



Monitoring IBM Db2

IBM: DB2 PowerPack version 100

Table of Contents

Introduction	3
What is IBM Db2?	3
What Does the IBM: DB2 PowerPack Monitor?	4
Installing the IBM: DB2 PowerPack	4
Configuring IBM Db2 Monitoring	6
Prerequisites for Monitoring IBM Db2	6
Prerequisites for Linux/Unix Users	7
Prerequisites for Windows Users	8
Creating Credentials for IBM Db2	9
Creating an SSH/Key Credential (Linux and Unix Users)	9
Creating a PowerShell Credential (Windows Users)	11
Creating a SOAP/XML Credential (Linux and Unix Users)	12
Creating a SOAP/XML Credential (Windows Users)	14
Discovering IBM Db2 Component Devices	15
Verifying Discovery and Dynamic Application Alignment	16
Viewing IBM Db2 Component Devices	21
IBM Db2 Dashboards	23
Device Dashboard	23
IBM DB2: Instance	24

Chapter

1

Introduction

Overview

This manual describes how to monitor IBM Db2 databases in SL1 using the *IBM: DB2 PowerPack*.

The following sections provide an overview of IBM Db2 and the *IBM: DB2 PowerPack*:

<i>What is IBM Db2?</i>	3
<i>What Does the IBM: DB2 PowerPack Monitor?</i>	4
<i>Installing the IBM: DB2 PowerPack</i>	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 Db2?

IBM Db2 is a family of data management products that includes database servers. The IBM Db2 Database is a relational database that delivers advanced data management and analytics capabilities for transactional workloads.

What Does the IBM: DB2 PowerPack Monitor?

To monitor IBM Db2 databases using SL1, you must install the *IBM: DB2* PowerPack. This PowerPack enables you to discover, model, and collect data about IBM Db2 databases.

The *IBM: DB2* PowerPack includes:

- Example credentials you can use as templates to create credentials to discover and connect to the IBM Db2 databases and instances you want to monitor
- Dynamic Applications to discover, model, and monitor performance metrics and collect configuration data for IBM Db2 databases
- Event Policies and corresponding alerts that are triggered when IBM Db2 databases meet certain status criteria
- A Run Book Action and Run Book Automation policy for aligning Dynamic Applications
- A device dashboard to display summary information about Db2 instances

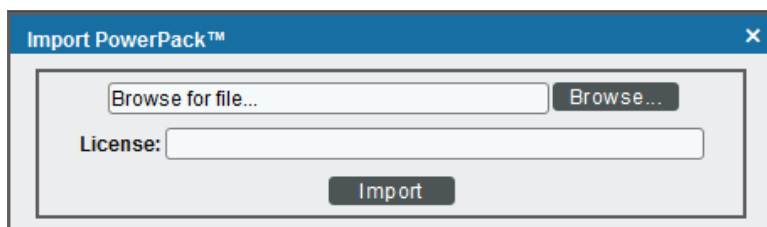
Installing the IBM: DB2 PowerPack

Before completing the steps in this manual, you must import and install the latest version of the *IBM: DB2* 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 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*.

Configuring IBM Db2 Monitoring

Overview

The following sections describe how to configure and discover IBM Db2 databases for monitoring by SL1 using the *IBM: DB2 PowerPack*:

Prerequisites for Monitoring IBM Db2	6
<i>Prerequisites for Linux/Unix Users</i>	7
<i>Prerequisites for Windows Users</i>	8
Creating Credentials for IBM Db2	9
<i>Creating an SSH/Key Credential (Linux and Unix Users)</i>	9
<i>Creating a PowerShell Credential (Windows Users)</i>	11
<i>Creating a SOAP/XML Credential (Linux and Unix Users)</i>	12
<i>Creating a SOAP/XML Credential (Windows Users)</i>	14
Discovering IBM Db2 Component Devices	15
Verifying Discovery and Dynamic Application Alignment	16
Viewing IBM Db2 Component Devices	21

Prerequisites for Monitoring IBM Db2

To configure the SL1 system to monitor IBM Db2 databases using the *IBM: DB2 PowerPack*, you must first perform the following prerequisites based on your operating system:

Prerequisites for Linux/Unix Users

1. Create a shell session and SSH into the Db2 database you want to monitor.
2. Create a new group to monitor by entering the following command:

```
sudo groupadd <group_name>
```

2. Create a new user for the group you created by entering the following command:

```
sudo useradd -u <user_id> -g <group_name> -m -d /home/<user_name> <user_name>
```

3. Set a password for the user you created by entering the following command:

```
sudo passwd <user_name>
```

4. Log in with the instance admin user. For example: `su - db2inst1`

5. Run the following commands:

```
db2 update database manager configuration using SYSMON_GROUP <group_name>
```

```
db2stop
```

```
db2start
```

6. Connect to your database with the following command:

```
db2 connect to <db_name>
```

7. Run the following command to grant the DATAACCESS privilege to the user:

```
db2 "grant DATAACCESS ON DATABASE TO USER <user_name>"
```

8. Verify permissions with the following commands:

```
db2 connect to <db_name> user <user_name> using <user_password>
```

```
db2 "select SUBSTR(AUTHORITY,1,30), D_USER, D_GROUP, D_PUBLIC, ROLE_USER, ROLE_
GROUP, ROLE_PUBLIC, D_ROLE from table (sysproc.auth_list_authorities_for_authid
(CURRENT_USER, 'U'))"
```

NOTE: Repeat steps 4 - 7 for each Db2 instance.

