Monitoring IBM Db2

IBM: Db2 PowerPack version 103

Table of Contents

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:

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: Db2PowerPack 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

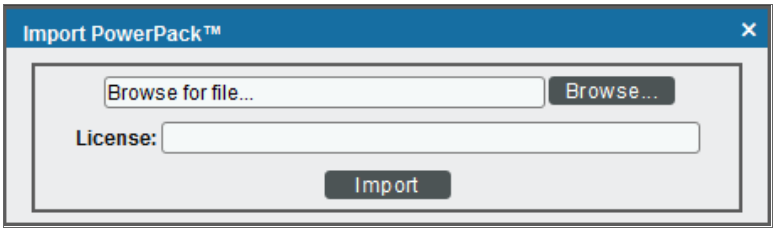
Installing the IBM: Db2 PowerPack

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 Support Site.
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*.

Chapter 2

Configuring IBM Db2 Monitoring

Overview

Use the following menu options to navigate the SL1 user interface:

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

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

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>
   ```

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>"
   ```

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 4 - 7 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, 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-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: 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*

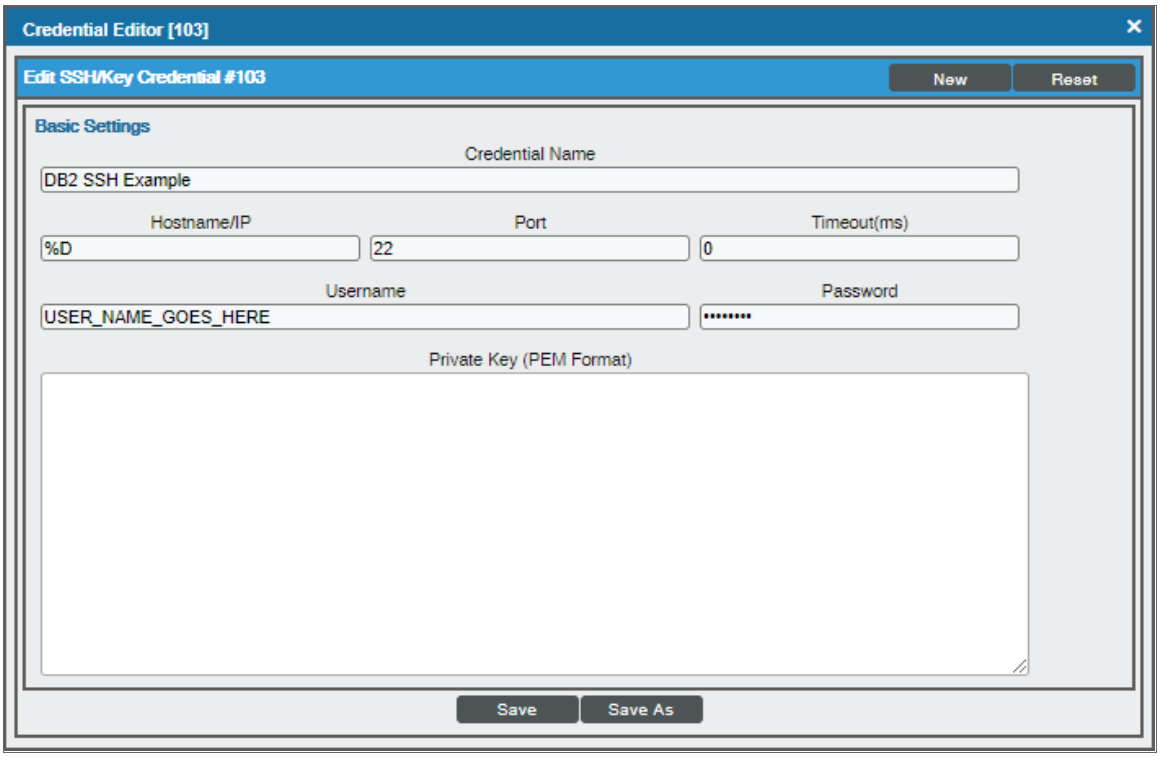
In addition, if the password has changed for the account with access to the Db2 database, you will need to update the corresponding *Database credential*.

