns the number of report deliveries, per second, from any delivery extension.

**MSRS Windows Service: Events/Sec**

This monitor returns the number of events processed per second. Events that are monitored include SnapshotUpdated and TimedSubscription.

**MSRS Windows Service: Memory Cache Hits/Sec**

This monitor returns the number of times per second that reports are retrieved from the in-memory cache. In-memory cache is a part of the cache that stores reports in CPU memory. When in-memory cache is used, the report server does not query SQL Server for cached content.

**MSRS Windows Service: Memory Cache Miss/Sec**

This monitor returns the number of times per second that reports could not be retrieved from the in-memory cache.

**MSRS Windows Service: Reports Executed/Sec**

This monitor returns the number of successful report executions per second. This counter provides statistics about report volume. Use this counter with Request/Sec to compare report execution to report requests that can be returned from cache.

**MSRS Windows Service: Total Processing Failures**

This monitor returns the number of errors in report server web service request processing.

**Note:** This counter has the Count statistic as difference option enabled and will show the statistical difference from the last polling cycle.

**MSRS Windows Service: Total Rejected Threads**

This monitor returns the total number of threads rejected for asynchronous processing, and subsequently handled as synchronous processes in the same thread. Each data source is processed on one thread. If the volume of threads exceeds capacity, threads are rejected for asynchronous processing, and are then processed in a serial manner.

**Note:** This counter has the Count statistic as difference option enabled and will show the statistical difference from the last polling cycle.

**Report Server: Active Connections**

This monitor returns the number of connections currently active on the server.

**Report Server: Bytes Received/sec**

This monitor returns the number of bytes received per second by the server. This counter is updated only when a transfer is complete. This means that the counter remains at 0 and then the value increases after a transfer is complete.

**Report Server: Bytes Sent/sec**
This monitor returns the number of bytes sent per second from the server. This counter is updated only when a transfer is complete. This means that the counter remains at 0 and then the value increases after a transfer is complete.

**Report Server: Errors/sec**

This monitor returns the total number of errors that occur per second during the processing of HTTP requests. These errors include HTTP status codes in the 400s and 500s.

**Report Server: Logon Attempts/sec**

This monitor returns the rate of logon attempts.

**Report Server: Logon Successes/sec**

This monitor returns the rate of successful logons.

**Report Server: Memory Pressure State**

This monitor returns the memory pressure state. One of the following numbers, from 1-5, which indicates the current memory state of the server:

1. No pressure
2. Low pressure
3. Medium pressure
4. High pressure
5. Exceeded pressure

**Report Server: Memory Shrink Amount**

This monitor returns the number of bytes that the server requested to shrink the memory in use.

**Report Server: Memory Shrink Notifications/sec**

This monitor returns the number of notifications that the server issued in the last second to shrink the memory in use. This value indicates how often the server experiences memory pressure.

**Report Server: Requests Executing**

This monitor returns the number of requests that are currently processing.

**Report Server: Requests/sec**

This monitor returns the number of requests that are processed per second. This value represents the current throughput of the application.

**Report Server: Tasks Queued**

This monitor returns the number of tasks that are waiting for a thread to become available for processing. Each request made to the report server corresponds to one or more tasks. This counter represents only the number of tasks that are ready for processing; it does not include
the number of tasks that are currently running.

**Service: SQL Server Reporting Services**

This monitor returns CPU and memory usage of SQL Server Reporting Services. This service manages, executes, renders, schedules and delivers reports.

**Report Server TCP Port**

This component monitor tests the ability of a Report Server to accept incoming sessions. By default, it monitors TCP port 80.

**SQL Server 2008 Reporting Services R2**

This template uses Windows performance counters to assess the status and performance of Microsoft SQL Server 2008 R2 Reporting Services.

**Prerequisites**

WMI access to the target server.

**Credentials**

Windows Administrator on the target server.

**Monitored Components**

For details on monitors, see [SAM Component Monitor Types](#).

**MSRS Windows Service: Active Sessions**

This monitor returns the number of active sessions. This counter provides a cumulative count of all browser sessions generated from report executions, whether they are still active or not. The counter is decremented as session records are removed. By default, sessions are removed after ten minutes of no activity.

**MSRS Windows Service: Cache Flushes/Sec**

This monitor returns the number of cache flushes per second.

**MSRS Windows Service: Cache Hits/Sec**

This monitor returns the number of requests per second for cached reports. These are requests for re-rendered reports, not requests for reports processed directly from the cache.

**MSRS Windows Service: Cache Hits/Sec (Semantic Models)**

This monitor returns the number of requests per second for cached models. These are requests for re-rendered reports, not requests for reports processed directly from the cache.

**MSRS Windows Service: Cache Misses/Sec**

This monitor returns the number of requests per second that failed to return a report from
Use this counter to find out whether the resources used for caching (disk or memory) are sufficient.

**MSRS Windows Service: Cache Misses/Sec (Semantic Models)**
This monitor returns the number of requests per second that failed to return a model from cache. Use this counter to find out whether the resources used for caching (disk or memory) are sufficient.

**MSRS Windows Service: Delivers/Sec**
This monitor returns the number of report deliveries per second, from any delivery extension.

**MSRS Windows Service: Events/Sec**
This monitor returns the number of events processed per second. Events that are monitored include SnapshotUpdated and TimedSubscription.

**MSRS Windows Service: Memory Cache Hits/Sec**
This monitor returns the number of times per second that reports are retrieved from the in-memory cache. In-memory cache is a part of the cache that stores reports in CPU memory. When in-memory cache is used, the report server does not query SQL Server for cached content.

**MSRS Windows Service: Memory Cache Miss/Sec**
This monitor returns the number of times per second that reports could not be retrieved from the in-memory cache.

**MSRS Windows Service: Reports Executed/Sec**
This monitor returns the number of successful report executions per second. This counter provides statistics about report volume. Use this counter with Request/Sec to compare report execution to report requests that can be returned from cache.

**MSRS Windows Service: Requests/Sec**
This monitor returns the number of requests per second made to the report server. This counter tracks all types of requests that are handled by the report server.

**MSRS Windows Service: Snapshot Updates/Sec**
This monitor returns the total number of report execution snapshot updates per second.

**MSRS Windows Service: Total Processing Failures**
This monitor returns the number of errors in report server web service request processing. 
*Note:* This counter has the Count statistic as difference option enabled and will show the statistical difference from the last polling cycle.

**MSRS Windows Service: Total Rejected Threads**
This monitor returns the total number of threads rejected for asynchronous processing, and subsequently handled as synchronous processes in the same thread. Each data source is processed on one thread. If the volume of threads exceeds capacity, threads are rejected for
asynchronous processing, and are then processed in a serial manner.  
**Note:** This counter has the Count statistic as difference option enabled and will show the statistical difference from the last polling cycle.

**Report Server: Active Connections**  
This monitor returns the number of connections currently active on the server.

**Report Server: Bytes Received/sec**  
This monitor returns the number of bytes received per second by the server. This counter is updated only when a transfer is complete. This means that the counter remains at 0 and then the value increases after a transfer is complete.

**Report Server: Bytes Sent/sec**  
This monitor returns the number of bytes sent per second from the server. This counter is updated only when a transfer is complete. This means that the counter remains at 0 and then the value increases after a transfer is complete.

**Report Server: Errors/sec**  
This monitor returns the total number of errors that occur per second during the processing of HTTP requests. These errors include HTTP status codes in the 400s and 500s.

**Report Server: Logon Attempts/sec**  
This monitor returns the rate of logon attempts.

**Report Server: Logon Successes/sec**  
This monitor returns the rate of successful logons.

**Report Server: Memory Pressure State**  
This monitor returns memory pressure state. One of the following numbers, from 1-5, which indicates the current memory state of the server:

1. No pressure  
2. Low pressure  
3. Medium pressure  
4. High pressure  
5. Exceeded pressure

**Report Server: Memory Shrink Amount**  
This monitor returns the number of bytes that the server requested to shrink the memory in use.

**Report Server: Memory Shrink Notifications/sec**  
This monitor returns the number of notifications that the server issued in the last second to shrink the memory in use. This value indicates how often the server experiences memory pressure.

**Report Server: Requests Executing**
This monitor returns the number of requests that are currently processing.

**Report Server: Requests/sec**
This monitor returns the number of requests that are processed per second. This value represents the current throughput of the application.

**Report Server: Tasks Queued**
This monitor returns the number of tasks that are waiting for a thread to become available for processing. Each request made to the report server corresponds to one or more tasks. This counter represents only the number of tasks that are ready for processing; it does not include the number of tasks that are currently running.

**Service: SQL Server Reporting Services**
This monitor returns CPU and memory usage of SQL Server Reporting Services. This service manages, executes, renders, schedules and delivers reports.

**Report Server TCP Port**
This component monitor tests the ability of a Report Server to accept incoming sessions. By default, it monitors TCP port 80.

---

**SQL Server 2008-2012 Reporting Services (Events)**
This template checks critical events of Microsoft SQL Server 2008-2012 Reporting Services.

**Prerequisites**
WMI access to the target server.

**Credentials**
Windows Administrator on the target server.

**Monitored Components**

<i> For details on monitors, see [SAM Component Monitor Types](#).</i>

**Scheduling: SQL Server Agent Must Be Running**
This monitor returns the following event: SQL Server Agent must be running when you define a scheduled operation (for example, report subscription and delivery).
Event ID: 106 (Application Log)

**No Connection to Report Server Database**
This monitor returns the following event: The SQL Server Report Server service cannot connect to the report server database. This error occurs during a service restart if a connection to the report server database cannot be established.
Start the Database Engine service if it is not running and check that remote connections are enabled for TCP/IP protocol. Use the Reporting Services Configuration tool to configure the report server database and service account.

Event ID: 107 (Application Log)

**Extensions Loading Error**

This monitor returns the following event: Report Server cannot load a delivery, data processing, or rendering extension. Most likely, this is the result of an incomplete deployment or removal of an extension.

Event ID: 108 (Application Log)

**Trace Log Creation Error**

This monitor returns the following event: Report Server cannot create the trace log.

Event ID: 111 (Application Log)

**Possible Denial of Service Attack**

This monitor returns the following event: The report server has detected a possible denial of service attack.

Event ID: 112 (Application Log)

**Performance Counters Creation Error**

This monitor returns the following event: The report server cannot create a performance counter.

Event ID: 113 (Application Log)

**No Connection to Report Manager**

This monitor returns the following event: Report Manager cannot connect to the Report Server service.

Event ID: 114 (Application Log)

**Internal Error**

This monitor returns the following event: An internal error occurred.

Event ID: 116 (Application Log)

**Database Invalid Version**

This monitor returns the following event: The report server database is an invalid version. For more information, see [http://technet.microsoft.com/en-us/library/ms156468(v=sql.100).aspx](http://technet.microsoft.com/en-us/library/ms156468(v=sql.100).aspx)

Event ID: 117 (Application Log)

**Access Denied to Server Database**

This monitor returns the following event: Report server has not been granted access to the
contents of the report server database.

Event ID: 119 (Application Log)

**Symmetric Key Cannot Be Decrypted**

This monitor returns the following event: The symmetric key cannot be decrypted. Most likely, there has been a change to the account that the service runs as.

Event ID: 120 (Application Log)

**RPC Failed to Start**

This monitor returns the following event: Remote Procedure Call (RPC) Service failed to start.

Event ID: 121 (Application Log)

**No Connection to SMTP Server**

This monitor returns the following event: Scheduling and Delivery Processor cannot connect to the SMTP server that is used for e-mail delivery.

Event ID: 122 (Application Log)

**Trace Log Writing Error**

This monitor returns the following event: The report server failed to write to the trace log.

Event ID: 123 (Application Log)

**Components Version Mismatch**

This monitor returns the following event: Reporting Services components from different editions cannot be used together.

Event ID: 128 (Application Log)

**Configuration Decryption Error**

This monitor returns the following event: An encrypted configuration file setting in cannot be decrypted.

Event ID: 129 (Application Log)

**Configuration File Not Found**

This monitor returns the following event: Report server cannot find the configuration file. Configuration files are required by the report server.

Event ID: 130 (Application Log)

**User Data Decryption Error**

This monitor returns the following event: An encrypted user data value could not be decrypted.

Event ID: 131 (Application Log)

**User Data Encryption Error**
This monitor returns the following event: A failure occurred during encryption of user data. The value cannot be saved.

Event ID: 132 (Application Log)

**Configuration File Loading Error**

This monitor returns the following event: A configuration file failed to load. This error may occur if the XML is not valid.

Event ID: 133 (Application Log)

**Configuration File Encryption Error**

This monitor returns the following event: The report server failed to encrypt values for a setting in a configuration file.

Event ID: 134 (Application Log)
SQL Server 2012 Analysis Services

This template uses Windows performance counters to assess the status and performance of Microsoft SQL Server 2012 Analysis Services.

Prerequisites

WMI access to the target server.

Credentials

Windows Administrator on the target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Service: SQL Server Analysis Services

This monitor returns CPU and memory usage of SQL Server Analysis Services. This service supplies online analytical processing (OLAP) and data mining functionality for business intelligence applications.

Cache: Direct hits/sec

This monitor returns the rate of cache direct hits. Queries were answered from an existing cache entry.

Cache: Lookups/sec

This monitor returns the rate of cache lookups.

Cache: Direct hit ratio

This monitor returns the ratio of cache direct hits to cache lookups, for the period between obtaining counter values.

Cache: Current entries

This monitor returns the current number of cache entries.

Cache: Current KB

This monitor returns the current memory used by the aggregation cache, in KB.

Cache: Inserts/sec

This monitor returns the rate of insertions into the cache. This is per partition per cube per database.

Cache: Evictions/sec

This monitor returns the rate of evictions from the cache. This is per partition per cube per database. Typically due to background cleaner.
Cache: Misses/sec
This monitor returns the rate of cache misses.

Connection: Current connections
This monitor returns the current number of client connections established.

Connection: Current user sessions
This monitor returns the current number of user sessions established. A connection is always tied to a session, but there could be sessions without active user connections.

Connection: Requests/sec
This monitor returns the rate of connection requests (arrivals).

Connection: Failures/sec
This monitor returns the rate of connection failures.

Connection: Successes/sec
This monitor returns the rate of successful connection completions.

Data Mining Prediction: Queries/sec
This monitor returns the rate of Data Mining queries.

Data Mining Prediction: Predictions/sec
This monitor returns the rate of Data Mining prediction queries.

Locks: Current latch waits
This monitor returns the current number of threads waiting for a latch. These are latch requests that could not be given immediate grants and are in a wait state.

Locks: Current lock waits
This monitor returns the current number of clients waiting for a lock.

Locks: Current locks
This monitor returns the current number of locked objects.

Locks: Lock waits/sec
This monitor returns the number of lock waits per second. These are lock requests that could not be given immediate lock grants and were put in a wait state.

Locks: Total deadlocks detected
This monitor returns the total number of deadlocks detected.

This counter has the Count statistic as difference option enabled and will show the statistical difference from the last polling cycle.
MDX: Total NON EMPTY unoptimized

This monitor returns the total number of times unoptimized a non empty algorithm is used. Total non empty un-optimized is the number of Calculate Non Empty operations that are using an un-optimized algorithm. If this number continues to grow, there may be MDX queries that are running slowly for this reason and we might want to find them and optimize them.

This counter has the Count statistic as difference option enabled and will show the statistical difference from the last polling cycle.

MDX: Total recomputes

This monitor returns the total number of cells recomputed due to error

This counter has the Count statistic as difference option enabled and will show the statistical difference from the last polling cycle.

MDX: Total Sonar subcubes

This monitor returns the total number of subcubes that query optimizer generated

This counter has the Count statistic as difference option enabled and will show the statistical difference from the last polling cycle.

Memory: Cleaner Memory shrinkable KB

This monitor returns the amount of memory, in KB, subject to purging by the background cleaner.

Memory: Cleaner Memory nonshrinkable KB

This monitor returns the amount of memory, in KB, not subject to purging by the background cleaner.

Memory: Cleaner Memory KB

This monitor returns the amount of memory, in KB, known to the background cleaner. (Cleaner memory shrinkable + Cleaner memory nonshrinkable.) Note that this counter is calculated from internal accounting information so there may be some small deviation from the memory reported by the operating system.

Memory: Cleaner Balance/sec

This monitor returns the rate of balance+shrink operations. Shows how many times the current memory usage is compared against the settings. Memory usage is checked every 500ms, so the counter will trend towards 2 with slight deviations when the system is under high stress. Preferred Value 2

Memory: Filestore KB

This monitor returns the current memory allocated to filestore (file cache), in KB.

Memory: Filestore Writes/sec

This monitor returns the rate of filestore written pages (asynchronous writes).
Memory: Filestore IO Errors/sec
This monitor returns the rate of filestore IO Errors.

Memory: Quota Blocked
This monitor returns the current number of quota requests that are blocked until other memory quotas are freed.

Memory: Filestore Reads/sec
This monitor returns the filestore pages read/sec.

Proactive Caching: Notifications/sec
This monitor returns the rate of notifications from relational database.

Proactive Caching: Processing Cancellations/sec
This monitor returns the rate of processing cancellations caused by notifications.

Proc Aggregations: Temp file bytes written/sec
This monitor returns the rate of writing bytes to a temporary file. Temporary files are written when aggregations exceed memory limits.

Processing: Rows read/sec
This monitor returns the rate of rows read from all relational databases.

Processing: Rows written/sec
This monitor returns the rate of rows written during processing.

Storage Engine Query: Queries from cache direct/sec
This monitor returns the rate of queries answered from cache directly. Rate of queries answered from cache directly.

Storage Engine Query: Queries from cache filtered/sec
This monitor returns the rate of queries answered by filtering existing cache entry. Rate of queries answered by filtering existing cache entry.

Storage Engine Query: Queries from file/sec
This monitor returns the rate of queries answered from files. Rate of queries answered from files.

Storage Engine Query: Avg time/query
This monitor returns the average time per query, in milliseconds. Response time based on queries answered since the last counter measurement.

Storage Engine Query: Measure group queries/sec
This monitor returns the rate of measure group queries.

Storage Engine Query: Dimension queries/sec
This monitor returns the rate of dimension queries.
Threads: Processing pool idle I/O job threads
   This monitor returns the number of idle threads for I/O jobs in the processing thread pool.

Threads: Processing pool busy I/O job threads
   This monitor returns the number of threads running I/O jobs in the processing thread pool.

 Threads: Processing pool job queue length
   This monitor returns the number of jobs in the queue of the processing thread pool.

Threads: Processing pool job rate
   This monitor returns the rate of jobs through the processing thread pool.

**SQL Server 2012 Reporting Services**

This template uses Windows performance counters to assess the status and performance of Microsoft SQL Server 2012 Reporting Services.

**Prerequisites**

WMI access to the target server.

**Credentials**

Windows Administrator on the target server.

**Monitored Components**

For details on monitors, see [SAM Component Monitor Types](#).

**MSRS Windows Service: Active Sessions**

This monitor returns the number of active sessions. This counter provides a cumulative count of all browser sessions generated from report executions, whether they are still active or not. The counter is decremented as session records are removed. By default, sessions are removed after ten minutes of no activity.

**MSRS Windows Service: Cache Flushes/Sec**

This monitor returns the number of cache flushes per second.

**MSRS Windows Service: Cache Hits/Sec**

This monitor returns the number of requests per second for cached reports. These are requests for re-rendered reports, not requests for reports processed directly from the cache.

**MSRS Windows Service: Cache Hits/Sec (Semantic Models)**

This monitor returns the number of requests per second for cached models. These are requests for re-rendered reports, not requests for reports processed directly from the cache.

**MSRS Windows Service: Cache Misses/Sec**
This monitor returns the number of requests per second that failed to return a report from cache. Use this counter to find out whether the resources used for caching (disk or memory) are sufficient.

**MSRS Windows Service: Cache Misses/Sec (Semantic Models)**

This monitor returns the number of requests per second that failed to return a model from cache. Use this counter to find out whether the resources used for caching (disk or memory) are sufficient.

**MSRS Windows Service: Delivers/Sec**

This monitor returns the number of report deliveries per second, from any delivery extension.

**MSRS Windows Service: Events/Sec**

This monitor returns the number of events processed per second. Events that are monitored include SnapshotUpdated and TimedSubscription.

**MSRS Windows Service: Memory Cache Hits/Sec**

This monitor returns the number of times per second that reports are retrieved from the in-memory cache. In-memory cache is a part of the cache that stores reports in CPU memory. When in-memory cache is used, the report server does not query SQL Server for cached content.

**MSRS Windows Service: Memory Cache Miss/Sec**

This monitor returns the number of times per second that reports could not be retrieved from the in-memory cache.

**MSRS Windows Service: Reports Executed/Sec**

This monitor returns the number of successful report executions per second. This counter provides statistics about report volume. Use this counter with Request/Sec to compare report execution to report requests that can be returned from cache.

**MSRS Windows Service: Requests/Sec**

This monitor returns the number of requests per second made to the report server. This counter tracks all types of requests that are handled by the report server.

**MSRS Windows Service: Snapshot Updates/Sec**

This monitor returns the total number of report execution snapshot updates per second.

**MSRS Windows Service: Total Processing Failures**

This monitor returns the number of errors in report server web service request processing. **Note:** This counter has the Count statistic as difference option enabled and will show the statistical difference from the last polling cycle.

**MSRS Windows Service: Total Rejected Threads**

This monitor returns the total number of threads rejected for asynchronous processing, and
subsequently handled as synchronous processes in the same thread. Each data source is processed on one thread. If the volume of threads exceeds capacity, threads are rejected for asynchronous processing, and are then processed in a serial manner.

**Note:** This counter has the Count statistic as difference option enabled and will show the statistical difference from the last polling cycle.

**Report Server: Active Connections**

This monitor returns the number of connections currently active on the server.

**Report Server: Bytes Received/sec**

This monitor returns the number of bytes received per second by the server. This counter is updated only when a transfer is complete. This means that the counter remains at 0 and then the value increases after a transfer is complete.

**Report Server: Bytes Sent/sec**

This monitor returns the number of bytes sent per second from the server. This counter is updated only when a transfer is complete. This means that the counter remains at 0 and then the value increases after a transfer is complete.

**Report Server: Errors/sec**

This monitor returns the total number of errors that occur per second during the processing of HTTP requests. These errors include HTTP status codes in the 400s and 500s.

**Report Server: Logon Attempts/sec**

This monitor returns the rate of logon attempts.

**Report Server: Logon Successes/sec**

This monitor returns the rate of successful logons.

**Report Server: Memory Pressure State**

This monitor returns memory pressure state. One of the following numbers, from 1-5, which indicates the current memory state of the server:

1. No pressure
2. Low pressure
3. Medium pressure
4. High pressure
5. Exceeded pressure

**Report Server: Memory Shrink Amount**

This monitor returns the number of bytes that the server requested to shrink the memory in use.

**Report Server: Memory Shrink Notifications/sec**

This monitor returns the number of notifications that the server issued in the last second to
shrink the memory in use. This value indicates how often the server experiences memory pressure.

**Report Server: Requests Executing**

This monitor returns the number of requests that are currently processing.

**Report Server: Requests/sec**

This monitor returns the number of requests that are processed per second. This value represents the current throughput of the application.

**Report Server: Tasks Queued**

This monitor returns the number of tasks that are waiting for a thread to become available for processing. Each request made to the report server corresponds to one or more tasks. This counter represents only the number of tasks that are ready for processing; it does not include the number of tasks that are currently running.

**Service: SQL Server Reporting Services**

This monitor returns CPU and memory usage of SQL Server Reporting Services. This service manages, executes, renders, schedules and delivers reports.

**Report Server TCP Port**

This component monitor tests the ability of a Report Server to accept incoming sessions. By default, it monitors TCP port 80.
Microsoft Windows Internet Name Service (WINS)

The following templates are available:

- Microsoft Windows Internet Name Service (WINS) Events
- Microsoft Windows Internet Name Service (WINS) Statistic

Microsoft Windows Internet Name Service (WINS) Events

This template assesses the status and overall performance of a Microsoft WINS server by monitoring critical errors in the Windows Application Log file.

Prerequisites

WMI access to the target server.

Credentials

Windows Administrator on the target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

All monitors should return values of zero. Returned values other than zero may indicate an abnormality. If you believe an abnormality exists, you should examine the Windows System log for details. Source name: WINS.

Network related events

This monitor returns the following events:

- The Winsock send or receive function returned with an unexpected error;
- The WinSock send function returned with an unexpected error;
- WINS could not free a User Datagram Protocol (UDP) Buffer;
- The WINS User Datagram Protocol (UDP) Listener thread encountered an error;
- WINS encountered an error while processing a push trigger or update notification;
- The WINS server cannot make or accept connections because the connections limit has been reached;
- WINS tried to get its addresses but failed;
- WINS did not get back any names from NetBIOS over TCP/IP (NetBT) when it did an adapter status;
- The computer running the WINS server does not have a valid address;
- WINS Push thread encountered an exception;
- The Name Release or Query Response could not be sent due to an error;
- INS could not send a User Datagram Protocol (UDP) message to a WINS client.

Event ID: 4210, 4211, 4219, 4246, 4283, 4286, 4291, 4292, 4301, 4242, 4188, 4189, 4208.

**WINS encountered an error while processing a push trigger or update notification:** check to see if the remote WINS that sent the trigger went down. If the remote WINS is on a different subnet, then maybe the router is down.

**The WINS server cannot make or accept connections because the connections limit has been reached:** Examine your replication topology, and make sure that you are configured for a true Hub-and-Spokes replication topology. Verify that there is not a TCP connection shortage. Before the TCP packet is sent, the computer verifies that it has sufficient resources, for example free outgoing TCP ports. To verify that there is not a TCP connection shortage, follow these steps: Run the following command on the failing computer (at the time that this computer is logging the event ID 4286 errors), and then save the output to a file. To do so, run the following command from a command prompt:

```
netstat -a
```

Look for the total number of sessions and used ports, examine the state of the sessions to determine whether the number of sessions has reached the maximum value. By default, the maximum value is 5000.

**The computer running the WINS server does not have a valid address:** WINS binds to the first adapter in a machine with more than one adapter bound to TCP/IP. Check the binding order of adapters and make sure the first one has a valid IP address for the WINS server.

**Other events:** Try to restart your network adapter.

**Low resources events**

This monitor returns the following events:

- WINS could not allocate a responder association;
- WINS could not allocate an initiator association;
- WINS could not allocate an implicit dialogue;
- WINS could not allocate an explicit dialogue;
- WINS could not allocate a User Datagram Protocol (UDP) Buffer;
- WINS could not create a communication subsystem thread;
- WINS encountered a low memory condition;
- The WINS server started the burst handling of incoming requests.

Event ID: 4213, 4214, 4215, 4216, 4218, 4220, 4297, 4338.

For all of these events, check to see if the system is running out of memory.

**Database related events**

This monitor returns the number of events, such as:

- WINS encountered a database error;
• An error has prevented WINS from updating the WINS database, the database may be corrupt;
• The static data file that is used to initialize the WINS database is too big;
• WINS is trying to update the version number of a database record that it does not own;
• WINS encountered an error doing a database backup to directory;
• WINS has found some database corruption;
• WINS could not start due to a missing or corrupt database;
• WINS could not start because the existent database must be converted to the Windows 2000 format.

Event ID: 4224, 4254, 4258, 4275, 4289, 4302, 4311, 4318, 4319, 4320, 4322, 4323, 4324.

**WINS encountered a database error:** This may or may not be a serious error. WINS will try to recover from it. You can check the database error events under 'Application Log' category of the Event Viewer for the Exchange Component, ESENT, source to find out more details about database errors. If you continue to see a large number of these errors consistently over time (a span of few hours), you may want to restore the WINS database from a backup. The error number is in the second DWORD of the data section.

**WINS is trying to update the version number of a database record that it does not own:** This is a serious error if the WINS server is updating the record after a conflict. It is not a serious error if the WINS server is updating the record as a result of a request to do so from a remote WINS server (When a remote WINS server notices a conflict between an active owned entry and a replica it informs the owner of the replica to update the version number of the record. It is possible that the replica is no longer owned by the remote WINS). Check the previous log entry to determine which situation applies here.

**WINS has found some database corruption:** It will try to recover. This recovery process can take a long time. Do not kill WINS in the middle of the recovery. If you do, you will have to restart WINS with a clean database.

**WINS could not start due to a missing or corrupt database:** Restore the database using WINS Manager (or winscl.exe found in the Windows 2000 Resource Kit) and restart WINS. If WINS still does not start, begin with a fresh copy of the database. To do this: delete all the files in the %SystemRoot%\system32\WINS directory.

1. If the WINS database file (typically named wins.mdb) is not in the above directory, check the registry for the full filepath. Delete the .mdb file.
   
   If jet*.log files are not in the above directory, check the registry for the directory path. Delete all log files. After that restart WINS.

**WINS could not start because the existent database must be converted to the Windows 2000 format:** If this is the first invocation of WINS after an upgrade From NT3.51, you need to run the convert utility (upg351db.exe in the %SystemRoot%\system32 directory) on the WINS database to convert it to the new database format. Once you have done that, you should restart WINS.
Corrupted WINS Database: In rare situations the WINS database may be corrupted. To recover from this situation, follow these steps:

1. Stop replication.
2. Delete the replication partners.
3. Use the Jetpack tool on the database on the hub server.
4. Reestablish replication, and then force a replication.
5. Use the WINS Microsoft Management Console (MMC) to examine the consistency of the WINS database.
6. In a large WINS environment where IP addresses constantly change, do not configure the Replicate on Address Change option on an NT4 WINS server. The equivalent setting on a Windows 2000 WINS server is the When Address Changes check box in the WINS snap-in. Click to clear the check box to restore the default setting.

Registry related events

This monitor returns the following events:

- WINS could not get information about a key;
- WINS could not get information about the Pull key;
- WINS could not get information about the Push key;
- INS could not get information about the DATAFILES key;
- WINS could not get information about the SPEC_GRP_MASKS key;
- WINS could not open a Pull subkey;
- WINS could not open a Push subkey;
- WINS could not close an open key;
- WINS could not read the Refresh interval from the registry;
- WINS could not read the Tombstone interval from the registry;
- WINS could not read the Verify interval from the registry;
- WINS could not read the retry count for retrying communication with a remote WINS;
- WINS could not read the Tombstone Timeout from the registry;
- WINS could not read the ConsistencyCheck value (type DWORD) from the Parameters\ConsistencyCheck subkey in the registry;
- WINS could not read the MaxRecsAtATime value (type DWORD) in the Wins\Parameters\ConsistencyCheck subkey of the registry;
- WINS could not read the UseRplPnrs value of the Wins\Parameters\ConsistencyCheck key.

Event ID: 4230, 4231, 4232, 4233, 4234, 4235, 4236, 4240, 4109, 4110, 4111, 4112, 4113, 4114, 4115, 4116.
WINS could not read the ConsistencyCheck value (type DWORD) from the Parameters\ConsistencyCheck subkey in the registry: The first consistency check is done at the time specified in the SpTime entry under the ConsistencyCheck subkey and is limited by the MaxRecsAtATime value. If the time is not specified, the check is done at 2 am. To correct the problem, open the registry and verify that the ConsistencyCheck subkey has been correctly sent up and all required values have been set. Correct the values as needed.

WINS could not read the MaxRecsAtATime value (type DWORD) in the Wins\Parameters\ConsistencyCheck subkey of the registry: Set this value if you do not want WINS to replicate more than a set number of records in one cycle while doing periodic consistency checks of the WINS database. When doing a consistency check, WINS replicates all records of an owner WINS by either going to that WINS or to a replication partner. At the end of doing a consistency check for an owner's records, it checks to see if it has replicated more than the specified value in the current consistency check cycle. If the value has been exceeded, the consistency check stops, otherwise it continues. In the next cycle, it starts from where it left off and wraps around to the first owner if required.

WINS could not read the UseRplPnrs value of the Wins\Parameters\ConsistencyCheck key: If this value is set to a non-zero (DWORD) value, WINS will do a consistency check of the owners in its database by going to one or more of its replication partners. If the owner of the records happens to be a replication partner, WINS will go to it, otherwise it will pick one at random. Set this value if you have a large number of WINSs in your configuration and/or if you do not want the local WINS to go to any WINS that is not a replication partner.

Other events: Check to see if the permissions on the key are set properly, system resources are low, or the registry is having a problem.

Operation events

This monitor returns the number of events, such as:

- WINS received an error while trying to register a group's replica with name;
- WINS received an error while trying to register a unique replica with name;
- WINS received an error while trying to register the unique entry with the name;
- WINS received an error while trying to register the group entry with the name;
- WINS received an error while trying to update the version number of a record in the WINS database;
- WINS received an error while trying to release a record in the WINS database;
- WINS received an error while trying to query a record in the WINS database;
- WINS encountered an error while deleting the file;
- WINS encountered an error while deleting one or more records of a WINS;
- WINS encountered an error while getting the browser names for a client.

Event ID: 4261, 4262, 4263, 4265, 4266, 4267, 4303, 4304, 4305.

Examine event in Event Viewer for details.

Replication events

This monitor returns the number of events, such as:
The WINS Replication Pull Handler could not connect to a WINS server;
WINs received a replica whose state is incorrect;
The WINS replicator Pull thread encountered an error while processing a request;
WINs received an error while registering replicas;
WINs's Replicator could not find any records in the WINS database;
The replication Pull or Push thread is shutting down due to an error.

Event ID: 4251, 4268, 4307, 4260, 4121, 4166, 4167.

**The WINS Replication Pull Handler could not connect to a WINS server:** Check network configuration.

**The WINS replicator Pull thread encountered an error while processing a request:** Check other log entries to determine what went wrong.

**WINs received an error while registering replicas:** It will not register any additional replicas of this WINS at this time (the address is in the data section 4th-8th byte). Check a previous log entry to determine the reason for this. If you get the same error during subsequent replication with the above partner WINs, you may want to restore the WINs database from the backup.

**WINs's Replicator could not find any records in the WINs database:** This means there are no active or tombstone records in the database. It could be that the records being requested by a remote WINs server have either been released or do not exist.

**The replication Pull or Push thread is shutting down due to an error:** Restart WINs.

**Other events**

This monitor returns the number of events, such as:

- A WINs Remote Procedure Call (RPC) thread encountered an error;
- The WINs TCP Listener thread encountered an error;
- The WINs Scavenger thread encountered an error;
- The WINs Challenger thread encountered an error;
- A WINs worker thread encountered an error;
- The Push Thread was requested for a range of records but could not find any records in the range;
- The WINs Server could not initialize security to allow the read-only operations.

Event ID: 4244, 4245, 4247, 4248, 4249, 4227, 4337.

**The Push Thread was requested for a range of records but could not find any records in the range:** Make sure that the replication time intervals are set properly. If the tombstone interval and timeout intervals are not correct (that is, much less than the replication interval), the above condition is possible. This is because the records might get changed into tombstones and then deleted before the remote WINs can pull them. Similarly, if the refresh interval is set to be much less than the replication interval then the records could get released before a WINs can pull them (a released record is not sent). Make sure that the replication time intervals are set properly.

**Other errors:** Restart WINs.
Microsoft Windows Internet Name Service (WINS) Statistic

This template assesses the status and overall performance of a Microsoft WINS server by retrieving statistics from performance counters.

**Prerequisites**

WMI access to the target server.

**Credentials**

Windows Administrator on the target server.

**Monitored Components**

For details on monitors, see [SAM Component Monitor Types](#).

- **Failed Queries/sec**
  This component returns the total number of failed queries per second. This counter should be as low as possible.

- **Failed Releases/sec**
  This component returns the total number of failed releases per second. This counter should be as low as possible.

- **Group Conflicts/sec**
  This component returns the rate at which group registration received by the server resulted in conflicts with records in the database.

- **Group Registrations/sec**
  This component returns the rate at which group registration are received by the server.

- **Group Renewals/sec**
  This component returns the rate at which group renewals are received by the server.

- **Queries/sec**
  This component returns the rate at which queries are received by the server.

- **Releases/sec**
  This component returns the rate at which releases are received by the server.

- **Successful Queries/sec**
  This component returns the total number of successful queries per second.

- **Successful Releases/sec**
  This component returns the total number of successful releases per second.
Total Number of Conflicts/sec

This component returns the sum of the Unique and Group conflicts per second. This is the total rate at which conflicts were seen by the server.

Total Number of Registrations/sec

This component returns the sum of the Unique and Group registrations per second. This is the total rate at which registration are received by the server.

Total Number of Renewals/sec

This component returns the sum of the Unique and Group renewals per second. This is the total rate at which renewals are received by the server.

Unique Conflicts/sec

This component returns the rate at which unique registrations/renewals received by the server resulted in conflicts with records in the database. This counter should be as low as possible.

Unique Registrations/sec

This component returns the rate at which unique registration are received by the server.

Unique Renewals/sec

This component returns the rate at which unique renewals are received by the server.

Service: WINS

This component returns the CPU and memory usage of Microsoft WINS service. This service manages the Windows Internet Name Service (WINS), which translates NetBIOS computer names to IP addresses.

WINS Replication TCP Port

This component monitor tests the ability of a WINS Replication service to accept incoming sessions.

⚠ By default, TCP port 42 is monitored.
Microsoft Windows Server

The following templates are available:

- Microsoft Windows Server 2003 Failover Cluster
- Microsoft Windows Server 2008 Failover Cluster
- Microsoft Windows Server 2008 R2-2016 Failover Cluster (Advanced)
- Microsoft Windows Server 2012 - 2016 Failover Cluster
- Microsoft Windows Server 2012 Failover Cluster
- Windows 2003 -2008 FTP Service
- Windows 2008 R2 - 2012 FTP Service
- Microsoft Windows 2016 FTP service
- Microsoft Windows DHCP Server
- Windows DNS Server
- Windows Network Load Balancing
- Microsoft Windows Servers Print Services
- Windows Print Services 2016
- Windows Remote Desktop Services (Session Host Role)
- Windows Scheduled Tasks
- Windows Server 2003 Domain Controller Security
- Microsoft Windows Server 2003-2012 Services and Counters
- Microsoft Windows Server 2008 - 2016 Domain Controller Security
- Microsoft Windows Server 2016 Services and Counters
- Windows Update Monitoring

Periodically, SolarWinds releases SAM templates to support the latest product versions such as Microsoft Server 2016. You can continue using templates for older product versions, but updating to the latest template is recommended.
Microsoft Windows Server 2003 Failover Cluster

This template assesses the status and overall health and status of a Microsoft Windows 2003 Failover Cluster by retrieving information from the Windows System Event Log. For more information, refer to the following Microsoft article: http://technet.microsoft.com/en-us/library/cc720058(WS.10).aspx.

Prerequisites

WMI access to the target server.

Credentials

Windows Administrator on the target server.

All Windows Event Log monitors should return zero values. Returned values other than zero indicates an abnormality. Examining the Windows system log files should provide information pertaining to the issue. Detailed information about these events can be found here: http://technet.microsoft.com/en-us/library/dd353290(WS.10).aspx.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Service: Windows Time

This monitor returns the CPU and memory usage of the Windows Time service. This service maintains date and time synchronization on all clients and servers in the network. If this service is stopped, date and time synchronization will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

Service: Cluster Service

This monitor returns the CPU and memory usage of the Cluster service. This service enables servers to work together as a cluster to keep server-based applications highly available, regardless of individual component failures. If this service is stopped, clustering will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

Backup and Restore Functionality Problems

This monitor returns the number of events that occur when:

- The backup operation for the cluster configuration data has been aborted because quorum for the cluster has not yet been achieved;
- The restore request for the cluster configuration data has failed during the "pre-restore" or "post-restore" stage.

Type of event: Error. Event ID: 1541, 1542, 1543.
Check for the following pre-conditions to make sure they have been met, and then retry the backup or restore operation:

- The cluster must achieve quorum. In other words, enough nodes must be running and communicating (perhaps with a witness disk or witness file share, depending on the quorum configuration) that the cluster has achieved a majority, that is, quorum.
- The account used by the person performing the backup must be in the local Administrators group on each clustered server, and must be a domain account, or must have been delegated the equivalent authority.
- During a restore, the restore software must obtain exclusive access to the cluster configuration database on a given node. If other software has access (open handles to the database), the restore cannot be performed.

**Cluster Network Connectivity Problems**

This monitor returns the number of events that occur when:

- The Cluster network interface for some cluster node on a special network failed;
- The Cluster network is partitioned and some attached failover cluster nodes cannot communicate with each other over the network;
- The Cluster network is down;
- The Cluster IP address resource failed to come online;
- Attempting to use IPv4 for a special network adapter failed.

**Type of event:** Warning and Error. Event ID: 1127, 1129, 1130, 1360, 1555.

Run the Validate a Configuration Wizard, selecting only the network tests. Also check network devices (adapters, cables, hubs, switches, etc) and quorum configuration.

Compare the properties of the IP Address resource with the properties of the corresponding network to ensure that the network and subnet information match. If this is an IPv6 resource, make sure that the cluster network for this resource has at least one IPv6 prefix that is not link-local or tunnel.

**Cluster Service Startup Problems**

This monitor returns the number of events that occur when:

- The Cluster service suffered an unexpected fatal error;
- The Cluster service was halted due to incomplete connectivity with other cluster nodes;
- The Cluster service was halted to prevent an inconsistency within the failover cluster;
- The Cluster resource host subsystem (RHS) stopped unexpectedly;
- The Cluster resource either crashed or deadlocked;
- The Cluster service encountered an unexpected problem and will be shut down;
- The Cluster service has prevented itself from starting on this node. (This node does not have the latest copy of cluster configuration data.)
- The membership engine detected that the arbitration process for the quorum device has stalled.

**Type of event:** Error. Event ID: 1000, 1006, 1073, 1146, 1230, 1556, 1561, 1178.
There are various software or hardware related causes that can prevent the Cluster service from starting on a node. Sometimes the Cluster service can restart successfully after it has been interrupted by one of those causes. Review the event logs for indications of the problem.

Check network hardware and configuration. Use the Validate a Configuration Wizard to review the network configuration.

Check to see which resource DLL is causing the issue and report the problem to the resource vendor. Consider configuring the resource to run in its own Resource Monitor. Note that while a problem with a resource DLL will not stop the Cluster service from running, it can prevent other resource DLLs from running unless the resource runs in its own Resource Monitor.

Try starting the Cluster service on all other nodes in the cluster. If the Cluster service can be started on a node with the latest copy of the cluster configuration data, then the node that previously could not be started will probably be able to obtain the latest copy and then join the cluster successfully.

**Cluster Shared Volume Functionality Problems**

This monitor returns the number of events that occur when:

- The Cluster Shared Volume is no longer available on this node;
- The Cluster Shared Volume is no longer directly accessible from this cluster node;
- The Cluster service failed to create the Cluster Shared Volumes root directory;
- The Cluster service failed to set the permissions (ACL) on the Cluster Shared Volumes root directory;
- The Cluster Shared Volume is no longer accessible from this cluster node;
- The Cluster service failed to create a cluster identity token for Cluster Shared Volumes.

**Type of event:** Error. Event ID: 5120, 5121, 5123, 5134, 5135, 5142, 5200.

Review events related to communication with the volume.

Check storage and network configuration.

Check Cluster Shared Volumes folder creation and permissions.

Check communication between domain controllers and nodes.

**Cluster Storage Functionality Problems**

This monitor returns the number of events that occur when:

- The Cluster Physical Disk resource cannot be brought online because the associated disk could not be found;
- While the disk resource was being brought online, access to one or more volumes failed with an error;
- The file system for one or more partitions on the disk for the resource may be corrupt;
- The Cluster disk resource indicates corruption for specific volume;
- The Cluster disk resource contains an invalid mount point.

**Type of event:** Error. Event ID: 1034, 1035, 1037, 1066, 1208.
Confirm that the affected disk is available.

Check the underlying storage hardware and confirm that the device is being presented correctly to the cluster nodes.

If you have problems with partitions on the disk or corruption, we recommend that you run Chkdsk so that it can correct any problems with the file system.

Confirm that the mounted disk is configured according to the following guidelines:

Clustered disks can only be mounted onto clustered disks (not local disks);
The mounted disk and the disk it is mounted onto must be part of the same clustered service or application. They cannot be in two different clustered services or applications, and they cannot be in the general pool of Available Storage in the cluster.

**Cluster Witness Problems**

This monitor returns the number of events that occur when:

- The Cluster service failed to update the cluster configuration data on the witness resource due to resource inaccessibility;
- The Cluster service detected a problem with the witness resource;
- The File Share Witness resource failed a periodic health check;
- The File Share Witness resource failed to come online;
- The File Share Witness resource failed to arbitrate for the specific file share;
- The node failed to form a cluster because the witness was not accessible.

**Type of event:** Error. Event ID: 1557, 1558, 1562, 1563, 1564, 1573.

Confirm witness accessibility by viewing the quorum configuration of a failover cluster and the status of a witness disk.

**Configuration Availability Problems**

This monitor returns the number of events that occur when:

- The cluster configuration database could not be loaded or unloaded;
- The cluster service cannot start due to failed attempts to read configuration data.

**Type of event:** Error. Event ID: 1057, 1090, 1574, 1575, 1593.

When the cluster configuration on a node is missing or corrupt, the Cluster service cannot load the configuration and therefore cannot start. Where possible, the Cluster service will obtain the latest cluster configuration from other nodes in the cluster. Ensure that other nodes are started. If the only node or nodes that can be started appear to have a missing or corrupt cluster configuration database, you will probably need to restore one of the nodes from a system state backup. (For a failover cluster node, the system state backup includes the cluster configuration.) Sometimes when the node attempts to unload the cluster configuration database, the action does not fully complete. Try stopping and restarting the Cluster service. If this does not succeed, restart the operating system on the affected node.
**DFS Namespace Resource Availability Problems**

This monitor returns the number of events that occur when:

- The creation of DFS namespace root failed with error;
- The resynchronization of DFS root target failed with error;
- The cluster file share resource for DFS Namespace cannot be brought online due to error.

**Type of event:** Error. Event ID: 1138, 1141, 1142.

Check DFS namespace configuration.

**Encrypted Settings for Cluster Resource Could not Applied**

This monitor returns the number of events when encrypted settings for a cluster resource could not be successfully applied to the container on this node.

**Type of event:** Error. Event ID: 1121.

Close any application that might have an open handle to the registry checkpoint indicated by the event. This will allow the registry key to be replicated as configured with the resource properties. If necessary, contact the application vendor about this problem. You can use a utility called Handle with the -a option to view handles to the registry.

**Failed to Form Cluster**

This monitor returns the number of Failed to Form cluster events.

**Type of event:** Error. Event ID: 1092, 1009.

You might be able to correct this issue by restarting the Cluster service.

**File Share Resource Availability Problems**

This monitor returns the number of events that occur when:

- The Cluster File Share cannot be brought online because a file share could not be created;
- The retrieving of information for a specific share returned an error code;
- The retrieving of information for a specific share indicated that the share does not exist;
- The Creation of a file share failed due to an error;
- The Cluster file share resource has detected shared folder conflicts;
- The Cluster file server resource failed a health check because some of its shared folders were inaccessible.

**Type of event:** Warning and Error. Event ID: 1053, 1054, 1055, 1068, 1560, 1585, 1586, 1587, 1588.

Confirm that the share exists and that the permissions allow access to the share.

If possible, determine whether the path to the share has been changed. If so, recreate the share with the correct name.
View all the resources in the clustered file server instance to ensure that they are coming online, and review the dependencies among the resources. Reconfigure as necessary to correct any problems.

Ensure that no two shared folders have the same share name.

Check shared folder accessibility and the State of Server service.

**Generic Application Could not be Brought Online**

This monitor returns the number of events that occur when a generic application could not be brought online during an attempt to create the process due to: the application not being present on this node, an incorrect path name, or an incorrect binary name.

**Type of event:** Error. Event ID: 1039.

Confirm that the following are true for the application used by the clustered Generic Application instance:

- The application is fully installed on all nodes that are possible owners of the Generic Application resource;
- The configuration for the Generic Application resource specifies the correct application and path;
- The configuration for the Generic Application resource specifies the appropriate parameters and settings for registry replication.

**Generic Service Resource Availability Problems**

This monitor returns the number of events that occur when:

- The generic service is either not installed or the specified service name is invalid;
- The specified generic service parameters might be invalid;
- The generic service failed with an error.

**Type of event:** Error. Event ID: 1040, 1041, 1042.

Confirm that the correct service is specified in the configuration for the Generic Service resource and confirm that the service is fully installed on all nodes that are possible owners of the resource.

Check service operation and examine the application event log.

**IP address Resource Availability Problems**

This monitor returns the number of events that occur when:

- The Cluster IP address resource cannot be brought online because the subnet mask value is invalid;
- The Cluster IP address resource cannot be brought online because the address value is invalid;
- The configuration data for the network adapter corresponding to the cluster network interface could not be determined;
- The Cluster IP address resource cannot be brought online because a duplicate IP address was detected on the network;
- The Cluster IP address resource cannot be brought online because WINS registration;
- The lease of the IP address associated with the cluster IP address resource has expired or is about to expire, and currently cannot be renewed;
- The IPv6 Tunnel address resource failed to come online because it does not depend on an IP Address (IPv4) resource;
- The Cluster network associated with dependent IP address (IPv4) resource does not support ISATAP tunneling.

**Type of event:** Error. Event ID: 1046, 1047, 1048, 1049, 1078, 1242, 1361, 1363.

Check the address, subnet, and network properties of the IP Address resource.

If the resource is an IPv6 Tunnel address resource, make sure it depends on at least one IP Address (IPv4) resource. Also make sure the network supports Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) tunneling.

If the IP Address resource appears to be configured correctly, check the condition of network adapters and other network components used by the cluster.

**Network Connectivity and Configuration Problems**

This monitor returns the number of events that occur when:

- The Cluster Service was unable to access the network adapter or the cluster node has no network connectivity;
- The Cluster node has no network connectivity;
- The Cluster node has lost all network connectivity;
- The failover cluster virtual adapter failed to initialize the miniport adapter.

**Type of event:** Error. Event ID: 1289, 1553, 1554, 4871.

Correct any problems with the physical network adapters and the cluster virtual adapter. If a previous change in the configuration is interfering with the function of the cluster virtual adapter, it might be necessary to reinstall the failover clustering feature on the node. Also, use the Validate a Configuration Wizard to review the network configuration.

**Node Failed to Join Cluster**

This monitor returns the number of events that occur when the node failed to join the failover cluster due to an error.

**Type of event:** Error. Event ID: 1070.

You might be able to correct this issue by restarting the Cluster service.

**Problems with Cluster Service**

This monitor returns the number of events that occur when:

- The cluster resource in the Clustered service or application failed;
- The Cluster service failed to bring the Clustered service or application completely online or offline and one or more resources may be in a failed state.

**Type of event:** Warning and Error. Event ID: 1039, 1205.
Check and correct any problems with the application or service associated with the resource.

Check and correct any problems with cables or cluster-related devices.

Adjust the properties for the resource in the cluster configuration, especially the value for the Pending Timeout for the resource. This value must allow enough time for the associated application or service to start.

Check the state of all resources in the clustered service or application.

**Quorum was Lost**

This monitor returns the number of events that occur when the Cluster service is shutting down because quorum was lost.

**Type of event:** Error. Event ID: 1177.

This can occur when network connectivity is lost between some or all of the nodes in the cluster, or the witness disk fails over. It can also occur if you make a change in the cluster configuration such as increasing the number of nodes, when the number of nodes currently online is too few to achieve quorum in the new configuration. Run the Validate a Configuration Wizard, selecting only the network tests. Also check network devices (adapters, cables, hubs, switches, etc.) and quorum configuration.

**Registry Checkpoint Could not be Restored to Registry Key**

This monitor returns the number of events that occur when the Registry Checkpoint for Cluster resource could not be restored to a registry key.

**Type of event:** Error. Event ID: 1024.

Close any application that might have an open handle to the registry checkpoint indicated by the event. This will allow the registry key to be replicated as configured with the resource properties. If necessary, contact the application vendor about this problem. You can use a utility called Handle with the -a option to view handles to the registry.

**System is not being Responsive**

This monitor returns the number of events that occur when the Failover cluster virtual adapter has lost contact with the process.

**Type of event:** Error. Event ID: 4869, 4870.

Use Resource Monitor to determine, in real time, how many system resources a service or application is utilizing. This may take several minutes if the system is critically low on resources.

**Windows 2003 -2008 FTP Service**

This template assesses the status and overall of services and performance of a Microsoft Windows Server 2003-2008 FTP service.

**Prerequisites**

WMI access to the target server.
Credentials

Windows Administrator on the target server.

Monitored Components

For details on monitors, see [SAM Component Monitor Types](#).

You should manually put thresholds for component monitors according to your requirements.

**FTP Publishing Service**

This monitor returns CPU and memory usage for the FTP Publishing Service, which enables this server to be a File Transfer Protocol (FTP) server. If this service is stopped, the server cannot function as an FTP server. If this service is disabled, any services that explicitly depend on it will fail to start.

**FTP User Experience Monitor**

This component monitor tests the ability of an FTP server to accept an incoming session, process the user login, and then transmit the specified file to the APM server. After receiving the file, APM performs a file integrity test comparing the MD5 checksum of the downloaded file against a previously generated checksum. If the checksums match, the component monitor reports its status as up.

This monitor should be properly configured before using it on the target FTP server. By default, this monitor is disabled.

**Bytes Received/sec**

This monitor returns the number of bytes received per second by the FTP service.

**Bytes Sent/sec**

This monitor returns the number of bytes sent per second by the FTP service.

**Current Anonymous Users**

This monitor returns the number of users who currently have an anonymous connection using the FTP service.

**Current Connections**

This monitor returns the current number of connections established with the FTP service.

**Current Non-Anonymous Users**

This monitor returns the number of users who currently have a non-anonymous connection using the FTP service.

**Total Connection Attempts**

This monitor returns the number of connections that have attempted to use the FTP service since service startup. This counter is for all instances listed.
Total Files Received

This monitor returns the total number of files received by the FTP service since service startup.

This counter has the Count statistic as difference option enabled and will show the statistical difference from the last polling cycle.

Total Files Sent

This monitor returns the total number of files sent by the FTP service since service startup.

This counter has the Count statistic as difference option enabled and will show the statistical difference from the last polling cycle.

Total Files Transferred

This counter has the Count statistic as difference option enabled and will show the statistical difference from the last polling cycle.
Microsoft Windows Server 2008 Failover Cluster

This template assesses the status and overall performance of a Microsoft Windows 2008 Failover Cluster by retrieving information from performance counters and the Windows System Event Log. For more information, refer to the following Microsoft article: http://technet.microsoft.com/en-us/library/cc720058(WS.10).aspx.

Prerequisites

WMI access to the target server.

Credentials

Windows Administrator on the target server.

All Windows Event Log monitors should return zero values. Returned values other than zero indicates an abnormality. Examining the Windows system log files should provide information pertaining to the issue. Detailed information about these events can be found here: http://technet.microsoft.com/en-us/library/dd353290(WS.10).aspx.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

You need to set thresholds for counters according to your environment. It is recommended to monitor counters for some period of time to understand potential value ranges and then set the thresholds accordingly.

Service: Windows Time

This monitor returns the CPU and memory usage of the Windows Time service. This service maintains date and time synchronization on all clients and servers in the network. If this service is stopped, date and time synchronization will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

Service: Cluster Service

This monitor returns the CPU and memory usage of the Cluster service. This service enables servers to work together as a cluster to keep server-based applications highly available, regardless of individual component failures. If this service is stopped, clustering will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

Network Reconnections: Reconnect Count

This monitor returns the number of times the nodes have reconnected.

The instance field is installation-specific. You need to specify the hostname of your cluster node (for example: node1). By default, this component monitor is disabled and should only be enabled for troubleshooting purposes.
Network Reconnections: Normal Message Queue Length

This monitor returns the number of normal messages that are in the queue waiting to be sent. Normally this number is 0, but if the TCP connection breaks, you might observe it going up until the TCP connection is re-established and we can send all of them through.

![The instance field is installation-specific. You need to specify the hostname of your cluster node (for example: node1). By default, this component monitor is disabled and should only be enabled for troubleshooting purposes.]

Network Reconnections: Urgent Message Queue Length

This monitor returns the number of urgent messages that are in the queue waiting to be sent. Normally this number is 0, but if the TCP connection breaks, you might observe it going up until the TCP connection is re-established, thereby allowing all messages to be sent.

![The instance field is installation-specific. You need to specify the hostname of your cluster node (for example: node1). By default, this component monitor is disabled and should only be enabled for troubleshooting purposes.]

Messages Outstanding

This monitor returns the number of cluster MRR outstanding messages. The returned value should be near zero.

Resource Control Manager: Groups Online

This monitor returns the number of online cluster resource groups on this node. The returned value should be above zero at all times.

Resource Control Manager: RHS Processes

This monitor returns the number of running resource host subsystem processes (rhs.exe). The returned value should be above zero at all times.

Resource Control Manager: RHS Restarts

This monitor returns the number of resource host subsystem process (rhs.exe) restarts.

![By default, this component monitor is disabled and should only be enabled for troubleshooting purposes.]

Resources: Resource Failure

This monitor returns the number of resource failures. The returned value should be as low as possible.

Resources: Resource Failure Access Violation

This monitor returns the number of resource failures caused by access violation. The returned value should be as low as possible.

![By default, this component monitor is disabled and should only be enabled for troubleshooting purposes.]
Resources: Resource Failure Deadlock

This monitor returns the number of resource failures caused by deadlock. Deadlocks are usually caused by the resource taking too long to execute certain operations. The returned value should be as low as possible.

By default, this component monitor is disabled and should only be enabled for troubleshooting purposes.

Backup and Restore Functionality Problems

This monitor returns the number of events that occur when:

- The backup operation for the cluster configuration data has been aborted because quorum for the cluster has not yet been achieved;
- The restore request for the cluster configuration data has failed during the "pre-restore" or "post-restore" stage.

Type of event: Error. Event ID: 1541, 1542, 1543.

Check for the following pre-conditions to make sure they have been met, and then retry the backup or restore operation:

- The cluster must achieve quorum. In other words, enough nodes must be running and communicating (perhaps with a witness disk or witness file share, depending on the quorum configuration) that the cluster has achieved a majority, that is, quorum.
- The account used by the person performing the backup must be in the local Administrators group on each clustered server, and must be a domain account, or must have been delegated the equivalent authority.
- During a restore, the restore software must obtain exclusive access to the cluster configuration database on a given node. If other software has access (open handles to the database), the restore cannot be performed.

Cluster Network Connectivity Problems

This monitor returns the number of events that occur when:

- The Cluster network interface for some cluster node on a special network failed;
- The Cluster network is partitioned and some attached failover cluster nodes cannot communicate with each other over the network;
- The Cluster network is down;
- The Cluster IP address resource failed to come online;
- Attempting to use IPv4 for a special network adapter failed.

Type of event: Warning and Error. Event ID: 1127, 1129, 1130, 1360, 1555.

Run the Validate a Configuration Wizard, selecting only the network tests. Also check network devices (adapters, cables, hubs, switches, etc) and quorum configuration.
Compare the properties of the IP Address resource with the properties of the corresponding network to ensure that the network and subnet information match. If this is an IPv6 resource, make sure that the cluster network for this resource has at least one IPv6 prefix that is not link-local or tunnel.

**Cluster Service Startup Problems**

This monitor returns the number of events that occur when:

- The Cluster service suffered an unexpected fatal error;
- The Cluster service was halted due to incomplete connectivity with other cluster nodes;
- The Cluster service was halted to prevent an inconsistency within the failover cluster;
- The Cluster resource host subsystem (RHS) stopped unexpectedly;
- The Cluster resource either crashed or deadlocked;
- The Cluster service encountered an unexpected problem and will be shut down;
- The Cluster service has prevented itself from starting on this node. (This node does not have the latest copy of cluster configuration data.)
- The membership engine detected that the arbitration process for the quorum device has stalled.

**Type of event:** Error. Event ID: 1000, 1006, 1073, 1146, 1230, 1556, 1561, 1178.

There are various software or hardware related causes that can prevent the Cluster service from starting on a node. Sometimes the Cluster service can restart successfully after it has been interrupted by one of those causes. Review the event logs for indications of the problem.

Check network hardware and configuration. Use the Validate a Configuration Wizard to review the network configuration.

Check to see which resource DLL is causing the issue and report the problem to the resource vendor. Consider configuring the resource to run in its own Resource Monitor. Note that while a problem with a resource DLL will not stop the Cluster service from running, it can prevent other resource DLLs from running unless the resource runs in its own Resource Monitor.

Try starting the Cluster service on all other nodes in the cluster. If the Cluster service can be started on a node with the latest copy of the cluster configuration data, then the node that previously could not be started will probably be able to obtain the latest copy and then join the cluster successfully.

**Cluster Shared Volume Functionality Problems**

This monitor returns the number of events that occur when:

- The Cluster Shared Volume is no longer available on this node;
- The Cluster Shared Volume is no longer directly accessible from this cluster node;
- The Cluster service failed to create the Cluster Shared Volumes root directory;
- The Cluster service failed to set the permissions (ACL) on the Cluster Shared Volumes root directory;
- The Cluster Shared Volume is no longer accessible from this cluster node;
- The Cluster service failed to create a cluster identity token for Cluster Shared Volumes.