	D_USER	D_GROUP	D_PUBLIC	ROLE_USER	ROLE_GROUP	ROLE_PUBLIC	D_ROLE
1							
SYSADM	*	N	*	*	*	*	*
DBADM	N	N	N	N	N	N	*
CREATETAB	N	N	Y	N	N	N	*
BINDADD	N	N	Y	N	N	N	*
CONNECT	N	Y	Y	N	N	N	*
CREATE_NOT_FENCED_ROUTINE	N	N	N	N	N	N	*
SYSCTRL	*	N	*	*	*	*	*
SYMAINT	*	N	*	*	*	*	*
IMPLICIT_SCHEMA	N	N	Y	N	N	N	*
LOAD	N	N	N	N	N	N	*
CREATE_EXTERNAL_ROUTINE	N	N	N	N	N	N	*
QUIESCE_CONNECT	N	N	N	N	N	N	*
SECADM	N	N	N	N	N	N	*
SYSMON	*	Y	*	*	*	*	*
SQLADM	N	N	N	N	N	N	*
WLMADM	N	N	N	N	N	N	*
EXPLAIN	N	N	N	N	N	N	*
DATAACCESS	Y	N	N	N	N	N	*
ACCESSCTRL	N	N	N	N	N	N	*

For Unix systems, the user created will likely need to use the kornshell. To do this, run the following commands:

```
sudo useradd -u <user_id> -g <group_name> -s <shell_directory> -m -d /home/<user_name> <user_name>
```

Prerequisites for Windows Users

NOTE: Before performing the steps for the Windows prerequisites, ensure that you have followed the steps in the *Configuring Windows Servers for Monitoring with PowerShell* section of the **Monitoring Windows Systems with PowerShell** manual.

Windows users will need to create a local user and group for the Db2 database. If you have already done so, proceed to [adding the group to the instance database manager](#). To create the user and group, perform the following steps:

1. Click **[Start]** and select **Run**.
2. In the **Run** window, enter `lusrmgr.msc` and click **[OK]**.
3. In the **Local Users and Groups** pane, select the **Users** folder.
4. Click the **Action** menu and select *New User...* Enter the new user's information in the **New User** window and click **[Create]**.
5. In the **Local Users and Groups** pane, select the **Groups** folder.
6. Click the **Action** menu and select *New Group...* Enter the new group's information in the **New Group** window and click **[Create]**.
7. To add the new user to the group, double-click on the group name.
8. Click the **[Add...]** button under the **Members** window and enter the username. Click **[OK]**.

NOTE: You may need to add the user to the Administrators group in order to use PowerShell remoting if you don't have a PowerShell group/policy in place for non-administrative users.

Next, you will need to add the group you created to the instance database manager:

1. Log in to the Db2 database as the instance admin user.
2. Open the Db2 admin shell.
3. Run the following commands:

```
db2 update database manager configuration using SYSMON_GROUP <group_name>
db2stop
db2start
```

Next, you will grant the DATAACCESS privilege to the new user:

1. Log in to the Db2 database as the instance admin user.
2. Open the Db2 admin shell.
3. Run the following commands:

```
db2 connect to <database>
db2 "grant DATAACCESS on database to user <user_name>"
```

NOTE: You will need to grant this access to each database.

NOTE: Perform the steps to add the group to the instance database manager and to grant the DATAACCESS privilege for each Db2 instance that you will monitor.

Creating Credentials for IBM Db2

To monitor Db2 databases using SL1, you must create two credentials. These credentials enable SL1 to collect data from your Db2 databases. The types of credentials that are required for monitoring depend on the type of database being monitored:

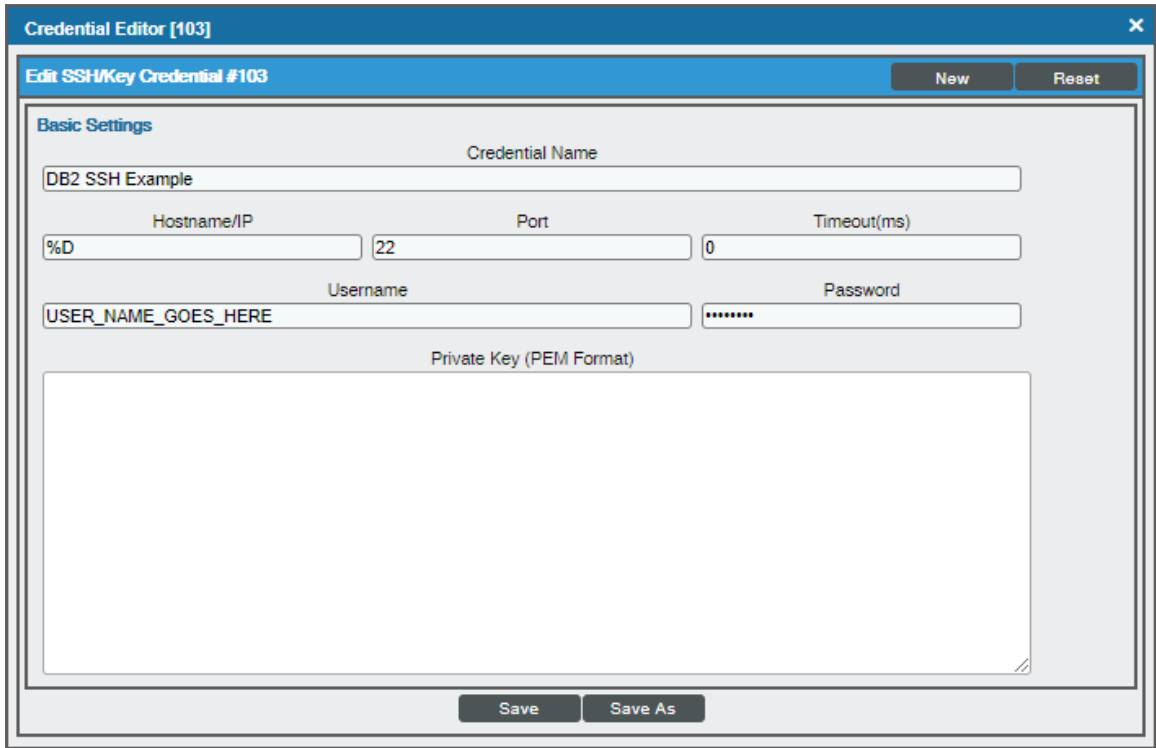
- Linux and Unix users must use an [SSH/Key credential](#) and a [SOAP/XML credential](#)
- Windows users must use a [PowerShell credential](#) and a [SOAP/XML credential](#)

Creating an SSH/Key Credential (Linux and Unix Users)

Linux and Unix users must create an SSH/Key credential.

To create an SSH/Key credential :

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click the wrench icon (🔧) for the "DB2 SSH Example" credential. The **Credential Editor** modal page appears:



The screenshot shows a modal window titled "Credential Editor [103]". Inside, there's a sub-header "Edit SSH/Key Credential #103" with "New" and "Reset" buttons. The main area is labeled "Basic Settings" and contains several input fields: "Credential Name" (with "DB2 SSH Example" entered), "Hostname/IP" (with "%D"), "Port" (with "22"), "Timeout(ms)" (with "0"), "Username" (with "USER_NAME_GOES_HERE"), and "Password" (with "*****"). There is also a large text area for "Private Key (PEM Format)". At the bottom, there are "Save" and "Save As" buttons.

3. Supply values in the following fields:
 - **Credential Name**. Type a new name for the credential.
 - **Hostname/IP**. Type the IP address or hostname of the Db2 database you want to monitor.
 - **Port**. Keep the default setting.
 - **Timeout(ms)**. Keep the default setting.
 - **Username**. Type the username for a user with access to the Db2 database.
 - **Password**. Required. Type the password for the account with access to the Db2 database.
 - **Private Key (PEM Format)**. Optional. Use if required for SSH authentication.
4. Click the **[Save As]** button.
5. When the confirmation message appears, click **[OK]**.

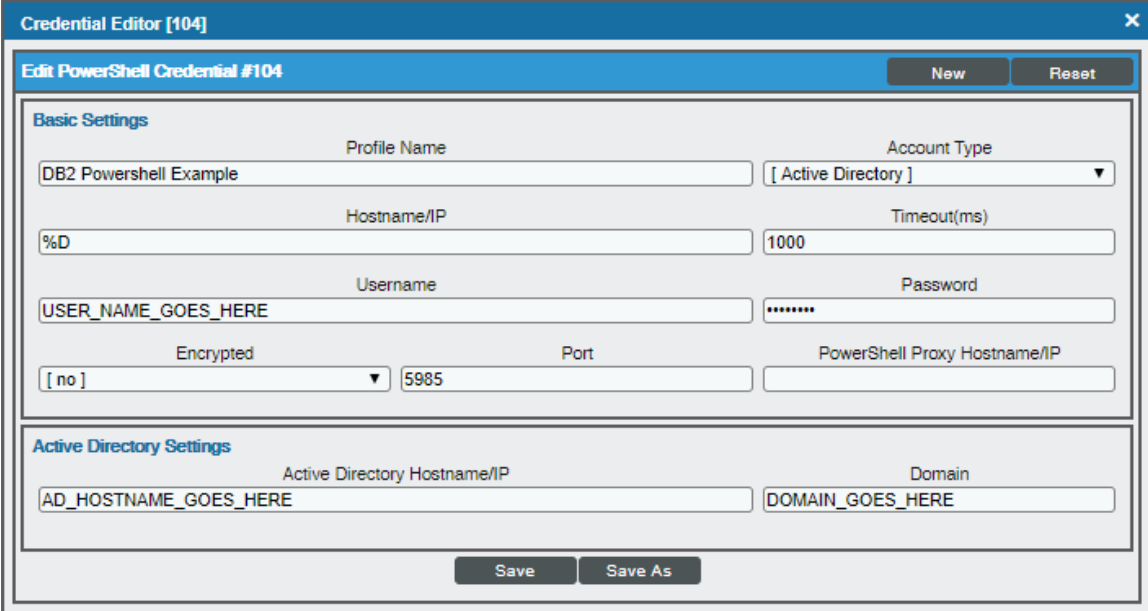
NOTE: The credential ID will appear at the top of the window after it has been saved. Take note of the ID as you will need it when creating the SOAP/XML credential.

