ScienceLogic

Monitoring IBM MQ

IBM: MQ PowerPack version 102

Table of Contents

Introduction	3
What is IBM MQ?	
What Does the IBM: MQPowerPack Monitor?	4
Installing the IBM: MQ PowerPack	4
Configuration and Discovery	6
Prerequisites for Monitoring IBM MQ	
Installing the IBM MQ PowerShell Snap-In for Monitoring on Windows Servers	
Creating a PowerShell Credential for IBM MQ on Windows Systems	
Creating a PowerShell Credential for IBM MQ on Windows Systems in the Classic SL1 User Interface	
Creating an SSH/Key Credential for IBM MQ on Linux Systems	
Creating an SSH/Key Credential for IBM MQ on Linux Systems in the SL1 Classic User Interface	
Creating a SOAP/XML Credential for IBM MQ on Aix and Linux Systems	12
Creating a SOAP/XML Credential for IBM MQ on Aix and Linux Systems in the Classic SL1 User	
Interface1	
Discovering IBM MQ Component Devices	
Discovering IBM Component Devices in the SL1 Classic User Interface	17
Verifying Discovery and Dynamic Application Alignment	
Configuring the IBM: MQ Queue Discovery Snippet	
Configuring the IBM: MQ Error Log Configuration Snippet	21
Viewing IBM MQ Component Devices	
Dashboards	
IBM MQ Device Dashboards	24
IBM MQ: Queue	
IBM MQ: Queue Manager	25

Chapter

Introduction

Overview

This manual describes how to monitor IBM MQ messaging systems in SL1 using the IBM: MQ PowerPack.

The following sections provide an overview of IBM MQ and the IBM: MQ PowerPack:

This chapter covers the following topics:

What is IBM MQ?	3
What Does the IBM: MQPowerPack Monitor?	4
Installing the IBM: MQ PowerPack	4

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 is IBM MQ?

The IBM MQ is message-queing middleware that supports messaging between applications, systems, services, and files. An IBM MQ messaging system is made up of one or more queue managers that support asynchronous routing of messages between systems, with producing and consuming applications connected to different queue managers.

What Does the IBM: MQPowerPack Monitor?

To monitor IBM MQ messaging systems using SL1, you must install the *IBM*: MQ PowerPack. This PowerPack enables you to discover, model, and collect data about IBM MQ messaging systems.

The IBM: MQ PowerPack includes:

- Example credentials you can use as a template to create a PowerShell credential, a SOAP/XML credential, or an SSH/Key credential to connect to the IBM MQ messaging system you want to monitor
- Dynamic Applications to discover, model, and monitor performance metrics and collect configuration data for IBM MQ messaging systems
- Device classes for the IBM MQ components that the SL1 monitors
- Event policies and corresponding alerts that are triggered when IBM MQ systems meet certain status criteria

Installing the IBM: MQ PowerPack

Before completing the steps in this manual, you must import and install the latest version of the *IBM*: *M*Q 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 Support Site at https://support.sciencelogic.com/s/powerpacks.
- 2. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).
- 3. In the **PowerPack Manager** page, click the **[Actions]** button, then select *Import PowerPack*. The **Import PowerPack** dialog box appears:

Imp	rt PowerPack™	×
	Browse for file Browse License: Import	

- 4. Click the [Browse] button and navigate to the PowerPack file.
- 5. When the **PowerPack Installer** modal 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

Overview

The following sections describe how to configure and discover IBM MQ messaging systems for monitoring by SL1 using the *IBM*: MQ PowerPack:

This chapter covers the following topics:

Prerequisites for Monitoring IBM MQ	6
Creating a PowerShell Credential for IBM MQ on Windows Systems	8
Creating an SSH/Key Credential for IBM MQ on Linux Systems	10
Creating a SOAP/XML Credential for IBM MQ on Aix and Linux Systems	12
Discovering IBM MQ Component Devices	14
Verifying Discovery and Dynamic Application Alignment	18
Viewing IBM MQ Component Devices	22

Prerequisites for Monitoring IBM MQ

To configure the SL1 system to monitor IBM MQ messaging systems using the *IBM*: MQ PowerPack, you must first perform the following:

- Install the IBM MQ PowerShell Snap-in for Monitoring on Windows Servers
- Give all SSH credential users the "mqm" group permission

Installing the IBM MQ PowerShell Snap-In for Monitoring on Windows Servers

NOTE: Users monitoring MQ on Linux servers do not need to perform these steps.

