Monitoring SQL Servers

Microsoft: SQL Server Enhanced PowerPack version 104, rev. 1

Table of Contents

Chapter

1

Introduction

Overview

This manual describes how to monitor Microsoft SQL Servers in SL1 using the *Microsoft: SQL Server Enhanced* PowerPack.

The following sections provide an overview of SQL Servers and the *Microsoft: SQL Server Enhanced* PowerPack:

NOTE: ScienceLogic provides this documentation for the convenience of ScienceLogic customers. Some of the configuration information contained herein pertains to third-party vendor software that is subject to change without notice to ScienceLogic. ScienceLogic makes every attempt to maintain accurate technical information and cannot be held responsible for defects or changes in third-party vendor software. There is no written or implied guarantee that information contained herein will work for all third-party variants. See the End User License Agreement (EULA) for more information.

What Does the Microsoft: SQL Server Enhanced PowerPack Monitor?

The *Microsoft: SQL Server Enhanced* PowerPack enables you to discover, model, and collect data about SQL 2008, 2012, 2014, and 2016 servers and their component devices.

The *Microsoft: SQL Server Enhanced* PowerPack includes:

- An example credential you can use to create PowerShell credentials to connect to SQL Servers
- Dynamic Applications to discover and monitor SQL Servers and their component devices
- Device Classes for each type of SQL Server component device monitored by SL1
- Event Policies and corresponding alerts that are triggered when SQL Servers and their component devices meet certain status criteria

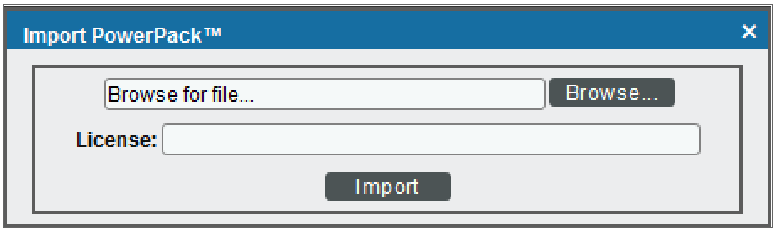
Installing the Microsoft: SQL Server Enhanced PowerPack

Before completing the steps in this manual, you must import and install the latest version of the *Microsoft: SQL Server Enhanced* PowerPack.

TIP: By default, installing a new version of a PowerPack overwrites all content from a previous version of that PowerPack that has already been installed on the target system. You can use the ***Enable Selective PowerPack Field Protection*** setting in the **Behavior Settings** page (System > Settings > Behavior) to prevent new PowerPacks from overwriting local changes for some commonly customized fields. (For more information, see the ***System Administration*** manual.)

To download and install a PowerPack:

1. Download the PowerPack from the ScienceLogic Customer Portal.
2. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).
3. In the **PowerPack Manager** page, click the **[Actions]** button, then select *Import PowerPack*.
4. The **Import PowerPack** dialog box appears:



5. Click the **[Browse]** button and navigate to the PowerPack file.
6. When the **PowerPack Installer** modal page appears, click the **[Install]** button to install the PowerPack.

NOTE: If you exit the **PowerPack Installer** modal without installing the imported PowerPack, the imported PowerPack will not appear in the **PowerPack Manager** page. However, the imported PowerPack will appear in the **Imported PowerPacks** modal. This page appears when you click the **[Actions]** menu and select *Install PowerPack*.

Chapter 2

Configuration and Discovery

OverviewConfiguration and Discovery

The following sections describe how to configure and discover Microsoft SQL Servers for monitoring in SL1 using the *Microsoft: SQL Server Enhanced* PowerPack:

NOTE: If you already have Windows Server discovered, you might not need to create a new SQL Server credential or run a separate discovery session for SQL Servers if the PowerShell credential information is the same as that used for the Windows Server credential. In this scenario, you need only to install the *Microsoft: SQL Server Enhanced* PowerPack and ensure that the Windows user account used in the credential has the appropriate permissions, as outlined in the ***Prerequisites*** section.