Creating a PowerShell Credential (Windows Users)

Windows users must create a PowerShell credential.

To create a PowerShell credential:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click the wrench icon (🔧) for the "DB2 Powershell Example" credential. The **Credential Editor** modal page appears:



The screenshot shows the "Credential Editor [104]" window. The title bar is blue with a close button (X). Below the title bar is a header bar with "Edit PowerShell Credential #104" and "New" and "Reset" buttons. The main area is divided into two sections: "Basic Settings" and "Active Directory Settings".

Basic Settings:

- Profile Name: DB2 Powershell Example
- Account Type: [Active Directory]
- Hostname/IP: %D
- Timeout(ms): 1000
- Username: USER_NAME_GOES_HERE
- Password: [masked with dots]
- Encrypted: [no]
- Port: 5985
- PowerShell Proxy Hostname/IP: [empty]

Active Directory Settings:

- Active Directory Hostname/IP: AD_HOSTNAME_GOES_HERE
- Domain: DOMAIN_GOES_HERE

At the bottom of the window are "Save" and "Save As" buttons.

3. Supply values in the following fields:

- **Profile Name.** Type a new name for the credential. Can be any combination of alphanumeric characters.
- **Account Type.** Select the type of authentication for the username and password in this credential. Choices are:
 - *Active Directory.* On the device, Active Directory will authenticate the username and password in this credential.
 - *Local.* Local security on the device will authenticate the username and password in this credential.
- **Hostname/IP.** Type the IP address of the Db2 database from which you want to retrieve data, or enter the variable **%D**.
- **Timeout (ms).** Type the time, in milliseconds, after which SL1 will stop trying to collect data from the authenticating server. For collection to be successful, SL1 must connect to the authenticating server, execute the PowerShell command, and receive a response within the amount of time specified in this field.
- **Username.** Type the username for a user with access to the Db2 database to be monitored.
- **Password.** Type the password for the user account with access to the Db2 database to be monitored.
- **Encrypted.** Select whether SL1 will communicate with the device using an encrypted connection. Choices are:
 - *yes.* When communicating with the Windows server, SL1 will use a local user account with authentication of type "Basic Auth". You must then use HTTPS and can use a Microsoft Certificate or a self-signed certificate.
 - *no.* When communicating with the Windows server, SL1 will not encrypt the connection.
- **Port.** Leave as default value.
- **PowerShell Proxy Hostname/IP.** Leave this field blank.

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

Creating a SOAP/XML Credential (Linux and Unix Users)

After configuring the SSH/Key credential, you must then create a SOAP/XML credential.

To create the SOAP/XML credential:

1. Go to the **Credential Management** page (System > Manage > Credentials).

- Click the wrench icon () for either the "DB2 Soap with SSH Example" credential for Linux users. The **Credential Editor** modal page appears:

- Update the values in the following fields:

Basic Settings

- **Profile Name.** Type a new name for the credential.
- **URL.** Leave the default value of `https://%D`.

HTTP Headers

- **HTTP Headers.** Add the following headers by clicking **+ Add a header**:
 - `base_db2_path:<DB2 Installation Path>`. For example: `base_db2_path:/opt/ibm/db2/V11.5`
 - `instance:<Instance Name>:<Port>:<DB Name>` For example: `instance:db2inst1:50000:ONE`
 - `instance:<Instance Name2>:<Port2>:<DB Name2>` For example: `instance:db2inst2:50000:TWO`

NOTE: You can create a header for each Db2 instance you have.

- `ssh:<SSH Credential ID>`

NOTE: During the discovery process, these headers will either find an existing Database credential that matches the user, password, port, and default database, or it will create a new Database credential.

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

Creating a SOAP/XML Credential (Windows Users)

After configuring the PowerShell credential, you must then create a SOAP/XML credential.

To create the SOAP/XML credential:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click the wrench icon (🔧) for either the "DB2 Soap with PowerShell Example" credential for Windows users. The **Credential Editor** modal page appears:

The screenshot shows the 'Credential Editor [104]' window with the following sections:

- Basic Settings:** Profile Name: 'DB2 Soap with Powershell Example', Content Encoding: '[text/xml]', Method: '[POST]', HTTP Version: '[HTTP/1.1]'. URL: 'http://%D'. HTTP Auth User, HTTP Auth Password, and Timeout (seconds): '2'.
- Proxy Settings:** Hostname/IP, Port: '0', and User.
- CURL Options:** A list of options including CAINFO, CAPATH, CLOSEPOLICY, CONNECTTIMEOUT, COOKIE, COOKIEFILE, COOKIEJAR, COOKIELIST, CRLF, CUSTOMREQUEST, and DNSCACHETIMEOUT.
- Soap Options:** Embedded Password [%P], Embed Value [%1], Embed Value [%2], Embed Value [%3], and Embed Value [%4].
- HTTP Headers:** '+ Add a header' button and two headers: 'instance:<Instance Name>:<Port>:<DB Nar' and 'powershell:<Powershell Credential ID>'.