**Type of event:** Error. Event ID: 5120, 5121, 5123, 5134, 5135, 5142, 5200.
Review events related to communication with the volume.
Check storage and network configuration.
Check Cluster Shared Volumes folder creation and permissions.
Check communication between domain controllers and nodes.

**Cluster Storage Functionality Problems**

This monitor returns the number of events that occur when:

- The Cluster Physical Disk resource cannot be brought online because the associated disk could not be found;
- While the disk resource was being brought online, access to one or more volumes failed with an error;
- The file system for one or more partitions on the disk for the resource may be corrupt;
- The Cluster disk resource indicates corruption for specific volume;
- The Cluster disk resource contains an invalid mount point.

**Type of event:** Error. Event ID: 1034, 1035, 1037, 1066, 1208.

Confirm that the affected disk is available.
Check the underlying storage hardware and confirm that the device is being presented correctly to the cluster nodes.

If you have problems with partitions on the disk or corruption, we recommend that you run Chkdsk so that it can correct any problems with the file system.

Confirm that the mounted disk is configured according to the following guidelines:

Clustered disks can only be mounted onto clustered disks (not local disks);

The mounted disk and the disk it is mounted onto must be part of the same clustered service or application. They cannot be in two different clustered services or applications, and they cannot be in the general pool of Available Storage in the cluster.

**Cluster Witness Problems**

This monitor returns the number of events that occur when:

- The Cluster service failed to update the cluster configuration data on the witness resource due to resource inaccessibility;
- The Cluster service detected a problem with the witness resource;
- The File Share Witness resource failed a periodic health check;
- The File Share Witness resource failed to come online;
- The File Share Witness resource failed to arbitrate for the specific file share;
- The node failed to form a cluster because the witness was not accessible.

**Type of event:** Error. Event ID: 1557, 1558, 1562, 1563, 1564, 1573.
Confirm witness accessibility by viewing the quorum configuration of a failover cluster and the status of a witness disk.

**Configuration Availability Problems**

This monitor returns the number of events that occur when:

- The cluster configuration database could not be loaded or unloaded;
- The cluster service cannot start due to failed attempts to read configuration data.

**Type of event:** Error. Event ID: 1057, 1090, 1574, 1575, 1593.

When the cluster configuration on a node is missing or corrupt, the Cluster service cannot load the configuration and therefore cannot start. Where possible, the Cluster service will obtain the latest cluster configuration from other nodes in the cluster. Ensure that other nodes are started. If the only node or nodes that can be started appear to have a missing or corrupt cluster configuration database, you will probably need to restore one of the nodes from a system state backup. (For a failover cluster node, the system state backup includes the cluster configuration.) Sometimes when the node attempts to unload the cluster configuration database, the action does not fully complete. Try stopping and restarting the Cluster service. If this does not succeed, restart the operating system on the affected node.

**DFS Namespace Resource Availability Problems**

This monitor returns the number of events that occur when:

- The creation of DFS namespace root failed with error;
- The resynchronization of DFS root target failed with error;
- The cluster file share resource for DFS Namespace cannot be brought online due to error.

**Type of event:** Error. Event ID: 1138, 1141, 1142.

Check DFS namespace configuration.

**Encrypted Settings for Cluster Resource Could not Applied**

This monitor returns the number of events when encrypted settings for a cluster resource could not be successfully applied to the container on this node.

**Type of event:** Error. Event ID: 1121.

Close any application that might have an open handle to the registry checkpoint indicated by the event. This will allow the registry key to be replicated as configured with the resource properties. If necessary, contact the application vendor about this problem. You can use a utility called Handle with the -a option to view handles to the registry.

**Failed to Form Cluster**

This monitor returns the number of Failed to Form cluster events.

**Type of event:** Error. Event ID: 1092, 1009.

You might be able to correct this issue by restarting the Cluster service.
File Share Resource Availability Problems

This monitor returns the number of events that occur when:

- The Cluster File Share cannot be brought online because a file share could not be created;
- The retrieving of information for a specific share returned an error code;
- The retrieving of information for a specific share indicated that the share does not exist;
- The Creation of a file share failed due to an error;
- The Cluster file share resource has detected shared folder conflicts;
- The Cluster file server resource failed a health check because some of its shared folders were inaccessible.

**Type of event:** Warning and Error. Event ID: 1053, 1054, 1055, 1068, 1560, 1585, 1586, 1587, 1588.

Confirm that the share exists and that the permissions allow access to the share.

If possible, determine whether the path to the share has been changed. If so, recreate the share with the correct name.

View all the resources in the clustered file server instance to ensure that they are coming online, and review the dependencies among the resources. Reconfigure as necessary to correct any problems.

Ensure that no two shared folders have the same share name.

Check shared folder accessibility and the State of Server service.

Generic Application Could not be Brought Online

This monitor returns the number of events that occur when a generic application could not be brought online during an attempt to create the process due to; the application not being present on this node, an incorrect path name, or an incorrect binary name.

**Type of event:** Error. Event ID: 1039.

Confirm that the following are true for the application used by the clustered Generic Application instance:

- The application is fully installed on all nodes that are possible owners of the Generic Application resource;
- The configuration for the Generic Application resource specifies the correct application and path;
- The configuration for the Generic Application resource specifies the appropriate parameters and settings for registry replication.

Generic Service Resource Availability Problems

This monitor returns the number of events that occur when:

- The generic service is either not installed or the specified service name is invalid;
- The specified generic service parameters might be invalid;
- The generic service failed with an error.

**Type of event:** Error. Event ID: 1040, 1041, 1042.
Confirm that the correct service is specified in the configuration for the Generic Service resource and confirm that the service is fully installed on all nodes that are possible owners of the resource.

Check service operation and examine the application event log.

**IP address Resource Availability Problems**

This monitor returns the number of events that occur when:

- The Cluster IP address resource cannot be brought online because the subnet mask value is invalid;
- The Cluster IP address resource cannot be brought online because the address value is invalid;
- The configuration data for the network adapter corresponding to the cluster network interface could not be determined;
- The Cluster IP address resource cannot be brought online because a duplicate IP address was detected on the network;
- The Cluster IP address resource cannot be brought online because WINS registration;
- The lease of the IP address associated with the cluster IP address resource has expired or is about to expire, and currently cannot be renewed;
- The IPv6 Tunnel address resource failed to come online because it does not depend on an IP Address (IPv4) resource;
- The Cluster network associated with dependent IP address (IPv4) resource does not support ISATAP tunneling.

**Type of event:** Error. Event ID: 1046, 1047, 1048, 1049, 1078, 1242, 1361, 1363.

Check the address, subnet, and network properties of the IP Address resource.

If the resource is an IPv6 Tunnel address resource, make sure it depends on at least one IP Address (IPv4) resource. Also make sure the network supports Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) tunneling.

If the IP Address resource appears to be configured correctly, check the condition of network adapters and other network components used by the cluster.

**Network Connectivity and Configuration Problems**

This monitor returns the number of events that occur when:

- The Cluster Service was unable to access the network adapter or the cluster node has no network connectivity;
- The Cluster node has no network connectivity;
- The Cluster node has lost all network connectivity;
- The failover cluster virtual adapter failed to initialize the miniport adapter.

**Type of event:** Error. Event ID: 1289, 1553, 1554, 4871.
Correct any problems with the physical network adapters and the cluster virtual adapter. If a previous change in the configuration is interfering with the function of the cluster virtual adapter, it might be necessary to reinstall the failover clustering feature on the node. Also, use the Validate a Configuration Wizard to review the network configuration.

**Node Failed to Join Cluster**

This monitor returns the number of events that occur when the node failed to join the failover cluster due to an error.

*Type of event:* Error. Event ID: 1070.

You might be able to correct this issue by restarting the Cluster service.

**Problems with Cluster Service**

This monitor returns the number of events that occur when:

- The cluster resource in the Clustered service or application failed;
- The Cluster service failed to bring the Clustered service or application completely online or offline and one or more resources may be in a failed state.

*Type of event:* Warning and Error. Event ID: 1039, 1205.

Check and correct any problems with the application or service associated with the resource.

Check and correct any problems with cables or cluster-related devices.

Adjust the properties for the resource in the cluster configuration, especially the value for the Pending Timeout for the resource. This value must allow enough time for the associated application or service to start.

Check the state of all resources in the clustered service or application.

**Quorum was Lost**

This monitor returns the number of events that occur when the Cluster service is shutting down because quorum was lost.

*Type of event:* Error. Event ID: 1177.

This can occur when network connectivity is lost between some or all of the nodes in the cluster, or the witness disk fails over. It can also occur if you make a change in the cluster configuration such as increasing the number of nodes, when the number of nodes currently online is too few to achieve quorum in the new configuration. Run the Validate a Configuration Wizard, selecting only the network tests. Also check network devices (adapters, cables, hubs, switches, etc.) and quorum configuration.

**Registry Checkpoint Could not be Restored to Registry Key**

This monitor returns the number of events that occur when the Registry Checkpoint for Cluster resource could not be restored to a registry key.

*Type of event:* Error. Event ID: 1024.
Close any application that might have an open handle to the registry checkpoint indicated by the event. This will allow the registry key to be replicated as configured with the resource properties. If necessary, contact the application vendor about this problem. You can use a utility called Handle with the -a option to view handles to the registry.

**System is not being Responsive**

This monitor returns the number of events that occur when the Failover cluster virtual adapter has lost contact with the process.

**Type of event:** Error. Event ID: 4869, 4870.

Use Resource Monitor to determine, in real time, how many system resources a service or application is utilizing. This may take several minutes if the system is critically low on resources.

### Microsoft Windows Server 2008 R2-2016 Failover Cluster (Advanced)

This template assesses the status and overall performance of a Microsoft Windows Server 2008 R2-2016 Failover Cluster by using PowerShell scripts.

**Prerequisites**

WinRM must be installed and properly configured on the target server.

**Credentials**

Windows Administrator on the target server.

Tips: Periodically, SolarWinds releases SAM templates to support the latest product versions such as Microsoft Server 2016. You can continue using templates for older product versions, but updating to the latest template is recommended.

**Monitored Components**

For details on monitors, see [SAM Component Monitor Types](#).

**Cluster Groups State**

This monitor returns the number of cluster resource groups in different states: Online, Offline, and Other states.

**Cluster Networks State**

This monitor returns the number of cluster networks in different states: Up, Down, and Other states.

**Cluster Network Interfaces State**

This monitor returns the number of cluster network interfaces in different states: Up, Down,
and Other states.

**Cluster Nodes**

This monitor returns the number of cluster nodes in different states: Up, Down, and Other states.

**Cluster Shared Volumes**

This monitor returns the number of cluster shared volumes in different states: Online, Offline, and Other states.

---

**Microsoft Windows Server 2012 - 2016 Failover Cluster**

This template assesses the status and overall performance of a Microsoft Windows 2012 - 2016 Failover Cluster by retrieving information from performance counters and the Windows System Event Log.

**Prerequisites**

WMI access to the target server.

**Credentials**

Windows Administrator on the target server.

---

**Monitored Components**

For details on monitors, see [SAM Component Monitor Types](#).

You need to set thresholds for counters according to your environment. It is recommended to monitor counters for some period of time to understand potential value ranges and then set the thresholds accordingly.

**Service: Windows Time**

This monitor returns the CPU and memory usage of the Windows Time service. This service maintains date and time synchronization on all clients and servers in the network. If this service is stopped, date and time synchronization will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

**Service: Cluster Service**

This monitor returns the CPU and memory usage of the Cluster service. This service enables
servers to work together as a cluster to keep server-based applications highly available, regardless of individual component failures. If this service is stopped, clustering will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

**Network Reconnections: Reconnect Count**

This monitor returns the number of times the nodes have reconnected.

The instance field is installation-specific. You need to specify the hostname of your cluster node (for example: node1). By default, this component monitor is disabled and should only be enabled for troubleshooting purposes.

**Network Reconnections: Normal Message Queue Length**

This monitor returns the number of normal messages that are in the queue waiting to be sent. Normally this number is 0, but if the TCP connection breaks, you might observe it going up until the TCP connection is re-established and we can send all of them through.

The instance field is installation-specific. You need to specify the hostname of your cluster node (for example: node1). By default, this component monitor is disabled and should only be enabled for troubleshooting purposes.

**Network Reconnections: Urgent Message Queue Length**

This monitor returns the number of urgent messages that are in the queue waiting to be sent. Normally this number is 0, but if the TCP connection breaks, you might observe it going up until the TCP connection is re-established, thereby allowing all messages to be sent.

The instance field is installation-specific. You need to specify the hostname of your cluster node (for example: node1). By default, this component monitor is disabled and should only be enabled for troubleshooting purposes.

**Messages Outstanding**

This monitor returns the number of cluster MRR outstanding messages. The returned value should be near zero.

**Resource Control Manager: Groups Online**

This monitor returns the number of online cluster resource groups on this node. The returned value should be above zero at all times.

**Resource Control Manager: RHS Processes**

This monitor returns the number of running resource host subsystem processes (rhs.exe). The returned value should be above zero at all times.

**Resource Control Manager: RHS Restarts**

This monitor returns the number of resource host subsystem process (rhs.exe) restarts.

By default, this component monitor is disabled and should only be enabled for troubleshooting purposes.
Resources: Resource Failure
This monitor returns the number of resource failures. The returned value should be as low as possible.

Resources: Resource Failure Access Violation
This monitor returns the number of resource failures caused by access violation. The returned value should be as low as possible.

By default, this component monitor is disabled and should only be enabled for troubleshooting purposes.

Resources: Resource Failure Deadlock
This monitor returns the number of resource failures caused by deadlock. Deadlocks are usually caused by the resource taking too long to execute certain operations. The returned value should be as low as possible.

By default, this component monitor is disabled and should only be enabled for troubleshooting purposes.

Network Messages: Bytes Received/sec
The Bytes Received/sec performance counter shows the number of new cluster message bytes received on the network per second.

Network Messages: Bytes Sent/sec
The Bytes Sent/sec performance counter shows the number of new cluster message bytes sent over the network per second.

Network Messages: Messages Received/sec
The Messages Received/sec performance counter shows the number of new cluster messages received on the network per second.

Network Messages: Messages Sent/sec
The Messages Sent/sec performance counter shows the number of new cluster messages sent over the network per second.

Global Update: Average Database Messages Execution Time
The Average Database Messages Execution Time performance counter shows the average time the database messages are executed across all nodes.

Global Update: Average Messages Execution Time
The Average Messages Execution Time performance counter shows the average time the messages are executed across all nodes.

Global Update: Database Messages Queue Length
The Database Messages Queue Length performance counter shows the number of new cluster
database update messages waiting to be sent over the network.

**Backup and Restore Functionality Problems**

This monitor returns the number of events that occur when:

- The backup operation for the cluster configuration data has been aborted because quorum for the cluster has not yet been achieved;
- The restore request for the cluster configuration data has failed during the "pre-restore" or "post-restore" stage.

Type of event: Error. Event ID: 1541, 1542, 1543.

Check for the following pre-conditions to make sure they have been met, and then retry the backup or restore operation:

- The cluster must achieve quorum. In other words, enough nodes must be running and communicating (perhaps with a witness disk or witness file share, depending on the quorum configuration) that the cluster has achieved a majority, that is, quorum.
- The account used by the person performing the backup must be in the local Administrators group on each clustered server, and must be a domain account, or must have been delegated the equivalent authority.

During a restore, the restore software must obtain exclusive access to the cluster configuration database on a given node. If other software has access (open handles to the database), the restore cannot be performed.

**Cluster Network Connectivity Problems**

This monitor returns the number of events that occur when:

- The Cluster network interface for some cluster node on a special network failed;
- The Cluster network is partitioned and some attached failover cluster nodes cannot communicate with each other over the network;
- The Cluster network is down;
- The Cluster IP address resource failed to come online;
- Attempting to use IPv4 for a special network adapter failed.

Type of event: Warning and Error. Event ID: 1127, 1129, 1130, 1360, 1555.

Run the Validate a Configuration Wizard, selecting only the network tests. Also check network devices ( adapters, cables, hubs, switches, etc) and quorum configuration.

Compare the properties of the IP Address resource with the properties of the corresponding network to ensure that the network and subnet information match. If this is an IPv6 resource, make sure that the cluster network for this resource has at least one IPv6 prefix that is not link-local or tunnel.

**Cluster Service Startup Problems**

This monitor returns the number of events that occur when:

- The Cluster service suffered an unexpected fatal error;
- The Cluster service was halted due to incomplete connectivity with other cluster nodes;
• The Cluster service was halted to prevent an inconsistency within the failover cluster;
• The Cluster resource host subsystem (RHS) stopped unexpectedly;
• The Cluster resource either crashed or deadlocked;
• The Cluster service encountered an unexpected problem and will be shut down;
• The Cluster service has prevented itself from starting on this node. (This node does not have the latest copy of cluster configuration data.)
• The membership engine detected that the arbitration process for the quorum device has stalled.

Type of event: Error. Event ID: 1000, 1006, 1073, 1146, 1230, 1556, 1561, 1178.

There are various software or hardware related causes that can prevent the Cluster service from starting on a node. Sometimes the Cluster service can restart successfully after it has been interrupted by one of those causes. Review the event logs for indications of the problem.

• Check network hardware and configuration. Use the Validate a Configuration Wizard to review the network configuration.
• Check to see which resource DLL is causing the issue and report the problem to the resource vendor. Consider configuring the resource to run in its own Resource Monitor. Note that while a problem with a resource DLL will not stop the Cluster service from running, it can prevent other resource DLLs from running unless the resource runs in its own Resource Monitor.
• Try starting the Cluster service on all other nodes in the cluster. If the Cluster service can be started on a node with the latest copy of the cluster configuration data, then the node that previously could not be started will probably be able to obtain the latest copy and then join the cluster successfully.

**Cluster Shared Volume Functionality Problems**

This monitor returns the number of events that occur when:

• The Cluster Shared Volume is no longer available on this node;
• The Cluster Shared Volume is no longer directly accessible from this cluster node;
• The Cluster service failed to create the Cluster Shared Volumes root directory;
• The Cluster service failed to set the permissions (ACL) on the Cluster Shared Volumes root directory;
• The Cluster Shared Volume is no longer accessible from this cluster node;
• The Cluster service failed to create a cluster identity token for Cluster Shared Volumes.

Type of event: Error. Event ID: 5120, 5121, 5123, 5134, 5135, 5142, 5200.

Review events related to communication with the volume.

• Check storage and network configuration.
• Check Cluster Shared Volumes folder creation and permissions.
• Check communication between domain controllers and nodes.

**Cluster Storage Functionality Problems**

This monitor returns the number of events that occur when:
The Cluster Physical Disk resource cannot be brought online because the associated disk could not be found;
While the disk resource was being brought online, access to one or more volumes failed with an error;
The file system for one or more partitions on the disk for the resource may be corrupt;
The Cluster disk resource indicates corruption for specific volume;
The Cluster disk resource contains an invalid mount point.

Type of event: Error. Event ID: 1034, 1035, 1037, 1066, 1208.

- Confirm that the affected disk is available.
- Check the underlying storage hardware and confirm that the device is being presented correctly to the cluster nodes.
- If you have problems with partitions on the disk or corruption, we recommend that you run Chkdsk so that it can correct any problems with the file system.
- Confirm that the mounted disk is configured according to the following guidelines:
- Clustered disks can only be mounted onto clustered disks (not local disks);

The mounted disk and the disk it is mounted onto must be part of the same clustered service or application. They cannot be in two different clustered services or applications, and they cannot be in the general pool of Available Storage in the cluster.

**Cluster Witness Problems**

This monitor returns the number of events that occur when:

- The Cluster service failed to update the cluster configuration data on the witness resource due to resource inaccessibility;
- The Cluster service detected a problem with the witness resource;
- The File Share Witness resource failed a periodic health check;
- The File Share Witness resource failed to come online;
- The File Share Witness resource failed to arbitrate for the specific file share;
- The node failed to form a cluster because the witness was not accessible.

Type of event: Error. Event ID: 1557, 1558, 1562, 1563, 1564, 1573.

- Confirm witness accessibility by viewing the quorum configuration of a failover cluster and the status of a witness disk.

**Configuration Availability Problems**

This monitor returns the number of events that occur when:

- The cluster configuration database could not be loaded or unloaded;
- The cluster service cannot start due to failed attempts to read configuration data.

Type of event: Error. Event ID: 1057, 1090, 1574, 1575, 1593.
When the cluster configuration on a node is missing or corrupt, the Cluster service cannot load the configuration and therefore cannot start. Where possible, the Cluster service will obtain the latest cluster configuration from other nodes in the cluster. Ensure that other nodes are started. If the only node or nodes that can be started appear to have a missing or corrupt cluster configuration database, you will probably need to restore one of the nodes from a system state backup. (For a failover cluster node, the system state backup includes the cluster configuration.) Sometimes when the node attempts to unload the cluster configuration database, the action does not fully complete. Try stopping and restarting the Cluster service. If this does not succeed, restart the operating system on the affected node.

**DFS Namespace Resource Availability Problems**

This monitor returns the number of events that occur when:

- The creation of DFS namespace root failed with error;
- The resynchronization of DFS root target failed with error;
- The cluster file share resource for DFS Namespace cannot be brought online due to error.

Type of event: Error. Event ID: 1138, 1141, 1142.

- Check DFS namespace configuration.
- Encrypted Settings for Cluster Resource Could not Applied

This monitor returns the number of events when encrypted settings for a cluster resource could not be successfully applied to the container on this node.

Type of event: Error. Event ID: 1121.

Close any application that might have an open handle to the registry checkpoint indicated by the event. This will allow the registry key to be replicated as configured with the resource properties. If necessary, contact the application vendor about this problem. You can use a utility called Handle with the -a option to view handles to the registry.

**Failed to Form Cluster**

This monitor returns the number of Failed to Form cluster events.

Type of event: Error. Event ID: 1092, 1009.

You might be able to correct this issue by restarting the Cluster service.

**File Share Resource Availability Problems**

This monitor returns the number of events that occur when:

- The Cluster File Share cannot be brought online because a file share could not be created;
- The retrieving of information for a specific share returned an error code;
- The retrieving of information for a specific share indicated that the share does not exist;
- The Creation of a file share failed due to an error;
- The Cluster file share resource has detected shared folder conflicts;
The Cluster file server resource failed a health check because some of its shared folders were inaccessible.

Type of event: Warning and Error. Event ID: 1053, 1054, 1055, 1068, 1560, 1585, 1586, 1587, 1588.

- Confirm that the share exists and that the permissions allow access to the share.
- If possible, determine whether the path to the share has been changed. If so, recreate the share with the correct name.
- View all the resources in the clustered file server instance to ensure that they are coming online, and review the dependencies among the resources. Reconfigure as necessary to correct any problems.
- Ensure that no two shared folders have the same share name.
- Check shared folder accessibility and the State of Server service.

**Generic Application Could not be Brought Online**

This monitor returns the number of events that occur when a generic application could not be brought online during an attempt to create the process due to; the application not being present on this node, an incorrect path name, or an incorrect binary name.

Type of event: Error. Event ID: 1039.

- Confirm that the following are true for the application used by the clustered Generic Application instance:
  - The application is fully installed on all nodes that are possible owners of the Generic Application resource;
  - The configuration for the Generic Application resource specifies the correct application and path;
  - The configuration for the Generic Application resource specifies the appropriate parameters and settings for registry replication.

**Generic Service Resource Availability Problems**

This monitor returns the number of events that occur when:

- The generic service is either not installed or the specified service name is invalid;
- The specified generic service parameters might be invalid;
- The generic service failed with an error.

Type of event: Error. Event ID: 1040, 1041, 1042.

- Confirm that the correct service is specified in the configuration for the Generic Service resource and confirm that the service is fully installed on all nodes that are possible owners of the resource.
- Check service operation and examine the application event log.

**IP address Resource Availability Problems**

This monitor returns the number of events that occur when:
• The Cluster IP address resource cannot be brought online because the subnet mask value is invalid;
• The Cluster IP address resource cannot be brought online because the address value is invalid;
• The configuration data for the network adapter corresponding to the cluster network interface could not be determined;
• The Cluster IP address resource cannot be brought online because a duplicate IP address was detected on the network;
• The Cluster IP address resource cannot be brought online because WINS registration;
• The lease of the IP address associated with the cluster IP address resource has expired or is about to expire, and currently cannot be renewed;
• The IPv6 Tunnel address resource failed to come online because it does not depend on an IP Address (IPv4) resource;
• The Cluster network associated with dependent IP address (IPv4) resource does not support ISATAP tunneling.

Type of event: Error. Event ID: 1046, 1047, 1048, 1049, 1078, 1242, 1361, 1363.

• Check the address, subnet, and network properties of the IP Address resource.
• If the resource is an IPv6 Tunnel address resource, make sure it depends on at least one IP Address (IPv4) resource. Also make sure the network supports Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) tunneling.
• If the IP Address resource appears to be configured correctly, check the condition of network adapters and other network components used by the cluster.

**Network Connectivity and Configuration Problems**

This monitor returns the number of events that occur when:

• The Cluster Service was unable to access the network adapter or the cluster node has no network connectivity;
• The Cluster node has no network connectivity;
• The Cluster node has lost all network connectivity;
• The failover cluster virtual adapter failed to initialize the miniport adapter.

Type of event: Error. Event ID: 1289, 1553, 1554, 4871.

Correct any problems with the physical network adapters and the cluster virtual adapter. If a previous change in the configuration is interfering with the function of the cluster virtual adapter, it might be necessary to reinstall the failover clustering feature on the node. Also, use the Validate a Configuration Wizard to review the network configuration.

**Node Failed to Join Cluster**

This monitor returns the number of events that occur when the node failed to join the failover cluster due to an error.

Type of event: Error. Event ID: 1070.

You might be able to correct this issue by restarting the Cluster service.
Problems with Cluster Service

This monitor returns the number of events that occur when:

- The cluster resource in the Clustered service or application failed;
- The Cluster service failed to bring the Clustered service or application completely online or offline and one or more resources may be in a failed state.

Type of event: Warning and Error. Event ID: 1039, 1205.

- Check and correct any problems with the application or service associated with the resource.
- Check and correct any problems with cables or cluster-related devices.
- Adjust the properties for the resource in the cluster configuration, especially the value for the Pending Timeout for the resource. This value must allow enough time for the associated application or service to start.
- Check the state of all resources in the clustered service or application.

Quorum was Lost

This monitor returns the number of events that occur when the Cluster service is shutting down because quorum was lost.

Type of event: Error. Event ID: 1177.

This can occur when network connectivity is lost between some or all of the nodes in the cluster, or the witness disk fails over. It can also occur if you make a change in the cluster configuration such as increasing the number of nodes, when the number of nodes currently online is too few to achieve quorum in the new configuration. Run the Validate a Configuration Wizard, selecting only the network tests. Also check network devices (adapters, cables, hubs, switches, etc.) and quorum configuration.

Registry Checkpoint Could not be Restored to Registry Key

This monitor returns the number of events that occur when the Registry Checkpoint for Cluster resource could not be restored to a registry key.

Type of event: Error. Event ID: 1024.

Close any application that might have an open handle to the registry checkpoint indicated by the event. This will allow the registry key to be replicated as configured with the resource properties. If necessary, contact the application vendor about this problem. You can use a utility called Handle with the -a option to view handles to the registry.

System is not being Responsive

This monitor returns the number of events that occur when the Failover cluster virtual adapter has lost contact with the process.

Type of event: Error. Event ID: 4869, 4870.

Use Resource Monitor to determine, in real time, how many system resources a service or application is utilizing. This may take several minutes if the system is critically low on resources.
Microsoft Windows Server 2012 Failover Cluster

This template assesses the status and overall performance of a Microsoft Windows 2012 Failover Cluster by retrieving information from performance counters and the Windows System Event Log.

Prerequisites

WMI access to the target server.

Credentials

Windows Administrator on the target server.

- All Windows Event Log monitors should return zero values. Returned values other than zero indicate an abnormality. Examining the Windows system log files should provide information pertaining to the issue.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

You need to set thresholds for counters according to your environment. It is recommended to monitor counters for some period of time to understand potential value ranges and then set the thresholds accordingly.

Service: Windows Time

This monitor returns the CPU and memory usage of the Windows Time service. This service maintains date and time synchronization on all clients and servers in the network. If this service is stopped, date and time synchronization will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

Service: Cluster Service

This monitor returns the CPU and memory usage of the Cluster service. This service enables servers to work together as a cluster to keep server-based applications highly available, regardless of individual component failures. If this service is stopped, clustering will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

Network Reconnections: Reconnect Count

This monitor returns the number of times the nodes have reconnect.

The instance field is installation-specific. You need to specify the hostname of your cluster node (for example: node1). By default, this component monitor is disabled and should only be enabled for troubleshooting purposes.
Network Reconnections: Normal Message Queue Length
This monitor returns the number of normal messages that are in the queue waiting to be sent. Normally this number is 0, but if the TCP connection breaks, you might observe it going up until the TCP connection is re-established and we can send all of them through.

The instance field is installation-specific. You need to specify the hostname of your cluster node (for example: node1). By default, this component monitor is disabled and should only be enabled for troubleshooting purposes.

Network Reconnections: Urgent Message Queue Length
This monitor returns the number of urgent messages that are in the queue waiting to be sent. Normally this number is 0, but if the TCP connection breaks, you might observe it going up until the TCP connection is re-established, thereby allowing all messages to be sent.

The instance field is installation-specific. You need to specify the hostname of your cluster node (for example: node1). By default, this component monitor is disabled and should only be enabled for troubleshooting purposes.

Messages Outstanding
This monitor returns the number of cluster MRR outstanding messages. The returned value should be near zero.

Resource Control Manager: Groups Online
This monitor returns the number of online cluster resource groups on this node. The returned value should be above zero at all times.

Resource Control Manager: RHS Processes
This monitor returns the number of running resource host subsystem processes (rhs.exe). The returned value should be above zero at all times.

Resource Control Manager: RHS Restarts
This monitor returns the number of resource host subsystem process (rhs.exe) restarts.

By default, this component monitor is disabled and should only be enabled for troubleshooting purposes.

Resources: Resource Failure
This monitor returns the number of resource failures. The returned value should be as low as possible.

Resources: Resource Failure Access Violation
This monitor returns the number of resource failures caused by access violation. The returned value should be as low as possible.

By default, this component monitor is disabled and should only be enabled for troubleshooting purposes.
Resources: Resource Failure Deadlock

This monitor returns the number of resource failures caused by deadlock. Deadlocks are usually caused by the resource taking too long to execute certain operations. The returned value should be as low as possible.

By default, this component monitor is disabled and should only be enabled for troubleshooting purposes.

Microsoft Windows 2016 FTP service

This template assesses the status and overall of services and performance of a Microsoft Windows 2016 FTP service.

Prerequisites

WMI access to the target server.

Credentials

Windows Administrator on the target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

You should manually enter thresholds for component monitors according to your requirements.

Microsoft FTP Service

This monitor returns CPU and memory usage for the Microsoft FTP Service, which enables this server to be a File Transfer Protocol (FTP) server. If this service is stopped, the server cannot function as an FTP server. If this service is disabled, any services that explicitly depend on it will fail to start.

FTP User Experience Monitor

This component monitor tests the ability of an FTP server to accept an incoming session, process the user login, and then transmit the specified file to the SAM server. After receiving the file, SAM performs a file integrity test comparing the MD5 checksum of the downloaded file against a previously generated checksum. If the checksums match, the component monitor reports its status as up.

This monitor should be properly configured before using it on the target FTP server. By default this monitor is disabled.

Bytes Received/sec

This monitor returns the number of bytes received per second by the FTP service.
**Bytes Sent/sec**

This monitor returns the number of bytes sent per second by the FTP service.

**Current Anonymous Users**

This monitor returns the number of users who currently have an anonymous connection using the FTP service.

**Current Connections**

This monitor returns the current number of connections established with the FTP service.

**Current Non-Anonymous Users**

This monitor returns the number of users who currently have a non-anonymous connection using the FTP service.

**Total Connection Attempts**

This monitor returns the number of connections that have attempted to use the FTP service since service startup. This counter is for all instances listed.

> ! This counter has the Count statistic as difference option enabled and will show the statistical difference from the last polling cycle.

**Total Files Received**

This monitor returns the total number of files received by the FTP service since service startup.

> ! This counter has the Count statistic as difference option enabled and will show the statistical difference from the last polling cycle.

**Total Files Sent**

This monitor returns the total number of files sent by the FTP service since service startup.

> ! This counter has the Count statistic as difference option enabled and will show the statistical difference from the last polling cycle.

**Total Files Transferred**

This monitor returns the total number of files transferred by the FTP service since service startup.

> ! This counter has the Count statistic as difference option enabled and will show the statistical difference from the last polling cycle.

**Windows Update Monitoring**

This template allows you to check the status of Windows' updates. It monitors how many updates are available and how many updates are installed. It also checks if a reboot is required before or after the installation of updates. It also monitors the number of reboots that have passed since the last update is also monitored.
Prerequisites

WinRM must be installed and properly configured on the target server.

Credentials

Administrator on target server.

Configuring Windows Remote Management (WinRM)

Take the following steps to properly configure Windows Remote Management:

1. If not already done so, install PowerShell 2.0 or later and WinRM on the SAM and target servers. PowerShell 2.0 can be found here: [http://support.microsoft.com/kb/968930](http://support.microsoft.com/kb/968930). (© 2018 Microsoft Corp., link available at https://docs.microsoft.com, obtained on October 30, 2018)

2. On the SAM server, open a command prompt as an Administrator. To do this, go to the Start menu and right-click the cmd.exe and then select Run as Administrator.

3. Enter the following in the command prompt:

   ```
   winrm quickconfig
   winrm set winrm/config/client @{TrustedHosts="*"}
   ```

4. On the target server, open a command prompt as an Administrator and enter the following:

   ```
   winrm quickconfig
   winrm set winrm/config/client @{TrustedHosts="IP_ADDRESS"}
   ```
   
   where IP address is the IP address of your SAM server.

Monitored Components

For details on monitors, see [SAM Component Monitor Types](#).

Available hidden updates

This component monitor returns the number of available hidden updates.

Available critical updates

This component monitor returns the number of available critical updates. This should always be zero.

Available optional updates

This component monitor returns the number of available optional updates.

Installed updates

This component monitor returns the number of installed updates.

Days passed from last Windows Update

This component monitor returns the number of days that have passed from the last Windows update installation. Additionally, this component returns the name of the last installed update.

Windows Updates activity status

This component monitor returns the installation status of Windows update.
Possible values:

- 0 – Windows currently is not installing updates.
- 1 – Windows currently is installing updates.

Machine restart status before installing Windows Updates

This component monitor shows the restart status before installing Windows updates.

Possible values:

- 0 – No reboot requires.
- 1 – Reboot required before installing updates.

Machine restart status after installing Windows Updates

This component monitor shows the restart status after installing Windows updates.

Possible values:

- 0 – No reboot requires.
- 1 – Updates installed. Reboot required.

Service: Windows Updates

This component monitors the Windows update service which enables the detection, download, and installation of updates for Windows and other programs. If this service is disabled, users of this computer will not be able to use Windows update or its automatic updating feature. If this service is down, programs will not be able to use the Windows Update Agent (WUA) API.

Windows 2008 R2 - 2012 FTP Service

This template assesses the status and overall of services and performance of a Microsoft Windows 2008 R2 - 2012 FTP service.

Prerequisites

WMI access to the target server.

Credentials

Windows Administrator on the target server.

Monitored Components

For details on monitors, see [SAM Component Monitor Types](#).

You should manually enter thresholds for component monitors according to your requirements.
Microsoft FTP Service

This monitor returns CPU and memory usage for the Microsoft FTP Service, which enables this server to be a File Transfer Protocol (FTP) server. If this service is stopped, the server cannot function as an FTP server. If this service is disabled, any services that explicitly depend on it will fail to start.

FTP User Experience Monitor

This component monitor tests the ability of an FTP server to accept an incoming session, process the user login, and then transmit the specified file to the SAM server. After receiving the file, SAM performs a file integrity test comparing the MD5 checksum of the downloaded file against a previously generated checksum. If the checksums match, the component monitor reports its status as up.

1. This monitor should be properly configured before using it on the target FTP server. By default this monitor is disabled.

Bytes Received/sec

This monitor returns the number of bytes received per second by the FTP service.

Bytes Sent/sec

This monitor returns the number of bytes sent per second by the FTP service.

Current Anonymous Users

This monitor returns the number of users who currently have an anonymous connection using the FTP service.

Current Connections

This monitor returns the current number of connections established with the FTP service.

Current Non-Anonymous Users

This monitor returns the number of users who currently have a non-anonymous connection using the FTP service.

Total Connection Attempts

This monitor returns the number of connections that have attempted to use the FTP service since service startup. This counter is for all instances listed.

1. This counter has the Count statistic as difference option enabled and will show the statistical difference from the last polling cycle.

Total Files Received

This monitor returns the total number of files received by the FTP service since service startup.

1. This counter has the Count statistic as difference option enabled and will show the statistical difference from the last polling cycle.
Total Files Sent

This monitor returns the total number of files sent by the FTP service since service startup.

This counter has the Count statistic as difference option enabled and will show the statistical difference from the last polling cycle.

Total Files Transferred

This monitor returns the total number of files transferred by the FTP service since service startup.

This counter has the Count statistic as difference option enabled and will show the statistical difference from the last polling cycle.

Microsoft Windows DHCP Server

This template assesses the status and overall health of services and performance of a Microsoft Windows DHCP server.

Periodically, SolarWinds releases SAM templates to support the latest product versions such as Microsoft Server 2016. You can continue using templates for older product versions, but updating to the latest template is recommended.

Prerequisites

WMI access to the target server.

Credentials

Windows Administrator on the target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

You need to set thresholds for counters according to your environment. It is recommended that you monitor counters for a length of time to understand potential value ranges and then set the thresholds accordingly.

All Windows Event Log monitors (beginning with Warning or Error) should return zero values. Returned values other than zero indicate an abnormality. Examining the Windows System log file should provide information pertaining to the issue.

Packets Received/sec

This component monitor returns the rate at which packets are received by the DHCP server.

A high value indicates heavy DHCP-related message traffic to the server.

Duplicates Dropped/sec

This component monitor returns the rate at which the DHCP server received duplicate packets.
A high value indicates that clients are probably timing out too fast or that the server is taking a great deal of time to respond.

**Packets Expired/sec**

This component monitor returns the rate at which packets expire in the DHCP server message queue. Packets expire because they are in the server's internal message queue too long.

A large number indicates that the server is either taking too long to process some packets while other packets are queued and becoming stale, or traffic on the network is too high for the DHCP server to handle. This suggests either a disk or memory bottleneck.

**Milliseconds per Packet (Avg)**

This component monitor returns the average time per packet taken by the DHCP server to send a response.

This number can vary depending upon the server hardware and its I/O subsystem. A sudden or unreasonable increase may indicate a problem, either with the I/O subsystem slowing or because of intrinsic processing overhead on the server computer.

**Active Queue Length**

This component monitor returns the number of packets in the processing queue of the DHCP server. This number equals the number of unprocessed messages received by the server.

A high value may indicate heavy server traffic.

**Conflict Check Queue Length**

This component monitor returns the number of packets waiting in the DHCP server queue due to conflict detection. This queue holds messages that have not been responded to while the DHCP server performs address conflict detection.

A high value may indicate that conflict detection attempts have been set too high in DHCP server properties or that there is heavy lease traffic at the server.

**Discovers/sec**

This component monitor returns the rate at which DHCP Discovers have been received by the DHCP server.

A sudden or abnormal increase indicates that a large number of clients are probably attempting to initialize and obtain an IP address lease from the server. This may indicate that a number of client computers are started at one time.

**Offers/sec**

This component monitor returns the rate at which DHCP Offers have been sent out by the DHCP server.

A sudden or abnormal increase in this value indicates heavy traffic on the server.
Requests/sec

This component monitor returns the rate at which DHCP Requests have been received by the DHCP server.

A sudden or abnormal increase in this value may indicate a large number of clients trying to renew their leases with the DHCP server. This may indicate that scope lease times are too short.

Informs/sec

This component monitor returns the rate at which DHCP Informs have been received by the DHCP server.

DHCP inform messages are used when the DHCP server queries the directory service for the enterprise root and when dynamic updates are being done on behalf of clients by the server.

Acks/sec

This component monitor returns the rate at which DHCP Acknowledgements have been sent by the DHCP server.

A sudden or abnormal increase in this number indicates that a large number of clients are being renewed by the DHCP server. This may indicate that scope lease times are too short.

Nacks/sec

This component monitor returns the rate at which DHCP negative acknowledgments (Nacks) have been sent by the DHCP server.

A high value may indicate potential network problems such as misconfiguration of clients or the server. One possible cause of server problems is a deactivated scope. For clients, a very high value could be caused by computers moving between subnets, such as laptop portables or other mobile devices.

Declines/sec

This component monitor returns the rate at which DHCP Declines have been received by the DHCP server.

A high value indicates that several clients have found their address to be in conflict, possibly indicating network trouble. It may help to enable conflict detection on the DHCP server. Conflict detection should only be used temporarily on the server.

Releases/sec

This component monitor returns the rate at which DHCP Releases have been received by the DHCP server.

This number is only incremented when clients manually release their address, such as when the ipconfig/release command is used at the client computer. Because clients rarely release their address, this counter should not be high for most networks and configurations.
Service: DHCP Server

This component monitor performs TCP/IP configuration for DHCP clients, including dynamic assignments of IP addresses, specification of the WINS and DNS servers, and connection-specific DNS names. If this service is stopped or disabled, the DHCP server will not perform TCP/IP configuration for clients and any services that explicitly depend on it will fail to start.

DHCP User Experience Monitor

This component monitor measures the time it takes to get a lease from a DHCP server. The monitor verifies that the DHCP responds with an IP address, but neither confirms nor accepts the lease.

Warning: Jet Database Error

This component monitors events when a problem occurs with the Jet database.

Type of event: Warning. Event ID: 1014.

If the DHCP server database becomes corrupted or is lost, you should restore your backup database file. More information can be found here: http://technet.microsoft.com/en-us/library/cc726907(WS.10).aspx.

Error: DHCP Server is Shutting Down with Error

This component monitors events when the DHCP Server service is shutting down due to an error.

Type of event: Error. Event ID: 1008.

The Dynamic Host Configuration Protocol (DHCP) Server service is dependent on these services: Service Controller, Global parameters initialization, Registry parameters initialization, RPC server start, Winsock data initialization. The failure of any of these services to initialize or start can cause the DHCP Server service to fail.


Error: Failed to Restore Database

This component monitors events when the DHCP service failed to restore the database.

Type of event: Error. Event ID: 1018.

If the DHCP server database becomes corrupted or is lost, you should restore your backup database file. More information can be found here: http://technet.microsoft.com/en-us/library/cc726880(WS.10).aspx.

Error: Failed to Initialize Database

This component monitors events when the DHCP service failed to initialize the database.

Type of event: Error. Event ID: 1004.

If the DHCP server database becomes corrupted or is lost you should restore your backup database file. More information can be found here: http://technet.microsoft.com/en-us/library/cc726910(WS.10).aspx.
Warning: Server Scope is Almost Full

This component monitors events when the server scope is almost full and there are few free IP addresses left.

**Type of event:** Warning. Event ID: 1020.

If the DHCP server does not have IP addresses available to provide to the requesting client, then the request fails, and the client might not be able to communicate with other computers on the network.

To resolve this issue, you can extend the DHCP scopes or reduce the lease duration. More information can be found here: [http://social.technet.microsoft.com/wiki/contents/articles/event-id-1020-microsoft-windows-dhcp-server.aspx](http://social.technet.microsoft.com/wiki/contents/articles/event-id-1020-microsoft-windows-dhcp-server.aspx).

Error: Server Scope is Full

This component monitors events when there are no IP addresses available for lease in the scope or super-scope.

**Type of event:** Error. Event ID: 1063.

If the DHCP server does not have IP addresses available to provide to the requesting client, then the request fails, and the client might not be able to communicate with other computers on the network.


Windows DNS Server

This template assesses the status and overall health of services and performance of a Microsoft DNS server.

**Prerequisites**

- WMI access to the target server.

**Credentials**

- Windows Administrator on the target server.

**Monitored Components**

For details on monitors, see [SAM Component Monitor Types](#).

You need to set thresholds for counters according to your environment. It is recommended to monitor counters for some length of time to understand potential value ranges and then set the thresholds accordingly.

**Service: DNS Server**

This component monitor enables DNS clients to resolve DNS names by answering DNS queries and dynamic DNS update requests. If this service is stopped or disabled, DNS updates will not occur and any services that explicitly depend on it will fail to start.
Memory: Caching Memory

This component monitor returns the total amount of system memory in use by the DNS Server service for caching.

Monitor this counter to determine whether cache use is optimizing the use of available memory.

Memory: Database Node Memory

This component monitor returns the total amount of system memory in use by the DNS Server service for database nodes.

Memory: Nbstat Memory

This component monitor returns the total amount of system memory in use by the DNS Server service for Nbtstat.

Memory: Record Flow Memory

This component monitor returns the total amount of system memory in use by the DNS Server service for record flow.

Dynamic Update: NoOperation/sec

This component monitor returns the average number of No-operation/Empty dynamic update requests received by the DNS server per second.

Dynamic Update: Received

This component monitor returns the total number of dynamic update requests received by the DNS server.

Monitor this counter after enabling dynamic updates to determine whether DNS clients are attempting to update their DNS addresses.

Dynamic Update: Rejected

This component monitor returns the total number of dynamic updates rejected by the DNS server.

Monitor this counter and compare this value against Dynamic Update: Received to determine how many systems are experiencing problems updating DNS addresses.

Dynamic Update: TimeOuts

This component monitor returns the total number of dynamic update time-outs of the DNS server.

Dynamic Update: Written to Database

This component monitor returns the total number of dynamic updates written to the database by the DNS server.

Monitor this counter and compare this value against Dynamic Update: Received to determine how many systems are successfully updating DNS records.

Recursive: Queries/sec

This component monitor returns the average number of recursive queries received by the DNS server per second.
Recursive: Query Failure/sec

This component monitor returns the average number of recursive query failures per second.

Recursive: TimeOut/sec

This component monitor returns the average number of recursive query sending time-outs per second.

Secure Update: Failure

This component monitor returns the total number of secure updates that failed on the DNS server.

Monitor this counter to determine whether or not clients can perform secure dynamic updates. Also, compare this value against Secure Update: Received to determine how many systems fail to perform secure updates in DNS.

Secure Update: Received

This component monitor returns the total number of secure update requests received by the DNS server.

Monitor this counter and compare this value against Secure Update: Failure to determine how many systems are successfully performing secure updates in DNS.

TCP: Message Memory

This component monitor returns the total amount of TCP message memory used by the DNS server.

TCP: Query Received/sec

This component monitor returns the average number of TCP queries received by the DNS server per second.

TCP: Response Sent/sec

This component monitor returns the average number of TCP responses sent by the DNS server per second.

Total Query Received/sec

This component monitor returns the average number of queries received by the DNS server per second.

Monitor this counter to create baselines of server usage in heavily trafficked networks.

Total Response Sent/sec

This component monitor returns the average number of responses sent by the DNS server per second.

Monitor this counter to create baselines of server usage in heavily trafficked networks.

UDP: Message Memory

This component monitor returns the total amount of UDP message memory used by the DNS server.
UDP: Query Received/sec
This component monitor returns the average number of UDP queries received by the DNS server per second.

UDP: Response Sent/sec
This component monitor returns the average number of UDP responses sent by the DNS server per second.

Zone Transfer: Failure
This component monitor returns the total number of failed zone transfers of the master DNS server.
Monitor this counter to troubleshoot name resolution failures.

Zone Transfer: Success
This component monitor returns the total number of successful zone transfers of the master DNS server.
Monitor this counter to troubleshoot name resolution failures.

DNS User Experience Monitor
This component monitor tests a DNS server's ability to respond to a record query, compares the query response against a list of IP addresses, and measures the response time. The component monitor passes if the DNS response matches the expected IP addresses.

Windows Network Load Balancing
This template assesses the status and overall performance of Microsoft Windows Network Load Balancing by retrieving information from the MicrosoftNLB namespace and the Windows System Event Log.

Prerequisites
WMI access to the target server.

Credentials
Windows Administrator on the target server.

All Windows Event Log monitors should return zero values. A returned value other than zero indicates an abnormality. Examining the Windows system log files should provide information pertaining to the issue. Detailed information about these events can be found at:


Monitored Components
For details on monitors, see SAM Component Monitor Types.
NLB Cluster Node status

This component monitor returns the current state of an NLB node.

Possible values:

- **0 - Node is remote**: The StatusCode value cannot be retrieved on the remote node
- **1005 – Stopped**: Cluster operations have stopped on the node
- **1006 – Converging**: The cluster node is converging. Convergence is the process of redistributing the existing connection load to operational cluster nodes according to the current load balancing rules
- **1008 – Converged**: The cluster node has converged successfully
- **1009 – Draining**: The cluster nodes are draining; meaning, this is a state in which a node is no longer accepting incoming traffic and is draining. No new connections are allowed, but existing connections are allowed to complete their jobs and terminate naturally. While draining, a node can participate in convergence and remains part of the cluster
- **1013 – Suspended**: Cluster operations have been suspended on the node

Before using this monitor, you should set the correct NLB node name. Replace NLB_node with the NLB node name on which you applied this template in the WQL query section. If you assign the template on NLB_node1 and put NLB_node2 in the WQL query, the returned value will be zero.

Network Adapter Functionality

This monitor returns the number of events that occur when:

- The NLB driver failed to bind or attach to the adapter;
- The NLB failed to add a multicast MAC address to the network adapter;
- The adapter does not support dynamic changing of its MAC address;
- The NLB driver failed to register with the NDIS;
- The NLB failed to update the adapter multicast list;
- The MTU reported by the adapter is too small.

**Type of event: Error.** Event ID: 9, 50, 53, 85, 89, 90, 94, 98.

If you have problems with binding to the adapter, ensure that NLB is bound to an Ethernet network adapter.

If you have problems with MAC addresses, change the network adapter operating mode.

If the NLB driver failed to register or update the adapter multicast list, disable and re-enable NLB network adapters.

When the MTU is small, ensure that the MTU is properly configured.

**NLB Bi-Directional Affinity (BDA) Configuration**

This monitor returns the number of events that occur when:

- An inconsistent teaming configuration is detected;
- An invalid bi-directional affinity (BDA) team ID is detected;
- An invalid bi-directional affinity (BDA) teaming port rule is detected;
- The bi-directional affinity (BDA) team, which this cluster has attempted to join, already has a designated master;
- The bi-directional affinity (BDA) team, in which this cluster participates, has no designated master;
- This cluster has left a bi-directional affinity (BDA) team in which it was the designated master;
- NLB failed to initialize bi-directional affinity (BDA) teaming on the adapter.

**Type of event:** Error and Warning. Event ID: 55, 56, 57, 59, 60, 62, 114.

Reconfigure the BDA teaming configuration. The bi-directional affinity (BDA) configuration must be identical on all cluster hosts. The team in which this cluster participates will be marked inactive and this cluster will remain in the converging state until consistent teaming configuration is achieved. You should first reconfigure the BDA configuration, and then restart the NLB cluster.

**NLB Cluster Control**

This monitor returns the number of events that occur when:

- A version mismatch between the driver and control programs is detected;
- The NLB driver failed to register the device object.

**Type of event:** Error. Event ID: 37, 88.

If a host is not running the same version of all Network Load Balancing (NLB) components as other hosts in the cluster, you should first delete the host that is not running the correct NLB version, remove NLB from the host, reinstall NLB, and then rejoin the cluster.

If the Network Load Balancing (NLB) driver fails to register a device, such as a network adapter, the cluster will converge and operate normally, but controlling the cluster might not work properly. You should disable all network adapters with NLB bound on this host, and then re-enable the adapters.

**NLB Connection Tracking and Load Balancing**

This monitor returns the number of events that occur when:

- The NLB driver could not allocate enough memory resources to perform driver operations;
- The maximum number of actively serviced connections that could be tracked by NLB is reached;
- NLB cannot track TCP connections because it was unable to open the TCP connection callback object;
- A load distribution error was detected during convergence;
- NLB failed to register as a WMI provider;
- The maximum number of actively serviced connections (using extended affinity) that could be tracked by NLB is reached.

**Type of event:** Error and Warning. Event ID: 10, 19, 81, 87, 115, 117.
If the Network Load Balancing (NLB) driver cannot allocate enough memory resources to operate the driver, you should close all programs on this cluster host that might be consuming memory, and then rebind NLB to the adapters. If this problem persists, you might need to add additional memory (RAM) to this host.

When the maximum number of actively serviced connections is reached, you can either add more hosts to the NLB cluster, (which distributes the number of incoming connections across more cluster hosts), or increase the connection tracking limit.

When NLB cannot track TCP connections or fails to register as a WMI provider, disable and re-enable NLB network adapters.

If load distribution errors were detected during convergence, this may result in either client traffic not being handled, general cluster traffic errors, or connections being reset. Convergence is a process by which hosts exchange messages to determine a new, consistent state of the cluster and to elect the default host. During convergence, a new load distribution is determined for hosts that share the handling of network traffic for specific Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) ports. To resolve the load distribution error, you should restart the NLB cluster.

**NLB Dedicated IP (DIP) Addresses Functionality**

This monitor returns the number of events that occur when:

- The dedicated IP (DIP) address or mask is invalid;
- NLB detected an unequal number of dedicated IP (DIP) addresses and network masks;
- Duplicate dedicated IP (DIP) addresses were detected on the network;
- NLB failed to add all the dedicated IP (DIP) addresses to this host because the maximum number of DIPs that can be added to this network adapter have been exhausted.

**Type of event:** Error. Event ID: 15, 30, 32, 83, 107.

You should verify that the dedicated IP address and subnet mask are correctly specified.

On all Network Load Balancing (NLB) cluster hosts, the dedicated IP addresses must have an equal number of subnet masks specified. If there are an unequal number, the NLB cluster will continue to operate, but the IP address that has no corresponding network mask will be ignored. To use this IP address, make sure that the number of IP addresses and network masks are the same.

All dedicated IP addresses must be unique in a Network Load Balancing (NLB) cluster.

If the number of dedicated IP addresses added to a network adapter has exceeded the maximum number allowed by the adapter, you will need to remove one or more IP addresses. The extra dedicated IP addresses will be ignored by the Network Load Balancing (NLB) cluster.

**NLB Denial-of-service Protection**

This monitor returns the number of events that occur when:

- A SYN attack has been detected;
- The NLB driver failed to open the SYN attack callback object;
- The NLB driver failed to open the timer starvation callback object;
Timer starvation has been detected due to a denial of service attack or a very high server load.

**Type of event:** Error and Warning. Event ID: 92, 99, 104, 105.

Analyze the threats against the Network Load Balancing (NLB) cluster, including potential denial-of-service attacks, and then take the appropriate measures. If this is not an attack, the NLB cluster may be overloaded. To distribute the cluster traffic load over more hosts, you can add more hosts to the NLB cluster.

Disable and re-enable NLB network adapters.

**NLB Extended Affinity Configuration**

This monitor returns the number of events that occur when:

- The NLB driver has detected an inconsistency in the extended affinity configuration on the cluster host;
- The NLB driver has detected an inconsistency in the extended affinity configuration between cluster hosts.

**Type of event:** Warning. Event ID: 118, 119.

Confirm that the extended affinity configurations for all port rules are identical on all Network Load Balancing (NLB) hosts.

**NLB Network Host Configuration**

This monitor returns the number of events that occur when:

- The NLB driver failed to initialize because the cluster IP, network address, or mask is invalid;
- NLB detected duplicate cluster subnets;
- The NLB cluster IGMP multicast IP address is invalid;
- The NLB driver failed to register for notifications with the IPv4 or IPv6 NSI provider;
- The virtual IP (VIP) address or mask is invalid;
- NLB detected an unequal number of virtual IP (VIP) addresses and network masks.

**Type of event:** Error and Warning. Event ID: 14, 16, 18, 31, 73, 102, 103, 108, 109, 110, 112.

If the network media access control (MAC) address is not in the following format: XX-XX-XX-XX-XX-XX, where X is a hexadecimal value, it needs to be reconfigured.

If the Network Load Balancing (NLB) driver fails to initialize because the cluster IP address is not in a valid format, you should check that the network IP address is specified in a valid IPv4 or IPv6 address format.

If Network Load Balancing (NLB) detects that there are duplicate subnets in the cluster, it may be due to network partitioning, which prevents NLB heartbeats of one or more hosts from reaching the other cluster hosts. You may need to restart the NLB cluster to resolve this issue.

If the Network Load Balancing (NLB) driver fails to initialize because the cluster network mask is not in a valid format, you should check that the network mask is specified in a valid format.
If the Network Load Balancing (NLB) cluster detects that the Internet Group Management Protocol (IGMP) multicast IP address is invalid, you should check the NLB configuration and make sure that the cluster IGMP multicast IP address is in a valid format.

If the NLB driver failed to register for notifications, the correct IP stack version (IPv4 or IPv6) must be installed on the network adapter to which Network Load Balancing (NLB) is bound. The virtual IP address must be in a valid IPv4 or IPv6 format.

The virtual IP address and mask must be in a valid IPv4 or IPv6 format. On all Network Load Balancing (NLB) cluster hosts, the virtual IP addresses must have an equal number of subnet masks specified.

**NLB Host State Persistence**

This monitor returns the number of events that occur when NLB failed to update the NLB host state in the registry

**Type of event:** Warning. Event ID: 74.

To check the initial Network Load Balancing (NLB) host state, you must first delete the registry key defined in the event log, and then confirm that the initial host state is correct.

Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.

**NLB Port Rules Configuration**

This monitor returns the number of events that occur when:

- NLB failed to converge due to port rules with a duplicate single host priority in the cluster;
- NLB failed to converge due to inconsistencies in the port rules between hosts;
- Configured port rules conflict with the port rules of another host;
- A port rule operation on the port was issued but there is no port rule that contains this port;
- The NLB driver has detected one or more sessions corresponding to a port rule that is improperly configured;
- The virtual IP (VIP) address in a port rule is invalid;

**Type of event:** Error and Warning. Event ID: 20, 21, 22, 25, 95, 111.

When single host filtering mode is used, traffic to the port or ports governed by that port rule is handled exclusively by the host whose priority has the lowest numeric value. When the host's single host priority is identical to the single host priority of another host, the cluster will not converge until the problem is corrected. You should check the NLB configuration of all port rules and make sure that each has a unique host priority (a number between 1 and 32).
When a Network Load Balancing (NLB) host in the cluster either contains a different number of port rules from another host, or its configured port rules conflict with the port rules of another host, the cluster will not converge until the problem is corrected. You should first ensure that all NLB hosts have identical port rules, and then, if there are port rules that are not identical and if there are not the same number of port rules on each NLB host, you should reconfigure the port rules to make them identical.

If there is no port rule that contains a specified port, you should confirm that the port rules are identical on all Network Load Balancing (NLB) hosts.

If the virtual IP address for a port rule is not in a valid format, the Network Load Balancing (NLB) cluster will converge and operate normally, but the port rule will be ignored. You should check that the virtual IP address is specified in a valid IPv4 or IPv6 address format.

**NLB Host Configuration**

This monitor returns the number of events that occur when:

- NLB detected a duplicate host priority that is shared between cluster hosts;
- NLB failed to query parameters from the registry key;
- NLB failed to verify its parameters due to an improper configuration;
- Host converged with legacy host(s) during rolling upgrades;
- NLB received a heartbeat from a host with an invalid ID;
- An unsupported legacy host was discovered on the network.

**Type of event:** Error and Warning. Event ID: 17, 34, 35, 86, 91, 97.

If a Network Load Balancing (NLB) host has a host priority that is identical to the host priority on another host, or the host priority is not valid, the cluster will not converge until the problem is corrected. The host priority must be a number from 1 through 32, and this value must be unique for all hosts in the cluster.

If Network Load Balancing (NLB) is unable to process its configuration settings, you should confirm that the settings are correctly configured, and then, if changes are made, restart the NLB cluster.

A Network Load Balancing (NLB) cluster operating in a mixed mode (where hosts have different versions of an operating system installed) is only supported during rolling upgrades. Until all hosts are upgraded to the latest operating system version, newer NLB features will not be available. You should upgrade all hosts to the latest operating system version.

If an unsupported legacy host is discovered on the Network Load Balancing (NLB) cluster, you should remove the legacy host from the cluster. The cluster will remain in a converging state until all deprecated legacy hosts are removed.

**Microsoft Windows Servers Print Services**

These templates assess the status of Windows Print services.
Periodically, SolarWinds releases SAM templates to support the latest product versions such as Microsoft Server 2016. You can continue using templates for older product versions, but updating to the latest template is recommended.

Prerequisites

WMI access to print server.

