Monitoring IBM Db2

IBM: Db2 PowerPack version 107

Table of Contents

Introduction ... **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 ... 10

Creating Credentials for IBM Db2 ... 11

Creating an SSH/Key Credential (Linux and Unix Users) ... 12

Creating an SSH/Key Credential (Linux and Unix Users) in the Skylar One Classic User Interface ... 14

Creating a PowerShell Credential (Windows Users) ... 15

Creating a PowerShell Credential (Windows Users) in the Skylar One Classic User Interface ... 17

Creating a SOAP/XML Credential (Linux and Unix Users) ... 18

Creating a SOAP/XML Credential (Linux and Unix Users) in the Skylar One Classic User Interface ... 19

Creating a SOAP/XML Credential for an SSL Certificate (Linux and Unix Users) ... 21

Creating a SOAP/XML Credential for an SSL Certificate (Linux and Unix Users) in the Skylar One Classic User Interface ... 24

Creating a SOAP/XML Credential (Windows Users) ... 26

Creating a SOAP/XML Credential (Windows Users) in the Skylar One Classic User Interface ... 27

Creating a SOAP/XML Credential for an SSL Certificate (Windows Users) ... 28

Creating a SOAP/XML Credential for an SSL Certificate (Windows Users) in the Skylar One Classic User Interface ... 31

Updating the Database Credential ... 33

Discovering IBM Db2 Component Devices ... 34

Discovering IBM Db2 Component Devices in the Skylar One Classic User Interface ... 36

Verifying Discovery and Dynamic Application Alignment ... 36

Viewing IBM Db2 Component Devices ... 40

IBM Db2 Dashboards in the Skylar One Classic User Interface ... **41**

Device Dashboard ... 41

IBM Db2: Database ... 41

IBM: DB2 Tablespace ... 42

Chapter 1

Introduction

Overview

This manual describes how to monitor IBM Db2 databases in Skylar One using the "IBM: Db2" PowerPack.

Use the following menu options to navigate the Skylar One user interface:

- To view a pop-out list of menu options, click the menu icon ( ).
- To view a page containing all of the menu options, click the Advanced menu icon ( ).

This chapter covers the following topics:

What Does the IBM: Db2 PowerPack Monitor? 4

Installing the IBM: Db2 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 Does the IBM: Db2 PowerPack Monitor?

To monitor IBM Db2 databases using Skylar One, 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 section on *Global Settings*.

NOTE: For details on upgrading Skylar One, see the relevant *Skylar One Platform Release Notes*.

To download and install the PowerPack:

1. Search for and download the PowerPack from the **PowerPacks** page at the ScienceLogic Support Center (Skylar One > PowerPacks, login required).
2. In Skylar One, go to the **PowerPacks** page (System > Manage > PowerPacks).
3. Click the **[Actions]** button and choose *Import PowerPack*. The **Import PowerPack** dialog box appears.
4. Click **[Browse]** and navigate to the PowerPack file from step 1.
5. Select the PowerPack file and click **[Import]**. The **PowerPack Installer** modal displays a list of the PowerPack contents.
6. Click **[Install]**. The PowerPack is added to the **PowerPacks** page.

NOTE: If you exit the **PowerPack Installer** modal without installing the imported PowerPack, the imported PowerPack will not appear in the **PowerPacks** 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

Configuring IBM Db2 Monitoring

Overview

This section describes how to configure and discover IBM Db2 databases for monitoring by Skylar One using the "IBM: Db2" PowerPack.

Use the following menu options to navigate the Skylar One user interface:

- To view a pop-out list of menu options, click the menu icon ( ).
- To view a page containing all of the menu options, click the Advanced menu icon (•••).

This chapter covers the following topics:

Prerequisites for Monitoring IBM Db2 ..... *6*

Creating Credentials for IBM Db2 ..... *11*

Discovering IBM Db2 Component Devices *34*

Verifying Discovery and Dynamic Application Alignment *36*

Viewing IBM Db2 Component Devices *40*

Prerequisites for Monitoring IBM Db2

To configure the Skylar One system to monitor IBM Db2 databases using the "IBM: Db2" PowerPack, you must first perform the following prerequisites, which are based on your operating system.

NOTE: After you have configured Skylar One to monitor IBM Db2 databases and you have discovered an IBM Db2 server and all associated component devices, make sure that the ports for the IBM Db2 instance are open to the Skylar One Data Collector.

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>
   ```

3. 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>
   ```

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

   ```
   sudo passwd <user_name>
   ```

5. Log in with the instance admin user. For example: `su - db2inst1`
6. Run the following commands:

   ```
   db2 update database manager configuration using SYSMON_GROUP <group_
   name>
   ```

   ```
   db2stop
   ```

   ```
   db2start
   ```

7. Connect to your database with the following command:

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

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

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

NOTE: If you do not want to grant DATAACCESS privilege to the user, ScienceLogic provides a Bash and SQL scripts in a .zip file in the PowerPack download folder that grants the user permissions required to monitor Db2 databases.

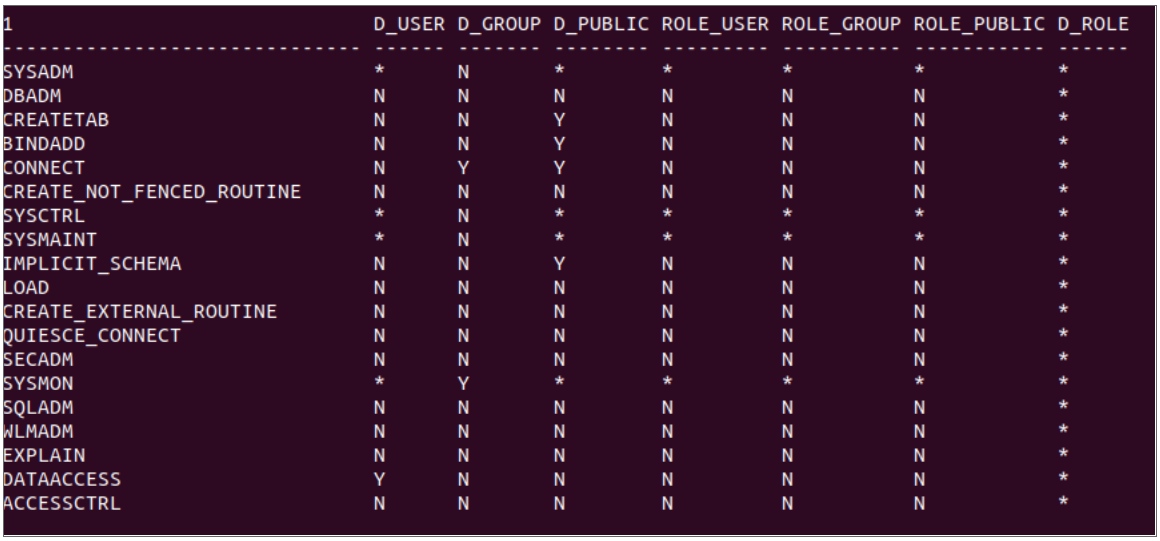
- The Bash script grants required permissions to monitor Linux Db2 databases. To use the Bash script in the Linux Db2 server:
  - Copy the Bash script named **grant_mon_per.sh** to the Linux Db2 server.
  - Give the execute permission to the script with: `chmod +x grant_mon_per.sh`
  - Log in with the instance administrator user, for example: `su -db2inst1`.
  - Run the script with the following command in the same directory where you copied the script above. Replace the required information before running the command: `./grand_mon_per.sh <DB_NAME> <DB_USER> <mon_user_name>`
    - DB_NAME: Database name you want to grant permissions
    - DB_USER: The Db2 instance admin user. For example: su - db2inst1
    - mon_user_name: The new user name that you want to grant the permissions to.
  - Enter the database password of the instance admin user. The required permissions should be configured.

9. 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 5 - 8 for each Db2 instance.



1	D_USER	D_GROUP	D_PUBLIC	ROLE_USER	ROLE_GROUP	ROLE_PUBLIC	D_ROLE
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	*	*	*	*	*
SYSMAINT	*	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	*

NOTE: The user you create will likely need to use KornShell (for Unix systems) or Bash (for Linux systems).

If you are unsure of the shell directory, you can use the command `which ksh` to determine the KornShell directory, or `which bash` to determine the Bash directory.

After you have determined shell directory, run the following commands, replacing *<shell_directory>* with the KornShell or Bash directory:

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

You ***should not*** use Shell (`sh`) as the shell for the user. Using Shell for the user shell could result in shell-related errors appearing in the Device Log.

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:

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-adminstrative 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: If you do not want to grant DATAACCESS privilege to the user, ScienceLogic provides a Bash and SQL scripts in a .zip file in the PowerPack download folder that grants the user permissions required to monitor Db2 databases.

- The SQL script grants required permissions to monitor Windows Db2 databases. To use the SQL script in the Windows Db2 server:
  - Log in to the Windows Db2 database as the instance admin user.
  - Copy the SQL script named **grant_mon_per.sql** to the Windows Db2 server.
  - With a text editor, open the SQL script and replace `<mon_user_name>` with the user name that you want to grant the permissions to.
  - Save your changes and close the script window.
  - Open the "DB2 Command window" and at the Db2 command line, navigate to the directory where you copied the SQL script above.
  - Connect your database with the following command:
    `db2 connect to <db_name>`
  - Run the query with the following command:
    `db2 -vtf grant_mon_per.sql`
  - The required permissions should be configured.