Prerequisites for Monitoring SQL Servers

To configure the SL1 system to monitor SQL servers using the *Microsoft: SQL Server Enhanced* PowerPack, you must first have the following information about the SQL Servers that you want to monitor:

- IP addresses and ports for the SQL Servers
- Username and password for a Windows user account with access to the SQL Servers

The SQL Servers that you monitor must be running PowerShell version 3.0 or later and need to have the SQL Server PowerShell (SQLPS) module installed. This SQLPS module is installed by SQL Server Management Studio. You can also install the SqlServer PowerShell module found here: https://www.powershellgallery.com/packages/Sqlserver/21.1.18218

To determine if the proper cmdlets are available for this PowerPack to collect, run `Get-Command Invoke-SqlCmd` to see if the Invoke-SqlCmd cmdlet is installed.

In addition, the *Microsoft: SQL Server Enhanced* PowerPack requires the following permissions for the user account used for monitoring:

- SQL 2014 and newer versions require one of the following configurations:
    - The user account has an enabled login on every instance and database to be monitored, with CONNECT SQL, VIEW SERVER STATE, and CONNECT ANY DATABASE permission granted to the login on each instance. The login should have VIEW DATABASE STATE permission and DB_DATAREADER role granted on the 'master' database, and the DB_DATAREADER role granted on the 'msdb' database.
    - The user account has an enabled login on every instance and has the SYSADMIN role.
- SQL 2008 to SQL 2012 versions require one of the following configurations:
    - The user account has an enabled login on every instance and database to be monitored, with CONNECT SQL and VIEW SERVER STATE granted to the login on each instance. The login should also have VIEW DATABASE STATE permission and the DB_DATAREADER role granted on the 'master' database, and the DB_DATAREADER role granted on the 'msdb' database. In addition, every database in the instance should have CONNECT access granted to the login.
    - The user account has an enabled login on every instance and has the SYSADMIN role.

ScienceLogic provides a PowerShell script on the ScienceLogic customer portal that automates the permissions-granting that is required as stated above. The script can be downloaded here: https://portal-cdn.sciencelogic.com/powerpackextras/5819/19047/winrm_configuration_wizardv3.0.zip

After downloading the script, perform the following steps:

1. Copy the winrm_configuration_scriptv3.0.zip file to the Windows server where Microsoft SQL Server is installed and from which you will be collecting data. Unzip the file.
2. Using the credentials for an account that is a member of the Administrator's group, log in to the Windows server you want to monitor. You can log in directly or use Remote Desktop to log in.
3. Right-click on the Windows PowerShell icon and select ***Run As Administrator***.

4. At the Windows PowerShell prompt, navigate to the directory where you unzipped the PowerShell script named winrm_configuration_wizard.ps1.
5. At the PowerShell prompt, enter the following to enable execution of the script:

```
Set-ExecutionPolicy -ExecutionPolicy Unrestricted -Scope Process -Force
```

> **NOTE:** The execution policy setting persists only during the current PowerShell session.

6. After the warning text, select Y.
7. To set the required, least-privileged permissions for the user account SL1 will use to monitor all SQL Server instances and databases on the server, run the following script:

```
.\winrm_configuration_wizard.ps1 -user <domain>\<username> -sql_only
```