Credentials

Windows Administrator on print server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Job Errors

This monitor returns the total number of job errors in a print queue since the last restart. Job errors can occur if the connection to the printer has errors due to network issues.

Jobs

This monitor returns the current number of jobs in a print queue. Use this counter to identify excessive use.

Jobs Spooling

This monitor returns the current number of spooling jobs (incoming or incomplete) in a print queue.

Not Ready Errors

This monitor returns the total number of printer-not-ready errors in a print queue since the last restart.

Out of Paper Errors

This monitor returns the total number of out-of-paper errors in a print queue since the last restart.

Print Server Spooler Service

This monitor returns CPU and memory usage of the Print Server Spooler Service.

Print Server Thread Count

This component monitor returns the number of threads currently executing in Print Server.

Total Jobs Printed

This monitor returns the total number of jobs printed from a print queue since the last restart.

This component has the Count statistic as difference option enabled. It will return the
Total Pages Printed

This monitor returns the total number of pages that have printed through the Graphics Device Interface (GDI) in a print queue since the last restart.

Windows Print Services 2016

This template defines the monitors required for monitoring the Print Server role on Windows 2016 Server.

Prerequisites

WMI access to print server.

Credentials

Windows Administrator on print server.

Monitored Components

Job Errors

This monitor returns the total number of job errors in a print queue since the last restart. Job errors can occur if the connection to the printer has errors due to network issues.

Jobs

This monitor returns the current number of jobs in a print queue. Use this counter to identify excessive use.

Jobs Spooling

This monitor returns the current number of spooling jobs (incoming or incomplete) in a print queue.

Not Ready Errors

This monitor returns the total number of printer-not-ready errors in a print queue since the last restart.
Out of Paper Errors

This monitor returns the total number of out-of-paper errors in a print queue since the last restart.

Print Server Spooler Service

This monitor returns CPU and memory usage of the Print Server Spooler Service.

Print Server Thread Count

This component monitor returns the number of threads currently executing in Print Server.

Total Jobs Printed

This monitor returns the total number of jobs printed from a print queue since the last restart.

This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

Total Pages Printed

This monitor returns the total number of pages that have printed through the Graphics Device Interface (GDI) in a print queue since the last restart.

This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

Windows Remote Desktop Services (Session Host Role)

This template assesses the status and overall performance of a Microsoft Windows Remote Desktop Services Session Host Role by monitoring RDS services and retrieving information from performance counters and the Windows System Event Log.

Prerequisites

WMI access to the target server.

Credentials

Windows Administrator on the target server.

All Windows Event Log monitors should return zero values. A returned value other than zero indicates an abnormality. Examining the Windows system log files should provide information pertaining to the issue. Detailed information about these events can be found here: http://technet.microsoft.com/en-us/library/ee891242(WS.10).aspx.

Monitored Components:

For details on monitors, see SAM Component Monitor Types.
Service: Remote Desktop Configuration

This monitor returns the CPU and memory usage of the Remote Desktop Configuration service. Remote Desktop Configuration Service (RDCS) is responsible for all Remote Desktop Services and Remote Desktop related configuration and session maintenance activities that require system context. These include per-session temporary folders, Remote Desktop themes, and Remote Desktop certificates.

Service: Remote Desktop Services

This monitor returns the CPU and memory usage of the Remote Desktop Services. This service allows users to connect interactively to a remote computer. Remote Desktop and Remote Desktop Session Host Server depend on this service. To prevent remote use of this computer, clear the checkboxes on the Remote tab of the System properties control panel item.

Service: Remote Desktop UserMode Port Redirector

This monitor returns the CPU and memory usage of the Remote Desktop UserMode Port Redirector service, which allows the redirection of Printers/Drives/Ports for RDP connections.

RDP TCP port availability

This monitor tests the ability of an RDP service to accept incoming sessions. By default, it monitors TCP port 3389.

Active Sessions

This monitor returns the number of active Terminal Services sessions.

Inactive Sessions

This monitor returns the number of inactive Terminal Services sessions.

Total Sessions

This monitor returns the total number of Terminal services sessions.

Events: Remote Desktop Services Authentication and Encryption

This monitor returns the number of events that occur when:

- The Terminal Server listener is configured with inconsistent authentication and encryption settings;
- The Terminal Server is configured to use SSL with a user selected certificate, however, no usable certificate was found on the server;
- The Terminal Server is configured to use a certificate that will expire soon or is expired;
- The Terminal Server is configured to use a certificate that does not contain an Enhanced Key Usage attribute of Server Authentication;
- The Terminal Server is configured to use a certificate but is unable to access the private key associated with this certificate;
- The Terminal Server has failed to create a new, or replace an expired, self-signed certificate to be used for Terminal Server authentication on SSL connections;
• The Terminal Server authentication certificate configuration data was invalid and the service reset it;
• The Terminal Server is configured to use a template-based certificate for Transport Layer Security, but the subject name on the certificate is invalid;
• The Terminal Server cannot install a new template-based certificate to be used for Transport Layer Security;
• The template-based certificate that is being used by the Terminal Server for Transport Layer Security has expired and cannot be replaced by the Terminal Server;
• The certificate issued by the Remote Desktop license server to the Remote Desktop Session Host server is not valid.

**Type of event:** Error and Warning. Event ID: 1050, 1051, 1052, 1053, 1054, 1055, 1057, 1058, 1059, 1062, 1064, 1065, 1133.

If the Terminal Server listener is configured with inconsistent authentication and encryption settings, check the Encryption and Authentication settings on the Remote Desktop Session Host server to ensure that they are compatible, and that they are appropriate for your security requirements and the level of security that your client computers can support.

If the Terminal Server is configured to use SSL with a user selected certificate and cannot find a usable certificate or is unable to access the private key, install a certificate onto the Remote Desktop Session Host server that meets the requirements for an Remote Desktop Session Host server certificate. Configure the Remote Desktop Session Host server to use the certificate for TLS 1.0 (SSL).

If the Terminal Server certificate or template-based certificate will expire soon or is expired, take the following steps:

1. Use Remote Desktop Session Host Configuration to determine which certificate needs to be renewed.
2. Renew the certificate being used by the Remote Desktop Session Host server with the same or new key.
3. Configure the Remote Desktop Session Host server to use the certificate for TLS 1.0 (SSL).

If the certificate does not contain an Enhanced Key Usage attribute, confirm that the certificate for the Remote Desktop Session Host server is configured to use TLS 1.0 (SSL) and has the correct Enhanced Key Usage (EKU) value. The certificate must have an Enhanced Key Usage of Server Authentication (1.3.6.1.5.5.7.3.1) or no Enhanced Key Usage at all. If the certificate does not meet these requirements, install an alternate certificate on the Remote Desktop Session Host server that does meet these requirements, and then configure the Remote Desktop Session Host server to use this certificate for TLS 1.0 (SSL).

If there are problems with the self-signed certificate for Terminal Server authentication on SSL connections, you should increase available memory. One way to increase the amount of available memory is to determine if there are any programs or processes running on the Remote Desktop Session Host server that can be closed. Use Task Manager to determine which processes are using the most memory, and end those processes if possible.
If the configuration data is not valid, check the certificate store for the certificate that the Remote Desktop Session Host server is configured to use for TLS 1.0 (SSL). Configure the Remote Desktop Session Host server to use the certificate for TLS 1.0 (SSL).

If Terminal Server is configured to use a template-based certificate for Transport Layer Security and the subject name on the certificate is not valid, you must modify the certificate template that Active Directory Certificate Services (ADCS) uses as the basis for server certificates enrolled to Remote Desktop Session Host servers. The certificate template must be modified so that the alternate subject name for the certificate matches the DNS name of the Remote Desktop Session Host server.

If the Terminal Server cannot install a new template-based certificate for Transport Layer Security, one or more of the following conditions may apply:

- The correct certificate template name is not specified in the Group Policy.
- The permissions on the certificate template do not allow the RD Session Host server to enroll for this type of certificate.
- The certificate is not valid for the requested usage.
- The certificate template does not exist.
- The certificates that are based on the certificate template are not being issued to computers.

If the Terminal Server is configured to use SSL with a user selected certificate and cannot find a usable certificate, you should install a certificate onto the Remote Desktop Session Host server that meets the requirements for an Remote Desktop Session Host server certificate. Configure the Remote Desktop Session Host server to use the certificate for TLS 1.0 (SSL).

If the certificate is not valid, you should delete the certificate from the Remote Desktop Session Host server and then restart the Remote Desktop Services service.

**Events: Remote Desktop Services Availability**

This monitor returns the number of events that occur when:

- The Local Multi-User session manager failed to start;
- The Remote Desktop Service start failed;
- The Remote Desktop Service is shut down for an unknown reason;
- Registering with the Service Control Manager to monitor the Remote Desktop Service status failed;
- An attempt to send a message to the Windows video subsystem failed.

**Type of event:** Warning and Error. Event ID: 16, 17, 18, 19, 20.

To resolve these issues, you should start the Remote Desktop Services service on the computer. If the problem persists, restart the computer.

When there is a failed attempt to send messages to the Windows video subsystem, the error code will indicate the issue.

**Events: Remote Desktop Services Client Access License Availability**

This monitor returns the number of events that occur when:
• The remote desktop client has provided an invalid license;
• The Remote Desktop Session Host server cannot issue a client license;
• The remote session could not be established from the remote desktop client because its temporary license has expired;
• The remote session could not be established from the remote desktop client because its license could not be renewed;
• The Remote Desktop Session Host server was unable to retrieve users licensing information from the Active Directory;
• The Remote Desktop Licensing mode has not been configured;
• The Remote Desktop Licensing grace period has expired and licensing mode for the Remote Desktop Session Host server has not been configured.

Type of event: Warning and Error. Event ID: 1003, 1004, 1011, 1028, 1043, 1061, 1068, 1069.

If the remote desktop client provides an invalid license, delete the MS Licensing registry subkey on the client computer, restart the client computer, and then try to connect remotely to the Remote Desktop Session Host server from the client computer. If the issue persists, delete the following: X509 Certificate, X509 Certificate2, and X509 Certificate ID registry entries on the Remote Desktop Session Host server. Next, restart the Remote Desktop Session Host server, and then try again to connect to the Remote Desktop Session Host server from the client computer.

If the Remote Desktop Session Host server cannot issue a client license, it might be caused by one of the following conditions:

• The licensing mode for the Remote Desktop Session Host server does not match the type of RDS CALs installed on the license server.
• The RDP encryption levels on the Remote Desktop Session Host server and the client are not compatible.
• The certificate on the Remote Desktop Session Host server is corrupt.

If the temporary license has expired, ensure that the Remote Desktop Session Host server can contact a Remote Desktop license server with a sufficient number of the appropriate type of Remote Desktop Services client access licenses (RDS CALs).

If the client's license could not be renewed, determine if the Remote Desktop Session Host server can discover a license server.

If the Remote Desktop Session Host server cannot communicate with the Remote Desktop license server, add the computer account for the Remote Desktop Session Host server to the Terminal Server Computers local group on the Remote Desktop license server.

If the Remote Desktop Session Host server was unable to retrieve users licensing information from the Active Directory, identify and fix any network connectivity problems between the Remote Desktop Session Host server and the Active Directory domain.

If there are problems with Remote Desktop licensing mode, specify the Remote Desktop licensing mode on the Remote Desktop Session Host server.

Events: Remote Desktop Session Host Connections

This monitor returns the number of events that occur when:
- The Terminal Server received a large number of incomplete connections;
- Autoreconnect failed to reconnect the user to the session because authentication failed;
- The Terminal Server cannot register the "TERMSRV" Service Principal Name;
- A logon request was denied because the Terminal Server is currently in drain mode;
- A connection request was denied because the Terminal Server is currently configured to not accept connections;
- The Remote Desktop Session Host server does not have a Remote Desktop license server specified;
- The Remote Desktop Session Host server could not contact the Remote Desktop license server.

**Type of event:** Warning and Error. Event ID: 1006, 1041, 1067, 1070, 1071, 1130, 1131.

If the Terminal Server received a large number of incomplete connections, use Remote Desktop Services Manager to check which users are connecting to the Remote Desktop Session Host server. Ensure that there are no suspicious accounts.

If Autoreconnect failed to reconnect the user, establish a new connection to the Remote Desktop Session Host server by using a Remote Desktop Protocol (RDP) client such as Remote Desktop Connection.

If the Terminal Server cannot register the "TERMSRV" Service Principal Name, manually register the Service Principal Name (SPN) for the Remote Desktop Session Host server.

If a logon request was denied because the Terminal Server is currently in drain mode, configure the Remote Desktop Session Host server to allow new user logons by using Remote Desktop Session Host Configuration.

If the connection request was denied because the terminal server is currently configured to not accept connections, configure the Remote Desktop Session Host server to allow connections by using the chglogon command-line tool.

If the Remote Desktop Session Host server does not have a Remote Desktop license server specified, specify a Remote Desktop license server on the Remote Desktop Session Host server.

If the Remote Desktop Session Host server could not contact the Remote Desktop license server, identify and fix any network connectivity problems between the Remote Desktop Session Host server and the Active Directory domain controller.

**Events: Remote Desktop Session Host Listener Availability**

This monitor returns the number of events that occur when:

- The listener has stopped listening;
- The listener failed while listening with an error code;
- The Terminal Server listener stack was down;
- The Terminal Server session creation failed;
- The remote control session connection failed.

**Type of event:** Error. Event ID: 259, 260, 1035, 1036, 1148.
If the Listener has stopped listening or the listener stack was down, attempt to restart the listener on the Remote Desktop Session Host server. If restarting the listener is not successful, attempt to increase available system resources, such as memory, on the Remote Desktop Session Host server.

If the Listener failed while listening with an error code or the Terminal Server session creation failed, this could indicate that another application on the Remote Desktop Session Host server is using the same TCP port as the Remote Desktop Protocol (RDP). The default port assigned to RDP is 3389.

If the remote control session connection failed, you must ensure that the user account has Remote Control permissions on the Remote Desktop Session Host Listener.

Events: Remote Desktop Session Host User Configuration

This monitor returns the number of events that occur when:

- The Terminal Server Profile path failed to load;
- The Terminal Services User Home Directory was not set because the path specified does not exist or is not accessible.

**Type of event:** Warning and Error. Event ID: 1046, 1060.

If the Terminal Server Profile path failed to load, specify a new location for the Remote Desktop Services profile path, ensuring that the path does not exceed 256 characters.

If the Terminal Services User Home Directory was not set because the path specified does not exist or is not accessible, one or more of the following conditions may be the culprit:

- The Remote Desktop Services home folder name for a user is incorrect.
- The computer on which the home folder is located is not accessible.
- The user does not have sufficient permissions to the home folder.

Events: Remote Desktop IP Virtualization Availability

This monitor returns the number of events that occur when:

- An error occurs when the computer tries to start Remote Desktop IP Virtualization;
- Remote Desktop IP Virtualization detected more than one network adapter;
- Remote Desktop IP Virtualization could not find the network adapter;
- Remote Desktop IP Virtualization could not allocate the IP address.

**Type of event:** Warning and Error. Event ID: 102, 111, 113, 118.

If an error occurred when the computer tried to start Remote Desktop IP Virtualization or the network adapter could not be found, or the IP address could not be allocated, ensure that the network adapter used for Remote Desktop IP Virtualization is enabled. Freeing up memory on the Remote Desktop Session Host server may help.

If Remote Desktop IP Virtualization detected more than one network adapter, you must disable additional network adapters that are installed on the Remote Desktop Session Host server.
Windows Scheduled Tasks template

You can use the Windows Scheduled Tasks template to monitor the status of scheduled tasks configured to execute on a monitored Windows host.

Windows Scheduled Task Monitor does not function like traditional application templates. When enabled on a node through List Resources or manual assignment, these Scheduled Tasks appear as a new widget on the Node Details view for that node. There is no separate/dedicated view solely for Windows Scheduled Tasks.

Only tasks from root directory are monitored. The WSTM does not work for tasks from every level of the Task Scheduler Library.

Nodes should be managed via WMI for discovery of Windows Scheduled Tasks to work properly.

See also [Windows Scheduled Tasks (THWACK)](https://community.solarwinds.com).
Windows Server 2003 Domain Controller Security

This template allows you to check locked and/or disabled users as well as events from the Windows security log in relation to Windows 2003 Domain Controller security.

Prerequisites:

- WinRM must be installed and properly configured on the target server.
- WMI access to the target server.
- Auditing on domain controller (success and failure) must be enabled for the following items: Account Management, Logon Events, Policy Changes and System Events.

To learn how to enable auditing, see Upgrade Domain Controllers (© Microsoft Corp., available at http://technet.microsoft.com, obtained on December 31, 2018).

Credentials: Administrator on target server.

Configuring Windows Remote Management (WinRM)

Take the following steps to properly configure Windows Remote Management:

1. If necessary, install PowerShell 2.0 or later and WinRM on the SAM and target servers. PowerShell 2.0 can be found here: http://support.microsoft.com/kb/968930. (© 2018 Microsoft Corp., available at http://support.microsoft.com, obtained on October 31, 2018)

2. On the SAM server, open a command prompt as an Administrator. To do this, perform the following step:
   - Go to the Start menu and right-click cmd.exe and then select Run as Administrator.

3. Enter the following in the command prompt:
   winrm quickconfig
   winrm set winrm/config/client @{TrustedHosts="*"}

4. On the target server, open a command prompt as an Administrator and enter the following:
   winrm quickconfig
   winrm set winrm/config/client @{TrustedHosts="IP_ADDRESS"}
   where IP address is the IP address of your SAM server.

Monitored Components:

Note: All monitors, except Locked out users and Disabled users, should return zero values. Returned values other than zero may indicate an abnormality. If you believe an abnormality exists, you should examine the Windows security log for details.

Locked out users

This monitor returns the number of currently locked out users. Set the threshold value according to your requirements.
Disabled users

This monitor returns the number of currently disabled users. Set the threshold value according to your requirements.

User Account: Creating a user account

This monitor returns the number of events generated from creating new user accounts.

Event ID: 624.

Only authorized people and processes should create network accounts. Examine the Primary User Name field to detect whether an authorized person or process created an account. This event also detects if administrators create accounts outside organizational policy guidelines.

User Account: Deleting a user account

This monitor returns the number of events generated from deleting user accounts.

Event ID: 630.

Only authorized people and processes should delete network accounts. Search for these events and examine the Primary Account Name field to detect if unauthorized people have deleted accounts.

User Account: Changing a user account

This monitor returns the number of events generated from changes that were made to security-related properties of user accounts.

Event ID: 642.

User Account: Change password attempt

This monitor returns the number of account password change attempts.

Event ID: 627.

This event results from a password change request in which the user supplies the original password to the account. Compare Primary Account Name to Target Account Name to determine whether the account owner or someone else attempted to change the password. If Primary Account Name does not equal Target Account Name, someone other than the account owner tried to change the password.

User Account: Password set or reset

This monitor returns the number of times a user or process resets an account password through an administrative interface, such as Active Directory Users and Computers, rather than through a password change process.

Event ID: 628.

Only authorized people or processes should carry out this process, such as help desk or user self-service password reset.
Logon Failure: Unknown user name or password

This monitor returns the number of failed login attempts with an incorrect username and/or password.

Event ID: 529.

Check for attempts where Target Account Name equals Administrator or the renamed default administrator account. Check multiple logon failures that are below the account lockout threshold.

Logon Failure: Disabled account

This monitor returns the number of failed login attempts using a disabled account.

Event ID: 531.

Always investigate this event. Check Target Account Name value and Workstation Name. This event can signal attempted abuse by former internal users.

Logon Failure: Expired account

This monitor returns the number of failed login attempts using an expired account.

Event ID: 532.

Always investigate this event. This event can signal attempted abuse by contractors or temporary internal users.

Logon Failure: Logon type not allowed

This monitor returns the number of failed attempts to log on interactively with service account credentials when Group Policy settings prevent that account from interactive logon.

Event ID: 534.

Logon Failure: Account locked out

This monitor returns the number of failed login attempts using an account that has been locked out.

Event ID: 539.

Correlate with Event 529 to detect a pattern of continued lockouts.

Logon Failure: User account automatically locked

This monitor returns the number of accounts that have been automatically locked out.

Event ID: 644.

A user account has been locked out because the number of sequential failed logon attempts is greater than the account lockout limit.

Logon Failure: Time restrictions

This monitor returns the number of attempts to logon outside the permitted times.

Event ID: 530.

Check User Account Name and Workstation Name.
Logon Failure: Replay attack detected

This monitor returns the number of detected attempts by the authentication package to log on by replaying a user's credentials.

Event ID: 553.

Investigate immediately. Alternatively, this could be a sign of improper network configuration.

System: Change directory services restore mode password

This monitor returns the number of attempts to change the Directory Services Restore Mode password on a domain controller.

Event ID: 698.

Check Workstation IP and Account Name and investigate immediately.

System: Windows is shutting down

This monitor returns the number of times Windows goes to shut down.

Event ID: 513.

Usually appears before Event 512. On high-value computers, authorized personnel should restart computers in accordance with established policies. Investigate immediately when this event occurs on any server.

System: Clearing the security event logs

This monitor returns the number of times security logs have been cleared.

Event ID: 517.

Administrators should not clear security event logs without authorization. Check Client User Name and Client Domain, then cross-correlate with authorized personnel.

System: Changing system time

This monitor returns the number of times the system time has been changed.

Event ID: 520.

This action can mislead forensic investigation or provide an attacker with a false alibi. The process name is %windir%\system32\svchost.exe. Check Client User Name and Client Domain, then cross-correlate with authorized personnel.

System: Changing audit policy

This monitor returns the number of times audit policies have been changed.

Event ID: 612.

This event does not necessarily indicate a problem. However, an attacker can change audit policy as part of a computer system attack. You should monitor for this event on high value computers and domain controllers.
System: Changing the domain security policy

This monitor returns the number of attempts to modify a password policy or other domain security policy settings.

Event ID: 643.

Check user name of subject and correlate with authorization.
Microsoft Windows Server 2003-2012 Services and Counters

This template assesses the status and overall performance of services and counters in Microsoft Windows Server 2003, Windows Server 2008, or Windows Server 2012.

Prerequisites

- WMI access to the target server.

Credentials

- Windows Administrator on the target server.

> Windows Performance Counters use RPC for communication which runs over TCP port 445.

> Periodically, SolarWinds releases SAM templates to support the latest product versions such as Microsoft Server 2016. You can continue using templates for older product versions, but updating to the latest template is recommended.

Monitored Components

For details on monitors, see [SAM Component Monitor Types](#).

**Service: Distributed Transaction Coordinator**

Coordinates transactions that span multiple resource managers, such as databases, message queues, and file systems. If this service is stopped, these transactions will fail. If this service is disabled, any services that explicitly depend on it will fail to start.

**Service: Security Accounts Manager**

The startup of this service signals other services that the Security Accounts Manager (SAM) is ready to accept requests. Disabling this service will prevent other services in the system from being notified when the SAM is ready, which may in turn cause those services to fail to start correctly. This service should not be disabled.

**Service: Remote Registry**

Enables remote users to modify registry settings on this computer. If this service is stopped, the registry can be modified only by users on this computer. If this service is disabled, any services that explicitly depend on it will fail to start.

**Total Available Memory (MBytes)**

Shows the amount of physical memory, in megabytes (MB), immediately available for allocation to a process or for system use. It is equal to the sum of memory assigned to the standby (cached), free, and zero page lists. For a full explanation of the memory manager, refer to Microsoft Developer Network (MSDN) or "System Performance and Troubleshooting Guide" in the Windows Server 2003 Resource Kit.

This should remain above 100 MB at all times.
Page File Usage

This is a measure of how much of the pagefile is actually being used. This is the counter you should use to determine whether the pagefile is an appropriate size. If this counter reaches 100, the pagefile is completely full and operations stop working.

Depending on the volatility of your workload, you probably want to set the pagefile large enough so that no more than 50 to 75 percent of it is used. If a large part of the pagefile is in use, having more than one pagefile on different physical disks may improve performance.

Disk Queue Length

Tracks the number of requests that are queued and waiting for a disk during the sample interval, as well as requests in service. As a result, this might overstate activity. If more than two requests are continuously waiting on a single-disk system, the disk might be a bottleneck.

To analyze queue length data further, use Avg. Disk Read Queue Length and Avg. Disk Write Queue Length.

Virtual Memory

This is a measure of the demand for virtual memory. It shows how many bytes have been allocated by processes and to which the operating system has committed a RAM page frame or a page slot in the pagefile (or both).

As Committed Bytes grows above the available RAM, paging increases, and the amount of the pagefile in use also increases. At some point, paging activity starts to significantly affect perceived performance.

% Processor Time

Shows the percentage of time that the processor is executing application or operating system processes. This is when the processor is not idle.

This should be less than 75% on average.

Service: Server

Supports file, print, and named-pipe sharing over the network for this computer. If this service is stopped, these functions will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

Service: Plug and Play

Enables a computer to recognize and adapt to hardware changes with little or no user input. Stopping or disabling this service will result in system instability.

Pages/sec

Pages/sec is the number of pages read from the disk or written to the disk to resolve memory references to pages that were not in memory at the time of the reference. This is the sum of Pages Input/sec and Pages Output/sec. This counter includes paging traffic on behalf of the system Cache to access file data for applications.
This should be 0-20 at all times. It is unhealthy if this is greater than 80, which probably indicates there is not enough RAM.

**Logical Disk: Avg. Disk Queue Length**

Tracks the number of requests that are queued and waiting for a disk during the sample interval, as well as requests in service. As a result, this might overstate activity.

If more than two requests are continuously waiting on a single-disk system, the disk might be a bottleneck.

This should be less than 4 at all times.

ℹ️ When looking at hard disks using `perfmon.exe`, an understanding of the underlying hard disk subsystem is required to determine which counters (physical disk or logical disk) to look at.

**Physical Disk: Avg. Disk Queue Length**

Tracks the number of requests that are queued and waiting for a disk during the sample interval, as well as requests in service. As a result, this might overstate activity.

If more than two requests are continuously waiting on a single-disk system, the disk might be a bottleneck.

This should be less than 4 at all times.

ℹ️ When looking at hard disks using `perfmon.exe`, an understanding of the underlying hard disk subsystem is required to determine which counters (physical disk or logical disk) to look at.
Microsoft Windows Server 2008 - 2016 Domain Controller Security

This template allows you to check locked and/or disabled users and events from the Windows security log related with Windows 2008 - 2016 Domain Controller Security.

Prerequisites:

- WinRM must be installed and properly configured on the target server;
- WMI access to the target server;
- Auditing on domain controller (success and failure) must be enabled for the following items: Account Management, Logon Events, Policy Changes and System Events.

To learn how to enable auditing, see Upgrade Domain Controllers (© Microsoft Corp., available at http://technet.microsoft.com, obtained on December 31, 2018).

Credentials

Administrator on target server.

Configuring Windows Remote Management (WinRM)

To configure WinRM:

1. If not already installed, install PowerShell 2.0 or later and WinRM on the Orion server and target servers.
2. On the Orion server, open a command prompt as an Administrator.
3. Enter the following in the command prompt:
   
   ```
   Important: "TrustedHosts" is case sensitive.
   winrm quickconfig winrm
   set winrm/config/client @{TrustedHosts="*"}
   ```
4. On the target server, open a command prompt as an Administrator and enter the following:
   ```
   winrm quickconfig winrm
   set winrm/config/client @{TrustedHosts="IP_ADDRESS"}
   ```
   where IP address is the IP address of your SAM server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

All monitors, except Locked out users and Disabled users, should return zero values. Returned values other than zero may indicate an abnormality. If you believe an abnormality exists, you should examine the Windows security log for details.
Locked out users

This monitor returns the number of currently locked out users. Set the threshold value according to your requirements.

Disabled users

This monitor returns the number of currently disabled users. Set the threshold value according to your requirements.

User Account: User account was created

This monitor returns the number of new user accounts created.

Event ID: 4720.

Only authorized people and processes should create network accounts. Examine the Primary User Name field to detect whether an authorized person or process created an account. This event also detects if administrators create accounts outside organizational policy guidelines.

User Account: Attempt to change password

This monitor returns the number of account password change attempts.

Event ID: 4723.

This event is logged as a failure if his new password fails to meet the password policy.

This event results from a password change request in which the user supplies the original password to the account. Compare Primary Account Name to Target Account Name to determine whether the account owner or someone else attempted to change the password. If Primary Account Name does not equal Target Account Name, someone other than the account owner tried to change the password.

User Account: Attempt to reset password

This monitor returns the number of times a user or process resets an account password through an administrative interface, such as Active Directory Users and Computers, rather than through a password change process.

Event ID: 4724.

This event is logged as a failure if the new password fails to meet the password policy.

Only authorized people or processes should carry out this process, such as help desk or user self-service password reset.

User Account: Account was disabled

This monitor returns the number of times an account becomes disabled.

Event ID: 4725.

Always investigate this event.

User Account: Account was deleted

This monitor returns the number of deleted user accounts.
Event ID: 4726.

Only authorized people and processes should delete network accounts. Search for these events and examine the Primary Account Name field to detect if unauthorized people have deleted accounts.

**User Account: Account was changed**

This monitor returns the number of times when changes were made to security-related properties of user accounts.

Event ID: 4738.

**User Account: Account was locked out**

This monitor returns the number of automatically locked out accounts.

Event ID: 4740.

A user account has locked out because the number of sequential failed logon attempts is greater than the account lockout limit.

**User Account: Account name was changed**

This monitor returns the number of changes to the normal logon name or the pre-Win2k logon name.

Event ID: 4781.

When an account name is changed, the SID remains the same. However the Target ID in this event indicates the new name. This is because when the operating system displays this event it evidently queries the database where the SID is stored and translates the SID to the domain\username.

A rogue administrator might change his account name or computer name seeking to cover his tracks.

**Logon: Account failed to log on**

This monitor returns the number of failed login attempts with an incorrect username and/or password.

Event ID: 4625.

Check for attempts where Target Account Name equals Administrator or the renamed default administrator account. Check multiple logon failures that are below the account lockout threshold.

**Logon: Replay attack detected**

This monitor returns the number of detected attempts by the authentication package to log on by replaying a user's credentials.

Event ID: 4649.

Investigate immediately. Alternatively, this could be a sign of improper network configuration.

**Logon: Attempted logon using explicit credentials**

This monitor returns a number for the following events:
A user connects to a server or runs a program locally using alternate credentials (run as);

- A process logs on as a different account; such as when the Scheduled Tasks service starts a task as the specified user;
- With User Account Control enabled, an end user runs a program requiring administrative authority.

Event ID: 4648.

**Policy: Domain policy was changed**

This monitor returns the number of events when the computer's Security Settings\Account Policy or Account Lockout Policy was modified, either via Local Security Policy or Group Policy in the Active Directory.

Event ID: 4739.

Unfortunately, the Subject fields don't identify who actually changed the policy because this policy is not directly configured by administrators. Instead, it is edited in a group policy object which then gets applied to the computer. Therefore, this event always shows the local computer as the one who changed the policy since the computer is the security principal under which gpupdate runs.

**Policy: Kerberos policy was changed**

This monitor returns the number of times Windows detects a change to the domain's Kerberos policy. Kerberos policy is defined in GPOs linked to the root of the domain under Computer Configuration\Windows Settings\Security Settings\Account Policy\Kerberos Policy.

Event ID: 4713.

Unfortunately, the Subject fields do not identify who actually changed the policy because this policy is not directly configured by administrators. Instead, it is edited in a group policy object which then gets applied to the computer. Therefore, this event always shows the local computer as the one who changed the policy since the computer is the security principal under which gpupdate runs.

**Policy: System audit policy was changed**

This monitor returns the number of times audit policies have been changed either via Local Security Policy, Group Policy in Active Directory, or the audipol command.

Event ID: 4719.

According to Microsoft, this event is always logged when an audit policy is disabled, regardless of the "Audit Policy Change" sub-category setting.

If group policy was used to configure audit policy, the Subject fields do not identify who actually changed the policy. In such cases, this event always shows the local computer as the one who changed the policy since the computer is the security principal under which gpupdate runs.

This event does not necessarily indicate a problem; however, an attacker can change audit policy as part of a computer system attack. You should monitor this event on high value computers and domain controllers.
**Policy: Encrypted data recovery policy was changed**

This monitor returns the number of times a computer's Security Settings\Public Key Policies\Encrypting File System data recovery agent policy was modified either via Local Security Policy or Group Policy in an Active Directory.

Event ID: 4714.

Unfortunately, the Subject fields do not identify who actually changed the policy because this policy is not directly configured by administrators. Instead, it is edited in a group policy object which then gets applied to the computer. Therefore, this event always shows the local computer as the one who changed the policy since the computer is the security principal under which gpupdate runs.

**System: Windows Firewall setting has changed**

This monitor returns the number of changes that were made to the Windows Firewall with the Advanced Services MMC console.

Event ID: 4950.

**System: Windows is shutting down**

This monitor returns the number of times Windows goes to shut down.

Event ID: 4609.

On high-value computers, authorized personnel should restart computers in accordance with established policies. Investigate immediately when this event occurs on any server.

**System: The system time was changed**

This monitor returns the number times the system time has changed.

Event ID: 520.

This event indicates the old and new system times, as well as who changed the time as specified in the Subject section. It is routine to see this event, where the subject is "LOCAL SERVICE," and can probably be ignored. You will frequently see this event logged twice in a row.

**System: Service installed in the system**

This monitor returns the number of new services installed by the user as indicated in the subject.

Event ID: 4697.

Subject often identifies the local system (SYSTEM) for services installed as part of native Windows components and therefore you cannot determine who actually initiated the installation.

This is a key change control event as new services are significant extensions of the software running on a server and the roles it performs.
Microsoft Windows Server 2016 Services and Counters

This template assesses the status and overall of services and performance of a Microsoft Windows Server 2016 operating system.

**Prerequisites**

- WMI access to the target server.

**Credentials**

- Windows Administrator on the target server.

> Windows Performance Counters use RPC for communication which runs over TCP port 445.

> Periodically, SolarWinds releases SAM templates to support the latest product versions such as Microsoft Server 2016. You can continue using templates for older product versions, but updating to the latest template is recommended.

**Monitored Components**

> For details on monitors, see [SAM Component Monitor Types](#).

**Service: Distributed Transaction Coordinator**

Coordinates transactions that span multiple resource managers, such as databases, message queues, and file systems. If this service is stopped, these transactions will fail. If this service is disabled, any services that explicitly depend on it will fail to start.

**Service: Security Accounts Manager**

The startup of this service signals other services that the Security Accounts Manager (SAM) is ready to accept requests. Disabling this service will prevent other services in the system from being notified when the SAM is ready, which may in turn cause those services to fail to start correctly. This service should not be disabled.

**Service: Remote Registry**

Enables remote users to modify registry settings on this computer. If this service is stopped, the registry can be modified only by users on this computer. If this service is disabled, any services that explicitly depend on it will fail to start.

**Total Available Memory (MBytes)**

Shows the amount of physical memory, in megabytes (MB), immediately available for allocation to a process or for system use. It is equal to the sum of memory assigned to the standby (cached), free, and zero page lists. For a full explanation of the memory manager, refer to Microsoft Developer Network (MSDN) or "System Performance and Troubleshooting Guide" in the Windows Server 2003 Resource Kit.

This should remain above 100 MB at all times.
Page File Usage

This is a measure of how much of the pagefile is actually being used. This is the counter you should use to determine whether the pagefile is an appropriate size. If this counter reaches 100, the pagefile is completely full and operations stop working.

Depending on the volatility of your workload, you probably want to set the pagefile large enough so that no more than 50 to 75 percent of it is used. If a large part of the pagefile is in use, having more than one pagefile on different physical disks may improve performance.

Disk Queue Length

Tracks the number of requests that are queued and waiting for a disk during the sample interval, as well as requests in service. As a result, this might overstate activity. If more than two requests are continuously waiting on a single-disk system, the disk might be a bottleneck.

To analyze queue length data further, use Avg. Disk Read Queue Length and Avg. Disk Write Queue Length.

Virtual Memory

This is a measure of the demand for virtual memory. It shows how many bytes have been allocated by processes and to which the operating system has committed a RAM page frame or a page slot in the pagefile (or both).

As Committed Bytes grows above the available RAM, paging increases, and the amount of the pagefile in use also increases. At some point, paging activity starts to significantly affect perceived performance.

% Processor Time

Shows the percentage of time that the processor is executing application or operating system processes. This is when the processor is not idle.

This should be less than 75% on average.

Service: Server

Supports file, print, and named-pipe sharing over the network for this computer. If this service is stopped, these functions will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.

Service: Plug and Play

Enables a computer to recognize and adapt to hardware changes with little or no user input. Stopping or disabling this service will result in system instability.

Pages/sec

Pages/sec is the number of pages read from the disk or written to the disk to resolve memory references to pages that were not in memory at the time of the reference. This is the sum of Pages Input/sec and Pages Output/sec. This counter includes paging traffic on behalf of the system Cache to access file data for applications.
This should be 0-20 at all times. It is unhealthy if this is greater than 80, which probably indicates there is not enough RAM.

**Logical Disk: Avg. Disk Queue Length**

Tracks the number of requests that are queued and waiting for a disk during the sample interval, as well as requests in service. As a result, this might overstate activity.

If more than two requests are continuously waiting on a single-disk system, the disk might be a bottleneck.

This should be less than 4 at all times.

When looking at hard disks using `perfmon.exe`, an understanding of the underlying hard disk subsystem is required to determine which counters (physical disk or logical disk) to look at.

**Physical Disk: Avg. Disk Queue Length**

Tracks the number of requests that are queued and waiting for a disk during the sample interval, as well as requests in service. As a result, this might overstate activity.

If more than two requests are continuously waiting on a single-disk system, the disk might be a bottleneck.

This should be less than 4 at all times.

When looking at hard disks using `perfmon.exe`, an understanding of the underlying hard disk subsystem is required to determine which counters (physical disk or logical disk) to look at.
Microsoft System Center

The following templates are available:

- Microsoft System Center Configuration Manager 2012
- Microsoft System Center Operations Manager 2012 (Agent)
- Microsoft System Center Operations Manager 2012 (Management Server)

Microsoft System Center Operations Manager 2012 (Agent)

This template assesses the status and overall health of services as well as the performance of the Agent of Microsoft System Center Operations Manager 2012.

Prerequisites

   WMI access to the target server.

Credentials

   Windows Administrator on the target server.

Monitored Components

For details on monitors, see [SAM Component Monitor Types](#).

You need to set thresholds for these counters according to your environment. It is recommended to monitor these counters for some period of time to understand potential value ranges and then set the thresholds accordingly.

**Service: System Center Management**

This monitor returns the CPU and memory usage of System Center Management service. This service monitors the health of the computer. The service may be configured to monitor the health of other computers in addition to this computer. If this service is stopped, detection of failures may not occur. If this service is disabled, any services that explicitly depend on it will fail to start.

**Health Service: Active File Downloads**

This monitor returns the number of file downloads to this health service that are currently active.

**Health Service: Active File Uploads**

This monitor returns the number of file uploads from this health service that are currently active.

**Health Service: Data Batches Dropped Rate**

This monitor returns the rate at which data batches are being dropped.

**Health Service: Data Items Dropped Rate**

This monitor returns the rate at which data items are being dropped.
Health Service: Malformed Data Items Dropped Rate
This monitor returns the rate at which malformed data items are being dropped.

Health Service: Module Count
This is the number of modules running in the Health Service.

Health Service: Send Queue Routes
The number of items in the send queue routing table.

Health Service: Send Queue Virtual Queues
The number of items in the send queue virtual queues table.

Health Service: Task Count
This is the number of tasks running in the Health Service.

Health Service: Workflow Count
This is the number of workflows running in the Health Service.

Events: Health Service Events
This is the number of Health Service Events.

Configuring Windows Remote Management (WinRM)

1. If you have not already done so, install PowerShell 2.0 or later and WinRM on the SAM and target servers. (For installation details, see Microsoft's documentation website (https://docs.microsoft.com/en-us/powershell/).

2. On the SAM server, open a command prompt as an Administrator. To do this, go to the Start menu and right-click the cmd.exe and then select Run as Administrator.

3. Enter the following in the command prompt:
   winrm quickconfig
   winrm set winrm/config/client @{TrustedHosts="*"}

4. On the target server, open a command prompt as an Administrator and enter the following:
   winrm quickconfig
   winrm set winrm/config/client @{TrustedHosts="IP_ADDRESS"}
   where IP address is the IP address of your SAM server.

Microsoft System Center Operations Manager 2012 (Management Server)

This template assesses the status and overall health of services as well as the performance of the Microsoft System Center Operations Manager 2012 Management Server.

Prerequisites
WMI access to the target server.
Credentials

Windows Administrator on the target server.

Monitored Components

For details on monitors, see [SAM Component Monitor Types](#).

You need to set thresholds for these counters according to your environment. It is recommended to monitor these counters for some period of time to understand potential value ranges and then set the thresholds accordingly.

**Service: System Center Data Access**

This monitor returns the memory and CPU usage of the Microsoft System Center Data Access Service.

**Service: System Center Management Configuration**

This monitor returns the memory and CPU usage of the Microsoft System Center Management Configuration service.

**Service: Operations Manager Audit Collection**

This monitor returns the memory and CPU usage of the Operations Manager Audit Collection service. This service is used for receiving audit events over the network and writing them to a database.

**DB Write Action Caches: Cache Hit Ratio**

This monitor returns the hit ratio for the cache.

By default, this counter monitors the `managedentityidcache` instance. You may change it if you need. Look in the Windows `perfmon` utility to see all the available instances for this counter.

**DB Write Action Caches: Cache Size**

This monitor returns the number of entries in the cache.

By default, this counter monitors the `managedentityidcache` instance. You may change it if you need. Look in the Windows `perfmon` utility to see all the available instances for this counter.

**DB Write Action Modules: Avg. Batch Size**

This monitor returns the number of entries processed by the module, on average.

By default, this counter monitors the `performancewritemodule` instance. You may change it if you need. Look in the Windows `perfmon` utility to see all available instances for this counter.

**DB Write Action Modules: Avg. Processing Time**

This monitor returns the amount of time it takes to process an incoming batch, on average.
By default, this counter monitors the `performancewritemodule` instance. You may change it if you need. Look in the Windows `perfmon` utility to see all available instances for this counter.

**DW Synchronization Module: Avg Batch Processing Time, ms**

This monitor returns the amount of time it takes to process an incoming batch, on average, in ms.

By default, this counter monitors the `managedentityidcache` instance. You may change it if you need. Look in the Windows `perfmon` utility to see all the available instances for this counter.

**DW Synchronization Module: Avg. Batch Size**

This monitor returns the number of entries processed by the module, on average.

Note: By default, this counter monitors the `managedentity` instance. You may change it if you need. Look in the Windows `perfmon` utility to see all available instances for this counter.

**DW Synchronization Module: Batches/sec**

This monitor returns the number of batches per second.

Note: By default, this counter monitors the `managedentity` instance. You may change it if you need. Look in the Windows `perfmon` utility to see all available instances for this counter.

**DW Synchronization Module: Data Items/sec**

This monitor returns the number of data items, per second.

By default, this counter monitors the `managedentity` instance. You may change it if you need. Look in the Windows `perfmon` utility to see all the available instances for this counter.

**DW Synchronization Module: Errors/sec**

This monitor returns the number of errors, per second.

By default, this counter monitors the `managedentity` instance. You may change it if you need. Look in the Windows `perfmon` utility to see all available instances for this counter.

**DW Writer Module: Avg Batch Processing Time, ms**

This monitor returns the amount of time it takes to process an incoming batch, on average, in ms.

By default, this counter monitors the `performance` instance. You may change it if you need. Look in the Windows `perfmon` utility to see all available instances for this counter.

**DW Writer Module: Avg. Batch Size**

This monitor returns the number of entries processed by the module, on average.
By default, this counter monitors the performance instance. You may change it if you need. Look in the Windows perfmon utility to see all available instances for this counter.

**DW Writer Module: Batches/sec**

This monitor returns the number of batches, per second.

By default, this counter monitors the performance instance. You may change it if you need. Look in the Windows perfmon utility to see all available instances for this counter.

**DW Writer Module: Data Items/sec**

This monitor returns the number of data items, per second.

By default, this counter monitors the performance instance. You may change it if you need. Look in the Windows perfmon utility to see all available instances for this counter.

**DW Writer Module: Errors/sec**

This monitor returns the number of errors, per second.

By default, this counter monitors the performance instance. You may change it if you need. Look in the Windows perfmon utility to see all available instances for this counter.

**OpsMgr Connector: Bytes Received**

This monitor returns the total number of network bytes which have been received by the MOM connector, per second. This may be more or less than the number of data bytes received due to compression and encryption.

**OpsMgr Connector: Bytes Transmitted**

This monitor returns the total number of network bytes which have been transmitted by the MOM connector, per second. This may be more or less than the number of data bytes submitted for transmission due to compression and encryption.

**OpsMgr Connector: I/O Errors**

This monitor returns the number of I/O errors encountered by the connector, per second.

**OpsMgr Connector: I/O Operations Timed Out**

This monitor returns the number of I/O operations that have timed out.

**OpsMgr Connector: Open Connections**

This monitor returns the number of TCP/IP connections currently open in the connector.
OpsMgr Connector: Server Listen Queue Length

This monitor returns the number of outstanding listen requests which are queued. If this drops to zero, the connector will not be able to accept incoming connections.

OpsMgr Connector: Fragmented Compression Packets

This monitor returns the number of compression packets which were received by the connector and had to be reassembled, per second. This can be caused by a number of factors, including the size of the packet, the MTU of the network interface, quantity of traffic on the network, and/or the amount of load on the connector. Packet re-assembly can hurt performance and the ability of the server to scale.

OpsMgr Connector: Fragmented Data Packets

This monitor returns the number of data packets which were received by the connector and had to be reassembled, per second. This can be caused by a number of factors, including the size of the packet, the MTU of the network interface, quantity of traffic on the network, and/or the amount of load on the connector. Packet re-assembly can hurt performance and the ability of the server to scale.

OpsMgr Connector: Fragmented Encryption Packets

This monitor returns the number of encrypted packets which were received by the connector and had to be reassembled, per second. This can be caused by a number of factors, including the size of the packet, the MTU of the network interface, quantity of traffic on the network, the encryption algorithm used and/or the amount of load on the connector. Packet re-assembly can hurt performance and the ability of the server to scale.

OpsMgr Connector: Fragmented Session Packets

This monitor returns the number of session packets which were received by the connector and had to be reassembled, per second. This can be caused by a number of factors, including the size of the packet, the MTU of the network interface, quantity of traffic on the network, and/or the amount of load on the connector. Packet re-assembly can hurt performance and the ability of the server to scale.

OpsMgr Connector: Fragmented SSPI Packets

This monitor returns the number of SSPI negotiation packets which were received by the connector and had to be reassembled, per second. This can be caused by a number of factors, including the size of the packet, the MTU of the network interface, quantity of traffic on the network, and/or the amount of load on the connector. Packet re-assembly can hurt performance and the ability of the server to scale.

Events: OpsMgr Management Configuration Events

This monitor returns the number of warning and error events with the following source name: OpsMgr Management Configuration.

For any and all events, you should investigate the “Operations Manager” Event Log.
**Events: OpsMgr Connector and Network Discovery Events**

This monitor returns the number of warning and error events with the following source names: OpsMgr Connector, OpsMgr Network Discovery, OpsMgr Root Connector.

For any and all events, you should investigate the “Operations Manager” Event Log.

**Events: OpsMgr Config Service Events**

This monitor returns the number of warning and error events with the following source name: OpsMgr Config Service.

For any and all events, you should investigate the “Operations Manager” Event Log.

**Events: OpsMgr SDK Service Events**

This monitor returns the number of warning and error events with the following source name: OpsMgr SDK Service.

For any and all events, you should investigate the “Operations Manager” Event Log.

**TCP Port: SCOM (5723)**

This component monitor tests the ability of a SCOM to accept incoming sessions. By default, this component monitors TCP port **5723**.

**TCP Port: SCOM (5724)**

This component monitor tests the ability of a SCOM to accept incoming sessions. By default, this component monitors TCP port **5724**.

**Configuring Windows Remote Management (WinRM)**

1. If not already done so, install PowerShell 2.0 or later and WinRM on the SAM and target servers. (For installation details, see Microsoft's documentation website [https://docs.microsoft.com/en-us/powershell/](https://docs.microsoft.com/en-us/powershell/).)

2. On the SAM server, open a command prompt as an Administrator. To do this, go to the Start menu and right-click the cmd.exe and then select Run as Administrator.

3. Enter the following in the command prompt:

   ```
   winrm quickconfig
   winrm set winrm/config/client @{TrustedHosts="*"}
   ```

4. On the target server, open a command prompt as an Administrator and enter the following:

   ```
   winrm quickconfig
   winrm set winrm/config/client @{TrustedHosts="IP_ADDRESS"}
   ```

   where IP address is the IP address of your SAM server.

**Microsoft System Center Configuration Manager 2012**

This template assesses the status and overall health of services as well as the performance of the Microsoft System Center Configuration Manager 2012.
Prerequisites

WMI access to the target server.

Credentials

Windows Administrator on the target server.

Monitored Components

For details on monitors, see [SAM Component Monitor Types](#).

**Service: SMS Agent Host**

This monitor returns the CPU and memory usage of SMS Agent Host. It provides change and configuration services for computer management systems.

**Service: SMS Executive**

This monitor returns the CPU and memory usage of SMS Executive. This is the main service that calls many threads.

**Service: SMS Notification Server**

This monitor returns the CPU and memory usage of SMS Notification Server. It provides notifications for SCCM environment.

**Service: SMS Site Component Manager**

This monitor returns the CPU and memory usage of SMS Site Component Manager. It provides change and configuration services for sites.

**Service: SMS Site SQL Backup**

This monitor returns the CPU and memory usage of SMS Site SQL Backup. It provides sites backup.

**Service: SMS Site VSS Writer**

This monitor returns the CPU and memory usage of SMS Site VSS Writer. It provides VSS for SCCM environment.

**TCP Port: Site Client Requests (HTTP)**

This component monitor tests the ability of a SCCM to accept incoming requests from clients by using HTTP protocol. By default it monitors TCP port 80.

**TCP Port: Site Client Requests (HTTPS)**

This component monitor tests the ability of a SCCM to accept incoming requests from clients by using HTTPS protocol. By default it monitors TCP port 443.

**TCP Port: Site Client Notifications**

This component monitor tests the ability of a SCCM to accept incoming notifications. By default it monitors TCP port 10123.
Executive Thread States: Running Thread Count

This is the number of running threads in the SMS Executive service (smsexec.exe). When this counter is associated with a single thread instead of the entire service, its value is zero (the thread is not running) or one (the thread is running).

Executive Thread States: Sleeping Thread Count

This is the number of blocked threads in the SMS Executive service (smsexec.exe) that are waiting for an operation to complete or new work to arrive. When this counter is associated with a single thread instead of the entire service, its value is zero (the thread is not sleeping) or one (the thread is sleeping).

Executive Thread States: Yielding Thread Count

This is the number of blocked threads in the SMS Executive service (smsexec.exe) that are waiting to run but cannot because the administrator limited the number of threads that can run at the same time. When the currently-running threads become blocked, the yielding threads will be allowed to run. When this counter is associated with a single thread instead of the entire service, its value is zero (the thread is not yielding) or one (the thread is yielding).

Inventory Data Loader: Average MIF size (KB)

This is the average size of SMS hardware inventory records (in MIF files) processed by Inventory Data Loader since it was last started.

Inventory Data Loader: MIFs Processed/minute

This is the number of SMS hardware inventory records (in MIF files) processed by Inventory Data Loader during the last minute.

Notification Server: Failed SignIn requests/sec

This is the current number of failed SignIn requests per second processed by SMS Notification server during the last sampling interval.

Notification Server: Keep alive messages/sec

This is the current number of keep alive message per second processed by SMS Notification server during the last sampling interval.

Notification Server: Online clients/sec

This is the current number of online clients per second processed by SMS Notification server during the last sampling interval.

Notification Server: Task responses/sec

This is the current number of tasks response retrieved per second by SMS Notification server during the last sampling interval.

Notification Server: Tasks sent/sec

This is the current number of tasks sent per second by the SMS Notification server during the last sampling interval.
Notification Server: Total online clients

This is the number of current online clients.

Scheduler: Number of Jobs

This is the total number of jobs that the Scheduler needs to process.

Scheduler: Number of Send Requests

This is the total number of send requests that are waiting to be processed.

Server Availability: Avg. Request Latency

The average request latency, in milliseconds. This is a moving average for a fixed number of requests.

Server Availability: Failed Requests

Number of failed requests made.

**Note:** By default, this monitor has the **Count statistic as difference** box checked. It will show statistic since the last polling period.

Server Availability: Successful Requests

Number of successful requests made.

**Note:** By default, this monitor has the **Count statistic as difference** box checked. It will show statistic since the last polling period.

Software Inventory Processor: Total Bad SINVs Processed

This is the total number of bad (ill-formed or otherwise invalid) SMS software inventory records (SINVs) processed by Software Inventory Processor since it was last started.

**Note:** By default, this monitor has the **Count statistic as difference** box checked. It will show statistic since the last polling period.

Software Inventory Processor: Total SINVs Enqueued

This is the number of SMS software inventory records (SINVs) waiting in Software Inventory Processor's input queue the last time Software Inventory Processor scanned the queue, minus the SINVs processed since then. When many SINVs are being written to the input queue, this counter is too low until Software Inventory Processor scans the input queue again. SINVs can be Software Inventory Complete records (SICs) or Software Inventory Delta records (SIDs). If there are any SICs enqueued, this counter shows only the number of enqueued SICs. If only SIDs are enqueued, this counters shows the number of enqueued SIDs.

**Note:** By default, this monitor has the **Count statistic as difference** box checked. It will show statistic since the last polling period.

Software Inventory Processor: Total SINVs Processed

This is the total number of SMS software inventory records (SINVs) processed by Software Inventory Processor since it was last started.
Note: By default, this monitor has the **Count statistic as difference** box checked. It will show statistic since the last polling period.

**Software Metering Processor: Total SWM Usage Processing Threads**
This is the number of threads the Software Metering Processor is currently using to process incoming SMS software metering usage files.

**Standard Sender: Average Bytes/sec**
This is the average throughput of this SMS sender, either to all sites or to the specified site, since it was last started.

**Standard Sender: Sending Thread Count**
This is the number of threads of this SMS sender currently sending data, either to all sites or to the specified site.

**State System: Message File Processing Threads**
This is the number of threads currently being used to process message files.

**Status Messages: Corrupt**
This is the number of corrupt SMS SVF files received by Status Manager since it was last started.

Note: By default, this monitor has the **Count statistic as difference** box checked. It will show statistic since the last polling period.

**Status Messages: Processed/sec**
This is the average number of SMS status messages processed per second by Status Manager during the last sampling interval.

**Status Messages: Written To SMS Database**
This is the number of SMS status messages queued by Status Manager to be written to the SMS site database since Status Manager was last started. This number equals the number of status messages actually written to the database, unless Status Manager cannot write to the database (because it is full, for example), in which case the number of queued messages (shown by this counter) will increase even though no messages are being written to the database. (Queued messages are stored as .SQL files in \SMS\Inboxes\Statmgr.box\Retry.) When the database becomes writable again, the queued messages will rapidly be written to it, and this counter will again reflect the actual number of messages written to the database.

Note: By default, this monitor has the **Count statistic as difference** box checked. It will show statistic since the last polling period.

**CCM Message Queue: Messages Queued**
The count of messages currently in the queue.

**Site Status**
This monitor returns status of different sites on server. The returned values are as follows:

**Active** – This component returns the current number of sites in active state.
Pending – This component returns the current number of sites in pending state.
Failed – This component returns the current number of sites in failed state.
Deleted – This component returns the total number of sites in deleted state.
Upgrade – This component returns the total number of sites in active state.

Note: By default this monitor is disabled.

Site Role Status
This monitor returns status of site system on server. The returned values are as follows:
OK – This component returns the current number of sites in OK state.
Warning – This component returns the current number of sites in warning state.
Error – This component returns the current number of sites in error state.

Note: By default this monitor is disabled.

Error and Warning Events: SMS Server
This monitor returns number of SCCM warning and error events.

Source name: SMS Server.

Configuring Windows Remote Management (WinRM)
1. If not already done so, install PowerShell 2.0 or later and WinRM on the SAM and target servers. (For installation details, see Microsoft's documentation website (https://docs.microsoft.com/en-us/powershell/).
2. On the SAM server, open a command prompt as an Administrator. To do this, Go to the Start menu and right-click the cmd.exe and then select Run as Administrator.
3. Enter the following in the command prompt:
   winrm quickconfig
   winrm set winrm/config/client @{TrustedHosts="*"}
4. On the target server, open a command prompt as an Administrator and enter the following:
   winrm quickconfig
   winrm set winrm/config/client @{TrustedHosts="IP_ADDRESS"}

where IP address is the IP address of your SAM server.
Mongo

The following templates are available:

- MongoDB (Linux)
- MongoDB (Windows)
MongoDB (Windows)

This template allows you to monitor the performance of MongoDB installed on a Windows machine by using PowerShell monitors.

Prerequisites

WinRM must be installed and properly configured on the target server.

Credentials

User under which MongoDB was installed.

Each PowerShell monitor uses the same argument structure.

For Example:

```
c:\mongodb\bin\mongo.exe,test
```

where:

- `c:\mongodb\bin\mongo.exe` is the full path to Mongo client;
- `test` is the name of the target database.

You must specify the correct arguments for each monitored component in the Script Arguments field. If you fail to do this, the monitor will return with a status error of "Undefined."

This template have been created on MongoDB 2.4.5.

Monitored Components

For details on monitors, see [SAM Component Monitor Types](page737).

Server: Global Lock Statistic

This monitor returns global lock statistics. The returned values are as follows:

- **Queue_total** – This component returns the current number of operations queued and waiting for the global lock.
- **Queue_readers** – This component returns the current number of operations queued and waiting on a read lock.
- **Queue_writers** – This component returns the current number of operations queued and waiting for a write lock.
- **Clients_total** – This component returns the total number of active clients connected to this server.
- **Clients_readers** – This component returns the total number of active clients currently performing read operations.
- **Clients_writers** – This component returns the total number of active clients currently performing write operations.

**Server: Connections Statistic**

This monitor returns connection statistics. The returned values are as follows:

- **Connections_current** – This component returns the number of currently active connections to this server.
- **Connections_available** – This component returns the number of available connections remaining. This value should be as high as possible.

**Server: Network Statistic**

This monitor returns network statistics. The returned values are as follows:

- **Network_bytes_in** – This component returns the total number of bytes sent to this database.
- **Network_bytes_out** – This component returns the total number of bytes sent from this database.
- **Network_requests** – This component returns the total number of requests that have been sent to this database.

**Server: Messages Statistic**

This monitor returns the messages statistic. The returned value for these components should be as low as possible.

- **Asserts_warnings** – This component returns the number of warnings raised since this process started.
- **Asserts_messages** – This component returns the number of message asserts. These are internal server errors that have a well-defined text string. Stack traces are logged.
- **Asserts_user_errors** – This component returns the number of user asserts. These are errors that can be generated by a user such as Out of Disk Space or Duplicate Key.

By default, this monitor has the Count statistic as difference box checked. It will show the total number of byte requests in the Message field while the Statistic field will only show the number of new byte requests since the last polling period.

**Server: Operations Statistic**

This monitor returns operations statistics. The returned values are as follows:

- **Insert** – This component returns the total number of inserts performed since this process started.
- **Query** – This component returns the total number of queries performed since this process started.
• **Update** – This component returns the total number of updates performed since this process started.

• **Delete** – This component returns the total number of deletes performed since this process started.

• **GetMore** – This component returns the total number of times getMore has been called on any cursor since this process started.

• **Command** – This component returns the total number of other commands performed since this process started.

By default, this monitor has the Count statistic as difference box checked. It will show the total number of operations in the Message field while the Statistic field will only show the new operations since the last polling period.

**Server: Other Statistic**

This monitor returns other MongoDB statistics. The returned values are as follows:

• **Memory_virtual** – This component returns the number of virtual memory megabytes for the mongod process. In general, virtual memory should be a little larger than mapped memory. If the virtual memory is significantly larger, this could indicate a memory leak. With journaling enabled, virtual memory is twice the amount of mapped memory.

• **Memory_mapped** – This component returns the number of megabytes of data mapped by the database. MongoDB memory maps all the data files. As a result, this number is likely to be similar to your total database(s) size.

• **Flushes_total** – This component returns the number of times the database has flushed writes to the disk.

• **Flushes_average_time** – This component returns the average number of milliseconds it takes to perform a single flush.

• **Cursors_opened** – This component returns the total number of cursors that the server is maintaining for clients.

• **Cursors_timed_out** – This component returns the number of cursors that have timed out since this server was started.

**Database Statistic**

This monitor returns database statistics. The returned values are as follows:

• **Collections** – This component returns the total number of collections in the database.

• **Objects** – This component returns the total number of objects in the database.

• **Average_Object_Size** – This component returns the average size of objects in the database, measured in bytes.