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:



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: If your SSH access to the Db2 database allows you to only use a PEM key and prevents you from using a username and password, enter a PEM key in the SSH/Key credential and then include a username and password in the SOAP/XML credential instead.

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

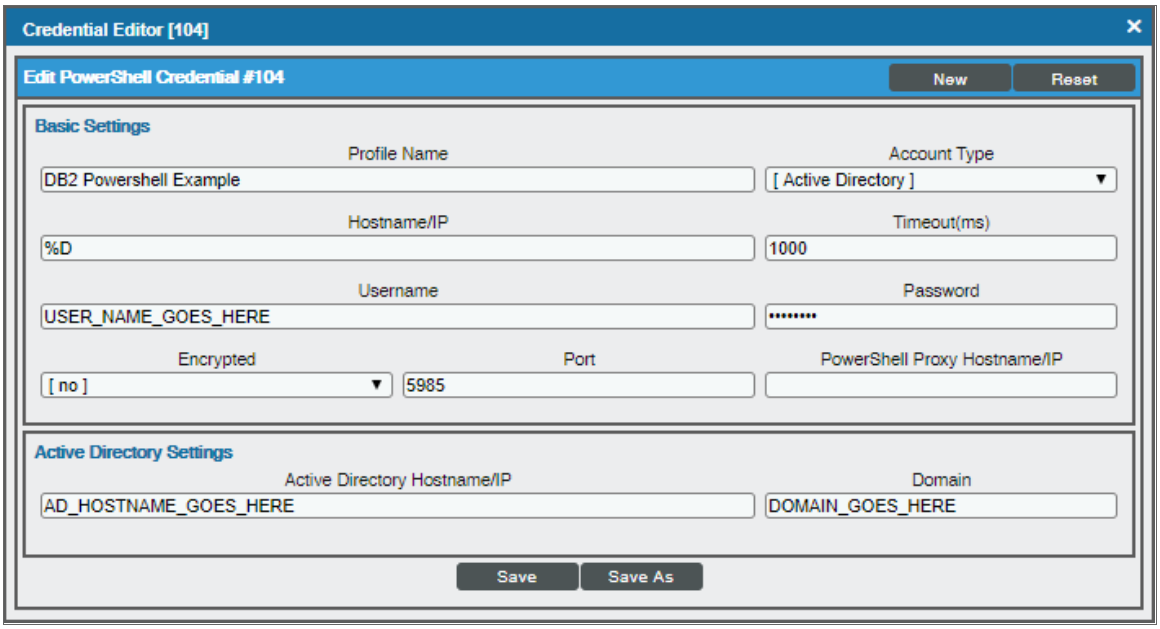
NOTE: The credential ID will appear at the top of the window after it has been saved. Take note of the ID as you will need it when creating the SOAP/XML credential.

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:



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.