- **NOTE**: On 64-bit versions of Microsoft Windows, both 32-bit and 64-bit versions of Windows PowerShell are installed. SL1's collection processes using Windows PowerShell will default to using the version of powershell.exe whose folder exists first in the PATH environment variable. Because this will vary from system to system, these steps ensure the WebSphereMQ.dll file is registered for both Windows PowerShell environments.
- Download the Windows PowerShell library package (mo74.zip) for IBM MQ from the following location: <u>https://www.ibm.com/support/pages/mo74-websphere-mq-windows-powershell-</u> library#:~:text=Download%20Description,queue%20managers%20from%20the%20PowerShell
- 2. Extract the contents of the zip file to your Windows server, and find the "manual" subfolder from the extracted files (under the mo74_v2.0.1_x86_x64 folder). Create a new folder on your desktop and move the files in the "manual" subfolder to that folder.
- 3. Register the IBM WebSphere MQ library for use by both 32-bit and 64-bit Windows PowerShell. To do this:
 - Start a 32-bit Windows PowerShell console window (this will be the Windows PowerShell (x86) application if running on a 64-bit version of Microsoft Windows) using "Run as adminstrator", run the following:

 $WINDIR\Microsoft.NET\Framework\v4.0.30319\installutil <Directory where WebsphereMQ.dll resides>$ WebSphereMQ.dll

• Start a 64-bit Windows PowerShell console window (this will be the Windows PowerShell application without (x86) in its program name on a 64-bit version of Microsoft Windows) using "Run as adminstrator" and run the following:

```
%WINDIR%\Microsoft.NET\Framework64\v4.0.30319\installutil <Directory where WebsphereMQ.dll resides>\WebSphereMQ.dll
```

4. Open your Windows PowerShell console and add the WebSphere MQ for PowerShell snap-in by running the following command:

Add-PSSnapin IBM.PowerShell.WebSphereMQ

Creating a PowerShell Credential for IBM MQ on Windows Systems

To configure SL1 to monitor IBM MQ messaging systems on Windows systems, you must first create a PowerShell credential. This credential allows the Dynamic Applications in the *IBM*: *M*Q PowerPack to connect with an IBM MQ system.

The PowerPack includes an example PowerShell credential that you can edit for your own use.

NOTE: If you are using an SL1 system prior to version 11.1.0, the new user interface does not include the Duplicate option for sample credential(s). ScienceLogic recommends that you use the classic user interface and the Save As button to create new credentials from sample credential(s). This will prevent you from overwriting the sample credential(s).

To configure a PowerShell credential to access an IBM MQ system:

- 1. Go to the **Credentials** page (Manage > Credentials).
- 2. Locate the IBM MQ PowerShell Example sample credential, click its [Actions] icon (---) and select Duplicate. A copy of the credential, called IBM MQ PowerShell - Example copy appears.
- 3. Click the [Actions] icon (--) for the IBM MQ PowerShell Example copy credential and select *Edit*. The Edit Credential modal page appears.

IBM MQ SSH - Example copy			Credential Tester	
Organizations Select the organ	nizations the credential belongs to "	Timeout (mi) 3000	Select Credential Test	
Hostware/IP*	Port*		Select Collector CUG KNT-ISO-AIO-50: 10.2.5.50	
%D	22			
Username USERNAME_HERE	Paseword		IP or Hostname to test*	
Private Key				Test Creder
PEM Format				
		Save & Test		

- 4. Supply values in the following fields:
 - Name. Type a new name for the credential.
 - Hostname/IP. Keep the default value.

- **Username**. Type the username for a user with administrator access to the IBM MQ messaging system.
- **Password**. Type the password for the IBM MQ system account username.
- 5. Click [Save & Close].

Creating a PowerShell Credential for IBM MQ on Windows Systems in the Classic SL1 User Interface

To configure SL1 to monitor IBM MQ messaging systems on Windows systems, you must first create a PowerShell credential. This credential allows the Dynamic Applications in the *IBM*: *M*Q PowerPack to connect with an IBM MQ system.

The PowerPack includes an example PowerShell credential that you can edit for your own use.

To configure a PowerShell credential to access an IBM MQ system:

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

Credential Editor [168]	
Edit PowerShell Credential #168	New Reset
Basic Settings	
Profile Name	Account Type
IBM MQ PowerShell - Example	[Active Directory]
Hostname/IP	Timeout(ms)
(%D	10000
Username	Password
USERNAME_GOES_HERE	[
Encrypted Port	PowerShell Proxy Hostname/IP
([no] V) (5985	
Active Directory Settings	
Active Directory Hostname/IP	Domain
AD_HOSTNAME_GOES_HERE	DOMAIN_GOES_HERE
Save Save As	

- 3. Complete the following fields:
 - Credential Name. Type a new name for the credential.
 - Hostname/IP. Keep the default value.
 - **Username**. Type the username for a user with administrator access to the IBM MQ messaging system.
 - Password. Type the password for the IBM MQ system account username.
- 4. Click the **[Save As]** button.

Creating an SSH/Key Credential for IBM MQ on Linux Systems

To configure SL1 to monitor IBM MQ messaging systems on Linux systems, you must first create an SSH/Key credential. This credential allows the Dynamic Applications in the *IBM*: *M*Q PowerPack to connect with an IBM MQ system.

The PowerPack includes an example SSH/Key credential that you can edit for your own use.

NOTE: If you are using an SL1 system prior to version 11.1.0, the new user interface does not include the *Duplicate* option for sample credential(s). ScienceLogic recommends that you use the classic user *interface and the Save As button* to create new credentials from sample credential(s). This will prevent you from overwriting the sample credential(s).