Buttons at the bottom include 'Save' and 'Save As'.

3. Update the values in the following fields:

Basic Settings

- **Profile Name.** Type a new name for the credential.
- **URL.** Leave the default value of https://%D.

HTTP Headers

- **HTTP Headers.** Add the following headers by clicking + **Add a header**:
 - `instance:<Instance Name>:<Port>:<DB Name>` For example:
`instance:db2inst1:50000:ONE`
 - `instance:<Instance Name2>:<Port2>:<DB Name2>` For example:
`instance:db2inst2:50000:TWO`

NOTE: You can create a header for each Db2 instance you have.

- `powershell:<PowerShell Credential ID>`

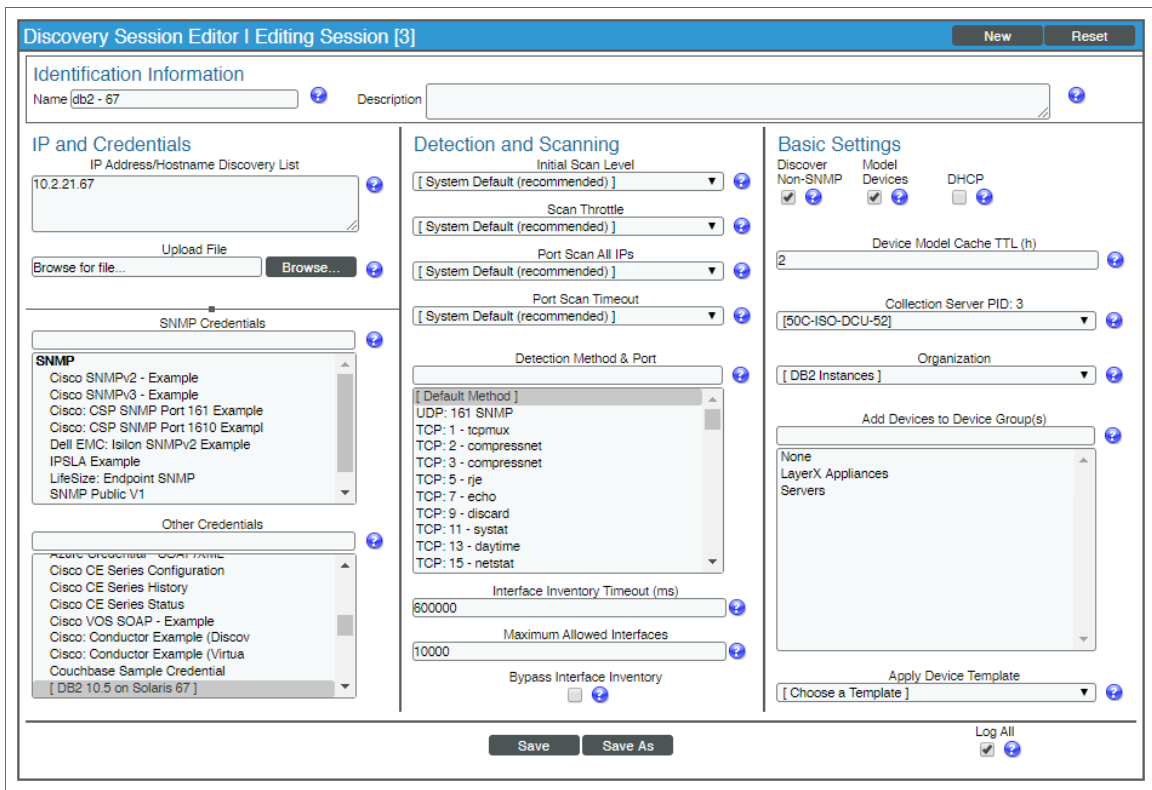
NOTE: During the discovery process, these headers will either find an existing Database credential that matches the user, password, port, and default database, or it will create a Database credential.



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

Discovering IBM Db2 Component Devices

To discover an IBM Db2 database:


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



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 Db2 database.
 - **Other Credentials**. Select the SOAP/XML credential you created for the Db2 database.
 - **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 () 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:

1. After the discovery session has completed, go to the **Device Manager** (Registry > Devices > Device Manager) page and find the device(s) you discovered. When you have located the device in the **Device Manager**, click on its edit icon ().
2. In the **Device Properties** page, click the **[Collections]** tab.
3. All applicable Dynamic Applications for the Db2 devices 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.

To verify alignment of the IBM Db2 Dynamic Applications:

1. After discovery has completed, click the device icon for the IBM Db2 device (). From the **Device Properties** page for the IBM Db2 device, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.

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


2. All applicable Dynamic Applications are automatically aligned to the root device and component devices during discovery:

You should see the following Dynamic Application aligned to the root device:

- IBM DB2: Server Discovery

Close	Properties	Thresholds	Collections	Monitors	Schedule		
Logs	Toolbox	Interfaces	Relationships	Tickets	Redirects	Notes	Attributes

Device Name	10.2.21.67	Managed Type	Physical Device
IP Address /ID	10.2.21.67 12	Category	Pingable
Class	Ping	Sub-Class	ICMP
Organization	DB2 Instances	Uptime	0 days, 00:00:00
Collection Mode	Active	Collection Time	2020-05-12 11:42:00
Description		Group / Collector	group_all 50C-ISO-DCU-52
Device Hostname			



Ping Device
10.2.21.67

Dynamic Application™ Collections							Expand	Actions	Reset	Guide
	Dynamic Application	ID	Poll Frequency	Type	Credential	Collector				
+	IBM DB2: Server Discovery	1801	15 mins	Snippet Configuration	DB2 10.5 on Solaris 67	50C-ISO-DCU-52				

Copyright © 2003 - 2020 ScienceLogic, Inc. All rights reserved.