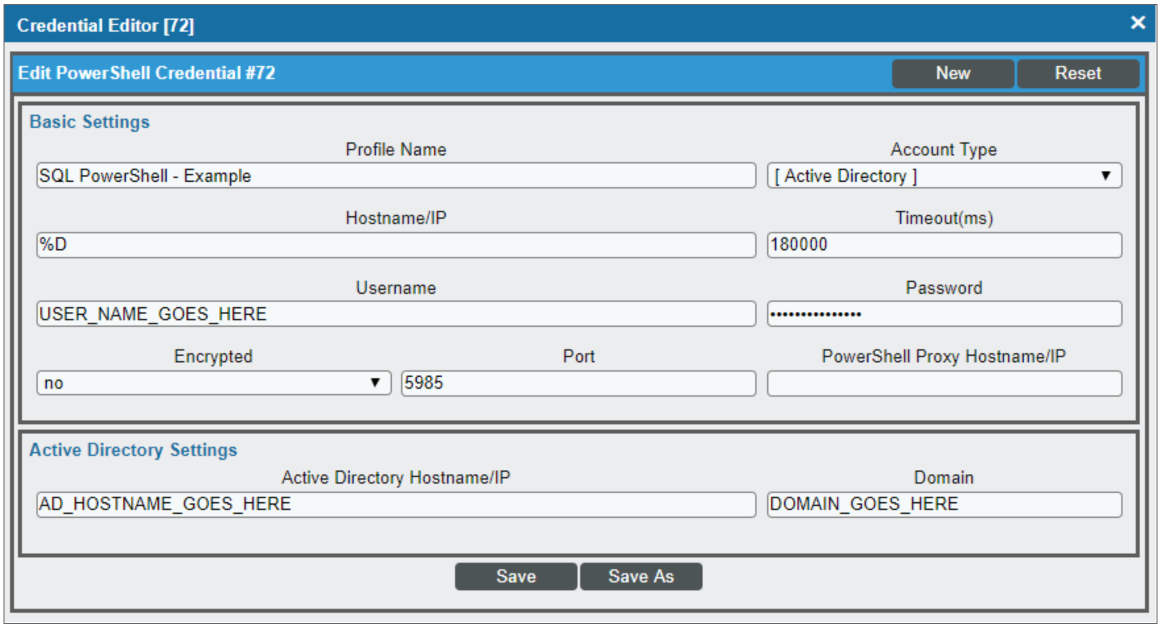
Creating a PowerShell SQL Server Credential

To configure SL1 to monitor SQL Servers, you must first create a PowerShell credential. This credential allows the Dynamic Applications in the *Microsoft: SQL Server Enhanced* PowerPack to connect with an SQL Server. An example PowerShell credential that you can edit for your own use is included in the PowerPack.

To create a PowerShell credential for an SQL Server:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the **SQL PowerShell - Example** credential, and then click its wrench icon (🔧). The **Edit PowerShell Credential** modal page appears.

3. Complete the following fields:



Edit PowerShell Credential #72

Basic Settings

Profile Name	SQL PowerShell - Example
Account Type	[Active Directory] ▼
Hostname/IP	%D
Timeout(ms)	180000
Username	USER_NAME_GOES_HERE
Password	•••••••••••••••
Encrypted	no ▼
Port	5985
PowerShell Proxy Hostname/IP	

Active Directory Settings

Active Directory Hostname/IP	AD_HOSTNAME_GOES_HERE
Domain	DOMAIN_GOES_HERE

- ***Profile Name***. Type a new name for your SQL Server credential.
- ***Account Type***. Select *Active Directory*.
- ***Hostname/IP***. Type "%D".
- ***Timeout***. Type "18000".
- ***Username***. Type the username for a Windows user with access to the SQL Server.
- ***Password***. Type the password for the Windows account username.

> NOTE: The user account whose username and password are provided in the credential must have certain permissions in all SQL Server instances that SL1 will monitor. For a list of these permissions, see the *Prerequisites* section.

- ***Encrypted***. Select *no*.
- ***Port***. Type "5985".
- ***PowerShell Proxy Hostname/IP***. Leave this field blank.
- ***Active Directory Hostname/IP***. Specify the hostname or IP address of the Active Directory server that will authenticate the credential.
- ***Domain***. Specify the domain where the monitored SQL Server resides.

4. Click the **[Save As]** button.
5. When the confirmation message appears, click **[OK]**.

SQL Cluster Monitoring

For SQL Clusters that only include SQL Instances in an Active/Active configuration, follow the steps in the *Discovering SQL Servers* section.

For SQL Clusters that include an SQL Instance in an Active/Passive configuration, additional discovery steps are required and listed below.

> **NOTE:**SL1's Active/Passive SQL Instance monitoring leverages the SL1 GUID Component Identifier to allow the SQL Instance component and its child database components to move between SQL Servers during a failover. Adding this GUID Component Identifier on SL1 versions prior to 8.12.1 will create a duplicate SQL Instance component on any already discovered SQL Servers. To prevent this, the GUID Component Identifier is not used by default. The "Enable Active Passive Cluster Failover" threshold in the "Microsoft: SQL Server Discovery" Dynamic Application provides the option to use the GUID Component Identifier when enabled. A value of "0" in the ***Threshold Value*** disables Active/Passive cluster failover; a value of "1" enables it.

