© 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 Configuration Monitor ........................................................................ 5
SCM licensing model .................................................................................................................. 6
Log into the Orion Web Console to use and manage SCM ....................................................... 7
Add a node to Server Configuration Monitor (SCM) ................................................................. 9
  Add a node through Network Discovery in Server Configuration Monitor (SCM) ................ 9
  Add a node through the Add Node wizard in Server Configuration Monitor (SCM) ............ 19
Monitor Linux nodes in SCM ..................................................................................................... 20
  Monitor Linux files .................................................................................................................. 20
  Monitor hardware and software ............................................................................................... 21
Monitor a SQL database with SCM ............................................................................................ 22
  Set up and install .................................................................................................................... 22
  Configure SCM to monitor a Database query element ......................................................... 22
  Out-of-the-box database profiles ............................................................................................ 25
  Additional notes on database monitoring ................................................................................ 25
Understand database queries in SCM ........................................................................................ 27
  Custom ODBC Drivers ........................................................................................................... 27
Server configuration profiles in SCM ......................................................................................... 28
Out-of-the-box profiles in Server Configuration Monitor (SCM) .............................................. 29
  HW inventory profiles in Server Configuration Monitor (SCM) ............................................ 29
  SW inventory profiles in Server Configuration Monitor (SCM) ............................................ 31
  IIS server configuration profiles in Server Configuration Monitor (SCM) ......................... 31
  Linux Essentials profiles in Server Configuration Monitor (SCM) ...................................... 32
  Linux Security and Permission profiles in SCM ................................................................. 34
  Database profiles in SCM ....................................................................................................... 34
User restrictions in Server Configuration Monitor (SCM) ....................................................... 38
Assign configuration profiles to a node in Server Configuration Monitor (SCM) ........................................39
  Through Server Configuration Monitor Settings ..........................................................39
  Through List Resources .........................................................................................47
  From the Server Configuration Summary page .........................................................47
  Assign or unassign from the Manage Nodes page .....................................................48

Unassign configuration profiles in Server Configuration Monitor (SCM) .......................49
  Through Server Configuration Monitor Settings ..........................................................49
  Through List Resources .........................................................................................49
  From the Manage Nodes page ..............................................................................50

Monitor configuration changes on a node in SCM ......................................................51
  See detected candidates for configuration monitoring in Server Configuration Monitor (SCM) .51
  Learn about near real-time change detection in SCM ..............................................52
  Monitor who made server configuration changes ......................................................52
  Enable near real-time file monitoring and 'who made the change' detection in Server
  Configuration Monitor (SCM) ..................................................................................55
  Test SCM profile elements before deploying them ....................................................57

Learn about baselines in SCM ...............................................................................61
  Define or redefine a baseline individually or in bulk ...............................................62

Compare configurations over time in Server Configuration Monitor (SCM) ............63
  See recent configuration changes in Server Configuration Monitor (SCM) .............63
  See configuration changes between two points in time using SCM .....................63
  View the structural diff in SCM ...........................................................................67
  Correlate configuration changes to performance metrics in SCM .......................67
  Change how long configuration data is kept in Server Configuration Monitor (SCM) .....69
Get Started with Server Configuration Monitor

This guide picks up right after the Server Configuration Monitor (SCM) installation process and walks you through the first steps you need to take to monitor your server configurations.

ℹ️ If you haven't installed SCM yet, start with the SolarWinds Orion Installer.

Who this guide is for

<table>
<thead>
<tr>
<th>New SCM users</th>
<th>Existing SCM users</th>
</tr>
</thead>
<tbody>
<tr>
<td>This guide is meant for you and is the best place to start with SCM.</td>
<td>You'll find more advanced information in the SCM Admin Guide.</td>
</tr>
<tr>
<td></td>
<td>Or if you're looking for tips on how to upgrade to SCM 2020.2, see the SCM Upgrade Guide.</td>
</tr>
</tbody>
</table>

What's in this guide

- **Log into the Orion Web Console to use and manage SCM** - An introduction to logging into the Orion Web Console, which you'll use to do everything in SCM.

- **Add a node to SCM** - The first step to start monitoring with SCM.

- **Assign configuration profiles, compare your first changes**, and **set baselines** so you can get the most out of SCM.

Once you have the basics, check out the Server Configuration Monitor Administrator Guide to learn about more advanced functionality.

Have a question? Join the THWACK SolarWinds IT community, and find more information in the SolarWinds Success Center.
SCM licensing model

SCM is licensed per node. A node counts toward your total while it has at least one SCM profile assigned to it.

Orion Platform products support both perpetual licenses and subscription licenses. See License types in the Orion Platform help for details.

The following SCM license tiers are available:

<table>
<thead>
<tr>
<th>License Tier</th>
<th>Number of Managed Nodes</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCM10</td>
<td>10</td>
</tr>
<tr>
<td>SCM25</td>
<td>25</td>
</tr>
<tr>
<td>SCM50</td>
<td>50</td>
</tr>
<tr>
<td>SCM100</td>
<td>100</td>
</tr>
<tr>
<td>SCM250</td>
<td>250</td>
</tr>
<tr>
<td>SCM500</td>
<td>500</td>
</tr>
<tr>
<td>SCM1000</td>
<td>1000</td>
</tr>
<tr>
<td>SCM2000</td>
<td>2000</td>
</tr>
</tbody>
</table>
Log into the Orion Web Console to use and manage SCM

As with all Orion Platform products, you'll use Server Configuration Monitor (SCM) by logging into the Orion Web Console to manage all aspects of SCM.

In a web browser, go to: [http://hostnameOrIPAddress:port] where:

- **hostnameOrIPAddress** is the hostname or IP address of the Orion server where SCM is installed.
- **port** is the Orion Web Console port defined for the website. This is configurable during installation. The default port is 8787.

You'll see the Orion server login page:

The first time you log in, you'll be asked to create a user name and password. Later, you'll also want to create users with their own credentials and groups, each with their own specialized views and permissions.
If you're logging into a new installation of SCM, you'll be prompted to add a password to the main Admin account.
Add a node to Server Configuration Monitor (SCM)

To add servers already monitored by the Orion Platform to SCM, start configuration monitoring on the device.