To configure an SSH/Key credential to access an IBM MQ system:

- 1. Go to the **Credentials** page (Manage > Credentials).
- 2. Locate the IBM MQ SSH Example sample credential, click its [Actions] icon (---) and select Duplicate. A copy of the credential, called IBM MQ SSH Example copy appears.
- 3. Click the [Actions] icon (--) for the IBM MQ SSH Example copy credential and select Edit. The Edit Credential modal page appears.

IBM MQ SSH - Example copy			Credential Tester	
All Organizations Select the organiza	tions the credential belongs to " \neg	Timecut (ma) 3000	Select Credential Test	
			Select Collector CUG KNT-ISO-AIO-50: 10.2.5.50	
Hostname/IP* %D	Port* 22			
Username USERNAME. HERE	Password		IP or Hostname to test *	
Private Key				Test Credent
PEM Format				
		Save & Test		

- 4. Supply values in the following fields:
 - Name. Type a new name for the credential.
 - Hostname/IP. Keep the default value.
 - Username. Type the username for a user with administrator access, and who is a member of the "mgm" group, to the IBM MQ messaging system.
 - Password. Type the password for the IBM MQ system account username.

NOTE: The private key can have a maximum of 64 characters per line. Therefore, you cannot use keys in the OpenSSH format, because that format uses 70 characters per line. When you attempt to save the credential, SL1 will validate that the private key entered is in the correct format. You will be able to save the credential only if the private key is correctly formatted.

5. Click [Save & Close].

Creating an SSH/Key Credential for IBM MQ on Linux Systems in the SL1 Classic User Interface

To configure SL1 to monitor IBM MQ messaging systems on Linux systems, you must first create an SSH/Key credential. This credential allows the Dynamic Applications in the *IBM*: MQ PowerPack to connect with an IBM MQ system.

The PowerPack includes an example SSH/Key credential that you can edit for your own use.

To configure an SSH/Key credential to access an IBM MQ system:

- 1. Go to the Credential Management page (System > Manage > Credentials).
- 2. Locate the IBM MQ SSH Example credential, then click its wrench icon (*P*). The Edit SSH/Key Credential modal page appears:

Credential Editor [167]			×
Edit SSH/Key Credential #167		New	Reset
Basic Settings			
Credential Name			_
IBM MQ SSH - Example			
Hostname/IP Port	Timeout(n	ns)	
(%D) (22	3000		
Username	Passwor	d	
USERNAME_HERE]		
Private Key (PEM Format)			
			//
Save Save As			

- 3. Complete the following fields:
 - Credential Name. Type a new name for the credential.
 - Hostname/IP. Keep the default value.

- **Username**. Type the username for a user with administrator access, and who is a member of the "mgm" group, to the IBM MQ messaging system.
- Password. Type the password for the IBM MQ system account username.

NOTE: The private key can have a maximum of 64 characters per line. Therefore, you cannot use keys in the OpenSSH format, because that format uses 70 characters per line. When you attempt to save the credential, SL1 will validate that the private key entered is in the correct format. You will be able to save the credential only if the private key is correctly formatted.

4. Click the **[Save As]** button.

Creating a SOAP/XML Credential for IBM MQ on Aix and Linux Systems

To configure SL1 to monitor IBM MQ messaging systems on your Aix and Linux systems, you must first create a SOAP/XML credential. This credential allows the Dynamic Applications in the *IBM*: MQ PowerPack to connect with an IBM MQ system.

NOTE: You are only required to create SOAP/XML credential for your Linux system if you want to utilize the Kornshell and sudo commands.

The PowerPack includes an example SOAP/XML credential that you can edit for your own use.

NOTE: If you are using an SL1 system prior to version 11.1.0, the new user interface does not include the Duplicate option for sample credential(s). ScienceLogic recommends that you use the classic user interface and the Save As button to create new credentials from sample credential(s). This will prevent you from overwriting the sample credential(s).

To configure a SOAP/XML credential to access an IBM MQ system:

- 1. Go to the **Credentials** page (Manage > Credentials).
- 2. Locate the IBM MQ SOAP Example sample credential, click its [Actions] icon (---) and select Duplicate. A copy of the credential, called IBM MQ SOAP - Example copy appears.
- 3. Click the [Actions] icon (---) for the IBM MQ SOAP Example copy credential and select Edit. The Edit Credential modal page appears.

Name* IBM MQ SOAP - Example copy									Credential Tester	
II Organizations	lect the organization	ns the credential belong	is to * 👻		Timeout (ms) 3000000		Select Cr	redential Test		
Content Encoding text/xml		Method POST	~	HTTP Version http/1.1		v	Select Colle CUG KI	ector NT-ISO-AIO-50: 10.2	2.5.50	
URL*							IP or Hos	stname to test*		
http://%D:22										Test Credenti:
HTTP Auth User USER_NAME			HTTP Auth Password							
Proxy Hostname/IP			Proxy Port 0							
optional										
Proxy User			Proxy Password							
optional										
Embedded Password [%P]										
Embed Value [%1]			Embed Value [%2]							
Embed Value [%3]			Embed Value [%4]							
						Add Header				
HTTP Headers						Add Header				

- 4. Supply values in the following fields:
 - Name. Type a new name for the credential.
 - Hostname/IP. Keep the default value.
 - HTTP Auth User. Type the username for a user with administrator access to the IBM MQ messaging system.
 - HTTP Auth Password. Type the password for the IBM MQ system account username.