Monitoring SQL Clusters on SL1 8.12.1 or greater.

1. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).
2. Click the wrench icon (🔧) for the "Microsoft: SQL Server Discovery" Dynamic Application to open the **Dynamic Applications Properties Editor**page.
3. In the **[Thresholds]** tab, click the wrench icon (🔧) for the "Enable Active Passive Cluster Failover" threshold and change the ***Threshold Value*** to *1*.
4. Click **[Save]**.
5. Follow the steps in the *Discovering SQL Servers* section on each Windows Server in the cluster.

Monitoring SQL CLusters on SL1 8.8.1 to 8.12.0

1. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).
2. Click the wrench icon (🔧) for the "Microsoft: SQL Server Discovery" Dynamic Application to open the **Dynamic Applications Properties Editor**page.
3. In the **[Properties]** tab, change the ***Operational State*** field to *Disabled*.
4. Click **[Save]**.
5. Follow the steps in the *Discovering SQL Servers* section on each Windows Server in the cluster.
6. Go to the **Device Components** page (Registry > Devices > Device Components).
7. Click the wrench icon (🔧) for one of the Windows Servers that make up the SQL Cluster to open its **Device Properties** page.

8. In the **[Thresholds]** tab, under **Dynamic App Thresholds | Microsoft: SQL Server Discovery**, change ***Enable Active Passive Cluster*** to *1*.
9. Repeat steps 7 and 8 for each of the Windows Servers that make up the SQL Cluster.
10. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).
11. Click the wrench icon (🔧) for the "Microsoft: SQL Server Discovery" Dynamic Application to open the **Dynamic Applications Properties Editor**page.
12. In the **[Properties]** tab, change the ***Operational State*** field to *Enabled*.
13. Click **[Save]**.

Discovering SQL Servers

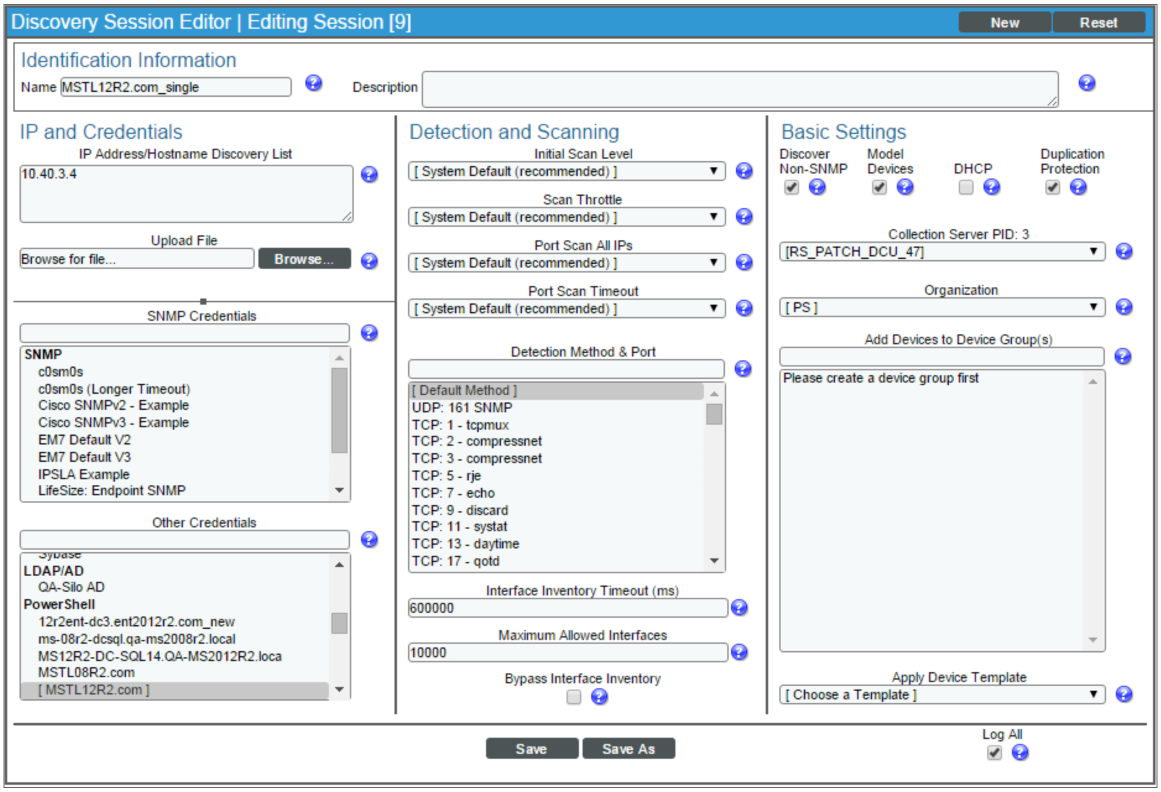
When you discover SQL Servers in SL1, SL1 auto-aligns a series of Dynamic Applications to discover, configure, and monitor the following SQL Server component devices:

- SQL Servers
    - SQL Server instances
        - SQL Server databases

To discover SQL Servers and their component devices, perform the following steps:

1. Go to the **Discovery Control Panel** page (System > Manage > Discovery).

2. Click the **[Create]** button. The **Discovery Session Editor** page appears:



Discovery Session Editor | Editing Session [9]

Identification Information

Name: MSTL12R2.com_single

Description:

IP and Credentials

IP Address/Hostname Discovery List: 10.40.3.4

Upload File: Browse for file...

SNMP Credentials:

SNMP
- c0sm0s
- c0sm0s (Longer Timeout)
- Cisco SNMPv2 - Example
- Cisco SNMPv3 - Example
- EM7 Default V2
- EM7 Default V3
- IPSLA Example
- LifeSize: Endpoint SNMP

Other Credentials:

Sybase

LDAP/AD
- QA-Silo AD

PowerShell
- 12r2ent-dc3.ent2012r2.com_new
- ms-08r2-dcsql.qa-ms2008r2.local
- MS12R2-DC-SQL14.QA-MS2012R2.loca
- MSTL08R2.com
- [MSTL12R2.com]

Detection and Scanning

Initial Scan Level: [System Default (recommended)]

Scan Throttle: [System Default (recommended)]

Port Scan All IPs: [System Default (recommended)]

Port Scan Timeout: [System Default (recommended)]

Detection Method & Port:
- [Default Method]
- UDP: 161 SNMP
- TCP: 1 - tcpmux
- TCP: 2 - compressnet
- TCP: 3 - compressnet
- TCP: 5 - rje
- TCP: 7 - echo
- TCP: 9 - discard
- TCP: 11 - systat
- TCP: 13 - daytime
- TCP: 17 - qotd

Interface Inventory Timeout (ms): 600000

Maximum Allowed Interfaces: 10000

Bypass Interface Inventory: ☐

Basic Settings

Discover Non-SNMP ☑ Model Devices ☑ DHCP ☐ Duplication Protection ☑

Collection Server PID: 3: [RS_PATCH_DCU_47]

Organization: [PS]

Add Devices to Device Group(s): Please create a device group first

Apply Device Template: [Choose a Template]

Log All ☑

3. Supply values in the following fields:

   - ***IP Address/Hostname Discovery List***. Type the IP addresses or the range of IP addresses for the SQL Servers you want to discover.
   - ***Other Credentials***. Select the *PowerShell credential you created*.
   - ***Discover Non-SNMP***. Because the discovery session is not using an SNMP credential, select this checkbox.

4. Optionally, supply values in the other fields in this page. For a description of the fields in this page, see the ***Discovery & Credentials*** manual.

5. Click the **[Save]** button.

6. The **Discovery Control Panel** page will refresh. Click the lightning bolt icon (⚡) for the discovery session you created.

7. In the pop-up window that appears, click the **[OK]** button. The **Discovery Session** page displays the progress of the discovery session.

