Server & Application Monitor

Version 2020.2
GETTING STARTED GUIDE: SERVER & APPLICATION MONITOR

© 2020 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

- **Get started with Server & Application Monitor** .......................................................... 5
  - Who this guide is for ........................................................................................................ 5
  - Product terminology ....................................................................................................... 7
  - How SAM works ............................................................................................................. 8
  - Navigate through your SAM environment ..................................................................... 12
  - Explore SAM widgets ................................................................................................... 14

- **Discover your SAM environment** ............................................................................. 17
  - What should I monitor in SAM? ................................................................................... 17
  - Discover your servers and applications in SAM ....................................................... 21
  - Add discovered servers and applications to SAM ....................................................... 24

- **Set up monitoring in your SAM environment** ......................................................... 28
  - Use AppInsight for IIS to monitor an IIS server ....................................................... 29
  - Monitor your operating system .................................................................................... 32
  - Monitor hardware health in SAM ................................................................................. 36
  - Monitor cloud instances and VMs ................................................................................ 38
  - Introduction to AppStack .............................................................................................. 40
  - Investigate application performance with PerfStack ............................................... 43

- **Explore alerts and reports in SAM** .......................................................................... 48
  - How alerts work in SAM .............................................................................................. 48
  - Work with preconfigured alerts in SAM .................................................................... 50
  - Create a custom alert in SAM ...................................................................................... 56
  - How reports work in SAM ............................................................................................ 60
  - Run a preconfigured report in SAM ............................................................................. 61
  - Create a custom SAM report ....................................................................................... 64

- **Work with SAM templates** ...................................................................................... 73
Understand the application/template relationship .................................................................74
Create custom templates in SAM ...........................................................................................75
Set thresholds in SAM ............................................................................................................78
Get started with Server & Application Monitor

This guide picks up right after the SAM installation process and walks you through the first steps you need to take to monitor applications, hardware health, asset inventory, and operating performance in your SolarWinds SAM environment.

After learning how SAM works, you can start exploring the Orion Web Console, which you’ll use to do everything in SAM, from discovering applications to setting up alerts, thresholds, and application monitoring templates.

Additional sections in this guide include:

- **Discover your SAM environment**: Identify the servers and applications you want to monitor and add them to SAM.
- **Set up monitoring in your SAM environment**: Learn how to use AppInsight for IIS, monitor an OS, track hardware health, monitor your cloud infrastructure, work with AppStack™, and use PerfStack™.
- **Explore alerts and reports in SAM**: Manage and use alerts, and then set up reports.
- **Work with SAM templates**: Explore application monitor templates included in SAM and create templates for custom applications.
- **Set thresholds in SAM**: Learn how to set up global and local thresholds to automate monitoring.

Who this guide is for

<table>
<thead>
<tr>
<th>New SAM users</th>
<th>Existing SAM users</th>
</tr>
</thead>
<tbody>
<tr>
<td>This guide is the best place to start with SAM. When finished, move on to the <a href="#">SAM Administrator Guide</a> for more advanced information.</td>
<td>This guide provides a high-level view of SAM features but you’ll find more advanced information in the <a href="#">SAM Administrator Guide</a>.</td>
</tr>
</tbody>
</table>

Existing customers: Access your licensed software from the [SolarWinds Customer Portal](#). If upgrading from SAM 6.9 or later, you can upgrade via the Settings > My Orion Deployment page. For implementation help, contact [Customer Support](#). See [Working with Support](#) to learn how to open a support case with the correct level of visibility.
**Evaluators:** To evaluate SAM, download a **free 30-day evaluation** that is a full version of the product, functional for 30 days. After the evaluation period, you can easily convert your evaluation license to a production license by obtaining and applying a license key. If you need assistance during evaluation, contact sales@solarwinds.com.

Here are additional learning resources for SAM:

- Review the [system requirements](#) and [release notes](#) before installing SAM.
- To upgrade SAM, see the [Orion Platform Installation and Upgrade Guide](#).
- The [SAM Administrator Guide](#) describes how to use product features and related technologies. It also contains recommendations on best practices, and troubleshooting information for common situations.
- Use [SAM online help](#) to explore individual widgets that appear on SAM views in the Orion Web Console. Online help includes information from the main SAM documentation set, plus additional troubleshooting topics.
- To learn about features shared by SAM and other Orion Platform products, such as user accounts, views, dashboards, and alerts, see the [Orion Platform Administration Guide](#). Use this document to fine-tune your SAM deployment by working with custom properties and groups, creating custom views, reducing alerting noise, and more.
- Visit the [SolarWinds Success Center](#) for product guides, training resources, and technical support articles.
- Use the [Server & Application Monitor product forum](#) in our online IT community, THWACK, to connect with SolarWinds developers, product managers, and other SAM users. Download templates, reports, and scripts to customize and extend SAM.
Product terminology

**Orion Platform:** The common backend platform used by the SolarWinds Orion Platform suite of products, including NPM, SAM, NCM, NTA, WPM, and more. The Orion Platform is the backbone for navigation, settings, and common features like alerts and reports. It also provides a consistent look-and-feel across products, giving you a "single pane of glass" for your Orion monitoring tools.

**Orion Web Console:** The web interface you see when you log into the Orion Web Console that is used to view, configure, and manage monitored objects.

**Orion server:** A Microsoft Windows server that hosts the Orion Web Console and collects data from monitored objects. Also called the Orion Main Poller or Main Polling Engine.

**Orion database server:** A dedicated server that hosts the Orion database that is separate from the Orion server. It stores Orion Platform configuration data plus collected performance and Syslog data.

**Polling engine:** A polling engine controls polling job scheduling, data processing, and queries your monitored devices for performance metrics like CPU, memory, and up/down status. By default, the Orion server provides one polling engine, that is often called the "Main Polling Engine." You can add Additional Polling Engines (APEs) to provide enhanced scalability and capacity, as described in the [Scalability Engine Guidelines](#).

**Node:** A node is an endpoint of a given network. For example, any application, server, device, or computer on a network is considered a node.

**Template:** A template is the blueprint for an application. It is a collection of component monitors designed to monitor a server or application. You can customize numerous templates using only the component monitors you need for a specific environment. For a list of out-of-the-box templates included in SAM, see the [SAM Template Reference](#).

**Application:** An application or application monitor in SAM monitors a specific application or server using a collection of component monitors.

**Component Monitor:** A component monitor is the fundamental element of an application or application monitor. Component monitors return the current status or value of a monitored service or process. All component monitors return at least one value or one status condition. Click [here](#) for a list of component monitors,
How SAM works

Using UDP, TCP, SNMP, WMI, and WinRM calls to your environment and application servers, SAM provides real-time feedback about applications and trends through statistics stored in the Orion database. Thanks to the SolarWinds common components infrastructure, there are no agents installed on your servers and no remote software to maintain. All calls are made in real time and displayed in the Orion Platform accessible from any supported browser.

As a standalone product, SAM operations can be visualized with the following flowchart:
Installed as a module in your family of SolarWinds products, SAM can be visualized with the following flowchart:

SAM includes many features that are common to all Orion Platform products, including user accounts, views, alerts, and reports. To learn more, see the [Orion Platform Administration Guide](#).
Understand how SAM uses Orion agents

An Orion agent is software that provides a communication channel between the Orion server and a monitored computer. Agents are used as an alternative to WMI or SNMP to provide information about selected devices and applications.