• **Data_Size** – This component returns the size of database files, measured in megabytes.

• **Indexes** – This component returns the total number of indexes in the database.

• **Index_Size** – This component returns the size of indexes in the database, measured in megabytes.

• **File_Size** – This component returns the total size of all files allocated for the database, measured in megabytes.
**MongoDB server TCP port**

This component monitor tests the ability of a MongoDB service to accept incoming sessions. By default, it monitors TCP port 27017.

**Process: mongod**

This monitors returns CPU and memory usage of the MongoDB server process.
MongoDB (Linux)

This template allows you to monitor the performance of MongoDB installed on a Linux machine by using Perl scripts.

Prerequisites

- SSH and Perl installed on the target server;
- SNMP installed on the target server;
- Permission to monitor mongod processes.

Credentials

User under which MongoDB were installed.

Each Linux/Unix monitor uses the same arguments structure.

For Example:

```bash
perl ${SCRIPT} /mongodb/bin/mongo test
```

where:

`/usr/bin/mongo` is the full path to Mongo client. On different Linux/Unix distributions this path could be different; `test` is the name of target database.

Notes:

- You must specify the correct arguments for each monitored component in the Script Arguments field. If you fail to do this, the monitor will return with a status error of "Undefined."
- This template have been created on MongoDB 2.4.5.
- These statistics can be obtained with any user with "read" or "readAnyDatabase" roles permissions if authentication is enabled. If not, it should be accessible through a localhost exception.

Monitored Components

For details on monitors, see [SAM Component Monitor Types](http://www.example.com).  

Server: Global Lock Statistic

This monitor returns global lock statistics. The returned values are as follows:

- **Queue_total** – This component returns the current number of operations queued and waiting for the global lock.
- **Queue_readers** – This component returns the current number of operations queued and waiting on a read lock.
- **Queue_writers** – This component returns the current number of operations queued and waiting for a write lock.
- **Clients_total** - This component returns the total number of active clients connected to this server.
- **Clients_readers** - This component returns the total number of active clients currently performing read operations.
- **Clients_writers** - This component returns the total number of active clients currently performing write operations.

**Server: Connections Statistic**

This monitor returns connection statistics. The returned values are as follows:

- **Connections_current** - This component returns the number of currently active connections to this server.
- **Connections_available** - This component returns the number of available connections remaining. This value should be as high as possible.

**Server: Network Statistic**

This monitor returns network statistics. The returned values are as follows:

- **Network_bytes_in** - This component returns the total number of bytes sent to this database.
- **Network_bytes_out** - This component returns the total number of bytes sent from this database.
- **Network_requests** - This component returns the total number of requests that have been sent to this database.

> By default, this monitor has the Count statistic as difference box checked. It will show the total number of byte requests in the Message field while the Statistic field will only show the number of new byte requests since the last polling period.

**Server: Messages Statistic**

This monitor returns the messages statistic. The returned value for these components should be as low as possible.

- **Asserts_warnings** - This component returns the number of warnings raised since this process started.
- **Asserts_messages** - This component returns the number of message asserts. These are internal server errors that have a well-defined text string. Stack traces are logged.
- **Asserts_user_errors** - This component returns the number of user asserts. These are errors that can be generated by a user such as Out of Disk Space or Duplicate Key.

> By default, this monitor has the Count statistic as difference box checked. It will show the total number of messages in the Message field while the Statistic field will only show the number of new messages since the last polling period.

**Server: Operations Statistic**

This monitor returns operations statistics. The returned values are as follows:
- **Insert** – This component returns the total number of inserts performed since this process started.
- **Query** – This component returns the total number of queries performed since this process started.
- **Update** – This component returns the total number of updates performed since this process started.
- **Delete** – This component returns the total number of deletes performed since this process started.
- **GetMore** – This component returns the total number of times getMore has been called on any cursor since this process started.
- **Command** – This component returns the total number of other commands performed since this process started.

By default, this monitor has the Count statistic as difference box checked. It will show the total number of operations in the Message field while the Statistic field will only show the new operations since the last polling period.

**Server: Other Statistic**

This monitor returns other MongoDB statistics. The returned values are as follows:

- **Memory virtual** – This component returns the number of virtual memory megabytes for the mongod process. In general, virtual memory should be a little larger than mapped memory. If the virtual memory is significantly larger, this could indicate a memory leak. With journaling enabled, virtual memory is twice the amount of mapped memory.
- **Memory mapped** – This component returns the number of megabytes of data mapped by the database. MongoDB memory maps all the data files. As a result, this number is likely to be similar to your total database(s) size.
- **Flushes total** – This component returns the number of times the database has flushed writes to the disk.
- **Flushes average time** – This component returns the average number of milliseconds it takes to perform a single flush.
- **Cursors opened** – This component returns the total number of cursors that the server is maintaining for clients.
- **Cursors timed out** – This component returns the number of cursors that have timed out since this server was started.

**Database Statistic**

This monitor returns database statistics. The returned values are as follows:

- **Collections** – This component returns the total number of collections in the database.
- **Objects** – This component returns the total number of objects in the database.
- **Average Object Size** – This component returns the average size of objects in the database, measured in bytes.
- **Data Size** – This component returns the size of database files, measured in megabytes.
- **Indexes** – This component returns the total number of indexes in the database.
- **Index Size** – This component returns the size of indexes in the database, measured in megabytes.
- **File Size** – This component returns the total size of all files allocated for the database, measured in megabytes.

**MongoDB server TCP port**

This component monitor tests the ability of a MongoDB service to accept incoming sessions. By default, it monitors TCP port 27017.

**Process: mongod**

This monitors returns CPU and memory usage of the MongoDB server process.
MySQL templates

Sam provides the following MySQL templates:

- MySQL (5.7.9 or later) for Linux/Unix
- MySQL (5.7.9 or later) for Windows
- MySQL (pre 5.7.9) for Linux/Unix
- MySQL (pre 5.7.9) for Windows

MySQL (5.7.9 or later) for Linux/Unix

This template assesses the performance of a MySQL Server database by retrieving performance data from the built-in performance_schema.global_status pseudo-table.

Works with the Orion Agent for Linux.

Prerequisites

MySQL 5.7.9 or later. MySQL ODBC must be installed on Orion server. Remote Access to MySQL Database Server must be enabled. Log into the MySQL database to monitor and execute the following query:

;CREATE USER USERNAME@ADDRESS IDENTIFIED BY "PASSWORD";

where:

USERNAME is a user with administrative privileges;
ADDRESS is the IP address of your Orion server;
PASSWORD is the user password.

Credentials

Database user name and password.

Configuration for Orion agent for Linux monitoring

For the following instructions, you should have MySQL installed on a Linux-based computer.

Depending on your Linux distribution, verify the example commands used. These examples use CentOS commands.

1. Login to the Linux-based computer with administrator privileges.
   You will need to create a user account on the server and in the MySQL database.

2. (Required) To begin, you should have unixODBC installed to support Microsoft Windows ODBC. If not, download and install the unixODBC driver to the Linux-based computer.
3. Install the **MySQL ODBC driver**.
   
   **Command:** `yum install mysql-connector-odbc`

4. Create a user account for the database.
   
   The following commands create a MySQL account of dbuser with the password Password1 for the database dbtest. The commands also grant all access to the user account.

   ```sql
   create database testdb;
   create user 'dbuser'@'localhost' identified by 'Password1';
   grant all on dbtest.* to 'dbuser' identified by 'Password1';
   ```

5. (Required) Grant the following access for local access to monitor through SAM and the Orion Platform.
   
   Enter the IP address of this MySQL Linux-based computer, replacing the example value of 10.100.100.100.

   ```sql
   mysql -uroot -p
   CREATE USER 'dbuser'@'%' IDENTIFIED BY 'Password1';
   GRANT ALL ON testdb.* TO dbuser@'%' IDENTIFIED BY 'Password1';
   GRANT SELECT ON performance_schema.* TO dbuser@'10.100.100.100' IDENTIFIED BY 'Password1';
   ```

6. Test access to the database using the newly created account credentials.
   
   **Command:** `mysql -u testuser -p`

Configure and assign a SAM template with the credentials.

1. In the Orion Web Console, click Settings > All Settings > SAM Settings > Manage Templates.

2. Search for the MySQL templates. SolarWinds recommends creating a copy of the template. Select a template based on version and click Copy.

3. Modify the settings of the template and component monitors based on the metrics you want to monitor.

4. To enter credentials, select the component monitor checkboxes and click Assign Credentials.

5. Enter the credentials you created for the database and click OK.

6. Test the access for the template by assigning it to a node. Click Test Node to assign and test the access. If you encounter issues, verify the credentials and privileges for the account.
Troubleshooting

Error: Data source name not found and no default driver specified. This error occurs on a CentOS system.

Solution: Verify the CentOS system has the mysql-connector-odbc installed. Use the following command to receive a package and version name on the target Linux-based computer: `rpm -q mysql-connector-odbc`

Verify you have the appropriate credentials assigned for each component monitor.

1. In the Orion Web Console, click Settings > All Settings > SAM Settings > Manage Templates.
2. Search for the SAM template. Select and click Edit.
3. Select the component monitor to check assigned credentials.
4. To modify, click Assign Credentials, enter credentials, and click OK.
5. Test the template.

If you continue to encounter issues, verify the appropriate driver is defined on the CentOS system to match the connection string, as shown in the next example.

```
cat /etc/odbcinst.ini
[MySQL]
Description=ODBC for MySQL
Driver=/usr/lib/x86_64-linux-gnu/odbc/libmyodbc.so
Setup=/usr/lib/x86_64-linux-gnu/odbc/libodbcmyS.so
UsageCount=1

[MySQL ODBC 5.3 Unicode Driver]
Driver=/usr/lib/x86_64-linux-gnu/odbc/libmyodbc.so
Setup=/usr/lib/x86_64-linux-gnu/odbc/libodbcmyS.so
UsageCount=1
```

Portions of this document are based on the following article:
http://dev.mysql.com/doc/refman/5.6/en/server-system-variables.html#sysvar_thread_cache_size
http://dba.stackexchange.com/questions/20083/whats-the-formula-for-calculating-key-efficiency-key-buffer-used-and-query-ca

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Components without predetermined threshold values provide guidance such as "Use the lowest threshold possible" or "Use the highest threshold possible" to help you find a threshold appropriate for your application.
Total Memory Used (MB)

This component monitor returns the possible total memory usage of MySQL, in MB, using the following formula: `read_buffer_size + sort_buffer_size) * max_connections + key_buffer_size`.

Kilobytes Received

This counter returns the number of kilobytes received from all clients.

This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

Kilobytes Sent

This counter returns the number of kilobytes sent to all clients.

This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

Created Temporary Disk Tables

This counter returns the number of internal, on-disk, temporary tables created by the server while executing statements. This value should be as low as possible.

If an internal temporary table is initially created as an in-memory table but becomes too large, MySQL automatically converts it to an on-disk table. The maximum size for in-memory temporary tables is the minimum of the `tmp_table_size` or `max_heap_table_size` values, whichever is less.

If the value returned from this counter is large, you may want to increase the value of `tmp_table_size` or `max_heap_table_size` to lessen the likelihood that internal temporary tables in memory will be converted to on-disk tables.

Created Temporary Files

This counter the number of temporary files MySQL has created.

This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

Opened Table Definitions

This counter returns the number of `.frm` files that have been cached.

This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.
Opened Tables

This counter returns the number of tables that have been opened. This should be as low as possible. If the value returned is large, you may want to increase the value of `table_open_cache`.

- This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

Opened Files

This counter returns the number of files that have been opened with the `my_open()` function.

- If the `my_open()` function is not used, the count will not be incremented.
- This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

Statements Executed

This counter returns the number of statements executed by the server.

- This includes only statements sent to the server by clients and no longer includes statements executed within stored programs, unlike the Queries variable. This variable does not count the following commands: `COM_PING`, `COM_STATISTICS`, `COM_STMT_PREPARE`, `COM_STMT_CLOSE`, or `COM_STMT_RESET`.
- This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

Key Reads

This counter returns the number of physical reads of a key block from disk. This value should be as low as possible. If the value returned from this counter is large, you may want to increase the value of `key_buffer_size`.

- This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

Key Writes

This counter returns the number of physical writes of a key block to disk.

- This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

Table Locks Immediate

This counter returns the number of times that a request for a table lock could be granted immediately.
Table Locks Waited

This counter returns the number of times that a request for a table lock could not be granted immediately and a wait was needed. This value should be as low as possible. If the counter returns a value that is high and you have performance problems, you may want to optimize your queries. You may also consider either splitting your tables or using replication.

Threads Cached

This counter returns the number of threads in the thread cache.

Threads Connected

This counter returns the number of currently open connections.

Threads Created

This counter returns the number of threads created to handle connections. This value should be as low as possible. If the counter returns a value that is high, you may want to increase the value of `thread_cache_size`.

Threads Running

This counter returns the number of threads that are running.

Up Time

This counter returns the number of seconds that the server has been up.

Transactions that use disk

This counter returns the number of transactions that used the temporary binary log cache but exceeded the value of `binlog_cache_size` and used a temporary file to store statements from the transaction. This value should be as low as possible.

Transactions that use cache

This counter returns the number of transactions that used the temporary binary log cache.
Joins that perform table scans

This counter returns the number of joins that perform table scans because they do not use indexes. If the returned value is not zero, you should carefully check the indexes of your tables.

Select_scan refers to a table that is completely read in sequence from the hard drive. For such tables Explain lists "All" in the "Type" column. Table scans are not desirable because they are slow (meaning they are limited by the speed of the hard drive). However, table scans are prevalent. It is not uncommon to see a server where 50% of all Select queries are Select_scan. The fundamental reason why a Select results in a table scan is because no index on the table can satisfy the conditions of the query (i.e., everything after Where), or there are no indexes, so all queries will result in a table scan. From a performance perspective it is safe to say you always want to decrease this value. However, in some cases this value may be increased after optimization because the server is then able to do more. Ultimately, it will have to decrease again when the QPS (queries per second) increases.

ℹ️ This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

Joins that check for key usage

This counter returns the number of joins without keys that check for key usage after each row. If this is not zero, you should carefully check the indexes of your tables.

Select_range_check is a little better than Select_full_join and uses the same range principles as Select_range. The difference is Select_range_check is not sure whether it can use a range to join the table so it keeps checking in case it finds that it can. This "uncertainty" is an effect of the join. With Select_range there is only one table, therefore, MySQL can be certain ahead of time. With multiple tables, the preceding tables may alter the range conditions and MySQL cannot be certain ahead of time. For such tables, Explain still lists type All because a type range is not certain. For such tables, MySQL also lists "Range checked for each record (index map: #)" in the "Extra" column. Like Select_range at least one of the tables require an index for this optimization to be possible, otherwise the table will probably cause a Select_full_join. If MySQL does use a range to join the table it will not increment Select_range, it still only increments Select_range_check.

ℹ️ This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

Joins that perform full scan

This counter returns the number of joins that did a full scan of the first table. This value should be as low as possible.

Select_full_join is the same as Select_scan with the difference being that Select_full_join applies to the second and subsequent tables in the join's plan for a multiple table query. For such tables, Explain lists type: All. Select_full_join results if there are no indexes on the table, or if no indexes can be used to join the table.
A query similar to: `SELECT * FROM tbl1, tbl2 WHERE tbl1.col1 = tbl2.col1;` without any indexes results in a `Select_scan` and a `Select_full_join`; `Select_scan` for the first table, and `Select_full_join` for the second. `Select_full_join` is no more desirable than `Select_scan`. Together, the two are even worse. When Explain lists type: All for each table in a join, "this output indicates that MySQL is generating a Cartesian product of all the tables; that is, every combination of rows," (MySQL manual). In simpler terms, two tables of 10 rows each joined together does not result in 20 rows, it results in 100 rows (10 multiplied by 10). In real-world applications, tables usually have at least a few thousand rows, so the cross product (a.k.a. Cartesian product) of even two small tables can quickly become enormous.

This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

**Slow Queries**

This counter returns the number of queries that have taken more than `long_query_time` seconds. The returned value should be less than 10.

To enable the slow query log, start `mysqld` with the `--log-slow-queries [=file_name]` option. The slow query log can be used to find queries that take a long time to execute and are therefore candidates for optimization.

This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

**Max Used Connections**

This counter returns the maximum number of connections that have simultaneously been in use since the server started.

**Free Memory in Query Cache (MB)**

This counter returns the amount of free memory in MB for the query cache.

**Queries Registered in Query Cache**

This counter returns the number of queries registered in the query cache.

This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

**Deleted Queries from Cache**

This counter returns the number of queries that were deleted from the query cache because of low memory. The value returned should consistently be zero.

This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

**Opened Connections**

This counter returns the number of active connections.
Aborted Connections

This counter returns the number of failed attempts to connect to the MySQL server.

This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

Aborted Clients

This counter returns the number of connections that were aborted because the client died without closing the connection properly.

This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

Thread Cache Size

This counter returns the number of threads the server should cache for reuse.

When a client disconnects, the client's threads are put in the cache. If there are fewer threads than the thread cache size, the threads remain in the cache. Requests for threads are satisfied by reusing threads taken from the cache, if possible. When the cache is empty, a new thread created.

This variable can be increased to improve performance if you have a lot of new connections. Normally, this does not provide noticeable performance improvement if you have good thread implementation. However, if your server sees hundreds of connections per second, you should set the thread cache size high enough so that most new connections use cached threads.

Slow Launch Threads

This counter returns the number of threads that have taken more than slow_launch_time seconds to create.

This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

Sort Scan

This counter returns the number of sorts that were done by scanning the table by using Order By or Group By commands.

This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

Sort Rows

This counter returns the number of sorted rows.
Sort_rows is a total count of the number of rows sorted in step two. Since step two can be bypassed in some cases, Sort_rows is not entirely inclusive. Also, since Sort_scan and Sort_range in step two are essentially the same, the Sort_rows value is not very indicative of anything. Suffice to say, most servers sort hundreds of millions of rows.

**Queries**

This counter returns the number of statements executed by the server.

**Key Read Efficiency**

This counter returns the ratio of the number of physical reads of a key block from the cache to the number of requests to read a key block from the cache in percentage. The MySQL performance is good if the value of Key Read Efficiency is 90 percent and above. Increasing the size of the cache improves the value of Key Read Efficiency and hence an improved performance.

**Key Write Efficiency**

This counter returns the ratio of the number of physical writes of a key block to the cache to the number of requests to write a key block to the cache in percentage. For a good performance of the MySQL server, the value of Key Write Efficiency must be 90 percent and above. If it is found less, then you can increase the size of the cache to improve the performance.

**Key Buffer Size**

This counter returns the size of the buffer used for index blocks. Also known as the key cache.

**MySQL Process**

This monitor checks whether MySQL is up and running.

**MySQL (5.7.9 or later) for Windows**

This template assesses the performance of a MySQL Server database by retrieving performance data from the built-in performance_schema.GLOBAL_STATUS pseudo-table.

**Prerequisites**

MySQL 5.7.9 or later. MySQL ODBC must be installed on Orion server. Remote Access to MySQL Database Server must be enabled. Log into the MySQL database to monitor and execute the following query:

```
;CREATE USER USERNAME@ADDRESS IDENTIFIED BY "PASSWORD";
```

where:

USERNAME is a user with administrative privileges;
ADDRESS is the IP address of your Orion server;

PASSWORD is the user password.

Credentials

Database user name and password.

Portions of this document are based on the following article:
http://dev.mysql.com/doc/refman/5.6/en/server-system-variables.html#sysvar_thread_cache_size
http://dba.stackexchange.com/questions/20083/whats-the-formula-for-calculating-key-efficiency-key-buffer-used-and-query-ca

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Components without predetermined threshold values provide guidance such as "Use the lowest threshold possible" or "Use the highest threshold possible" to help you find a threshold appropriate for your application.

Total Memory Used (MB)

This component monitor returns the possible total memory usage of MySQL, in MB, using the following formula: read_buffer_size+sort_buffer_size)*max_connections+key_buffer_size.

Kilobytes Received

This counter returns the number of kilobytes received from all clients.

This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

Kilobytes Sent

This counter returns the number of kilobytes sent to all clients.

This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

Created Temporary Disk Tables

This counter returns the number of internal, on-disk, temporary tables created by the server while executing statements. This value should be as low as possible.

If an internal temporary table is initially created as an in-memory table but becomes too large, MySQL automatically converts it to an on-disk table. The maximum size for in-memory temporary tables is the minimum of the tmp_table_size or max_heap_table_size values, whichever is less.
If the value returned from this counter is large, you may want to increase the value of `tmp_table_size` or `max_heap_table_size` to lessen the likelihood that internal temporary tables in memory will be converted to on-disk tables.

Created Temporary Files

This counter the number of temporary files MySQL has created.

Opened Table Definitions

This counter returns the number of `.frm` files that have been cached.

Opened Tables

This counter returns the number of tables that have been opened. This should be as low as possible. If the value returned is large, you may want to increase the value of `table_open_cache`.

Opened Files

This counter returns the number of files that have been opened with the `my_open()` function.

Statements Executed

This counter returns the number of statements executed by the server.

- This includes only statements sent to the server by clients and no longer includes statements executed within stored programs, unlike the Queries variable. This variable does not count the following commands: `COM_PING`, `COM_STATISTICS`, `COM_STMT_PREPARE`, `COM_STMT_CLOSE`, or `COM_STMT_RESET`.
Key Reads

This counter returns the number of physical reads of a key block from disk. This value should be as low as possible. If the value returned from this counter is large, you may want to increase the value of `key_buffer_size`.

Key Writes

This counter returns the number of physical writes of a key block to disk.

Table Locks Immediate

This counter returns the number of times that a request for a table lock could be granted immediately.

Table Locks Waited

This counter returns the number of times that a request for a table lock could not be granted immediately and a wait was needed. This value should be as low as possible. If the counter returns a value that is high and you have performance problems, you may want to optimize your queries. You may also consider either splitting your tables or using replication.

Threads Cached

This counter returns the number of threads in the thread cache.

Threads Connected

This counter returns the number of currently open connections.

Threads Created

This counter returns the number of threads created to handle connections. This value should be as low as possible. If the counter returns a value that is high, you may want to increase the value of `thread_cache_size`.

Threads Running

This counter returns the number of threads that are running.

Up Time

This counter returns the number of seconds that the server has been up.
Transactions that use disk

This counter returns the number of transactions that used the temporary binary log cache but exceeded the value of `binlog_cache_size` and used a temporary file to store statements from the transaction. This value should be as low as possible.

This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

Transactions that use cache

This counter returns the number of transactions that used the temporary binary log cache.

This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

Joins that perform table scans

This counter returns the number of joins that perform table scans because they do not use indexes. If the returned value is not zero, you should carefully check the indexes of your tables.

`Select_scan` refers to a table that is completely read in sequence from the hard drive. For such tables Explain lists "All" in the "Type" column. Table scans are not desirable because they are slow (meaning they are limited by the speed of the hard drive). However, table scans are prevalent. It is not uncommon to see a server where 50% of all `Select` queries are `Select_scan`. The fundamental reason why a `Select` results in a table scan is because no index on the table can satisfy the conditions of the query (i.e., everything after Where), or there are no indexes, so all queries will result in a table scan. From a performance perspective it is safe to say you always want to decrease this value. However, in some cases this value may be increased after optimization because the server is then able to do more. Ultimately, it will have to decrease again when the QPS (queries per second) increases.

This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

Joins that check for key usage

This counter returns the number of joins without keys that check for key usage after each row. If this is not zero, you should carefully check the indexes of your tables.

`Select_range_check` is a little better than `Select_full_join` and uses the same range principles as `Select_range`. The difference is `Select_range_check` is not sure whether it can use a range to join the table so it keeps checking in case it finds that it can. This "uncertainty" is an effect of the join. With `Select_range` there is only one table, therefore, MySQL can be certain ahead of time. With multiple tables, the preceding tables may alter the range conditions and MySQL cannot be certain ahead of time. For such tables, Explain still lists type All because a type range is not certain. For such tables, MySQL also lists "Range checked for each record (index map: #)" in the "Extra" column. Like `Select_range` at least one of the tables require an index for this optimization to be possible, otherwise the table will probably cause a `Select_full_join`. If MySQL does use a range to join the table it will not increment `Select_range`, it still only increments `Select_range_check`.
Joints that perform full scan

This counter returns the number of joins that did a full scan of the first table. This value should be as low as possible.

`Select_full_join` is the same as `Select_scan` with the difference being that `Select_full_join` applies to the second and subsequent tables in the join's plan for a multiple table query. For such tables, `Explain` lists type: All. `Select_full_join` results if there are no indexes on the table, or if no indexes can be used to join the table.

A query similar to: `SELECT * FROM tbl1, tbl2 WHERE tbl1.col1 = tbl2.col1;` without any indexes results in a `Select_scan` and a `Select_full_join`; `Select_scan` for the first table, and `Select_full_join` for the second. `Select_full_join` is no more desirable than `Select_scan`. Together, the two are even worse. When `Explain` lists type: All for each table in a join, "this output indicates that MySQL is generating a Cartesian product of all the tables; that is, every combination of rows," (MySQL manual). In simpler terms, two tables of 10 rows each joined together does not result in 20 rows, it results in 100 rows (10 multiplied by 10). In real-world applications, tables usually have at least a few thousand rows, so the cross product (a.k.a. Cartesian product) of even two small tables can quickly become enormous.

Slow Queries

This counter returns the number of queries that have taken more than `long_query_time` seconds. The returned value should be less than 10.

To enable the slow query log, start `mysqld` with the `--log-slow-queries=[file_name]` option. The slow query log can be used to find queries that take a long time to execute and are therefore candidates for optimization.

Max Used Connections

This counter returns the maximum number of connections that have simultaneously been in use since the server started.

Free Memory in Query Cache (MB)

This counter returns the amount of free memory in MB for the query cache.

Queries Registered in Query Cache

This counter returns the number of queries registered in the query cache.
Deleted Queries from Cache
This counter returns the number of queries that were deleted from the query cache because of low memory. The value returned should consistently be zero.

Opened Connections
This counter returns the number of active connections.

Aborted Connections
This counter returns the number of failed attempts to connect to the MySQL server.

Aborted Clients
This counter returns the number of connections that were aborted because the client died without closing the connection properly.

Thread Cache Size
This counter returns the number of threads the server should cache for reuse. When a client disconnects, the client's threads are put in the cache. If there are fewer threads than the thread cache size, the threads remain in the cache. Requests for threads are satisfied by reusing threads taken from the cache, if possible. When the cache is empty, a new thread created.

This variable can be increased to improve performance if you have a lot of new connections. Normally, this does not provide noticeable performance improvement if you have good thread implementation. However, if your server sees hundreds of connections per second, you should set the thread cache size high enough so that most new connections use cached threads.

Slow Launch Threads
This counter returns the number of threads that have taken more than slow_launch_time seconds to create.
Sort Scan
This counter returns the number of sorts that were done by scanning the table by using Order By or Group By commands.

Sort Rows
This counter returns the number of sorted rows.

Sort_rows is a total count of the number of rows sorted in step two. Since step two can be bypassed in some cases, Sort_rows is not entirely inclusive. Also, since Sort_scan and Sort_range in step two are essentially the same, the Sort_rows value is not very indicative of anything. Suffice to say, most servers sort hundreds of millions of rows.

Queries
This counter returns the number of statements executed by the server.

Key Read Efficiency
This counter returns the ratio of the number of physical reads of a key block from the cache to the number of requests to read a key block from the cache in percentage. The MySQL performance is good if the value of Key Read Efficiency is 90 percent and above. Increasing the size of the cache improves the value of Key Read Efficiency and hence an improved the performance.

Key Write Efficiency
This counter returns the ratio of the number of physical writes of a key block to the cache to the number of requests to write a key block to the cache in percentage. For a good performance of the MySQL server, the value of Key Write Efficiency must be 90 percent and above. If it is found less, then you can increase the size of the cache to improve the performance.

Key Buffer Size
This counter returns the size of the buffer used for index blocks. Also known as the key cache.

MySQL Process
This monitor checks whether MySQL is up and running.
MySQL (pre 5.7.9) for Linux/Unix

This template assesses the performance of a MySQL Server database by retrieving performance data from the built-in INFORMATION_SCHEMA.global_status pseudo-table.

Works with the Orion Agent for Linux.

Prerequisites

MySQL 5.7.9 or later. MySQL ODBC must be installed on Orion server. Remote Access to MySQL Database Server must be enabled. Log into the MySQL database to monitor and execute the following query:

```
;CREATE USER USERNAME@ADDRESS IDENTIFIED BY “PASSWORD”;
```

where:

USERNAME is a user with administrative privileges
ADDRESS is the IP address of your Orion server
PASSWORD is the user password

Credentials

Database user name and password.

Configuration for Orion agent for Linux monitoring

For the following instructions, you should have MySQL installed on a Linux-based computer.

Depending on your Linux distribution, verify the example commands used. These examples use CentOS commands.

1. Login to the Linux-based computer with administrator privileges.
   You will need to create a user account on the server and in the MySQL database.

2. (Required) To begin, you should have unixODBC installed to support Microsoft Windows ODBC. If not, download and install the unixODBC driver to the Linux-based computer.

3. Install the MySQL ODBC driver.
   Command: `yum install mysql-connector-odbc`

4. Create a user account for the database.
   The following commands create a MySQL account of dbuser with the password Password1 for the database dbtest. The commands also grant all access to the user account.

```
create database testdb;
create user 'dbuser'@'localhost' identified by 'Password1';
grant all on dbtest.* to 'dbuser' identified by 'Password1';
```
5. (Required) Grant the following access for local access to monitor through SAM and the Orion Platform.

Enter the IP address of this MySQL Linux-based computer, replacing the example value of 10.100.100.100.

```
mysql -uroot -p
CREATE USER 'dbuser'@'%' IDENTIFIED BY 'Password1';
GRANT ALL ON testdb.* TO dbuser@'%' IDENTIFIED BY 'Password1';
GRANT SELECT ON performance_schema.* TO dbuser@'10.100.100.100' IDENTIFIED BY 'Password1';
```

6. Test access to the database using the newly created account credentials.

Command: `mysql -u testuser -p`

Configure and assign a SAM template with the credentials.

1. In the Orion Web Console, click Settings > All Settings > SAM Settings > Manage Templates.
2. Search for the MySQL templates. SolarWinds recommends creating a copy of the template. Select a template based on version and click Copy.
3. Modify the settings of the template and component monitors based on the metrics you want to monitor.
4. To enter credentials, select the component monitor checkboxes and click Assign Credentials.
5. Enter the credentials you created for the database and click OK.
6. Test the access for the template by assigning it to a node. Click Test Node to assign and test the access. If you encounter issues, verify the credentials and privileges for the account.

**Troubleshooting**

**Error:** Data source name not found and no default driver specified. This error occurs on a CentOS system.

**Solution:** Verify the CentOS system has the mysql-connector-odbc installed. Use the following command to receive a package and version name on the target Linux-based computer: `rpm -q mysql-connector-odbc`

Verify you have the appropriate credentials assigned for each component monitor.

1. In the Orion Web Console, click Settings > All Settings > SAM Settings > Manage Templates.
2. Search for the SAM template. Select and click Edit.
3. Select the component monitor to check assigned credentials.
4. To modify, click Assign Credentials, enter credentials, and click OK.

5. Test the template.

If you continue to encounter issues, verify the appropriate driver is defined on the CentOS system to match the connection string, as shown in the next example.

```
cat /etc/odbcinst.ini
[MySQL]
Description=ODBC for MySQL
Driver=/usr/lib/x86_64-linux-gnu/odbc/libmyodbc.so
Setup=/usr/lib/x86_64-linux-gnu/odbc/libodbcmyS.so
UsageCount=1

[MySQL ODBC 5.3 Unicode Driver]
Driver=/usr/lib/x86_64-linux-gnu/odbc/libmyodbc.so
Setup=/usr/lib/x86_64-linux-gnu/odbc/libodbcmyS.so
UsageCount=1
```

Portions of this document are based on the following article:
http://dev.mysql.com/doc/refman/5.6/en/server-system-variables.html#sysvar_thread_cache_size
http://dba.stackexchange.com/questions/20083/whats-the-formula-for-calculating-key-efficiency-key-buffer-used-and-query-ca

**Monitored Components**

For details on monitors, see [SAM Component Monitor Types](#).

Components without predetermined threshold values provide guidance such as "Use the lowest threshold possible" or "Use the highest threshold possible" to help you find a threshold appropriate for your application.

**Total Memory Used (MB)**

This component monitor returns the possible total memory usage of MySQL, in MB, using the following formula: \( \text{read\_buffer\_size + sort\_buffer\_size} \times \text{max\_connections + key\_buffer\_size} \).

**Kilobytes Received**

This counter returns the number of kilobytes received from all clients.

This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

**Kilobytes Sent**

This counter returns the number of kilobytes sent to all clients.

This component has the Count statistic as difference option enabled. It will return the
Created Temporary Disk Tables

This counter returns the number of internal, on-disk, temporary tables created by the server while executing statements. This value should be as low as possible.

If an internal temporary table is initially created as an in-memory table but becomes too large, MySQL automatically converts it to an on-disk table. The maximum size for in-memory temporary tables is the minimum of the `tmp_table_size` or `max_heap_table_size` values, whichever is less.

If the value returned from this counter is large, you may want to increase the value of `tmp_table_size` or `max_heap_table_size` to lessen the likelihood that internal temporary tables in memory will be converted to on-disk tables.

Created Temporary Files

This counter the number of temporary files MySQL has created.

Opened Table Definitions

This counter returns the number of `.frm` files that have been cached.

Opened Tables

This counter returns the number of tables that have been opened. This should be as low as possible. If the value returned is large, you may want to increase the value of `table_open_cache`.

Opened Files

This counter returns the number of files that have been opened with the `my_open()` function.

Statements Executed

This counter returns the number of statements executed by the server.
This includes only statements sent to the server by clients and no longer includes statements executed within stored programs, unlike the Queries variable. This variable does not count the following commands: COM_PING, COM_STATISTICS, COM_STMT_PREPARE, COM_STMT_CLOSE, or COM_STMT_RESET.

This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

Key Reads
This counter returns the number of physical reads of a key block from disk. This value should be as low as possible. If the value returned from this counter is large, you may want to increase the value of key_buffer_size.

This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

Key Writes
This counter returns the number of physical writes of a key block to disk.

This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

Table Locks Immediate
This counter returns the number of times that a request for a table lock could be granted immediately.

This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

Table Locks Waited
This counter returns the number of times that a request for a table lock could not be granted immediately and a wait was needed. This value should be as low as possible. If the counter returns a value that is high and you have performance problems, you may want to optimize your queries. You may also consider either splitting your tables or using replication.

This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

Threads Cached
This counter returns the number of threads in the thread cache.

Threads Connected
This counter returns the number of currently open connections.
Threads Created

This counter returns the number of threads created to handle connections. This value should be as low as possible. If the counter returns a value that is high, you may want to increase the value of thread_cache_size.

Transactions that use disk

This counter returns the number of transactions that used the temporary binary log cache but exceeded the value of binlog_cache_size and used a temporary file to store statements from the transaction. This value should be as low as possible.

Transactions that use cache

This counter returns the number of transactions that used the temporary binary log cache.

Joins that perform table scans

This counter returns the number of joins that perform table scans because they do not use indexes. If the returned value is not zero, you should carefully check the indexes of your tables.

Select_scan refers to a table that is completely read in sequence from the hard drive. For such tables Explain lists "All" in the "Type" column. Table scans are not desirable because they are slow (meaning they are limited by the speed of the hard drive). However, table scans are prevalent. It is not uncommon to see a server where 50% of all Select queries are Select_scan. The fundamental reason why a Select results in a table scan is because no index on the table can satisfy the conditions of the query (i.e., everything after Where), or there are no indexes, so all queries will result in a table scan. From a performance perspective it is safe to say you always want to decrease this value. However, in some cases this value may be increased after optimization because the server is then able to do more. Ultimately, it will have to decrease again when the QPS (queries per second) increases.

Joins that check for key usage

This counter returns the number of joins without keys that check for key usage after each row. If this is not zero, you should carefully check the indexes of your tables.
Select_range_check is a little better than Select_full_join and uses the same range principles as Select_range. The difference is Select_range_check is not sure whether it can use a range to join the table so it keeps checking in case it finds that it can. This "uncertainty" is an effect of the join. With Select_range there is only one table, therefore, MySQL can be certain ahead of time. With multiple tables, the preceding tables may alter the range conditions and MySQL cannot be certain ahead of time. For such tables, Explain still lists type All because a type range is not certain. For such tables, MySQL also lists "Range checked for each record (index map: #)" in the "Extra" column. Like Select_range at least one of the tables require an index for this optimization to be possible, otherwise the table will probably cause a Select_full_join. If MySQL does use a range to join the table it will not increment Select_range, it still only increments Select_range_check.

1. This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

Joins that perform full scan

This counter returns the number of joins that did a full scan of the first table. This value should be as low as possible.

Select_full_join is the same as Select_scan with the difference being that Select_full_join applies to the second and subsequent tables in the join's plan for a multiple table query. For such tables, Explain lists type: All. Select_full_join results if there are no indexes on the table, or if no indexes can be used to join the table.

A query similar to: SELECT * FROM tbl1, tbl2 WHERE tbl1.col1 = tbl2.col1; without any indexes results in a Select_scan and a Select_full_join; Select_scan for the first table, and Select_full_join for the second. Select_full_join is no more desirable than Select_scan. Together, the two are even worse. When Explain lists type: All for each table in a join, "this output indicates that MySQL is generating a Cartesian product of all the tables; that is, every combination of rows," (MySQL manual). In simpler terms, two tables of 10 rows each joined together does not result in 20 rows, it results in 100 rows (10 multiplied by 10). In real-world applications, tables usually have at least a few thousand rows, so the cross product (a.k.a. Cartesian product) of even two small tables can quickly become enormous.

1. This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

Slow Queries

This counter returns the number of queries that have taken more than long_query_time seconds. The returned value should be less than 10.

1. To enable the slow query log, start mysqld with the --log-slow-queries[=filename] option. The slow query log can be used to find queries that take a long time to execute and are therefore candidates for optimization.

1. This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.
Max Used Connections
This counter returns the maximum number of connections that have simultaneously been in use since the server started.

Free Memory in Query Cache (MB)
This counter returns the amount of free memory in MB for the query cache.

Queries Registered in Query Cache
This counter returns the number of queries registered in the query cache.

Deleted Queries from Cache
This counter returns the number of queries that were deleted from the query cache because of low memory. The value returned should consistently be zero.

Opened Connections
This counter returns the number of active connections.

Aborted Connections
This counter returns the number of failed attempts to connect to the MySQL server.

Aborted Clients
This counter returns the number of connections that were aborted because the client died without closing the connection properly.

Thread Cache Size
This counter returns the number of threads the server should cache for reuse.

When a client disconnects, the client's threads are put in the cache. If there are fewer threads than the thread cache size, the threads remain in the cache. Requests for threads are satisfied by reusing threads taken from the cache, if possible. When the cache is empty, a new thread created.
This variable can be increased to improve performance if you have a lot of new connections. Normally, this does not provide noticeable performance improvement if you have good thread implementation. However, if your server sees hundreds of connections per second, you should set the thread cache size high enough so that most new connections use cached threads.

1. This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

**Slow Launch Threads**

This counter returns the number of threads that have taken more than slow_launch_time seconds to create.

1. This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

**Sort Scan**

This counter returns the number of sorts that were done by scanning the table by using Order By or Group By commands.

1. This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

**Sort Rows**

This counter returns the number of sorted rows.

Sort_rows is a total count of the number of rows sorted in step two. Since step two can be bypassed in some cases, Sort_rows is not entirely inclusive. Also, since Sort_scan and Sort_range in step two are essentially the same, the Sort_rows value is not very indicative of anything. Suffice to say, most servers sort hundreds of millions of rows.

1. This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

**Queries**

This counter returns the number of statements executed by the server.

1. This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

**Key Read Efficiency**

This counter returns the ratio of the number of physical reads of a key block from the cache to the number of requests to read a key block from the cache in percentage. The MySQL performance is good if the value of Key Read Efficiency is 90 percent and above. Increasing the size of the cache improves the value of Key Read Efficiency and hence an improved the performance.
Key Write Efficiency

This counter returns the ratio of the number of physical writes of a key block to the cache to the number of requests to write a key block to the cache in percentage. For a good performance of the MySQL server, the value of Key Write Efficiency must be 90 percent and above. If it is found less, then you can increase the size of the cache to improve the performance.

Key Buffer Size

This counter returns the size of the buffer used for index blocks. Also known as the key cache.

MySQL Process

This monitor checks whether MySQL is up and running.

MySQL (pre 5.7.9) for Windows

This template assesses the performance of a MySQL Server database by retrieving performance data from the built-in INFORMATION_SCHEMA.GLOBAL_STATUS pseudo-table.

Prerequisites

MySQL 5.7.9 or later. MySQL ODBC must be installed on Orion server. Remote Access to MySQL Database Server must be enabled. Log into the MySQL database to monitor and execute the following query:

```sql
;CREATE USER USERNAME@ADDRESS IDENTIFIED BY "PASSWORD";
```

where:

- **USERNAME** is a user with administrative privileges;
- **ADDRESS** is the IP address of your Orion server;
- **PASSWORD** is the user password.

Credentials

Database user name and password.

Portions of this document are based on the following article:

- [http://dba.stackexchange.com/questions/20083/whats-the-formula-for-calculating-key-efficiency-key-buffer-used-and-query-ca](http://dba.stackexchange.com/questions/20083/whats-the-formula-for-calculating-key-efficiency-key-buffer-used-and-query-ca)

Monitored Components

For details on monitors, see [SAM Component Monitor Types](#).

Components without predetermined threshold values provide guidance such as "Use the lowest threshold possible" or "Use the highest threshold possible" to help you find a threshold appropriate for your application.
Total Memory Used (MB)

This component monitor returns the possible total memory usage of MySQL, in MB, using the following formula: \( \text{read_buffer_size} + \text{sort_buffer_size} \) * \( \text{max_connections} + \text{key_buffer_size} \).

Kilobytes Received

This counter returns the number of kilobytes received from all clients.

1. This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

Kilobytes Sent

This counter returns the number of kilobytes sent to all clients.

1. This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

Created Temporary Disk Tables

This counter returns the number of internal, on-disk, temporary tables created by the server while executing statements. This value should be as low as possible.

If an internal temporary table is initially created as an in-memory table but becomes too large, MySQL automatically converts it to an on-disk table. The maximum size for in-memory temporary tables is the minimum of the \text{tmp_table_size} or \text{max_heap_table_size} values, whichever is less.

If the value returned from this counter is large, you may want to increase the value of \text{tmp_table_size} or \text{max_heap_table_size} to lessen the likelihood that internal temporary tables in memory will be converted to on-disk tables.

1. This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

Created Temporary Files

This counter the number of temporary files MySQL has created.

1. This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

Opened Table Definitions

This counter returns the number of .frm files that have been cached.

1. This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.
Opened Tables

This counter returns the number of tables that have been opened. This should be as low as possible. If the value returned is large, you may want to increase the value of `table_open_cache`.

- This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

Opened Files

This counter returns the number of files that have been opened with the `my_open()` function.

- If the `my_open()` function is not used, the count will not be incremented.
- This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

Statements Executed

This counter returns the number of statements executed by the server.

- This includes only statements sent to the server by clients and no longer includes statements executed within stored programs, unlike the Queries variable. This variable does not count the following commands: `COM_PING`, `COM_STATISTICS`, `COM_STMT_PREPARE`, `COM_STMT_CLOSE`, or `COM_STMT_RESET`.
- This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

Key Reads

This counter returns the number of physical reads of a key block from disk. This value should be as low as possible. If the value returned from this counter is large, you may want to increase the value of `key_buffer_size`.

- This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

Key Writes

This counter returns the number of physical writes of a key block to disk.

- This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

Table Locks Immediate

This counter returns the number of times that a request for a table lock could be granted immediately.

- This component has the Count statistic as difference option enabled. It will return the
Table Locks Waited

This counter returns the number of times that a request for a table lock could not be granted immediately and a wait was needed. This value should be as low as possible. If the counter returns a value that is high and you have performance problems, you may want to optimize your queries. You may also consider either splitting your tables or using replication.

Threads Cached

This counter returns the number of threads in the thread cache.

Threads Connected

This counter returns the number of currently open connections.

Threads Created

This counter returns the number of threads created to handle connections. This value should be as low as possible. If the counter returns a value that is high, you may want to increase the value of thread_cache_size.

Threads Running

This counter returns the number of threads that are running.

Up Time

This counter returns the number of seconds that the server has been up.

Transactions that use disk

This counter returns the number of transactions that used the temporary binary log cache but exceeded the value of binlog_cache_size and used a temporary file to store statements from the transaction. This value should be as low as possible.

Transactions that use cache

This counter returns the number of transactions that used the temporary binary log cache.

Joins that perform table scans

This counter returns the number of joins that perform table scans because they do not use indexes. If the returned value is not zero, you should carefully check the indexes of your tables.
Select_scan refers to a table that is completely read in sequence from the hard drive. For such tables Explain lists "All" in the "Type" column. Table scans are not desirable because they are slow (meaning they are limited by the speed of the hard drive). However, table scans are prevalent. It is not uncommon to see a server where 50% of all Select queries are Select_scan. The fundamental reason why a Select results in a table scan is because no index on the table can satisfy the conditions of the query (i.e., everything after Where), or there are no indexes, so all queries will result in a table scan. From a performance perspective it is safe to say you always want to decrease this value. However, in some cases this value may be increased after optimization because the server is then able to do more. Ultimately, it will have to decrease again when the QPS (queries per second) increases.

Joins that check for key usage

This counter returns the number of joins without keys that check for key usage after each row. If this is not zero, you should carefully check the indexes of your tables.

Select_range_check is a little better than Select_full_join and uses the same range principles as Select_range. The difference is Select_range_check is not sure whether it can use a range to join the table so it keeps checking in case it finds that it can. This "uncertainty" is an effect of the join. With Select_range there is only one table, therefore, MySQL can be certain ahead of time. With multiple tables, the preceding tables may alter the range conditions and MySQL cannot be certain ahead of time. For such tables, Explain still lists type All because a type range is not certain. For such tables, MySQL also lists "Range checked for each record (index map: #)" in the "Extra" column. Like Select_range at least one of the tables require an index for this optimization to be possible, otherwise the table will probably cause a Select_full_join. If MySQL does use a range to join the table it will not increment Select_range, it still only increments Select_range_check.

Joins that perform full scan

This counter returns the number of joins that did a full scan of the first table. This value should be as low as possible.

Select_full_join is the same as Select_scan with the difference being that Select_full_join applies to the second and subsequent tables in the join's plan for a multiple table query. For such tables, Explain lists type: All. Select_full_join results if there are no indexes on the table, or if no indexes can be used to join the table.
A query similar to: `SELECT * FROM tbl1, tbl2 WHERE tbl1.col1 = tbl2.col1;` without any indexes results in a `Select_scan` and a `Select_full_join`; `Select_scan` for the first table, and `Select_full_join` for the second. `Select_full_join` is no more desirable than `Select_scan`. Together, the two are even worse. When Explain lists type: All for each table in a join, "this output indicates that MySQL is generating a Cartesian product of all the tables; that is, every combination of rows," (MySQL manual). In simpler terms, two tables of 10 rows each joined together does not result in 20 rows, it results in 100 rows (10 multiplied by 10). In real-world applications, tables usually have at least a few thousand rows, so the cross product (a.k.a. Cartesian product) of even two small tables can quickly become enormous.

Slow Queries

This counter returns the number of queries that have taken more than `long_query_time` seconds. The returned value should be less than 10.

To enable the slow query log, start `mysql` with the `--log-slow-queries[=file_name]` option. The slow query log can be used to find queries that take a long time to execute and are therefore candidates for optimization.

Max Used Connections

This counter returns the maximum number of connections that have simultaneously been in use since the server started.

Free Memory in Query Cache (MB)

This counter returns the amount of free memory in MB for the query cache.

Queries Registered in Query Cache

This counter returns the number of queries registered in the query cache.

Deleted Queries from Cache

This counter returns the number of queries that were deleted from the query cache because of low memory. The value returned should consistently be zero.

Opened Connections

This counter returns the number of active connections.
Aborted Connections

This counter returns the number of failed attempts to connect to the MySQL server.

- This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

Aborted Clients

This counter returns the number of connections that were aborted because the client died without closing the connection properly.

- This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

Thread Cache Size

This counter returns the number of threads the server should cache for reuse.

When a client disconnects, the client's threads are put in the cache. If there are fewer threads than the thread cache size, the threads remain in the cache. Requests for threads are satisfied by reusing threads taken from the cache, if possible. When the cache is empty, a new thread created.

This variable can be increased to improve performance if you have a lot of new connections. Normally, this does not provide noticeable performance improvement if you have good thread implementation. However, if your server sees hundreds of connections per second, you should set the thread cache size high enough so that most new connections use cached threads.

- This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

Slow Launch Threads

This counter returns the number of threads that have taken more than slow_launch_time seconds to create.

- This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

Sort Scan

This counter returns the number of sorts that were done by scanning the table by using Order By or Group By commands.

- This component has the Count statistic as difference option enabled. It will return the difference between two polling intervals.

Sort Rows

This counter returns the number of sorted rows.
Sort_rows is a total count of the number of rows sorted in step two. Since step two can be bypassed in some cases, Sort_rows is not entirely inclusive. Also, since Sort_scan and Sort_range in step two are essentially the same, the Sort_rows value is not very indicative of anything. Suffice to say, most servers sort hundreds of millions of rows.

Queries

This counter returns the number of statements executed by the server.

Key Read Efficiency

This counter returns the ratio of the number of physical reads of a key block from the cache to the number of requests to read a key block from the cache in percentage. The MySQL performance is good if the value of Key Read Efficiency is 90 percent and above. Increasing the size of the cache improves the value of Key Read Efficiency and hence an improved the performance.

Key Write Efficiency

This counter returns the ratio of the number of physical writes of a key block to the cache to the number of requests to write a key block to the cache in percentage. For a good performance of the MySQL server, the value of Key Write Efficiency must be 90 percent and above. If it is found less, then you can increase the size of the cache to improve the performance.

Key Buffer Size

This counter returns the size of the buffer used for index blocks. Also known as the key cache.

MySQL Process

This monitor checks whether MySQL is up and running.
Nagios Linux File & Directory Count Script

This template uses one Nagios script monitor to provide file and directory count statistics using multiple value script outputs.

Works with the Orion agents for Linux and AIX.

Prerequisites

SSH and Perl installed on the target server.

Credentials

Root credentials on the target server.

A maximum of 10 output pairs can be returned. The monitor in this template uses three.

Prerequisites for Orion agent for Linux

This template uses the Nagios Script monitor. You need to include credentials that can run scripts on the monitored Linux-based computer. Agentless monitoring does not require these credentials.

If you are using this component monitor with Nagios and polled by Orion agent for Linux, you need to enter a script as follows. The argument would be `python $(SCRIPT)` with a body of:

```python
from random import randint
STAT_PAIRS_COUNT = 10

for stat_id in range(STAT_PAIRS_COUNT):
    print 'Statistic.random%d: %d\nMessage.random%d: %s' % (stat_id, randint(1,100), stat_id, 'random number: ' + str(randint(1,100)))
```

For details on the component monitor, see Nagios Script monitor.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

File & Directory Count Monitor

This component monitor uses SSH to upload a script to a server, runs the script, then processes the script exit code and text output. Statistic: Defined by the script. This component monitor has the ability to return multiple results and has the ability to process Nagios resulting output.

If you are using this component monitor with Nagios and polled by Orion agent for Linux, you
need to enter a script as follows. The argument would be `python $(SCRIPT)` with a body of:

```python
from random import randint
STAT_PAIRS_COUNT = 10

for stat_id in range(STAT_PAIRS_COUNT):
    print 'Statistic.random%d: %d
Message.random%d: %s' % (stat_id, randint(1,100), stat_id, 'random number: ' + str(randint(1,100)))
```

### Field Descriptions

#### Description
This field allows you to provide a description as to what this monitor will actually do for easy reference.

#### Component Type
This describes the type of monitor you are using.

#### Enable Component
This option determines if the component is enabled. Disabling this component leaves it in the application as deactivated and does not influence application availability or status.

#### Credential for Monitoring
Select a credential that can access the Linux or Unix server over SSH and that has sufficient rights to run scripts.

Click a credential in the list, or use the <Inherit credential from node> option. If the credential you need is not in the credentials list, add it in the Credentials Library that you can access by clicking Settings > All Settings > SAM Settings in the Orion Web Console.

#### Port Number
This field allows you to specify the port number used for the SSH connection. The default value is 22.

#### Script Working Directory
This field allows you to specify the working directory of the script process.

#### Check Type
This determines how the return code is evaluated.

<table>
<thead>
<tr>
<th>RETURN CODE</th>
<th>SERVICE STATE</th>
<th>HOST STATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Ok</td>
<td>Up</td>
</tr>
<tr>
<td>1</td>
<td>Warning</td>
<td>Up or Down/Unreachable†</td>
</tr>
<tr>
<td>Return Code</td>
<td>Service State</td>
<td>Host State</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>2</td>
<td>Critical</td>
<td>Down/Unreachable</td>
</tr>
<tr>
<td>3</td>
<td>Unknown</td>
<td>Down/Unreachable</td>
</tr>
</tbody>
</table>

† If the Use Aggressive Host Checking option is enabled, return codes of 1 will result in a host state of DOWN, otherwise return codes of 1 will result in a host state of UP.

**Command Line**

This field is in the script editing window and allows you to specify the script you want to run on the target node followed by the arguments. To enter your script, click the Edit button that reveals the script editing window. For more information, see [http://nagios.sourceforge.net/docs/3.0/pluginapi.html](http://nagios.sourceforge.net/docs/3.0/pluginapi.html).

In this template, the following code is used in the Command Line field:

```perl
perl ${SCRIPT} /etc -sub
```

**Body**

This field is in the script editing window and allows you to enter your script via typing or pasting. In this template, the following code is used in the Script Body field to provide three script outputs:

Parameters:

- directory - This is the path of the directory (e.g. /bin,/etc,/usr/local,/).
- -sub - Include subdirectories. This parameter is optional.

1 This Perl script counts the number of files, directories, and symbolic links in a given directory.

```perl
#!/usr/bin/perl
if ($#ARGV != 0 && $#ARGV != 1) {
    print "Invalid arguments count. Usage: perl FileCount.pl directory\n";
    exit 3;
}
$dir=$ARGV[0];
$sub="";
if ($#ARGV == 1) {
    $sub=$ARGV[1];
}
if ($sub ne "-sub") {
    $fcount=`find $dir -maxdepth 1 -type f | wc -l`;
    $dcount=`find $dir -maxdepth 1 -type d | wc -l`;
}`
```
Script Output #X

Each script output has the following fields:

- **Unique ID** - This is the statistic identifier from the script output.
- **Display Name** - This is the name displayed in the User Interface. After generation of the script output, the Unique ID and Display Name become the same. You can change the Display Name to something more user friendly if you so desire.
- **Convert Value** - If this option is selected, you can convert your output with a variety of mathematical functions to suit your needs using either a selection from the drop down menu or selecting Custom Conversion. With the Custom Conversion option, you can enter your own formulas to manipulate the data output further.
- **Warning threshold** - Select a threshold level in conjunction with the logical operators to alert you when the warning threshold has been breached.
- **Critical Threshold** - Select a threshold level in conjunction with the logical operators to alert you when the critical threshold has been breached.

**Status Roll-Up**

This option allows you to choose how you would like the monitor to report based on the output provided by the script. The default selection is “Show worst status.”
User Notes

This field allows you to add notes for easy reference. You can access this field by using the variable, ${UserNotes}.

Linux/Unix Script monitor

This component monitor uses SSH to upload a script to a Linux/Unix server, runs the script on the server, and then processes the return value and text output. To create this monitor, see Create a Linux or Unix script monitor.

💡 To use scripts with Nagios formats, we recommend using the Nagios Script monitor.

Statistic

The statistic for this component monitor is the Statistic value returned by the script.

ℹ️ A maximum of 10 output pairs can be returned. If you exceed the maximum allowed, remove the excess output pairs or they will simply be ignored.

Prerequisites for Orion agent for Linux

You need to include credentials that can run scripts on the monitored Linux-based computer. Agentless monitoring does not require these credentials.

You need to verify your installation of python and python-xml. Depending on your Linux distribution, you may have need to install these libraries. You can verify your Python installed libraries with the following command:

```
python -c "import sys; from xml.dom.minidom import parseString; print sys.version"
```

See the Python site for documentation and install commands. The following command typically updates and installs the required Python libraries:

```
apt-get install python
```

Depending on your Linux distribution, you may need to verify install and configure specific applications and services to use the Linux/Unix Script monitor. For example, to use the Linux/Unix Script monitor with Apache services (as with the Apache template), you need to configure Apache access. For full configuration details for all services, see Linux/Unix system configurations for component monitors.

Troubleshooting high CPU usage

This component monitor uses SSH for connecting to target machines. Due to supported key exchange algorithms, the JobWorker process used by SAM may encounter high CPU usage. If the issue is due to the algorithm, you can modify the order of supported algorithms. If you have concerns making these changes, contact Support.

1. Locate the file c:\Program Files (x86)\SolarWinds\Orion\APM\SolarWinds.APM.Probes.dll.config.
2. Edit the text file and locate:

```xml
<LinuxScriptSettings PromptWait="2" ColumnCount="200"
TemporaryScriptFileNamePrefix="APM_" />
```

3. Modify the order of algorithms, such as:

```xml
<LinuxScriptSettings PromptWait="2" ColumnCount="200"
TemporaryScriptFileNamePrefix="APM_"
KeyExchangeList="diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group1-sha1,diffie-hellman-group14-sha1" />
```

4. Save changes.

**Field Descriptions**

**Description**

This field provides a default description of the monitor. You can override the default description by adding to or replacing the text, which is automatically saved. The variable to access this field is `${UserDescription}`.

**Enable Component**

Determines whether the component is enabled. Disabling the component leaves it in the application in a deactivated state not influencing either SolarWinds SAM application availability or status.

**Authentication Type**

Choose either User name and Password or User name and Private Key. The second option allows you to use certificates for authentication.

**Credential for Monitoring**

Select a credential from the list provided or use the `<Inherit credential from node>` option. If the credential you need is not in the credentials list, add it in the Credentials Library that you can access by clicking Settings > All Settings > SAM Settings in the Orion Web Console.

When providing credentials, make sure that the account:

- Can access the Linux or Unix server over SSH.
- Has sufficient rights to run scripts.
- Exists on the system receiving the executed script.

To learn about credentials used by Orion agents, see the [Orion Platform Administrator Guide](#).

> If you do not enter credentials or use the Inherit-from-node option, the monitor executes the script using the agent credentials (SWIAgent). These credentials may not have the elevated permissions required for executing scripts.

**Port Number**

This field allows you to specify the port number used for the SSH connection. The default value for this field is 22.

**Script Working Directory**

This field allows you to specify the working directory of the script process.
**Count Statistic as Difference**

Changes the statistic to be the difference in query values between polling cycles.

**Command Line**

This field allows you to specify the shell command run after the SSH connection is established. The default command line value `perl ${SCRIPT} arg1 arg2` attempts to run in a Perl interpreter the script defined in the Script Body field using the parameters `arg1` `arg2`.

The length of the Command Line field is limited to 266 characters for Solaris systems, minus the length of the `${SCRIPT}` variable after being resolved to a file name such as the following: APM_937467589.pl. Since the length of the file name will typically be around 16 characters, this means that the actual user Command Line input cannot be longer than 266 – 16, or about 250 characters (not including the length of the 9 characters for the “${SCRIPT}” variable itself).

If you need to pass a longer command line to the target node, you can create a shell script on the target node (for example `myscript.sh`) that contains the long command line, and place the call to this script in the Command Line field, for example: `/opt/sw/myscript.sh`

**Script Body**

This field allows you to specify the script you want to run on the Linux or Unix server.

**Status Roll-Up**

This option allows you to choose how you would like the monitor to report based on the output provided by the script. The default selection is “Show worst status.”

**User Notes**

This field allows you to add notes for easy reference. You can access this field by using the variable, `${UserNotes}`.

---

**Create a Linux or Unix script monitor**

Linux and Unix Script component monitors allow you to execute a command line script that can return statistical data. When collecting information for this monitor, SAM runs the script with the credentials defined with the Credential Library.

A maximum of 10 output pairs can be monitored per script monitor. More than 10 defined pairs results in a failure of the monitor.

Adapt an existing Perl script to a Linux/Unix Script component monitor in a new template

1. In the Orion Web Console, click Settings > All Settings > SAM Settings > Create a new template, and then name the template
2. Click Add Component Monitor, expand the Custom Component Monitors group, and then select Linux/Unix Script Monitor.