To monitor servers using SCM, you must first add them to the Orion Platform. There are several ways to add devices to the Orion Platform, but the following ways allow you to start SCM monitoring at the same time:

- Add a node through Network Discovery
- Add a node through the Add Node wizard

To learn more about adding nodes to the Orion Platform, see the Orion Platform Administrator Guide.

Add a node through Network Discovery in Server Configuration Monitor (SCM)

1. In the Orion Web Console menu, navigate to 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>IP Ranges</td>
<td>Use this option when you want Orion to scan one or more IP ranges.</td>
</tr>
<tr>
<td></td>
<td>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>Subnets</td>
<td>Use this option to scan every IP address in a subnet. SolarWinds recommends scanning at most a /23 subnet (512 addresses max).</td>
</tr>
<tr>
<td></td>
<td>Scanning a subnet returns everything that responds to ping, so we recommend scanning subnets only where the majority of devices are objects you want to monitor.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IP Addresses</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>
<tr>
<td>Active Directory</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Network Sonar Wizard**

*Network Selection*

How do you want to add devices to Orion monitor? You can use one or more of the options below, but for fastest results, we recommend scanning a maximum of 512 devices at a time.

- **Using discovery for the first time?**
  - WE RECOMMEND SCANNING...

  - ... a small subnet (/24) with your test environment
  - OR
  - ... a few individual IP addresses for servers, routers and switches, and VMs

  This will let you see the wealth of data that Orion provides as quickly as possible. You can always add more later!

**IP RANGES**

Add Range

**SUBNETS**

Add

**IP ADDRESSES**

Write one IP address or hostname per line:

- 192.168.2.33
- 20.123.0.128

Validate

**ACTIVE DIRECTORY**

Add Active Directory Domain Controller to query...
4. If the Agent panel is displayed, you enabled the Quality of Experience (QoE) agent during installation. The QoE agent monitors packet-level traffic. If there are any nodes using agents, select the Check all existing nodes check box. Click Next.

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 SNMP panel:
   a. If all devices on your network require only the default SNMPv2 public and private community strings, click Next.
   b. If any device on your network uses a community string other than public or private, or if you want to use an SNMPv3 credential, click Add Credential and provide the required information. Click Add, and then click Next.

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

texts:

- **To monitor for configuration changes on Windows, you must deploy an agent.**
7. On the Monitoring Settings panel, you can choose to manually set up monitoring the first time you run discovery, or you can automatically monitor based on settings that you define.

   a. To manually set up monitoring after devices are discovered, click Manually set up monitoring after devices are discovered, and then click Next.
b. To define monitoring settings and then automatically monitor based on those settings, click Automatically monitor based on my defined settings, and then click Define monitoring settings. Click Next.
Select the Volume Types to monitor, and then click Next.
Hardware and software inventory are automatically assigned for nodes with enabled Asset Inventory, and the IIS profile is assigned when IIS is detected on a node.

Select the server configuration profiles to monitor, or if you prefer not to automatically assign profiles to newly discovered nodes, deselect any or all of the profile types. Click Finish, and then click Next.
Only out-of-the-box profiles can be added this way. Selected profiles will be applied to all discovered nodes that are eligible for that type of monitoring. This eligibility is determined by the presence of specific files or registries on the node. For example, IIS configuration files must be present for the IIS profile to be applied. Profiles other than hardware and software inventories require polling via an Orion Agent for Windows or Linux.

8. On the Discovery Settings panel, click Next.
9. Accept the default frequency and click Discover to run discovery immediately.

![Network Sonar Wizard](image)

Discovery can take anywhere from a few minutes to a few hours, depending on the number of network elements the system discovers.

![DISCOVERING NETWORK...](image)

10. After discovery has completed:

   a. If you defined your monitoring settings above, this procedure is complete, and your results are displayed.

   b. If you chose to manually set up monitoring after devices are discovered, select the devices types to import, and click Next.

![Network Sonar Results Wizard](image)

Select the volume types to import, and click Next.
Select the server configuration profiles to import, and then click Next.

Select the devices and volumes you want to import (or ignore), and then click Import (or Ignore).

Then click Finish.
Your results are displayed.

Add a node through the Add Node wizard in Server Configuration Monitor (SCM)

1. In the Orion Web Console menu, navigate to Settings > Manage Nodes.
2. Click Add Node.
3. Specify the node, and click Next.
   a. Provide the host name or IP address.
   b. Select the polling method, and provide credentials.

   ![Most SCM monitoring requires polling via an Orion Agent for Windows or Linux.]

4. In the Choose Resources step, select the profiles you would like to monitor under Server Configuration. Click Next.

   ![Only out-of-the-box profiles can be assigned this way. To assign custom profiles, see Assign configuration profiles to a node.]

5. Review and adjust the device properties. Click OK, Add Node.
Monitor Linux nodes in SCM

Starting with Server Configuration Monitor (SCM) 2019.4, you can monitor Linux nodes via Orion agent. Just as on Windows nodes, the SCM agent plugin must be installed on monitored nodes to monitor files, and the Asset Inventory agent plugin is required for HW and SW inventory profiles. Linux machines with Linux kernel 2.6.23 or later are supported.

The Orion agent runs under the swiagent user. For more information about the Orion agent, see SolarWinds Orion agent requirements.

To monitor your Linux environment, see this page for instructions on how to configure SNMP for agents deployed by SCM. (These instructions apply to SAM, SCM, and other products.) Once installed, it should auto-configure for you.

Monitor Linux files

The dialog for adding file elements remains the same, using the generic File profile elements. SCM automatically distinguishes between files with Linux filepaths, such as /etc/init.d/*.config and Windows filepaths, such as C:\Program Files\Solarwinds\*.config. You can monitor individual files or use wildcard characters to dynamically monitor any sub-directory and file. SCM also supports Linux system variables such as ${HOME}.
The polling is interval-based. The polling frequency setting is shared with Windows file polling.