SAM uses Orion agents to gather information for component monitors (and their parent application monitors) from target servers across your environment. Agents are also used to monitor servers hosted by cloud-based services such as Amazon EC2, Rackspace, Microsoft Azure, and other Infrastructure as a Service (IaaS) products.

Using the Orion agent instead of traditional polling methods can provide many advantages, including the ability to:

- Poll hosts and applications behind firewall NAT or proxies.
- Perform secure, encrypted polling over a single port.
- Poll nodes across:
  - Multiple discrete networks with overlapping IP addresses.
  - Low bandwidth, high latency connections.
  - Domains where no domain trusts are established.
- Leverage full, end-to-end encryption between the monitored host and the Main Polling Engine, which is usually the Orion server.

After agent deployment, all communication between the Orion server and the agent occur over a fixed port. The agent protocol supports Network Address Translation (NAT) traversal and passing through proxy servers that require authentication.

If an agent is used, all SAM application data is collected by the agent. You can override this behavior at both the template and application monitor level to use another polling method. For example, if a SAM template includes a User Experience Monitor but you do not want to measure response time locally from the server where the application is installed, you can switch to Agentless polling. To learn more, see Decide between agent vs. agentless polling methods in the SolarWinds Success Center.
Agent communication modes

You can configure agent communication modes that determine how the agent and the Orion server communicate. This is frequently influenced by where the device you want to monitor is on your network.

- **Server initiated communication**: Any communication between the Orion server or additional polling engines and the agent is initiated by the Orion server itself. To allow communication from the Orion server, the firewall service running on the monitored device or the network firewall must allow incoming connections through port 17790. If the agent is configured to use another port, update the firewall rules to allow incoming connections from the other port.

  This communication method is also known as a passive agent.

- **Agent initiated communication**: Any communication between the Orion server or additional polling engines and the agent service is initiated by the agent service itself. Update your firewall rules to allow outgoing connections through port 17778 to enable communication between the agent and the Orion server. Open port 17791 if the agent is on a Windows 2008 R2 server.

  This communication method is also known as an active agent. In active mode, there are no listening ports on the agent.

To learn more about agents, see [Monitor with Orion agents in SAM](#) and also the [Orion Platform Administrator Guide](#).
Navigate through your SAM environment

As with all Orion Platform products, you can access SAM in a web browser by navigating to http://hostnameOrIPAddress:port where:

- hostnameOrIPAddress is the hostname or IP address of the Orion server where SAM is installed.
- port is the port defined for the Orion Web Console website, as configured during initial deployment. The default port is 8787.

When the Login page appears, provide a User name and Password, and then click Login to access the Orion Web Console, where you’ll view, configure, and manage your monitored objects. You can access the Orion Web Console from any computer connected to the Internet.

The Orion Web Console consists of various pages known as views for which there are two main types: high-level Summary views and in-depth Detail views. Views contain informational blocks called widgets that display data for different aspects of monitoring, usually in a chart or table. Some widgets are intended for use on Summary views, some are suitable for Detail views, and some can be useful on both view types.

💡 Check out this video about navigating the Orion Web Console.
The following figure shows several widgets in the Application Summary view, a page you can access by clicking My Dashboards > Applications > SAM Summary in the Orion Web Console:

Some views and widgets are not visible by default and can be added by editing settings. To learn more, see Customize the Orion Web Console.
Explore SAM widgets

Most widgets (formerly called "resources") in the SAM environment are actionable. For example, drilling down to and clicking an individual node in the All Nodes widget on the Summary page takes you to the Node Details page. The Node Details page contains widgets that provide information about this node.

Watch Customizing SAM views and widgets (3:08).

The following example shows the Management widget, one of many widgets available on the Node Details page.

Click Manage Nodes in the All Nodes widget to open the Manage Nodes view where you can take action on multiple nodes.
Use the All Applications widget on the Summary page to drill down to individual applications and component monitors of an application. The Application Details page provides details about the individual application and actions you can perform on that application. This allows you to manage templates and applications to node assignments, or "unmanage" (that is, stop managing) multiple applications at one time.

Click Manage Applications in the All Applications widget to open the Manage Applications page where you can troubleshoot and resolve issues on multiple applications.
Expand an application name to show all component monitors associated with that application. Click a component monitor to access the Component Monitor details page to view detailed information and perform additional actions.

To learn about individual widgets, see SAM online help.
Discover your SAM environment

After installing SAM, identify the network objects that you want to add to the Orion database for monitoring.

- To automatically discover and add a large number of network objects, use the Network Sonar Discovery and Network Sonar Results Wizards. For an overview, watch this video.
- To add individual network objects for monitoring, you can also add single nodes in the Orion Web Console, as shown in this video.

For SAM, the Orion Platform term "network objects" refers to servers and applications.

Before you build your environment, we recommend reviewing these topics:

- What should I monitor in SAM?
- Discover your servers and applications in SAM
- Add discovered servers and applications to SAM

See the Orion Platform Administrator Guide to learn about related functionality shared by multiple Orion Platform modules, such as how to:

- Add nodes using Active Directory
- Choose polling methods
- Import nodes
- Manage scheduled discovery results
- Minimize SNMP processing load during Discovery
- Group objects and mirroring network dependencies

What should I monitor in SAM?

Discovery is a term that describes how the Orion Platform identifies network elements. During Discovery, the system scans the network for application servers and applications that you can add to the Orion database for monitoring. For details, see Discover your network with the Discovery Wizard.

SAM can monitor an application, or you can configure SAM to monitor a custom collection of application components, process monitors, services, and performance counters. Depending on your needs, SAM can assess the status of every aspect of your application, and the health of the application as a whole.
SAM also monitors Amazon Web Services (AWS) cloud instances and Microsoft Azure VMs. With access to your cloud services account, SAM can poll cloud service APIs for cloud metrics and status. This data aggregates and displays through the Orion Web Console to monitor, manage, and troubleshoot issues in your cloud environment. See Manage your cloud infrastructure for details.

SolarWinds recommends adding a limited number of servers and applications to begin monitoring and gauging performance, including Microsoft Exchange, IIS, SQL, Linux, and Unix. After monitoring, alerts, and reports are set up, continue adding applications and servers to expand your infrastructure monitoring.

Discovery checklist

When you run the Discovery Wizard (also called the "Network Sonar Wizard"), you'll be prompted to provide IP addresses and credentials for servers you want to monitor. SolarWinds recommends gathering these details before running the wizard.