HTTP Headers

- *HTTP Headers*. The following headers can be entered to use KornShell and sudo. Create a separate header for each feature:
 - ° KORNSHELL
 - ° SUDO
- 5. For all remaining fields, use the default values.
- 6. Click [Save & Close] .

Creating a SOAP/XML Credential for IBM MQ on Aix and Linux Systems in the Classic SL1 User Interface

To configure SL1 to monitor IBM MQ messaging systems on your Aix and Linux systems, you must first create a SOAP/XML credential. This credential allows the Dynamic Applications in the *IBM*: *M*Q PowerPack to connect with an IBM MQ system.

The PowerPack includes an example SOAP/XML credential that you can edit for your own use.

To configure a SOAP/XML credential to access an IBM MQ system:

- 1. Go to the **Credential Management** page (System > Manage > Credentials).
- 2. Locate the IBM MQ SOAP Example credential, then click its wrench icon (²). The Edit SOAP/XML Credential modal page appears:

Credential Editor [96]	×
Edit SOAP/XML Credential #96	New Reset
Basic Settings Profile Name Content Encoding Method HTTP Version IBM M2 SOAP - Example [textlxmi] ([POST]) [HTTP/1.1]) URL [https://Host Port/Path %D = Aligned Device Address %N = Aligned Device Host Name]	Soap Options Embedded Password [%P] Embed Value [%1] Embed Value [%2] Embed Value [%3] Embed Value [%4]
Proxy Settings Hostname/IP Port User	HTTP Headers + Add a header
CURL Options CANNFO CAPATH CLOSEPOULCY CONNECTINEOUT COONEL COONELAR COONELIST COONELIST CONSCACHETIMEOUT	
Save Save As	

3. Complete the following fields:

Basic Settings

- **Profile Name**. Type a new name for the credential.
- URL. Keep the default value.
- HTTP Auth User. Type the username for a user with administrator access to the IBM MQ messaging system.
- HTTP Auth Password. Type the password for the IBM MQ system account username.

HTTP Headers

- *HTTP Headers*. The following headers can be entered to use KornShell and sudo. Create a separate header for each feature:
 - KORNSHELL
 - SUDO
- 4. Click the **[Save As]** button.

Discovering IBM MQ Component Devices

To discover an IBM MQ messaging system:

On the Devices page (I) or the Discovery Sessions page (Devices > Discovery Sessions), click the [Add Devices] button. The Select page appears:

Select the type of devices you want to monitor	×
	Chemical Information Control Inf
	Select

- 2. Click the **[Unguided Network Discovery]** button. Additional information about the requirements for discovery appears in the **General Information** pane to the right.
- 3. Click [Select]. The Add Devices page appears.
- 4. Complete the following fields:
 - Name. Type a unique name for this discovery session. This name is displayed in the list of discovery sessions on the [Discovery Sessions] tab.
 - **Description**. Optional. Type a short description of the discovery session. You can use the text in this description to search for the discovery session on the **[Discovery Sessions]** tab.
 - Select the organization to add discovered devices to. Select the name of the organization to which you want to add the discovered devices.

5. Click [Next]. The Credentials page of the Add Devices wizard appears:

	ose credentials that connect your	devices	 Create New 	lest Credent	lais
Q Typ	be to search credentials			=	•
•	NAME	ТҮРЕ	LASTEDIT		
	Azure Credential - Proxy	SOAP/XML	Tue Apr 23 2019 15:50:16 GMT+0000 (UTC)		^
	Azure Credential - SOAP/XML	SOAP/XML	Tue Apr 23 2019 15:50:16 GMT+0000 (UTC)		
	Cisco CE Series Configuration	SOAP/XML	Tue Apr 23 2019 15:50:29 GMT+0000 (UTC)		1
	Cisco CE Series History	SOAP/XML	Tue Apr 23 2019 15:50:29 GMT+0000 (UTC)		
	Cisco CE Series Status	SOAP/XML	Tue Apr 23 2019 15:50:29 GMT+0000 (UTC)		
	Cisco CUCM Example	Basic/Snippet	Tue Apr 23 2019 15:49:26 GMT+0000 (UTC)		
	Cisco Meeting Server Example	Basic/Snippet	Tue Apr 23 2019 15:49:41 GMT+0000 (UTC)		
	Cisco SNMPv2 - Example	SNMP	Tue Apr 23 2019 15:50:10 GMT+0000 (UTC)		
	Cisco SNMPv3 - Example	SNMP	Tue Apr 23 2019 15:50:10 GMT+0000 (UTC)		
	Cisco VOS CUC Cluster Status	Basic/Snippet	Tue Apr 23 2019 15:49:07 GMT+0000 (UTC)		
	Cisco VOS IM&P Cluster Status	Basic/Snippet	Tue Apr 23 2019 15:49:07 GMT+0000 (UTC)		~