Relationships Between Component Devices

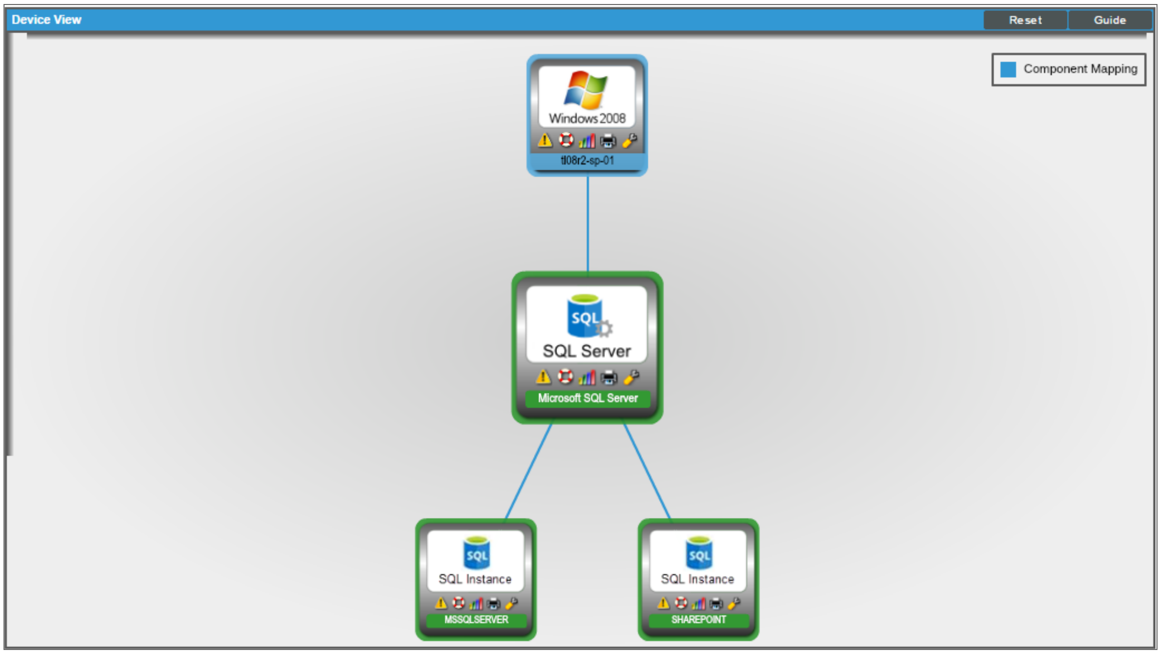
SL1 can automatically build relationships between SQL servers and other associated devices:

- If you discover Windows server clusters using the Dynamic Applications in the *Microsoft: Windows Server Cluster* PowerPack version 100 or later, SL1 will automatically create relationships between SQL servers and Windows server clusters.