- Determine the devices you want to monitor.
- Determine the protocol used to monitor devices, such as SNMP or WMI. See the Monitoring overview for details.
- Gather IP ranges or individual IP addresses you want the system to scan as it discovers your network.
- Collect SNMP v1/2c community strings and SNMP v3 community strings and credentials of the servers you want to monitor.
- Obtain login credentials for each monitored server, including
  - VMware host credentials: The Orion Platform requires at least read-only permissions.
  - Windows credentials: domain or local admin.
- For AWS cloud monitoring, add an AWS IAM user account (up to 10) and Account Access Key ID and Secret Access Key for access. For more details, including required permissions, see Configure AWS accounts for cloud monitoring.
- For Microsoft Azure cloud monitoring, configure Azure to interact with the Orion Platform before adding an Azure cloud account to the Orion Web Console. Each account requires sufficient Azure Active Directory (AD) and subscription permissions to add an AD app in the Azure Portal so the Orion Platform can retrieve status and metrics for VMs. IAM permissions must also be set up.

  Visit the SolarWinds Success Center and review Configure Microsoft Azure for cloud monitoring in the Orion Platform for details.
Monitoring overview

You can configure an application or template to collect data through a preferred polling method as agent or agentless.

Monitor with Orion agents

An agent is software that provides a communication channel between the Orion server and a Windows or Linux computer. Products install plugins on agents to collect the data that the agents send back. Orion agents are available for Windows and Linux. For requirements and information, see Monitoring with Orion agents in SAM.

Monitor with SNMP

To monitor devices using SNMP, you must enable SNMP on those devices because it is not enabled by default. SNMP is primarily used to monitor network devices, for example, routers, firewalls, and switches. To enable SNMP, consult the device vendor documentation.

When configuring SNMP-enabled network devices for monitoring, note these details:

- Steps to enable SNMP communications differ by device; consult the documentation provided by your device vendor.
- For correct device identification, monitored devices must allow access to the SysObjectID.
- Unix-based devices should use the version of Net-SNMP (5.5 or later) that is specific to the Unix-based operating system in use.
- If SNMPv2c is enabled on a device, NMPv2c is used to poll the device for performance details by default. To poll with SNMPv1, disable SNMPv2c on the device to be polled.
- SolarWinds SAM can monitor VMware ESX and ESXi Servers versions 4.0 and later.
- Linux/Unix servers are generally monitored with SNMP and SSH Script Monitors that require user credentials.

💡 VMware Tools is not required on virtual machines (VMs) running on monitored ESXi and ESX servers, but additional details such as IP addresses are made available if VMware Tools is installed on VMs hosted by monitored ESXi and ESX Servers.

Monitor with WMI

If monitoring Windows servers, use Windows Management Instrumentation (WMI), which is usually enabled on Windows devices by default. Capable of gathering more data than SNMP, WMI is the preferred polling method because some SolarWinds SAM features are not available if you use SNMP.
Agentless monitoring using WMI is not recommended when the polling engine and the device are separated by a firewall. To overcome this limitation, SolarWinds provides an optional agent that allows you to securely monitor Windows servers and applications by WMI. If you want to use SNMP for Windows, then you must install and configure an SNMP agent.

Starting in SAM 2020.2, WinRM is the default polling method for WMI-based component monitors. For details, see Use WinRM for application monitor polling.

Deciding between SNMP and WMI

SNMP is typically used to monitor servers and network devices without agents. For Windows servers, WMI usually provides better metrics than can be obtained through SNMP monitoring alone. For many Windows-based servers and applications, agentless monitoring via the WMI gateway provides strong monitoring capabilities.

The availability of some features depends on which Orion Platform modules you’re using. For example, NPM supports polling via WMI, SNMP, and agents. However, interface polling via WMI and the Orion Agent is not supported unless you have a SAM license. You must use SNMP as a polling method to obtain interface data in an NPM-only installation. For details, see Polling methods used by the Orion Platform.

To learn more, see:

- Choose the polling method to use in the Orion Platform (Orion Platform Administrator Guide)
- Monitor with Orion agents in SAM (SAM Administrator Guide)
- Feature availability based on monitoring methods (Success Center)
Discover your servers and applications in SAM

*Discovery* is a term that describes how the Orion Platform identifies application servers and applications. Before you begin:

- Ensure that you determine what to monitor.
- Enable Windows devices for WMI.
- Enable the networking devices you want to monitor for SNMP.

Watch [this video](#) about discovering your servers and applications. To learn more, see the Orion Platform Administrator Guide.

The first time you run the Discovery Wizard (also called the "Network Sonar Wizard"), SolarWinds recommends adding a limited number of application servers, including Exchange, IIS, SQL, Linux, and Unix. The examples in this guide focus on monitoring IIS and the operating system of your application server, but the same steps apply to monitoring any application.

1. If the Discovery Wizard does not start automatically after configuration, click Settings > Network Discovery.
2. Click Add New Discovery, and then click Start.
3. On the Network panel, if this is your first Discovery, add a limited number of IP addresses.

As you scale your implementation, you can use the following scanning options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP Ranges</strong></td>
<td>Use this option when you want the Orion Platform to scan one or more IP ranges. If you have many IP ranges to scan, consider adding multiple Discovery jobs rather than including all ranges in a single job.</td>
</tr>
<tr>
<td><strong>Subnets</strong></td>
<td>Use this option to scan every IP address in a subnet. SolarWinds recommends scanning at most a /23 subnet (512 addresses max). Scanning a subnet returns everything that responds to ping, so we recommend only scanning subnets where most devices are objects you want to monitor.</td>
</tr>
<tr>
<td><strong>IP Addresses</strong></td>
<td>Use this option for a limited number of IP addresses that do not fall in a range. Since a network discovery job can take a long time to complete, SolarWinds recommends using this option when you are first starting out.</td>
</tr>
</tbody>
</table>
Use this option to scan an Active Directory Domain Controller.

Using Active Directory for Discovery is particularly useful for adding large subnets because Orion can use the devices specified in Active Directory instead of scanning every IP address.

4. The Agents panel appears. The QoE agent monitors packet-level traffic. If there are any nodes using agents, select the Check all existing nodes.

   This setting ensures that any agents you deploy, including the one on your Orion server, are up-to-date. If there are no nodes using agents, you can leave this option unchecked.

5. On the Virtualization panel, to discover VMware vCenter or ESX hosts on your network, enter the credentials, and click Next.

6. On the SNMP panel, to monitor an SNMP-enabled device, enter the credentials, and click Next.

7. On the Windows panel, to discover WMI or RPC-enabled Windows devices, click Add New Credential and provide the required information.

   🟢 SolarWinds recommends that you monitor Windows devices with WMI instead of SNMP.
8. On the Monitoring Settings panel, SolarWinds recommends manually setting up monitoring the first time you run Discovery so you can review the list of discovered objects and select what you want to monitor. Otherwise, you can configure Discovery to automatically start monitoring objects it finds.


10. Accept the default frequency and run the Discovery immediately.
Discovery can last from 5 minutes to several hours, depending on the number of servers involved.

If the status of a node remains Unknown after Discovery, see Troubleshoot nodes and interfaces that are Unknown.

Add discovered servers and applications to SAM

After the Discovery Wizard analyzes available devices and interfaces in your network, the Network Sonar Results Wizard opens, allowing you to import network elements into SAM. Discovered servers (that is, nodes) do not count against node-based licensing; only servers that you import into the Orion database count against your license.

When you run Discovery manually, the system automatically selects all network elements to be monitored. You must clear the check boxes for elements you do not want monitored. This example highlights Windows devices with IIS.