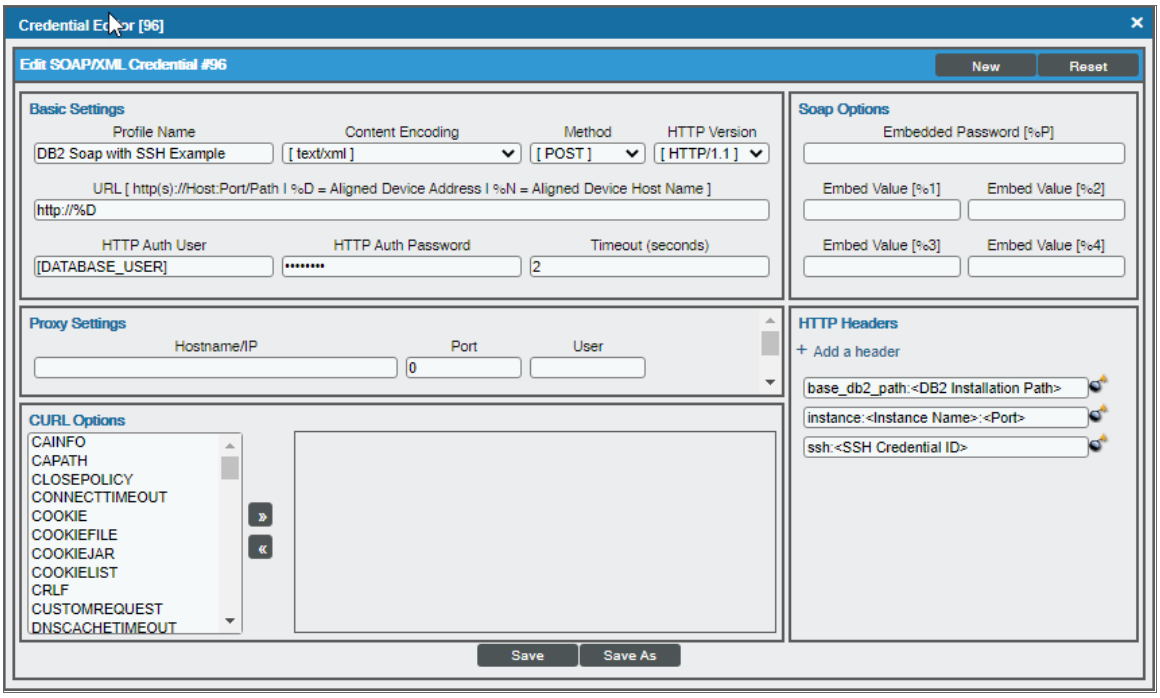
Creating a SOAP/XML Credential (Linux and Unix Users)

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).

2. Click the wrench icon ( ) for the "DB2 Soap with SSH Example" credential for Linux/Unix 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 your SSH access to the Db2 database allows you to only use a PEM key and prevents you from using a username and password, type the username for a user with access to the Db2 database in this field. Otherwise, if you are inserting the database username and password in the SSH/Key credential, leave this field blank.
- ***HTTP Auth Password***. If your SSH access to the Db2 database allows you to only use a PEM key and prevents you from using a username and password, type the password for the account with access to the Db2 database in this field. 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.

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.

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">

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

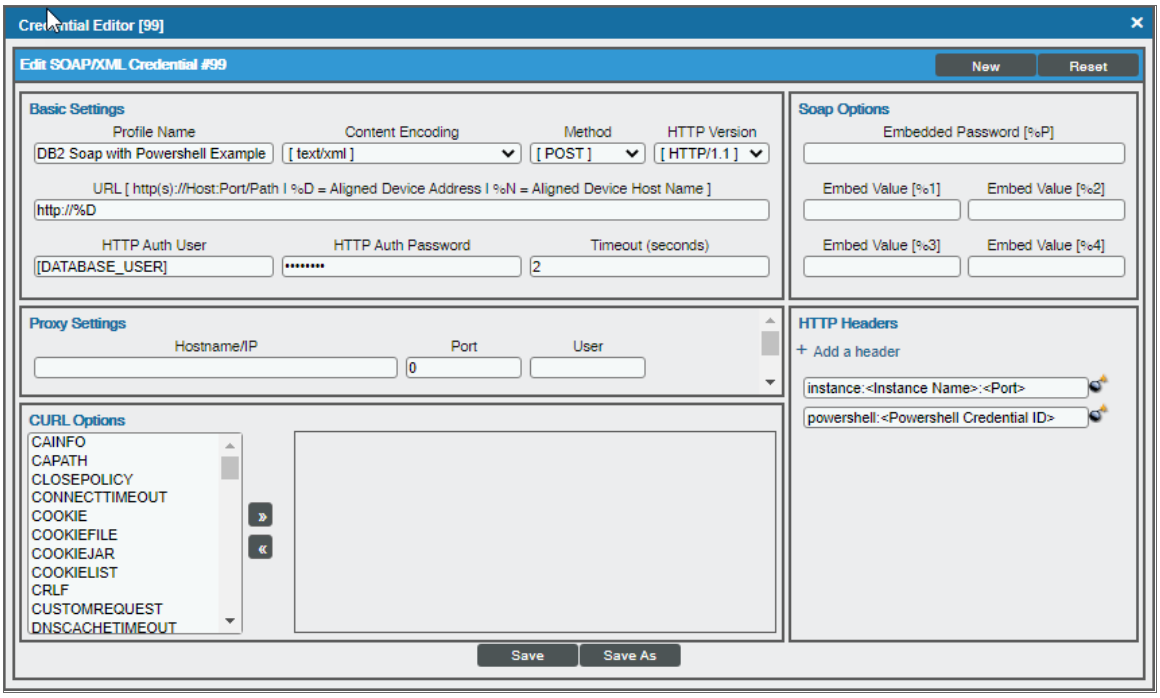
Creating a SOAP/XML Credential (Windows Users)