- 6. On the **Credentials** page, locate and select the PowerShell, SOAP/XML, or SSH/Key credential you created for the IBM MQ system.
- 7. Click [Next]. The Discovery Session Details page of the Add Devices wizard appears:

Step 1 Basic Information		Step 2 Credential Selection	3	Step 3 Discovery Session Details	×
	Ent	er basic discovery session details			
	List of IPs/Hostnames		File Upload		
	1 2000 2000 2000 2000 2000 2000 2000 20		~	¢	
✓ Back				Save An	id Run

- 8. Complete the following fields:
 - List of IPs/Hostnames. Type the IP addresses for the IBM MQ messaging system.
 - Which collector will monitor these devices?. Select an existing collector to monitor the discovered devices. Required.
 - Run after save. Select this option to run this discovery session as soon as you save the session.

In the **Advanced options** section, click the down arrow icon (\checkmark) to complete the following fields:

- Discover Non-SNMP. Enable this setting.
- Model Devices. Enable this setting.
- 9. Click **[Save and Run]** if you enabled the Run after save setting, or **[Save and Close]** to save the discovery session. The **Discovery Sessions** page (Devices > Discovery Sessions) displays the new discovery session.
- 10. If you selected the **Run after save** option on this page, the discovery session runs, and the **Discovery Logs** page displays any relevant log messages. If the discovery session locates and adds any devices, the **Discovery Logs** page includes a link to the **Device Investigator** page for the discovered device.

Discovering IBM Component Devices in the SL1 Classic User Interface

To discover an IBM MQ messaging system:

- 1. Go to the **Discovery Control Panel** page (System > Manage > Classic Discovery).
- 2. In the Discovery Control Panel, click the [Create] button. The Discovery Session Editor page appears.

Discovery Session Editor Editing Session	ו [5]	New	Reset
Identification Information Name 10.2.10.100 Windows Besteen Destination	cription		0
IP and Credentials IP Address/Hostname Discovery List 10.2.10.100 Upload File Browse for file Browse SNMP Credentials SNMP Credentials SNMP Credentials SNMP Credentials Edit Cisco SNMP42 - Example Cisco SNMP42 - Example Cisco SNMP42 - Example Cisco SNMP4 - Example Cisco SNMP4 - Example Cisco CSP SNMP Port 161 Example Cisco CSP SNMP Credentials CMT DB CMT	Scan Throttie [System Default (recommended)] Port Scan All IPs [System Default (recommended)] Port Scan Timeout [System Default (recommended)] Detection Method & Port Detection Method & Port Detection Method & Port Default Method UDP: 161 SNMP TCP: 1 - topmux TCP: 2 - compressnet TCP: 3 - compressnet TCP: 5 - rje TCP: 7 - echo TCP: 9 - discard TCP: 1 - systat	Basic Settings Discover Model Non-SNMP Devices DHCP Collection Server PID: 4 [RNG-MIG-C-CU7] Collection Server PID: 4 [RNG-MIG-C-CU7] Organization [MQ WIN.100] Add Devices to Device Group(s) None LayerX Appliances Servers	 ✓ ✓
IBM MQ PowerShell - Example [IBM Windows .100]	Bypass Interface Inventory	Apply Device Template [Choose a Template]	✓ 🕄
	Save Save As	Log All	

- 3. In the **Discovery Session Editor** page, complete the following fields:
 - Name. Type a name for the discovery session.
 - IP Address/Hostname Discovery List. Type the IP address for the IBM MQ messaging system.

- Other Credentials. Select the PowerShell or SSH/Key credential you created for the IBM MQ messaging system.
- Discover Non-SNMP. Select this checkbox.
- Model Devices. Select this checkbox.
- 4. Optionally, you can enter values in the other fields on this page. For more information about the other fields on this page, see the **Discovery & Credentials** manual.
- 5. Click the **[Save]** button to save the discovery session and then close the **Discovery Session Editor** window.
- 6. The discovery session you created appears at the top of the **Discovery Control Panel** page. Click its lightning-bolt icon (*F*) to run the discovery session.
- 7. The **Discovery Session** window appears. When the cluster root device(s) are discovered, click the device icon () to view the **Device Properties** page for each device.

Verifying Discovery and Dynamic Application Alignment

To verify that SL1 has automatically aligned the correct Dynamic Applications during discovery:

- After discovery has completed, click the device icon for the IBM MQ device (I). From the Device Properties page for the IBM MQ device, click the [Collections] tab. The Dynamic Application Collections page appears.
- 2. All applicable Dynamic Applications for the device are automatically aligned during discovery.

NOTE: It can take several minutes after the discovery session has completed for Dynamic Applications to appear in the **Dynamic Application Collections** page.