Before you begin, ensure that you discover your servers and applications.

If discovering your network for the first time, SolarWinds recommends monitoring a small number of critical servers.
1. Make sure that only the device types you want to monitor are selected, and click Next.

![Network Sonar Results Wizard](image)

- After Discovery, if the status of a node is Unknown, you may need to check settings in SolarWinds NPM. See [Troubleshoot Unknown Nodes](#).

2. Ensure the interfaces you want to monitor are selected, and click Next.

SolarWinds recommends that you do not monitor WAN, QoS, multi-port, and virtual NIC interfaces.

![List of Interfaces](image)

- SolarWinds SAM only discovers interfaces on WMI nodes.

3. Ensure the volume types you want to monitor are selected, and click Next.

SolarWinds recommends that you do not monitor compact disks and removable disks.
4. Select the applications to monitor, and click Next.

5. Review the list of elements to be imported, and click Import.

6. On the Results tab, click Finish.
7. Click My Dashboards > SAM Summary.

The SAM Summary view widgets may take several minutes to populate with data.

---

**All Applications**

**GROUPED BY APPLICATION TEMPLATE, NODE NAME**

- **AppInsight for IIS**
  - All applications up
- **AppInsight for SQL**
  - All applications up
Set up monitoring in your SAM environment

This section describes how to configure basic monitoring for your environment and includes the following topics:

- Use AppInsight for IIS to monitor an IIS server
- Monitor your operating system
- Monitor hardware health in SAM
- Monitor cloud instances and VMs
- Introduction to AppStack
- Investigate application performance with PerfStack

For more advanced monitoring topics, see these sections of the [SAM Administrator Guide]:

- Monitor with Orion agents
- Monitor your virtual infrastructure
- Monitor your environment using AppStack
- Use API pollers to monitor metrics via remote APIs
- Monitor application dependencies
- Use SAM templates, application monitors, and component monitors
- Monitor with AppInsight applications
- Use alerts to monitor your SAM environment
- Monitor processes, services, tasks, and events in real time with SAM

See the [Orion Platform Administrator Guide] to learn how to:

- Integrate SAM with ServiceNow®
- Group monitored objects
- Monitor Cisco UCS Devices
- Monitor container services
- Monitor hardware health for Nutanix clusters
- Monitor SNMP traps
- Monitor Quality of Experience (QOE) metrics
- Optimize and scale Orion Platform products
- View events, alerts, traps, and Syslogs in the Orion Web Console Message Center
Use AppInsight for IIS to monitor an IIS server

SAM includes a set of specially-designed AppInsight templates that you can assign to nodes to monitor key business tools such as Microsoft IIS. These "super templates" include a variety of component monitors that provide a comprehensive level of detail beyond what other templates can provide, allowing you to monitor virtually every aspect of your application.

SAM provides the following AppInsight applications:

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

This example explains how to assign the AppInsight for IIS template to any WMI node running IIS, which provides you with:

- Control over web sites and application pools
- Separate, detailed metrics on each website or pool, instead of just a summary level
- Monitoring log space usage on each website individually, ASP.NET requests monitoring
- SSL expiration monitoring

If you added AppInsight for IIS to a node during Discovery, skip to [View IIS application data](#) to get started.

Add AppInsight for IIS to an existing WMI node

1. In the Orion Web Console, navigate to the Node Details page of any WMI node running IIS.

   You must know which nodes are running IIS.

2. From the Management widget, click List Resources.

   ![Management widget](image)

3. Select Microsoft IIS to enable AppInsight for IIS data collection, then click Submit.

   List Resources shows all monitorable features of a node.
4. Click the All Applications widget to verify the addition by clicking the Applications.

5. Enter your IIS credentials when prompted, and click Configure Server.

For troubleshooting information, see Troubleshoot AppInsight for IIS.
View IIS application data

SolarWinds SAM displays IIS data in views. The type of view determines the level of detail. For example, the AppInsight for IIS Details view provides a rollup of information about that IIS server, including statistics about all the sites on the server, application pools, and connections.

Navigate to the AppInsight for IIS Application Details view

1. Click My Dashboards > Applications > IIS to open the IIS Application Summary view.
2. In the All Applications widget, expand a node, drill down, and click Microsoft IIS to open the Application Details view.
3. Click an IIS application to view.

The AppInsight for IIS Application Details view includes different widgets that display details for sites, applications pools, and more. Click hyperlinks in each widget to learn more about the data.

For example, click a website link in the Sites widget to open the IIS Site Details view for that website. To return to the AppInsight for IIS Application Details view, click the Back button in your browser.

Navigate to the Performance Counter Details view

From the AppInsight for IIS Details view, click a performance counter in any widget to open the IIS Statistic Details view for the counter. For example, click ASP.NET > Requests Rejected.
An Expert Knowledge widget appears on IIS Statistic Details view for each performance counter. General information about the selected counter, along with possible problems and troubleshooting steps, where applicable. Find expert knowledge on the Performance Counter Details view.

**Expert Knowledge**

**Description:**
This displays the number of milliseconds that the most recent request was waiting in the queue.

**Information:**
This does not include any time spent waiting in application queues. The threshold for this counter is 1,000.

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

### What’s next

AppInsight for IIS can help you monitor and troubleshoot IIS. However, a software monitoring solution cannot detect failed hardware issues, such as insufficient RAM or a failed cooling fan. To detect hardware issues, [Hardware Health monitoring](#) must be enabled.

## Monitor your operating system

SAM provides over 250 out-of-the-box templates that you can use to monitor business-critical applications. You can assign these templates as-is to nodes, or create copies to modify settings or add and modify component monitors. SolarWinds recommends deploying a single template, making necessary edits to customize it to your environment, and then deploying the edited template on all similar applications. To learn more about templates, see [Work with SAM templates](#).

The following example shows how to apply the Windows Server 2016 Services and Counters template to monitor a Windows 2016 OS with the component monitors:

- Service: Distributed Transaction Coordinator
- Service: Security Accounts Manager
- Service: Remote Registry
- Total Available Memory (MB)
- Page File Usage
- Disk Queue Length
- Virtual Memory
- % Processor Time
- Service: Server
- Service: Plug and Play
- Pages per second
- Logical Disk: Average Disk Queue Length
- Physical Disk: Average Disk Queue Length
Before you begin

Ensure you have Remote Procedure Call (RPC) and Windows Management Instrumentation (WMI) access to the target server, plus Windows Administrator credentials for the server.

Windows Performance Counters use RPC for communication which uses TCP port 445. If testing fails after assigning the template to a node, use the WMI protocol.

Apply a template to a node

1. Click Settings > All Settings > SAM Settings.
2. Under Application Monitor Templates, click Manage Templates.
3. Locate the template and click Assign to Node.
4. Select the Windows nodes you want to monitor for the operating system on the left pane, click the green arrow to move it to the right pane, and click Next.