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 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 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.

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.

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">

4. 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 SL1. Otherwise, you can skip this section.

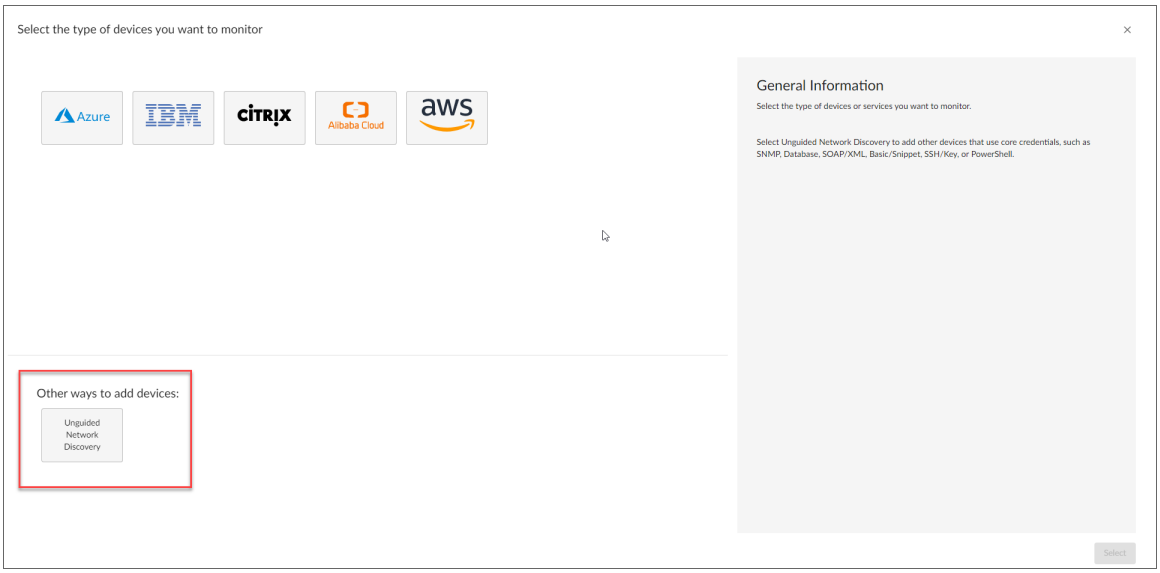
To update the Database credential:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. In the ***Type*** column filter, type "Database". This filters the list so that only Database credentials appear on the page.
3. Search for and locate the credential that includes the name and port of the database with the updated password, then click the credential's wrench icon ().
4. On the **Credential Editor** modal page that appears, type the new password in the Password field.
5. Click **[Save]**.