**Monitor hardware and software**

Monitoring hardware and software inventory also works on Linux machines via the Asset Inventory Linux agent plugin.
Monitor a SQL database with SCM

You can now monitor databases for changes using Server Configuration Monitor (SCM), by running SQL queries to connect to any relational database such as Microsoft SQL Server, PostgreSQL, Oracle, or MySQL. SCM can collect data through SQL queries, then store that data and watch it for changes. This process enables SCM to track and alert you to changes made to user permissions, tables, indexes, views, stored procedures, scheduled jobs, and any other data you can gather using SQL queries.

Monitoring databases in SCM does not require an agent and can be performed on any type of node (Agent, WMI, SNMP, ICMP, and external). You must provide database account credentials required to monitor databases. Windows authentication is not supported. Along with supporting the use of credentials for databases, you can now add credentials for scripts and files. For more information on using credentials in SCM, see the SCM Administrator Guide topic, Specify element credentials in SCM.

Set up and install

To monitor a SQL element with Server Configuration Monitor (SCM), follow these instructions.

1. Ensure that you can connect to the SQL database and that your SQL server is set to allow remote connections.

2. The ODBC drivers are automatically installed with SCM 2020.2 or later unless FIPS is enabled on the system.

Configure SCM to monitor a Database query element

1. Open SCM and go to the Server Configuration Monitor Settings page.

2. Click the Profiles tab, and create new or edit an existing profile with a Database Query Element to test connectivity.
3. Select, modify, or create a new connection string using the drop-down menu.

4. Fill in or edit the element with the database query you want to test or that is collecting the desired configuration data.
5. Specify SQL credentials and click TEST to test the connection.

Note: Due to security concerns, SolarWinds recommends that you avoid using username and password values in the Connection String. Instead, use the ${username} and ${password} macros along with specified credentials to ensure that sensitive values are properly secured.

6. Select the node you want to test.
7. After following these steps, the test should be successful. The success of the test is indicated on your test results page.

However, if there is an issue, an error message is displayed to help you start troubleshooting.

Out-of-the-box database profiles

There are new out-of-the-box profiles available to help you maximize this functionality:

- MS SQL Server
- PostgreSQL
- MySQL

These out-of-the-box profiles provide a starting point for you to start monitoring your databases, and they can be customized to meet your organization's needs.

Additional notes on database monitoring

Users should take note of the following:

- The SQL element in SCM can use only 32-bit ODBC drivers to connect to a database. This is not an issue for the databases, which use ODBC drivers provided by SolarWinds. However, if you use different drivers that are 64-bit, they would not work.

- If you choose the Use Orion default credentials needed option and enter your login directly into the connection string, your credential information will be stored in the database in plaintext. Therefore, SolarWinds recommends that you use ${Username} and ${Password} macros and use credentials that are stored in the Orion Platform.
- ODBC drivers are not installed with SCM if you have FIPS enabled on your system.
Understand database queries in SCM

You can run SQL queries in Server Configuration Monitor (SCM) to connect to relational databases such as SQL Server, PostgreSQL, Oracle, and MySQL. When adding configuration elements for monitoring, there is now an option to choose the element type Database query. The connection string drop-down menu contains one example connection string for each pre-installed driver, and a list of all connection strings used in all elements. The following macros are available in the connection string:

- ${NodeIP} - IP address of polled database
- ${NodeHostname} - Hostname of polled database
- ${Username} - assigned credential username
- ${Password} - assigned credential password

The following is an example of a connection string:

```
Driver={MariaDB ODBC 3.1 Driver};Server=${NodeIP};User=${Username};Password=${Password};Option=3;Port=3306
```

Custom ODBC Drivers

You can poll the database with any other driver if you install it on the poller. Only 32-bit drivers are allowed because the process that it polls is a 32-bit process.
Server configuration profiles in SCM

Configuration profiles in Server Configuration Monitor (SCM) are collections of elements you want to monitor. Each profile element results in one or more configuration items (for example, individual files or registry entries) being monitored. There are several out-of-the-box profiles for commonly monitored elements, or you can create custom profiles with exactly the elements you want to monitor.
Out-of-the-box profiles in Server Configuration Monitor (SCM)

SCM comes with several predefined configuration profiles for server inventory and commonly monitored applications. These out-of-the-box configurations are:

- **HW Inventory**
- **SW Inventory**
- **IIS**
- **Linux Essentials**
- **Linux Security and Permissions**
- **Database profiles:**
  - MS SQL Server Essentials
  - PostgreSQL Essentials
  - MySQL Essentials

**HW inventory profiles in Server Configuration Monitor (SCM)**

The hardware (HW) inventory profile monitors changes to the server's hardware, including:

- Drivers
- Hard drives
- Logical drives
- Memory modules
- Network interfaces
- OutOfBand management
- Peripherals
- Processors
- Removable media
- Storage controllers
- Video card

Monitoring this profile requires that Asset Inventory be enabled on the server. To enable Asset Inventory:

1. Navigate to List Resources for the server you would like to monitor. There are multiple ways to get to List Resources:
From the Node Details Summary page, click List Resources in the Management widget.

- Click Settings > Manage Nodes. Select the node, and then click List Resources in the Node Management toolbar.

2. In the list that displays, check the box next to Asset Inventory.

3. Click Submit to save your changes.
SW inventory profiles in Server Configuration Monitor (SCM)

The software (SW) inventory profile monitors changes to:

- Firmware
- OS updates
- Server information
- Software installed

Monitoring this profile requires that Asset Inventory be enabled on the server. To enable Asset Inventory:

1. Navigate to List Resources for the server you would like to monitor. There are multiple ways to get to List Resources:
   - From the Node Details Summary page, click List Resources in the Management widget.
   - Click Settings > Manage Nodes. Select the node, and then click List Resources in the Node Management toolbar.

2. In the list that displays, check the box next to Asset Inventory.

3. Click Submit to save your changes.

IIS server configuration profiles in Server Configuration Monitor (SCM)

The IIS profile is the predefined profile for IIS servers. It monitors the following configuration files.