![Image of Create Assigned Application Monitor](image)

5. Choose the credentials, and click Assign Application Monitors.

![Image of Create Assigned Application Monitor](image)

6. On the Finish panel, click Done.

   It will take several minutes for the initial poll to complete and widgets to display data.
View the application data

Click My Dashboards > SAM Summary to view the All Applications widget. The All Applications widget is an excellent method for at-a-glance monitoring with hover-over information and icons status to provide a quick overview of data. When software is ruled out as the problem, check the hardware health.
Monitor hardware health in SAM

You can get immediate insight into hardware issues in your SAM environment by tracking key parameters for servers such as fan status, power supply status, and temperature. Monitoring hardware health on supported devices lets you know their status so you can:

- **Pinpoint performance issues caused by hardware failure.** SAM provides instant visibility of the device status (Up, Down, Critical, Warning, or Unknown) and allows you to set baseline values that trigger alerts if levels fall below set thresholds.
- **Optimize resource utilization and hardware procurement.** Gain deep visibility into usage of server resources to make informed decisions about hardware purchases.
- **Use one interface to manage a heterogeneous IT infrastructure.** From a single console, monitor multi-vendor infrastructure, including Cisco UCS, Dell, HP, IBM, Nutanix, and VMware hosts.

To get started monitoring hardware health for Dell, HP, HPE ProLiant, and IBM servers:

1. Review [hardware health monitoring requirements](#), including supported devices.
2. Download, install, and configure hardware monitoring agent software from third-party vendors. Click [here](#) for details.
3. Run [Discovery](#) to detect third-party agent software and enable hardware health monitoring automatically across multiple nodes.

You can also enable hardware health monitoring for individual nodes.

When SAM enables hardware health monitoring during Discovery, it also enables [Asset Inventory data collection](#) to track each node’s hardware and software. Polling jobs begin immediately, and are later scheduled to occur at random times over a 24-hour period. If necessary, you can [adjust the default interval for Asset Inventory polling](#).

To monitor hardware health for UCS devices, start by adding the parent UCS controller to the Orion Platform. See [Monitor Cisco UCS Devices](#) for details.

To monitor hardware health in Nutanix environments, add Hyper-V or VMware nodes for monitoring, add the parent Nutanix cluster, and provide Controller VM (CVM) credentials. See [Monitor hardware health for Nutanix clusters](#).

Documentation about Orion Platform features available in multiple modules is stored in the [Orion Platform Administrator Guide](#). Because hardware health monitoring for UCS and Nutanix is a shared feature, you’ll find related information in that document.
To display hardware health in the Orion Web Console:

1. Click My Dashboards > Home, and then locate the Hardware Health Overview widget.

2. To view a status, click its label.

3. Click the node you want to review.

4. Review the Current Hardware Health widget. Sensors listed as Critical should be investigated.

To learn more about hardware health monitoring, see the [SAM Administrator Guide](#) and the [Orion Platform Administrator Guide](#).
Monitor cloud instances and VMs

This section provides an overview about monitoring your cloud infrastructure. See the Orion Platform Administrator Guide for more information.

Cloud service platforms provide on-demand computing resources to third-party organizations over the Internet. As organizations migrate systems to the cloud to distribute workloads, deliver applications, and expand resources for growing databases, infrastructure can become difficult to map in sprawling environments, leading to lost resources or hidden instances.

To support hybrid environments, the Orion Platform can retrieve data from the Amazon Web Services (AWS) and Microsoft Azure cloud service platforms to track availability, performance, applications, and more for instances and VMs. Examples of data gathered include status, storage capacity, memory usage, and IP addresses.

After configuring cloud accounts, you can use the Cloud Infrastructure Monitoring feature to:

- Manage hybrid environment metrics and status through a single console so you can compare performance, locate bottlenecks, and better plan capacity and resource allocation.
- Track end user and business context for performance by gathering extended metrics that provide visibility into cloud and on-premises systems.
- Dynamically monitor cloud instances and VMs to better handle resource churn during provisioning. Instances and VMs can be removed as needed to support expanding environments or performance peaks.
- Determine usage trends and troubleshoot issues. Captured metrics over time provide historical references to track trends for resource consumption (such as CPU spikes and lulls) and help determine when those trends become issues.
- Use cloud monitoring data, Orion alerts, and the Performance Analysis dashboard (PerfStack) to review historical performance and pinpoint when significant usage changes began to trigger issues.

For example, add a series of EC2 cloud instances for an AWS account for the east coast. Select My Dashboards > Cloud to review overall AWS infrastructure data and cloud details. Use the Cloud Instances Status Summary and Cloud Server Infrastructure widgets to review status and health at-a-glance. To quickly review cloud status, metrics, and node management details, hover over any cloud instance name.
The tooltip provides quick information for the cloud service and status.

When managed as a node, the tooltip provides enhanced data.

Cloud instances encountering issues display in the following widgets with linked instances and nodes to investigate:

- Active Cloud Alerts lists all active alerts affecting monitoring and managed cloud instances.
- Cloud Applications with Problems lists all applications with issues on cloud instances managed as nodes in SAM.

Select a cloud instance or VM to view its Details page. Exceeded thresholds are highlighted in warning and critical values, charts, and graphs with hover-over points to compare collected data and linked alerts. The following widgets provide important data to determine issues, as well as track performance and usage trends:

- Active Alerts lists all active alerts affecting the cloud instance.
- Min/Max/Average of Average CPU load displays average CPU load collected and calculated for the cloud instance.
Min/Max/Average of Network Utilization provides a chart of the minimum, maximum, and average bits per second transmitted and received over a cloud instance for a custom period of time.

**Introduction to AppStack**

A key tool in SAM is the Application Stack, commonly known as "AppStack," an interactive visual map that displays a detailed view of your environment so you can identify the root cause of performance and availability issues. Use AppStack to assess the overall health of your environment and to troubleshoot specific and related problems.

An AppStack view is also available at the application layer that only shows the relationships for that application. This view is called the Mini-Stack.

AppStack provides a more thorough analysis of root cause problems in your environment if combined with Storage Resource Manager, Virtualization Manager, and Web Performance Monitor.
To access the AppStack Environment page:

1. Click My Dashboards > Environment.

The AppStack environment generates categories that show the status of objects in your environment. Objects on the left are the highest priority.

2. Click an object to highlight related objects and gray out unrelated objects.
3. Click Spotlight to remove unrelated objects.

4. To investigate further, click the selected object.

The relevant Details page appears.
Investigate application performance with PerfStack

With complex networks consisting of cloud, hybrid IT, virtualization, storage area networks, and so on, multi-faceted IT issues can be difficult to pinpoint and diagnose. When an issue surfaces, for example a badly performing application or server, the investigation can take significant time to locate the core issue. The problem could be in storage, network connectivity, user access, or a mix of resources and configurations.

To investigate the issue, create troubleshooting projects with the Performance Analysis (PerfStack™) dashboard that visually correlate historical and real-time data from multiple SolarWinds products and entity types in a single view.

With Performance Analysis dashboards, you can do the following:

- Compare and analyze multiple metric types in a single view, including status, events, and statistics.
- Compare and analyze metrics for multiple entities in a single view, including, nodes, interfaces, volumes, applications, and more.
- Correlate data from across the Orion Platform on a single, shared time line.
- Visualize hybrid data for on-premises, cloud, and everything in between.
- Share a troubleshooting project with your teams and experts to review historical data for an issue.