You should see the following Dynamic Application aligned to the Db2 server:

- IBM DB2: Instance Discovery

Close	Properties	Thresholds	Collections	Monitors	Schedule		
Logs	Toolbox	Interfaces	Relationships	Tickets	Redirects	Notes	Attributes

Device Name	IBM DB2 Server	Managed Type	Component Device
ID	13	Category	Servers Software
Class	IBM	Sub-Class	DB2 Server
Organization	DB2 Instances	Uptime	0 days, 00:00:00
Root Device	10.2.21.67	Group / Collector	group_all 50C-ISO-DCU-52
Parent Device	10.2.21.67		
Device Hostname			

Dynamic Application™ Collections							Expand	Actions	Reset	Guide
	Dynamic Application	ID	Poll Frequency	Type	Credential	Collector				
+ IBM DB2:	Instance Discovery	1802	15 mins	Snippet Configuration	DB2 10.5 on Solaris 67	50C-ISO-DCU-52				<input checked="" type="checkbox"/>

[Select Action]

Copyright © 2003 - 2020 ScienceLogic, Inc. All rights reserved.

You should see the following Dynamic Application aligned to the Db2 instances:

- IBM DB2: Authorizations Configuration
- IBM DB2: Buffer Pools Performance
- IBM DB2: Containers Configuration
- IBM DB2: Diagnostics Log Configuration
- IBM DB2: Indexes Configuration
- IBM DB2: Instance Status
- IBM DB2: Product Configuration
- IBM DB2: Subclass Performance
- IBM DB2: Summary Performance
- IBM DB2: System Utilization Performance
- IBM DB2: Tables Performance
- IBM DB2: Tablespace Capacity Performance
- IBM DB2: Tablespace Configuration
- IBM DB2: Tablespace Container Performance

- IBM DB2: Tablespace Performance
- IBM DB2: Workload Performance


Close	Properties	Thresholds	Collections	Monitors	Schedule				
Logs	Toolbox	Interfaces	Relationships	Tickets	Redirects	Notes	Attributes		
Device Name	db2inst1	Managed Type	Component Device						
ID	14	Category	Servers Software						
Class	IBM	Sub-Class	DB2 Instance						
Organization	DB2 Instances	Uptime	0 days, 00:00:00						
Root Device	10.2.21.67	Group / Collector	group_all 50C-ISO-DCU-52						
Parent Device	IBM DB2 Server								
Device Hostname									
Dynamic Application™ Collections									
Dynamic Application	ID	Poll Frequency	Type	Credential	Collector	Expand	Actions	Reset	Guide
+ IBM DB2: Buffer Pools Performance	1796	5 mins	Snippet Performance	DB2 Port: 50000 DB: SAMPLE	50C-ISO-DCU-52				<input checked="" type="checkbox"/>
+ IBM DB2: Subclass Performance	1792	5 mins	Snippet Performance	DB2 Port: 50000 DB: SAMPLE	50C-ISO-DCU-52				<input type="checkbox"/>
+ IBM DB2: Summary Performance	1788	5 mins	Snippet Performance	DB2 Port: 50000 DB: SAMPLE	50C-ISO-DCU-52				<input type="checkbox"/>
+ IBM DB2: System Utilization Performance	1800	5 mins	Snippet Performance	DB2 Port: 50000 DB: SAMPLE	50C-ISO-DCU-52				<input type="checkbox"/>
+ IBM DB2: Tables Performance	1805	5 mins	Snippet Performance	DB2 Port: 50000 DB: SAMPLE	50C-ISO-DCU-52				<input type="checkbox"/>
+ IBM DB2: Tablespace Capacity Performance	1790	5 mins	Snippet Performance	DB2 Port: 50000 DB: SAMPLE	50C-ISO-DCU-52				<input type="checkbox"/>
+ IBM DB2: Tablespace Container Performance	1793	5 mins	Snippet Performance	DB2 Port: 50000 DB: SAMPLE	50C-ISO-DCU-52				<input type="checkbox"/>
+ IBM DB2: Tablespace Performance	1798	5 mins	Snippet Performance	DB2 Port: 50000 DB: SAMPLE	50C-ISO-DCU-52				<input type="checkbox"/>
+ IBM DB2: Workload Performance	1797	5 mins	Snippet Performance	DB2 Port: 50000 DB: SAMPLE	50C-ISO-DCU-52				<input type="checkbox"/>
+ IBM DB2: Authorizations Configuration	1799	15 mins	Snippet Configuration	DB2 Port: 50000 DB: SAMPLE	50C-ISO-DCU-52				<input type="checkbox"/>
+ IBM DB2: Containers Configuration	1794	15 mins	Snippet Configuration	DB2 Port: 50000 DB: SAMPLE	50C-ISO-DCU-52				<input type="checkbox"/>
+ IBM DB2: Diagnostics Log Configuration	1804	15 mins	Snippet Configuration	DB2 10.5 on Solaris 67	50C-ISO-DCU-52				<input type="checkbox"/>
+ IBM DB2: Indexes Configuration	1795	15 mins	Snippet Configuration	DB2 Port: 50000 DB: SAMPLE	50C-ISO-DCU-52				<input type="checkbox"/>
+ IBM DB2: Instance Status	1803	15 mins	Snippet Configuration	DB2 10.5 on Solaris 67	50C-ISO-DCU-52				<input type="checkbox"/>
+ IBM DB2: Product Configuration	1791	15 mins	Snippet Configuration	DB2 Port: 50000 DB: SAMPLE	50C-ISO-DCU-52				<input type="checkbox"/>
+ IBM DB2: Tablespace Configuration	1789	15 mins	Snippet Configuration	DB2 Port: 50000 DB: SAMPLE	50C-ISO-DCU-52				<input type="checkbox"/>
[Select Action] <input type="button" value="Go"/>									
<input type="button" value="Save"/>									