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 Skylar One, you must create two credentials. These credentials enable Skylar One 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
    - If your Db2 server contains an SSL connection, you can create a *SOAP/XML credential with an SSL certificate*; otherwise, you create a *SOAP/XML credential without an SSL certificate*.
- Windows users must use a *PowerShell credential* and a SOAP/XML credential
    - If your Db2 server contains an SSL connection, you can create a *SOAP/XML credential with an SSL certificate*; otherwise, you create a *SOAP/XML credential without an SSL certificate*.
- In addition, if the password has changed for the account with access to the Db2 database, you will need to update the corresponding *Database credential*.

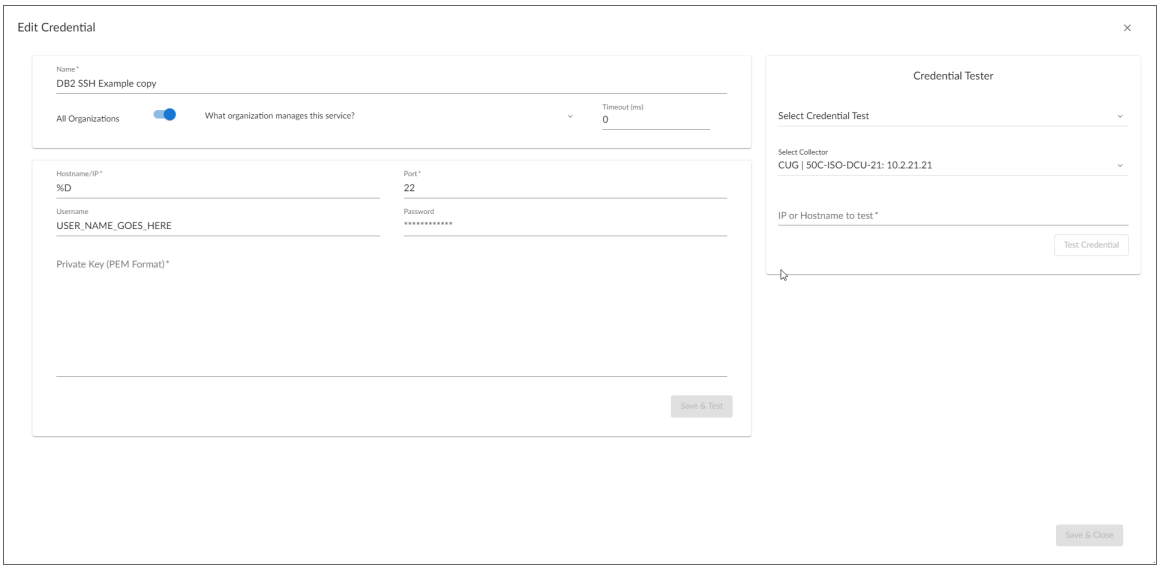
NOTE: Skylar One will use SSH or PowerShell at the beginning, and then the client provided by IBM. Skylar One uses the instance database manager user to connect to the Db2 database.

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 **Credentials** page (Manage > Credentials).
2. Locate the **DB2 SSH Example** credential, click its **[Actions]** icon (⋮) and select ***Duplicate***. A copy of the credential, called **DB2 SSH Example copy** appears.
3. Click the **[Actions]** icon (⋮) for the **DB2 SSH Example copy** credential and select ***Edit***. The **Edit Credential** page appears. Update the following fields:



4. Supply values in the following fields:
    - ***Name***. Type a new name for the credential.
    - ***All Organizations***. Toggle on (blue) to align the credential to all organizations, or toggle off (gray) and then select one or more specific organizations from the ***What organization manages this service?*** drop-down field to align the credential with those specific organizations.
    - ***Timeout(ms).*** Keep the default setting.
    - ***Hostname/IP.*** Type the IP address or hostname of the Db2 database you want to monitor.
    - ***Port.*** Keep the default setting.
    - ***Username***. Type the username for a user with access to the Db2 database.
    - ***Password***. Type the password for the account with access to the Db2 database.
    - ***Private Key (PEM Format)***. Optional. Use if required for SSH authentication.

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, Skylar One 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.

NOTE: If you are using a PEM key in the SSH/Key credential, then in your SOAP/XML credential you must fill in the ***HTTP Auth User*** and ***HTTP Auth Password*** fields with credentials for the same user.

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

NOTE: The credential ID will appear in the **Credentials** page (Manage > Credentials) after it has been saved. Take note of the ID as you will need it when creating the SOAP/XML credential. If you cannot see the ***ID*** column in the **Credentials** page, click the gear icon (⚙) in the upper-left corner of the page and select *Id* to view the column.

Creating an SSH/Key Credential (Linux and Unix Users) in the Skylar One Classic User Interface

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.
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***. Type the password for the account with access to the Db2 database.
   - ***Private Key (PEM Format)***. Optional. Use if required for SSH authentication.

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, Skylar One 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.

NOTE: If you are using a PEM key in the SSH/Key credential, then in your SOAP/XML credential you must fill in the ***HTTP Auth User*** and ***HTTP Auth Password*** fields with credentials for the same user.

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 **Credentials** page (Manage > Credentials).
2. Locate the **DB2 PowerShell Example** credential, click its **[Actions]** icon (⋮) and select ***Duplicate***. A copy of the credential, called **DB2 PowerShell Example copy** appears.
3. Click the **[Actions]** icon (⋮) for the **DB2 PowerShell Example copy** credential and select ***Edit***. The **Edit Credential** page appears.
4. Supply values in the following fields:

NOTE: The following fields reflect fields that appear in generic PowerShell credentials and might not yet appear in the **DB2 PowerShell Example copy** credential.

- ***Name***. Type a new name for the credential. Can be any combination of alphanumeric characters.
- ***All Organizations***. Toggle on (blue) to align the credential to all organizations, or toggle off (gray) and then select one or more specific organizations from the ***What organization manages this service?*** drop-down field to align the credential with those specific organizations.
- ***Timeout (ms)***. Type the time, in milliseconds, after which Skylar One will stop trying to collect data from the authenticating server. For collection to be successful, Skylar One must connect to the authenticating server, execute the PowerShell command, and receive a response within the amount of time specified in this field.
- ***Hostname/IP***. Type the IP address of the Db2 database from which you want to retrieve data, or enter the variable **%D**.
- ***Port***. Leave as default value.
- ***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.
- ***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.

- ***Use SSL (HTTPS)*** / ***Encrypted***. Toggle on (blue) if you want Skylar One to communicate with the device using an encrypted connection over HTTPS. If enabled, Skylar One will communicate with the Windows server using 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.

> **NOTE:** In Skylar One versions prior to 12.3.7, this field is labeled ***Encrypted***. In versions 12.3.7 and above, it is labeled ***Use SSL (HTTPS)***.

> **NOTE:** In Skylar One versions 11.3.0 and later, a newer Kerberos library is used that allows for message encryption over HTTP. This feature is on by default and may eliminate the need for you to configure an HTTPS certificate depending on your security requirements.

- ***Validate Certificate (when HTTPS is used)***. This field is visible when the ***Use SSL (HTTPS)*** toggle field is enabled for the connection and enables you to select whether a certificate is validated for the credential. Choices are:
  - *Ignore*. Skylar One will not validate a certificate for the credential. This is the default setting.
  - *Validate*. Skylar One will require a validated certificate for the credential. If you select *Validate*, then the target device must include a non-expired certificate issued from a certificate authority.
- ***Active Directory Host/IP***. Type the AD hostname or IP here if you selected *Active Directory* under ***Account Type***.
- ***Active Directory Domain***. Type the AD domain if you selected *Active Directory* under ***Account Type***.
- ***Message Encryption Setting***. If you selected Active Directory in the ***Account Type*** field, select whether Kerberos packages sent over PowerShell Remoting Protocol (PSRP) or Windows Remote Management (WinRM) are encrypted. Choices are:
  - *Auto*. Encryption is enabled if the package supports it; otherwise, encryption is disabled. This is the default setting.
  - *Never*. Messages are never encrypted. If selected, the target device must support this option.
  - *Always*. Messages are always encrypted. If selected, the target device must support this option.
- ***PowerShell Proxy Hostname/IP***. Leave this field blank.

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

Creating a PowerShell Credential (Windows Users) in the Skylar One Classic User Interface

Windows users must create a PowerShell credential.