For SAM, the possibilities are endless for application analysis and hybrid environments:

- Visually walk through historical data for applications in your environment
- Verify resource allocation issues in hybrid environments for a specific application
- Correlate application data from templates, component monitors, hardware health monitoring, and more into a single view

To learn more about PerfStack, see the Orion Platform Administrator Guide.

The following example shows how to identify a root cause for a Windows Server 2012 application performance issue. In this scenario, the application performance has degraded to the point where users encounter slower responses and access. As you review the Windows Server 2003-2012 template dashboard, you find triggered alerts. These alerts notified your application owner, who escalated the issue to system and network administrators.

Rather than digging into the alerts and multiple Node Details pages to troubleshoot the issue, create a new troubleshooting project to investigate the issue.
1. Click My Dashboards > Home > Performance Analysis.

This opens the PerfStack, dashboard where you can build charts and graphs using metrics pulled from monitored applications and servers in the Metric Palette. Each chart can hold multiple metrics to directly correlate data.

2. In the New Analysis Project, click Add Entities.

Entities include all monitored and managed servers, applications, devices, services, and more.

3. Select Entities and click Add selected items.

To get started, locate and add the Windows 2012 application in distress. In the search field, enter Windows to get a list of all monitored nodes, component monitors, and more with Windows in the name or type. Expand and select Types or Status to filter the list.

From the list, we find the application monitor watching Windows Server 2003-2012 Services and Counters. Select and add it to the dashboard Metric Palette.
Click the related entities icon to display nodes, applications, servers, and other entities related to the selected node in the Metric Palette so you can check if metrics are causing issues.

4. Select the Windows 2012 node to view and select metrics to drag and drop onto the dashboard. You can drag them into the same chart to compare values between metrics.

To start investigating, pull a series of metrics for the IOPS throughput for the server. For this scenario, add the following metrics to investigate latency and connectivity:

- Logical Disk Average: Disk Queuing
- Average IOPS Read
- Maximum IOPS Write
- Maximum IOPS Read
- Average IOPS Write
- IO Latency Write
- IO Latency Read
- IOPS Total
The charts and graphs show data and alerts for the Last 12 hours of metrics.

5. Add more metrics from the virtual and storage layers to investigate and confirm any bandwidth spikes.

For example, add metrics for the IO latency from the virtual and storage layers to locate issues:

- IO Latency Write
- IO Latency Read
- IOPS Total
- Throughput Total

Analyzing the data, the issue looks to be a noisy neighbor. Basically, another server, service, or application is consuming higher bandwidth, disk I/O, CPU, and other resources causing issues for this specific application.

This information gives your network and system administrators a direction for further investigation and resolving latency issues. To resolve, they can reallocate resources or move the high-consumption application to another location.

6. Click Save and give the project a name.

The project saves as a dashboard with the selected metrics in the set date and time range.
When saved, the URL becomes a shareable link. Copy and share the link to the saved dashboard in tickets or emails sent by the system, network administrators, and the product owner. They can access the link to review the gathered data and troubleshoot.

`yourSolarWindsDomain/ui/perfstack/PSTK-50A2738DF0FEF6B7460F7A6BFA812250A67EFH89`

After reallocating resources and making network changes, reopen the dashboard to verify changes and new usage trends for polled metrics.
Explore alerts and reports in SAM

This section includes information on working with preconfigured alerts and reports:

- How alerts work in SAM
- Work with preconfigured alerts in SAM
- How reports work in SAM
- Run a preconfigured report in SAM
- Create a custom alert in SAM
- Create a custom SAM report

To learn more about alerts, see Use alerts to monitor your environment in the Orion Platform Getting Started Guide.

How alerts work in SAM

An alert is notification that there is a problem with a monitored element. Orion comes with hundreds of predefined alerts for common problems such as a node or application going down, SSL certificate expiration, website failures, and many other problems.

Many predefined alerts are enabled by default, so if there are problems, you are alerted as soon as you use Discovery to find servers and applications in your environment and add them to the Orion database.

SolarWinds recommends that you identify who will receive warning or critical alerts.

- **Alerting on an application**: SolarWinds SAM provides many preconfigured application alerts that notify you if the status of an application changes (for example: up, down, or unknown) based on whether a component monitor reached a warning or critical threshold. One alert can notify you about a warning, critical, down, or unknown state for the application.
- **Alerting on a component**: If you create an alert for each component monitor in a SAM template, you will receive one alert for each component that exceeds a threshold. Alerting on a component monitor can be beneficial if you have custom scripts where you must be notified if the output of the script crosses a specific threshold.
By default, alerts appear in the Active Alerts widget on the Orion Home page.

### All Active Alerts (17)

<table>
<thead>
<tr>
<th>ALERT NAME</th>
<th>MESSAGE</th>
<th>TRIGGERING OBJECT</th>
<th>ACTIVE TIME</th>
<th>RELATED NODE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert me when a component goes into warning or critical state</td>
<td>Alert me when a component goes into warning or critical state</td>
<td>Free pages</td>
<td>1h 7m</td>
<td>LAB-NABLE-FS</td>
</tr>
<tr>
<td>Alert me when a component goes into warning or critical state</td>
<td>Alert me when a component goes into warning or critical state</td>
<td>Cache Hit Ratio</td>
<td>5h 47m</td>
<td>LAB-NABLE-FS</td>
</tr>
<tr>
<td>Alert me when a component goes into warning or critical state</td>
<td>Alert me when a component goes into warning or critical state</td>
<td>Buffer Cache Hit Ratio</td>
<td>19h 10m</td>
<td>lab-apm-demo</td>
</tr>
</tbody>
</table>

To see all alerts, click the All Active Alerts button in the Active Alerts widget, or click Alerts & Activity > Alerts. When the All Active Alerts page appears, you can:

- Acknowledge an alert that you are working on
- Click on any alert to go to the Alert Details page for more information
- Click Manage Alerts to enable/disable, add or edit any alert.

You can create your own alerts, either by duplicating and editing a predefined alert, or by creating a custom alert. Alerting is very powerful and can be complex, with multiple trigger conditions, reset conditions, and actions.

To learn more about alerts, see [Use alerts to monitor your environment](#) in the Orion Platform Getting Started Guide.
Work with preconfigured alerts in SAM

SAM includes out-of-the-box alerts with preconfigured triggers, actions, and settings to automatically start monitoring and triggering against events. These alerts provide immediate notifications through the Orion Web Console as SAM monitors applications, servers, and other nodes.

These alerts allow you to configure additional options for actions including sending an email with event and alert information and resetting manually or automatically according to specific settings. You can also create copies of preconfigured alerts to customize and add triggers, conditions, actions, and more.

List preconfigured, enabled alerts

SAM includes several preconfigured, enabled alerts, plus some disabled alerts that you can enable, as needed.

1. Click Alerts & Activity > Alerts
2. Click Manage Alerts.
3. In the Group by field, select Enabled.

4. In the Type field, sort by Out-of-the-box.

5. Review the list of preconfigured, enabled alerts.
Enable and disable alerts

To enable or disable alerts, on the Manage Alerts page, click On or Off in the Enabled column.