<table>
<thead>
<tr>
<th>Path</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%WINDIR%\Microsoft.NET**\machine.config</td>
<td>The machine.config for .NET Framework settings.</td>
</tr>
<tr>
<td>%WINDIR%\Microsoft.NET**\web.config</td>
<td>The root web.config for .NET Framework settings.</td>
</tr>
<tr>
<td>%WINDIR%\System32\inetsrv\MBSchema.xml</td>
<td>The MetaBase schema definition used in IIS 6.0 instead of applicationHost.config.</td>
</tr>
<tr>
<td>%WINDIR%\System32\inetsrv\MetaBase.xml</td>
<td>This configuration file is used in IIS 6.0 instead of applicationHost.config.</td>
</tr>
</tbody>
</table>
This configuration file stores the settings for IIS management. These settings include the list of management modules that are installed for the IIS Manager tool, as well as configuration settings for management modules.

IIS 7 and later support the management of several IIS servers from a single, centralized configuration file. This configuration file contains the settings that indicate the location where the centralized configuration files are stored.

The full schema reference for config files, including default values for all properties in every section, their valid ranges, etc.

Parsing applicationHost.config file to search for distributed configuration via web.config files specific for a particular IIS site, application or virtual directory and located within its directory.

All web.config files found from parsing applicationHost.config.

### Linux Essentials profiles in Server Configuration Monitor (SCM)

The Linux Essentials profile is the predefined profile for monitoring the essentials of your Linux system, including file system configuration, network settings, operating system and application software, and startup configuration.

<table>
<thead>
<tr>
<th>Path</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*/etc/apt/**/</td>
<td>Monitors all of the configuration files that apt uses as its sources.</td>
</tr>
<tr>
<td>fstab /etc/</td>
<td>Monitors the fstab configuration file.</td>
</tr>
<tr>
<td>Path</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>*/etc/init.d/**/</td>
<td>Monitors all of the configuration scripts used to control services.</td>
</tr>
<tr>
<td>*/etc/init/**/</td>
<td>Monitors the configuration files for the init subsystem used to start services.</td>
</tr>
<tr>
<td>inittab /etc/</td>
<td>Monitors the configuration file for the initialization system.</td>
</tr>
<tr>
<td>*/etc/modprobe.d/**/</td>
<td>Monitors all of the configuration files that are used by modprobe to manage the loading of modules during the system boot.</td>
</tr>
<tr>
<td>modules /etc/</td>
<td>Monitors the list of modules to load at boot time.</td>
</tr>
<tr>
<td>*/etc/modules-load.d/</td>
<td>Monitors the list of modules to load at boot time.</td>
</tr>
<tr>
<td>sysctl.conf /etc/</td>
<td>Monitors the configuration file that syscti uses to change kernel parameters at runtime.</td>
</tr>
<tr>
<td>*.conf /etc/sysctl.d/</td>
<td>Monitors the configuration files that syscti uses to change kernel parameters at runtime.</td>
</tr>
<tr>
<td>yum.conf /etc/</td>
<td>Monitors the file that yum uses for global configuration.</td>
</tr>
<tr>
<td>*/etc/yum.repos.d/</td>
<td>Monitors the files that define the extra repositories yum can use.</td>
</tr>
<tr>
<td>*/etc/yum/**/</td>
<td>Monitors the files that store extra yum configurations.</td>
</tr>
<tr>
<td>Listening Ports</td>
<td>Monitors the ports the system is listening on (excludes UDP).</td>
</tr>
<tr>
<td>Networking Items</td>
<td>Monitors for changes in your networking configuration, including the system’s DNS name and aliases, network interfaces, hosts file, resolve.conf file, and the nsswitch.conf file.</td>
</tr>
<tr>
<td>Services Configuration</td>
<td>Monitors the services that are enabled on the system.</td>
</tr>
<tr>
<td>Hardware Info</td>
<td>Monitors a detailed list of system information. List includes cpu (lscpu), general hardware (lshw), PCI bus (lspci), USB (lsusb), and SCSI (lsscsi).</td>
</tr>
<tr>
<td>Package List</td>
<td>Monitors all installed packages for changes (both rpm and dpkg).</td>
</tr>
<tr>
<td>Kernel Uname</td>
<td>Monitors the system's nodename, kernel-version, and kernel-release.</td>
</tr>
<tr>
<td>Block Device List</td>
<td>Monitors changes to file system block devices (via lsblk).</td>
</tr>
<tr>
<td>Mounted Filesystems</td>
<td>Monitors changes to file system mounts.</td>
</tr>
</tbody>
</table>
Linux Security and Permission profiles in SCM

The Linux Security and Permissions profile in Server Configuration Monitor (SCM) is the predefined profile for monitoring security, groups, and user permissions.

<table>
<thead>
<tr>
<th>Path</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group /etc/</td>
<td>Monitors the group configuration file, which defines the groups to which users belong.</td>
</tr>
<tr>
<td>login.defs /etc/</td>
<td>Monitors configurations that are used as defaults by user and group utilities.</td>
</tr>
<tr>
<td>pam.conf /etc/</td>
<td>Monitors the configuration file used by PAM to define user access to server resources and applications.</td>
</tr>
<tr>
<td>*/etc/pam.d/</td>
<td>Monitors the configuration files used by PAM to define user access to server resources and applications.</td>
</tr>
<tr>
<td>passwd /etc/</td>
<td>Monitors the file that contains the attributes of all users or accounts on the system.</td>
</tr>
<tr>
<td>*.conf /etc/security/**/</td>
<td>Monitors the configuration files that control the resources available to user processes. Often used by PAM modules.</td>
</tr>
<tr>
<td>*/etc/selinux</td>
<td>Monitors the configuration files that control the behavior of Security Enhanced Linux.</td>
</tr>
<tr>
<td>World Writable Files</td>
<td>List of files that are world writable.</td>
</tr>
</tbody>
</table>