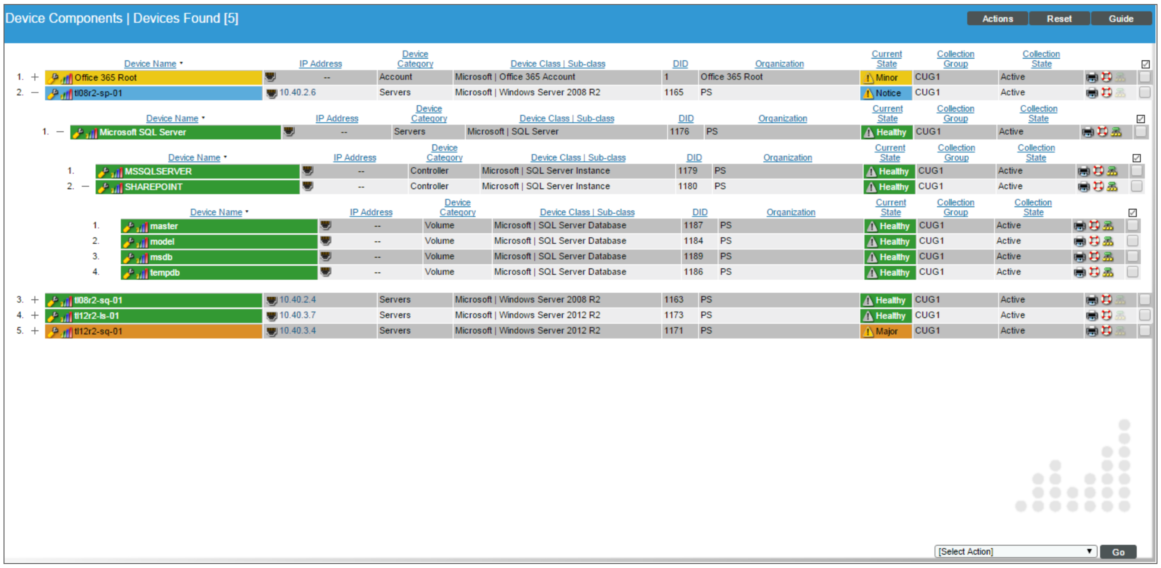
Viewing SQL Server Component Devices

In addition to the **Device Manager** page (Registry > Devices > Device Manager), you can view the SQL Server and all associated component devices in the following places in the user interface:

- The **Device View** modal page displays a map of a particular device and all of the devices with which it has parent-child relationships. Double-clicking any of the devices listed reloads the page to make the selected device the primary device:



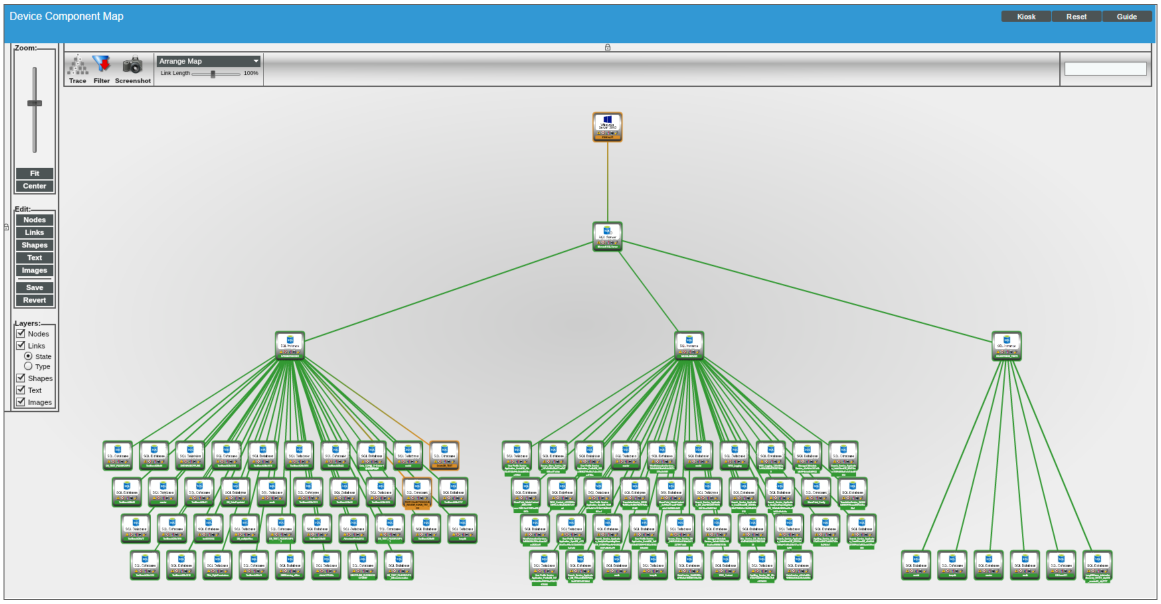
- The **Device Components** page (Registry > Devices > Device Components) displays a list of all root devices and component devices discovered by SL1 in an indented view, so you can easily view the hierarchy and relationships between child devices, parent devices, and root devices. To view the component devices associated with a SQL Server, find the server and click its plus icon (**+**):



Device Components | Devices Found [5]