Action types

You can configure an alert to trigger one or more actions, such as:

- Send an email
- Send a page
- Manage a virtual machine (for example, power on/off)
- Log the alert to send a file

A complete list of alert actions is available on the Add Action dialog box that you see when you configure an alert.

Configure the default email action

A common alert action is to send an email. To send an email, Orion requires a designated SMTP server that you configure.

1. Click Settings > All Settings, and in the Alerts & Reports section, click Configure Default Send Email Action.
2. In the Default Recipients section, enter recipient email addresses, separated by a semicolon.

3. Under the Default Sender Details heading, provide the default Name of Sender and the default Reply Address.

4. Under the Default SMTP Server section:
   a. Provide the Host name or IP Address of the SMTP Server and the designated SMTP Port Number.
      
      For example, 192.168.10.124, port 25.
   b. If you want to use SSL encryption for your alert emails, select Use SSL.
      
      Selecting SSL automatically changes the SMTP port number to 465.
   c. If your SMTP server requires authentication, select This SMTP Server requires
Authentication, and then provide the credentials.

d. Click Use as Default.

Manage active alerts

When an alert triggers, any associated alert actions also trigger, and the alert appears on the All Active Alerts page and in the SAM Summary Page. Through the Orion Web Console, you can view the details of alert, the monitored element that triggered the alert, and take action.

1. To view the alert details, click the alert.

The Active Alert Details page appears.
2. To view the details of the network object that triggered the alert, click an object.

The details page of the selected object appears.
3. To acknowledge an alert:
   a. Click Acknowledge.
   b. Enter a note and click Acknowledge.

When acknowledged, the alert will not trigger again.
Create a custom alert in SAM

Alerts give you the ability to trigger actions and notifications according to monitored events and metrics. In this example, an alert is configured to trigger and send an email to an IIS Administrator when an IIS application goes into a warning or critical state.

The $\{variable\}$ syntax is required for variables. To learn more, see Variables and examples used in the Orion Platform.

1. Click Settings > All Settings > Manage Alerts.
2. Select an alert, and click Duplicate & Edit.
3. On the Properties panel, enter a name and any other properties, and click Next.

In this example, a group of IIS administrators is identified as the responsible team.

4. On the Trigger Conditions panel, select an object to alert on, and then complete the trigger condition fields.

In this example, the first trigger condition tests for Node status (Down), the second and third conditions test for application thresholds, and the fourth condition specifies the applications to alert on (indicated by 5 Objects).
5. On the Trigger Actions panel, click Add Action.
6. Select send an Email/Page, and click Configure Action.

7. Modify the alert to email the IIS administrators.

💡 This is an example of creating a custom alert, as opposed to using a predefined default alert that comes with SolarWinds SAM. You can define additional alerts that can be customized to email specific users or email groups.
8. You can optionally add and configure an action to log the event to the NetPerfMon event log.

9. Enter the required information for each action, click Next, then continue through the wizard.

10. Edit the Reset Actions to send an email to the default recipients, then click Next.

11. Continue through the wizard, review the Summary, then click Submit.

The Manage Alerts page indicates the alert was created successfully.
How reports work in SAM

Reports provide a bridge between detailed views (which provide point-in-time information) and alerts (which tell you there is a problem). Reports can contain detailed, current state information, or they can contain historical data.

You can run an ad-hoc report, or schedule reports to be sent to you automatically, as a PDF, a web page, or email. For example, use a schedule when you want to receive the Asset Inventory report every Monday morning.

💡 SolarWinds recommends that you identify who needs to receive performance or status reports, and how often they should receive them.

Reports populate when you:

- Discover your servers and applications in SAM
- Add discovered servers and applications to SAM
- There is enough data to include in the report. Depending on the polling interval and data type, some reports do not populate immediately. For example, it takes two weeks for baseline reports to populate.

SolarWinds provides predefined reports for each Orion module. Click Reports > All Reports to see the available predefined reports.
On the All Reports page, click a report to view it.

You can create your own custom reports by either editing an existing report or creating a report from scratch. Reports can combine any number or type of Orion widgets, including charts, tables, and gauges. You can customize the size of the report, the layout, and add a logo and a footer.

**Run a preconfigured report in SAM**

This example shows how to run and schedule the Asset Inventory preconfigured report in SAM.

The Asset Inventory dashboard allows you to maintain a current and detailed inventory of your environment’s hardware and software. Automatic inventory data collection benefits those interested in tracking asset depreciation, gathering information for insurance purposes, or managing and maintaining your infrastructure.

**Enable Asset Inventory data collection**

You must enable Asset Inventory data collection before you generate the Hardware Asset Inventory report.

1. In the Orion Web Console, click Settings > Manage Node.
2. Click Add Node.
3. On the Choose Resource panel, click Asset Inventory.

![Add Node](image)

**Generate the report**

The following example illustrates how to generate an asset inventory report.

1. In the Orion Web Console, click Reports > All Reports.
2. Locate the report, and click the report title.

![View Report](image)

The system generates the report.
**Schedule a report**

1. In the Orion Web Console, click Reports > All Reports.
2. Click Manage Reports.
4. Configure the properties, frequency, and actions as needed in the wizard.
5. When completed, review the summary, and click Create Schedule.

<table>
<thead>
<tr>
<th>NODE NAME</th>
<th>IP ADDRESS</th>
<th>SERVICE TAG</th>
<th>DEVICE TYPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>NABLE-IBRE-03</td>
<td>10.199.6.101</td>
<td></td>
<td>Server</td>
</tr>
<tr>
<td>QA-NABLE-AT-04</td>
<td>10.199.6.106</td>
<td>7377-3622-4837-3237-8123-5474-05</td>
<td>Workstation</td>
</tr>
<tr>
<td>QA-NABLE-AT-05</td>
<td>10.199.6.107</td>
<td>0216-1442-4986-9376-0790-3288-76</td>
<td>Workstation</td>
</tr>
</tbody>
</table>
Create a custom SAM report

You can combine any Orion Web Console widget or chart into a report. In this example, a custom report for IIS servers is created by modifying a predefined report, then adding a few more widgets for a complete picture of your IIS servers. To create this custom report, you will first need to create a custom property to identify nodes running IIS.

This report provides information about:

- IIS servers with disks approaching 100%
- Capacity for all disk volumes from the last seven days
- The percentage of disk space used for all disk volumes from the last seven days
- IIS instances with problems
- Availability of IIS Nodes
- Nodes with problems

Create a custom property to identify nodes running IIS

1. In the Orion Web Console, click Settings > All Settings > Manage Custom Properties.
2. Click Add Custom Properties.
3. On the Select Object panel, select Nodes, and click Next.
4. On the Choose Properties panel, in the Property Name field, enter Type.
5. In the Format field, select Text.
6. Select Restrict values, and in the Value 1 field, enter IIS.

You can enter more values to identify other server types. This example uses just the IIS server type.
7. For Usage, select everything except Asset Inventory, and click Next.

8. On the Assign Values panel, click Select Nodes.

9. Select the nodes to which you want to assign the property, and click Add.
10. In the list of Selected Nodes, click Select All, then click Select Nodes.