To create a PowerShell credential:

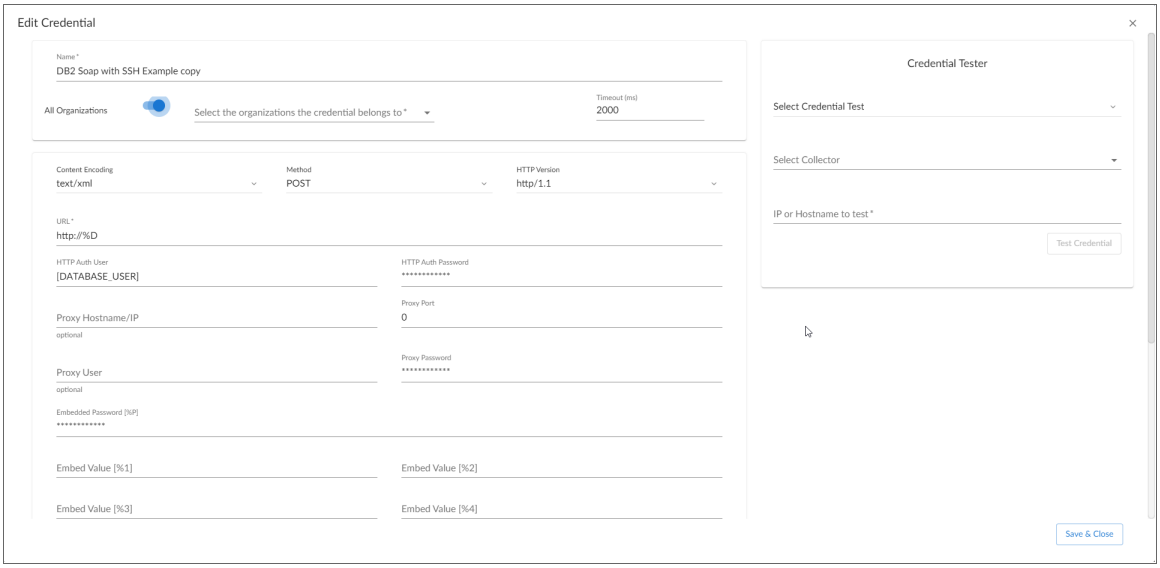
1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click the wrench icon ( ) for the "DB2 Powershell Example" credential. The **Credential Editor** modal page appears.
3. Supply values in the following fields:
    - ***Profile Name***. Type a new name for the credential. 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 Skylar One will stop trying to collect data from the authenticating server. For collection to be successful, Skylar One 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 Skylar One will communicate with the device using an encrypted connection. Choices are:
        - *yes*. When communicating with the Windows server, Skylar One 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, Skylar One 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 **Credentials** page (Manage > Credentials).
2. Locate the **DB2 Soap with SSH Example** credential, click its **[Actions]** icon (⋮) and select ***Duplicate***. A copy of the credential, called **DB2 Soap with SSH Example copy** appears.
3. Click the **[Actions]** icon (⋮) for the **DB2 Soap with SSH Example copy** credential and select ***Edit***. The **Edit Credential** page appears. Update the following fields:



4. Update the values in the following fields:
   - ***Name***. Type a new name for the credential.
   - ***All Organizations***. Toggle on (blue) to align the credential to all organizations, or toggle off (gray) and then select one or more specific organizations from the ***What organization manages this service?*** drop-down field to align the credential with those specific organizations.
   - ***URL***. Leave the default value of https://%D.
   - ***HTTP Auth User***. If you used a PEM key in the SSH/Key credential, type the username for the same user. Otherwise, if you are inserting the database username and password in the SSH/Key credential, leave this field blank.
   - ***HTTP Auth Password***. If you used a PEM key in the SSH/Key credential, type the password for the same user. Otherwise, if you are inserting the database username and password in the SSH/Key credential, leave this field blank.

NOTE: If the ***HTTP Auth User*** and ***HTTP Auth Password*** fields are blank, then the Dynamic Applications in the *IBM: Db2* PowerPack will use the credentials provided in the SSH/Key credential.

- ***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>` For example: `instance:db2inst1:50000`
  - `instance:<Instance Name2>:<Port2>` For example: `instance:db2inst2:50000`
  - `ssh:<SSH Credential ID>`

NOTE: In versions of the PowerPack prior to version 103, headers required the "<*DB_NAME*>" value. This value is no longer needed and can be deleted after you upgrade the PowerPack.

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

NOTE: By default, the SOAP/XML credential deletes any white space before and after the colon (:) in the credential headers. If you want to include paths with white spaces in the credential, surround the path with double quotes after the colon. For example: <base_db2_path:"/opt/folder name/program files">

NOTE: If your database port changes, you must also update the credential to reflect that change.

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

Creating a SOAP/XML Credential (Linux and Unix Users) in the Skylar One Classic User Interface

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).
2. Click the wrench icon (🔧) for the "DB2 Soap with SSH Example" credential for Linux/Unix users. The **Credential Editor** modal appears.
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 Auth User***. If you used a PEM key in the SSH/Key credential, type the username for the same user. Otherwise, if you are inserting the database username and password in the SSH/Key credential, leave this field blank.
   - ***HTTP Auth Password***. If you used a PEM key in the SSH/Key credential, type the password for the same user. Otherwise, if you are inserting the database username and password in the SSH/Key credential, leave this field blank.

> **NOTE:** If the ***HTTP Auth User*** and ***HTTP Auth Password*** fields are blank, then the Dynamic Applications in the *IBM: Db2* PowerPack will use the credentials provided in the SSH/Key credential.

   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>` For example: `instance:db2inst1:50000`
     - `instance:<Instance Name2>:<Port2>` For example: `instance:db2inst2:50000`
     - `ssh:<SSH Credential ID>`

> **NOTE:** In versions of the PowerPack prior to version 103, headers required the "<*DB_NAME*>" value. This value is no longer needed and can be deleted after you upgrade the PowerPack.

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

NOTE: By default, the SOAP/XML credential deletes any white space before and after the colon (:) in the credential headers. If you want to include paths with white spaces in the credential, surround the path with double quotes after the colon. For example: <base_db2_ path:"/opt/folder name/program files">

NOTE: If your database port changes, you must also update the credential to reflect that change.

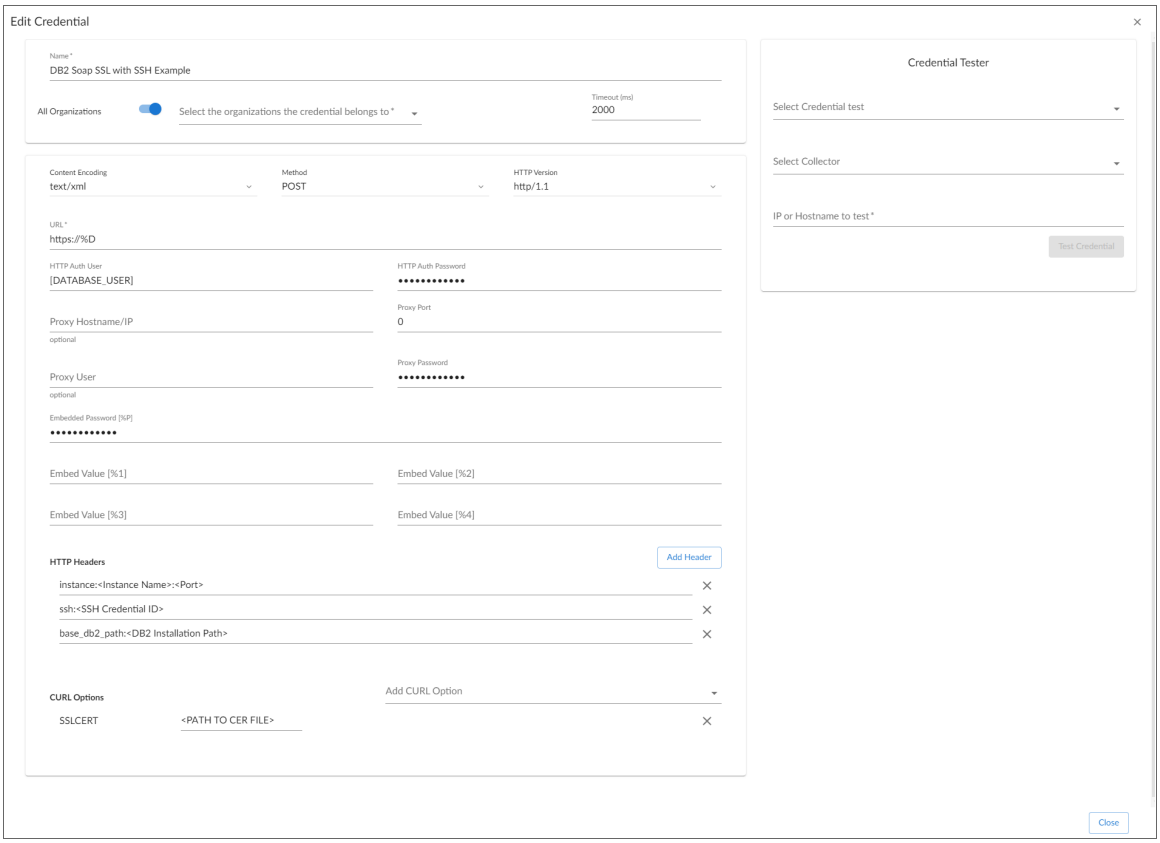
4. Click the **[Save As]** button.

Creating a SOAP/XML Credential for an SSL Certificate (Linux and Unix Users)

After configuring the SSH key, you must create a SOAP/XML credential with an SSL certificate if your Db2 server contains an SSL connection.

To create the SOAP/XML credential:

1. Go to the **Credentials** page (*Manage > Credentials*).
2. Locate the **DB2 Soap SSL with SSH Example** credential, click its **[Actions]** icon (⋮) and select ***Duplicate***. A copy of the credential called **DB2 Soap SSL with SSH Example copy** appears.
3. Click the **[Actions]** icon (⋮) for the **DB2 Soap SSL with SSH Example copy** credential and select ***Edit***. The **Edit Credentials** page appears.



4. Update the values in the following fields:

- ***Name***. Type a new name for the credential.
- ***All Organizations***.Toggle on (blue) to align the credential to all organizations, or toggle off (gray) and then select one or more specific organizations from the ***What organization manages this service?*** drop-down field to align the credentials with those specific organizations.
- ***URL***. Leave the default value of https://%D.
- ***HTTP Auth User***. If you used a PEM key in the SSH credential, type the username for the same user. Otherwise, if you are inserting the database username and password in the SSH credential, leave this field blank.
- ***HTTP Auth Password***. If you used a PEM key in the SSH credential, type the password for the same user. Otherwise, if you are inserting the database username and password in the SSH credential, leave this field blank.