3. Click Submit then select credentials with SSH permissions in the Credential for Monitoring field.

4. Type a valid working directory in the Script Working Directory field

5. Click Edit to open the script dialog and enter your script into the Script Body field.

6. Type the Linux command that runs the script in the Command Line field. It should be similar to the following:
   perl ${SCRIPT} arg1 arg2.

   {SCRIPT} is replaced by the actual file name of the script after it's deployed to the target node. A temporary file is created in temp directory for the script.

7. Click Get Script Output. SAM then tests the script by executing it and parse its output, then return the values.

8. Click Save, then specify the critical and warning thresholds and click Submit.

Here is a sample Perl script using the Linux/Unix component monitor returning multiple output pairs, in this case, two:

```
#!/usr/bin/perl
if (@ARGV[0] =~ /help/) {
    print "MemoryUsage.pl SNMPver community hostname\n";
    print "SNMPver - version of SNMP protocol\n";
    print "community - community name of SNMP protocol\n";
    print "hostname - Target host\n";
    exit 1;
}
# Get hostname and trim newline
$localhost = \`hostname\`;
$localhost =~ s/\s*$//g;
$hostname = shift ||
$localhost;$community = shift || "public";
$version = shift || "v1";
$results = "";
$MIB_TotalMemory = "UCD-SNMP-MIB::memTotalReal.0";
#$MIB_TotalMemory = "UCD-SNMP-MIB::memTotalReal.0";
$outres = "snmpget -$version -c $community $hostname $MIB_TotalMemory |";
open(OUTMEM,$outres) || die "Unable read pipe\n";
while ($line = &lt;OUTMEM&gt;) {
    if ($line =~ /INTEGER\b/) {
        $indval = index($line,="");
```

The code in red shows where the output pairs are defined.
Below is the output from this script:

```
Script Output: Message.1: Available memory at host "lab-fedora32": 1027012 in kB
Statistic.1: 1027012
Message.2: Again, the available memory at host "lab-fedora32": 1027012 in kB
Statistic.2: 1027012
```

Linux/Unix scripts

Linux/Unix scripts are uploaded by SSH and then run on the target node using the string from the Command Line field.

You can use the following variable in the command line field:

- `${SCRIPT}` - Replaced with the script body.

You can use the following variables in the script body field:

- `${IP}` - Replaced with the target node's IP address.
- `${USER}` - Replaced with the user name from the credential.
- `${PASSWORD}` - Replaced with the password from the credential.

Example scripts

There are several sample scripts installed with SolarWinds SAM you can use to create Linux/Unix script component monitors. These sample scripts are installed on your Orion server, in the following folder:

```
C:\Program Files\SolarWinds\Orion\APM\SampleScriptMonitors\LinuxScripts
```

Scripts must report status through exit codes

Scripts must report their status by exiting with the appropriate exit code. The exit code is used to report the status of the monitor, which is seen by the user through the interface.
To correctly create this component monitor, you must first return an exit code which results in an Up (0), Warning (2), or Critical (3) status. When one of these exit codes is received the appropriate dynamic evidence table structure is created and all further exit codes are handled correctly. If the component only returns Down (1) or Unknown (4) on first use, the appropriate dynamic evidence table structure is not created appropriately.

<table>
<thead>
<tr>
<th>EXIT CODE</th>
<th>MEANING</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Up</td>
</tr>
<tr>
<td>1</td>
<td>Down</td>
</tr>
<tr>
<td>2</td>
<td>Warning</td>
</tr>
<tr>
<td>3</td>
<td>Critical</td>
</tr>
<tr>
<td>Any other value</td>
<td>Unknown, for example 4</td>
</tr>
</tbody>
</table>

For example, if you want to inform SolarWinds SAM that a script reports an Up status, exit the script using code similar to the following, where 0 reports Up: `Wscript.quit(0)`

**Scripts with Text Output**

Scripts report additional details by sending text to the script's standard output.

SAM supports multiple values returned by a script using the following format.

Statistic.Name1: xMessage.Name1: abc
Statistic.Name2: yMessage.Name2: abc

<table>
<thead>
<tr>
<th>DETAIL TYPE</th>
<th>REQUIRED</th>
<th>MEANING</th>
</tr>
</thead>
<tbody>
<tr>
<td>Statistic</td>
<td>Yes</td>
<td>A numeric value used to determine how the monitor compares to its set thresholds. This must be an integer value. Negative numbers are supported. Statistic.Name1: 123 Statistic.Name2: 456</td>
</tr>
<tr>
<td>Message</td>
<td>No</td>
<td>An error or information message to be displayed in the monitor status details. Note: Multi-line messages are supported. To use this functionality, print each line using a separate command. For example: Message.Name1: abc Message.Name2: def</td>
</tr>
</tbody>
</table>

There is a limit of ten Statistic and Message pairs for the script. These can be placed anywhere in the script output. The Statistic and Message names you give must contain valid letters and/or numbers.

Sample output:
# Script comment: This shows two pairs. Ten pairs are possible.
Statistic.CPU: 31.08
Message.CPU: svchost.exe cpu usage

Statistic.RAM: 1234.56
Message.RAM: svchost.exe ram usage

Nagios scripting

If you are using this component monitor with Nagios and polled by Orion agent for Linux, you need to enter a script as follows. The argument would be `python $(SCRIPT)` with a body of:

```python
from random import randint
STAT_PAIRS_COUNT = 10

for stat_id in range(STAT_PAIRS_COUNT):
    print 'Statistic.random%d: %d
Message.random%d: %s' % (stat_id, randint(1,100), stat_id, 'random number: ' + str(randint(1,100)))
```

To use scripts with Nagios formats, we recommend using the [Nagios Script monitor](http://nagios.sourceforge.net/docs/3_0/pluginapi.html).

Nagios Script monitor

This component uses SSH to upload a Nagios script to a Linux/Unix server, runs the Nagios script on the server and then processes the script's exit code and text output. This monitor can return multiple values.

**Statistic**

The statistic for this component monitor is the value returned by the script. This component monitor can return multiple results and process Nagios resulting output. For more information, see [http://nagios.sourceforge.net/docs/3_0/pluginapi.html](http://nagios.sourceforge.net/docs/3_0/pluginapi.html).

A maximum of 10 output pairs can be returned. If you exceed the maximum allowed, remove the excess output pairs or they are ignored.

**Prerequisites for Orion agent for Linux**

Include credentials that can run scripts on the monitored Linux-based computer. Agentless monitoring does not require these credentials.

If you are using this component monitor with Nagios and polled by Orion agent for Linux, you need to enter a script as follows. The argument would be `python $(SCRIPT)` with a body of:

```python
from random import randint
STAT_PAIRS_COUNT = 10
```
for stat_id in range(STATPAIRS_COUNT):
    print 'Statistic.random%d: %d\nMessage.random%d: %s' % (stat_id, randint(1,100), stat_id, 'random number: ' + str(randint(1,100)))

Troubleshooting high CPU usage

This component monitor uses SSH to connect to target machines. Due to supported key exchange algorithms, the Job Worker process used by SAM may encounter high CPU usage. If the issue is due to the algorithm, you can modify the order of supported algorithms. If you have concerns making these changes, contact Support.

1. Locate the file c:\Program Files (x86)\SolarWinds\Orion\APM\SolarWinds.APM.Probes.dll.config.
2. Edit the text file and locate
   <LinuxScriptSettings PromptWait="2" ColumnCount="200"
   TemporaryScriptFileNamePrefix="APM_" />
3. Modify the order of algorithms, such as:
   <LinuxScriptSettings PromptWait="2"
   ColumnCount="200" TemporaryScriptFileNamePrefix="APM_"
   KeyExchangeList="diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group1-shal,diffie-hellman-group14-shal" />
4. Save changes.

Field Descriptions

Description

This field provides a default description of the monitor. You can override the default description by adding to or replacing the text, which is automatically saved. The variable to access this field is `${UserDescription}`.

Component Type

This describes the type of monitor you are using.

Enable Component

This option determines if the component is enabled. Disabling this component leaves it in the application as deactivated and does not influence application availability or status.

Authentication Type

Choose either User name and Password or User name and Private Key. The second option allows you to use certificates for authentication.

Credential for Monitoring

Select a Windows credential that is both a user who can log on to the Orion server, and has sufficient rights on the target node to do whatever the script needs to do. For example, if the script does something with WMI, the credentials also need WMI rights on the target node.
Click a credential in the list, or use the <Inherit credential from node> option. If the credential you need is not in the credentials list, add it in the Credentials Library that you can access by clicking Settings > All Settings > SAM Settings in the Orion Web Console.

Port Number

This field allows you to specify the port number used for the SSH connection. The default value is 22.

Script Working Directory

This field allows you to specify the working directory of the script process.

Check Type

Set the check type to Service or Host. To prevent false positives, Nagios allows you to define how many times a service or host should be (re)checked before alerting for an issue. Depending on the select, the monitor checks using the configured value on the server for max_check_attempts option in the host and service definitions.

Count Statistic as Difference

Changes the statistic to be the difference in query values between polling cycles.

Command Line

This field is in the script editing window and allows you to specify the script you want to run on the target node followed by the arguments. To enter your script, click the Edit button that reveals the script editing window. For more information, see http://nagios.sourceforge.net/docs/3.0/pluginapi.html.

1 The length of the Command Line field is limited to 266 characters for Solaris systems, minus the length of the ${SCRIPT} variable after being resolved to a file name such as the following: APM_937467589.pl. Since the length of the file name will typically be around 16 characters, this means that the actual user Command Line input cannot be longer than 266 - 16, or 250 characters (not including the length of the 9 characters for the "${SCRIPT}" variable itself). If you need to pass a longer command line to the target node, you can create a shell script on the target node (for example: myscript.sh) that contains the long command line and place the call to this script in the Command Line field, for example: /opt/sw/myscript.sh

Script Body

This field is in the script editing window and allows you to enter your script via typing or pasting. You can test the script to receive output definitions. You can save these definitions to the component monitor for further configurations. Every saved definition is listed as Script Output with an assigned number and name. See Test script output for details.

Status Roll-Up

This option allows you to choose how you would like the monitor to report based on the output provided by the script. The default selection is “Show worst status.”
User Notes

This field allows you to add notes for easy reference. You can access this field by using the variable, `${UserNotes}`.

Scripts must report status through return codes

Nagios determines the status of a host or service by evaluating the return code. The following table shows a list of valid return codes, along with their corresponding service or host states.

To correctly create this component monitor, you must first return an exit code which results in an Up (0), Warning (2), or Critical (3) status. When one of these exit codes is received the appropriate dynamic evidence table structure is created and all further exit codes are handled correctly. If the component only returns Down (1) or Unknown (4) on first use, the appropriate dynamic evidence table structure is not created appropriately.

<table>
<thead>
<tr>
<th>RETURN CODE</th>
<th>SERVICE STATE</th>
<th>HOST STATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>OK</td>
<td>Up</td>
</tr>
<tr>
<td>1</td>
<td>Warning</td>
<td>Up or Down/Unreachable†</td>
</tr>
<tr>
<td>2</td>
<td>Critical</td>
<td>Down/Unreachable</td>
</tr>
<tr>
<td>3</td>
<td>Unknown</td>
<td>Down/Unreachable</td>
</tr>
</tbody>
</table>

†If the Use Aggressive Host Checking option is enabled, return codes of 1 will result in a host state of Down, otherwise return codes of 1 will result in a host state of Up.

Nagios scripts must exit with a valid return code and a line of text output. The exit code determines the status of the component. If the exit code is 0 (OK), the component status may be further modified by thresholds from the optional statistics. To return up to ten optional statistics, separate the statistics from the status message with the pipe (|) symbol using the following syntax:

```
statusMessage | [statisticName]=value
```

Below is an example of valid output with a status message and two statistics:

```
The script ran. | 'CPU%'=75.2 'MemoryRemainingInKB'=600784
```

Test script output

You should test the script output while editing the script prior to testing the script in the template or application component pages. If the output formatting or values are not correctly defined or missing, you may receive an error: "Script output values are not defined or improperly defined." This error displays if the named fields could not be located in the script output.

To test the script and save output definitions:
1. Open the template or application monitor using the Nagios Script monitor. To open, click Settings > All Settings > SAM Settings > Manage Application Monitors. Locate and edit the application monitor or template with the Nagios Script monitor.

2. Locate and expand the component using the Nagios Script monitor type in the template.

3. Locate the Script Body field and click Edit Script.

4. On the Edit Script dialog, click Get Script Output. You may be prompted to specify a test node and credentials.

5. Wait for the Output Result. The results should populate with values returned by the script. Review the results to ensure all formatting is correct and fields properly load.

   ▪ If you receive an error, you may have an issue in the script. For more information on formatting and outputs, see [http://nagios.sourceforge.net/docs/3_0/pluginapi.html](http://nagios.sourceforge.net/docs/3_0/pluginapi.html).

6. You can store the output definitions returned by the script test as Script Output in the component monitor. Click Save to add the output definitions. The component monitor will display the definitions with a unique ID, display name, and additional configuration options.

7. To save changes to the template or application monitor, click Submit.
Novell GroupWise

The following templates are available:

- Novell GroupWise Message Transfer Agent (Unix)
- Novell GroupWise Message Transfer Agent (Windows)
- Novell GroupWise Post Office Agent (Unix)
- Novell GroupWise Post Office Agent (Windows)
Novell GroupWise Message Transfer Agent (Unix)

This template allows you to check GroupWise Message Transfer Agent (MTA) statistics by retrieving it from MTA's webpage.

Prerequisites

Perl must be installed on the target server. SNMP installed on the target server and permission to monitor gwmta processes.

Credentials

Root on target server.

Monitored Components

For details on monitors, see [SAM Component Monitor Types](#).

**Message Transfer Agent: Statistic 1**

This monitor returns different MTA statistics. The returned values are as follows:

- **Total Domains** - This component returns the total number of domains the MTA links to.
- **Closed Domains** - This component returns the number of domains that are currently closed.
- **Total Post Offices** - This component returns the total number of post offices in the domain.
- **Closed Post Offices** - This component returns the number of post offices that are currently closed.
- **Total Gateways** - This component returns the total number of gateways in the domain.
- **Closed Gateways** - This component returns the number of gateways that are currently closed.

You should set correct arguments in the following order:

```per1 ${SCRIPT} IP_address, port```

where

- **IP_address** – IP address of target server with installed MTA. By default it uses value `${IP}` which will automatically set the IP address of target node;

- **port** – MTA HTTP access port. By default it is set to **7180**.

If the monitor returns a value of -1, this can mean that the statistic cannot be found on MTA's web page.

**Message Transfer Agent: Statistic 2**

This monitor returns different MTA statistic. The returned values are as follows:
- **Total Routed Messages** - This component returns the total number of messages successfully routed to the domains, post offices, and gateways serviced by the MTA.

- **Routed Messages In Last 10 Minutes** - This component returns the number of messages successfully routed to the domains, post offices, and gateways serviced by the MTA in last ten minutes.

- **Total Undeliverable Messages** - This component returns the total number of messages that could not be delivered to a domain, post office, or gateway. This value should be as low as possible. For assistance, see: [http://www.novell.com/documentation/gw8/gw8_tsh2/?page=/documentation/gw8/gw8_tsh2/data/h0m5qtmo.html#h6fxfw51](http://www.novell.com/documentation/gw8/gw8_tsh2/?page=/documentation/gw8/gw8_tsh2/data/h0m5qtmo.html#h6fxfw51).

- **Undeliverable Messages In Last 10 Minutes** - This component returns the number of messages that could not be delivered to a domain, post office, or gateway in last ten minutes. This value should be as low as possible. For assistance, see: [http://www.novell.com/documentation/gw8/gw8_tsh2/?page=/documentation/gw8/gw8_tsh2/data/h0m5qtmo.html#h6fxfw51](http://www.novell.com/documentation/gw8/gw8_tsh2/?page=/documentation/gw8/gw8_tsh2/data/h0m5qtmo.html#h6fxfw51).

- **Total Errors** - This component returns the total number of errors the MTA encounters while processing messages in its input queues. This value should be as low as possible. For assistance, see: [http://www.novell.com/documentation/gw8/gw8_tsh2/?page=/documentation/gw8/gw8_tsh2/data/h0m5qtmo.html#h2cqddkv](http://www.novell.com/documentation/gw8/gw8_tsh2/?page=/documentation/gw8/gw8_tsh2/data/h0m5qtmo.html#h2cqddkv).

- **Errors In Last 10 Minutes** - This component returns the number of errors the MTA encounters while processing messages in its input queues in last ten minutes. This value should be as low as possible. For assistance, see: [http://www.novell.com/documentation/gw8/gw8_tsh2/?page=/documentation/gw8/gw8_tsh2/data/h0m5qtmo.html#h2cqddkv](http://www.novell.com/documentation/gw8/gw8_tsh2/?page=/documentation/gw8/gw8_tsh2/data/h0m5qtmo.html#h2cqddkv).

You should set correct arguments in the following order:

```
perl ${SCRIPT} IP_address,port
```

where

- **IP_address** – IP address of target server with installed MTA. By default it uses value `${IP}` which will automatically set the IP address of target node;

- **port** – MTA HTTP access port. By default it is set to 7180.

---

**Message Transfer port**

This component monitor tests the ability of a Message Transfer to accept incoming sessions. By default it monitors 7100 TCP port. You should put correct Message Transfer port here, which you set during MTA installation.
HTTP port

This component monitor tests the ability of a MTA HTTP access to accept incoming sessions. By default it monitors 7180 TCP port. You should put correct MTA HTTP port here, which you set during MTA installation.

Process: Message Transfer Agent

This monitor returns CPU and memory usage of Message Transfer Agent process (gwmta). If this counter is unavailable, there may be problems with SNMP configuration or this process has stopped.

HTTP Monitor

This component monitor tests a web server's ability to accept incoming sessions and transmit the requested page. By default it monitors web site on 7180 TCP port.
Novell GroupWise Message Transfer Agent (Windows)

This template allows you to check GroupWise Message Transfer Agent (MTA) statistics by retrieving it from MTA's webpage.

Prerequisites

WinRM must be installed and properly configured on the target server.

Credentials

Administrator on target server.

This template is based on this article: http://www.novell.com/documentation/gw8/gw8_admin/?page=/documentation/gw8/gw8_admin/data/a7q4zpk.html.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

**Message Transfer Agent: Statistic 1**

This monitor returns different MTA statistic. The returned values are as follows:

- **Total Domains** - This component returns the total number of domains the MTA links to.
- **Closed Domains** - This component returns the number of domains that are currently closed.
- **Total Post Offices** - This component returns the total number of post offices in the domain.
- **Closed Post Offices** - This component returns the number of post offices that are currently closed.
- **Total Gateways** - This component returns the total number of gateways in the domain.
- **Closed Gateways** - This component returns the number of gateways that are currently closed.

You should set correct arguments in the following order:

**IP_address, port**

where

**IP_address** – IP address of target server with installed MTA. By default it uses value `{IP}` which will automatically set the IP address of target node;

**port** – MTA HTTP access port. By default it is set to **7180**.

If the monitor returns a value of -1, this can mean that the statistic cannot be found on MTA's web page.

**Message Transfer Agent: Statistic 2**

This monitor returns different MTA statistic. The returned values are as follows:
SAM TEMPLATE REFERENCE: SERVER & APPLICATION MONITOR

- **Total Routed Messages** - This component returns the total number of messages successfully routed to the domains, post offices, and gateways serviced by the MTA.

- **Routed Messages In Last 10 Minutes** - This component returns the number of messages successfully routed to the domains, post offices, and gateways serviced by the MTA in last ten minutes.

- **Total Undeliverable Messages** - This component returns the total number of messages that could not be delivered to a domain, post office, or gateway. This value should be as low as possible. For assistance, see: [http://www.novell.com/documentation/gw8/gw8_tsh2/?page=/documentation/gw8/gw8_tsh2/data/h0m5qtmo.html#h6fxfw51](http://www.novell.com/documentation/gw8/gw8_tsh2/?page=/documentation/gw8/gw8_tsh2/data/h0m5qtmo.html#h6fxfw51).

- **Undeliverable Messages In Last 10 Minutes** - This component returns the number of messages that could not be delivered to a domain, post office, or gateway in last ten minutes. This value should be as low as possible. For assistance, see: [http://www.novell.com/documentation/gw8/gw8_tsh2/?page=/documentation/gw8/gw8_tsh2/data/h0m5qtmo.html#h6fxfw51](http://www.novell.com/documentation/gw8/gw8_tsh2/?page=/documentation/gw8/gw8_tsh2/data/h0m5qtmo.html#h6fxfw51).

- **Total Errors** - This component returns the total number of errors the MTA encounters while processing messages in its input queues. This value should be as low as possible. For assistance, see: [http://www.novell.com/documentation/gw8/gw8_tsh2/?page=/documentation/gw8/gw8_tsh2/data/h0m5qtmo.html#h2cqddkv](http://www.novell.com/documentation/gw8/gw8_tsh2/?page=/documentation/gw8/gw8_tsh2/data/h0m5qtmo.html#h2cqddkv).

- **Errors In Last 10 Minutes** - This component returns the number of errors the MTA encounters while processing messages in its input queues in last ten minutes. This value should be as low as possible. For assistance, see: [http://www.novell.com/documentation/gw8/gw8_tsh2/?page=/documentation/gw8/gw8_tsh2/data/h0m5qtmo.html#h2cqddkv](http://www.novell.com/documentation/gw8/gw8_tsh2/?page=/documentation/gw8/gw8_tsh2/data/h0m5qtmo.html#h2cqddkv).

You should set correct arguments in the following order:

\[ \text{IP}\_\text{address}, \text{port} \]

where

- **IP_address** – IP address of target server with installed MTA. By default it uses value ${IP}$ which will automatically set the IP address of target node;

- **port** – MTA HTTP access port. By default it is set to 7180.

1. If the monitor returns a value of -1, this can mean that the statistic cannot be found on MTA's web page.

**Message Transfer port**

This component monitor tests the ability of a Message Transfer to accept incoming sessions. By default it monitors 7100 TCP port. You should put correct Message Transfer port here, which you set during MTA installation.
HTTP port

This component monitor tests the ability of a MTA HTTP access to accept incoming sessions. By default it monitors 7180 TCP port. You should put correct MTA HTTP port here, which you set during MTA installation.

Process: Message Transfer Agent

This monitor returns CPU and memory usage of Message Transfer Agent process (gwmta.exe).

HTTP Monitor

This component monitor tests a web server's ability to accept incoming sessions and transmit the requested page. By default it monitors web site on 7180 TCP port.
Novell GroupWise Post Office Agent (Unix)

This template allows you to check GroupWise Post Office Agent (POA) statistics by retrieving it from POA's webpage.

Prerequisites

Perl must be installed on the target server. SNMP installed on the target server and permission to monitor the gwpoa processes.

Credentials

Root on target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Post Office Agent: Statistic 1

This monitor returns different POA statistics. The returned values are as follows:

- **Users** – This component returns the number of users, who are connected to the post office using client/server connections. These could be Windows clients or Cross-Platform clients.

- **Application Connections** – This component returns the number of active application ("virtual") TCP/IP connections between the POA and GroupWise clients (Windows or Cross-Platform). Each GroupWise user uses one application connection when he or she starts GroupWise. Depending on what activities the user is doing in the GroupWise client, additional application connections are used. For example, the GroupWise Address Book and GroupWise Notify will use individual application connections.

- **Physical Connections** – This component returns the number of active physical TCP/IP connections between the post office and the GroupWise clients run by GroupWise users.

- **Priority Queues** – This component returns the number of messages waiting in the high priority message queues. You can control the number of threads processing message files.

- **Normal Queues** – This component returns the number of messages waiting in the normal priority message queues. You can control the number of threads processing message files.

- **Requests** – This component returns the number of active client/server requests between GroupWise clients and the POA.

- **Requests Pending** – This component returns the number of client/server requests from GroupWise clients the POA has not yet been able to respond to. If the number is large, increase the number of POA connections so that more users can be serviced by the POA.

- **Users Timed Out** – This component returns the number of GroupWise clients no longer communicating with the POA. Having users timed out does not indicate a problem with the POA, but rather a problem with users. Users who have timed out are users for which the POA has closed the connection because the GroupWise client was no longer communicating. Timed
out users might not be exiting GroupWise normally or might be having other problems with their workstations. The number of timed-out users might tend to increase on a daily basis during the hour after users leave to go home. This is not a problem.

- **Rules Executed** – This component returns the number of users' rules executed by the POA.

You should set correct arguments in the following order:

```
perl ${SCRIPT} IP_address port
```

where

- **IP_address** – IP address of target server with installed POA. By default it uses value `${IP}` which will automatically set the IP address of target node

- **port** – POA HTTP access port. By default it is set to 7181

> If the monitor returns a value of -1, this can mean that the statistic cannot be found on POA's web page.

**Post Office Agent: Statistic 2**

This monitor returns different POA statistic. The returned values are as follows:

- **Users Delivered** – This component returns the number of user messages delivered to recipients in the post office. A message with six recipients in the local post office is counted six times.

- **Message Files Processed** – This component returns the total number of messages processed by the POA. This includes user messages, status messages, and service requests processed by the POA.

- **Messages Undelivered** – This component returns the number of messages that could not be delivered because the user was not found in that post office or because of other similar problems. Senders of undeliverable messages are notified. This value should be as low as possible. For assistance, see: http://www.novell.com/documentation/gw65/?page=/documentation/gw65/gw65_tsh2/data/a40l3e4.html#a40l3e4.

- **b** – This component returns the number of invalid message files that have problems not related to user error. It also displays requests the POA cannot process because of error conditions. This value should be as low as possible. For assistance, see: http://www.novell.com/documentation/gw65/?page=/documentation/gw65/gw65_tsh2/data/a41g7r8.html#a41g7r8.

- **Users Deleted** – This component returns the number of GroupWise user accounts that the POA has deleted.

- **Statuses Processed** – This component returns the number of status notifications that the POA has delivered.

- **Databases Recovered** – This component returns the number of databases that the POA has recovered. When database damage is detected, the POA can repair the post office database, user databases, and message databases.
GWCheck Messages Processed – This component returns the number of GWCheck (mailbox/library maintenance) requests that the POA has received from scheduled mailbox/library maintenance events and from a GroupWise administrator in ConsoleOne.

GWCheck Problem Messages – This component returns the number of GWCheck (mailbox/library maintenance) requests that the POA was unable to process successfully. Look in the POA log file on the Log Files page for more information about the problem. This value should be as low as possible.

You should set correct arguments in the following order:

perl ${SCRIPT} IP_address port

where

IP_address – IP address of target server with installed POA. By default it uses value ${IP} which will automatically set the IP address of target node.

If the monitor returns a value of -1, this can mean that the statistic cannot be found on POA's web page.

Post Office Agent: Statistic 3

This monitor returns different POA statistic. The returned values are as follows:

- **Caching Requests** – This component returns the number of times GroupWise clients running in Caching mode have requested to download messages into Caching mailboxes. These could be Windows clients or Cross-Platform clients.

- **Caching Primings** – This component returns the number of times GroupWise clients have needed to download entire mailboxes when Caching mode is first selected by client users.

- **Rejected Caching Requests** – This component returns the number of caching requests that the POA was too busy to respond to successfully. Rejected caching requests are retried until they are successful. The number of rejected caching requests helps you fine tune the number of C/S handler threads the POA should be configured to use. This value should be as low as possible.

- **Rejected Caching Primings** – This component returns the number of priming requests that the POA was too busy to respond to successfully. Rejected caching primings mean that some GroupWise users have been unable to change over to Caching mode immediately. The GroupWise client will retry the priming at a later time. This value should be as low as possible.

- **Total Handler Threads** – This component returns the maximum number of client/server handler threads the POA can start. C/S handler threads service client/server requests from GroupWise users.

- **Busy Handler Threads** – This component returns the number of how many handler threads are currently busy. C/S handler threads service client/server requests from GroupWise users. To handle occasional heavy client activity when there are pending client/server requests but CPU utilization is still below the configured threshold, the POA automatically starts additional
C/S handler threads above the number configured in ConsoleOne to handle the workload. When the workload returns to normal, the C/S handler threads return to the number configured in ConsoleOne.

- **Total Message Worker Threads** – This component returns the maximum number of message worker threads the POA can start. Message worker threads process message files, delivering messages to users’ mailboxes.

- **Busy Message Worker Threads** – This component returns the number of how many message worker threads are currently busy. Message worker threads process message files, delivering messages to users' mailboxes.

- **Total GWCheck Worker Threads** – This component returns the maximum number of GWCheck worker threads the POA can start. GWCheck worker threads perform mailbox/library maintenance.

- **Busy GWCheck Worker Threads** – This component returns the number of how many GWCheck worker threads are currently busy. GWCheck worker threads perform mailbox/library maintenance.

You should set correct arguments in the following order:

```perl
perl ${SCRIPT} IP_address port
```

where

- **IP_address** – IP address of target server with installed POA. By default it uses value `${IP}` which will automatically set the IP address of target node;

- **port** – POA HTTP access port. By default it is set to 7181.

If the monitor returns a value of -1, this can mean that the statistic cannot be found on POA's web page.

**Client and Server port**

This component monitor tests the ability of a POA to accept incoming sessions. By default it monitors 1677 TCP port. You should put correct POA Client/Server port here, which you set during POA installation.

**Message Transfer port**

This component monitor tests the ability of a POA Message Transfer to accept incoming sessions. By default it monitors 7101 TCP port. You should put correct POA Message Transfer port here, which you set during POA installation.

**HTTP port**

This component monitor tests the ability of a POA HTTP access to accept incoming sessions. By default it monitors 7181 TCP port. You should put correct POA HTTP port here, which you set during POA installation.
Process: Post Office Agent

This monitor returns CPU and memory usage of Post Office Agent process (gwpoa). If this counter is unavailable, there may be problems with SNMP configuration or this process has stopped.

HTTP Monitor

This component monitor tests a web server’s ability to accept incoming sessions and transmit the requested page. By default it monitors web site on 7181 TCP port.
Novell GroupWise Post Office Agent (Windows)

This template allows you to check GroupWise Post Office Agent (POA) statistics by retrieving it from POA's webpage.

**Prerequisites:**

WinRM must be installed and properly configured on the target server.

**Credentials:**

Administrator on target server.

**Monitored Components**

For details on monitors, see [SAM Component Monitor Types](#).

**Post Office Agent: Statistic 1**

This monitor returns different POA statistics. The returned values are as follows:

- **Users** – This component returns the number of users who are connected to the post office using client/server connections. These could be Windows clients or Cross-Platform clients.

- **Application Connections** – This component returns the number of active application ("virtual") TCP/IP connections between the POA and GroupWise clients (Windows or Cross-Platform). Each GroupWise user uses one application connection when he or she starts GroupWise. Depending on what activities the user is doing in the GroupWise client, additional application connections are used. For example, the GroupWise Address Book and GroupWise Notify will use individual application connections.

- **Physical Connections** – This component returns the number of active physical TCP/IP connections between the post office and the GroupWise clients run by GroupWise users.

- **Priority Queues** – This component returns the number of messages waiting in the high priority message queues. You can control the number of threads processing message files.

- **Normal Queues** – This component returns the number of messages waiting in the normal priority message queues. You can control the number of threads processing message files.

- **Requests** – This component returns the number of active client/server requests between GroupWise clients and the POA.

- **Requests Pending** – This component returns the number of client/server requests from GroupWise clients the POA has not yet been able to respond to. If the number is large, increase the number of POA connections so that more users can be serviced by the POA.

- **Users Timed Out** – This component returns the number of GroupWise clients no longer communicating with the POA. Having users timed out does not indicate a problem with the POA, but rather a problem with users. Users who have timed out are users for which the POA has closed the connection because the GroupWise client was no longer communicating. Timed
out users might not be exiting GroupWise normally or might be having other problems with their workstations. The number of timed-out users might tend to increase on a daily basis during the hour after users leave to go home. This is not a problem.

- **Rules Executed** – This component returns the number of users' rules executed by the POA.

You should set correct arguments in the following order:

\[ \text{IP_address, port} \]

where

- **IP_address** – IP address of target server with installed POA. By default it uses value \${IP} which will automatically set the IP address of target node;

- **port** – POA HTTP access port. By default it is set to 7181.

If the monitor returns a value of -1, this can mean that the statistic cannot be found on POA's web page.

**Post Office Agent: Statistic 2**

This monitor returns different POA statistic. The returned values are as follows:

- **Users Delivered** – This component returns the number of user messages delivered to recipients in the post office. A message with six recipients in the local post office is counted six times.

- **Message Files Processed** – This component returns the total number of messages processed by the POA. This includes user messages, status messages, and service requests processed by the POA.

- **Messages Undelivered** – This component returns the number of messages that could not be delivered because the user was not found in that post office or because of other similar problems. Senders of undeliverable messages are notified. This monitor should be as low as possible.

- **Problem Messages** – This component returns the number of invalid message files that have problems not related to user error. It also displays requests the POA cannot process because of error conditions. This monitor should be as low as possible.

- **Users Deleted** – This component returns the number of GroupWise user accounts that the POA has deleted.

- **Statuses Processed** – This component returns the number of status notifications that the POA has delivered.

- **Databases Recovered** – This component returns the number of databases that the POA has recovered. When database damage is detected, the POA can repair the post office database, user databases, and message databases.

- **GWCheck Messages Processed** – This component returns the number of GWCheck (mailbox/library maintenance) requests that the POA has received from scheduled mailbox/library maintenance events and from a GroupWise administrator in ConsoleOne.
GWCheck Problem Messages – This component returns the number of GWCheck (mailbox/library maintenance) requests that the POA was unable to process successfully. Look in the POA log file on the Log Files page for more information about the problem. This monitor should be as low as possible.

You should set correct arguments in the following order:
IP_address,port

where

IP_address – IP address of target server with installed POA. By default it uses value ${IP} which will automatically set the IP address of target node;

port – POA HTTP access port. By default it is set to 7181.

If the monitor returns a value of -1, this can mean that the statistic cannot be found on POA’s web page.

Post Office Agent: Statistic 3

This monitor returns different POA statistics. The returned values are as follows:

- **Caching Requests** – This component returns the number of times GroupWise clients running in Caching mode have requested to download messages into Caching mailboxes. These could be Windows clients or Cross-Platform clients.

- **Caching Primings** – This component returns the number of times GroupWise clients have needed to download entire mailboxes when Caching mode is first selected by client users.

- **Rejected Caching Requests** – This component returns the number of caching requests that the POA was too busy to respond to successfully. Rejected caching requests are retried until they are successful. The number of rejected caching requests helps you fine tune the number of C/S handler threads the POA should be configured to use. This value should be as low as possible.

- **Rejected Caching Primings** – This component returns the number of priming requests that the POA was too busy to respond to successfully. Rejected caching primings mean that some GroupWise users have been unable to change over to Caching mode immediately. The GroupWise client will retry the priming at a later time. This value should be as low as possible.

- **Total Handler Threads** – This component returns the maximum number of client/server handler threads the POA can start. C/S handler threads service client/server requests from GroupWise users.

- **Busy Handler Threads** – This component returns the number handler threads are currently busy. C/S handler threads service client/server requests from GroupWise users. To handle occasional heavy client activity when there are pending client/server requests but CPU utilization is still below the configured threshold, the POA automatically starts additional C/S handler threads above the number configured in ConsoleOne to handle the workload. When the workload returns to normal, the C/S handler threads return to the number configured in ConsoleOne.
- **Total Message Worker Threads** – This component returns the maximum number of message worker threads the POA can start. Message worker threads process message files, delivering messages to users' mailboxes.

- **Busy Message Worker Threads** – This component returns the number of how many message worker threads are currently busy. Message worker threads process message files, delivering messages to users' mailboxes.

- **Total GWCheck Worker Threads** – This component returns the maximum number of GWCheck worker threads the POA can start. GWCheck worker threads perform mailbox/library maintenance.

- **Busy GWCheck Worker Threads** – This component returns the number of how many GWCheck worker threads are currently busy. GWCheck worker threads perform mailbox/library maintenance.

You should set the correct arguments in the following order:

```
IP_address, port
```

where

- **IP_address** – IP address of target server with installed POA. By default it uses value `${IP}` which will automatically set the IP address of target node;

- **port** – POA HTTP access port. By default it is set to 7181.

1. If the monitor returns value of -1, this can mean that the statistic cannot be found on the POA's web page.

**Client and Server port**

This component monitor tests the ability of a POA to accept incoming sessions. By default it monitors TCP port 1677. You should put correct POA Client/Server port here, which you set during POA installation.

**Message Transfer port**

This component monitor tests the ability of a POA Message Transfer to accept incoming sessions. By default it monitors 7101 TCP port. You should put correct POA Message Transfer port here, which you set during POA installation.

**HTTP port**

This component monitor tests the ability of a POA HTTP access to accept incoming sessions. By default it monitors 7181 TCP port. You should put correct POA HTTP port here, which you set during POA installation.

**Process: Post Office Agent**

This monitor returns CPU and memory usage of Post Office Agent process (gwpoa.exe).
HTTP Monitor

This component monitor tests a web server’s ability to accept incoming sessions and transmit the requested page. By default it monitors web site on 7181 TCP port.
OpenLDAP

This template assesses the performance of the OpenLDAP server by retrieving performance data from the cn=Monitor sub-tree.

Prerequisites:

- Perl must be installed on the target server.
- SNMP must be installed on the target server.
- You must have permission to monitor slapd processes on the target server.
- The OpenLDAP monitoring branch must be enabled. You can enable this by adding the following lines to the slapd.conf file, which is located here: /etc/openldap/slapd.conf.

database monitor access to dn.subtree="cn=Monitor" by * read by * none

Create a user on the Linux/Unix server with the same, case sensitive, username and password, as OpenLDAP. OpenLDAP has Manager as the default user, which is equivalent to the OpenLDAP administrator. Create the user, Manager, on the server and set the password to be the same for Manager in OpenLDAP.

See the following example:

[root@centos56 ~]# useradd Manager
[root@centos56 ~]# passwd Manager
Changing password for user Manager. New UNIX password:Retype new UNIX password:passwd: all authentication tokens updated successfully.

[root@centos56 ~]#

Credentials

User with access to the OpenLDAP and Linux/Unix servers.

Component Arguments and Syntax

All components use the ldapsearch command with arguments to get the required values, as in the following: ldapsearch -x -D 'cn=User,dc=your,dc=domain' -w password -b 'cn=Monitor' -s base '(objectClass=*)' '+'

The three arguments below are used in the following order:

perl ${SCRIPT} cn=${USER} ${PASSWORD} dc=your,dc=domain

- **Username** – This argument specifies which user will get the required statistic from the OpenLDAP server using the following format: cn=${USER}. By default, this argument will use the username from the application. Normally, this argument should remain unchanged.
- **Password** – This argument specifies the user's password. By default, it will use the password from the application's username. Normally, this argument should remain unchanged.
- **Domain** – This argument specifies the domain name and should be formatted in the following manner: dc=your,dc=domain. This is where you set your domain. For example: dc=example,dc=com or dc=test1,dc=testing,dc=com
Below is an example using the Command Line field with arguments used in any component monitor:

```perl
perl ${SCRIPT} cn=${USER} ${PASSWORD} dc=example,dc=com
```

# Monitored Components

For details on monitors, see [SAM Component Monitor Types](#).

## Operations Rate per Sec

This monitor returns the rates per second of different LDAP operations. All rates are calculated as the number of specific queries for five seconds, and then divided by five. Information about LDAP operations are taken from the `cn=Operations,cn=Monitor` sub-tree. Returned values are as follows:

- **Total** – This component returns the total number of LDAP operations.
- **Bind** – This component returns the number of Bind operations occurring on the server. The LDAP Bind operation can be used to authenticate to the LDAP Server.
- **Unbind** – This component returns the number of Unbind operations occurring on the server. The LDAP Unbind operation is used to indicate that the client wants to disconnect from the server.
- **Add** – This component returns the number of Add operations occurring on the server. The LDAP Add operation can be used to create an entry in the LDAP Server.
- **Delete** – This component returns the number of Delete operations occurring on the server. The LDAP Delete operation can be used to remove an entry or sub-tree from the server.
- **Modify** – This component returns the number of Modify operations occurring on the server. The LDAP Modify operation can be used to alter an existing entry in the LDAP Server.
- **Compare** – This component returns the number of Compare operations occurring on the server. The LDAP Compare operation can be used to determine whether a specified entry contains a given attribute value.
- **Search** – This component returns the number of Search operations occurring on the server. The LDAP Search operation can be used to identify entries in the LDAP Server that match a given set of criteria.

## Active Operations

This monitor returns the number of active operations.

## Current Connections

This monitor returns the number of current OpenLDAP connections.

## Bytes Sent Rate per Sec

This monitor returns the number of bytes sent, per second, by the server.
Uptime

This monitor shows the server uptime, in seconds. The returning message shows the time in days, hours, minutes, and seconds.

Read Waiters

This monitor returns the number of connections that are waiting to read data.

Write Waiters

This monitor returns the number of connections that are waiting to write data.

Process Monitor (SNMP): slapd

This component monitor returns CPU and memory usage of the slapd daemon. If this counter is unavailable, there may be a problem with your SNMP configuration or the slapd service has stopped.

LDAP User Experience Monitor

This component monitor tests the capabilities of the Light Weight Directory Access Protocol (LDAP) server and measures the time it takes to perform an LDAP query.

ℹ️ By default, this monitor is disabled.
Oracle

The following templates are available:

- Oracle Automatic Storage Management
- Oracle Database monitor
- Oracle WebLogic (JMX)

Oracle Automatic Storage Management

This template assesses the status and performance of an Oracle Automatic Storage Management by retrieving performance data from the built-in Oracle views.

Prerequisites

This template is included with SolarWinds SAM during installation. It is also posted in the SolarWinds online IT community, THWACK.

To use this template, download the Oracle Client from the SolarWinds Customer Portal and install it on the main Orion server.

If you have Additional Polling Engines (APEs), install the Oracle client software on those machines also.

Credentials

An Oracle user name and password with read access to the Oracle tables: v_asm_diskgroup and v_asm_disk.

If you have issues connecting to Oracle databases, see "Use the SAM Oracle Database template and Oracle User Experience monitor without ODBC" article in the SolarWinds Success Center.

Monitored components

Components without predetermined threshold values provide guidance such as "Use the lowest threshold possible" or "Use the highest threshold possible" to help you find an appropriate threshold for your application. For more information, see "Using the Orion APM Min/Max/Average statistics data for creating threshold settings" in the SolarWinds Success Center.
Before using this template, you should provide the correct disk group name in all SQL queries by changing the last line of the SQL query in all monitors:

```
WHERE A.NAME LIKE 'DISK_GROUP_NAME'
```

where `DISK_GROUP_NAME` – disk group name which you want to monitor. For example:

```
WHERE A.NAME LIKE 'DATA'
```

To get the names of disk groups, run the following command from Oracle SQL plus utility:

```
SELECT NAME FROM V$ASM_DISKGROUP;
```

**Mount Status**

This component monitor returns the status of the disk relative to group mounts.

Possible values:

- **0 – Opened** - Disk is present in the storage system and is being accessed by Automatic Storage Management (ASM). This is the normal state for disks in a database instance which are part of a Disk Group being actively used by the instance.
- **1 – Cached** - Disk is present in the storage system, and is part of a disk group being accessed by the Automatic Storage Management instance. This is the normal state for disks in an ASM instance which are part of a mounted disk group.
- **2 – Closing** - ASM is in the process of closing this disk.
- **3 – Closed** - Disk is present in the storage system but is not being accessed by ASM.
- **4 – Ignored** - Disk is present in the system, but is ignored by ASM because of one of the following:
  - The disk is detected by the system library, but is ignored because an ASM library discovered the same disk.
  - ASM determined that the membership claimed by the disk header is no longer valid.
- **5 – Missing** - ASM metadata indicates that the disk is known to be part of the ASM disk group, but no disk in the storage system was found with the indicated name.
- **6 – Unknown**

**Header Status**

This component monitor returns status of the disk as seen by discovery.

Possible values:

- **0 – Member** - Disk is a member of an existing disk group. No attempt should be made to add the disk to a different disk group. The ALTER DISKGROUP statement will reject such an addition unless overridden with the FORCE option.
- **1 – Former** - Disk was once part of a disk group but has been dropped cleanly from the group. It may be added to a new disk group with the ALTER DISKGROUP statement.
• **2 - Provisioned** - Disk is not part of a disk group and may be added to a disk group with the ALTER DISKGROUP statement. The PROVISIONED header status is different from the CANDIDATE header status in that PROVISIONED implies that an additional platform-specific action has been taken by an administrator to make the disk available for ASM.

• **3 - Candidate** - Disk is not part of a disk group and may be added to a disk group with the ALTER DISKGROUP statement.

• **4 - Foreign** - Disk contains data created by an Oracle product other than ASM. This includes datafiles, logfiles, and OCR disks.

• **5 - Incompatible** - Version number in the disk header is not compatible with the ASM software version.

• **6 - Conflict** - ASM disk was not mounted due to a conflict.

• **7 - Unknown** - ASM disk header was not read.

**Mode Status**

This component monitor returns status about which kinds of I/O requests are allowed to the disk.

Possible values:

• **0 - Online** - Disk is online and operating normally. Reads and writes are attempted.

• **1 - Offline** - Disk is offline and access to data is not permitted. Reads and writes are not attempted. An offline disk remains logically part of its disk group.

• **2 - Unknown** - ASM disk mode is not known (typically the disk is not mounted).

**State**

This component monitor returns state of the disk with respect to the disk group.

Possible values:

• **0 - Normal** - Disk is online and operating normally.

• **1 - Adding** - Disk is being added to a disk group, and is pending validation by all instances that have the disk group mounted.

• **2 - Dropping** - Disk has been manually taken offline and space allocation or data access for the disk halts. Rebalancing will commence to relocate data off the disks to other disks in the disk group. Upon completion of the rebalance, the disk is expelled from the group.

• **3 - Dropped** - Disk was fully expelled from the disk group.

• **4 - Forcing** - Disk is being removed from the disk group without attempting to offload its data. The data will be recovered from redundant copies, where possible.

• **5 - Hung** - Disk drop operation cannot continue because there is insufficient space to relocate the data from the disk being dropped.

• **6 - Unknown** - ASM disk state is not known (typically the disk is not mounted).

**Used Space (%)**

This component monitor returns the percentage of the used capacity of the disk group.

**Used Space (MB)**

This component monitor returns the used capacity of the disk group (in MBs).
Read Requests

This component monitor returns the total number of I/O read requests for the disk.

ℹ️ By default, this monitor has the Count statistic as difference box checked. The returned value will only show the results since the last polling period.

Write Requests

This component monitor returns the total number of I/O write requests for the disk.

ℹ️ By default, this monitor has the Count statistic as difference box checked. The returned value will only show the results since the last polling period.

Failed Read Requests

This component monitor returns the total number of failed I/O read requests for the disk.

ℹ️ By default, this monitor has the Count statistic as difference box checked. The returned value will only show the results since the last polling period.

Failed Write Requests

This component monitor returns the total number of failed I/O write requests for the disk.

ℹ️ By default, this monitor has the Count statistic as difference box checked. The returned value will only show the results since the last polling period.

Bytes Read

This component monitor returns the total number of bytes read from the disk.

ℹ️ By default, this monitor has the Count statistic as difference box checked. The returned value will only show the results since the last polling period.

Bytes Written

This component monitor returns the total number of bytes written to the disk.

ℹ️ By default, this monitor has the Count statistic as difference box checked. The returned value will only show the results since the last polling period.
Oracle Database monitor

This component monitor template assesses the status and performance of an Oracle database by retrieving performance data from the built-in Oracle statistics views.

Works with the Orion Agent for Linux.

Prerequisites

This template is included with SolarWinds SAM during installation. It is also posted in the SolarWinds online IT community, THWACK.

To use this template, download the Oracle Client from the SolarWinds Customer Portal and install it on the main Orion server.

If you have Additional Polling Engines (APEs), install the Oracle client software on those machines also.

Credentials

An Oracle user name and password with read access to the following Oracle views: dba_free_space, v$sysstat, v$rowcache, v$librarycache, v$sgastat, and v$session.

If customizing this template for the Oracle User Experience Monitor, the resulting output of the SQL query must return a single numeric value. A message field is optional.

If you have issues connecting to Oracle databases, see "Use the SAM Oracle Database template and Oracle User Experience monitor without ODBC" article in the SolarWinds Success Center.

Monitored components

For details on monitors, see SAM Component Monitor Types.

Components without predetermined threshold values provide guidance such as "Use the lowest threshold possible" or "Use the highest threshold possible" to help you find an appropriate threshold for your application.

SGA Size

This component monitor returns the System Global Area (SGA) that is the part of the system memory (RAM) shared by all the processes belonging to a single Oracle database instance, measured in bytes.

PGA Size

This component monitor returns the Program Global Area (PGA) memory currently allocated by the process (including free PGA memory not yet released to the operating system by the server process), measured in bytes.
PGA is a private memory region that contains the data and control information for a server process. Only a server process can access the PGA. The Oracle database reads and writes information in the PGA on behalf of the server process. The Oracle database automatically sizes the PGA by dynamically adjusting the portion of the PGA memory dedicated to work areas, based on 20% of the SGA memory size. The minimum value is 10 MB.

**Buffer Pool Size**

This component monitors the buffer pool size for the Oracle database, measured in bytes. The default buffer pool size is determined by the DB_CACHE_SIZE initialization parameter.

**Shared Pool Size**

This component monitors the shared pool area size, measured in bytes. The shared pool is a RAM area within the RAM heap that is created at startup time; it is a component of the System Global Area (SGA). Its size depends on size of your RAM.

**Buffer Pool Response Time**

This component monitors the Buffer pool response time, measured in seconds. Keep the value low for good performance. The query calculates response time for logical reads per second from buffer within an interval of 15 seconds.

**Single Block Read Response Time**

This component monitors the cumulative single-block read response time at the file level in seconds. Keep the value low; a high value means a high latency.

**Multi Block Read Response Time**

This component monitors the cumulative multi-block read response time at the file level in seconds. Keep the value low; a high value means a high latency.

**Log Write Response Time**

This component monitors the log write response time, which includes write time plus the wait time that the log writer spent waiting.

**Physical I/O Total Rate**

This component monitors the Physical I/O total rate, which includes the read rate plus the write rate per second. A high value means better performance.

**Physical I/O Read Rate**

This component monitors the Physical I/O read rate per second. A high value means better performance.

**Physical I/O Write Rate**

This component monitors the Physical I/O write rate per second. A high value means better performance.
Commit Latency
This component monitors latency for commits by all users. If the value is null, the number of commits per second is zero.

SQL*Net Receive Rate
This component monitors SQL*Net receive rate — bytes received via SQL*Net from client plus bytes received via SQL*Net from dblink.

SQL*Net Send Rate
This component monitors SQL*Net receive rate — bytes sent via SQL*Net to client plus bytes sent via SQL*Net to dblink.

Active sessions total
This component monitors total no of active sessions at any moment.

Active sessions waiting
This component monitors the number of active sessions waiting to be run.

Active sessions working
This component monitors the number of active sessions currently executing on the CPU.

Blocked sessions
This component monitors the total number sessions which are blocked by other sessions.

Connections
This component monitors the total number of active connections at any point.

Request rate
This component monitors the total number of incoming request per seconds. A high number of requests may result in slow response.

Database Size (size of all tablespaces)
This component monitors the total database size (that is, the size of all table spaces) of the Oracle database, measured in bytes.

Database Used Space (amount actually used)
This component monitors the total space used by the database.

SQL Parse to execute ratio
This component monitors the SQL-parsing-to-execute ratio, calculated by dividing parse count by execution count. A higher ratio means a better performance.

Available free space (MB)
This component monitor returns the available free space of the database in MB. This value should be as high as possible.
Buffer cache hit ratio (%)

This component monitor returns the percentage of pages found in the buffer cache without having to read from the disk.

This ratio should exceed 90%, and ideally be over 99%. If your Buffer Cache Hit Ratio is lower than 90%, you should consider adding more RAM, if possible. A higher ratio value returned indicates improved performance by your Oracle Server.

If your database is very large, you may not be able to get close to 99%, even if you put the maximum amount of RAM in your server.

Dictionary cache hit ratio (%)

This component monitor returns the ratio, as a percentage, of dictionary cache hits to total requests.

The dictionary cache stores data referenced from the data dictionary. A properly tuned dictionary cache can significantly improve overall database performance. Guidelines for acceptable ratios are as follows:

- 70% or above. 99% would be ideal.
- If the ratio is below 70%, increase the value of the initialization parameter, SHARED_POOL_SIZE. It is recommended that the SHARED_POOL_SIZE parameter be at least 4 MB.
- Large databases may require a shared pool of at least 10 MB.

Increasing the SHARED_POOL_SIZE parameter will increase the size of the System Global Area (SGA).

Library cache hit ratio (%)

This component monitor returns the percentage of Pin requests that result in hits.

- **PINS** - Defined as the number of times an item in the library cache was executed.
- **PINHITS** - Defined as the number of times an item was executed without reloads.

The library cache stores the executable form of recently referenced SQL and PL/SQL code. Ideally, the value of this component monitor should be greater than 95%. If the value is less than 95%, you may want to try the following:

- Increase the SHARED_POOL_SIZE parameter.
- The CURSOR_SHARING parameter may need to be set to FORCE.
- Increase the size of the SHARED_POOL_RESERVED_SIZE parameter.
- Sharing of SQL, PL/SQL or JAVA code may be inefficient.
- Use of bind variables may be insufficient.

Available free memory (MB)

This component monitor returns the free memory in MB, of all SGA pools. This value should be as high as possible.

Number of connected users to the database through SQL Net

This component monitor returns the number of currently connected users.
**Temp files size (MB)**

This component monitor returns the size of all temporary files in MB. This value should be as low as possible.

**Data files size (MB)**

This component monitor returns the size of all database files in MB.

**Total short table scans**

This component monitor returns the total number of full table scans that were performed on tables having less than five Oracle data blocks since database instance startup.

> It is generally more efficient to perform full table scans on short tables rather than access the data using indexes.

**Total long table scans**

This component monitor returns the total number of full table scans done on tables containing five or more Oracle data blocks since database instance startup.

> It may be advantageous to access long tables using indexes.

**User transactions**

This component monitor returns the total number of users’ transactions.

**Disk sort operations**

This component monitor returns the number of sort operations that require at least one disk write. This value should be as low as possible.

> Sorts that require continual reading and writing to disk can consume a great deal of resources. If this monitor returns a high value, consider increasing the size of the initialization parameter, SORT_AREA_SIZE. For more information, see: [http://download.oracle.com/docs/cd/B28359_01/server.111/b28320/initparams232.htm#i1134127](http://download.oracle.com/docs/cd/B28359_01/server.111/b28320/initparams232.htm#i1134127).

**Memory sort operations**

This component monitor returns the number of sort operations that were performed completely in memory meaning no disk writes were required.

**User rollbacks**

This component monitor returns the number of times that users manually issued the Rollback statement. Use of the Rollback statement may also indicate an error occurred during a user’s transactions. This value should be as low as possible.

**Used Space in Tablespace (%) from Max**

By default, this monitor returns a statistic for the System tablespace. To change the target
tablespace you should change the following line:

```
where a.tablespace_name (+) = b.tablespace_name AND a.tablespace_name = 'SYSTEM'
```

To identify which tablespaces are available, run the following command on the target oracle server:

```
select tablespace_name from dba_data_files;
```
Oracle WebLogic (JMX)

This template monitors for Oracle WebLogic server statistics by using the JMX protocol. You can use the Orion agent for Linux or SNMP agentless to monitor.

Prerequisites

Target server configured to allow JMX queries.

Template configuration changes

The following settings in the component monitors should be changed from defaults:

- This template is configured to send JMX requests on port 8686. For this Oracle WebLogic template, you should change the port to 7001.
- The URL is set to /jmxrmi by default. For this template, set the URL to /jndi/weblogic.management.mbeanservers.runtime.
- The JMX protocol default setting for this template is rmi. For this template, change the JMX protocol to ioo.

Credentials

Dependent upon JMX configuration.

Configurations for Orion agent for Linux

For JMX configurations, install and configure WebSphere per your Linux/Unix distribution. See the IBM Knowledge Center for details. The overall steps include:

1. Install WebSphere and note the following details:
   - You may need to create an administrator account and a new package group.
   - During installation, turn off the secure storage option as this is not needed.
   - Make sure to select the Application Server during installation.

2. Start and stop the WebSphere AppServer.

3. Use a browser to access the WebSphere AppServer console at http://websphere-host:9060/ibm/console

   - You may need to open a port to 9060 on the WebSphere host.
   - Use the credentials for the account created during installation.

4. In the console, expose the JMX platform mbeans in the WebSphere AppServer by:
   a. Clicking Servers > Server Types > WebSphere application servers.
   b. Selecting the listed application server.

5. Locate the Java and Process Management > Process definition. In the Generic JVM arguments dialog box, enter the following code:

   ```
   Djavax.management.builder.initial=
   ```

   Note: There is nothing after the = sign.
6. Restart the AppServer.

Monitored Components

For details on monitors, see [SAM Component Monitor Types](#).

All components may vary in a running environment. You can add your own threshold limits as needed.

**Classes Loaded Count**

This monitor returns the number of classes that are currently loaded in the Java virtual machine.

**Classes Total Loaded Count**

This monitor returns the total number of classes that have been loaded since the Java virtual machine has started execution.

**Classes Unloaded Count**

This monitor returns the total number of classes unloaded since the Java virtual machine has started execution.

**Memory Pending Final Count**

This monitor returns the approximate number of objects for which finalization is pending.

**Memory Heap Init Size (B)**

This monitor returns the initial amount of memory in bytes that the Java virtual machine allocates; or -1 if undefined.

**Memory Heap Used (B)**

This monitor returns the amount of used memory in bytes. The amount of used memory in the returned memory usage is the amount of memory occupied by both live objects and garbage objects that have not been collected, if any.

**Memory Heap Committed (B)**

This monitor returns the amount of committed memory in bytes.

**Memory Heap Max Size (B)**

This monitor returns the maximum amount of memory in bytes that can be used; or -1 if undefined.
Memory Non Heap Init Size (B)
This monitor returns the initial amount of memory in bytes that the Java virtual machine allocates; or -1 if undefined.

Memory Non Heap Used (B)
This monitor returns the amount of used memory in bytes.

Memory Non Heap Committed (B)
This monitor returns the amount of committed memory in bytes.

Memory Non Heap Max Size (B)
This monitor returns the maximum amount of memory in bytes that can be used; or -1 if undefined.

Memory Garbage Collections Count
This monitor returns the approximate accumulated collection elapsed time in milliseconds.

Memory Garbage Collection Time (ms)
This monitor returns the approximate accumulated collection elapsed time in milliseconds.

Memory Pool Init Size (B)
This monitor returns the initial amount of memory (in bytes) that the Java virtual machine requests from the operating system for memory management during startup. The Java virtual machine may request additional memory from the operating system and may also release memory to the system over time. The value of init may be undefined.

Memory Pool Used (B)
This monitor returns the amount of memory currently used (in bytes).

Memory Pool Committed Size (B)
This monitor returns the amount of memory (in bytes) that is guaranteed to be available for use by the Java virtual machine. The amount of committed memory may change over time (increase or decrease). The Java virtual machine may release memory to the system and committed could be less than init. committed will always be greater than or equal to used.

Memory Pool Max Size (B)
This monitor returns the maximum amount of memory (in bytes) that can be used for memory management. Its value may be undefined. The maximum amount of memory may change over time if defined. The amount of used and committed memory will always be less than or equal to max if max is defined. A memory allocation may fail if it attempts to increase the used memory such that used > committed even if used <= max would still be true (for example, when the system is low on virtual memory).

Memory Pool Peak Used (B)
This monitor returns the peak amount of memory currently used (in bytes).
Memory Pool Peak Committed (B)

This monitor returns the peak amount of memory (in bytes) that is guaranteed to be available for use by the Java virtual machine. The amount of committed memory may change over time (increase or decrease). The Java virtual machine may release memory to the system and committed could be less than init. committed will always be greater than or equal to used.

Memory Pool Peak Max Size (B)

This monitor returns the maximum peak amount of memory (in bytes) that can be used for memory management. Its value may be undefined. The maximum amount of memory may change over time if defined. The amount of used and committed memory will always be less than or equal to max if max is defined. A memory allocation may fail if it attempts to increase the used memory such that used > committed even if used <= max would still be true (for example, when the system is low on virtual memory).

Threads Total Started Count

This monitor returns the total number of threads created and also started since the Java virtual machine started.

Current Thread Count

This monitor returns the current number of live threads including both daemon and non-daemon threads.

Current Thread Cpu Time

This monitor returns the total CPU time for the current thread in nanoseconds.

Current Thread User Time

This monitor returns the CPU time that the current thread has executed in user mode in nanoseconds.

Runtime Uptime (ms)

This monitor returns the uptime of the Java virtual machine in milliseconds.

Compiler Time (ms)

This monitor returns the approximate accumulated elapsed time (in milliseconds) spent in compilation.

JVM Runtime: Heap Free Current

This monitor returns the current amount of memory (in bytes) that is available in the JVM heap.

JVM Runtime: Heap Free Percent

This monitor returns the percentage of the maximum memory that is free.

JVM Runtime: Heap Size Current

This monitor returns the current size (in bytes) of the JVM heap.
JVM Runtime: Heap Size Max

This monitor returns the maximum free memory configured for this JVM.

JVM Runtime: Uptime

This monitor returns the number of milliseconds that the Virtual Machine has been running.

JTA Recovery Runtime: Initial Recovered Transactions

This monitor returns the total number of transactions that are recovered from the transaction log initially.

JTA Recovery Runtime: Recovered Transaction Completion Percent

This monitor returns the percentage of transactions that are recovered from the transaction log initially.

Server Security Runtime: Invalid Login Attempts

This monitor returns the total number of invalid logins that have been attempted on this server instance.

Server Security Runtime: Current Locked Users

This monitor returns the current number of locked users on this server instance.

Server Security Runtime: Login Attempts While Locked

This monitor returns the total number of invalid logins that have been attempted on this server instance while a user was locked.

Server Security Runtime: Unlocked Users

This monitor returns the total number of times a user of this server instance has been unlocked.

Server Security Runtime: User Lockout

This monitor returns the total number of user lockouts that have occurred on this server instance.

JTA Coordinator: Threads Constraint Runtime: Out Of Order Executions

This monitor returns the number of requests executed out of turn to satisfy this constraint.

JTA Coordinator: Threads Constraint Runtime: Current Wait Time

This monitor returns the last measured time a request had to wait for a thread. Only requests whose execution is needed to satisfy the constraint are considered.

JTA Coordinator: Threads Constraint Runtime: Executing Requests

This monitor returns the number of requests that are currently executing.

JTA Coordinator: Threads Constraint Runtime: Must Run

This monitor returns the number of requests that must be executed to satisfy the constraint.

JTA Coordinator: Threads Constraint Runtime: Pending Requests

This monitor returns the pending requests that are waiting for an available thread.
**JTA Coordinator: Request Class: Pending Request**

This monitor returns the number of requests waiting for a thread to become available. A request class represents a class of work. Work using the same request class shares the same priority.

**JTA Coordinator: Work Manager: Pending Requests**

This monitor returns the number of pending requests in the queue of Work Manager.

**JTA Runtime: Active Transactions**

This monitor returns the number of active transactions on the server.

**JTA Runtime: Total Transaction**

This monitor returns the total number of transactions processed. This total includes all committed, rolled back, and heuristic transaction completions since the server was started.

**JTA Runtime: Total Rolled Back Transactions**

This monitor returns the number of transactions that were rolled back since the server was started.

**User Lockout: Threads Constraint Runtime: Deferred Requests**

This monitor returns the number of requests that are denied a thread for execution because the constraint is exceeded.

**User Lockout: Threads Constraint Runtime: Executing Requests**

This monitor returns the number of requests that are currently executing.

**User Lockout: Work Manager: Pending Requests**

This monitor returns the number of pending requests in the queue.

**User Lockout: Work Manager: Stuck Thread Count**

This monitor returns the number of threads that are considered to be stuck on the basis of any stuck thread constraints.

**WLS Admin Server: Allocated IO Buffer Bytes**

This monitor returns the amount of off-heap (native) memory, in bytes, reserved for file store use.

**WLS Admin Server: Allocated Window Buffer Bytes**

This monitor returns the amount of off-heap (native) memory, in bytes, reserved for file store window buffer use.

**WLS Admin Server: Object Count**

This monitor returns the number of objects contained in the store.
**POP3 Round Trip Email**

This template simulates an email round trip to test the ability of your SMTP server to receive and distribute email, and the ability of your users to retrieve messages from POP3-enabled email clients.

If you want to monitor Google gmail, you need to use the POP3 Roundtrip Email Template rather than the MAPI Roundtrip Email Template. MAPI is not compliant for gmail, because gmail is not a desktop email client.

**Prerequisites**

An SMTP server and a POP3 server.

**Credentials**

POP3 mailbox account. If the SMTP server requires authentication, the POP3 mailbox and the SMTP server must have identical user names and passwords.

**Monitored Components**

For details on monitors, see [SAM Component Monitor Types](#).

**POP3 User Experience Monitor**

This component monitor tests an email round trip from your SMTP mail server to your POP3 mail server and measures the time it takes to complete the trip. This response time is measured in milliseconds.
Postfix

This template assesses the performance of the Postfix MTA agent installed on the target server. Perl scripts are used for monitoring the performance of queries.

Prerequisites

SSH and Perl installed on the target server. SNMP installed on the target server and permission to monitor master, qmgr and pickup processes.

Credentials

Root credentials on the target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

You need to set thresholds for counters according to your environment. It is recommended to monitor counters for some period of time to understand potential value ranges and then set the thresholds accordingly.

Postfix statistic from maillog file

This monitor returns the Postfix mail statistic from the maillog file. The returned values are as follows:

- **Delivered** - This component returns the number of successfully delivered messages. Search for these messages in the maillog file using the following search pattern: “status=sent (delivered to”.
- **Forwarded** - This component returns the number of successfully forwarded messages. Search for these messages in the maillog file using the following search pattern: “status=sent (forwarded to”.
- **Rejected** - This component returns the number of rejected messages. Search for these messages in the maillog file using the following search pattern: “reject:“.
- **Received** - This component returns the number of received messages. Search for these messages in the maillog file using the following search pattern: “postfix/pickup”. (Look in the strings for: “sender=“ or “uid=“).
- **Discarded** - This component returns the number of discarded messages. Search for these messages in the maillog file using the following search pattern: “discard:“.
- **Deferred** - This component returns the number of deferred messages. If a message still has recipients for which delivery failed for some transient reason, and the message has been delivered to all the recipients possible, Postfix places the message into the deferred queue. Search for these messages in the maillog file using the following search pattern: “status=deferred“.
- **Bounced** - This component returns the number of bounced messages usually caused by undeliverable mail. Search for these messages in the maillog file using the following search pattern: "status=bounced".

- **Held** - This component returns the number of messages held. The administrator can define smtpd access policies and cleanup header and body checks that cause messages to be automatically diverted from normal processing and placed indefinitely in the hold queue. Messages placed in the hold queue stay there until the administrator intervenes. Search for these messages in the maillog file using the following search pattern: "hold:"

By default, the script retrieves this information from the /var/log/maillog file. If this file has another location on the target server, you should correct the path in the script argument box. By default, this monitor has the Count statistic as difference box checked. It will show the total number of messages in the Message field while the Statistic field will show only new messages since the last polling period.

### Messages from maillog file

This monitor returns the Postfix service messages statistic from the maillog file. The returned values are as follows:

- **Fatal** - This component returns the number of fatal service messages. Search for these messages in the maillog file using the following search pattern: " fatal:"

- **Warning** - This component returns the number of warning service messages. Search for these messages in the maillog file using the following search pattern: " warning:"

- **Panic** - This component returns the number of panic service messages. Search for these messages in the maillog file using the following search pattern: " panic:"

- **Error** - This component returns the number of error service messages. Search for these messages in the maillog file using the following search pattern: " error:"

By default, the script retrieves this information from the /var/log/maillog file. If this file has another location on the target server, you should correct the path in the script argument box. By default, this monitor has the Count statistic as difference box checked. It will show the total number of messages in the Message field while the Statistic field will show only new messages since the last polling period.

### Mail queue

This monitor shows the length of the mail queue.

### IMAP4 User Experience Monitor

This component monitor tests an email round trip from your SMTP mail server to your IMAP4 server and measures the time it takes to complete the trip.

By default, this component is disabled. To use this component, you should enable it and properly configure it.
POP3 User Experience Monitor

This component monitor tests an email round trip from your SMTP mail server to your POP3 mail server and measures the time it takes to complete the trip.

By default, this component is disabled. To use this component, you should enable it and properly configure it.

SMTP Monitor

This component monitor tests the ability of an SMTP server to accept incoming connections and respond with the correct code.

Process: master

This monitor returns the CPU and memory usage of the Postfix master process using SNMP. The Master daemon is the supervisor of Postfix, and it oversees all other Postfix daemons. The master waits for incoming jobs to be delegated to subordinate daemons. If there is a lot of work to do, the Master can invoke multiple instances of a daemon.

Process: qmgr

This monitor returns the CPU and memory usage of the Postfix qmgr process using SNMP. The qmgr daemon manages the Postfix queues; it is the heart of the Postfix mail system. It distributes delivery tasks to the local, smtp, lmtp, and pipe daemons. After delegating a job, it submits queue file pathname information, the message sender address, the target host (if the destination is remote), and one or more message-recipient addresses to the daemon it delegated the delivery task to.

Process: pickup

This monitor returns the CPU and memory usage of the Postfix pickup process using SNMP. The pickup daemon picks up messages put into the maildrop queue by the local sendmail user client program. After performing a few sanity checks, pickup passes messages to the cleanup daemon.
PostgreSQL

This template assesses the performance of a PostgreSQL 9 Server database by retrieving performance data from the built-in pg_stat_database, pg_locks, pg_trigger, pg_proc, pg_stat_all_tables and pg_indexes views.

Works with the Orion Agent for Linux.

Prerequisites

On the SAM Server, download and install the PostgreSQL 9 ODBC driver from the following location: http://www.postgresql.org/ftp/odbc/versions/msi/. On the PostgreSQL Server, find the following file:

```
C:\Program Files\PostgreSQL\9.0\data\pg_hba.conf
```

and add the following line to allow remote connections for the SAM Server:

```
hostallall 192.168.3.198/32 trust
```

where 192.168.3.198 is IP address of your SAM Server.

Configurations for Orion agent for Linux

For the following instructions, you should have PostgreSQL installed on a Linux-based computer.

1. Login to the Linux-based computer with administrator privileges.
   You will need to create a user account on the server and in the PostgreSQL database.

2. (Required) To begin, you should have unixODBC installed to support Microsoft Windows ODBC. If not, download and install the unixODBC driver to the Linux-based computer.
   Command: `yum install unixODBC`

3. Download and install the PostgreSQL ODBC driver on the target Linux-based computer.
   Command: `yum install postgresql-odbc`

4. Create a user account for the database.
   The example of commands adds a user account dbuser with the password Password1 to the Linux-based computer. The next commands login as the database superuser to the PostgreSQL server and modify the created user.

   ```
   # adduser dbuser
   # passwd Password1
   # su - postgres
   $ psql -d template1 -U postgres
   ```

   At the prompt, create the dbuser account with the Password1 password:
template1=# CREATE USER dbuser WITH PASSWORD 'Password1';

Next, grant privileges for your PostgreSQL database (TestDatabase) to the user account:

template1=# GRANT ALL PRIVILEGES ON DATABASE TestDatabase to dbuser;

Close the template:

template1=# \q

5. Test access to the database using the newly created account credentials.

$ su - dbuser
$ psql -d TestDatabase -U dbuser

Configure and assign a SAM template with the credentials.

1. In the Orion Web Console, click Settings > All Settings > SAM Settings > Manage Templates.
2. Search for the PostgreSQL template. SolarWinds recommends creating a copy of the template. Select the template and click Copy.
3. Modify the settings of the template and component monitors based on the metrics you want to monitor.
4. To enter credentials, select the component monitor checkboxes and click Assign Credentials.
5. Enter the credentials you created for the database and click OK.
6. Test the access for the template by assigning it to a node. Click Test Node to assign and test the access. If you encounter issues, verify the credentials and privileges for the account.

Troubleshooting

If you receive the error "FATAL: Peer authentication method failed for user 'postgresuser'", change the authentication method to md5.

Credentials

Database user name and password.

Monitored Components

For details on monitors, see [SAM Component Monitor Types](#).
Components without predetermined threshold values will provide guidance such as "Use the lowest threshold possible" or "Use the highest threshold possible" to help you find a threshold appropriate for your application.

**Database Cache Hit Ratio (%)**

This counter returns the percentage of pages found in the buffer cache without having to read from the disk in the specified database. This is the formula used: “cache reads”/ (“cache reads” + “physical reads”) * 100

This ratio should exceed 90%, and ideally be over 99%. If your counter is lower than 90%, you should consider adding more RAM if possible. A higher ratio value returned indicates improved performance by your server.

1. By default, this counter looks in the postgres database. If you want to monitor another database, you should change the database name in the Connection String field: (...DataBase=postgres;...) and the Sql Query field: (...where datname = 'postgres').

**Database Success Rate (%)**

This counter returns the percentage of successful transactions in the specified database. This is the formula used: “committed transactions”/ (“committed transactions” + “rolled back transactions”) * 100

This ratio should exceed 90%, and ideally be over 99%.

1. By default, this counter looks in the postgres database. If you want to monitor another database, you should change the database name in the Connection String field: (...DataBase=postgres;...) and the Sql Query field: (...where datname = 'postgres').

**Total Active Server Connections**

This counter returns the total number of server connections that are active. You should set the thresholds appropriate to your environment.

**Active Connections in Specified Database**

This counter returns the number of connections to the specified database. You should set the thresholds appropriate to your environment.

1. By default, this counter looks in the postgres database. If you want to monitor another database, you should change the database name in the Connection String field, (...DataBase=postgres;...) and the Sql Query field: (...where datname = 'postgres').

**Database Size (MB)**

This counter returns the size of the specified database in MB.

1. Note: By default, this counter looks in the postgres database. If you want to monitor another database, you should change the database name in the Connection String field, (...DataBase=postgres;...) and the Sql Query field, (...pg_database_size ('postgres')...).
Current Number of Locks on Server

This counter returns the total number of locks on the server.

This counter should be as low as possible. For more information about locks you should create a query and look in the pg_locks view.

Total Indexes in Current Database

This counter returns the total number of indexes for a current database. For more information about locks, you should look in the pg_indexes view.

By default this counter looks in the postgres database. If you want to monitor another database, you should change the database name in the Connection String field: (...DataBase=postgres;...).

Table with the biggest number of Sequential Scans

This counter returns the name of the table and its number of sequential scans for the current database.

By default, this counter looks in the postgres database. If you want to monitor another database, you should change the database name in the Connection String field: (...DataBase=postgres;...).

Table with the biggest number of Index Scans

This counter returns the name of the table and its number of index scans for the current database.

By default, this counter looks in the postgres database. If you want to monitor another database, you should change the database name in the Connection String field: (...DataBase=postgres;...).

Table with the biggest number of Row Reads

This counter returns the name of the table and its number of row reads for the current database.

By default, this counter looks in the postgres database. If you want to monitor another database, you should change the database name in the Connection String field: (...DataBase=postgres;...).

Total Number of Triggers

This counter returns the total number of triggers for the current database.

By default this counter looks in the postgres database. If you want to monitor another database, you should change the database name in the Connection String field: (...DataBase=postgres;...).

Size of the Largest Table (MB)

This counter returns the name of the largest table and its size in MB for the current database.
By default this counter looks in the postgres database. If you want to monitor another database, you should change database name in the Connection String filed: (...DataBase=postgres;...).

Total Number of Tables in Current Database

This counter returns the total number of tables for the current database.

By default this counter looks in the postgres database. If you want to monitor another database, you should change the database name in the Connection String field: (...DataBase=postgres;...).
Progress Database (Linux and Unix sh script)

This template assesses the status and overall performance of a Progress Database installed on Unix/Linux systems. This template uses sh scripts and the SNMP process monitor.

**Prerequisites**

SSH, sh installed on the target server and SNMP access to monitor the “_mprosrv” process.

**Credentials**

Root credentials on the target server.

ℹ️ This template was created and tested on the Progress Database v11.1. Some components in “Records Statistics”, “Database Activity Summary 1” and “Database Activity Summary 2” monitors may not correctly return information on different versions.

You should manually check your promon output and compare it to this one. To get this screen you need to execute the following commands:

```
promon /usr/wrk/test1.db
```

Inside promon you should select the following ordered options:

- R&D. Advanced options
- 2. Activity Displays
- 1. Summary

**Arguments in Linux/Unix monitors**

All scripts use the same argument structure:

```
sh ${SCRIPT} path_to_promon path_to_db
```

where

- `path_to_promon` - Full path to promon utility
- `path_to_db` - Full path to monitoring database file with .db extension.

**Example:**

```
sh ${SCRIPT} "/usr/bin/promon" "/usr/wrk/test1.db"
```

**Monitored Components**

ℹ️ For details on monitors, see [SAM Component Monitor Types](#).

**Records Statistics**

This monitor returns records statistics of the Progress Database. Returned values are as follows:
- **Record Reads** – This component returns the number of read records.
- **Record Updates** – This component returns the number of updated records.
- **Record Creates** – This component returns the number of created records.
- **Record Deletes** – This component returns the number of deleted records.
- **Record Locks** – This component returns the number of used locks on records.
- **Record Waits** – This component returns the number of users waited to gain access to locked records.

1. By default, this monitor has the Count statistic as difference box checked. It will show the new statistic since the last polling period.

**Database Activity Summary 1**

This monitor returns database activity summary. Returned values are as follows:

- **Commits** – This component returns the number of committed transactions.
- **Undos** – This component returns the number of canceled transactions.
- **DB Reads** – This component returns the number of read blocks from database.
- **DB Writes** – This component returns the number of written blocks to disk.
- **BI Reads** – This component returns the number of read BI blocks.
- **BI Writes** – This component returns the number of written BI blocks to disk.
- **AI Writes** – This component returns the number of written AI blocks to disk.
- **Active trans** – This component returns the number of active transactions.

1. By default, this monitor has the Count statistic as difference box checked. It will show the new statistic since the last polling period.

**Database Activity Summary 2**

This monitor returns database activity summary. Returned values are as follows:

- **Rec Lock Waits perc** – This component monitor returns the percentage of all requests to records that were waiting for unlocking. The returned value should be as low as possible. You should make your transactions as short as possible.
- **BI Buf Waits perc** – This component monitor returns the percentage of waiting for BI (Before-Image) buffers. This wait occurs when the database manager is waiting for BI buffers. The returned value should be as low as possible. If the returned value is large, you should increase the number of buffers with the database startup argument –bibufs.
- **AI Buf Waits perc** – This component monitor returns the percentage of waiting for AI (After-Image) buffers. This wait occurs when the database manager is waiting for AI buffers. The returned value should be as low as possible. If the returned value is large, you should increase the number of buffers with the database startup argument –aibufs.
- **Writes by APW perc** – This component monitor returns the percentage of written to disk blocks by using APW. The returned value should be as high as possible. If the returned value is low, you should increase the number of APW processes and increase the cluster size.
• **Writes by BIW perc** – This component monitor returns the percentage of written to disk blocks by using BIW. The returned value should be as high as possible. If the returned value is low, you should increase the number of buffers with the database startup argument –bibufs.

• **Writes by AIW perc** – This component monitor returns the percentage of written to disk blocks by using AIW. The returned value should be as high as possible. If the returned value is low, you should increase the number of buffers with the database startup argument –aibufs.

• **DB Size** – This component monitor returns the database size. The measured unit is shown in the returned message.

• **BI Size** – This component monitor returns the size of BI file. The measured unit is shown in the returned message.

• **AI Size** – This component monitor returns the size of AI file. The measured unit is shown in the returned message.

• **Buffer Hits perc** – This component monitor returns the number of buffer hits in a percentage format. The returned value should be near 100%. You can increase the number of buffers by using the –B argument.

**Database Status and Buffers**

This monitor returns the database status and buffer statistics. Returned values are as follows:

• **Empty blocks** – This component monitor returns the number of empty database blocks (never used).

• **Empty blocks perc** – This component monitor returns the number of empty database blocks (never used) in a percent format.

• **Free blocks** – This component monitor returns the number of free database blocks (were used before but now they are free).

• **Free blocks perc** – This component monitor returns the number of free database blocks (were used before but now they are free) in a percent format.

• **RM blocks with free space** – This component monitor returns the number of blocks in RM. RM chains consist of partially filled blocks of the database.

• **RM blocks with free space perc** – This component monitor returns the number of blocks in RM in a percent format. RM chains consist of partially filled blocks of the database.

• **Highest table number defined** – This component monitor returns the table's number.

• **Used buffers** – This component monitor returns the number of buffers currently in use.

• **Empty buffers** – This component monitor returns the number of buffers currently free.

**Database Startup Parameters and Shared Resources**

This monitor returns database startup parameters and shared resource statistic. Returned values are as follows:

• **Maximum clients** – This component monitor returns the number of allowed clients.

• **Maximum servers** – This component monitor returns the maximum number of servers.

• **Maximum clients per server** – This component monitor returns the maximum number of clients per server.

• **Number of servers** – This component monitor returns the number working servers.

• **Total users** – This component monitor returns the number of active users.
• **Number of page writers** – This component monitor returns the number of active APWs.
• **Number of monitors** – This component monitor returns the number of active monitor processes.
• **Number of semaphores allocated** – This component monitor returns the number allocated UNIX semaphores.

### Process: Database Broker

This monitor returns the CPU and memory usage of the Database Broker (mprsrv) process. The broker process manages shared resources and starts servers for remote users, if necessary.

ℹ️ This component monitor uses an SNMP monitor to gain process statistics. If it is not working, check your SNMP configurations on the target node.

### Database Broker TCP Port

This component monitor tests the ability of a database broker to accept incoming sessions.

ℹ️ By default, this monitor is disabled. Before using this monitor you should enter your broker database TCP port. This port is set by the “-S” argument during database startup.
RADIUS User Experience Monitor

This template allows test user authentication by using the RADIUS protocol.

Prerequisites

Access to the target RADIUS server.

Credentials

RADIUS credentials.

This monitor only supports PAP authentication.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

RADIUS User Experience Monitor

This component monitor tests the capabilities of a RADIUS server and measures the time it takes to perform a base user authentication operation. This component monitor uses synthetic transactions to test user authentication through the RADIUS protocol. The synthetic transaction does the following:

- Connect to server.
- Send RADIUS credentials and a shared secret.
- Validate response.
- Measure response time.

Before using this monitor, the correct Authentication and Accounting port numbers, as well as the Secret key, should be provided.
Remote Desktop Services Licensing


Prerequisites

- WMI access to the target server;
- Windows Server 2003 Resource Kit Tools should be installed on Terminal Licensing Server
- WinRM should be properly configured on target server.

Credentials

Windows Administrator on the target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

All Windows Event Log monitors should return zero values. Returned values other than zero indicate an abnormality. Examining the Windows System log file, with “TermServLicensing” and “TerminalServices-Licensing” source names, should provide information pertaining to the issue.

Detailed information about all these events can be found here:

- www.eventid.net

Licenses Usage

This monitor returns license usage statistics by running the lsreport tool from the Windows Server 2003 Resource Kit Tools. In the message fields, this component returns which machine connection is initialized (Client), which user currently uses a license (User), the License Type, and when the connection ends. Returned values are as follows:

- **Temporary** – This component returns the number of currently used Temporary licenses. Temporary licenses are given out when a client connects for the first time.
- **Active** – This component returns the number of currently used Active licenses. On the second connection and on successful logon, the client gets an Active license.
- **Upgraded** – This component returns the number of currently used Upgraded licenses. Windows 2000 licenses that were upgraded to a Windows 2003 license is called Upgraded.
- **Total Used** – This component returns the total number of currently used licenses.

This monitor uses the following arguments: path_to_lsreport, target_server:

- **path_to_lsreport** – This is the full path to the lsreport.exe file. If the Windows
Server 2003 Resource Kit Tools installed in the default location, this argument should be as follows:

- For x86 Windows: `C:\Program Files\Windows Resource Kits\Tools\lsreport.exe`;
- For x64 Windows: `C:\Program Files (x86)\Windows Resource Kits\Tools\lsreport.exe`.

**target_server** - This is the IP address of the target server. It should be: `${IP}`.

**Argument example:**

`C:\Program Files\Windows Resource Kits\Tools\lsreport.exe, ${IP}`

**Service: Remote Desktop Licensing**

This monitor returns the CPU and memory usage of the Remote Desktop Licensing server (Terminal Licensing Server on 2003). This service provides registered licenses for Remote Desktop Services clients. If this service is stopped, the server will be unavailable to issue Remote Desktop Services licenses to clients when they are requested.

**Events: Startup Errors**

This monitor returns the number of events that occur when:

- There is a Work Manager or Cannot Startup Work Scheduler error;
- The Terminal Services Licensing service could not create the service initialization thread;
- The Terminal Services Licensing service could not start due to a lack of system resources;
- The Terminal Services Licensing service cannot start due to an error;
- An error occurred during the Terminal Services license server initialization phase;
- The remote procedure call (RPC) port is not listening;
- TS Licensing is unable to allocate the required system memory to perform the operation;
- Cannot initialize policy module because of an error;
- A security descriptor cannot be set. As a result, terminal servers might not be able to connect to Terminal Services license servers.

**Type of event:** Error and Warning. Event ID: 43, 30, 36, 37, 4097, 4104, 4117, 41, 4142.

For **Work Manager** or **Cannot Startup Work Scheduler** errors, see the following article for details: [http://support.microsoft.com/kb/310122](http://support.microsoft.com/kb/310122). (© 2018 Microsoft Corp., available at [http://support.microsoft.com](http://support.microsoft.com), obtained on October 31, 2018)

**Terminal Services Licensing service:** If the service initialization thread cannot be created, or a lack of system resources events exist, you should increase the amount of available memory on the Terminal Services license server.

**Terminal Services Licensing service:** If this service cannot start due to an error event, ensure that the required groups are granted the correct permissions to the TermServLicensing registry key and that the value of the DBPath registry key matches the location of the LServer directory. If the problem persists, shut down and then restart the Terminal Services license server.
• For an error that occurred during the Terminal Services License Server Initialization Phase event, start the Terminal Services Licensing service, and if necessary, remove and then reinstall TS Licensing.
• For the remote procedure call (RPC) port is not listening event, verify that the Terminal Services license server is available and ensure that the Terminal Services Licensing service is running.
• For the Cannot Initialize Policy Module events, ensure that the Terminal Services Licensing registry key contains the following correct settings:
  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\TermServLicensing\Policy\MicrosoftCorporation\A02, and the registry subkey contains the following entry: String Name: DLL; String Value: %systemroot%\System32\tls236.dll.
• For Security Descriptor Cannot Be Set events, restart the Terminal Services Licensing service.

Events: License Errors

This monitor returns the number of events that occur when:

• Cannot generate a license for client because of an error;
• Terminal Services Licensing on the server has not been activated. Terminal Services Licensing will only issue temporary licenses until the server is activated;
• The Terminal Services Licensing server has no license pack registered product;
• The Terminal Server Licensing server has no permanent licenses for the product;
• A license could not be issued because it is not a member of the Terminal Server Computers group;
• One or more Terminal Services Licensing certificates on server are corrupt.

Type of event: Error and Warning. Event ID: 38, 18, 22, 21, 45, 17.

• For Cannot Generate A License For Client Because Of Error events, review this event in the Windows Event Monitor for details.
• For the Terminal Services Licensing On Server Has Not Been Activated events, activate your Terminal Services Licensing server.
• For the Terminal Services Licensing Server Has No License Pack Registered Product events: Use Terminal Services Licensing administrative tool to register the license pack.
• For the Terminal Server Licensing Server Has No Permanent Licenses For Product events, use the Terminal Server Licensing administrative tool to register more licenses.
• For A License Could Not Be Issued To Because It Is Not A Member Of The Terminal Server Computers Group events, check the status of the License Server Security Group. If the status is set to Enabled, a local group called Terminal Services Computers is created. The Terminal Server License Server grants licenses only to computers whose computer accounts are placed in this group. When the target computer is a domain controller, this group is a domain local group. If the status is set to Disabled, the Terminal Server License Server issues a license to any computer that requests one. The Terminal Services Computers group is not deleted or changed in any way. This is the default behavior. If the status is set to Not Configured, the Terminal Server License Server acts the same as if the status is set to Disabled. If you did not add any clients to this group, any machine attempting to connect to the terminal server would be denied.
For one or more Terminal Services Licensing certificates on server are corrupt events: you should reactivate this TS Licensing server or this RD Licensing server.

Events: Database Errors

This monitor returns the number of events that occur when:

- Cannot connect to the database;
- General database error occurred.

Type of event: Error and Warning. Event ID: 7, 44.

Refer to this article for more information: http://www.virtualizationadmin.com/articles-tutorials/terminal-services/licensing/troubleshooting-terminal-server-licensing-issues-part3.html.

Events: Service Stopped

This monitor returns the number of events that occur when:

- The Terminal Services Licensing service has stopped;
- TS Licensing has experienced a general initialization failure.

Type of event: Error and Warning. Event ID: 3, 4115.

For these events, start the Terminal Services Licensing service, and if necessary, remove and then reinstall TS Licensing.

Events: Connection Errors with SCM

This monitor returns the number of events that occur when:

- The Terminal Services Licensing service is unable to connect to the Service Control Manager;
- The Terminal Services Licensing service is unable to report status to the Service Control Manager.

Type of event: Error and Warning. Event ID: 27, 28.

For these events, restart the Terminal Services Licensing service, and if necessary, restart the server.

Configuring Windows Remote Management (WinRM)

If you have not already done so, install PowerShell 2.0 or later and WinRM on the SAM and target servers. For PowerShell installation details, see Microsoft's documentation website (https://docs.microsoft.com/en-us/powershell/).

1. On the SAM server, open a command prompt as an Administrator. To do this, go to the Start menu and right-click the cmd.exe and then select Run as Administrator.

2. Enter the following in the command prompt:
   winrm quickconfig
   winrm set winrm/config/client @{TrustedHosts="*"}
3. On the target server, open a command prompt as an Administrator and enter the following:
   `winrm quickconfig`
   `winrm set winrm/config/client @{TrustedHosts="IP_ADDRESS"}`
where IP address is the IP address of your SAM server.
Server Clock Drift

The following templates are available:

- Server Clock Drift (Perl)
- Server Clock Drift (PowerShell)
Server Clock Drift (PowerShell)

The template allows you to check the server clock drift by comparing the target server time with internet time.

Prerequisites

WinRM must be installed and properly configured on the target server.

Credentials

Administrator on the target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Clock Drift

This monitor shows the clock drift on the target server in seconds. Positive values of clock drift in the message field indicates that time on the target server is running faster than it should. Negative values indicates time on the target server is running slower than it should. This monitor also returns the current time on the target server.

In the Scripts Arguments field you should provide the hostname of the time server. Time servers can be found here: http://tf.nist.gov/tf-cgi/servers.cgi.

Following is an example of how to use the Scripts Arguments field: time.nist.gov
Server Clock Drift (Perl)

The template allows you to check server clock drift by comparing the target server time with internet time.

**Prerequisites**

Perl must be installed on the target server.

**Credentials**

Root on target server.

This template is based on the following script: [http://www.cs.cf.ac.uk/Dave/PERL/node174.html](http://www.cs.cf.ac.uk/Dave/PERL/node174.html).

**Monitored Components**

For details on monitors, see [SAM Component Monitor Types](#).

**Clock Drift**

This monitor shows the clock drift on the target server in seconds. Positive values of clock drift in the message field indicates that time on the target server is running faster than it should. Negative values indicates time on the target server is running slower than it should. This monitor also returns the current time on the target server.

In the Scripts Arguments field you should provide the hostname of the time server. Time servers can be found here: [http://tf.nist.gov/tf-cgi/servers.cgi](http://tf.nist.gov/tf-cgi/servers.cgi).

Following is an example of how to use the Scripts Arguments field: `perl ${SCRIPT} nist.netservicesgroup.com`
SOAP/JSON Example

This template includes three component monitor examples that point to the SolarWinds Information Service (SWIS) web service, which is a data access layer for the Orion product family that provides a hybrid of object-oriented and relational features. Similar to SQL, you can use SWQL to query your SolarWinds database for specific network information.

To learn more, see "About SWIS" at https://github.com/solarwinds/OrionSDK/wiki/About-SWIS.

Simple Object Access Protocol (SOAP) is a protocol used to exchange information in the implementation of web services in computer networks. It relies on XML for its message format, and usually relies on other application layer protocols, most notably Hypertext Transfer Protocol (HTTP). SOAP uses the POST method to send requests.

Prerequisites

WMI access to the SharePoint server.

Credentials

Windows Administrator on the target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

SOAP Monitor

You can use this component monitor to test a web service's ability to accept incoming sessions over a secure channel and then process the requested operation.

This example shows how a Web Services Description Language (WSDL) schema is loaded when the SOAP XML Request value is set to "Load from WSDL". For details, see Configure the SOAP monitor.

SOAP Monitor

You can use this component monitor to test a web service's ability to accept incoming sessions over a secure channel and then process the requested operation. This example monitor shows how to manually create a SOAP envelope works when the SOAP XML Request value is set to "Manually enter SOAP XML Request".

JSON Monitor

This component monitor tests a web server's ability to accept incoming sessions over a secure channel and then transmit the requested page. It can also test the security certificate.
Solaris

The following templates are available:

- Solaris
- Solaris LPD
Solaris

This template assesses the performance of the Solaris operating system installed on the target server. Perl scripts are used for monitoring the performance of queries.

Prerequisites

SSH and Perl installed on the target server.

Credentials

Root credentials on the target server.

Monitored Components

For details on monitors, see [SAM Component Monitor Types](#).

You need to set thresholds for counters according to your environment. It is recommended to monitor counters for some period of time to understand potential value ranges and then set the thresholds accordingly.

CPU statistic (%)

This monitor returns the percentage of CPU time used. The returned values are as follows:

- **User** – This component returns the percentage of CPU time spent running non-kernel code (user time). This represents the time spent executing user code. This statistic depends on the programs that the user is running. It is recommended to use the lowest threshold possible.
- **System** – This component returns the percentage of CPU time spent running the system kernel code (system time). It is recommended to use the lowest threshold possible.
- **Wait** – This component returns the percentage of CPU time waiting for I/O. It is recommended to use the lowest threshold possible.
- **Idle** – This component returns the percentage of CPU time spent idle. It is recommended to use the highest threshold possible at all times.

System faults statistic/sec

This monitor returns the rate of system faults, per second. The returned values are as follows:

- **Interrupts** – This component returns the number of interrupts per second. The threshold for this component depends on the processor. For modern CPUs, a threshold of 1,500 interrupts/sec is a acceptable. A dramatic increase in this value, without a corresponding increase in system activity, indicates a hardware problem.
- **System_Calls** – This component returns the number of system calls per second. This is a measure of how busy the system is handling applications and services. High System Calls/sec indicates high utilization caused by software. With today's faster CPUs, 20,000 would represent a reasonable threshold.
Context Switches – This component returns the number of context switches per second. High activity rates can result from inefficient hardware or poorly designed applications. The normal amount of Context Switches/Sec depends on your servers and applications. The threshold for Context Switches/sec is cumulative for all processors, so you need a minimum of 14,000 per processor (single=14,000, dual=28,000, quad=56,000, and so forth).

Kernel threads statistic

This monitor returns the number of kernel threads in different states. The returned values are as follows:

- **In_Run_Queue** – This component returns the average number of runnable kernel threads over the sampling interval. This should be as low as possible. If the run queue is constantly growing, it may indicate the need for a more powerful CPU or more CPUs. Set the thresholds appropriately for your environment.

- **Waiting_For_resources** – This component returns the average number of kernel threads placed in the VMM wait queue (awaiting resource, awaiting input/output) over the sampling interval. This should be as low as possible. Set the thresholds appropriately for your environment.

Memory and Swap statistic (MB)

This monitor returns the memory and swap statistic in MB. The returned values are as follows:

- **Free_Memory** – This component returns the amount of available memory in MB. Use the highest threshold possible at all times. Set the thresholds appropriately for your environment.

- **Used_Memory** – This component returns the amount of used memory in MB. Use the lowest threshold possible.

- **Free_Swap** – This component returns the amount of available swap in MB. Use the highest threshold possible at all times. Set the thresholds appropriately for your environment.

- **Used_Swap** – This component returns the amount of used swap in MB. Use the lowest threshold possible.

Paging statistic/sec

This monitor returns the different paging statistics. The returned values are as follows:

- **Page_Faults** – This component shows the number of page faults per second. This is not a count of page faults that generate I/O. Some page faults can be resolved without I/O. Use the lowest threshold possible.

- **Paged_In** – This component returns the rate of pages "paged in" from paging space in kB, per second. The operation of reading one inactive page or a cluster of inactive memory pages from the disk is called a "page in." Use the lowest threshold possible.

- **Paged_Out** – This component returns the rate of pages "paged out" from paging space in kB, per second. The operation of writing one inactive page or a cluster of inactive memory pages to the disk is called a "page out." Use the lowest threshold possible. Values above 20 pages (80 kB), or so, indicate a significant performance problem. In this situation, more memory should be installed.
Processes in different states

This monitor returns the different paging statistics. The returned values are as follows:

- **Sleeping** – This component returns the number of processes that are waiting for an event to complete.
- **Runnable** – This component returns the number of processes that are on run queue.
- **Zombie** – This component returns the number of processes that are terminated and where the parent is not waiting. This should always be zero. If it is not zero, you should manually kill zombie processes. Use the following commands to see these zombie processes: `ps -ecl | grep "Z"`.
- **Stopped** – This component returns the amount of processes that are stopped, either by a job control signal or because it is being traced.

Space on root (/) partition (MB)

This monitor returns the available and used space of the root (/) partition in MB. The returned values are as follows:

- **Available_Space** – This component returns the available space on the root (/) partition in MB. Use the highest threshold possible at all times.
- **Used_Space** – This component returns the used space on the root (/) partition in MB.

Percentage of using system devices

This monitor returns the name of the system device and the percentage of time the device was busy servicing a transfer request.

1. After applying this template on the target node, you should navigate to, Edit Application Page and click Get Script Output in the Script section. This will build the list of system devices that should be monitored.

Disk operations/sec of system devices

This monitor returns the name of the system device and its read/write transfers to or from the device.

1. After applying this template on the target node, you should navigate to, Edit Application Page and click Get Script Output in the Script section. This will build the list of system devices that should be monitored.

Top 10 active processes

This monitor returns the top 10 active processes and share of CPU usage in percent.
Solaris LPD

This template assesses the status and performance of a Solaris LPD print service. Perl scripts are used for retrieving performance data.

**Prerequisites**

SSH and Perl installed on the target server.

**Credentials**

Root credentials on the target server.

**Monitored Components**

For details on monitors, see [SAM Component Monitor Types](#).

**Daemon: lpsched**

This monitor returns the status of the Solaris LPD print server daemon.

Possible values:

- 0 – Print server daemon is stopped.
- 1 – Print server daemon is running.

**Print queue**

This monitor returns the current length of the default print queue.

**Successfully printed jobs**

This monitor returns the number of successfully printed jobs by retrieving data from the requests log file. Successful printed jobs have the following status string in the requests log file: `s 0x0014`


By default, the script retrieves this information from the `/var/spool/lp/logs/requests` file. If this file has another location on the target server, you should correct the path in the script argument box.

**Unsuccessfully printed jobs**

This monitor returns the number of jobs that were not successfully printed by retrieving data from the requests log file. The script in this component is looking for all print status strings in the requests log file other than `s 0x0014`.

By default, the script retrieves this information from the `/var/spool/lp/logs/requests` file. If this file has another location on the target server, you should correct the path in the script argument box.

**LP Print Server Listening TCP Port**

This component monitor tests the ability of an LP print service to accept incoming sessions.

By default, TCP port 631 is monitored. If your print server listens on another port, you should manually change it.
SolarWinds templates

The following templates are available:

- Orion Server 2017.3
- SolarWinds Failover Engine
- SolarWinds NetFlow Traffic Analyzer
- SolarWinds NetFlow Traffic Analyzer Database
- SolarWinds Web Performance Monitor (WPM) Player
- Kiwi Syslog Server
Orion Server 2017.3

This template assesses the status of Windows services related to SolarWinds Orion servers running Orion Platform 2017.3.

You can use this template with later versions of the Orion Platform also. It contains mostly service, process, and MSMQ counters that don't change much between Orion Platform versions.

Prerequisites

WMI access to the target server.

Credentials

Windows Administrator on the target server.

Monitored components

For details on monitors, see SAM Component Monitor Types.

SolarWinds Orion Job Engine

This monitor returns the CPU and memory usage of the SolarWinds Orion Job Engine service. This service is used to perform recurring work. This service creates various Job Engine Worker processes for scalability and robustness. The job engine writes information about each job to its database.

SolarWinds Orion Module Engine

This monitor returns the CPU and memory usage of the SolarWinds Orion Module Engine service. This service is used to talk to the database.

SolarWinds Orion Job Scheduler

This monitor returns the CPU and memory usage of the SolarWinds Orion Job Scheduler service. The Job Scheduler service dispatches work to local and/or remote job engines.

SolarWinds Syslog Service

This monitor returns the CPU and memory usage of the SolarWinds Syslog service. This service is responsible for logging events in log files.

SolarWinds Alerting Service V2

This monitor returns the CPU and memory usage of the SolarWinds Alerting Service V2. This service is responsible for evaluating alert conditions, triggering alerts and running alert actions.

SolarWinds Alerting Engine

This monitor returns the CPU and memory usage of the SolarWinds Alerting Engine service. This service is responsible for Advanced Alerting.
SolarWinds Website

This component monitor tests a web server's ability to accept incoming sessions and transmit the requested page. The component monitor can optionally search the delivered page for specific text strings and pass or fail the test based on that search. By default, it monitors TCP port 80.

SolarWinds Job Engine v2

This monitor returns the CPU and memory usage of the SolarWinds Job Engine v2 service. This service is used to perform recurring work. This service creates various Job Engine Worker processes for scalability and robustness. The job engine writes information about each job to its database.

SolarWinds Collector Data Processor

This monitor returns the CPU and memory usage of the SolarWinds Collector Data Processor service. This service is responsible for volume and node data synchronization between the Collector and the Standard Poller.

SolarWinds Collector Management Agent

This monitor returns the CPU and memory usage of the SolarWinds Collector Management Agent service. This service takes part in data synchronization between the Collector and the Standard Poller.

SolarWinds Collector Polling Controller

This monitor returns the CPU and memory usage of the SolarWinds Collector Polling Controller service. This service takes part in data synchronization between the Collector and the Standard Poller.

SolarWinds Information Service

This monitor returns the CPU and memory usage of the SolarWinds Information service. This service is used by websites to talk to the database. This service is also responsible for how the polling engines talk to each other.

SolarWinds Information Service V3

This monitor returns the CPU and memory usage of the SolarWinds Information service V3. This service is used by websites to talk to the database. This service is also responsible for how the polling engines to each other.

SolarWinds JMX Bridge

This monitor returns the CPU and memory usage of the SolarWinds JMX Bridge service. The JMX Bridge is only used if you are monitoring Java Application Servers such as WebSphere, WebLogic, or Apache Tomcat via JMX.

Note: By default, this monitor is disabled.

SolarWinds Trap Service

This monitor returns the CPU and memory usage of the SolarWinds Trap service. This service is responsible for catching and logging trap events.
File Count Monitor - JET Files

This monitor returns the number of JET files in C:\Windows\Temp. Excessive JET files can block new database connections and halt polling so this monitor should be less than 65,530. These files can be deleted. They usually stay in the system only if an application that uses them accessed a database that crashed so files were not properly deleted.

No more than 65 KB of JET files should be stored in the C:\Windows\Temp folder.

MSMQ Messages in Queue

This is the total number of Message Queuing messages that currently reside in the selected queue. When the Data Processor receives more results into MSMQ than it is able to process and pass to the Standard Poller, MSMQ continues growing. The size of MSMQ should be near 0 most of the time. Some spikes may appear, but the Data Processor needs to be able to clean up the MSMQ quickly, otherwise it may not be able to handle DB blackouts or maintenance. (Standard Poller performance is affected by DB performance significantly.)

Before using this counter, you should set the correct instance beginning with:
<HOSTNAME>\private$\solarwinds\collector\processingqueue
where  <HOSTNAME> is the hostname (without < >) of target server. For example: APMhost.

By default, the instance is set to:
<HOSTNAME>\private$\solarwinds\collector\processingqueue\solarwinds.nodehardwarehealth.wmi

All available instances can be found by running the perfmon utility and searching for “Messages in Queue” counter in the “MSMQ Queue” category.

This monitor is disabled by default. Enable through the component monitor settings.

Perfmon DPPL Avg. Time to Process Item

This monitor returns the time needed to process one item. If this number is 1, it means you are able to process one item per second. 0.01 means 100 items per second. The returned value should be as low as possible.

Perfmon DPPL Waiting Items

This monitor returns items in the queue pulled from the message queue but waiting for other results to be processed. This should be less than 40. If this number is holding at or above 40, this may indicate issues concerning DB response time, performance issues, or many down elements.

MSMQ Folder Size

This monitor returns the MSMQ folder size. This monitor should be less than 800 MB. MSMQ maximum size is 1GB. If the 1GB limit is reached, polling will stop working correctly.

To Increase the MSMQ size, you should open Computer Management > Features > Messaging Queuing. From here, right-click and change MSMQ Messaging 1 GB Limit to 1.5GB. For Windows Server 2003, this is found under the Storage section.
See this SolarWinds Success Center article for helpful information: Microsoft Message Queue Fills Directory with Orphaned Files.

Process Monitor - SWJobEngineWorker2.exe

This monitor returns the number of Job Engine worker processes and its CPU and memory usage. A value of 10 or lower is acceptable. If the returned value is 100 or greater, there may be problems with jobs hanging.

Job Engine v2: Jobs Queued

This monitor returns the number of jobs waiting for execution due to insufficient resources. This value should be zero at all times.

Job Engine v2: Jobs Lost

This monitor returns the number of lost jobs. This value should be zero at all times.

Job Engine v2: Jobs Running

This monitor returns the number of jobs currently running.

Job Engine v2: Worker Processes

This monitor returns the number of worker processes used. A value of 10 or lower is acceptable. If the returned value is 100 or greater, there may be problems with jobs hanging.

Job Scheduler v2: Average Execution Delay

This monitor returns the average delay, in milliseconds, between the time when the job is supposed to be executed and the time that it actually is executed. This value should be less than 100,000.

Job Scheduler v2: Results Notified Error

This monitor returns the number of errors that occurred when sending the results back. This value should be zero at all times.

SolarWinds Failover Engine

This template assesses the status and overall performance of a SolarWinds Failover Engine server.

Prerequisites

WMI access to the target server.

Credentials

Windows Administrator on the target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.
Service: SolarWinds FoE SCOPE Data Collector

This monitor returns CPU and memory usage of the Failover Engine cope Data Collector service, which collects and stores configuration and performance data.

Service: SolarWinds FoE Server

This monitor returns CPU and memory usage of Failover Engine.

Current Throughput

This monitor returns the current throughput via the CommsMgr in MBits/sec.

KB Dispatched from Receive Queue

This monitor returns the number of KB data applied from the Receive Queue. This is only available on the passive server.

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

KB Dispatched from Send Queue

This monitor returns the number of KB data sent from the Send Queue. This is only available on the active server.

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

MegaBytes Received

This monitor returns the number of MegaBytes received across all channels.

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

MegaBytes Sent

This monitor returns the number of MegaBytes sent across all channels.

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

Messages Received

This monitor returns the individual messages received by CommsMgr.

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

Messages Sent

This monitor returns the individual messages sent by CommsMgr.
This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

**Oldest Receive Update Queue Entry**
This monitor returns the age of the oldest Receive Update Queue entry in milliseconds.

**Oldest Send Update Queue Entry**
This monitor returns the age of the oldest Send Update Queue entry in milliseconds.

**Receive Queue Drain Rate**
This monitor returns the number of bytes drained per millisecond from CommsMgr Receive Queue.

**Receive Queue Size**
This monitor returns the number of bytes in CommsMgr Receive Queue.

**Send Queue Drain Rate**
This monitor returns the number of bytes drained per millisecond from CommsMgr Send Queue.

**Send Update Queue Size**
This monitor returns the number of bytes in CommsMgr Send Update Queue.

**TCP Port: Client**
This monitor tests the ability of a Failover Engine client to accept incoming sessions. By default, it monitors TCP port 52267.

By default, this monitor is disabled.

**Warning and Error Events: Interceptor Driver**
This monitor returns the number of Interceptor Drivers error and warning events.

Source name: Nfid.
Log name: System.

**Warning and Error Events: Packet Filter**
This monitor returns the number of Packet Filter errors and warning events.

Source name: NFPktfltr.
Log name: System.

**Warning and Error Events: Failover Server**
This monitor returns the number of Failover Server errors and warning events.

Source name: NFServerR2.
Log name: Application.
SolarWinds NetFlow Traffic Analyzer Database

This template assesses the performance of a SolarWinds NetFlow Traffic Analyzer by retrieving performance data from the Orion database.

**Prerequisites**

None.

**Credentials**

SQL Server user name and password.

**Monitored Components**

For details on monitors, see [SAM Component Monitor Types](#).

**Status of NetFlow maintenance**

This monitor checks to make sure maintenance is running properly. If the NetFlow Traffic Analyzer maintenance is functioning properly, this component will return a value of zero. If the returned value is greater than zero, NTA Maintenance is not performing properly which can lead to performance issues. If this is the case, run NTA Database Maintenance manually. (This application can be found in the SolarWinds directory). If the value returned is still greater than zero, contact SolarWinds support.

**Number of NetFlow Interfaces Receiving Data**

This monitor returns the number of NetFlow interfaces that have received data within two minutes. If this counter is consistently zero, problems with receiving this information exists.

- By default, this component monitor is disabled and should only be enabled for troubleshooting purposes.

**Number of CBQoS Interfaces Receiving Data**

This monitor returns the number of CBQoS interfaces that received data within two minutes. If this counter is consistently zero, problems with receiving this information exists.

- By default, this component monitor is disabled and should only be enabled for troubleshooting purposes.

**Number of NetFlow Interfaces not Receiving Data**

This monitor returns the number of NetFlow interfaces which should, but have not yet, received data within two minutes. The value returned should be as low as possible. If the returned value is greater than zero, the flow is not received even though the interfaces are configured to receive this type of flow. This could be an indication of an improperly configured switch. If this is the case, ensure that the switch exports a flow for that interface or disable the interface in NetFlow Sources.
Number of CBQoS Interfaces not Receiving Data

This monitor returns the number of CBQoS interfaces which should, but have not yet, received data within two minutes. The returned value should be as low as possible. If the returned value is greater than zero, a flow is not received even though the interfaces are configured to receive this type of flow. This could be an indication of an improperly configured switch. If this is the case, ensure that switch exports a flow for that interface or disable the interface in NetFlow Sources.

NetFlow Service Status

This monitor returns the running state of the NetFlow service by comparing the current time with the KeepAlive timestamp. If the difference is greater than 15 minutes, a zero value will be returned, indicating a problem with the service status; otherwise, a value of one is returned. If this is the case, verify the NTA service is running properly on the server. If there are persistent problems with this service, contact SolarWinds support.

1 By default, this component monitor is disabled and should only be enabled for troubleshooting purposes.

High Priority Queue Addresses that are not Processed

This monitor returns the number of addresses in the high priority queue that are not processed but should be processed. The returned value should be near or at zero. If the value fails to drop to zero, this means DNS server is not able to process all of the incoming IP addresses. If this is the case, adjust your DNS server to process more requests per second, or switch DNS resolving to On Demand. This counter will function only when the DNS resolution is set to "persistent."

Low Priority Queue Addresses that are not Processed

This monitor returns the number of addresses in the low priority queue that are not processed but should be processed. The returned value should be near or at zero. This queue contains IP addresses which were not resolved and should be resolved and is processed when the first queue is empty. If the returned value continues to grow, it can be an indication of an improperly configured DNS which is not able to resolve IP addresses. This counter will function only when the DNS resolution is set to "persistent."

Number of records in NTA Summary table 1

This monitor returns the number of records in NetFlowSummary1 table. This value should be around the same value for each summary table. Compare this monitor with Number of records in NTA Summary table 2 and Number of records in NTA Summary table 3 monitors. If the value is growing daily, this is an indication that the NTA Database Maintenance is not working properly. If this is the case, run NTA Database Maintenance manually. (This application can be found in the SolarWinds directory). If the value returned is still greater than zero, contact SolarWinds support.

Note: This query uses a great deal of resources and should be executed just once per day. By default, this component monitor is disabled and should only be enabled for troubleshooting purposes.
Number of records in NTA Summary table 2

This monitor returns the number of records in NetFlowSummary1 table. This value should be around the same value for each summary table. Compare this monitor with Number of records in NTA Summary table 1 and Number of records in NTA Summary table 3 monitors. If the value is growing daily, this is an indication that the NTA Database Maintenance is not working properly. If this is the case, run NTA Database Maintenance manually. (This application can be found in the SolarWinds directory). If the value returned is still greater than zero, contact SolarWinds support.

Note: This query uses a great deal of resources and should be executed just once per day. By default, this component monitor is disabled and should only be enabled for troubleshooting purposes.

Number of records in NTA Summary table 3

This monitor returns the number of records in NetFlowSummary1 table. This value should be around the same value for each summary table. Compare this monitor with Number of records in NTA Summary table 1 and Number of records in NTA Summary table 2 monitors. If the value is growing daily, this is an indication that the NTA Database Maintenance is not working properly. If this is the case, run NTA Database Maintenance manually. (This application can be found in the SolarWinds directory). If the value returned is still greater than zero, contact SolarWinds support.

- This query uses a great deal of resources and should be executed just once per day. By default, this component monitor is disabled and should only be enabled for troubleshooting purposes.

Number of Detail Tables

This monitor returns the number of Detail Tables in the database, per node. Each node has a specific number of Detail Tables which can be changed in the NetFlow Settings. The default is four.

If the number of Detail Tables per node exceeds the allowed maximum and continually grows, this could be an indication that there is a problem with the NTA service. If this is the case, verify that all services are running properly. If needed, run NTA Database Maintenance manually. (This application can be found in the SolarWinds directory). If the problem persists, contact SolarWinds Technical Support.

Number of polling Huawei devices

This monitor returns the number of Huawei devices with interface mapping that are enabled and working properly. If you do not have any Huawei devices, the value returned should be zero. If you have devices with interface mapping enabled and the returned value is zero, interface mapping may not be working properly.

- By default, this component monitor is disabled and should only be enabled for troubleshooting purposes.
SolarWinds NetFlow Traffic Analyzer


Prerequisites

WMI access to the target server.

Credentials

User with administrative privileges on the target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Service: SolarWinds NetFlow Service

This component returns CPU and memory usage of the SolarWinds NetFlow Service. This service is responsible for receiving and saving data to the database as well as providing licensing information to the web console. If this service is stopped, data will not be collected.

Cached Data Queue Length

This monitor returns the amount of data not currently saved to the database. If this service is stopped or disabled, this data will be lost. This value should be as low as possible. If the returned value grows, the NTA server will not be able to save processed flows into the database. It is recommended that you adjust Top Talkers Optimization.

Collapsed Records Per Second

This monitor returns the amount of incoming records that are collapsed, per second.

By default, this component monitor is disabled and should only be enabled for troubleshooting purposes.

IP Address Cache Size

This monitor returns the size of the IP address cache. This counter will function only when the DNS resolution is set to "persistent."

By default, this component monitor is disabled and should only be enabled for troubleshooting purposes.

IP Requests Per Second

This monitor returns the IP requests rate, per second. This counter will function only when the DNS resolution is set to "persistent."
By default, this component monitor is disabled and should only be enabled for troubleshooting purposes.

**IP Requests Queued**
This monitor returns the number of IP requests in the queue. This counter will function only when the DNS resolution is set to "persistent."

**IP Resolved Per Second**
This monitor returns the IP resolved rate, per second. This counter will function only when the DNS resolution is set to "persistent."

By default, this component monitor is disabled and should only be enabled for troubleshooting purposes.

**IP Responses Per Second**
This monitor returns the IP responses rate, per second. This counter will function only when the DNS resolution is set to "persistent."

By default, this component monitor is disabled and should only be enabled for troubleshooting purposes.

**IP Responses Queued**
This monitor returns the number of IP responses in the queue. This counter will function only when the DNS resolution is set to "persistent."

**IP UnResolved Per Second**
This monitor returns the IP unresolved rate, per second. This counter will function only when the DNS resolution is set to "persistent."

**Packets Received Per Second**
This monitor returns the packets received rate, per second, before the queue.

By default, this component monitor is disabled and should only be enabled for troubleshooting purposes.

**Packet Dropped: Unmanaged Node**
This monitor returns the number of packets dropped due to a node not being managed by NetFlow. This is caused by the node being disabled or the node not existing in NPM. The returned value should be zero. If the returned value is greater than zero, add these nodes to NPM or disable the exporting of these flows on your router.

**Packet Dropped: Unmonitored Node**
This monitor returns the number of packets dropped due to a node not being monitored by NetFlow. These nodes are monitored by NPM. The returned value should be zero. If the value is greater than zero, add these nodes as NetFlow Sources or disable the exporting of these flows on the router.
PDU Dropped: Unmanaged Interface

This monitor returns the number of PDUs dropped due to an interface not being managed by NetFlow. This is caused by the node being disabled or the node not being in the NetFlow Sources table. This counter will function only when the option, "Allow monitoring of flows from unmanaged interfaces," in the NTA settings is set.

PDU Dropped: Unmonitored Interface

This monitor returns the number of packets dropped due to an interface not being monitored by NetFlow. These Interfaces are in NPM. The value returned should be zero. If the value is greater than zero, add these interfaces into NetFlow Sources or disable the exporting of these flows on the router.

PDU Dropped: Unmonitored Port

This monitor returns the number of packets dropped due to an unmonitored application. This counter is connected to the "Enable data retention for traffic on unmonitored ports" setting in NTA settings. If checked, flows with unmonitored ports will remain stored in the database. If unchecked, flows will be dropped and this counter will continue to grow. The returned value should be zero. If the value returned is greater than zero, you should verify that all the ports you want to monitor are actually being monitored.

PDU Dropped: Unmonitored Protocol

This monitor returns the number of packets dropped due to a disabled protocol. Protocols to be monitored can be changed in the NetFlow Settings > Monitored Protocols section. The returned value for this monitor should be zero. If the value returned is greater than zero, you should verify that the protocols you want to monitor are actually being monitored.

PDUs Processed Per Second

This monitor returns the PDUs processed, per second.

Raw Packet Queue Length

This monitor returns the number of raw packets in the queue. If the value returned continues to grow, this indicates that the NetFlow service will not be able to handle the amount of incoming flows quickly enough, thereby placing them in the queue. Consider upgrading your APM server to improve performance.

Netflow V1 Bytes Received Per Second

This monitor returns the number of bytes NetFlow V1 received per second.

Note: By default, this component monitor is disabled and should only be enabled for troubleshooting purposes.

Netflow V1 Flows Received Per Second

This monitor returns the number of flows NetFlow V1 received per second.

By default, this component monitor is disabled and should only be enabled for troubleshooting purposes.
Netflow V5 Bytes Received Per Second

This monitor returns the number of bytes NetFlow V5 received per second.

- By default, this component monitor is disabled and should only be enabled for troubleshooting purposes.

Netflow V5 Flows Received Per Second

This monitor returns the number of flows NetFlow V5 received per second.

- By default, this component monitor is disabled and should only be enabled for troubleshooting purposes.

Netflow V9 Bytes Received Per Second

This monitor returns the number of bytes NetFlow V9 received per second.

- By default, this component monitor is disabled and should only be enabled for troubleshooting purposes.

Netflow V9 Flows Received Per Second

This monitor returns the number of flows NetFlow V9 received per second.

- By default, this component monitor is disabled and should only be enabled for troubleshooting purposes.

sFlow V5 Bytes Received Per Second

This monitor returns the number of bytes sFlow V5 received per second.

- By default, this component monitor is disabled and should only be enabled for troubleshooting purposes.

sFlow V5 Flows Received Per Second

This monitor returns the flow rate received, per second, for sFlow V5.

- By default, this component monitor is disabled and should only be enabled for troubleshooting purposes.

Packet Dropped: Insufficient performance

This monitor returns the amount incoming packets dropped due to the poor performance of the SQL server or NTA Service. The returned value should be zero. If this occurs in one specific instance, verify that the database server is not overloaded. Database Maintenance may be the culprit. If this is a persistent problem, the database server probably is not able to process the amount of incoming flows. It is recommended that you adjust Top Talkers Optimization.
Netflow service time difference error

This monitor returns the number of events when the time difference between the database server and the NTA Server is greater than 5 minutes.

**Type of event:** Error. Event ID: 340, 341.

Possible impact: Data in the database could be saved and represented wrongly.

Solution: Synchronize the time between the NTA Server(s) and the database server.

Unmonitored traffic record is missing

This monitor returns the number of events that occur when system records go missing in the NTA table.

**Type of event:** Event ID: 304.

Solution: Run the Configuration Wizard to repair this problem.

Unable to start listening on port

This monitor returns the number of events when the NTA service cannot start the port listener on NTA port. (Default is port 2055).

**Type of event:** Event ID: 323.

Impact: NTA Service is not able to receive flows.

Solution: Verify the actual port that is occupied and attempt to free it, or, change the port of the NTA service which can be located on the NTA Settings page.

PDUs Received Per Second

This monitor returns the PDUs received, per second.

**SolarWinds Web Performance Monitor (WPM) Player**

This template assesses the status and overall performance of SolarWinds Web Performance Monitor (WPM) Player installed on the SAM server by using Windows Performance Counters.

**Prerequisites**

WMI access to the target server. WinRM must be installed and properly configured on the target server.

**Credentials**

Windows Administrator on the target server.

**Monitored Components**

For details on monitors, see [SAM Component Monitor Types](#).
Service: SolarWinds WPM Playback Player

This monitor returns the CPU and memory usage of the SolarWinds WPM Playback Player service. This service is responsible for the automatic playbacks of web transactions. This is the main part of WPM Player that receives and manages transactions that should be played. If this service is not running, no transactions are played.

Service: SolarWinds WPM Playback Player Proxy

This monitor returns the CPU and memory usage of SolarWinds WPM Playback Player Proxy service. This service is responsible for communication with active players.

SeUM Agent dropped queue items

This monitor returns how many requests were dropped because they were already in the queue. The agent has an internal queue that it uses for transaction playback requests that cannot be immediately executed because there are no free worker processes. If a transaction is in the queue and a new playback request for the same transaction arrives, it is dropped because the queue cannot contain duplicate requests.

If the number of dropped requests increases significantly, it usually means that the Player is not able to play transactions as fast as they are requested. You should remove some transactions from the Player.

This counter has the Count statistic as difference option enabled and will show the statistical difference from the last polling cycle.

SeUM Agent enqueued items

This monitor returns the number of requests that are currently in the queue. The agent has an internal queue that it uses for transaction playback requests that cannot be immediately executed because there are no free worker processes. The queue cannot contain duplicate requests. If the number of items in the queue is close to the number of transactions assigned to the Player, it usually means that the Player is close to its capacity and is not able to play transactions fast enough.

SeUM Agent requested playbacks

This monitor returns the number of playback requests that were sent to the Player since it started. If the counter is not changing, the Player is not receiving any playback requests. There may be issues with the central WPM server or connection.

Size of internal WPM Player database

This monitor returns the size of the internal WPM Player database used for storing playback requests, results and screenshots. Depending on the number and complexity of assigned transactions, this file can grow rather large. This file can be found here:
c:\ProgramData\SolarWinds\SeUM\Data\AgentStorage.s3db.

If the file size grows too large, (over 2GB for example), this may mean that the playback results are not correctly downloaded from the Player. This can happen if there is a slow network connection between the WPM server and the Player. If this is the case, this file will continue to grow because results are generated faster than they are downloaded from Player.
Errors in AgentService.log file

This monitor returns errors from the AgentService.log. The returned values are as follows:

**Total** – This component monitor returns the total number of errors in the log file. The value returned should be as low as possible.

**New** – This component monitor returns the number of newly found error strings.

**Last_Message** – This component monitor returns the last error message and its position in the log file.

You must specify the correct arguments (path to AgentService.log file) for this monitored component in the Script Arguments field. By default it monitors: c:\ProgramData\SolarWinds\Logs\SeUM\AgentService.log.

Number of running WPM worker processes

This monitor returns the number of active WPM worker processes (SolarWinds.SeUM.Agent.Worker.exe). This process usually runs in multiple instances and is responsible for the actual playback of transactions. SolarWinds WPM Playback Player service uses these processes to execute playbacks. The default number of these processes is 2 on main WPM server.
Kiwi Syslog Server

This template assesses the status and overall performance of Kiwi Syslog Server v9.4.0 and higher.

Prerequisites

WMI access to the target server.

Credentials

Windows Administrator on the target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Service: Kiwi Syslog Server

This monitor returns CPU and memory usage of the Kiwi Syslog Server service. This service receives Syslog messages and SNMP traps.

Service: UltiDev Web Server Pro

This monitor returns CPU and memory usage of Kiwi UltiDev Web Server Pro. This is the web server used by Kiwi Syslog Server.

By default, this monitor is disabled. Before you enable this monitor you should provide the correct "Net Service Name" of your UltiDev Web Server. The service name changes from version to version. To do this, open Service mmc, then open Properties for the "UltiDev Web Server" service, copy "Service Name" and paste it into "Net Service Name" in this monitor in the template.

TCP Port: Kiwi Syslog Website

This component monitor tests the Kiwi Syslog website ability to accept incoming sessions and transmit the requested page. By default it monitors TCP port 8088.

TCP Port: Syslog Messages (TCP)

This component monitor tests the Kiwi Syslog Service's ability to accept incoming sessions and transmit the requested page by using the TCP protocol. By default it monitors TCP port 1468.

This monitor is disabled by default. Enable through the component configurations.

TCP Port: Syslog messages (Secure TCP)

This component monitor tests Kiwi Syslog Service's ability to accept incoming sessions and transmit the requested page by using a Secure TCP protocol. By default it monitors TCP port 6514.

This monitor is disabled by default. Enable through the component configurations.
TCP Port: Kiwi Syslog Server

This component monitor tests Kiwi Syslog Server's ability to accept incoming sessions and transmit the requested page. This is the port used by the KSS Console to communicate with the KSS Service. Failure to connect means that the service is not running, the service is not bound to that port, or it is too busy to respond. By default it monitors TCP port 3300.

File Count: DBCache folder

This component monitor counts the number of files in a DBCache directory. This directory should be empty. An accumulation in this directory indicates that the database inserts (by the Log to database Action) is falling behind or failing.

If Kiwi Syslog Server is installed on a 64-bit machine, you should monitor this directory (this is set by default):
```
\\${IP}\c$\Program Files (x86)\Syslogd\DBCache
```

For x86 machine:
```
\\${IP}\c$\Program Files\Syslogd\DBCache
```

File Count: Mail queue folder

This component monitor counts the number of files in a mail queue directory. This directory should be empty. An accumulation in this directory indicates that the email queued to be delivered are falling behind or failing.

If Kiwi Syslog Server is installed on a 64-bit machine, you should monitor this directory (this is set by default):
```
\\${IP}\c$\Program Files (x86)\Syslogd\MailQ
```

For x86 machine:
```
\\${IP}\c$\Program Files\Syslogd\MailQ
```

Directory Size: Web Server Application Data Folder

This component monitor counts the size of the Web Server Application Data directory. The total size of this directory should not exceed 4 GB and should grow fairly slowly. The returned value is shown in MB.

If Kiwi Syslog Server is installed on a 64-bit machine, you should monitor this directory (this is set by default):
```
\\${IP}\c$\Program Files (x86)\SolarWinds\Kiwi Syslog Web Access\html\App_Data
```

For x86 machine:
```
\\${IP}\c$\Program Files\SolarWinds\Kiwi Syslog Web Access\html\App_Data
```
Squid

The following templates are available:

- Squid (Linux and Unix)
- Squid (Windows)
**Squid (Windows)**

This template allows you to monitor the performance of Squid proxy server installed on a Windows machine by using SNMP and PowerShell monitors.

**Prerequisites**

WinRM must be installed and properly configured on the target server. SNMP should be installed and configured on the target server. The Squid SNMP module must be configured on the target server:

By default, Squid uses UPD port 3401 for SNMP. You can change this port by using the `snmp_port` directive in `squid.conf` file.

The following configuration should be present in the `squid.conf` file:

```plaintext
acl Snmppublic snmp_community <your_community_string>acl APMhost src <IP_address_of_SAM_server> snmp_access allow APMhost Snmppublic
```

For example:

```plaintext
acl Snmppublic snmp_community public acl APMhost src snmp_access allow APMhost Snmppublic
```

After these changes are made, restart Squid.

**Credentials**

Administrator on the target server.

**Components**

This was tested on Squid 3 for Windows.

**Monitored Components**

For details on monitors, see [SAM Component Monitor Types](#).

**Storage Mem Size**

This monitor returns the amount of memory (in kilobytes) currently used to store in-memory objects.

OID: `1.3.6.1.4.1.3495.1.1.2.0`

**Storage Swap Size**

This monitor returns the amount of disk space (in kilobytes) currently used to store on-disk objects.

OID: `1.3.6.1.4.1.3495.1.1.2.0`
Page Faults

This monitor returns the number of page faults for the Squid process since it was started.
OID: 1.3.6.1.4.1.3495.1.3.1.1.0

HTTP Reads

This monitor returns the number of times this process called read( ) on HTTP sockets connected to origin servers and neighbor caches.
OID: 1.3.6.1.4.1.3495.1.3.1.2.0

Accounted Memory

This monitor returns the amount of memory allocated by the memory pooling routines. Not the same as the total memory used by Squid.
OID: 1.3.6.1.4.1.3495.1.3.1.3.0

CPU Usage (%)

This monitor returns the CPU utilization, as a percentage, since Squid was started.
OID: 1.3.6.1.4.1.3495.1.3.1.5.0

Stored Objects

This monitor returns the total number of objects currently in the cache.
OID: 1.3.6.1.4.1.3495.1.3.1.7.0

Available File Descriptors

This monitor returns the current number of available (unused) file descriptors.
OID: 1.3.6.1.4.1.3495.1.3.1.10.0

Reserved File Descriptors

This monitor returns the number of reserved file descriptors.
OID: 1.3.6.1.4.1.3495.1.3.1.11.0

HTTP Requests Received

This monitor returns the total number of HTTP requests received from cache clients.
OID: 1.3.6.1.4.1.3495.1.3.2.1.1.0

HTTP Hits

This monitor returns the number of client requests that were cache hits.
OID: 1.3.6.1.4.1.3495.1.3.2.1.2.0

HTTP Errors

This monitor returns the number of client requests that resulted in an error.
OID: 1.3.6.1.4.1.3495.1.3.2.1.3.0

HTTP Received (KB)
This monitor returns the amount of network traffic, in kilobytes, read from cache clients.
OID: 1.3.6.1.4.1.3495.1.3.2.1.4.0

HTTP Transmitted (KB)
This monitor returns the amount of network traffic, in kilobytes, written to cache clients.
OID: 1.3.6.1.4.1.3495.1.3.2.1.5.0

ICP Transmitted (KB)
This monitor returns the amount of network traffic, in kilobytes, used for ICP messages sent to neighbors, not including UDP and IP headers.
OID: 1.3.6.1.4.1.3495.1.3.2.1.8.0

ICP Received (KB)
This monitor returns the amount of network traffic, in kilobytes, used for ICP messages received from neighbors, not including UDP and IP headers.
OID: 1.3.6.1.4.1.3495.1.3.2.1.9.0

Requests From Clients
This monitor returns the number of requests forwarded to origin servers and neighbor caches.
OID: 1.3.6.1.4.1.3495.1.3.2.1.10.0

Errors For Client Requests
This monitor returns the number of errors received from origin servers and neighbor caches.
OID: 1.3.6.1.4.1.3495.1.3.2.1.11.0

Traffic Received From Servers (KB)
This monitor returns the amount of network traffic, in kilobytes, read from origin servers and neighbor caches.
OID: 1.3.6.1.4.1.3495.1.3.2.1.12.0

Traffic Sent To Servers (KB)
This monitor returns the amount of network traffic, in kilobytes, written to origin servers and neighbor caches.
OID: 1.3.6.1.4.1.3495.1.3.2.1.13.0

Clients
This monitor returns the number of clients that sent HTTP requests to Squid since it was started.
OID: 1.3.6.1.4.1.3495.1.3.2.1.15.0

**IP Cache Requests**
This monitor returns the number of requests received by Squid's IP cache. If the ratio of hits to requests is less than 60-75%, you may want to increase the size of your IP cache.

OID: 1.3.6.1.4.1.3495.1.4.1.2.0

**IP Cache Hits**
This monitor returns the number of lookups that were hits in the IP cache. If the ratio of hits to requests is less than 60-75%, you may want to increase the size of your IP cache.

OID: 1.3.6.1.4.1.3495.1.4.1.3.0

**IP Cache Negative Hits**
This monitor returns the number of lookups that were negative hits in the IP cache. Certain failed queries may be negatively cached for an amount of time determined by the negative_dns_ttl directive.

OID: 1.3.6.1.4.1.3495.1.4.1.5.0

**IP Cache Misses**
This monitor returns the number of IP cache misses.

OID: 1.3.6.1.4.1.3495.1.4.1.6.0

**FQDN Cache Requests**
This monitor returns the number of requests to the FQDN cache.

OID: 1.3.6.1.4.1.3495.1.4.2.2.0

**FQDN Cache Hits**
This monitor returns the number of FQDN cache requests satisfied as hits.

OID: 1.3.6.1.4.1.3495.1.4.2.3.0

**FQDN Cache Negative Hits**
This monitor returns the number of FQDN requests satisfied as negative cache hits.

OID: 1.3.6.1.4.1.3495.1.4.2.5.0

**FQDN Cache Misses**
This monitor returns the number of FQDN cache misses.

OID: 1.3.6.1.4.1.3495.1.4.2.6.0

**External DNS Server Requests**
This monitor returns the number of DNS queries made by Squid. This counter is reset each time you reconfigure the running Squid process.
External DNS Server Replies

This monitor returns the number of DNS replies received by Squid. This counter is reset each time you reconfigure the running Squid process.

OID: 1.3.6.1.4.1.3495.1.4.3.2.0

External DNS Server Processes

For internal DNS (the default) this monitor reports the number of nameservers that Squid knows about. For external DNS, it reports the number of (running) dnsserver helper processes.

OID: 1.3.6.1.4.1.3495.1.4.3.3.0

Squid HTTP Port Monitor

This component monitor tests the ability of a Squid service to accept incoming sessions. By default it monitors 3128 TCP port.

Top 10 Active Sites

This monitor returns the top 10 of the most visited sites for specific proxy client.

- You must specify the correct arguments for this component in the Script Arguments field. This PowerShell monitor uses the following argument structure: IP_address,Path_to_logfile,Time
  1. IP_address – This is the IP address of the computer that uses the target squid server as a proxy server. This argument allows SAM to monitor specific proxy clients.
  2. Path_to_logfile – This is the full path to the squid access.log file. For example: 192.168.2.211,c:squid\var\logs\access.log,week
  3. Time – This argument allows the user to get statistics during the last minute/hour/day/month/year. For example: If you set Day, you will get the statistics for the last day. Possible values: Minute, Hour, Day, Week, Month, Year. By default, this value it set to Week.

Due to the specific way of determining the statistic, there is an issue with showing sites with the “-” symbol in its names. For example: “www.some-site.com”, in the message field we will only receive everything before the dash, as in “www.some”.

Top 10 Blocked Sites

This monitor returns the top 10 most blocked sites which the proxy client tried to open.

- You must specify the correct arguments for this component in the Script Arguments field. This PowerShell monitor uses the following argument structure: IP_address,Path_to_logfile,Time
1. **IP_address** – This is the IP address of the computer that uses the target squid server as a proxy server. This argument allows SAM to monitor specific proxy clients.

2. **Path_to_logfile** – This is the full path to the squid access.log file. 
   For example: 192.168.2.211, c:squid\var\logs\access.log, week

3. **Time** – This argument allows the user to get statistics during the last minute/hour/day/week/month/year. 
   For example: If you set Day, you will get the statistics for the last day. 
   Possible values: Minute, Hour, Day, Week, Month, Year. By default, this value it set to Week.

Due to the specific way of determining the statistic, there is an issue with showing sites with the “-” symbol in its names. For example: “www.some-site.com”, in the message field will only receive everything before the dash, as in “www.some”.

**Traffic Statistic**

This monitor returns the total amount of download and upload traffic in MB for a specific proxy client.

You must specify the correct arguments for this component in the Script Arguments field. This PowerShell monitor uses the following argument structure: **IP_address, Path_to_logfile, Time**

1. **IP_address** – This is the IP address of the computer that uses the target squid server as a proxy server. This argument allows SAM to monitor specific proxy clients.

2. **Path_to_logfile** – This is the full path to the squid access.log file. 
   For Example: 192.168.2.211, c:squid\var\logs\access.log, week

3. **Time** – This argument allows the user to get statistics during the last minute/hour/day/week/month/year. 
   For example: If you set Day, you will get the statistics for the last day. 
   Possible values: Minute, Hour, Day, Week, Month, Year. By default, this value it set to Week.

**Process: Squid**

This monitor returns the CPU and memory usage of the Squid process.
Squid (Linux and Unix)

This template allows you to monitor the performance of a Squid proxy server installed on a Linux/Unix machine by using SNMP monitors and Perl scripts. You can use the Orion agent for Linux or SNMP agentless to monitor.

Prerequisites for Orion agent for Linux

SSH and Perl must be installed and properly configured on the target server. SNMP should be installed and configured for monitoring squid process on target server. Squid SNMP module must be configured on target server:

On Linux/Unix, to enable the SNMP module on Squid, you should use the --enable-snmp option when running ./configure and recompile Squid. Starting from version 3, it should be enabled by default.

For SNMP, Squid uses UDP port 3401 by default. You can change this port by using the snmp_port directive in the squid.conf file.

The following configuration should be present in the squid.conf file:

```
acl Snmppublic snmp_community <your_community_string> acl APMhost src <IP_address_of_SAM_server> snmp_access allow APMhost Snmppublic
```

For example:

```
acl Snmppublic snmp_community public acl APMhost src 192.168.2.3 snmp_access allow APMhost Snmppublic
```

After these changes are made, restart Squid.

For further information on configuring SNMP with the Orion agent for Linux, see SNMP for agents.

Credentials

Root on the target server.

Tested on Squid 3.1 for Linux/Unix.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Storage Mem Size

This monitor returns the amount of memory (in kilobytes) currently used to store in-memory objects.

OID: 1.3.6.1.4.1.3495.1.1.2.0

Storage Swap Size

This monitor returns the amount of disk space (in kilobytes) currently used to store on-disk objects.
OID: 1.3.6.1.4.1.3495.1.1.2.0

Page Faults
This monitor returns the number of page faults for the Squid process since it was started.
OID: 1.3.6.1.4.1.3495.1.3.1.1.0

HTTP Reads
This monitor returns the number of times this process called read() on HTTP sockets connected to origin servers and neighbor caches.
OID: 1.3.6.1.4.1.3495.1.3.1.2.0

Accounted Memory
This monitor returns the amount of memory allocated by the memory pooling routines. Not the same as the total memory used by Squid.
OID: 1.3.6.1.4.1.3495.1.3.1.3.0

CPU Usage (%)
This monitor returns the CPU utilization, as a percentage, since Squid was started.
OID: 1.3.6.1.4.1.3495.1.3.1.5.0

Stored Objects
This monitor returns the total number of objects currently in the cache.
OID: 1.3.6.1.4.1.3495.1.3.1.7.0

Available File Descriptors
This monitor returns the current number of available (unused) file descriptors.
OID: 1.3.6.1.4.1.3495.1.3.1.10.0

Reserved File Descriptors
This monitor returns the number of reserved file descriptors.
OID: 1.3.6.1.4.1.3495.1.3.1.11.0

HTTP Requests Received
This monitor returns the total number of HTTP requests received from cache clients.
OID: 1.3.6.1.4.1.3495.1.3.2.1.1.0

HTTP Hits
This monitor returns the number of client requests that were cache hits.
OID: 1.3.6.1.4.1.3495.1.3.2.1.2.0

HTTP Errors
This monitor returns the number of client requests that resulted in an error.
OID: 1.3.6.1.4.1.3495.1.3.2.1.3.0

HTTP Received (KB)
This monitor returns the amount of network traffic, in kilobytes, read from cache clients.
OID: 1.3.6.1.4.1.3495.1.3.2.1.4.0

HTTP Transmitted (KB)
This monitor returns the amount of network traffic, in kilobytes, written to cache clients.
OID: 1.3.6.1.4.1.3495.1.3.2.1.5.0

ICP Transmitted (KB)
This monitor returns the amount of network traffic, in kilobytes, used for ICP messages sent to neighbors, not including UDP and IP headers.
OID: 1.3.6.1.4.1.3495.1.3.2.1.8.0

ICP Received (KB)
This monitor returns the amount of network traffic, in kilobytes, used for ICP messages received from neighbors, not including UDP and IP headers.
OID: 1.3.6.1.4.1.3495.1.3.2.1.9.0

Requests From Clients
This monitor returns the number of requests forwarded to origin servers and neighbor caches.
OID: 1.3.6.1.4.1.3495.1.3.2.1.10.0

Errors For Client Requests
This monitor returns the number of errors received from origin servers and neighbor caches.
OID: 1.3.6.1.4.1.3495.1.3.2.1.11.0

Traffic Received From Servers (KB)
This monitor returns the amount of network traffic, in kilobytes, read from origin servers and neighbor caches.
OID: 1.3.6.1.4.1.3495.1.3.2.1.12.0

Traffic Sent To Servers (KB)
This monitor returns the amount of network traffic, in kilobytes, written to origin servers and neighbor caches.
OID: 1.3.6.1.4.1.3495.1.3.2.1.13.0

Clients
This monitor returns the number of clients that sent HTTP requests to Squid since it was started.
OID: 1.3.6.1.4.1.3495.1.3.2.1.15.0
IP Cache Requests

This monitor returns the number of requests received by Squid’s IP cache. If the ratio of hits to requests is less than 60-75%, you may want to increase the size of your IP cache.

OID: 1.3.6.1.4.1.3495.1.4.1.2.0

IP Cache Hits

This monitor returns the number of lookups that were hits in the IP cache. If the ratio of hits to requests is less than 60-75%, you may want to increase the size of your IP cache.

OID: 1.3.6.1.4.1.3495.1.4.1.3.0

IP Cache Negative Hits

This monitor returns the number of lookups that were negative hits in the IP cache. Certain failed queries may be negatively cached for an amount of time determined by the negative_dns_ttl directive.

OID: 1.3.6.1.4.1.3495.1.4.1.5.0

IP Cache Misses

This monitor returns the number of IP cache misses.

OID: 1.3.6.1.4.1.3495.1.4.1.6.0

FQDN Cache Requests

This monitor returns the number of requests to the FQDN cache.

OID: 1.3.6.1.4.1.3495.1.4.2.2.0

FQDN Cache Hits

This monitor returns the number of FQDN cache requests satisfied as hits.

OID: 1.3.6.1.4.1.3495.1.4.2.3.0

FQDN Cache Negative Hits

This monitor returns the number of FQDN requests satisfied as negative cache hits.

OID: 1.3.6.1.4.1.3495.1.4.2.5.0

FQDN Cache Misses

This monitor returns the number of FQDN cache misses.

OID: 1.3.6.1.4.1.3495.1.4.2.6.0

External DNS Server Requests

This monitor returns the number of DNS queries made by Squid. This counter is reset each time you reconfigure the running Squid process.

OID: 1.3.6.1.4.1.3495.1.4.3.1.0
**External DNS Server Replies**

This monitor returns the number of DNS replies received by Squid. This counter is reset each time you reconfigure the running Squid process.

OID: 1.3.6.1.4.1.3495.1.4.3.2.0

**External DNS Server Processes**

For internal DNS (the default) this monitor reports the number of nameservers that Squid knows about. For external DNS, it reports the number of (running) dnsserver helper processes.

OID: 1.3.6.1.4.1.3495.1.4.3.3.0

**Squid HTTP Port Monitor**

This component monitor tests the ability of a Squid service to accept incoming sessions. By default it monitors 3128 TCP port.

**Top 10 Active Sites**

This monitor returns the top 10 of the most visited sites for specific proxy client.

ℹ️ You must specify the correct arguments for this component in the Script Arguments field. This monitor uses the following argument structure:

```perl
perl ${SCRIPT} IP_address Path_to_logfile Time
```

1. **IP_address** – This is the IP address of the computer that uses the target squid server as a proxy server. This argument allows SAM to monitor specific proxy clients.

2. **Path_to_logfile** – This is the full path to the squid access.log file.

3. **Time** – This argument allows a user to get the statistics during the last minute/hour/day/week/month/year.

   **For example:** if you set Day, you will get the statistic for the last day.

   Possible values: Minute, Hour, Day, Week, Month, Year. By default, this is set to Week.

   **For Example:**

   ```perl
   perl ${SCRIPT} 192.168.2.211 /var/log/squid/access.log week
   ```

   ℹ️ On some machines (Solaris, HP-UX, etc.), this component may not work because SAM cannot copy all of the script to the target server. You should manually copy this script to the target machine. Next, you should change the Script Arguments field by changing `${SCRIPT}` to the scripts path. For example: `perl /tmp/top10active.pl 192.168.2.211 /var/log/squid/access.log week`

**Top 10 Blocked Sites**

This monitor returns the top 10 blocked sites which the proxy client tried to open.
You must specify the correct arguments for this component in the Script Arguments field. This monitor uses the following argument structure:

```
perl ${SCRIPT} IP_address Path_to_logfile Time
```

1. **IP_address** – This is the IP address of the computer that uses the target squid server as a proxy server. This argument allows SAM to monitor specific proxy clients.

2. **Path_to_logfile** – This is the full path to the squid access.log file.

3. **Time** – This argument allows the user to get statistics during the last minute/hour/day/week/month/year.

   For example: If you set Day, you will get the statistic for the last day.

   Possible values: Minute, Hour, Day, Week, Month, Year. By default, this is set to Week.

   For Example:

   ```
   perl ${SCRIPT} 192.168.2.211 /var/log/squid/access.log week
   ```

**Traffic Statistic**

This monitor returns the total download and upload amount of traffic in MB for specific proxy client.

You must specify the correct arguments for this component in the Script Arguments field. This monitor uses the following argument structure:

```
perl ${SCRIPT} IP_address Path_to_logfile Time
```

1. **IP_address** – This is the IP address of computer that uses the target squid server as a proxy server. This argument allows SAM to monitor specific proxy clients.

2. **Path_to_logfile** – This is the full path to the squid access.log file.

3. **Time** – This argument allows a user to get statistics during the last minute/hour/day/week/month/year.

   For example: If you set Day, you will get the statistic for the last day.

   Possible values: Minute, Hour, Day, Week, Month, Year. By default, this is set to Week.

   For Example:

   ```
   perl ${SCRIPT} 192.168.2.211 /var/log/squid/access.log week
   ```
On some machines (Solaris, HP-UX, etc.), this component may not work because SAM cannot copy all of the script to the target server. You should manually copy this script to the target machine. Next, you should change the Script Arguments field by changing $\{\text{SCRIPT}\}$ to the scripts path. For example: perl /tmp/squid_traffic.pl 192.168.2.211 /var/log/squid/access.log week

**Process: squid**

This monitor returns the CPU and memory usage of the Squid process.
SSL Certificate Expiration Date Monitor

This template tests a web server's ability to accept incoming sessions over a secure channel and then test the security certificate's expiration date.

Prerequisites

None.

Credentials:

None.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

SSL Certificate Expiration Date Monitor

This component monitor tests a web server's ability to accept incoming sessions over a secure channel and then test the security certificate's expiration date.

By default, this monitor tests TCP port 443.

More information about this monitor can be found at SSL Certificate Expiration Date Monitor.
Streaming Media Services 2008

This template assesses the overall health of Streaming Media Services 2008 services and counters. It is recommended to use this template in conjunction with the Windows Server 2003-2008 Services and Counters template.

Prerequisites

RPC and WMI access to the domain controller.
For more information, see Monitors and templates using WMI.

Credentials

Windows Administrator on the domain controller.

For more information on how to optimize Windows Media Services, refer to the following article: http://www.microsoft.com/windows/windowsmedia/howto/articles/optimize_web.aspx#appendix_f.

Monitored Components

Components without predetermined threshold values provide guidance such as "Use the lowest threshold possible" or "Use the highest threshold possible" to help you find a threshold appropriate for your application.

Current Cache Downloads

This component monitor returns the number of concurrent streams being downloaded to the memory area of the cache/proxy server.

Current Connected Players

This component monitor returns the current number of players with unicast connections to the server. This number does not include distribution server connections.

Current Connection Queue Length

This component monitor returns the current number of connection requests that are pending on the server from both player and distribution servers. This value should be as low as possible.

Current Connection Rate

This component monitor returns the current number of clients per second that are connecting to the server.
Current File Read Rate (Kbps)
This component monitor returns the current rate, in kilobits per second (Kbps), at which data packets are read from a file.

Current Incoming Bandwidth (Kbps)
This component monitor returns the current bandwidth, in Kbps, allocated for streams from other servers.

Current Late Read Rate
This counter returns the current number of data packets per second that take longer than 400 milliseconds to read from the file system.

The value for this monitor should not be higher than zero for an extended period of time. If it is, this may indicate that the WMS server is not able to read from its data sources fast enough.

Current Late Send Rate
This component monitor returns the current number of packets that are sent out 0.5 seconds, or more, after the marked send time.

Current Outgoing Distribution Allocated Bandwidth (Kbps)
This component monitor returns the current bandwidth, in Kbps, allocated for streams to distribution servers.

Current Outgoing Distribution Connections
This component monitor returns the current number of distribution servers that are connected to the server.

Current Outgoing Distribution Send Rate (Kbps)
This component monitor returns the current rate, in Kbps, at which data packets are being streamed to distribution servers.

Current Player Allocated Bandwidth (Kbps)
This component monitor returns the current amount of bandwidth, in Kbps, that is allocated for all streams to players.

Current Player Send Rate (Kbps)
This component monitor returns the current rate, in Kbps, at which data packets are being streamed to players.

If the send rate continuously drops below the allocated bandwidth, WMS will be unable to service all the clients. This may indicate an outbound network bottleneck.

Current Stream Error Rate
This component monitor returns the current number of errors per second due to dropped packets.

If this value is higher than zero for an extended period of time, this may indicate that the WMS server is unable to keep up with the demand. This also may indicate late reads.
Current Streaming HTTP Players

This component monitor returns the current number of players that are being streamed through the HTTP protocol. This does not include players that are stopped or paused.

Current Streaming MMS Players

This component monitor returns the current number of players that are being streamed through the MMS protocol. This does not include players that are stopped or paused.

Current Streaming Players

This component monitor returns the current number of players that are being streamed across all protocols. This does not include players that are stopped or paused.

Current Streaming RTSP Players

This component monitor returns the current number of players that are being streamed through the RTSP protocol. This does not include players that are stopped or paused.

Current Streaming UDP Players

This component monitor returns the current number of players that are being streamed through the UDP transport protocol. This does not include players that are stopped or paused.

Current UDP Resend Requests Rate

This component monitor returns the current number of requests for UDP resends per second received from clients.

Current UDP Resends Sent Rate

This component monitor returns the current number of UDP resends per second that are sent to clients.

Service: Windows Media Services

This component monitor returns a status of up or down. This enables you to manage delivery of live or on-demand digital media content, including Windows Media Audio (WMA) and Windows Media Video (WMV), over networks by using administrative interfaces in Microsoft Windows Media Services 2008.

Total Advertisements

This counter returns the total number of advertisements that have been streamed from playlists since the last time the counter was reset.

Total Connected Players

This counter returns the total number of players that have connected to the server since the last time the counter was reset.

Total Late Reads

This counter returns the total number of times that the server required more than 400 milliseconds to read data from the file system since the last time the counter was reset.
Total Late Sends
This counter returns the total number of times the server sent out data packets, 0.5 seconds or more after the marked send time since the last time the counter was reset.

Total Outgoing Distribution Connections
This counter returns the total number of distribution servers that have connected to the server or publishing point since the last time the counter was reset.

Total Server Uptime (s)
This counter returns the elapsed time, in seconds, that the Windows Media Services service has been running since it was last started.

Total Stream Denials
This counter returns the total number of times the server refused to send a requested stream to a client since the last time the counter was reset. This includes denials that occurred due to authorization/authentication failure as well as denials that occurred because limits were exceeded.

Total Stream Errors
This counter returns the total number of stream errors due to dropped packets since the last time the counter was reset.

Total Streaming HTTP Players
This counter returns the total number of players that have streamed data through the HTTP protocol since the last time the counter was reset.

Total Streaming Players
This counter returns the total number of players that have streamed data since the last time the counter was reset.

Total Streaming RTSP Players
This counter returns the total number of players that have streamed data through the RTSP protocol since the last time the counter was reset.

Total Streaming UDP Players
This counter returns the total number of players that have streamed data through the UDP transport protocol since the last time the counter was reset.
Sybase

The following templates are available:

- Sybase ASE
- Sybase SQL Anywhere
Sybase ASE

This template assesses the performance of the Sybase ASE database by retrieving performance data from the monitoring tables.

Prerequisites

Sybase ASE 15.0. Sybase ASE ODBC must be installed on the SAM server. (Instructions can be found on the Sybase ASE installation media.) Complete the following before using this template:

1. Database user must have mon_role role.
2. The database server should have the following options enabled:
   - Enable monitoring
   - Wait event timing
   - Object lockwait timing
   - Statement statistic active
   - Per object statistic active
   - Statement pipe active
   - Statement pipe max messages
   - SQL batch capture
   - SQL text pipe active
   - SQL text pipe max messages

More information on how to enable these options can be found here: http://www.sypron.nl/mda.html.

3. The database server and the ODBC driver on the SAM server should use the same character set. If you receive the following error: "Could not load code page for requested charset," inspect what character set is used by the client by default by looking in SYBASE_PATH\locales\locales.dat. Also, look at which character set is used by the database server. More information about character sets can be found here: http://infocenter.sybase.com/help/index.jsp?topic=/com.sybase.help.ase_15.0.sag1/html/sag1/sag1462.htm.

4. Check the monitor tables installed on the database server by running the following command:
   
   SELECT * FROM monTables
   
   If the query returns an error, examine this error for troubleshooting clues. If monitor tables are not installed, you should manually install them. Installation instructions can be found here: http://infocenter.sybase.com/help/index.jsp?topic=/com.sybase.dc20022_1251/html/monitoring/monitoring33.htm.

Credentials

Database user name and password.
Monitored Components

For details on monitors, see [SAM Component Monitor Types](#).

Components without predetermined threshold values provide guidance such as "Use the lowest threshold possible" or "Use the highest threshold possible" to help you find a threshold appropriate for your application.

**Transactions/sec**

This component monitor returns the transactions rate, per second.

**Days Running**

This component monitor returns the number of days the Adaptive Server has been running.

**Deadlocks**

This component monitor returns the total number of deadlocks that have occurred. This number should be as low as possible.

**Active Connections**

This component monitor returns the number of active inbound connections.

**Lock Waits**

This component monitor returns the number of processes that have waited longer than LockWaitThreshold seconds (10 seconds by default).

**Lock Waits/sec**

This component monitor returns the lock waits rate, per second.

**Currently Opened Databases**

This component monitor returns the number of currently opened databases.

**Active Worker Processes**

This component monitor returns the number of active worker processes.

**Memory Used by Worker Process (kb)**

This component monitor returns the amount of memory, in kilobytes, currently in use by worker processes.

**Memory Used by Cache (kb)**

This component monitor returns the number of kilobytes of the cache the object is occupying.

**Active Processes**

This component monitor returns the number of currently active processes.
**Specific Database Used Space (MB)**

This component monitor returns the used size, in MB, for the specified database.

1. By default, this monitor returns the value for the master database. To change the database, replace "master" with your database name in the following SQL query:
   
   ```sql
   select @dbn = 'master'
   ```

**Specific Database Free Space (MB)**

This component monitor returns the available space, in MB, for the specified database.

1. By default, this monitor returns the value for the master database. To change the database, replace "master" with your database name in the following SQL query:
   
   ```sql
   select @dbn = 'master'
   ```

**Total Databases Size (MB)**

This component monitor returns the total size of all databases, in MB.

**Requests/sec**

This component monitor returns the rate of stored procedures requested per second.

**Procedure Cache Hit Ratio (%)**

This component monitor returns the procedure cache hit ratio. This value should be as high as possible.

**Cache Hit Ratio (%)**

This component monitor returns the percentage of times a requested data page has been found in the data cache. A cache hit ratio of 97% or less could indicate memory starvation. If this becomes a continual issue, allocate more memory to the data cache.

**Writes/sec**

This component monitor returns the number of buffers written from the cache to the disk.
Sybase SQL Anywhere

This template assesses the performance of the server database by retrieving performance data from the monitoring tables.

Prerequisites

Sybase SQL Anywhere Administrative Tools must be installed on the APM server, (Administrative Tools can be found on installation media during installation process).

Credentials

Database user name and password with DBA authorities.

Before using this template you should put correct database name (DBN property) in Connection String.
Example: Driver={SQL Anywhere 12};DBN=demo;Host=${IP};Uid=${USER};Pwd=${PASSWORD};

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Components without predetermined threshold values provide guidance such as "Use the lowest threshold possible" or "Use the highest threshold possible" to help you find a threshold appropriate for your application.

CPU usage (s)

This monitor returns the CPU usage for the database server process. Values are in seconds. The value returned for this property is cumulative since the database server was started.

Current Cache Size (kB)

This monitor returns the current cache size, in kilobytes.

Main Heap Pages

This monitor returns the number of pages used for global server data structures.

Pinned Cache Pages

This monitor returns the number of pinned cache pages.

Dirty Cache Pages

This monitor returns the number of cache pages that are dirty (needing a write).

Replaced Pages in Cache

This monitor returns the number of pages in the cache that have been replaced.
Disk Reads
This monitor returns the number of disk reads.

Free Space in System Dbspace (MB)
This monitor returns the amount of free disk space for System dbspace in MB.

Free Space in Translog Dbspace (MB)
This monitor returns the amount of free disk space for Translog dbspace in MB.

Free Space in Temporary Dbspace (MB)
This monitor returns the amount of free disk space for Translog dbspace in MB.

Current Connections
This monitor returns count of the number of licensed connections in use.

Unique Connections
This monitor returns the number of unique client network addresses connected to a network database server.

Open HTTP Connections
This monitor returns the number of HTTP connections that are currently open within the database server. They may be actively processing a request or waiting in a queue of long lived (keep-alive) connections.

Actively Processing HTTP Connections
This monitor returns the number of HTTP connections that are actively processing an HTTP request. An HTTP connection that has sent its response is not included.

Open HTTPS Connections
This monitor returns the number of HTTPS connections that are currently open within the database server. They may be actively processing a request or waiting in a queue of long lived (keep-alive) connections.

Actively Processing HTTPS Connections
This monitor returns the number of secure HTTPS connections that are actively processing an HTTPS request. An HTTPS connection that has sent its response is not included.

Requests in Queue
This monitor returns the number of requests that are currently queued up waiting for an available server thread. Returned value should be less than 5.
Bytes Received

This monitor returns the number of bytes received during client/server communications. This value is updated for HTTP and HTTPS connections.

- By default, this monitor has the Count statistic as difference box checked. It will only show the new statistic since the last polling period.

Bytes Sent

This monitor returns the number of bytes sent during client/server communications. This value is updated for HTTP and HTTPS connections.

- By default, this monitor has the Count statistic as difference box checked. It will only show the new statistic since the last polling period.

Optimized Queries

This monitor returns the number of requests fully optimized.

- By default, this monitor has the Count statistic as difference box checked. It will only show the new statistic since the last polling period.

Reused Queries

This monitor returns the number of reused query plans.

- By default, this monitor has the Count statistic as difference box checked. It will only show the new statistic since the last polling period.

Bypassed Queries

This monitor returns the number of requests reused from the plan cache.

- By default, this monitor has the Count statistic as difference box checked. It will only show the new statistic since the last polling period.

Cache Hits

This monitor returns the number of database page lookups satisfied by finding the page in the cache.

- By default, this monitor has the Count statistic as difference box checked. It will only show the new statistic since the last polling period.

File Reads

This monitor returns the current number of file reads those were issued by the server, but haven't yet completed.

- By default, this monitor has the Count statistic as difference box checked. It will only
show the new statistic since the last polling period.

**File Writes**

This monitor returns the current number of file writes those were issued by the server, but haven't yet completed.

By default, this monitor has the Count statistic as difference box checked. It will only show the new statistic since the last polling period.

**Pages Read from Disk**

This monitor returns the number of pages that have been read from disk.

By default, this monitor has the Count statistic as difference box checked. It will only show the new statistic since the last polling period.

**Pages Written to Disk**

This monitor returns the number of modified pages that have been written to disk.

By default, this monitor has the Count statistic as difference box checked. It will only show the new statistic since the last polling period.

**Free Pages in System Dbspace**

This monitor returns the number of free pages in the system dbspace. The FreePages property is only supported on databases created with version 8.0.0 or later.

**Locks**

This monitor returns the number of locks held by the database.
Symantec

The following templates are available:

- Symantec Backup Exec Remote Agent
- Symantec Backup Exec Server
- Symantec Endpoint Protection Client
- Symantec Endpoint Protection Server
- Symantec NetBackup Client
- Symantec NetBackup Server
Symantec Backup Exec Remote Agent

This template assesses the status and overall performance of a Symantec Backup Exec Remote Agent.

This template was created on Backup Exec version 13.0 R3, SP1.

Prerequisites:

WMI access to the target server.

Credentials:

Administrator on target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

You need to set thresholds for counters according to your environment. It is recommended to monitor counters for some period of time to understand potential value ranges and then set the thresholds accordingly. All Windows event monitors should return zero.

Service: Backup Exec Error Recording Service

This monitor returns CPU and memory usage of the Error Recording service.

Service: Backup Exec Remote Agent for Windows Systems

This monitor returns CPU and memory usage of the Remote Agent service. This service provides Backup and Restore services to Backup Exec.

TCP Port: Remote Agent

This component monitor tests the ability of the Remote Agent service to accept incoming sessions. By default, TCP port 10000 is monitored.

Event: Port conflict

This monitor returns the number of events when the Backup Exec Remote Agent for Windows Servers service did not start because TCP/IP port 10000 is already in use

Type of event: Error. Event ID: 58116.

Ensure that no other TCP/IP application is using port 10000.

Event: Port listen failed

This monitor returns the number of events when the Backup Exec Remote Agent for Windows Systems service did not start. The application failed to listen on the NDMP TCP/IP port

Type of event: Error. Event ID: 58117.

Check the network configuration.
Symantec Backup Exec Server

This template assesses the status and overall performance of a Symantec Backup Exec Server.

This template was created on Backup Exec version 13.0 R3, SP1.

Prerequisites

WMI access to the target server.

Credentials

Administrator on target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

You need to set thresholds for counters according to your environment. It is recommended to monitor counters for some period of time to understand potential value ranges and then set the thresholds accordingly. All Windows event monitors should return zero.

Service: Backup Exec Agent Browser

This monitor returns CPU and memory usage of the Agent Browser service. This service allows the Backup Exec job engine to discover the Backup Exec agents that are available on the network.

Service: Backup Exec Device and Media Service

This monitor returns CPU and memory usage of the Device and Media service. This service provides several COM server interfaces for managing and accessing devices and media.

Service: Backup Exec Error Recording Service

This monitor returns CPU and memory usage of the Error Recording service.

Service: Backup Exec Job Engine

This monitor returns CPU and memory usage of the Job Engine service. This service receives job requests from the Backup Exec Server and moves data to the specified media.

Service: Backup Exec Remote Agent for Windows Systems

This monitor returns CPU and memory usage of the Remote Agent service. This service provides Backup and Restore services to Backup Exec.

Service: Backup Exec Server

This monitor returns CPU and memory usage of the Backup Exec Server service. This service implements job scheduling, server configuration, job definitions, job history, and the Backup Exec Management SDK.
Engine: Aborted Jobs

This monitor returns the number of jobs that have been aborted since the Backup Exec Engine Service last started. The returned value should be as low as possible.

* By default, this monitor has the Count statistic as difference box checked, so it will return value between polling cycles.

Engine: Backup Job Count

This monitor returns the number of backup jobs that have been run since the Backup Exec Engine Service last started.

* By default, this monitor has the Count statistic as difference box checked, so it will return value between polling cycles.

Engine: Differential Job Count

This monitor returns the number of differential backup jobs that have been run since the Backup Exec Engine Service last started.

* By default, this monitor has the Count statistic as difference box checked, so it will return value between polling cycles.

Engine: Error Skipped Objects

This monitor returns the number of objects that have been skipped because there was an error opening the object during backup since the Backup Exec Engine Service last started. The returned value should be zero at all times.

* By default, this monitor has the Count statistic as difference box checked, so it will return value between polling cycles.

Engine: Failed Jobs

This monitor returns the number of jobs that have failed since the Backup Exec Engine Service last started. The returned value should be zero at all times.

* By default, this monitor has the Count statistic as difference box checked, so it will return value between polling cycles.

Engine: Failed Verify Objects

This monitor returns the number of objects that failed to verify during verify operations since the Backup Exec Engine Service last started. The returned value should be zero at all times.

* By default, this monitor has the Count statistic as difference box checked, so it will return value between polling cycles.
Engine: In Use Skipped Objects
This monitor returns the number of objects that have been skipped because they were in use during backup since the Backup Exec Engine Service last started.

By default, this monitor has the Count statistic as difference box checked, so it will return value between polling cycles.

Engine: Incremental Job Count
This monitor returns the number of incremental backup jobs that have been run since the Backup Exec Engine Service last started.

By default, this monitor has the Count statistic as difference box checked, so it will return value between polling cycles.

Engine: Normal Job Count
This monitor returns the number of normal backup jobs that have been run since the Backup Exec Engine Service last started.

By default, this monitor has the Count statistic as difference box checked, so it will return value between polling cycles.

Engine: Successful Jobs
This monitor returns the number of jobs that have completed successfully since the Backup Exec Engine Service last started.

By default, this monitor has the Count statistic as difference box checked, so it will return value between polling cycles.

Server: Active Job Count
This monitor returns the number of jobs that are currently active.

Server: Ready Job Count
This monitor returns the number of jobs that are ready and waiting for dispatch.

Server: Acknowledged Message Count
This monitor returns the number of messages acknowledged by the message queue.

Server: Acknowledged Message/sec
This monitor returns the number of messages acknowledged by the message queue per second.

Server: Active Message Count
This monitor returns the number of active messages in the message queue.

Server: Received Bytes/sec
This monitor returns the number of bytes received by the message queue per second.
Server: Received Message/sec

This monitor returns the number of messages received by the message queue per second.

Server: Sent Bytes/sec

This monitor returns the number of bytes sent out by the message queue per second.

Server: Sent Message/sec

This monitor returns the number of messages sent by the message queue per second.

Server: Currently Queued Work Items

This monitor returns the number of work items currently queued to the general thread pool.

Server: Active VSN Count

This monitor returns the number of simple notification messages currently being handled by the server.

Backup events

This monitor returns the number of events that occur when:

- There is an ODBC access error, possible lost connection to database, or unsuccessful access to the catalog index in the database;
- There is an error copying the machine specific Intelligent Disaster Recovery information to an alternate data path.

**Type of event:** Error. Event ID: 34338, 57751.

Check your network connections. Check the status of your database. Check the event log for other error messages. Ensure the remote agent service is running on the target server.

Job events

This monitor returns the number of events that occur when:

- The job was canceled;
- The job failed with an error;
- The Symantec ThreatCon Level is not up-to-date.

**Type of event:** Error and Warning. Event ID: 34114, 34113, 33919.

If the job was canceled, review the job log for details. The job may be canceled for various reasons.

If the job failed, you should look at this event in Event Viewer and determine what error occurred.

Device events

This monitor returns the number of events that occur when:

- There are different device errors;
- The dismount operation was canceled.

**Type of event:** Error and Warning. Event ID: 58053, 59054.
For canceled dismount operations, you should manually remove the media from the drive and then unpause the drive.

**Media events**

This monitor returns the number of events that occur when:

- The Backup-to-Disk device is offline;
- The Backup-to-Disk device is out of free space.

**Type of event:** Error and Warning. Event ID: 58057, 58058.

The first alert occurred because the server could not access the Backup-to-Disk device. This is typically caused by the folder becoming inaccessible due to it being deleted, renamed, or unshared. It may also be caused by a disk full condition or the folder state has been set to offline.

The second alert reported because the disk volume where the Backup-to-Disk device resides is out of free space. Either create additional free space on the disk volume where this Backup-to-Disk folder resides, or go to the Job Monitor and cancel the job. Media Overwrite Protection settings should also be reviewed and set to an appropriate level of retention.

**Tape events**

This monitor returns the number of different Tape events.

**Type of event:** Error and Warning. Event ID: 65314, 65313.

Look for details in the Event Viewer.

**Server and service events**

This monitor returns the number of events related with:

- Backup Exec Name Service failures;
- Database maintenance failures;
- Failed to initialize objects;
- Schema version mismatch.

**Type of event:** Error. Event ID: 34338, 57751.

For Backup Exec Name Service and database maintenance failures, look for details in the Event Viewer.

For Failed To Initialize Objects events, restart all Backup Exec services, reboot the Backup Exec Media Server and then ensure the latest Backup Exec patches and service packs have been installed.

**TCP Port: Agent Browser**

This component monitor tests the ability of the Agent Browser service to accept incoming sessions. By default, TCP port 6101 is monitored.

**TCP Port: Job Engine**

This component monitor tests the ability of the Job Engine service to accept incoming sessions. By default, TCP port 5633 is monitored.
**TCP Port: Remote Agent**

This component monitor tests the ability of the Remote Agent service to accept incoming sessions. By default, TCP port 10000 is monitored.

**TCP Port: Backup Server**

This component monitor tests the ability of the Backup Server service to accept incoming sessions. By default, TCP port 6106 is monitored.
Symantec Endpoint Protection Client

This template allows you to monitor Symantec Endpoint Protection client services and major events from the application event log.

**Prerequisites:**

WinRM must be installed and properly configured on the target server.

**Credentials:**

Administrator on target server.

**Monitored Components**

For details on monitors, see [SAM Component Monitor Types](#).

All monitors should return values of zero. Returned values other than zero indicate an abnormality. Examining the Windows system and application log files should provide information pertaining to the issue.

**Service: Symantec Endpoint Protection**

This monitor returns the CPU and memory usage of the Symantec Endpoint Protection service. This service provides malware and threat protection for Symantec Endpoint Protection.

**Service: Symantec Management Client**

This monitor returns the CPU and memory usage of the Symantec Management Client service. This service provides communication with the Symantec Endpoint Protection Manager. It also provides network threat protection and application and device control for the client.

**Days passed from last SEP client update**

This monitor returns the number of days passed since the last SEP update. In the Message field, this component returns the date of last SEP update in the following format: Month/Day/Year.

**Virus found events**

This monitor returns the number of the Virus Found events.

Type of event: Any event. Event ID: 5.

**Antivirus scan events**

This monitor returns the number of events that occur when:

- Antivirus scan started/stopped with errors;
- Scanning fails to gain access to a file or directory;
- Scan is stopped before it completes;
- Scheduled scan is snoozed/paused (delayed);
- Snoozed/paused scan is restarted.

**Type of event:** Warning, Error. Event ID: 2, 3, 6, 21, 26, 27.

**Adware and spyware scan events**

This monitor returns the number of events that occur when the adware and spyware scan started or stopped with errors.

**Type of event:** Warning, Error. Event ID: 2, 3, 6, 21, 26, 27.

**Definition file events**

This monitor returns the number of events that occur when:

- The parent server sends a .vdb file to a secondary server;
- Symantec AntiVirus loads a new .vdb file with errors;
- New definitions are downloaded with errors by a scheduled definitions update;
- Definitions are rolled back;
- The computer is not protected with definitions.

**Type of event:** Warning, Error. Event ID: 65, 66.

**Auto-Protect events**

This monitor returns the number of events that occur when:

- Auto-Protect is not fully operational;
- Auto-Protect fails to load;
- Auto-Protect is unloaded;
- An error occurs with Auto-Protect;
- Auto-Protect fails to perform a successful side-effects repair for adware or spyware.

**Type of event:** Warning, Error. Event ID: 11, 22, 24, 41, 49.

**Antivirus startup and shutdown events**

This monitor returns the number of events that occur when the AntiVirus starts and stops.

**Type of event:** Any event. Event ID: 13, 14.

**Backup and restore from quarantine events**

This monitor returns the number of events when the Symantec AntiVirus cannot back up a file or restore a file from quarantine.

**Type of event:** Warning, Error. Event ID: 20.

**Configuration events**

This monitor returns the number of events when a configuration file cannot be read.

**Type of event:** Warning, Error. Event ID: 42.

**Log forwarding events**

This monitor returns the number of events when there is a problem with the log forwarding process.
Type of event: Warning, Error. Event ID: 34.

TruScan events

This monitor returns the number of events that occur when:

- The TruScan component could not be started;
- The TruScan engine could not be started;
- The TruScan is enabled, but it is not supported on the platform.

Type of event: Warning, Error. Event ID: 74, 73, 76.

Symantec tamper protection alerts

This monitor returns the number of events when SymProtect blocks a tamper attempt.

Type of event: Warning, Error. Event ID: 45.
Symantec Endpoint Protection Server

This template allows you to monitor Symantec Endpoint Protection Server services and major TCP ports.

**Prerequisites:**

WMI access to target server.

**Credentials:**

Administrator on target server.

Monitored Components

For details on monitors, see [SAM Component Monitor Types](#).

**Service: Symantec Embedded Database**

This monitor returns the CPU and memory usage of the Symantec Embedded Database service. This service is responsible for the embedded database used by the Symantec Endpoint Protection Manager.

**Service: Symantec Endpoint Protection Manager**

This monitor returns the CPU and memory usage of the Symantec Endpoint Protection Manager service. This service is responsible for the application server which communicates with the Symantec Endpoint Protection Manager, Symantec Protection clients, and database.

**Service: Symantec Endpoint Protection Manager Webserver**

This monitor returns the CPU and memory usage of the Symantec Endpoint Protection Manager Webserver service. This service allows you to communicate with the SEPM manager using a web interface.

**SEPM manager old TCP port**

This component monitor tests the ability of a SEPM service to accept incoming sessions. This port is used for communication between the SEPM manager and the SEP clients and Enforcers. By default, port 80 is monitored. Port 8014 is used for builds MR3 and later.

**SEPM manager new TCP port**

This component monitor tests the ability of a SEPM service to accept incoming sessions. This port is used for communication between the SEPM manager and the SEP clients and Enforcers. By default, port 80 is monitored. Port 8014 is used for builds MR3 and later.

**HTTPS web console port**

This component monitor tests the ability of an HTTPS web console to accept incoming sessions. This port is used in HTTPS communications between a remote management console and the SEPM manager. All login information and administrative communication takes place using this secure port. By default, port 8443 is monitored.
Remote web console port

This component monitor tests the ability of an HTTP web console to accept incoming sessions. This port is used in initial HTTP communications between a remote management console and the SEPM manager. (This communication is used only to display the login screen.) By default, port 9090 is monitored.
Symantec NetBackup Server

This template allows you to monitor the performance of a Symantec NetBackup Server installed on a Windows machine by using Windows Services, TCP Port, and PowerShell monitors.

**Prerequisites:**

WinRM must be installed and properly configured on the target server.

**Credentials:**

Administrator on the target server.

ℹ️ This was tested on Symantec NetBackup 7 Server.

Monitored Components

ℹ️ For details on monitors, see [SAM Component Monitor Types](#).

**Service: NetBackup Agent Request Server**

This monitor returns CPU and memory usage of the NetBackup Agent Request Server service. This service populates the NetBackup catalog database with Database agent metadata and services request for agents. This service is also responsible for initiating certain actions, such as starting jobs for Oracle cloning.

**Service: NetBackup Audit Manager**

This monitor returns CPU and memory usage of the NetBackup Audit Manager service which manages NetBackup audit information.

**Service: NetBackup Compatibility Service**

This monitor returns CPU and memory usage of the NetBackup Compatibility service. This service is used internally by new NetBackup services to communicate with legacy NetBackup services.

**Service: NetBackup Database Manager**

This monitor returns CPU and memory usage of the NetBackup Database Manager which manages the NetBackup internal databases and catalogs. This service must be running on the NetBackup master server during all normal NetBackup operations.

**Service: NetBackup Enterprise Media Manager**

This monitor returns CPU and memory usage of the NetBackup Enterprise Media Manager service. This service is responsible for usages of Keeps track of volumes (tapes), devices, and storage units needed for backup or restore. This service performs media and device selection for all NetBackup job types.
Service: NetBackup Event Manager

This monitor returns CPU and memory usage of the NetBackup Event Manager service which creates and manages event channels and supporting objects used in communication among NetBackup services.

Service: NetBackup Job Manager

This monitor returns CPU and memory usage of the NetBackup Job Manager service which starts jobs once resources are available and tracks the status of their execution.

Service: NetBackup Policy Execution Manager

This monitor returns CPU and memory usage of the NetBackup Policy Execution Manager service. This service creates and cancels jobs based on the configured policies and images.

Service: NetBackup Relational Database Manager

This monitor returns CPU and memory usage of the NetBackup Relational Database Manager service. This service manages the NetBackup relational database. This service must be running on the NetBackup Enterprise Media Manager server during all normal NetBackup operations.

Service: NetBackup Remote Manager and Monitor Service

This monitor returns CPU and memory usage of NetBackup Remote Manager and Monitor Service. This service enables NetBackup to remotely manage and monitor resources on this system that are used for backup (or affected by backup activity).

Service: NetBackup Request Daemon

This monitor returns CPU and memory usage of the NetBackup Request Daemon. This service processes requests from NetBackup clients and servers. This service also starts the NetBackup scheduler to perform automatically scheduled backups. It must be running on the NetBackup master server to perform any backups or restores.

Service: NetBackup Resource Broker

This monitor returns CPU and memory usage of NetBackup Resource Broker. This service allocates resources to jobs and queues requests for later allocation when the resources are not immediately available.

Service: NetBackup Service Layer

This monitor returns CPU and memory usage of the NetBackup Service Layer service. This service is a gateway to NetBackup for user interfaces.

Service: NetBackup Service Monitor

This monitor returns CPU and memory usage of the NetBackup Service Monitor. This service monitors the NetBackup services and when a service unexpectedly terminates, this service will attempt to restart the terminated service.
**Service: NetBackup Storage Lifecycle Manager**

This monitor returns CPU and memory usage of NetBackup Storage Lifecycle Manager service. This service manages Storage Lifecycle operations and schedules duplication jobs. It also monitors disk capacity on capacity managed volumes and removes older images when required.

**Service: NetBackup Vault Manager**

This monitor returns CPU and memory usage of the NetBackup Vault Manager service. This service manages the NetBackup Vault. This service must be running on the NetBackup Vault server during all NetBackup Vault operations.

**Service: NetBackup Volume Manager**

This monitor returns CPU and memory usage of the NetBackup Volume Manager service. It acts as a proxy to nbemmm for volume, global database, and device allocator requests from pre-6.0 NetBackup servers.

**Backup and Restore to NetBackup Clients TCP Port**

This component monitor tests the ability of a NetBackup Server to accept incoming sessions. By default, it monitors TCP port 13724. For the server-initiated, this port is used for standard backup and restoration to NetBackup clients.

**Server to Server Communication TCP Port**

This component monitor tests the ability of a NetBackup Server to accept incoming sessions. By default, it monitors TCP port 1556. This port is used for server to server communications.

**Job Status**

This monitor returns the summary of the jobs database by using the `bpdbjobs` command. Returned values are as follows:

- QUEUED – This component returns the number of queued jobs.
- REQUEUED – This component returns the number of requeued jobs.
- ACTIVE – This component returns the number of active jobs.
- SUCCESSFUL – This component returns the number of successfully finished jobs.
- PARTIALLY – This component returns the number of partially finished jobs.
- FAILED – This component returns the number of failed jobs.
- INCOMPLETE – This component returns the number of uncompleted jobs.
- SUSPENDED – This component returns the number of suspended jobs.
- WAITING_RETRY – This component returns the number of jobs waiting for retry.
- TOTAL – This component returns the total number jobs.

**Arguments:**

All Perl scripts use the same argument structure:

```
path_to_bpdbjobs_command, master_server
```

where

- `path_to_bpdbjobs_command` – Full path to `bpdbjobs` utility;
- `master_server` – The name of master server which we want to monitor.
Example:
C:\Program Files\Veritas\NetBackup\bin\admincmd\bpdbjobs.exe,lab-netbackup7

**Warning Events**

This monitor returns the number of server warning events by using the berror command.

**Arguments:**
All Perl scripts use the same argument structure:
path_to_berror_command, hours_ago
where
path_to_berror_command - Full path to berror utility;
hours_ago - Monitoring time interval in hours. By default it set to return events from the last hour.

Example:
C:\Program Files\Veritas\NetBackup\bin\admincmd\berror.exe,1

**Error Events**

This monitor returns the number of server error events by using the berror command.

**Arguments:**
All Perl scripts use the same argument structure:
path_to_berror_command, hours_ago
where
path_to_berror_command - Full path to berror utility;
hours_ago - Monitoring time interval in hours. By default it set to return events from the last hour.

Example:
C:\Program Files\Veritas\NetBackup\bin\admincmd\berror.exe,1

**Critical Events**

This monitor returns the number of server critical events by using the berror command.

**Arguments:**
All Perl scripts use the same argument structure:
path_to_berror_command, hours_ago
where
path_to_berror_command - Full path to berror utility;
hours_ago - Monitoring time interval in hours. By default it set to return events from the last hour.

Example:
C:\Program Files\Veritas\NetBackup\bin\admincmd\berror.exe,1
Symantec NetBackup Client

This template allows you to monitor the performance of Symantec NetBackup Client installed on a Windows machine by using Windows Services, TCP Port, and Windows Event Log monitors.

Prerequisites:

WMI access on target server.

Credentials:

Administrator on the target server.

This was tested on Symantec NetBackup 7 Client.

Monitored Components

For details on monitors, see [SAM Component Monitor Types](#).

**Service: NetBackup Client Service**

This monitor returns CPU and memory usage of the NetBackup Client Service. This is the main NetBackup client service and it starts other necessary services. This network service is used to create “firewall friendly” socket connections.

**Service: NetBackup Legacy Client Service**

This monitor returns CPU and memory usage of the NetBackup Legacy Client Service. This service listens for connections from NetBackup servers in the network and when an authorized connection is made, starts the necessary NetBackup process to service the connection.

**Service: NetBackup Legacy Network Service**

This monitor returns CPU and memory usage of the Legacy Network Service

**NetBackup Client TCP Port**

This component monitor tests the ability of a NetBackup client to accept incoming sessions from the server. By default, it monitors TCP port 13724.

**Multistreamed Backups TCP port**

This component monitor tests the ability of a NetBackup client to accept incoming sessions from the server. By default, it monitors TCP port 13782. This port is used to get a list of mount points for multistreamed backups. It also accesses or updates host properties for the client.

**NetBackup Client Error and Warning Events**

This monitor returns the number of Warning and Error messages in the Windows Application log file. It looks for the following Source Names: NetBackup, NetBackup Client Service, NetBackup Job Manager, and NetBackup Legacy Client Service. This monitor should be zero at all times. If it is not, you should look in the Windows Event Viewer for details.
TACACS+ User Experience Monitor

This template tests user authentication through the TACACS+ protocol.

Prerequisites

A server with TACACS+ authentication. You must know the secret shared key.

Credentials

A valid TACACS+ username and password.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

TACACS+ User Experience Monitor

This component monitor uses synthetic transactions to test user authentication through the TACACS+ protocol. The synthetic transaction does the following:

1. Connect to server.
2. Send TACACS+ credential and shared secret.
3. Validate response.
4. Measure response time.
Terminal Licensing Server

This template assesses the status and overall performance of a Microsoft Terminal Licensing Server. This template uses Windows System Event Log, Windows Service, and PowerShell monitors.

Prerequisites

- WMI access to the target server
- Windows Server 2003 Resource Kit Tools should be installed on Terminal Licensing Server
- WinRM should be properly configured on target server

Credentials

Windows Administrator on the target server.

Monitored Components

For details on monitors, see [SAM Component Monitor Types](#).

All Windows Event Log monitors should return zero values. Returned values other than zero indicate an abnormality. Examining the Windows System log file, with “TermServLicensing” and “TerminalServices-Licensing” source names, should provide information pertaining to the issue.

Detailed information about all these events can be found here:

http://technet.microsoft.com/en-us/library/cc775125(v=ws.10)

www.eventid.net

Licenses Usage

This monitor returns license usage statistics by running the lsreport tool from the Windows Server 2003 Resource Kit Tools. In the message fields, this component returns which machine connection is initialized (Client), which user currently uses a license (User), the License Type, and when the connection ends. Returned values are as follows:

- **Temporary** – This component returns the number of currently used Temporary licenses. Temporary licenses are given out when a client connects for the first time.
- **Active** – This component returns the number of currently used Active licenses. On the second connection and on successful logon, the client gets an Active license.
- **Upgraded** – This component returns the number of currently used Upgraded licenses. Windows 2000 licenses that were upgraded to a Windows 2003 license is called Upgraded.
- **Total Used** – This component returns the total number of currently used licenses.
- This monitor uses the following arguments: path_to_lsamreport, target_server.
- **path_to_lsamreport** – This is the full path to the lsreport.exe file. If the Windows Server 2003 Resource Kit Tools installed in the default location, this argument should be as follows:
  For x86 Windows: C:\Program Files\Windows Resource
SAM TEMPLATE REFERENCE: SERVER & APPLICATION MONITOR

Kits\Tools\lsreport.exe;
For x64 Windows: C:\Program Files (x86)\Windows Resource Kits\Tools\lsreport.exe.

- **target_server** – This is the IP address of the target server. It should be: ${IP}.

Argument example:
C:\Program Files\Windows Resource Kits\Tools\lsreport.exe, ${IP}

**Service: Remote Desktop Licensing**

This monitor returns the CPU and memory usage of the Remote Desktop Licensing server (Terminal Licensing Server on 2003). This service provides registered licenses for Remote Desktop Services clients. If this service is stopped, the server will be unavailable to issue Remote Desktop Services licenses to clients when they are requested.

**Events: Startup Errors**

This monitor returns the number of events that occur when:

- There is a Work Manager or Cannot Startup Work Scheduler error;
- The Terminal Services Licensing service could not create the service initialization thread;
- The Terminal Services Licensing service could not start due to a lack of system resources;
- The Terminal Services Licensing service cannot start due to an error;
- An error occurred during the Terminal Services license server initialization phase;
- The remote procedure call (RPC) port is not listening;
- TS Licensing is unable to allocate the required system memory to perform the operation;
- Cannot initialize policy module because of an error;
- A security descriptor cannot be set. As a result, terminal servers might not be able to connect to Terminal Services license servers.

**Type of event:** Error and Warning. Event ID: 43, 30, 36, 37, 4097, 4104, 4117, 41, 4142.

For Work Manager or Cannot Startup Work Scheduler errors, review the following article:

**Terminal Services Licensing service:** If the service initialization thread cannot be created, or a lack of system resources events exist, you should increase the amount of available memory on the Terminal Services license server.

If this service cannot start due to an error event, ensure that the required groups are granted the correct permissions to the TermServLicensing registry key and that the value of the DBPath registry key matches the location of the LServer directory. If the problem persists, shut down and then restart the Terminal Services license server.

For an error that occurred during the Terminal Services License Server Initialization Phase event, start the Terminal Services Licensing service, and if necessary, remove and then reinstall TS Licensing.

For the remote procedure call (RPC) port is not listening event, verify that the Terminal Services license server is available and ensure that the Terminal Services Licensing service is running.
For the Cannot Initialize Policy Module events, ensure that the Terminal Services Licensing registry key contains the following correct settings:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\TermServLicensing\Policy\MicrosoftCorporation\A02, and the registry subkey contains the following entry: String Name: DLL; String Value: %systemroot%\System32\tls236.dll.

For Security Descriptor Cannot Be Set events, restart the Terminal Services Licensing service.

Events: License Errors

This monitor returns the number of events that occur when:

- Cannot generate a license for client because of an error;
- Terminal Services Licensing on the server has not been activated. Terminal Services Licensing will only issue temporary licenses until the server is activated;
- The Terminal Services Licensing server has no license pack registered product;
- The Terminal Server Licensing server has no permanent licenses for the product;
- A license could not be issued because it is not a member of the Terminal Server Computers group;
- One or more Terminal Services Licensing certificates on server are corrupt.

Type of event: Error and Warning. Event ID: 38, 18, 22, 21, 45, 17.

For Cannot Generate A License For Client Because Of Error events: Review this event in the Windows Event Monitor for details.

For the Terminal Services Licensing On Server Has Not Been Activated events: Activate your Terminal Services Licensing server.

For the Terminal Services Licensing Server Has No License Pack Registered Product events: Use Terminal Services Licensing administrative tool to register the license pack.

For the Terminal Server Licensing Server Has No Permanent Licenses For Product events: Use the Terminal Server Licensing administrative tool to register more licenses.

For A License Could Not Be Issued To Because It Is Not A Member Of The Terminal Server Computers Group events: check the status of the License Server Security Group. If the status is set to Enabled, a local group called Terminal Services Computers is created. The Terminal Server License Server grants licenses only to computers whose computer accounts are placed in this group. When the target computer is a domain controller, this group is a domain local group. If the status is set to Disabled, the Terminal Server License Server issues a license to any computer that requests one. The Terminal Services Computers group is not deleted or changed in any way. This is the default behavior. If the status is set to Not Configured, the Terminal Server License Server acts the same as if the status is set to Disabled. If you did not add any clients to this group, any machine attempting to connect to the terminal server would be denied.

For one or more Terminal Services Licensing certificates on server are corrupt events: You should reactivate this TS Licensing server or this RD Licensing server.
**Events: Database Errors**

This monitor returns the number of events that occur when:

- Cannot connect to the database;
- General database error occurred.

**Type of event:** Error and Warning. Event ID: 7, 44.


**Events: Service Stopped**

This monitor returns the number of events that occur when:

- The Terminal Services Licensing service has stopped;
- TS Licensing has experienced a general initialization failure.

**Type of event:** Error and Warning. Event ID: 3, 4115.

For these events, start the Terminal Services Licensing service, and if necessary, remove and then reinstall TS Licensing.

**Events: Connection Errors with SCM**

This monitor returns the number of events that occur when:

- The Terminal Services Licensing service is unable to connect to the Service Control Manager;
- The Terminal Services Licensing service is unable to report status to the Service Control Manager.

**Type of event:** Error and Warning. Event ID: 27, 28.

For these events, restart the Terminal Services Licensing service, and if necessary, restart the server.
Tomcat Server

This template collects server resource information from an Apache Tomcat server by retrieving status information from the Tomcat status page. You can use the Orion agent for Linux or SNMP agentless to monitor.

Prerequisites

None.

Credentials

User with manager role. Tomcat users and roles can be configured in tomcat-users.xml file.

Example:

```xml
<role rolename="manager"/>
<user username="user" password="pass" roles="manager"/>
```

Prerequisites for Orion Agent for Linux

If using the Orion Agent for Linux to monitor your Tomcat server, you need to complete installation and configuration of Tomcat to properly work with the component monitors working with the Tomcat Server template.

The following information walks through installing and configuring Tomcat servers to work with SAM component monitors. If you have Tomcat installed, you can skip to step 4 to create an account used for polling.

1. Determine the version of Tomcat you want to install. You may have multiple versions available to install. To locate all versions, use this command:

   ```bash
   yum search tomcat
   ```

2. After determining the version, you can install the tomcat package and the admin webapps package. Locate the versions to install from the search results. For example:

   ```
   tomcat5.i386 : Apache Servlet/JSP Engine, RI for Servlet 2.4/JSP 2.0 API
   tomcat5-admin-webapps.i386 : The administrative web applications for Jakarta Tomcat
   ```

3. Install the versions using the located versions. To install the example above:

   ```bash
   yum install tomcat5 tomcat5-admin-webapps
   ```
4. Next, you need to modify the tomcat-users.xml file to create and provide a user account to access the web manager ('manager','manager-gui'). To locate, use this command:

```
find /etc -iname tomcat-users.xml
```

5. Edit the file and locate the `<tomcat-users>` section. If commented out, uncomment the configuration. Edit to add a user of tomcat with the password of tomcat. The template uses this account to access data.

```
<tomcat-users>
  <user name="tomcat" password="tomcat"
       roles="tomcat,manager,manager-gui" />
  <user name="role1" password="tomcat" roles="role1" />
  <user name="both" password="tomcat" roles="tomcat,role1" />
</tomcat-users>
```

6. Restart the service. The command depends on the version you installed. For example, this command restarts the installed service above:

```
service tomcat5 restart
```

**Monitored Components**

For details on monitors, see [SAM Component Monitor Types](#).

You need to set thresholds for counters according to your environment. It is recommended to monitor counters for some length of time to understand potential value ranges and then set the thresholds accordingly.

By default all components use port 8080. If your Tomcat server uses another port, you should manually change the Port Number field in all components.

**Tomcat Free Memory**

This monitor returns the amount of heap space currently available to the Java Virtual Machine. This value should be as high as possible. The heap space may be of a fixed size or may be expanded and shrunk, depending on the garbage collector's strategy. More information can be found here: [http://javarevisited.blogspot.com/2011/05/java-heap-space-memory-size-jvm.html](http://javarevisited.blogspot.com/2011/05/java-heap-space-memory-size-jvm.html).

**Tomcat Total Memory**

This monitor returns the total amount of memory currently allocated to the Java Virtual Machine heap space. This value should be as low as possible. You should set thresholds according to your Tomcat Max Memory value. If the returned value is near the Tomcat Max Memory value or you received OutOfMemoryError errors, you may need to increase the heap size. More information can be found here: [http://javarevisited.blogspot.com/2011/05/java-heap-space-memory-size-jvm.html](http://javarevisited.blogspot.com/2011/05/java-heap-space-memory-size-jvm.html).
Tomcat Max Memory

This monitor returns the maximum size of the heap space, not including the permanent generation area.

Tomcat Total Processing Time

This monitor returns the total processing time, in milliseconds, since the server started.

Tomcat Total Request Count

This monitor returns the total number of requests from the server since the server started.

Tomcat Total Bytes Sent

This monitor returns the total number of bytes sent from the server since the server started.

Tomcat Total Bytes Received

This monitor returns the total number of bytes sent to the server since the server started.

Tomcat Total Errors Count

This monitor returns the total number of errors from all request processors.

Tomcat Server monitor

This component monitor collects server resource information from Apache Tomcat servers by retrieving status information from http://{$IP}:${$PORT}/manager/status/?XML=true.

This component monitor internally issues HTTP requests to the monitored Tomcat server. It expects a response in the form of XML, used to parse data and metrics.

If you are experiencing issues with the Tomcat Server Monitor on AIX computers, enable remote access in the following Tomcat configuration file:

conf/Catalina/localhost/manager.xml

Prerequisites for Orion Agent for Linux/Unix

If using the Orion Agent for Linux/Unix to monitor your Tomcat server, you need to complete installation and configuration of Tomcat to properly work with the component monitors working with the Tomcat Server template.

The following information walks through installing and configuring Tomcat servers to work with SAM component monitors. If you have Tomcat installed, you can skip to step 4 to create an account used for polling.

1. Determine the version of Tomcat you want to install. You may have multiple versions available to install. To locate all versions, use this command:

    yum search tomcat
2. After determining the version, you can install the tomcat package and the admin webapps package. Locate the versions to install from the search results. For example:

```
tomcat5.i386 : Apache Servlet/JSP Engine, RI for Servlet 2.4/JSP 2.0 API
tomcat5-admin-webapps.i386 : The administrative web applications for Jakarta Tomcat
```

3. Install the versions using the located versions. To install the example above:

```
yum install tomcat5 tomcat5-admin-webapps
```

4. Next, you need to modify the tomcat-users.xml file to create and provide a user account to access the web manager (‘manager’, ‘manager-gui’). To locate, use this command:

```
find /etc -iname tomcat-users.xml
```

5. Edit the file and locate the `<tomcat-users>` section. If commented out, uncomment the configuration. Edit to add a user of tomcat with the password of tomcat. The template uses this account to access data.

```
<tomcat-users>
  <user name="tomcat" password="tomcat"
    roles="tomcat,manager,manager-gui" />
  <user name="role1" password="tomcat" roles="role1" />
  <user name="both" password="tomcat" roles="tomcat,role1" />
</tomcat-users>
```

6. Restart the service. The command depends on the version you installed. For example, this command restarts the installed service above:

```
service tomcat5 restart
```

**Statistic**

One of the following Tomcat variables as specified in the Tomcat Variables Name field.

**Free Memory**

Amount of heap space currently available to the Java Virtual Machine.

**Total Memory**

Total memory currently allocated to the Java Virtual Machine heap space.

**Max Memory**

Maximum size of the heap space not including the permanent generation area.
Total Processing Time
Total processing time in milliseconds since server start.

Total Request Count
Total requests from server since server start.

Total Bytes Sent
Total bytes sent from server since server start.

Total Bytes Received
Total bytes sent to server since server start.

Total Error Count
Total error count from all request processors.

Field Descriptions

Description
This field provides a default description of the monitor. You can override the default description by adding to or replacing the text, which will then be automatically saved. The variable to access this field is ${UserDescription}.

Enable Component
Determines whether the component is enabled. Disabling the component leaves it in the application in a deactivated state not influencing either SolarWinds SAM application availability or status.

Credential for Monitoring
Select a credential that can access the password-protected portion of the web site. Click a credential in the list, or use the <Inherit credential from node> option. If the credential is not in the credentials list, add it in the Credentials Library that you can access by clicking Settings > All Settings > SAM Settings in the Orion Web Console..

Port Number
This field allows you to specify the port number used by the web site. The default value for this field is 8080.

Url
Allows you to specify the URL you want to monitor. The SolarWinds SAM variables ${IP} and ${PORT} contained in the default value for this field attempts to monitor a web site at the IP address of the assigned node.

Tomcat Variables Name
Specifies the Tomcat server variable to monitor.
Convert Value

Checking the Convert Value check box opens the Formula box. From here, you can manipulate the returned value with a variety of mathematical possibilities. You can choose common functions from the drop down lists to manipulate the returned value, or you can select the Custom Conversion option. See Conversion value.

Response Time Threshold

Use this field to set warning and critical threshold conditions based on response time. The response time is the time in milliseconds it takes SolarWinds SAM to determine that a component is not Down and to retrieve any statistical data. See Application Monitor Thresholds for details.

Statistic Threshold

This field allows you to specify when a threshold that indicates a warning or critical level has been breached. Logical operators are in the drop down followed by a blank field for you to enter the value of this threshold. For example: Less than 15 for warning, Less than 5 for critical. See Application Monitor Thresholds for details.

User Notes

This field allows you to add notes for easy reference. You can access this field by using the variable, ${UserNotes}.

Install and configure Tomcat

The following information walks through installing and configuring Tomcat servers to work with SAM component monitors. If you have Tomcat installed, you can skip to step 4 to create an account used for polling.

1. Determine the version of Tomcat you want to install. You may have multiple versions available to install. To locate all versions, use this command:

   yum search tomcat

2. After determining the version, you can install the tomcat package and the admin webapps package. Locate the versions to install from the search results. For example:

   | tomcat5.i386 | Apache Servlet/JSP Engine, RI for Servlet 2.4/JSP 2.0 API |
   | tomcat5-admin-webapps.i386 | The administrative web applications for Jakarta Tomcat |

3. Install the versions using the located versions. To install the example above:

   yum install tomcat5 tomcat5-admin-webapps
4. Next, you need to modify the tomcat-users.xml file to create and provide a user account to access the web manager ('manager', 'manager-gui'). To locate, use this command:

```
find /etc -iname tomcat-users.xml
```

5. Edit the file and locate the `<tomcat-users>` section. If commented out, uncomment the configuration. Edit to add a user of `tomcat` with the password of `tomcat`. The template uses this account to access data.

```xml
<tomcat-users>
  <user name="tomcat" password="tomcat" roles="tomcat,manager,manager-gui" />
  <user name="role1" password="tomcat" roles="role1" />
  <user name="both" password="tomcat" roles="tomcat,role1" />
</tomcat-users>
```

6. Restart the service. The command depends on the version you installed. For example, this command restarts the installed service above:

```
service tomcat5 restart
```

**Troubleshoot Tomcat**

To check the XML responses from the Tomcat server, you can send a simple HTTP request through any web browser to check for raw XML content. The URL should be in the following format:

http://host:port/manager/status/?XML=true

You can also query your Tomcat server through CLI using `wget`. 
Trend Micro

The following templates are available:

- Trend Micro OfficeScan Client
- Trend Micro OfficeScan Server
- Trend Micro Server Protect (Windows)

Trend Micro OfficeScan Client

This template assesses the status and overall health of Trend Micro OfficeScan Client.

**Prerequisites**

WMI access to the target server.

**Credentials**

Windows Administrator on the target server.

Monitored Components

For details on monitors, see [SAM Component Monitor Types](#).

**Service: OfficeScan NT RealTime Scan**

This monitor returns CPU and memory usage of OfficeScan NT RealTime Scan service. This service performs Real-time, Scheduled, and Manual scan on OfficeScan clients.

**Service: OfficeScan NT Listener**

This monitor returns CPU and memory usage of OfficeScan NT Listener service. This service receives commands and notifications from the OfficeScan server and facilitates communication from the client to the server.

**Files Scanned**

This monitor returns the total number of files scanned.

- This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

**Malware Detected**

This monitor returns the total number of viruses/malware detected.

- This component has Count statistic as difference enabled. It will return the difference between two polling intervals.
**Suspicious Files Detected**

This monitor returns the total number of files suspected to be infected with virus/malware.

> This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

**Trend Micro OfficeScan Server**

This template assesses the status and overall health of Trend Micro OfficeScan Server.

**Prerequisites**

WMI access to the target server.

**Credentials**

Windows Administrator on the target server.

**Monitored Components**

> For details on monitors, see [SAM Component Monitor Types](#).

**Service: OfficeScan Active Directory Integration**

This monitor returns CPU and memory usage of OfficeScan Active Directory Integration service. This service provides Active Directory support for OfficeScan Master Service.

> By default, this monitor is disabled.

**Service: OfficeScan Control Manager Agent**

This monitor returns CPU and memory usage of OfficeScan Control Manager Agent service. This service allows administrators to manage OfficeScan from the Control Manager console.

> By default, this monitor is disabled.

**Service: OfficeScan Master**

This monitor returns CPU and memory usage of OfficeScan Master service. This service accepts and responds to commands and requests from OfficeScan clients, Web console, and Control Manager.

**Service: OfficeScan Plug-in Manager**

This monitor returns CPU and memory usage of OfficeScan Plug-in Manager service. This service installs and manages Trend Micro OfficeScan plug-in programs.

**TCP Port: File Reputation**

This component monitor tests the ability of a File Reputation service to accept incoming
sessions. It monitors TCP port 4345.

**TCP Port: Web Reputation**

This component monitor tests the ability of a Web Reputation service to accept incoming sessions. It monitors TCP port 5274.

**TCP Port: OfficeScan Web Service (HTTP)**

This component monitor tests the ability of a Web service to accept incoming sessions by using HTTP protocol. It monitors TCP port 8080.

**TCP Port: OfficeScan Web Service (HTTPS)**

This component monitor tests the ability of a Web service to accept incoming sessions by using HTTPS protocol. It monitors TCP port 4343.

**Warning and Errors: OfficeScan**

This monitor returns OfficeScan warning and error events.

**Source name: Trend Micro OfficeScan Server**

Log file: Application.
Trend Micro Server Protect (Windows)

This template assesses the status and overall performance of Trend Micro Server Protect for Windows. You should assign this template on all Normal servers which you want to monitor. This template uses the Windows System Event Log, Windows Service, TCP Port, and PowerShell monitors.

Prerequisites

Before using this template you should open the Trend Micro Server Protect Management Console and create or reconfigure the STATISTIC task on the target Normal server. The STATISTIC task (Run Statistics) should be created as a scheduled task with Hourly frequency. The All Dates time range should be enabled as well as the Export Statistic to CSV file option. The task owner should be Admin and this task should be created as the default task.

WinRM should be properly configured on the target server.

Credentials

Windows administrator on target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Service: Trend Server Protect

This monitor returns CPU and memory usage of Trend Server Protect service.

Trend Server Protect TCP Port

This component monitor tests the ability of a Trend Server Protect service to accept incoming sessions. By default it monitors TCP port 5168.

Events: Update Failure

This monitor returns the number of events that occur when there is:

- A pattern update failure;
- An engine update failure;
- A program update failure;
- An encyclopedia update failure.

Type of event: Error. Event ID: 3, 5, 7, 9.

Check Event Viewer for more details.

Events: Start Scan Failure

This monitor returns the number of events when the following occurs:

- An error: starting a real-time scan;
- An error: starting a manual scan;
- An error: starting a scheduled scan.

**Type of event:** Error. Event ID: 11, 14, 17.

Check Event Viewer for more details.

**Events: Virus Pattern is Out of Date**

This monitor returns the number of virus pattern is out of date events.

**Type of event:** Error. Event ID: 52.

Check Event Viewer for more details.

**Events: Virus Found**

This monitor returns the number of events that occur when:

- A virus is found;
- Virus found during a real-time scan;
- Virus found during a manual scan;
- Virus found during a scheduled scan.

**Type of event:** Error. Event ID: 1, 101, 102, 103.

Check Event Viewer for more details.

**Events: Configuration Errors**

This monitor returns the number of events when the following occurs:

- An error: setting configuration data for real time scanning;
- An error: performing a scan-now task;
- An error: performing a pattern update task;
- An error: purging logs by a task;
- An error: exporting logs by a task;
- An error: printing logs by a task;
- An error: running statistics by a task.

**Type of event:** Error. Event ID: 304, 306, 308, 310, 312, 314, 316.

Check Event Viewer for more details.

**Events: Exception Occurred**

This monitor returns the number of events that occur when:

- An exception has occurred in "module name;"
- An exception has occurred in TmRpcSrv;
- An error: starting a RPC server.

**Type of event:** Error. Event ID: 201, 202, 203.

Check Event Viewer for more details.
**Client Statistics**

This monitor returns Normal Server statistics from an exported CSV file. Returned values are as follows:

- **Infected Users** – This component returns the number of network users who were detected handling infected files.
- **Infected Files** – This component returns the number of infected files detected by ServerProtect.
- **Non Cleanable Viruses** – This component returns the number of viruses detected on the network that could not be cleaned.
- **Non Cleanable Files** – This component returns the number of infected files that could not be cleaned of their virus code.

This monitor uses the following arguments:

```
path_to_CSV_stat_file
```

where

```
path_to_CSV_stat_file - Full path to exported statistic CSV file.
```

Example:

```
C:\Program Files\Trend\SProtect\Statistic.CSV
```
UniData Database (Windows)

This template assesses the status and overall performance of UniData Database using Windows Performance Counters.

Prerequisites

WMI access to the target server.

Credentials

Windows Administrator on the target server.

Tested on UniData v 7.3.

Limitations

- SAM will be unable to access some 32-bit counters of a x86 Unidata database on a 64-bit operating system.
- SAM will not be able to monitor a Unidata database server if it is installed on a 64-bit system.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

You need to set thresholds for counters according to your environment. It is recommended to monitor counters for some period of time to understand potential value ranges and then set the thresholds accordingly.

**Dynamic Array: COUNT**

This monitor returns the number of dynamic array counts from the Count command.

**Dynamic Array: DELETE**

This monitor returns the number of dynamic array deletions from the Del command.

**Dynamic Array: EXTRACT**

This monitor returns the number of dynamic array data extractions from the Extract command.

**Dynamic Array: FIELD**

This monitor returns the number of dynamic array string extractions from the Field command.

**Dynamic Array: FIND**

This monitor returns the number of dynamic array finds from the Find command.

**Dynamic Array: INDEX**

This monitor returns the number of dynamic array substring indices from the Index command.
Dynamic Array: INSERT

This monitor returns the number of dynamic array inserts from the Ins command.

Dynamic Array: LOCATE

This monitor returns the number of dynamic array locations from the Locate command.

Dynamic Array: MATCHFIELD

This monitor returns the number of dynamic array substring matches from the Matchfield command.

Dynamic Array: MATPARSE

This monitor returns the number of dynamic array matrix parses from the Matparse command.

Dynamic Array: REMOVE

This monitor returns the number of dynamic array element removals from the Remove command.

Dynamic Array: REPLACE

This monitor returns the number of dynamic array replacements from the Replace command.

Dynamic File: Dynamic File Group Split

This monitor returns the number of times a group in a dynamic file splits. If your application shows unusual activity and your performance is suffering, consider analyzing and possibly reconfiguring some of your dynamic files. Increasing Split.Load makes a file split less often.

Dynamic File: Dynamic File Group Merge

This monitor returns the number of times a split pair of groups merges back together. If your application shows unusual activity and your performance is suffering, consider analyzing and possibly reconfiguring some of your dynamic files. Increasing Merge.Load makes a file merge more often.

File I/O: File Close

This monitor returns the number of file closes at the operating system level.

File I/O: File Open

This monitor returns the number of files at the operating system level. On NT, if the average value in this field is more than 5 (opens per second), performance may suffer.

File I/O: Level 1 Overflow

This monitor returns the number of level 1 overflows. Compute the total activity by summing Record Read, Record Write, Record Delete. If Level 1 Overflow is more than 10% of the total activity, use guide to analyze your files and resize them appropriately.

File I/O: Level 2 Overflow

This monitor returns the number of level 2 overflows. If Level 2 Overflow is more than 2% of total activity, use the guide utility to identify files in level 2 overflow and resize them appropriately.
File I/O: Record Delete

This monitor returns the number of records deleted by UniBasic commands.

File I/O: Record Read

This monitor returns the number of records read by UniData commands (other than UniQuery).

File I/O: Record Write

This monitor returns the number of records written by UniData commands (other than UniQuery).

File I/O: TempFile Close

This monitor returns the number of events when UniData temporarily closes the least recently accessed open file when requests for file opens exceed the limit of open files per process.

Index Statistics: Index Log Read

This monitor returns the number of reads from an index log file. This occurs when an index which was disabled is re-enabled and updated with the contents of the index log.

Index Statistics: Index Log Write

This monitor returns the number of writes to an index log file. This occurs while an index is disabled, as UniData tracks changes by recording them in the index log.

Index Statistics: Index Node Merge

This monitor returns the number of times two nodes merge; this takes place when entries in one or both nodes decrease.

Index Statistics: Index Node Read

This monitor returns the number of index node reads; a node is a component of the B+ tree structure, and a node is analogous to a block in a hashed file.

Index Statistics: Index Node Reuse

This monitor returns the number of times a node previously freed by a node merge is used for a node split.

Index Statistics: Index Node Split

This monitor returns the number of times an index node splits in two; this happens when entries in the original node increase. An unusual amount of split/merge/reuse activity indicates that one or more indexes are not properly sized. Use the Ecl List.Index command to identify these, and then delete and rebuild them.

Index Statistics: Index Node Write

This monitor returns the number of index node write; a node is a component of the B+ tree structure, and a node is analogous to a block in a hashed file.
Index Statistics: Index Overflow Read

This monitor returns the number of times UniData reads from an index overflow node. The system creates overflow nodes when the number of keys in an index node exceeds a set limit. The overflow condition is created when the alternate key length of the index is too small for the selected attribute. Reads to and writes from overflow nodes slow system performance.

Index Statistics: Index Overflow Write

This monitor returns the number of times UniData writes an overflow node. If overflow activity (reads and writes) exceeds 5% of system activity (Index Node Reads and Index Node Writes), use the Ecl List.Index command to identify which indexes are overflowed, and delete and rebuild them using a larger key length. (The default key length is 20 characters.)

Lock Statistics: Exclusive Group Lock

This monitor returns the UniData-level exclusive lock on an entire group. For most applications, the number of shared group locks exceeds the number of exclusive group locks. If the number of exclusive group locks is larger than the number of shared group locks, one or more files may be overflowed. Identify these with the guide utility.

Lock Statistics: Exclusive Index Lock

This monitor returns the UniData-level exclusive lock on an index. For most applications, the number of shared index locks exceeds the number of exclusive index locks. If the number of exclusive index locks is larger than the number of shared index locks, one or more index files may be overflowed. Identify these with the List.Index Ecl command.

Lock Statistics: GLM Lock Failure

This monitor returns the number of times a process attempts to get a physical group lock and fails because the group is already locked. If performance is suffering, analyze your files for overflow.

Lock Statistics: GLM Lock Request

This monitor returns the number of times a process attempts to get a physical group lock.

Lock Statistics: Lock Failure

This monitor returns the number of times a process attempts to get a user-level lock and fails because the record is already locked. If performance is suffering, analyze your application for lock handling.

Lock Statistics: Record Lock

This monitor returns the number of user-level record locks set by commands such as Readl and Readu.

Lock Statistics: Record Unlock

This monitor returns the number of user-level locks released by commands such as Release.
Lock Statistics: Semaphore Lock

This monitor returns the number of user-level resource locks set by commands such as Lock and T.Att.

Lock Statistics: Semaphore Unlock

This monitor returns the number of user-level resource locks released by commands such as T.Det or Ulock.

Lock Statistics: Shared Group Lock

This monitor returns the UniData-level read-only lock on an entire group.

Lock Statistics: Shared Index Lock

This monitor returns the UniData-level read-only lock on an index.

Program Control: CALLC Call

This monitor returns the number of calls to an external C function, From UniBasic Callc statements.

Program Control: CHAIN Call

This monitor returns the number of UniBasic Chain statement executed.

Program Control: EXECUTE Call

This monitor returns the number of external UniData command executions (From UniBasic Execute commands).

Program Control: Global Call

This monitor returns the number of calls to globally cataloged UniBasic programs. In production environment, this number should be much higher than Local Call. If a program is globally cataloged, then users share a single copy of the object code in memory, which reduces both memory requirements and physical I/O load.

Program Control: Local Call

This monitor returns the number of calls to locally cataloged UniBasic programs. Locally cataloged UniBasic programs involve heavy I/O activity and increased memory demand, because each local call loads a copy of the executable in memory. In a development environment, using locally cataloged programs may be normal. In a production environment, if more than 5% of calls are local calls, examine your application and globally catalog programs for improved performance.

Program Control: PCPERFORM Call

This monitor returns the number of Pcperform statements, which execute shell or host operating system tasks. Pcperform statements are expensive on NT, because creating a process is slow. If Pcperform Call is consistently more than 1 per second, analyze your application and consider replacing Pcperform logic with C routines.
Unix

The following templates are available:

- Unix CPU Monitoring Perl
- Unix Disk Monitoring Perl
- Unix Memory Monitoring Perl
- Unix Sendmail Monitoring Perl
Unix CPU Monitoring Perl

This template uses Perl scripts to assess the CPU performance of computers running AIX 5.3 or 6.1; Solaris 8, 9, or 10; or HP-UX 11.0.

Prerequisites

SSH and Perl installed on the target server.

If Perl is installed in a location different from /usr/bin/perl, you should correct all components in the first line of the field “script body” (#!/usr/bin/perl), or you can create a symbolic link to Perl (refer to the documentation for the ln command).

You can find where Perl is installed by using the following command: `which perl`

Credentials

Root credentials on the target server.

Some Unix implementations such as Solaris have a character limit in the input buffers of SSH sessions that prevents SolarWinds SAM from copying over scripts. If a monitored component fails to return a result or returns error code 255, manually copy the script to the target machine and then make the appropriate path and file name change in the Command Line field. For example, if you manually copied the script over as /usr/script.pl, you should change the Command Line to: perl /usr/script.pl

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Components without predetermined threshold values have guidance such as "Use the lowest threshold possible" or "use the highest threshold possible" to help you find a threshold appropriate for your application.

CPU User Time (%)

Percent of CPU time spent running non-kernel code (user time). This represents the time spent executing user code. It depends on the programs that the user uses.

Use the lowest threshold possible.

CPU System Time (%)

Percent of CPU time spent running system kernel code (system time).

Use the lowest threshold possible.

CPU Idle Time (%)

Percent of CPU time spent idle.

Use the highest threshold possible at all times.
Interrupts/sec

The number of interrupts per second.

The threshold for this depends on the processor. For modern CPUs, a threshold of 1500 interrupts/sec is a good start. A dramatic increase in this counter value without a corresponding increase in system activity indicates a hardware problem.

System calls/sec

The number of system calls per second. This is a measure of how busy the system is taking care of applications and services. High System calls/sec indicates high utilization caused by software.

Context switches/sec

The number of context switches per second. High activity rates can result from inefficient hardware or poorly designed applications. The normal amount of Context Switches/Sec depends on your servers and applications.

To set the threshold, baseline the server. The threshold for Context Switches/sec is cumulative for all processors, so you need a minimum of 14000 per processor (single=14000, dual=28000, quad=56000 and so forth).

Kernel threads in run queue

AIX and Solaris: Average number of runnable kernel threads over the sampling interval. Runnable refers to threads that are ready but waiting to run and to those threads already running.

HP-UX: Rename this counter to “Processes in run queue” - average number of runnable processes over the sampling interval.

This should be as low as possible. If the run queue is constantly growing, it may indicate the need for a more powerful CPU or more CPUs.

Kernel threads blocked waiting resources

AIX and Solaris: Average number of kernel threads placed in the VMM wait queue (awaiting resource, awaiting input/output) over the sampling interval.

HP-UX: Rename this counter to “Processes blocked waiting resources” - average number of processes blocked for resources (I/O, paging, and so on) over the sampling interval.

This should be as low as possible.

Total amount of system calls after boot

The total number of system calls after boot.
**Total amount of device interrupts after boot**

The total number of interrupts after boot.

**Total amount of CPU context switches after boot**

The total number of CPU context switches after boot.
Unix Disk Monitoring Perl

This template uses Perl scripts to assess the disk performance of computers running AIX 5.3 or 6.1; Solaris 8, 9, or 10; or HP-UX 11.0.

Prerequisites

SSH and Perl installed on the target server.

If Perl is installed in a location different from /usr/bin/perl, you should correct all components in the first line of the field “script body” (#!/usr/bin/perl), or you can create a symbolic link to Perl (refer to the documentation for the ln command).

You can find where Perl is installed by using the following command: which perl

Credentials

Root credentials on the target server.

Some Unix implementations such as Solaris have a character limit in the input buffers of SSH sessions that prevents SolarWinds SAM from copying over scripts. If a monitored component fails to return a result or returns error code 255, manually copy the script to the target machine and then make the appropriate path and file name change in the Command Line field. For example, if you manually copied the script over as /usr/script.pl, you should change the Command Line to: perl/usr/script.pl.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Components without predetermined threshold values have guidance such as "Use the lowest threshold possible" or "use the highest threshold possible" to help you find a threshold appropriate for your application.

Available space on root (/) partition (MB)

This shows the available space on the root (/) partition in MB.

You should set this threshold according to your Unix installation and your requirements. In the worst case, it should be more than 512 MB.

Used space on root (/) partition (%)

This shows the used space on the root (/) partition in percentage.

Should be less than 95%.

Percent busiest device is in use

The percent of time the busiest device was busy servicing a transfer request. The name of the busiest device can be seen in the message field.
The next command allow you to see all devices currently connected to machine:

- For AIX: `lscfg`
- For Solaris: `cat /etc/mnttab`
- For HP-UX: `ioscan`

If no devices are currently active, the statistic is 0.

Use the lowest threshold possible.

ℹ️ This counter doesn't work on Solaris 8.

**Disk operations/sec of busiest device**

The number of read/write transfers to and from the busiest device. The name of the busiest device can be seen in the message field.

The next command allow you to see all devices currently connected to machine:

- For AIX: `lscfg`
- For Solaris: `cat /etc/mnttab`
- For HP-UX: `ioscan`

If no devices are currently active, the statistic is 0.

Use the lowest threshold possible.

ℹ️ This counter doesn't work on Solaris 8
Unix Memory Monitoring Perl

This template uses Perl scripts to assess the memory performance of computers running AIX 5.3 or 6.1; Solaris 8, 9, or 10; or HP-UX 11.0.

Prerequisites:

SSH and Perl installed on the target server.

If Perl is installed in a location different from /usr/bin/perl, you should correct all components in the first line of the field "script body" (#!/usr/bin/perl), or you can create a symbolic link to Perl (refer to the documentation for the ln command).

You can find where Perl is installed by using the following command: which perl

Credentials

Root credentials on the target server.

Some Unix implementations such as Solaris have a character limit in the input buffers of SSH sessions that prevents SolarWinds SAM from copying over scripts. If a monitored component fails to return a result or returns error code 255, manually copy the script to the target machine and then make the appropriate path and file name change in the Command Line field. For example, if you manually copied the script over as /usr/script.pl, you should change the Command Line to: perl /usr/script.pl.

This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

Monitored Components

Components without predetermined threshold values have guidance such as "Use the lowest threshold possible" or "use the highest threshold possible" to help you find a threshold appropriate for your application.

Total memory (MB)

This shows the amount of total usable RAM in MB.

Used memory (MB)

This shows the amount of used memory in MB.

This should be as low as possible.

Free memory (MB)

This shows the amount of available memory in MB.

This should be more than 100 MB at all times or paging will occur.
Total swap (MB)

This shows the amount of total swap space in MB.

Used swap (MB)

This shows the amount of used swap space in MB. Paging is one of the memory-management schemes by which a computer can store and retrieve data from secondary storage for use in main memory. Paging is an important part of virtual memory implementation in most contemporary general-purpose operating systems, allowing them to use disk storage for data that does not fit into physical random-access memory (RAM).

This should be as low as possible. Ideally it should be near zero. If the value is large, it may indicate that there is no free memory left.

Free swap (MB)

This shows amount of available swap space in MB.

It should be near the “total swap” value. If paging occurs in the system, the value should be as high as possible.

Page faults/sec

AIX and Solaris: Shows the number of page faults per second. This is not a count of page faults that generate I/O, because some page faults can be resolved without I/O.

HP-UX: Rename this counter to “Page address translation faults/sec” – shows the number of page address translation faults per second.

Should be as low as possible.

Zombie processes

This show the number of “zombie” processes. A “zombie” or defunct process is a process that has completed execution, but still has an entry in the process table. This entry is still needed to allow the process that started the (now zombie) process to read its exit status. When a process finishes execution, it will have an exit status to report to its parent process. Because of this last little bit of information, the process will remain in the operating system's process table as a zombie process, indicating that it is not to be scheduled for further execution, but that it cannot be completely removed (and its process ID cannot be reused) until it has been determined that the exit status is no longer needed.

This should always be zero (0). If it is not zero, you should manually kill zombie processes. Use the following commands to show these zombie processes:

- For AIX: `ps -ef | grep defunct`
- For Solaris: `ps -ecl | grep “Z”`
- For HP-UX: `ps -ef | grep defunct`

To kill zombie processes:

- The first option is to wait. It is possible that the parent process is intentionally leaving the process in a zombie state to ensure that future children it may create will not receive the same
pid. Or perhaps the parent is occupied, and will reap the child process momentarily.

- The second option is to send a SIGCHLD signal to the parent (kill -s SIGCHLD <ppid>). This will cause well-behaving parents to reap their zombie children.
- The third option is to kill the parent process of the zombie. At that point, all of the parent’s children will be adopted by the init process (pid 1), which periodically runs wait() to reap any zombie children.

**Page cache: page ins**

Amount of pages paged in from paging space.

The operation of reading one inactive page or a cluster of inactive memory pages to disk is called a page out.

Should be as low as possible.

**Page cache: page outs**

Amount of pages paged in from paging space.

The operation of writing one inactive page or a cluster of inactive memory pages to disk is called a page out.

Value numbers above 20 pages or so indicate a significant performance problem. In this situation more memory should be installed.

---

**Unix Sendmail Monitoring Perl**

This template uses Perl scripts to assess the sendmail performance of computers running AIX 5.3 or 6.1, or Solaris 8, 9, or 10.

**Prerequisites:**

SSH and Perl installed on the target server.

If Perl is installed in a location different from /usr/bin/perl, you should correct all components in the first line of the field "script body" (#!/usr/bin/perl), or you can create a symbolic link to Perl (refer to the documentation for the ln command).

You can find where Perl is installed by using the following command: which perl

**Credentials**

Root credentials on the target server.

---

Some Unix implementations such as Solaris have a character limit in the input buffers of SSH sessions that prevents SolarWinds SAM from copying over scripts. If a monitored component fails to return a result or returns error code 255, manually copy the script to the target machine and then make the appropriate path and file name change in the Command Line field. For example, if you manually copied the script over as /usr/script.pl, you should change the Command Line to: perl /usr/script.pl.
This component has Count statistic as difference enabled. It will return the difference between two polling intervals.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Components without predetermined threshold values have guidance such as "Use the lowest threshold possible" or "use the highest threshold possible" to help you find a threshold appropriate for your application.

Sendmail instances running

This shows how many instances of sendmail daemon are currently started.

- 0 – Sendmail is stopped. Run sendmail manually.
- >1 – Sendmail is up and running.

Daemon: syslog

This shows the status of syslogd daemon (Syslog is a standard for logging program messages).

- 0 – Syslog daemon is stopped. Run syslogd manually.
- 1 – Syslog daemon is up and running.

Disk space usage (kB) of mail folder

This shows the disk space in kB used by the user mailboxes in /var/mail.

Set thresholds according to your requirements.

Disk space usage (kB) of mail queue folder

This shows the disk space in kB used by queued mail in /var/spool/mqueue.

Set thresholds according to your requirements.

Mail queue length

This shows the mail queue length (how many items are in the queue for delivery). This should be as low as possible. If the mail queue value is constantly rising, it may indicate problems with delivering messages.

Set thresholds according to your requirements.

Available space on partition with /var/spool (MB)

This shows the available space on the partition with /var/spool folder in MB.
By default it checks available space on the root (/) partition. If you have created a separate partition /var or /var/spool you need change it in the script (grep "/\$"). You can investigate what partitions you have by using the following command: df

For the /var partition, you should make the following change: change grep "/\$" to grep "/var\$"

For the /var/spool partition, you should make the following change: change grep "/\$" to grep "/var/spool\$"

Set thresholds according to your requirements.
Veeam Backup and Replication Server

The template assesses the overall health and performance of Veeam Backup and Replication Server.

Prerequisites

- WinRM must be installed and properly configured on the target server.
- PowerShell 3.0 should be installed on the Veeam server.
- This template works on 6.x and 7.0 Veeam versions.


Credentials

Administrator on the target server.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Service: Veeam Backup Catalog Service

This monitor returns the CPU and memory usage of Veeam Backup Catalog Service. This service manages and replicates guest OS file system index data files.

Service: Veeam Backup Proxy Service

This monitor returns the CPU and memory usage of Veeam Backup Proxy Service. This service receives and sends virtual machines data over network.

Service: Veeam Backup Service

This monitor returns the CPU and memory usage of Veeam Backup Service. This service manages scheduled jobs and serves Enterprise Manager requests.

Service: Veeam Installer Service

This monitor returns the CPU and memory usage of Veeam Installer Service. This service enables installing, updating, and configuring additional Veeam Backup components.

Service: Veeam vPower NFS Service

This monitor returns CPU and memory usage of Veeam vPower NFS Service. This service implements vPower NFS server enabling you to run virtual machines directly from backup files.

Installer Service TCP Port
This component monitor tests the ability of a Veeam Installer service to accept incoming sessions. By default, it monitors TCP port 6160.

**Transport Service TCP Port**

This component monitor tests the ability of a Veeam Transport service to accept incoming sessions. By default, it monitors TCP port 6162.

**Failed Jobs**

This monitor returns the number of failed jobs and the names of these jobs. The returned value should be zero at all times.

**Job status**

This monitor returns the status of a specific Veeam job. The returned values are as follows:

**Last Job Result**

This component returns the last job result status.

Possible values:

- 0 – Success.
- 1 – None.
- 2 – Failed.
- 3 – Other results.

**Job State**

This component returns the number of incoming NS queries. This record is the authoritative name server for the domain.

Possible values:

- 0 – Stopped.
- 1 – Starting.
- 2 – Working.
- 3 – Stopping.
- 4 – Resuming.
- 5 – Pausing.
- 6 – Other job state.

**Last Session Backup Size**

This component returns the size of the backup of the last session.

**Last Session Compression Ratio**

This component returns the compression ratio of the last session.

**Last Session Data Size**

This component returns the data size of the last session.

**Last Session Deduplication Ratio**

page 958
This component returns the deduplication ratio of the last session.

1. In the Scripts Arguments field, you should provide the correct job name.

Configuring Windows Remote Management (WinRM)

If not already done so, install PowerShell 2.0 or later and WinRM on the SAM and target servers. PowerShell 2.0 can be found here: [http://support.microsoft.com/kb/968930](http://support.microsoft.com/kb/968930).

On the SAM server, open a command prompt as an Administrator. To do this, perform the following step:

1. Go to the Start menu and right-click the cmd.exe and then select Run as Administrator. Enter the following in the command prompt:
   ```
   winrm quickconfig
   winrm set winrm/config/client @{TrustedHosts="*"}
   ```

2. On the target server, open a command prompt as an Administrator and enter the following:
   ```
   winrm quickconfig
   winrm set winrm/config/client @{TrustedHosts="IP_ADDRESS"}
   ```
   where IP address is the IP address of your SAM server.
VMWare

The following templates are available:

- VMware ESX Host
- VMware vCenter Server 5.5

VMware vCenter Server 5.5

This template assesses the status and overall health of VMware vCenter Server.

Prerequisites

- WMI access to the target server.

Credentials

- Windows Administrator on the target server.

Monitored Components

For details on monitors, see [SAM Component Monitor Types](#).

Service: VMware Certificate

This monitor returns CPU and memory usage of VMware Certificate service. This service manages VMware certificates.

Service: VMware Directory

This monitor returns CPU and memory usage of VMware Directory Service. This service is a multi-tenanted, multi-mastered directory service that makes an LDAP directory available.

Service: VMware Identity Management

This monitor returns CPU and memory usage of VMware Identity Management Service.

Service: VMware Kdc

This monitor returns CPU and memory usage of VMware Kdc Service.

Service: VMware Log Browser

This monitor returns CPU and memory usage of VMware Log Browser service. This service enables browsing vSphere log files within the VMware Web Client.

Service: VMware Secure Token

This monitor returns CPU and memory usage of Secure Token service. It is part of VMware Single Sign-On.

Service: VMware USB Arbitration
This monitor returns CPU and memory usage of VMware USB Arbitration service. This service provides arbitration and enumeration of USB devices for virtual machines.

Service: VMware vCenter Inventory
This monitor returns CPU and memory usage of VMware vCenter Inventory service. This service provides centralized inventory and search functions for VMware vCenter objects.

Service: VMware VirtualCenter Management Webservices
This monitor returns CPU and memory usage of VMware VirtualCenter Management Webservices. This service allows configuration of VMware VirtualCenter Management services.

Service: VMware VirtualCenter Server
This monitor returns CPU and memory usage of VMware VirtualCenter Server. This service provides centralized management of VMware virtual machines.

Service: VMware vSphere Web Client
This monitor returns CPU and memory usage of VMware vSphere Web Client Service.

Service: VMware VirtualCenter Server LDAP
This monitor returns CPU and memory usage of VMware VirtualCenter Server LDAP service. This service provides VMware VirtualCenter Server LDAP directory services.

TCP Port: vCenter (HTTP)
This component monitor tests the ability of a vCenter service to accept incoming sessions by using HTTP protocol. It monitors TCP port 80.

TCP Port: vCenter (HTTPS)
This component monitor tests the ability of a vCenter service to accept incoming sessions by using HTTPS protocol. It monitors TCP port 443.

TCP Port: Web Services (HTTP)
This component monitor tests the ability of a VMware Web service to accept incoming sessions by using HTTP protocol. It monitors TCP port 8080.

TCP Port: Web Services (HTTPS)
This component monitor tests the ability of a VMware Web service to accept incoming sessions by using HTTPS protocol. It monitors TCP port 8443.

TCP Port: vCenter LDAP
This component monitor tests the ability of a vCenter LDAP service to accept incoming sessions. It monitors TCP port 389.

TCP Port: vCenter SSL
This component monitor tests the ability of a vCenter SSL service to accept incoming sessions. It monitors TCP port 636.

Warning and Errors: VMware VirtualCenter Server
This monitor returns VMware VirtualCenter Server warning and error events.

**Source name:** VMware VirtualCenter Server.

Log file: Application.
VMware ESX Host

This template reads the specified VMware performance counter data using the VMware vSphere Web Services API.

Prerequisites

The currently used vSphere Web Services API version is 4.0, which supports vSphere 4.0 servers and also is compatible with previous releases of ESX/ESXi, including the following: ESX/ESXi 3.5.x or later.

The vSphere Web Services SDK package includes WSDL files for vSphere API 4.0, which is a superset of API versions starting with API 2.5, and for VI API 2.0.

Credentials

Access to VMware performance counter data using the VMware vSphere Web Services API.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

**CPU.CPU Reserved Capacity.average**

This component monitor collects server resource information from VMware ESX server for the average CPU reserved capacity, providing most common data for monitoring VMware resources health state.

**CPU.CPU Usage (Average).average**

This component monitor collects server resource information from VMware ESX server for the average CPU usage, providing most common data for monitoring VMware resources health state.

**CPU.CPU Usage in MHz (Average).average**

This component monitor collects server resource information from VMware ESX server for the average CPU usage in MHz, providing most common data for monitoring VMware resources health state.

**Disk.Disk Usage (Average).average**

This component monitor collects server resource information from VMware ESX server for the average disk usage, providing most common data for monitoring VMware resources health state.

**Memory.Memory Active (Average).average**

This component monitor collects server resource information from VMware ESX server for the average active memory, providing most common data for monitoring VMware resources health state.
Memory.Memory Balloon (Average).average
This component monitor collects server resource information from VMware ESX server for the average memory ballooning for guest VMs, providing most common data for monitoring VMware resources health state.

Memory.Memory Consumed (Average).average
This component monitor collects server resource information from VMware ESX server for the average memory consumed, providing most common data for monitoring VMware resources health state.

Memory.Memory Granted (Average).average
This component monitor collects server resource information from VMware ESX server for the average memory granted, providing most common data for monitoring VMware resources health state.

Memory.Memory Heap (Average).average
This component monitor collects server resource information from VMware ESX server for the average memory heap for the VM, providing most common data for monitoring VMware resources health state.

Memory.Memory Heap Free (Average).average
This component monitor collects server resource information from VMware ESX server for the average free memory heap for the VM, providing most common data for monitoring VMware resources health state.

Memory.Memory Overhead (Average).average
This component monitor collects server resource information from VMware ESX server for the average memory overhead, providing most common data for monitoring VMware resources health state.

Memory.Memory Reserved Capacity.average
This component monitor collects server resource information from VMware ESX server for the average capacity for reserved memory, providing most common data for monitoring VMware resources health state.

Memory.Memory Shared (Average).average
This component monitor collects server resource information from VMware ESX server for the average amount of memory shared with other VMs, providing most common data for monitoring VMware resources health state.

Memory.Memory Shared Common (Average).average
This component monitor collects server resource information from VMware ESX server for the average memory shared by all powered-on VMs, providing most common data for monitoring VMware resources health state.
Memory.Memory State.latest
This component monitor collects server resource information from VMware ESX server for the latest state of the memory, providing most common data for monitoring VMware resources health state.

Memory.Memory Swap In (Average).average
This component monitor collects server resource information from VMware ESX server for average memory swapped in from disk, providing most common data for monitoring VMware resources health state.

Memory.Memory Swap Out (Average).average
This component monitor collects server resource information from VMware ESX server for the average memory swapped out to disk, providing most common data for monitoring VMware resources health state.

Memory.Memory Swap Used (Average).average
This component monitor collects server resource information from VMware ESX server for the average memory used by the swap, providing most common data for monitoring VMware resources health state.

Memory.Memory Unreserved (Average).average
This component monitor collects server resource information from VMware ESX server for the average memory unreserved, providing most common data for monitoring VMware resources health state.

Memory.Memory Usage (Average).average
This component monitor collects server resource information from VMware ESX server for the average memory usage, providing most common data for monitoring VMware resources health state.

Memory.Memory Used by vmkernel.average
This component monitor collects server resource information from VMware ESX server for the average memory used by the vmkernel, providing most common data for monitoring VMware resources health state.

Memory.Memory Zero (Average).average
This component monitor collects server resource information from VMware ESX server for the average memory zero areas, providing most common data for monitoring VMware resources health state.

Network.Network Usage (Average).average
This component monitor collects server resource information from VMware ESX server for the average network usage, providing most common data for monitoring VMware resources health state.

System.Uptime.latest
This component monitor collects server resource information from VMware ESX server for the latest uptime for the system, providing most common data for monitoring VMware resources health state.
Web Link

This template validates the hyperlinks on the web page served by the target web server. If any hyperlinks are invalid or unreachable, the test fails. The statistic is the number of invalid or unreachable hyperlinks.

**Prerequisites**

None.

**Credentials**

None.

Monitored Components

For details on monitors, see [SAM Component Monitor Types](#).

**Web Link Monitor**

This component monitor collects the number of broken or invalid links on a web page.
Websense Web Security

This template assesses the status and overall health of services as well as the performance of the Websense Web Security.

Prerequisites

WMI access to the target server.

Credentials

Windows Administrator on the target server.

This template was created on Websense Web Security v 7.7.3.

Monitored Components

For details on monitors, see SAM Component Monitor Types.

Service: Websense Control Service

This monitor returns CPU and memory usage of Websense Control Service. It is responsible for service configuration and management.

Service: Websense Filtering Service

This monitor returns CPU and memory usage of Websense Filtering Service. It interacts with your integration product and Network Agent to filter Internet requests. Filtering Service either permits the Internet request or sends an appropriate block message to the user.

Service: Websense Log Server

This monitor returns CPU and memory usage of Websense Log Server. It sends records of Internet activity to the Log Database. It also sends category names, protocol names, and risk class names from the Master Database to the Log Database.

Service: Websense Network Agent

This monitor returns CPU and memory usage of Websense Network Agent. In a stand-alone deployment, Network Agent manages the filtering of all protocols, including HTTP, HTTPS, and FTP. Network Agent detects network activity to support the bandwidth filtering and protocol management features, and to log the number of bytes transferred. In an integrated deployment, Network Agent is optional. In this case, Network Agent manages the Internet protocols that are not managed by your integration product. Network Agent can also be used to detect HTTP network activity and instruct Filtering Service to log this information.
**Service: Websense Policy Broker**

This monitor returns CPU and memory usage of Websense Policy Broker. It manages requests from Websense components for policy and general configuration information.

**Service: Websense Policy Database**

This monitor returns CPU and memory usage of Websense Policy Database. It stores Websense software settings and policy information. This database is installed with Policy Broker, and cannot be installed separately.

**Service: Websense Policy Server**

This monitor returns CPU and memory usage of Websense Policy Server. It identifies and tracks the location and status of other Websense components. Stores configuration information specific to a single Policy Server instance. Communicates configuration data to Filtering Service, for use in filtering Internet requests.

**Service: Websense TRITON - Web Security**

This monitor returns CPU and memory usage of Websense TRITON Web Security. It responds for configuration, management, and reporting interface to Websense software.

**Service: Websense TRITON Unified Security Center**

This monitor returns CPU and memory usage of Websense TRITON Unified Security Center. It is an application server for TRITON Unified Security Center.

**Service: Websense Information Service for Explorer**

This monitor returns CPU and memory usage of Websense Information Service for Explorer. Provides communication between Policy Server and other Websense components.

**TCP Port: Policy Server - Negotiate Encryption**

This component monitor tests the ability of Policy Server to accept incoming sessions by using negotiate encryption. By default it monitors TCP port 55807.

**TCP Port: Policy Server - Configuration Exchange**

This component monitor tests the ability of Policy Server to accept incoming sessions for configuration exchange. By default it monitors TCP port 55806.

**TCP Port: Network Agent**

This component monitor tests the ability of Network Agent to accept incoming sessions. By default it monitors TCP port 55811.

**TCP Port: Log Server**

This component monitor tests the ability of Log Server to accept incoming sessions. By default it monitors TCP port 55812.
TCP Port: Triton Web Security
This component monitor tests the ability of Triton Web Security to accept incoming sessions. By default it monitors TCP port 55824.

TCP Port: Policy Broker
This component monitor tests the ability of Policy Broker to accept incoming sessions. By default it monitors TCP port 55880.

TCP Port: Explorer Information Service
This component monitor tests the ability of Explorer Information Service to accept incoming sessions. By default it monitors TCP port 55818.

TCP Port: Master Database
This component monitor tests the ability of Master Database to accept incoming sessions. By default it monitors TCP port 80.

TCP Port: SQL Server Communication
This component monitor tests the ability of SQL Server Communication to accept incoming sessions. By default it monitors TCP port 1433.

TCP Port: Logging Port
This component monitor tests the ability of Logging Server to accept incoming sessions. By default it monitors TCP port 55805.

TCP Port: Admin TRITON console
This component monitor tests the ability of TRITON Admin console to accept incoming sessions. By default it monitors TCP port 9443.

Warning and Errors Events: Websense Reporter Scheduler
This monitor returns the number of Websense Reporter Scheduler warning and error events.
Source Name: Websense Reporter Scheduler.

By default, this monitor is disabled.

Warning and Errors Events: Websense EIM Server
This monitor returns the number of Websense EIM Server warning and error events.

By default, this monitor is disabled. Before using this monitor you should provide correct Source Name: Websense EIM Server@IP - where IP is the IP address of the Websense server.

Warning and Errors Events: Websense Log Server
This monitor returns the number of Websense Log Server warning and error events.
By default, this monitor is disabled. Before using this monitor you should provide correct Source Name: WebsenseLogServer@IP - where IP is the IP address of the Websense server.

**Warning and Errors Events: Websense Network Agent**

This monitor returns the number of Websense Network Agent warning and error events.

By default, this monitor is disabled. Before using this monitor you should provide correct Source Name: Websense Network Agent@IP - where IP is the IP address of the Websense server.

**Warning and Errors Events: Websense WF Report Server**

This monitor returns the number of Websense WF Report Server warning and error events.

By default, this monitor is disabled. Before using this monitor you should provide correct Source Name: Websense WF Report Server@IP - where IP is the IP address of the Websense server.

**Warning and Errors Events: Websense Communication Agent**

This monitor returns the number of Websense Communication Agent warning and error events.

By default, this monitor is disabled. Before using this monitor you should provide correct Source Name: Websense Communication Agent@IP - where IP is the IP address of the Websense server.

**Warning and Errors Events: Websense Policy Server**

This monitor returns the number of Websense Policy Server warning and error events.

Before using this monitor you should provide correct Source Name: Websense Policy Server@IP - where IP is the IP address of the Websense server.