Database profiles in SCM

Server Configuration Monitor (SCM) offers a number of out-of-the-box database profiles. See the table below for compatible versions and a comparison of the information you can track in each database profile type:
<table>
<thead>
<tr>
<th>Versions of database software that are compatible with SCM out-of-the-box profiles</th>
<th>MS SQL Server Essentials</th>
<th>PostgreSQL Essentials</th>
<th>MySQL Essentials</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• MS SQL 2012 and later</td>
<td>• PostgreSQL 12.1</td>
<td>• MySQL 8.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PostgreSQL 11.6</td>
<td>• MySQL 5.7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PostgreSQL 10.11</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PostgreSQL 9.6.16</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PostgreSQL 9.5.20</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PostgreSQL 9.4.25</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Global</th>
<th>• Configuration registry entries</th>
<th>• Server settings</th>
<th>• Version information</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Query optimizer hotfixes</td>
<td>• Time zones</td>
<td>• Global variables</td>
</tr>
<tr>
<td></td>
<td>• Instant file initialization</td>
<td>• Collations</td>
<td>• Character sets and collations</td>
</tr>
<tr>
<td></td>
<td>• Server configuration</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Server properties</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SSIS packages</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Server configuration</th>
<th>• Linked servers</th>
<th>• Publications</th>
<th>• Engines</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Database files</td>
<td>• Configuration files</td>
<td>• Plugins</td>
</tr>
<tr>
<td></td>
<td>• Database mail</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Database options</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Default data and log location</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• TempDB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DB Schema</td>
<td>MS SQL Server Essentials</td>
<td>PostgreSQL Essentials</td>
<td>MySQL Essentials</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------</td>
<td>--------------------------</td>
<td>-----------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Filegroups</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tables</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Columns</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Views</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indexes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Triggers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stored procedures</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System database objects</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Databases</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tablesites</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tables</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Views</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attributes (Columns)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indexes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Procedures and functions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Users</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Users and privileges                                                     |                          |                       |                  |
| Logins                                                                   |                          |                       |                  |
| Permissions                                                              |                          |                       |                  |
| Security                                                                 |                          |                       |                  |
| Suspect pages                                                            |                          |                       |                  |
| Database roles                                                           |                          |                       |                  |
| Authentication rules                                                     |                          |                       |                  |
| Users                                                                    |                          |                       |                  |
| Administrable role authorization                                        |                          |                       |                  |
| Enabled roles                                                            |                          |                       |                  |
| Database privileges (schema)                                             |                          |                       |                  |
| Table privileges                                                         |                          |                       |                  |
| User privileges                                                          |                          |                       |                  |
| Column privileges                                                        |                          |                       |                  |
| Role table grants                                                        |                          |                       |                  |
| Role column grants                                                       |                          |                       |                  |
| Role routine grants                                                      |                          |                       |                  |

<table>
<thead>
<tr>
<th>Events and jobs</th>
<th>SQL agent jobs</th>
<th>Events</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>MS SQL Server Essentials</td>
<td>PostgreSQL Essentials</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>--------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td><strong>Backup and recovery, mirroring</strong></td>
<td>• Database backup</td>
<td>• Subscriptions</td>
</tr>
<tr>
<td></td>
<td>• Recovery mode</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Mirroring</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• High availability</td>
<td></td>
</tr>
<tr>
<td><strong>Policy</strong></td>
<td>• Policy management</td>
<td></td>
</tr>
</tbody>
</table>
User restrictions in Server Configuration Monitor (SCM)

In order to make changes to profiles, profiles assignments, and data retention settings in Server Configuration Settings, a user must have the SCM role Admin and node management rights. These permissions can be granted or revoked through Manage Accounts.
Assign configuration profiles to a node in Server Configuration Monitor (SCM)

To begin monitoring server configurations, you must assign one or more configuration profiles to the server. There are multiple ways to assign configuration profiles:

**Through Server Configuration Monitor Settings**

1. Navigate to Server Configuration Monitor Settings, either from the link in the upper right of the Server Configuration Monitor Summary page or by going to Settings > All Settings > Server Configuration Monitor settings under the Product Specific Settings heading.

2. Pick either the Profiles tab or the Monitored Nodes tab. If you need to assign profiles to a node that is not already in SCM, choose Monitored Nodes.
   a. From Profiles:
      i. Select the profiles to assign, and click Assign To in the ribbon.
ii. Choose the nodes to assign the profiles to, then click Next.

iii. If you are required to set credentials (for database elements) or want to set optional credentials for other types of elements such as file elements, registry elements, or script elements, do so by following the prompts to set credentials.
Assign configuration profiles

Set credentials

Set credentials required by specific element types. If desired, set additional credentials as well. If you need more granular credentials settings, set them later on the Assigned elements page.

DATABASE QUERY: 31 elements found in 1 profile

Connection string

Select existing connection string or add new one...

Pick the connection string that matches the database type you want to monitor. You can use the following macros: $1(NodeF), $2(NodeHostname), $3(Username), and $4(Password). These macros will be substituted with the appropriate values during execution. Windows authentication is not supported, so you must provide database account credentials. Learn more about database queries.

Credentials

Select existing credentials or add new ones...

or
b. From Monitored Nodes:
   
i. Select the node(s) to assign profiles to from the list of nodes already in SCM, then choose Assign Profiles.
   If you do not see the node you want to assign profiles to, click Set Up Configuration
Monitoring to add a new node to SCM.
ii. Select the profiles to assign, then click Next.

iii. If you are required to set credentials (for database elements) or want to set optional credentials for other types of elements such as file elements, registry elements, or script elements, do so by following the prompts to set credentials.
Assign configuration profiles

Set credentials

Set credentials required by specific element types. If desired, set additional credentials as well. If you need more granular credentials settings, set them later on the Assigned elements page.

DATABASE QUERY: 25 elements found in 1 profile

Connection string

Select existing connection string or add new one...

Pick the connection string that matches the database type you want to monitor. You can use the following macros: $(Node), $(NodeHostname), $(Username), and $(Password). These macros will be substituted with the appropriate values during evaluation. Windows authentication is not supported, so you must provide database account credentials. Learn more about database queries.

Credentials

Select existing credentials or add new ones...