NOTE: If the ***HTTP Auth User*** and the ***HTTP Auth Password*** fields are blank, then the Dynamic Applications in the *IBM: Db2 PowerPack* will use the credentials provided in the SSH key.

- ***HTTP Headers.*** Add the following headers by clicking ***+ Add a header***:
  - `base_db2_path:<DB2 Insallation Path>`.
    For example: `base_db2_path:/opt/ibm/db2/v11.5`
  - `instance:<Instance Name>:<SSL Port>`
    For example:`instance:db2inst1:60000`
  - `instance:<Instance Name2>:<SSL Port2>`
    For example: `instance:db2inst2:60001`
  - `ssh:<SSH Credential ID>`

TIP: In versions of the PowerPack prior to version 103, headers required the <DB_NAME> value. This value is no longer needed and can be deleted after you upgrade the PowerPack.

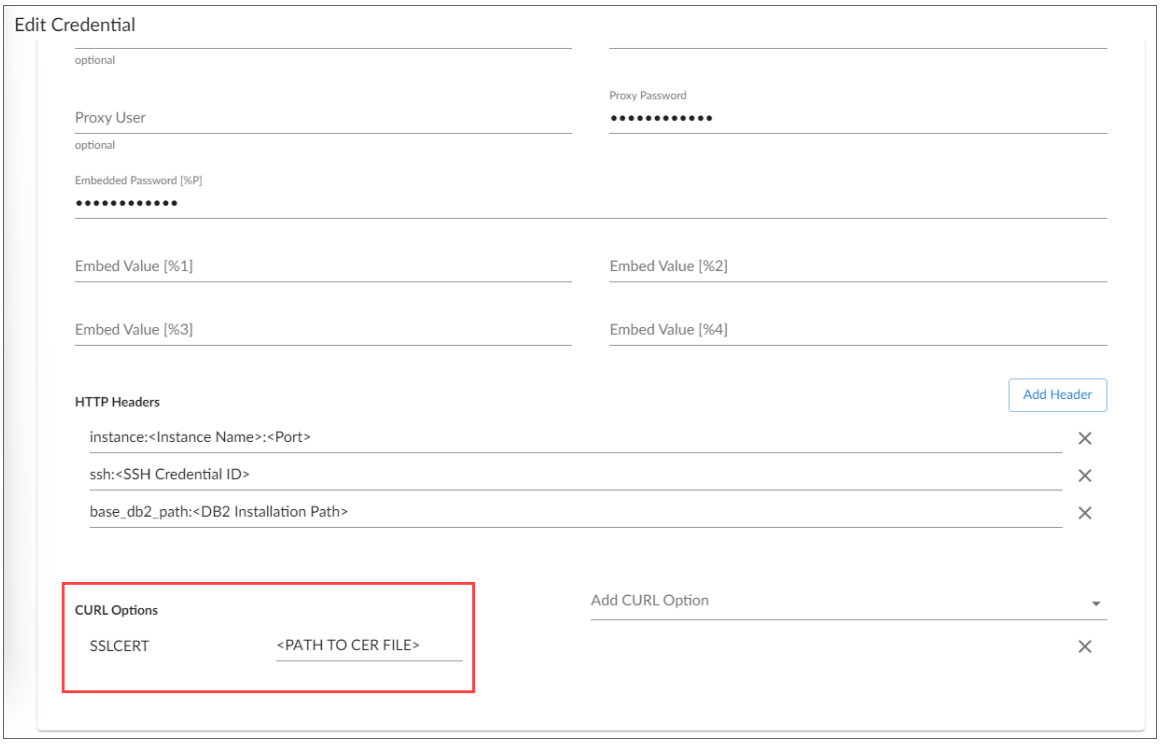
NOTE: You can create a header for each Db2 instance you have. During the discovery process, these headers will either find an existing Database credential that matches the user, password, port, and default database, or it will create a new Database credential.

IMPORTANT: By default, the SOAP/XML credential deletes any white space before and after the colon (:) in the credential headers. If you want to include paths with white spaces in the credential, surround the path with double quotes after the colon. For example: `<base_db2_path:"/opt/folder/name/program files">`

NOTE: If your database port changes, you must also update the credential to reflect that change.

- ***CURL options***: Edit the following field in this section:
  - SSLCERT. Type the certificate path for your SSL certificate.

NOTE: The certificate path should be a path of the Data Collectorwhere the SSL certificate is located. For example: `/tmp/certificate.cer`. The permissions for the SSL certificate file should be at least "read" and "write" for the owner, and "read" for the group and others. The permissions for the directory that contains the SSL certificate should be at least "read", "write", and "execute" for the owner, and "read" and "execute" for the group and others. ScienceLogic recommends that you put the SSL certificate in a persistent directory like `/etc` on every Data Collector that requires the SSL certificate and then run `chmod 644 /etc/<ssl_cert_file>` to ensure you have the correct permissions.



5. Use default values for all other fields.
6. Click **[Save & Close]**.

Creating a SOAP/XML Credential for an SSL Certificate (Linux and Unix Users) in the Skylar One Classic User Interface

After configuring the SSH key, you must create a SOAP/XML credential with an SSL certificate if your Db2 server contains an SSL connection.

To create the SOAP/XML credential:

1. Go to the **Credential Management** page (*System>Manage>Credentials*).
2. Click the wrench icon (🔧) for the "DB2 Soap SSL with SSH Example" credential for Linux/Unix users. The **Credentials Editor** modal appears.
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 Auth User***. If you used a PEM key in the SSH credential, type the username for the same user. Otherwise, if you are inserting the database username and password in the SSH credential, leave this field blank.

- ***HTTP Auth Password***. If you used a PEM key in the SSH credential, type the password for the same user. Otherwise, if you are inserting the database username and password in the SSH credential, leave this field blank.

NOTE: If the ***HTTP Auth User*** and the ***HTTP Auth Password*** fields are blank, then the Dynamic Applications in the *IBM: Db2 PowerPack* will use the credentials provided in the SSH key.

- ***HTTP Headers***. Add the following headers by clicking **+Add a header**:
  - `base_db2_path:<DB2 Insallation Path>`.
    For example: *`base_db2_path:/opt/ibm/db2/v11.5`*
  - `instance:<Instance Name>:<SSL Port>`
    For example:*`instance:db2inst1:60000`*
  - `instance:<Instance Name2>:<SSL Port2>`
    For example: *`instance:db2inst2:60001`*
  - `ssh:<SSH Credential ID>`

TIP: In versions of the PowerPack prior to version 103, headers required the <DB_NAME> value. This value is no longer needed and an be deleted after you upgrade the PowerPack.

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

IMPORTANT: By default, the SOAP/XML credential deletes any white space before and after the colon (:) in the credential headers. If you want to include paths with white spaces in the credential, surround the path with double quotes after the colon. For example: `<base_db2_path:"/opt/folder/name/program files">`

NOTE: If your database port changes, you must also update the credential to reflect that change.

- ***CURL Options***.
  - SSLCERT. Type the certificate path for your SSL certificate.

NOTE: The certificate path should be a path of the Data Collectorwhere the SSL certificate is located. For example: `/tmp/certificate.cer`. The permissions for the SSL certificate file should be at least "read" and "write" for the owner, and "read" for the group and others. The permissions for the directory that contains the SSL certificate should be at least "read", "write", and "execute" for the owner, and "read" and "execute" for the group and others. ScienceLogic recommends that you put the SSL certificate in a persistent directory like `/etc` on every Data Collector that requires the SSL certificate and then run `chmod 644 /etc/<ssl_cert_file>` to ensure you have the correct permissions.

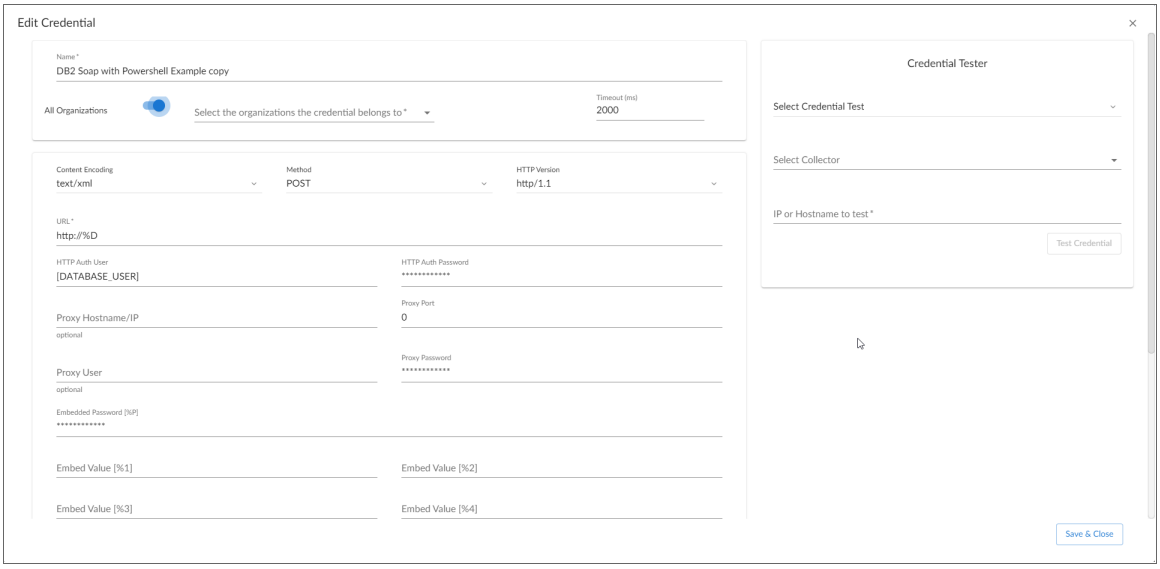
4. Use default values for all other fields.
5. Click the **[Save As]** button.