.2.10.80		<u>R</u> elationships	I	onitors ickets	<u>S</u> chedule Redirects <u>N</u> ote:	s <u>A</u> ttributes		
.2.10.80 3925 crosoft D_WIN_80 tive				Category Sub-Class Uptime Collection Time	Physical Device Servers Windows Server 2016 0 days, 00:00:00 2020-07-01 12:50:00 CU7 I RNG-MIG-C-CU7		Window Server 20 A D at a 102.10.80	016
^M Collections						Expand Actions	Reset Gi	uide
Dynamic	Application		<u>ID</u>	Poll Frequer	<u>icy Type</u>	Credential	Collector	
y	-		2863	5 mins	Snippet Configuration	IBM Windows .100	RNG-MIG-C-CU7	1
s DCM+R Relationship			1295	15 mins	Snippet Configuration	IBM Windows .100	RNG-MIG-C-CU7	1
s Server Service Config	uration		1635	5 mins	Snippet Configuration	IBM Windows .100	RNG-MIG-C-CU7	1
s Server Process List			1298	120 mins	Snippet Journal	IBM Windows .100	RNG-MIG-C-CU7	1
s Server CPU Performa	ince		1299	5 mins	PowerShell Performance	IBM Windows .100	RNG-MIG-C-CU7	1
s Server Disk Performa	nce		1306	15 mins	PowerShell Performance	IBM Windows .100	RNG-MIG-C-CU7	1
s Server Interface Perfo	ormance		1307	5 mins	PowerShell Performance	IBM Windows .100	RNG-MIG-C-CU7	1
s Server Memory Perfo	rmance		1300	5 mins	PowerShell Performance	IBM Windows .100	RNG-MIG-C-CU7	1
s Server BIOS Configur	ration		1308	360 mins	PowerShell Config	IBM Windows .100	RNG-MIG-C-CU7	1
s Server CPU Configure	ation		1301	360 mins	PowerShell Config	IBM Windows .100	RNG-MIG-C-CU7	1
s Server Disk Configura	ation		1305	360 mins	PowerShell Config	IBM Windows .100	RNG-MIG-C-CU7	1
s Server Interface Conf	iguration		1297	360 mins	PowerShell Config	IBM Windows .100	RNG-MIG-C-CU7	1
s Server Memory Confi	guration		1302	360 mins	PowerShell Config	IBM Windows .100	RNG-MIG-C-CU7	9
s Server OS Configurati	ion		1304	5 mins	PowerShell Config	IBM Windows .100	RNG-MIG-C-CU7	9
				60 mins				
	Collections DVM+R Relationship Server Service Config Server Process List Server Drocess List Server Disk Performa Server Interface Perfor Server INE Configur Server Disk Configur Server Disk Configur Server Disk Configur Server Disk Configur Server Interface Configur S	Collections Dynamic Application DOM+R Relationship Server Service Configuration Server Process List Server CPU Performance Server Disk Performance Server Interface Performance Server Memory Performance Server CPU Configuration Server CPU Configuration Server CPU Configuration Server CPU Configuration Server Interface Configuration	Collections Dynamic Application DCM+R Relationship Server Service Configuration Server Process List Server Disk Performance Server Interface Performance Server Interface Performance Server Memory Performance Server CPU Configuration Server CPU Configuration Server CPU Configuration Server CPU Configuration Server Interface Configuration	Collections	Broup / Collector Dynamic Accilication ID Poll Fraguer 2863 5 mins DCM+R Relationship 1295 15 mins Server Service Configuration 1635 5 mins Server Process List 1296 120 mins Server CPU Performance 1306 15 mins Server Interface Performance 1307 5 mins Server CPU Configuration 1308 800 mins Server CPU Performance 1307 5 mins Server Interface Performance 1307 5 mins Server CPU Configuration 1308 800 mins Server CPU Configuration 1308 800 mins Server CPU Configuration 1308 800 mins Server CPU Configuration 1303 800 mins Server Ubik Configuration 1305 800 mins Server Ubik Configuration 1302 800 mins	Group / Collector CU71 RNG-MIG-C-CU7 Collections Dynamic Application ID Foll Frequency Tyree DCM+R Relationship 1295 15 mins Shippet Configuration Server Service Configuration 1635 5 mins Shippet Configuration Server Process List 1298 120 mins Shippet Configuration Server DPU Performance 1309 5 mins Shippet Configuration Server DNA Performance 1307 5 mins PowerShell Performance Server Memory Performance 1300 5 mins PowerShell Performance Server DNA Configuration 1308 800 mins PowerShell Performance Server DNA Configuration 1301 360 mins PowerShell Config Server DNA Configuration 1303 800 mins PowerShell Config Server DNA Configuration 1303 800 mins PowerShell Config Server IDNA Configuration 1302 800 mins PowerShell Config Server IDNA Configuration 1302 800 mins PowerShell Config Server IDNA Configuration	Group / Collector CU7 I RNG-MIG-C-CU7 Collections Expand Actions Dynamic Accilcation ID Poll Frequency Tyree Credential DCM+R Relationship 1295 15 mins Snippet Configuration IBM Windows 100 DCM+R Relationship 1295 15 mins Snippet Configuration IBM Windows 100 Server Process List 1298 120 mins Snippet Configuration IBM Windows 100 Server DRV Performance 1299 5 mins Snippet Configuration IBM Windows 100 Server DRV Performance 1299 5 mins PowerShell Performance IBM Windows 100 Server Interface Performance 1307 5 mins PowerShell Performance IBM Windows 100 Server DRV Performance 1300 5 mins PowerShell Performance IBM Windows 100 Server DRV Performance 1300 5 mins PowerShell Performance IBM Windows 100 Server DRV Performance 1308 800 mins PowerShell Performance IBM Windows 100 Server DRV Configuration 1301 800 mins	Group / Collector CUT I RNG-MIG-C-CU7 Collector CUT I RNG-MIG-C-CU7 * Collections Expand Actions Reset G * Collections ID Foil Frequency Tyres Credental Collector DCM+R Relationship 1295 15 mins Snippet Configuration IBM Windows.100 RNG-MIG-C-CU7 Server Service Configuration 1355 5 mins Snippet Configuration IBM Windows.100 RNG-MIG-C-CU7 Server Process List 1298 120 mins Snippet Configuration IBM Windows.100 RNG-MIG-C-CU7 Server Process List 1298 120 mins Snippet Configuration IBM Windows.100 RNG-MIG-C-CU7 Server DNE Performance 1299 5 mins PowerShell Performance IBM Windows.100 RNG-MIG-C-CU7 Server Interface Performance 1307 5 mins PowerShell Performance IBM Windows.100 RNG-MIG-C-CU7 Server INE Apertormance 1300 5 mins PowerShell Performance IBM Windows.100 RNG-MIG-C-CU7 Server INertorono 1308 830 mins <t< td=""></t<>