SET ADDITIONAL CREDENTIALS

ELEMENT TYPE

File
Linux script

< BACK NEXT CANCEL

or
3. Review the assignments on the summary page. Here you will see warnings if there are any potential polling issues detected, such as Asset Inventory being disabled on a node when assigning a profile that requires it. You can still assign profiles if a warning occurs, but SCM will
not start collecting that data until the conflict is resolved. You also have the option to re-check problems and click Confirm to finish the assignment.

Through List Resources

Out-of-the-box profiles can be assigned through a node's List Resources.

1. Navigate to List Resources for the server you would like to monitor. There are multiple ways to get to List Resources:
   - From the Node Details Summary page, click List Resources in the Management widget.
   - Click Settings > Manage Nodes. Select the node, then click List Resources in the Node Management toolbar.

2. Under Server Configuration, select the profiles you want to assign or unassign.

   Custom profiles are not included in List Resources.

3. Click Submit to save your changes.

From the Server Configuration Summary page

Custom and out-of-the-box profiles can be assigned from the Server Configuration Summary page.
1. Navigate to My Dashboards > Server Configuration Summary.

2. In the Server Configuration Nodes widget, click Assign Configuration Profiles, or in the Candidate for Server Configuration Monitoring widget, click Assign profile to assign a profile to a node.

3. Select the profiles you wish to assign, then click Next.

4. Select the nodes to which those profiles should be assigned, then click Next. The list of nodes can be filtered by node properties, including custom properties.

5. If needed or desired, set credentials.

6. Review the profile assignments, then click Confirm to finish the profile assignments. Be sure to note potential errors that are indicated, including unsupported node assignments or improper combinations of profiles and nodes.

**Assign or unassign from the Manage Nodes page**

You can assign a profile to a selected node or unassign a profile from a selected node directly from the Manage Nodes page in Server Configuration Monitor (SCM). There is also an optional column on the Manage Nodes grid so you can view which profiles are assigned to selected nodes.
Unassign configuration profiles in Server Configuration Monitor (SCM)

This task is not available to all users. See User restrictions for details.

There are two ways to unassign configuration profiles:

**Through Server Configuration Monitor Settings**

1. Navigate to Server Configuration Monitor Settings, either from the link in the upper right of the Server Configuration Monitor Summary page or by going to Settings > All Settings > Server Configuration Monitor Settings.
2. Switch to the Monitored Nodes tab.
3. Select the node(s) you want to unassign profiles from.
4. Click Unassign Profiles on the ribbon.
5. Select the profiles you want to unassign, and then click Unassign.
6. You will be prompted with a question about keeping historical data. You can choose to keep the data SCM has collected from the unassigned profiles if you would like to see that information when looking at the configuration history. If you choose to delete the data, that history will be gone. Click either Keep Data or Delete Data to finish the unassignment.

**Through List Resources**

Out-of-the-box profiles can be unassigned through a node’s List Resources. There is no option to keep the historical data if unassigning profiles this way.

1. Navigate to List Resources for the server you would like to monitor. There are multiple ways to get to List Resources:
   - From the Node Details Summary page, click List Resources in the Management widget.
   - Click Settings > Manage Nodes. Select the node, then click List Resources in the Node Management toolbar.
2. Under Server Configuration, select the profiles you want to assign or unassign.

Custom profiles are not included in List Resources.
3. Click Submit to save your changes.

You may want to assign the same profile(s) to multiple servers. Instead of assigning and unassigning each profile individually, you can assign and unassign profiles in bulk.

**From the Manage Nodes page**

See instructions for [unassigning configuration profiles from the Manage Nodes page](#).
Monitor configuration changes on a node in SCM

In Server Configuration Monitor (SCM), set up configuration monitoring on a server, see suggestions of servers to monitor, and see the recent changes.

This assumes you have already added the node to the Orion Platform. See Add a node to SCM for details.

To begin monitoring server configurations, you must assign one or more configuration profiles to the server.

- See detected candidates for configuration monitoring
- Learn about near real-time change detection
- Monitor who made server configuration changes
- Enable near real-time file monitoring
- Test SCM profile elements before deploying

See detected candidates for configuration monitoring in Server Configuration Monitor (SCM)

SCM will automatically detect servers that have been added to the Orion Platform that might be eligible for monitoring one or more of the out-of-the-box profiles. You can view a list of candidate servers on the SCM Summary page, which can be found under My Dashboards.

The Candidates for Server Configuration Monitoring widget lists servers that might be eligible for configuration monitoring but do not have an agent, and servers that are eligible for monitoring each out-of-the-box profile. From there, you can push agents or assign the suggested profiles using the links provided. The Dismiss all link will stop those nodes from being suggested again.

Whether a node is eligible for configuration monitoring is determined in the following ways:

<table>
<thead>
<tr>
<th>Suggested action</th>
<th>Eligibility requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Push an agent</td>
<td>Any node running Windows Server 2008 R2 SP1 or later</td>
</tr>
<tr>
<td></td>
<td>OR</td>
</tr>
<tr>
<td></td>
<td>Any node running Linux kernel 2.6.23 or later</td>
</tr>
<tr>
<td>Assign HW/SW inventory profiles</td>
<td>Any node with AssetInventory enabled</td>
</tr>
</tbody>
</table>
Assign an out-of-the-box profile

If the node is monitored by a respective SAM application, it’s a candidate for SCM monitoring by a specific profile. For example, any node monitored by AppInsight for IIS, or another SAM app template tagged as 'IIS' is a candidate for SCM monitoring by IIS configuration profile.

Learn about near real-time change detection in SCM

Server Configuration Monitor (SCM) offers near real-time change detection to provide a more granular representation of changes to your environment. Rather than a view of periodic, aggregated server configuration changes, SCM actively listens to identify and track changes to configurations as they occur. This enables SCM users to see the full spectrum of changes that occurs between polling cycles so that they can proactively anticipate performance impacts.