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 **Credentials** page (Manage > Credentials).
2. Locate the **DB2 Soap with PowerShell Example** credential, click its **[Actions]** icon (⋮) and select ***Duplicate***. A copy of the credential, called **DB2 Soap with PowerShell Example copy** appears.
3. Click the **[Actions]** icon (⋮) for the **DB2 Soap with PowerShell Example copy** credential and select ***Edit***. The **Edit Credential** page appears. Update the following fields:



4. Update the values in the following fields:
    - ***Name***. Type a new name for the credential.
    - ***All Organizations***. Toggle on (blue) to align the credential to all organizations, or toggle off (gray) and then select one or more specific organizations from the ***What organization manages this service?*** drop-down field to align the credential with those specific organizations.
    - ***URL***. Leave the default value of https://%D.
    - ***HTTP Auth User***. If you are inserting the database username and password in the PowerShell credential, leave this field blank.
    - ***HTTP Auth Password***. If you are inserting the database username and password in the PowerShell credential, leave this field blank.
    - ***HTTP Headers***. Add the following headers by clicking ***+ Add a header***.
        - `instance:<Instance Name>:<Port>` For example: `instance:db2inst1:50000`
        - `instance:<Instance Name2>:<Port2>` For example: `instance:db2inst2:50000`
        - `powershell:<PowerShell Credential ID>`

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

NOTE: By default, the SOAP/XML credential deletes any white space before and after the colon (:) in the credential headers. If you want to include paths with white spaces in the credential, surround the path with double quotes after the colon. For example: <base_db2_ path:"/opt/folder name/program files">

NOTE: If your database port changes, you must also update the credential to reflect that change.

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

Creating a SOAP/XML Credential (Windows Users) in the Skylar One Classic User Interface

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 the "DB2 Soap with PowerShell Example" credential for Windows users. The **Credential Editor** modal page appears.
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 Auth User***. If ou are inserting the database username and password in the PowerShell credential, leave this field blank.
   - ***HTTP Auth Password***. If you are inserting the database username and password in the PowerShell credential, leave this field blank.

   HTTP Headers

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

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

NOTE: By default, the SOAP/XML credential deletes any white space before and after the colon (:) in the credential headers. If you want to include paths with white spaces in the credential, surround the path with double quotes after the colon. For example: <base_db2_ path:"/opt/folder name/program files">

NOTE: If your database port changes, you must also update the credential to reflect that change.

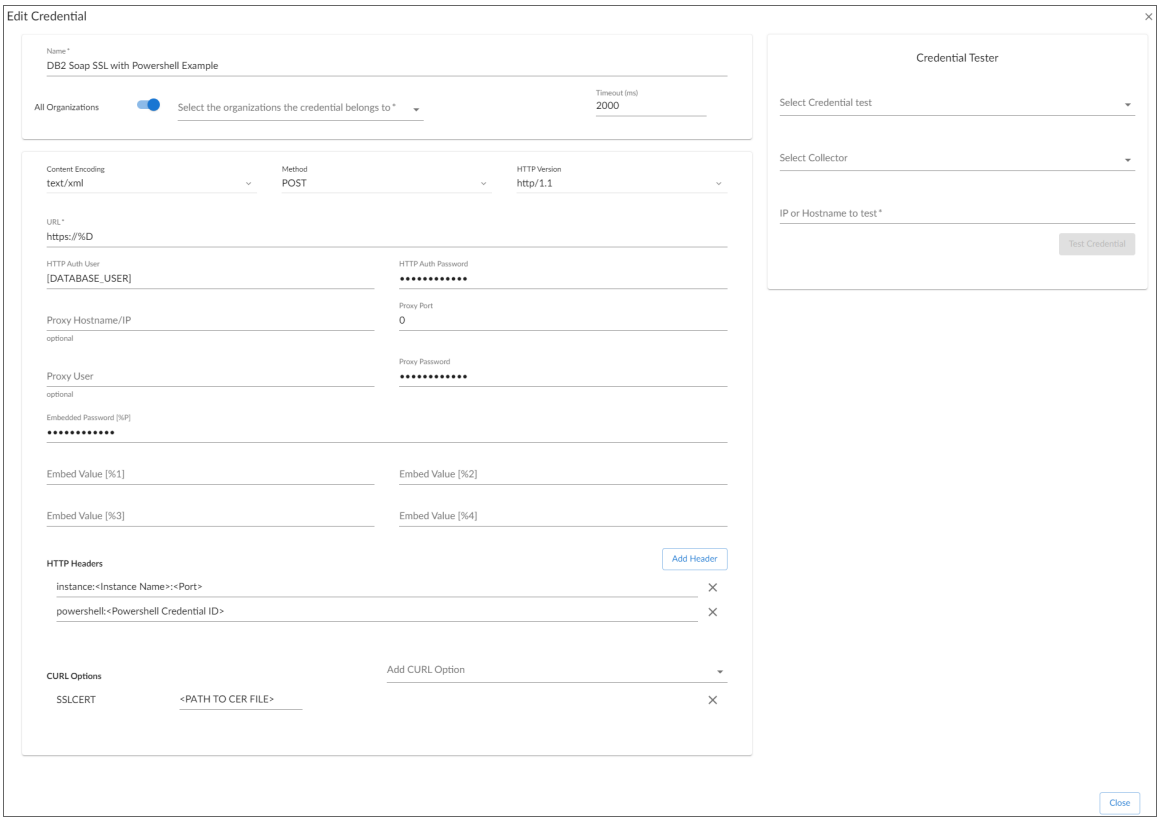
4. Click the **[Save As]** button.

Creating a SOAP/XML Credential for an SSL Certificate (Windows Users)

After configuring the PowerShell credential, you must create a SOAP/XML credential with an SSL certificate if your Db2 server contains an SSL connection.

To create the SOAP/XML credential:

1. Go to the **Credentials** page (*Manage > Credentials*).
2. Locate the **DB2 Soap SSL with PowerShell Example** credential, click its **[Actions]** icon (⋮) and select ***Duplicate***. A copy of the credential called **DB2 Soap SSL with PowerShell Example copy** appears.
3. Click the **[Actions]** icon (⋮) for the **DB2 Soap SSL with PowerShell Example copy** credential and select ***Edit***. The **Edit Credentials** page appears.



4. Update the values in the following fields:
    - ***Name***. Type a new name for the credential.
    - ***All Organizations***.Toggle on (blue) to align the credential to all organizations, or toggle off (gray) and then select one or more specific organizations from the ***What organization manages this service?*** drop-down field to align the credentials with those specific organizations.
    - ***URL***. Leave the default value of https://%D.
    - ***HTTP Auth User***. If you are inserting the database username and password in the PowerShell credential, leave this field blank.
    - ***HTTP Auth Password***. If you are inserting the database username and password in the PowerShell credential, leave this field blank.
    - ***HTTP Headers.*** Add the following headers by clicking ***+ Add a header***:
        - `instance: <Instance Name>:<Port>`
          For example:`instance:db2inst1:6000`
        - `instance:<Instance Name2>:<Port2>`
          For example: `instance:db2inst2:6000`
        - `powershell:<PowerShell Credential ID>`

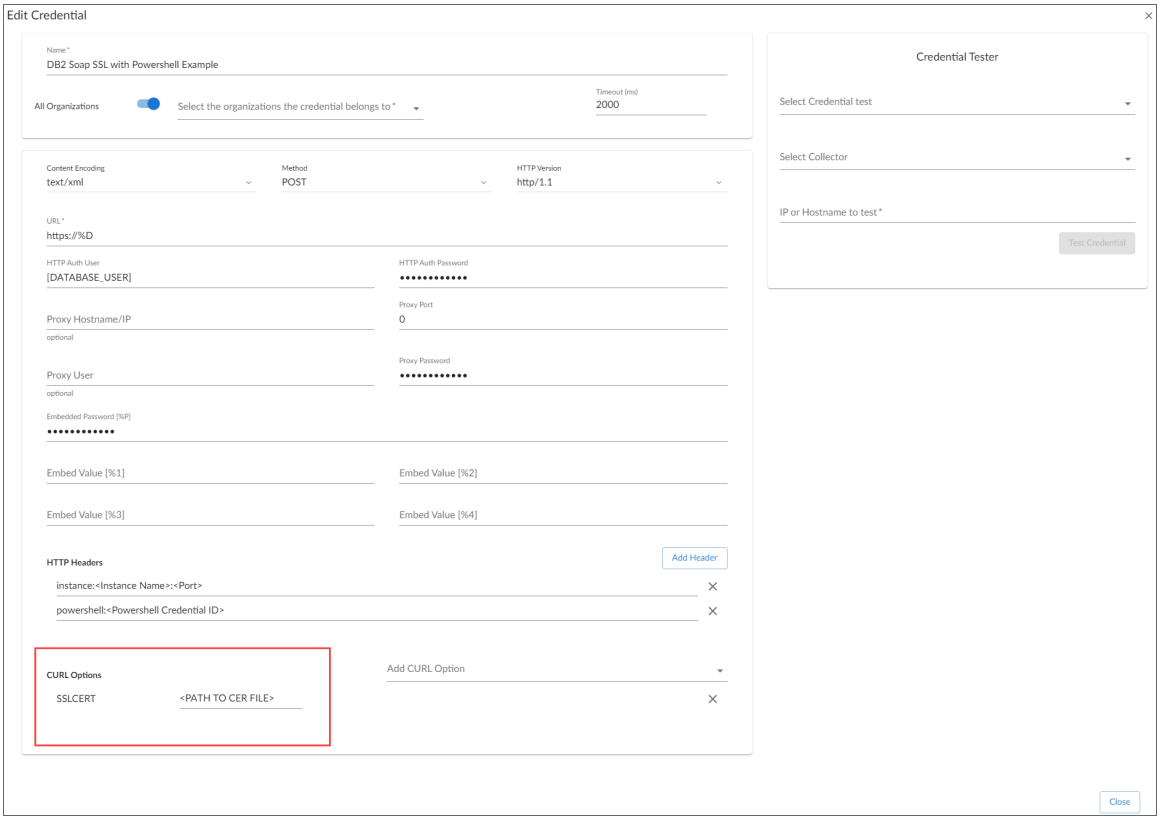
NOTE: You can create a header for each Db2 instance you have. During the discovery process, these headers will either find an existing Database credential that matches the user, password, port, and default database, or it will create a new Database credential.