	Device Name	IP Address	Device Category	Device Class | Sub-class	DID	Organization	Current State	Collection Group	Collection State
1. +	Office 365 Root	--	Account	Microsoft | Office 365 Account	1	Office 365 Root	Minor	CUG1	Active
2. −	tl08r2-sp-01	10.40.2.6	Servers	Microsoft | Windows Server 2008 R2	1165	PS	Notice	CUG1	Active
1. −	Microsoft SQL Server	--	Servers	Microsoft | SQL Server	1176	PS	Healthy	CUG1	Active
1.	MSSQLSERVER	--	Controller	Microsoft | SQL Server Instance	1179	PS	Healthy	CUG1	Active
2. −	SHAREPOINT	--	Controller	Microsoft | SQL Server Instance	1180	PS	Healthy	CUG1	Active
1.	master	--	Volume	Microsoft | SQL Server Database	1187	PS	Healthy	CUG1	Active
2.	model	--	Volume	Microsoft | SQL Server Database	1184	PS	Healthy	CUG1	Active
3.	msdb	--	Volume	Microsoft | SQL Server Database	1189	PS	Healthy	CUG1	Active
4.	tempdb	--	Volume	Microsoft | SQL Server Database	1186	PS	Healthy	CUG1	Active
3. +	tl08r2-sq-01	10.40.2.4	Servers	Microsoft | Windows Server 2008 R2	1163	PS	Healthy	CUG1	Active
4. +	tl12r2-ls-01	10.40.3.7	Servers	Microsoft | Windows Server 2012 R2	1173	PS	Healthy	CUG1	Active
5. +	tl12r2-sq-01	10.40.3.4	Servers	Microsoft | Windows Server 2012 R2	1171	PS	Major	CUG1	Active

- The **Component Map** page (Views > Device Maps > Components) allows you to view devices by root node and view the relationships between root nodes, parent components, and child components in a map. This page makes it easy to visualize and manage root nodes and their components. SL1 automatically updates the **Component Map** as new component devices are discovered. The platform also updates each map with the latest status and event information. To view the map for a SQL Server, go to the **Component Map** page and select the map from the list in the left NavBar. To learn more about the **Component Map** page, see the ***Views*** manual.



Device Component Map

LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

ALL INFORMATION AVAILABLE IN THIS GUIDE IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED. SCIENCELOGIC™ AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT.

Although ScienceLogic™ has attempted to provide accurate information on this Site, information on this Site may contain inadvertent technical inaccuracies or typographical errors, and ScienceLogic™ assumes no responsibility for the accuracy of the information. Information may be changed or updated without notice. ScienceLogic™ may also make improvements and / or changes in the products or services described in this Site at any time without notice.

Copyrights and Trademarks

ScienceLogic, the ScienceLogic logo, and EM7 are trademarks of ScienceLogic, Inc. in the United States, other countries, or both.

Below is a list of trademarks and service marks that should be credited to ScienceLogic, Inc. The ® and ™ symbols reflect the trademark registration status in the U.S. Patent and Trademark Office and may not be appropriate for materials to be distributed outside the United States.

- ScienceLogic™
- EM7™ and em7™
- Simplify IT™
- Dynamic Application™
- Relational Infrastructure Management™

The absence of a product or service name, slogan or logo from this list does not constitute a waiver of ScienceLogic's trademark or other intellectual property rights concerning that name, slogan, or logo.

Please note that laws concerning use of trademarks or product names vary by country. Always consult a local attorney for additional guidance.

Other

If any provision of this agreement shall be unlawful, void, or for any reason unenforceable, then that provision shall be deemed severable from this agreement and shall not affect the validity and enforceability of any remaining provisions. This is the entire agreement between the parties relating to the matters contained herein.

In the U.S. and other jurisdictions, trademark owners have a duty to police the use of their marks. Therefore, if you become aware of any improper use of ScienceLogic Trademarks, including infringement or counterfeiting by third parties, report them to Science Logic's legal department immediately. Report as much detail as possible about the misuse, including the name of the party, contact information, and copies or photographs of the potential misuse to: legal@sciencelogic.com

ScienceLogic

800-SCI-LOGIC (1-800-724-5644)

International: +1-703-354-1010