Copyright © 2003 - 2020 ScienceLogic, Inc. All rights reserved.

NOTE: The IBM DB2 PowerPack uses db2ilist to discover all Db2 instances, but the Dynamic Applications will be aligned to only the instances specified in the SOAP/XML credential headers.

Viewing IBM Db2 Component Devices

In addition to the **Device Manager** page (Registry > Devices > Device Manager), you can view the IBM Db2 server and all associated component devices in the following places in the user interface:

- The **Device View** modal page (click the bar-graph icon  for a device, then click the **Topology** tab) 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:

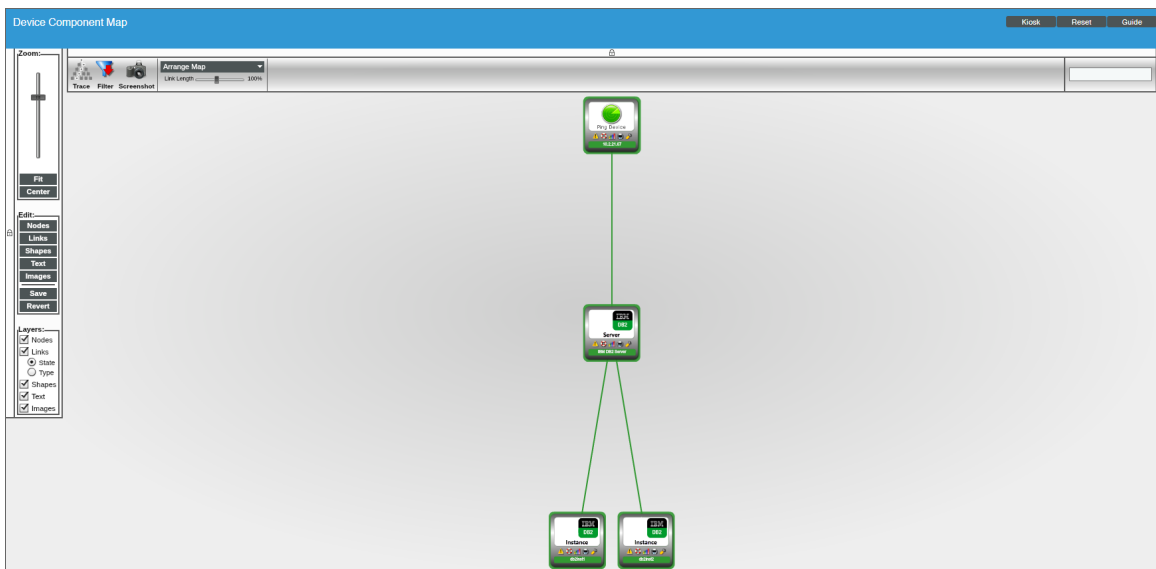


The screenshot displays the 'Device View' modal page. At the top, there is a navigation bar with tabs: Close, Summary, Performance, Topology (selected), Configs, Interfaces, TCP/UDP Ports, and Organization. Below the navigation bar, there are two columns of device details. The left column includes fields like Device Name, IP Address / ID, Class, Organization, Collection Mode, Description, and Device Hostname. The right column includes Managed Type, Category, Sub-Class, Uptime, Collection Time, and Group / Collector. A small Linux penguin icon is visible on the right side of the details section. Below the details, there is a 'Device View' header with 'Reset' and 'Guide' buttons. A 'Component Mapping' checkbox is checked. The main area shows a topology diagram with two nodes connected by a blue line. The top node is a Linux device with a penguin icon and IP address 10.2.21.176. The bottom node is an IBM Db2 Server with the text 'DB2 Server' and 'IBM DB2 Server' below it.