IMPORTANT: By default, the SOAP/XML credential deletes any white space before and after the colon (:) in the credential headers. If you want to include paths with white spaces in the credential, surround the path with double quotes after the colon. For example: `<base_db2_path:"/opt/folder/name/program files">`

NOTE: If your database port changes, you must also update the credential to reflect that change.

- ***CURL options***: Edit the following field in this section:
    - SSLCERT. Type the certificate path for your SSL certificate.

NOTE: The certificate path should be a path of the Data Collectorwhere the SSL certificate is located. For example: `/tmp/certificate.cer`. The permissions for the SSL certificate file should be at least "read" and "write" for the owner, and "read" for the group and others. The permissions for the directory that contains the SSL certificate should be at least "read", "write", and "execute" for the owner, and "read" and "execute" for the group and others. ScienceLogic recommends that you put the SSL certificate in a persistent directory like `/etc` on every Data Collector that requires the SSL certificate and then run `chmod 644 /etc/<ssl_cert_file>` to ensure you have the correct permissions.



5. Use default values for all other fields.
6. Click **[Save & Close]**.

Creating a SOAP/XML Credential for an SSL Certificate (Windows Users) in the Skylar One Classic User Interface

After configuring the PowerShell credential, you must create a SOAP/XML credential with an SSL certificate if your Db2 server contains an SSL connection.

To create the SOAP/XML credential:

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

   Basic Settings

   - ***Profile Name***. Type a new name for the credential.
   - ***All Organizations***.Toggle on (blue) to align the credential to all organizations, or toggle off (gray) and then select one or more specific organizations from the ***What organization manages this service?*** drop-down field to align the credentials with those specific organizations.
   - ***URL***. Leave the default value of https://%D.
   - ***HTTP Auth User***. If you are inserting the database username and password in the PowerShell credential, leave this field blank.
   - ***HTTP Auth Password***. If you are inserting the database username and password in the PowerShell credential, leave this field blank.
   - ***HTTP Headers***. Add the following headers by clicking **+Add a header**:
     - `instance:<Instance Name>:<SSL Port>`
       For example:*`instance:db2inst1:60000`*
     - `instance:<Instance Name2>:<SSL Port2>`
       For example: *`instance:db2inst2:60001`*
     - `powershell:<PowerShell Credential ID>`

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

IMPORTANT: By default, the SOAP/XML credential deletes any white space before and after the colon (:) in the credential headers. If you want to include paths with white spaces in the credential, surround the path with double quotes after the colon. For example: `<base_db2_path:"/opt/folder/name/program files">`

NOTE: If your database port changes, you must also update the credential to reflect that change.

- ***CURL Options***.
  - SSLCERT. Type the certificate path for your SSL certificate.

NOTE: The certificate path should be a path of the Data Collectorwhere the SSL certificate is located. For example: `/tmp/certificate.cer`. The permissions for the SSL certificate file should be at least "read" and "write" for the owner, and "read" for the group and others. The permissions for the directory that contains the SSL certificate should be at least "read", "write", and "execute" for the owner, and "read" and "execute" for the group and others. ScienceLogic recommends that you put the SSL certificate in a persistent directory like `/etc` on every Data Collector that requires the SSL certificate and then run `chmod 644 /etc/<ssl_cert_file>` to ensure you have the correct permissions.

4. Use default values for all other fields.
5. Click the **[Save As]** button.

Updating the Database Credential

If the password has changed for the account with access to the Db2 database, you must also update the corresponding Database credential in Skylar One. Otherwise, you can skip this section.

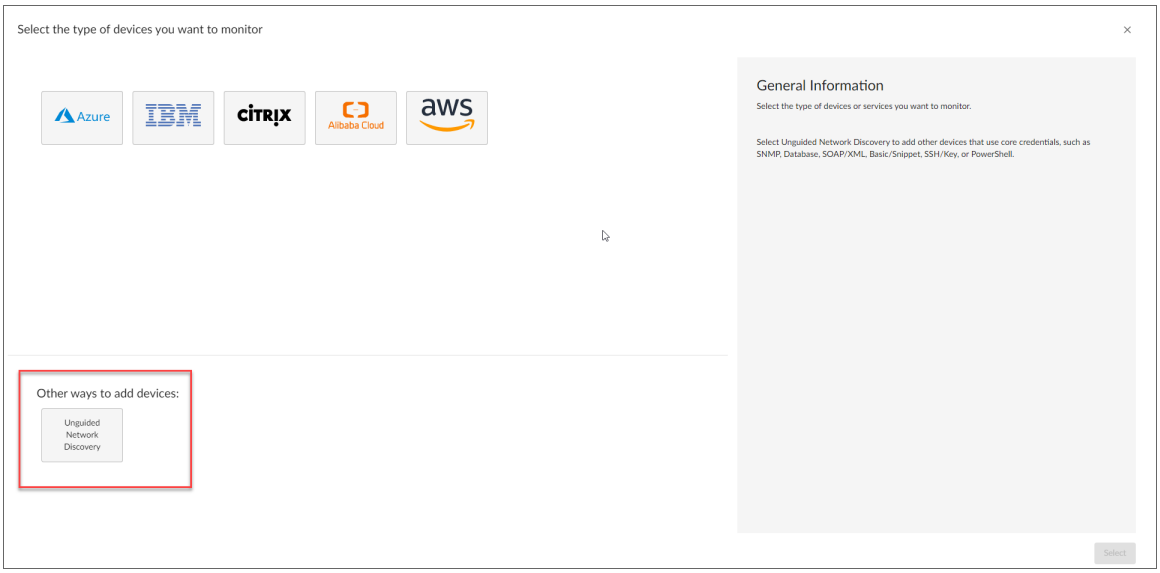
To update the Database credential:

1. Go to the **Credentials** page (Manage > Credentials).
2. Search for and locate the credential that includes the name and port of the database with the updated password, then click the credential's Actions icon (⋮) and select *Edit/Test*.
3. In the **Edit Credential** page that appears, type the new password in the ***Password*** field.
4. Click **[Save & Close]**.

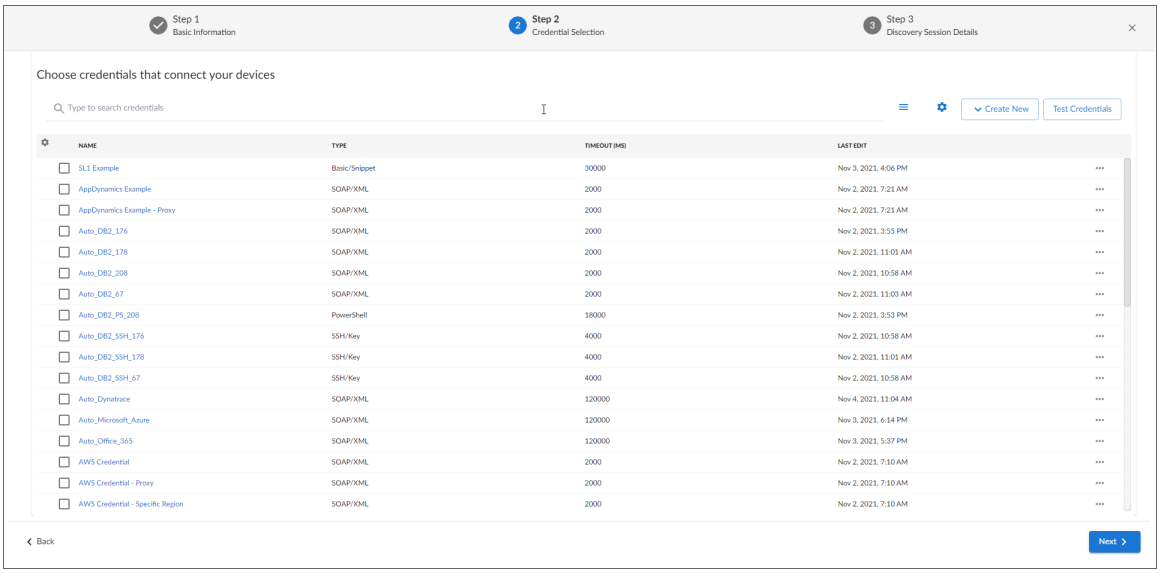
Discovering IBM Db2 Component Devices

To discover an IBM Db2 database:

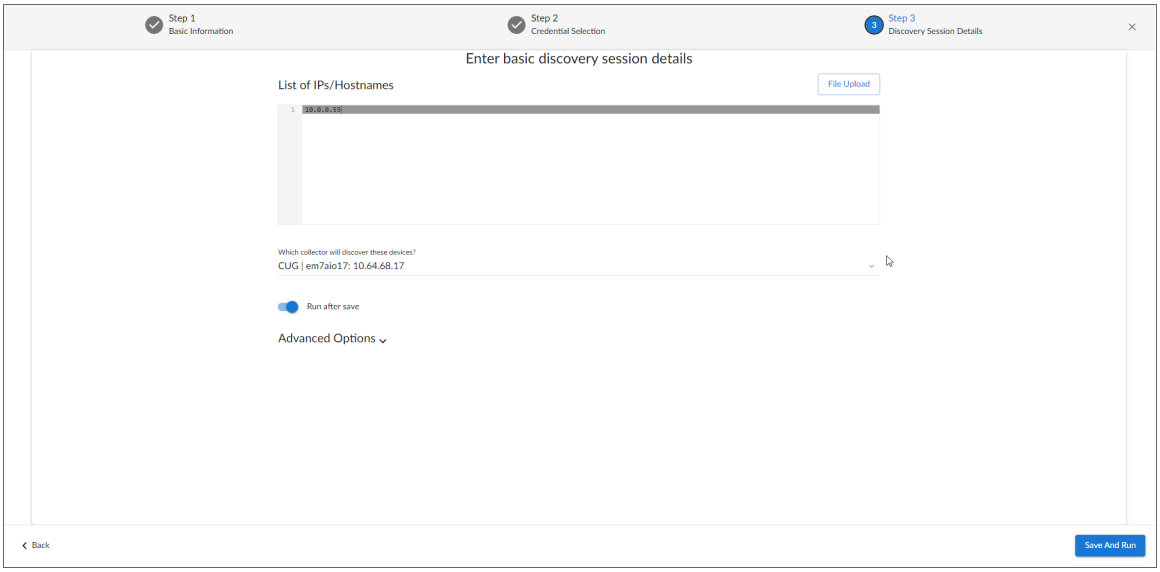
1. On the **Devices** page ( ) or the **Discovery Sessions** page (Devices > Discovery Sessions), click the **[Add Devices]** button. The **Select** page appears:



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:



6. On the **Credentials** page, locate and select the SOAP/XML *credential* you created for the Db2 database.
7. Click **[Next]**. The **Discovery Session Details** page of the **Add Devices** wizard appears:



8. Complete the following fields:
   - ***List of IPs/Hostnames***. Type the IP address of Type the IP address for the Db2 database.
   - ***Which collector will monitor these devices?***. Required. Select an existing collector to monitor the discovered devices.
   - ***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 ( ) 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 Db2 Component Devices in the Skylar One Classic User Interface

To discover an IBM Db2 database:

1. Go to the **Discovery Control Panel** page (System > Manage > Classic Discovery or System > Manage > Discovery in the classic user interface).
2. In the **Discovery Control Panel**, click the **[Create]** button. The **Discovery Session Editor** page appears.
   - ***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 Skylar One has automatically aligned the correct Dynamic Applications during discovery:

1. After the discovery session has completed, go to the **Devices** page or the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface) and find the device(s) you discovered. When you have located the device, click on its name or click

on its edit icon ( ).

2. 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:

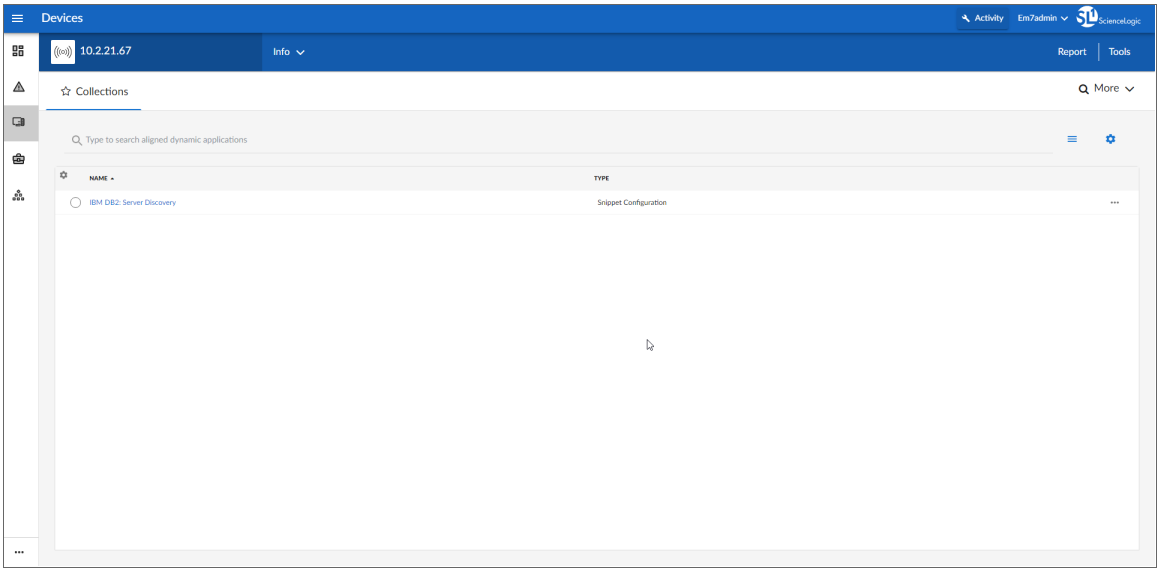
1. After discovery has completed, go to the **Discovery Logs** page (Devices > Discovery Sessions > click the Actions button ... for that session > click Show Logs) and click on the IP address of the device. If you are in the classic user interface, click the device icon for the IBM Db2 device ( ). From the **Device Investigator** page for the IBM Db2 device, or the **Device Properties** page if you are in the classic user interface, 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:

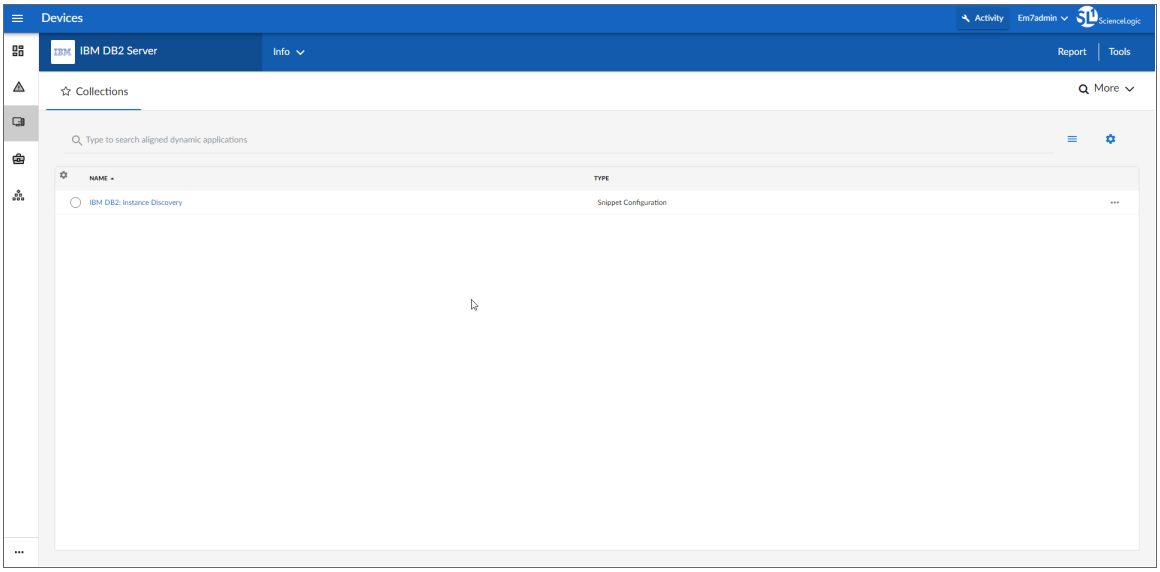
You should see the following Dynamic Application aligned to the root device:

- IBM DB2: Server Discovery



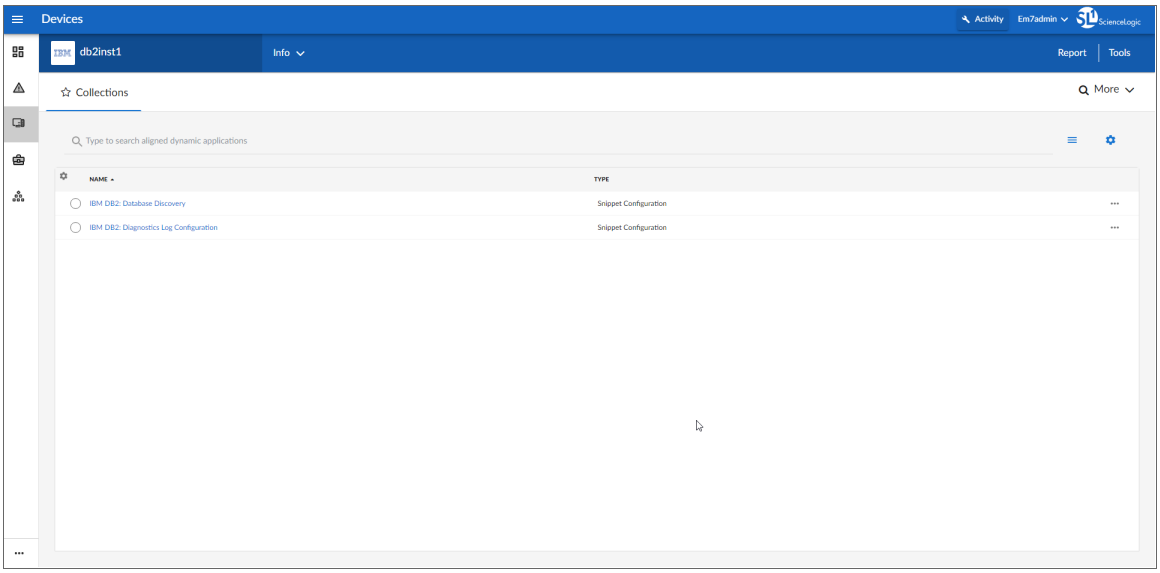
You should see the following Dynamic Application aligned to the Db2 server:

- IBM DB2: Instance Discovery



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

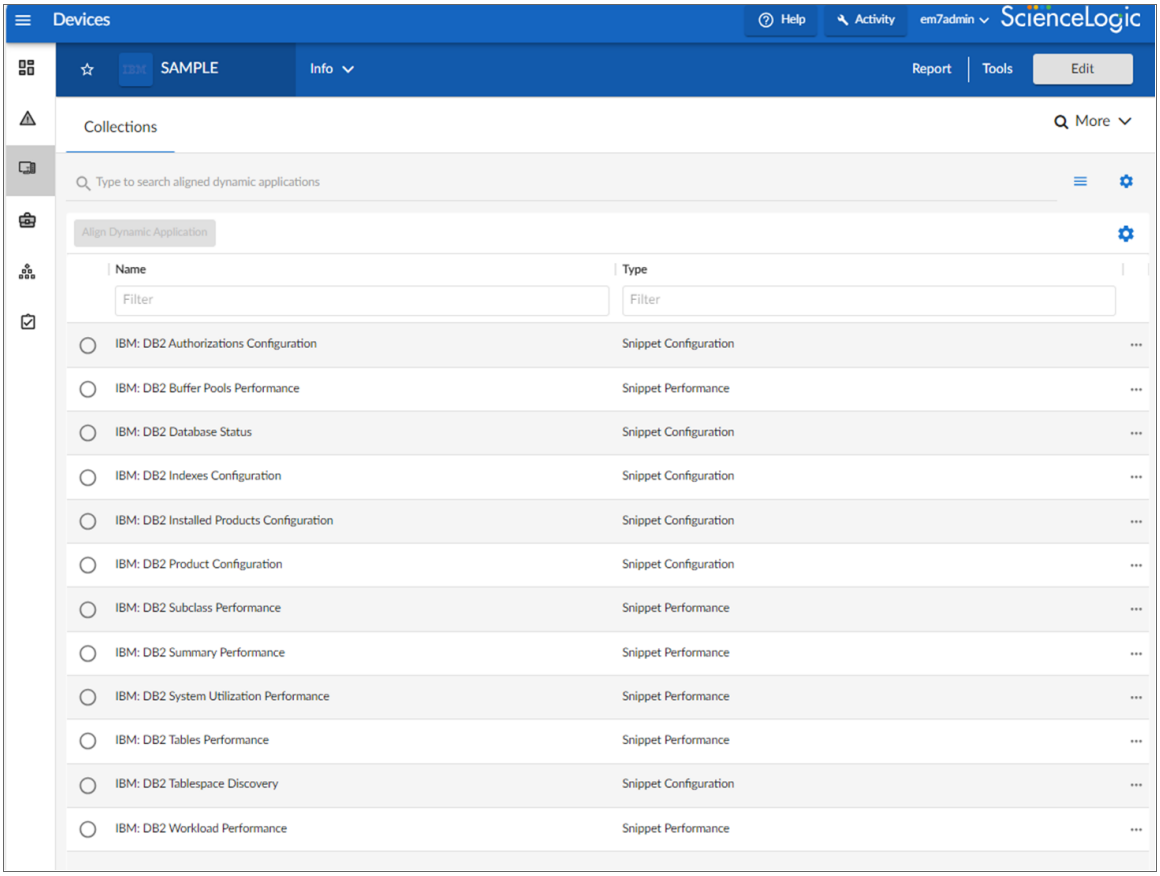
- IBM DB2: Database Discovery
- IBM DB2: Diagnostics Log Configuration



You should see some or all of the following Dynamic Applications aligned to the Db2 database:

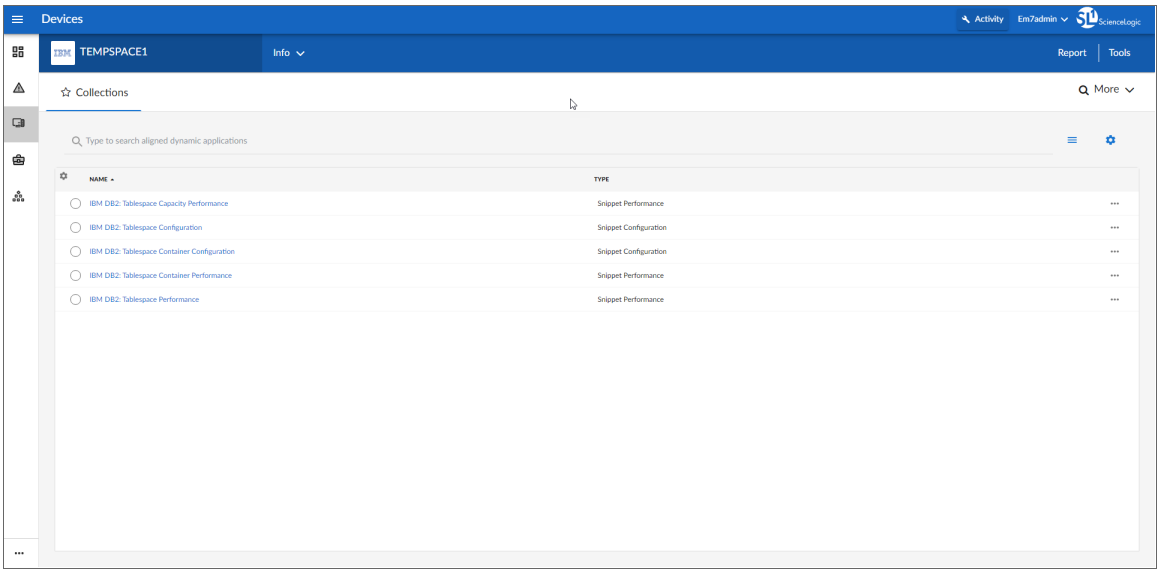
- IBM DB2: Authorizations Configuration
- IBM DB2: Buffer Pools Performance
- IBM DB2: Database Status
- IBM DB2: Indexes Configuration

- IBM DB2: Product Configuration
- IBM DB2: Subclass Performance
- IBM DB2: Summary Performance
- IBM DB2: System Utilization Performance
- IBM DB2: Tables Performance
- IBM DB2: Tablespace Discovery
- IBM DB2: Workload Performance
- IBM DB2: Installed Products Configuration



You should see the following Dynamic Applications aligned to the Db2 tablespace:

- IBM DB2: Tablespace Capacity Performance
- IBM DB2: Tablespace Configuration
- IBM DB2: Tablespace Container Configuration
- IBM DB2: Tablespace Container Performance
- IBM DB2: Tablespace Performance



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 (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface), you can view the IBM Db2 server 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 Skylar One 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 (**+**).
- 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. Skylar One 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 ***Maps*** manual.

Chapter 3

IBM Db2 Dashboards in the Skylar One Classic User Interface

Overview

This section describes the device dashboards that are included in the "IBM: Db2" PowerPack.

This chapter covers the following topics:

Device Dashboard *41*

Device Dashboard

The *IBM: Db2* PowerPack includes device dashboards that provide summary information for Db2 databases and tablespaces.

IBM Db2: Database

The IBM Db2: Database 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 (%)

IBM: DB2 Tablespace

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

- Three gauges that display the following metrics:
    - Hit Ratio
    - Size Utilization
    - Pages Utilization
- A line graph that displays the following information:

    - Total Pages (Count)
    - Usable Size (KB)
    - Total Size (KB)
    - Used Size (KB)
    - Free Size (KB)
- A line graph that displays the following information:
    - Direct Reads (Count)
    - Direct Writes (Count)
    - Logical Reads (Count)
- A line graph that displays the following information:
    - Direct Write Time (ms)
    - Direct Read Time (ms)
    - Pool Write Time (ms)
    - Pool Read Time (ms)

© 2003 - 2026, ScienceLogic, Inc.

All rights reserved.

ScienceLogic™, the ScienceLogic logo, and ScienceLogic's product and service names are trademarks or service marks of ScienceLogic, Inc. and its affiliates. Use of ScienceLogic's trademarks or service marks without permission is prohibited.

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 herein, the information provided in this document 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 herein at any time without notice.

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

International: +1-703-354-1010