The SCM agent plug-in requires deployment of the File Integrity Monitor to monitored servers to enable the capture of any file change in near real time and to indicate who made the change. To use this feature, you must turn on near real-time file monitoring, which enables 'who made the change monitoring.' See the topic Enable near real-time file monitoring and 'who made the change' detection for instructions.

When near real-time monitoring is disabled:

- File/parsed file elements use IntervalWatcher instead.
- Registry elements use RegistryWatcher instead.

When real-time monitoring is enabled:

- Parsed/file elements use the FIM driver, and 'who made the change' detection is enabled to show who made changes to server configurations.
- Registry elements use the FIM driver, and 'who made the change' detection is enabled to show who made changes to server configurations.

Monitor who made server configuration changes

Server Configuration Monitor (SCM) comes with a 'who made the change' detection capability to monitor who made server configuration changes. To use this feature, you must turn on near real-time file monitoring, which enables 'who made the change monitoring.' See the topic Enable near real-time file monitoring and 'who made the change' detection for instructions.

There are some limitations to the 'who made the change' functionality, which are described below, along with the messages a user may encounter in SCM when the 'who' value cannot be detected.
When is 'who made the change' detection available?

Consult the following table to determine when 'who made the change' detection is available.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Agent-less</th>
<th>Via agent</th>
<th>Supports 'Who made the change' detection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Software</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Registry (Windows only)</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows files</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Linux files</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>PowerShell</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Linux script</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Database</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

In addition, the following conditions affect 'who made the change' data:

- Historical data is lost if you switch the collection of hardware and software data between remote and agent.
- When looking at the profile, the 'who' value is displayed only when the most recent change is from an element that supports collecting 'who' information.
<table>
<thead>
<tr>
<th>Message Displayed in SCM</th>
<th>Explanation</th>
</tr>
</thead>
</table>
| The 'who' value is not available because this change event was not captured in time. Learn more. | SCM cannot determine 'who' made the change, as this change was not detected at the exact time it occurred. For example, the change was detected:  
  - After the node was remanaged.  
  - After the agent was restarted.  
  - When 'Poll Now' was triggered. |
| The 'who' value is not available because real-time change detection was disabled. Learn more. | The SCM polling method does not allow capture of 'who' made the change when real-time change detection is disabled. |
| The 'who' value is not available because more than one change was detected at the same time. Learn more. | When more than one change event is detected at the same time, SCM cannot determine the usernames associated with each change. |
| The 'who' value is not available because the changes were aggregated according to data retention settings. Learn more. | SCM cannot determine which username to associate with this change after changes are aggregated according to data retention settings. |
| The 'who' value is not available because this node is explicitly excluded from enhanced change detection. Learn more. | Even though global real-time polling is enabled, the selected node was specifically excluded from real-time polling in enhanced change detection settings. SCM does not collect the usernames associated with changes when real-time polling is not enabled. |
Enable near real-time file monitoring and 'who made the change' detection in Server Configuration Monitor (SCM)

To enable near real-time file monitoring and 'who made the change' detection, take the following steps:

1. Log into the Orion Web Console.
2. Click Settings > All Settings.
4. Select the Polling Settings tab, and at the right of your screen, click the switch to turn on 'Who made the change' detection.

5. Click Continue to Setup.
6. If there are nodes on which you do not want the FIM driver installed, you can exclude those nodes from near real-time monitoring and 'who made the change' detection by clicking Add exclusions. Then click Enable who detection.

![Who made the change' detection setup](image)

**Test SCM profile elements before deploying them**

Server Configuration Monitor (SCM) now features a TEST button for monitoring in the Add/Edit/View configuration element dialog box. Test any type of element to see whether it works on one of your monitored nodes before you deploy it to your servers.

1. To use the test function, add a configuration element for monitoring, and then select credentials from the drop-down menu under Access authentication.
Add configuration element

Element type
Linux script

Element name
script
This is the name used when referring to this configuration element.

Command line
bash ${Script-file}

e.g. "python ${Script-file}" where ${Script-file} macro is referring to the generated script file with content defined below.

Script file content

date

Working directory for script  Optional

Polling frequency [hh:mm:ss]  Polling timeout [hh:mm:ss]
00:05:00  00:01:00

Description  Optional

Access authentication
Configuration element may not be able to poll necessary information without proper access rights for specific server or database etc. Add necessary credentials if needed.

Use Orion default credentials

ADD  TEST  CANCEL
2. After setting the credential, click TEST.

SCM displays a list of nodes on your machine from which you can choose. (In the following example, a Linux machine is selected, as the user wants to execute a bash command.)
3. Click Select & Test.

4. SCM displays your test result.

See the following example of a successful test result:

See the following example of a successful test result using a file wildcard definition that returned multiple configuration items:
See the following example of a failing test result:

Learn about baselines in SCM

In Server Configuration Monitor (SCM), each node can have a snapshot of all configuration items from all profiles at a particular date set as its baseline configuration. A baseline is the ideal or standard configuration for that node. It is the configuration against which you want to judge that node going forward.
Define or redefine a baseline individually or in bulk

Baselines can be set from the Compare Configurations page, or from the Configuration Details widget on the SCM subview of a Node Details page.

- When comparing two configurations, if you would like to set one of them as the baseline, click the three dots to the right of the datetime and choose Set as baseline.
- From Node Details, if you would like to set the current configuration as the baseline, click Set as baseline in the upper right of the Configuration Details widget.

If a profile is assigned to a node after the baseline is defined, those configuration items are not included in the baseline.

After a baseline is set on a node, it can be reset or redefined if desired. You can also set or reset baselines for multiple nodes or all nodes at once. This capability saves time and reduces the number of adjustments you need to make in SCM. This feature can facilitate the roll-out of SCM across a large environment or help you to make need bulk changes as needed.

To redefine or delete all baselines at once:

1. Go to Settings > All Settings.
2. Under Product Specific Settings, click Server Configuration Monitor Settings.
3. Click the Monitored Nodes tab.
4. Select the desired profiles and then click Redefine Baselines or Delete Baselines as applicable.
Compare configurations over time in Server Configuration Monitor (SCM)

You can use SCM to see which configuration items changed between any two points in time, and drill down even further to see line by line what changes were made.