11. Select IIS from the drop-down menu, and click Submit.

Create the IIS application server issue rollup report

1. Click Reports > All Reports > Manage Reports, and locate Disks Approaching 100% Capacity - This Month.
2. Select the report, and click Duplicate & Edit.

3. Enter the report name, for example, IIS Application Server Issue Rollup.

4. For the widget in the first default row, click Edit Chart, rename the chart to IIS Servers with Disks Approaching 100% Capacity, and click Submit.

5. In the From field, select Last 7 Days.

6. Click Edit.

![IIS Servers with Disks Approaching 100% Capacity](image)

7. Click the plus sign (+), and click Add Simple Condition.

![Basic Selector](image)

8. Click Select Field, and then locate and select Node > Nodes Custom Properties > Type.
9. Click Add Column.

10. Select IIS from the drop-down menu, ensuring the query reads Type is equal to IIS.

11. Add another simple condition, and locate and select Percent Used under Volume Current Statistics.

12. Click Add Column.
13. Select the `is greater than` operator and enter 70.

The query should read: Percent used is greater than 70.

14. Click Add to Layout.
15. For the widget in the second default row, in the From field, select Last 7 Days.

16. Click Add Content.

17. In the Group By field, select Classic category.


19. Click Select and Continue.

20. On the Layout Builder panel, click Edit Resource, and in the Title field, enter **IIS Instance with Problems**.

21. Add the following SWQL filter: `Application.Name='Microsoft IIS'`

22. Click Submit.
23. Click Add Content > Classic Category > Summary Reports > Availability of Each Node.

24. Click Select and Continue.

25. Click Edit Resource, and in the Select a Time Period field, select Last 7 Days.

26. In the Filter Nodes (SQL) field, enter: `type='IIS'`.

27. Click Submit.
When complete, your report should look similar to the following:
Work with SAM templates

SAM includes over 250 out-of-the-box application monitor templates that cover a wide range of common applications. You can think of a template as a blueprint of what needs to monitored for a particular type of application. It lists all components or building blocks for that application and recommended, default thresholds.

A good analogy for this is a template to monitor a car. Your standard template covers basics like speed, fuel, and oil levels. After monitoring your fleet of vehicles, you may opt to adjust the warning threshold level for fuel - adjusting the level on the template propagates that change down to all applications based on that template (in this case, your entire fleet). If one driver tends to speed, you can adjust the warning and critical thresholds for that one car without affecting the standard monitoring of the rest of your fleet.

To display a list of templates included in SAM:

1. Click Settings > All Settings > SAM Settings..
2. Under Application Monitor Templates, click Manage Templates.

A searchable list of templates appears on the Manage Application Monitor Templates page, as shown here:

To learn more, see Use SAM templates, application monitors, and component monitors in the SAM Administrator Guide.
Understand the application/template relationship

In SAM, an application is a collection of component monitors inherited from a template when you assign the template to a node. A component monitor queries for values returned by a process, counter, status, or script. SAM uses the data received to display vital statistics concerning the health of the system.

Templates provide blueprints for the applications to be monitored. You can customize templates, and use only the component monitors you need to monitor a specific environment. SAM provides several types of templates:

- **AppInsight applications** are predefined templates that provide detailed information about business-critical Active Directory, Exchange, Microsoft IIS, or Microsoft SQL instances. Each AppInsight template is specifically designed to discover and monitor elements of an application dynamically.

- If you have other business-critical applications, apply one of the other templates included in SAM, as listed in the [SAM Template Reference](#). SolarWinds recommends deploying a single template, customizing it for your environment, and then deploying the edited template on all similar applications. You can also obtain templates in THWACK.

- For proprietary applications that you need to monitor, you can build custom templates.

If you make a change at the template level, application (also called application monitors) based on that template are affected. Conversely, if you make a change at the application level, only the individual application is affected. This inheritance relationship is beneficial if you need to make a lot of changes. For example, rather than making one change to 100 applications (and therefore 100 changes), you can change the parent template and that change is inherited by the 100 applications based on that template.
Create custom templates in SAM

SolarWinds SAM provides out-of-the-box (OOTB) templates that you can use to monitor over 200 applications. You can use pre-built templates "as is" or modify them. You can also create custom templates to monitor uncommon components or applications that are not included in the templates provided with SAM.

The following example shows how to create and assign a template that uses the File Size Monitor, one of the many component monitors included in SAM. You can add as many component monitors to a template as you need.

To learn more about creating your own templates, see the [SAM Custom Template Guide](#).

Create a template to monitor file size

1. Click Settings > All Settings.
2. In the Product specific settings group, click SAM Settings.
3. In the Application Monitor Templates group, click Create a New Template.
4. When the New Template page appears, provide basic details about your new template including a name and brief description.
5. Click Add Component Monitors > Manually add Component Monitors.
6. Select the File Size Monitor component, and click Add.

7. Enter the path and the file to monitor.

   - File Path: `c:\temp\logfile.txt`
   - Convert Value: Yes, convert returned value. The converted value will be used by thresholds & displayed. » Learn more

8. Enter warning and critical threshold values, and click Submit.

   - Warning: greater than 100 for a single poll
   - Critical: greater than 120 for a single poll

Assign the template to a node

1. Click Settings > All Settings.
2. In the Product specific settings group, click SAM Settings.
3. Click Manage Templates.
4. On the Manage Application Monitor Templates page, select your new template, and click Assign to Node.

![Assign to Node](image)

5. Select the node from the left pane, click the green arrow to move it to the right pane, and click Next.

6. Choose the credentials, click Assign Application Monitor, and click Done.
Set thresholds in SAM

Thresholds are markers that indicate certain levels were reached. The Orion Platform includes predefined thresholds for most statistics, such as Disk Usage and Response statistics for all monitored nodes, that you can override, as described in Thresholds in the Orion Platform. Many SAM templates, application monitors, and component monitors include predefined thresholds that you can adjust.

In the Orion Web Console, the color of a statistic indicates if reached either of two threshold levels: critical or warning. A value that crosses a warning threshold appears yellow, and a critical threshold appears red.

If thresholds are set too low, you’ll receive frequent alerts. If set too high, problems can occur without your knowledge.

You can customize thresholds by setting a static value or letting the Orion Platform calculate baseline values.

- **Static threshold.** A constant value set for your threshold. For example, the warning threshold for response time might be 500 ms, and the critical value might be 1000 ms. You should be familiar with the performance of that object to know what a reasonable value for a static threshold is.

- **Dynamic baseline threshold.** Data is collected for a week, and then used to calculate mean and standard deviation. The warning and critical threshold values are defined as 2 and 3 standard deviations above the mean, respectively. For example, if the mean value for packet loss for a specific node is 0%, the warning threshold for packet loss would be 3% (+2 standard deviations) and the critical threshold would be 4% (+3 standard deviations). Dynamic baseline thresholds are the most accurate way to define thresholds, and can be recalculated on demand.

To learn more about thresholds, see:

- Manage thresholds in SAM (SAM Administrator Guide)
- Thresholds in the Orion Platform (Orion Platform Administrator Guide)
- Baseline thresholds (THWACK)
- Use MIN/MAX Average Statistic charts to set thresholds based on 95th percentile data for component monitors (SolarWinds Success Center)