- 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 an IBM Db2 server, find the IBM Db2 device and click its plus icon (+):

Device Name	IP Address	Device Category	Device Class Sub-class	DID	Organization	Current State	Collection Group	Collection State
10.2.21.176	10.2.21.176	Unknown	Ping Generic Linux	951	System	Healthy	OCG	User-Disabled
10.2.21.67	10.2.21.67	Pingable	Ping ICMP	947	System	Healthy	OCG	User-Disabled
IBM Db2 Server	--	Software	IBM DB2 Server	948	System	Healthy	DCG	User-Disabled
dbinst1	--	Software	IBM DB2 Instance	949	System	Healthy	DCG	User-Disabled/Unavailable
dbinst2	--	Software	IBM DB2 Instance	950	System	Healthy	DCG	User-Disabled/Unavailable

- 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. The platform also updates each map with the latest status and event information. To view the map for an IBM Db2 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.



Chapter

3

IBM Db2 Dashboards

Overview

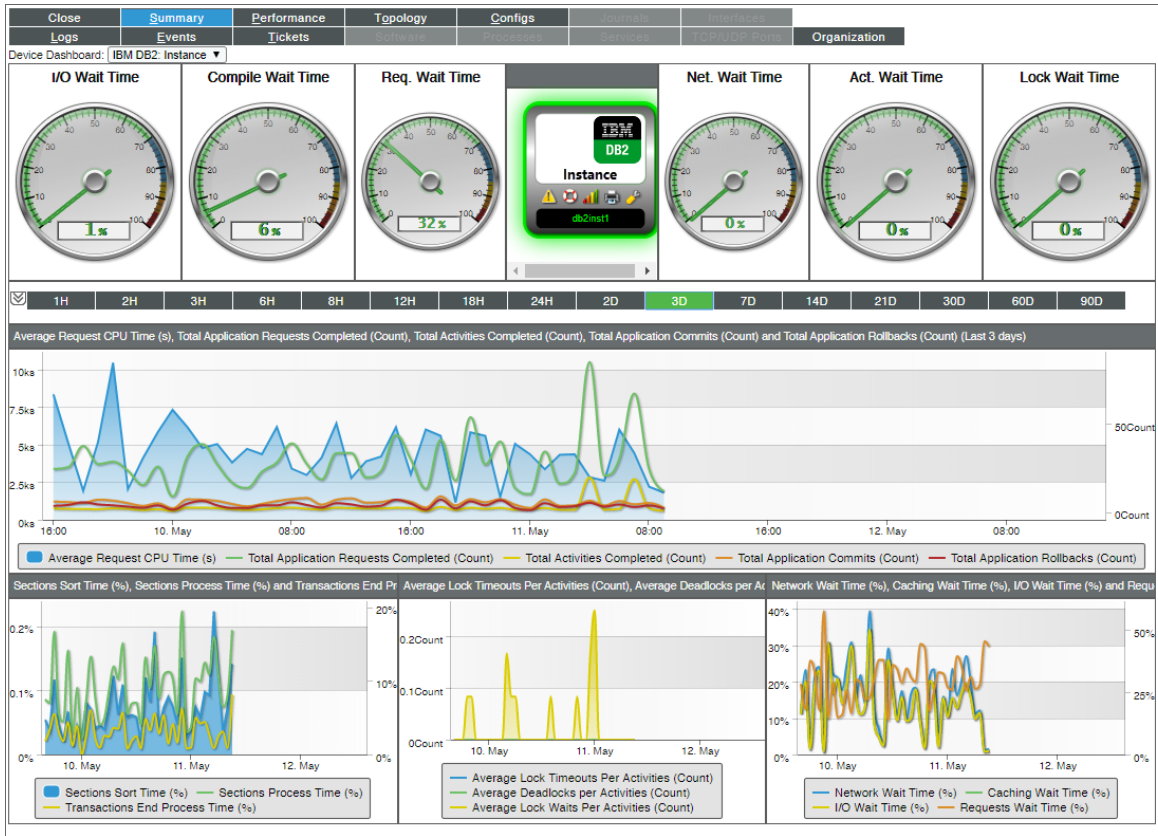
The following section describes the device dashboard that is included in the *IBM: DB2* PowerPack:

<i>Device Dashboard</i>	23
<i>IBM DB2: Instance</i>	24

Device Dashboard

The *IBM: DB2* PowerPack includes a device dashboard that provides summary information for Db2 instances. The device dashboard is aligned as the default device dashboard for the Db2 instances.

IBM DB2: Instance



The IBM DB2: Instance device dashboard displays the following information:

- Six gauges that display the following metrics:
 - I/O Wait Time
 - Compile Wait Time
 - Req. Wait Time
 - Net. Wait Time
 - Act. Wait Time
 - Lock Wait Time
- A line graph that displays the following information:
 - Average Request CPU Time (s)
 - Total Application Requests Completed (Count)
 - Total Activities Completed (Count)

- Total Application Commits (Count)
- Total Application Rollbacks (Count)
- A line graph that displays the following information on sections:
 - Sections Sort Time (%)
 - Sections Process Time (%)
 - Transactions End Process Time (%)
- A line graph that displays the following information on locks:
 - Average Lock Timeouts Per Activities (Count)
 - Average Deadlocks per Activities (Count)
 - Average Lock Waits Per Activities (Count)
- A line graph that displays the following information on wait times:
 - Network Wait Time (%)
 - Caching Wait Time (%)
 - I/O Wait Time (%)
 - Requests Wait Time (%)

© 2003 - 2020, 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



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

International: +1-703-354-1010