See recent configuration changes in Server Configuration Monitor (SCM)

To see the most recent configurations from all monitored nodes, find the Recent Configuration Changes widget on the Server Configuration Summary dashboard.

This widget shows all configuration changes in the selected time interval. Each row shows the name of the profile in bold, the node the change was made on, and the element name/path. The color to the left of each entry indicates the type of change: yellow for addition, blue for an update, and red for removal. Clicking a row will take you to a comparison between the two most recent versions.

The initial poll is not included in the list of all configuration changes. The initial data is not considered a change, since there was no previous data to compare to.

To see the most recent configuration changes on a particular node, see the Recent Configuration Changes widget on the Server Configuration page of Node Details.

See configuration changes between two points in time using SCM

Server Configuration Monitor (SCM) lets you see the difference between versions of a server’s configuration. You can see which configuration elements were added, deleted, or modified and how file attributes have changed. If is enabled for a particular element, you can also see which lines of that element were added, deleted, or modified.

See which configuration elements changed

To see which configuration elements were changed between two points in time:

1. From the Node Details page of the server you would like to monitor, navigate to the Server Configuration view in the left sidebar.
2. In the Configuration Management widget, click Compare Configuration.

3. In Configuration Comparison, you are presented with two side-by-side panels that show the monitored configuration items for that node, organized by profile and element type. By default, this comparison is between the current configuration and the baseline. If no baseline is set, the comparison is instead between the current configuration and 24 hours prior.
   a. To change the date and time displayed, click the datetime on either side and select a new date and time. If a baseline is set, you can select it quickly from the datetime selection pop-up.

4. Below the configuration item comparison panels (if there are configuration item changes), you can view changes to file attributes such as permissions.

See line-by-line changes

1. Follow the steps above, or find the Configuration Details widget on the Server Configuration view of the Node Details page.

2. Click the item you want to examine the contents of.

The Content Comparison page that opens shows a line comparison of the element’s contents at the times specified on the previous page. Unchanged lines will be collapsed by default, but can be expanded by clicking on the number of unchanged lines.

Use color-coding

There are two color-coding modes for the change comparison pages: simplified, and change-type-based. With simplified color-coding, all changes are highlighted in yellow. With change-type-based color-coding, additions are shown in green, deletions in red, and modifications in blue.

To switch color-coding modes, click the three dots in the upper right of either comparison page.

Set character encoding

By default, all items in the line-by-line comparison are displayed using UTF-8 encoding. Changing the encoding changes only the way the item is displayed and does not alter the underlying data. In environments that contain other character types, such as Japanese or Traditional Chinese, users can select the appropriate encoding settings so that characters are displayed correctly when viewing content comparisons.
To select encoding settings from the SCM home screen, under Recent Configuration Changes, click on a node to view Node Details. Next, click Configuration Comparison, and then click the three dots at the upper right of the page. Select Show encoding settings.

Next, select the appropriate character encoding type from the drop-down list and click Save.

Changing the encoding for one item changes the encoding for all other configuration items created by the same profile element. For example, if you have a File element in a profile that uses a wildcard character to match all the files in a certain directory, changing the encoding for one of those files changes the encoding for all the files in the directory.

View multiple versions of comparison content

SCM displays a list of each unique copy of the content over time. It handles aggregation of versions, so the tracked changes roll up, and the most recent content is shown. SCM saves the number of changes that are made in that time period, and it allows you to drill down to previous versions.
To select a version from the version picker on the Content Comparison page, click the hyperlinked date above the comparison panels. You can select any of the versions listed to view it.

If aggregation occurred, you can see it in this version picker drop-down menu. The number of aggregations are listed to the right of the version time information.

Download or copy comparison content

You can now download or copy comparison content to the clipboard. Click the three dots on the top right side of the Comparison page, and select Copy to clipboard or Download file from the drop-down menu.

⚠️ The copy comparison content feature is available on Chromium-based browsers only.
View the structural diff in SCM

Structural diff mode has been added to the Content diff mode page in Server Configuration Monitor (SCM). If the diff engine recognizes valid JSON or XML, structural diff is used for comparison by default. Structural diff means that content of JSON or XML files is compared by its values. Spaces, element positions, and other characters are not compared. If the file is invalid, then textual diff is used instead.

![Content Comparison](image)

Correlate configuration changes to performance metrics in SCM

In Server Configuration Monitor (SCM), you can see how a change in server configurations may have affected the server’s performance by viewing changes on a timeline with performance metrics using the Performance Analysis Dashboard (PerfStack™).

1. Navigate to the Node Details Summary page for the node you want to examine.
2. In the Management widget, click Performance Analyzer.

Configuration changes will be shown at the bottom in blue. The X-axis shows time, and the Y-axis of the SCM portion shows how many changes were made. To view configuration change details, hover over a column of changes and click the Inspect selection in the data explorer icon. Change details are displayed in the Data Explorer to the left.
You can also manually add Server Configuration Changes to any custom PerfStack view.

1. Select a node in the Metrics Palette.
2. Find Server Configuration Changes under Status, Events, Alerts.
3. Drag and drop Server Configuration Changes into the PerfStack view.
Change how long configuration data is kept in Server Configuration Monitor (SCM)

This task is not available to all users. See User restrictions for details.

SCM retains configuration data at three levels of granularity: detailed, hourly, and daily. Detailed data is every change detected for every configuration item. Hourly data is the most recent change detected within the hour for each configuration item. Daily data is the most recent change detected within a calendar day for each configuration item.

Data retention settings do not affect the data for a node’s baseline configuration. Baseline information is kept forever.

By default, detailed data is kept for 7 days, hourly data is kept for 30 days, and daily data is kept for 365 days.

The default values for each level of granularity can be changed in SCM Settings:

1. Navigate to Server Configuration Monitor Settings, either from the link in the upper right of the Server Configuration Monitor Summary page or by going to Settings > All Settings > Server Configuration Monitor Settings.

2. Click the Data Retention tab.

3. Change the settings for each level of data as desired, and then click Save Changes.