Copyrig

You should see the following Dynamic Applications aligned to the IBM MQ root device:

• IBM: MQ Discovery

You should see the following Dynamic Applications aligned to the IBM MQ server:

• IBM: MQ Queue Manager Discovery

You should see the following Dynamic Applications aligned to the IBM MQ queue managers:

• IBM: MQ Cluster Channel Configuration

NOTE: For Windows users, in the "IBM: MQ Cluster Channel Configuration" Dynamic Application, when a channel is configured with a cluster and that cluster is deleted, the status for that cluster cannot be returned.

NOTE: For Windows users, in the "IBM: MQ Cluster Channel Configuration" Dynamic Application, the "CLUSSDRA" and "CLUSSDRB" are shown as "CLUSSDR".

- IBM: MQ Channel Configuration
- IBM: MQ Queue Discovery

NOTE: For Windows users, the "IBM: MQ Discovery" Dynamic Application currently does not return "Connections", "Parent Queue Manager", or "Start Date" metrics. On some MQ installations, SL1 may be unable to collect the "Standby Host" property.

• IBM: MQ Queue Manager Configuration

NOTE: For Windows users, the "IBM: MQ Queue Manager Configuration" Dynamic Application currently does not return "Connections", "Parent Queue Manager", or "Start Date" metrics.

You should see the following Dynamic Applications aligned to the IBM MQ queues:

- IBM: MQ Queue Configuration
- IBM: MQ Queue Performance

If the listed Dynamic Applications have not been automatically aligned during discovery, you can align them manually. To do so, perform the following steps:

- 1. Click the **[Action]** button and then select Add Dynamic Application. The **Dynamic Application Alignment** page appears:
- 2. In the **Dynamic Applications** field, select the Dynamic Application you want to align.
- 3. In the **Credentials** field, select the credential specified in the table.
- 4. Click the **[Save]** button.
- 5. Repeat steps 1-4 for the other unaligned Dynamic Applications.

Configuring the IBM: MQ Queue Discovery Snippet

The "IBM: MQ Queue Discovery" Dynamic Application snippet allows you to customize the list of queue names and types of queues that SL1 will discover. Up to 20 queue names can be specified, and those names will be discovered under each queue manager where they are found.

For specifying queue types, an integer can be specified as one item in the list, and the allowed values for type are:

- 1 : Dead letter queue will be discovered
- 2 : Transmission queues will be discovered

To edit the snippet:

- 1. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).
- 2. Find the "IBM: MQ Queue Discovery" Dynamic Application and click its wrench icon (🥍).

- 3. In the Dynamic Applications Properties Editor, click the [Snippets] tab.
- 4. In the **Dynamic Applications Snippet Editor & Registry** page, click the wrench icon (***) of the "Discover-Queues" snippet.
- 5. The content of the snippet will appear. Add the following text to the snippet to customize the list of queue names and queue types that can be discovered:

QUEUES_TO_DISCOVER = ['<queue name>','<queue name>','<queue type>']

Use commas to separate queue names and queue types.

Close	Properties	Collections	Snippets	Thresholds	Alerts	Component	Subscribers	
Dynamic Applications [1977] I Snippet Editor & Registry I Editing Snippet [2364]						Guide	Reset	
Discover-G	Snippet Name Queues		[Enabled]	Active State Snippet Code	۲	[Required -	Required Stop Collection]	•
<pre># of que # and su # they a # as one # # 1 : D # 2 : T # #</pre>	<pre># QUEUES_TO_DISCOVER: customizable list of queue names and types # of queues SL1 will discover. Up to 20 queue names can be specified, # and such names will be discovered under each queue manager where # they are round. For specifying queue types, an integer can be specified # as one item in the list, and the allowed values for type are: # # 1 : Dead letter queue will be discovered</pre>							
QUEUES_TO_DISCOVER = ['SYSTEM.ADMIN.CHANNEL.EVENT', 'SYSTEM.ADMIN.COMMAND.EVENT', 'SYSTEM.CHANNEL.INITQ', 'SYSTEM.CLUSTER.TRANSMIT.QUEUE', 'SYSTEM.CLUSTER.TRANSMIT.QUEUE', 1, 2, 'Q1_LOCAL','Q2_LOCAL','Q1_LOCAL_CL','Q1']								

Configuring the IBM: MQ Error Log Configuration Snippet

By default, only some errors are monitored and alerted in SL1. The IDs of the errors supported can be found in the snippet of the "IBM: MQ Error Log Configuration" Dynamic Application. You can add other error messages by adding the alert ID to the ALERT_ID_LIST list in the snippet.

To edit the snippet:

- 1. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).
- 2. Find the "IBM: MQ Error Log Configuration" Dynamic Application and click its wrench icon (🥍).
- 3. In the Dynamic Applications Properties Editor, click the [Snippets] tab.
- 4. In the **Dynamic Applications Snippet Editor & Registry** page, click the wrench icon (*P*) of the "Get-ErrorLogRecords" snippet.
- 5. The content of the snippet will appear. Add the alert IDs you want added to the ALERT_ID_LIST in the snippet:

Viewing IBM MQ Component Devices

In addition to the **Devices** page, you can view the IBM MQ system and all associated component devices in the following places in the user interface:

- The **Device Investigator** Map page (click **Map** in the **Device Investigator** 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 listed devices reloads the page to make the selected device the primary device
- The **Device Components** page (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 Kubernetes cluster, find the cluster device and click its plus icon (+).
- The Component Map page (Classic Maps > 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 makes it easy to visualize and manage root nodes and their components. SL1 automatically
 updates the Component Map as new component devices are discovered. SL1 also updates each map with
 the latest status and event information. To view the map for a Kubernetes cluster, go to Classic Maps
 > Device Maps > Components, and select the map from the list in the left NavBar. To learn more about the
 Component Map page, see the Views manual.

Chapter



Dashboards

Overview

The *IBM*: MQ PowerPack contains device dashboards that present data related to your message queues and queue managers.

The following section provides a description of each dashboard:

This chapter covers the following topics:

IBM MQ Device Dashboards	
--------------------------	--

IBM MQ Device Dashboards

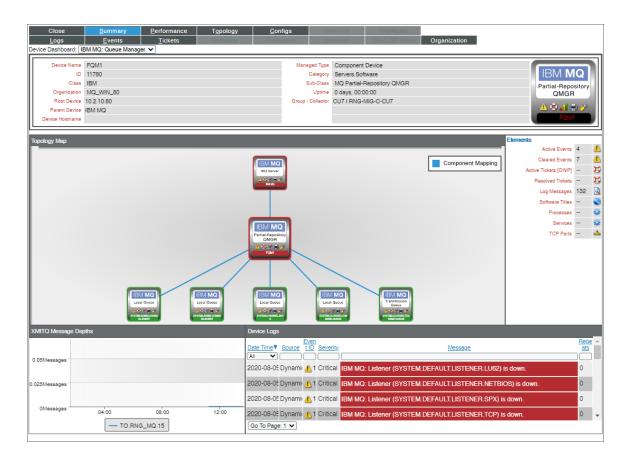
IBM MQ: Queue

Close Summary Performance Topology Logs Events Tickets Device Dashboard: [IBM MQ: Queue Image: State Sta	Configs designed and the second secon	Organization
Device Name SYSTEM.ADMIN.CHANNEL.EVENT 10 11838 Class IEM Organization IMQ_VINL_80 Root Device 10.2.10.80 Parent Device FQM1 Device Hostname	Managed Type Component Device Category Storage. Volume Sub-Class MIQ Local Oueue Uptime 0 days, 000000 Group / Collector CU7 I RNG-MIG-C-CU7	
Topology Map		Elements Active Events Cleared Event
Input/Output Handles	Device Logs Date Time V Source 110 Sevently All V	Heree Alson
0.025Application	2020-08-05 Internal 1: Notice Added dynamic application	I created (Class: IBM I MQ Local Queue) IBM I MQ Local Que 0 on for device: IBM: MQ Queue Configuration on for device: IBM: MQ Queue Performance 0

The IBM MQ: Queue device dashboard displays the following information:

- A line graph that displays message depth
- A line graph that displays input and output handles
- A list of device logs displaying events

IBM MQ: Queue Manager



The IBM MQ: Queue Manager device dashboard displays the following information:

- A line graph that displays XMITQ message depths
- A list of device logs displaying events

© 2003 - 2022, ScienceLogic, Inc.

All rights reserved.

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. For more information, see https://sciencelogic.com.



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

International: +1-703-354-1010