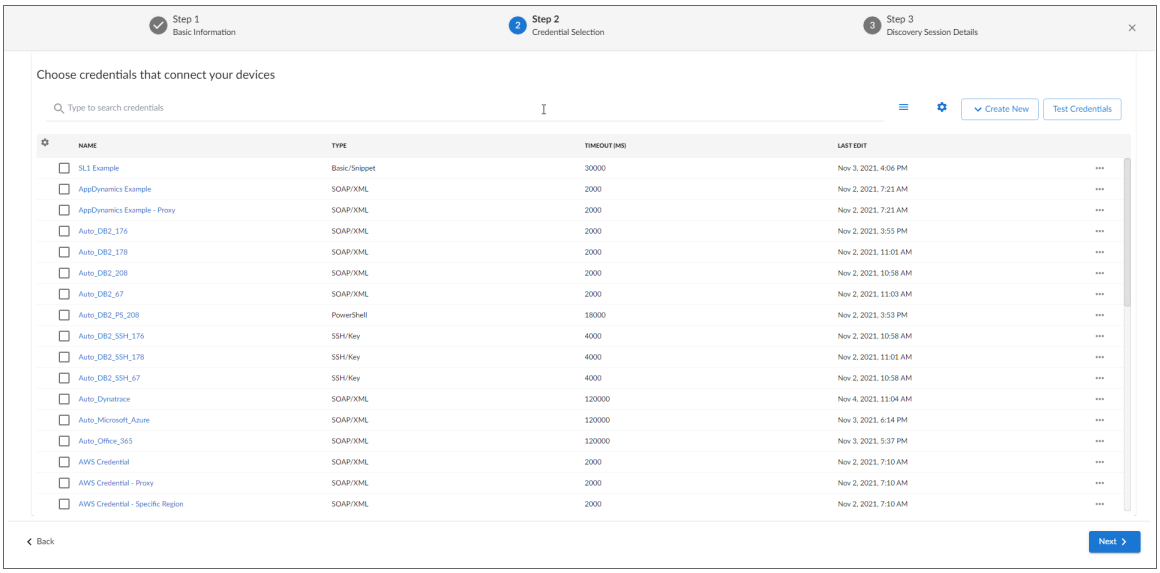
Discovering IBM Db2 Component Devices

To discover an IBM Db2 database, perform the following steps:

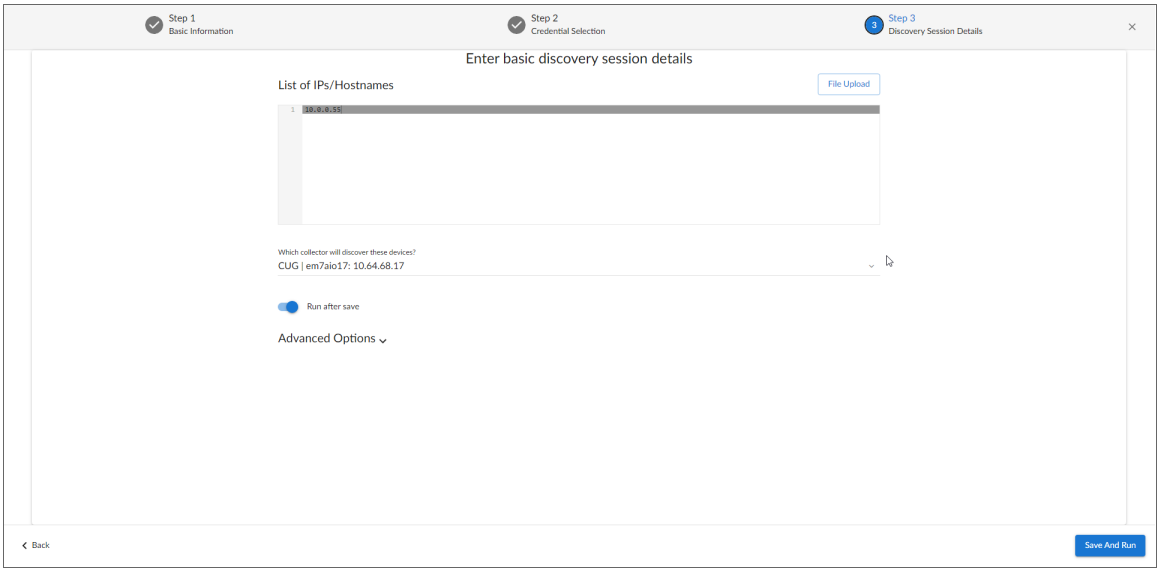
1. On the **Devices** page ( ) or the **Discovery Sessions** page (Devices > Discovery Sessions), click the **[Add Devices]** button. The **Select** page appears:



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:

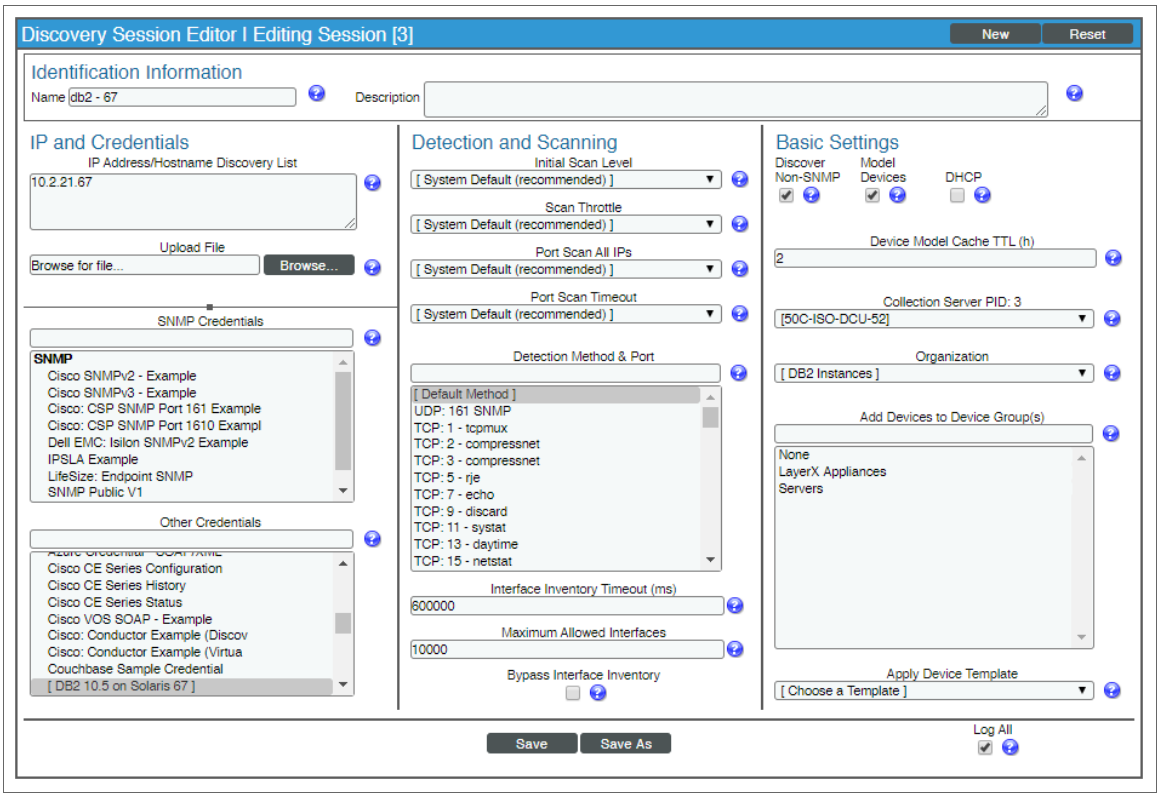
- ***Discover Non-SNMP***. Enable this setting.
- ***Model Devices***. Enable this setting.

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 SL1 Classic User Interface

To discover an IBM Db2 database:

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



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 **Devices** page—or the **Device Manager** (Registry > Devices > Device Manager) page in the SL1 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 ( ) if you are in the SL1 classic user interface.
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:

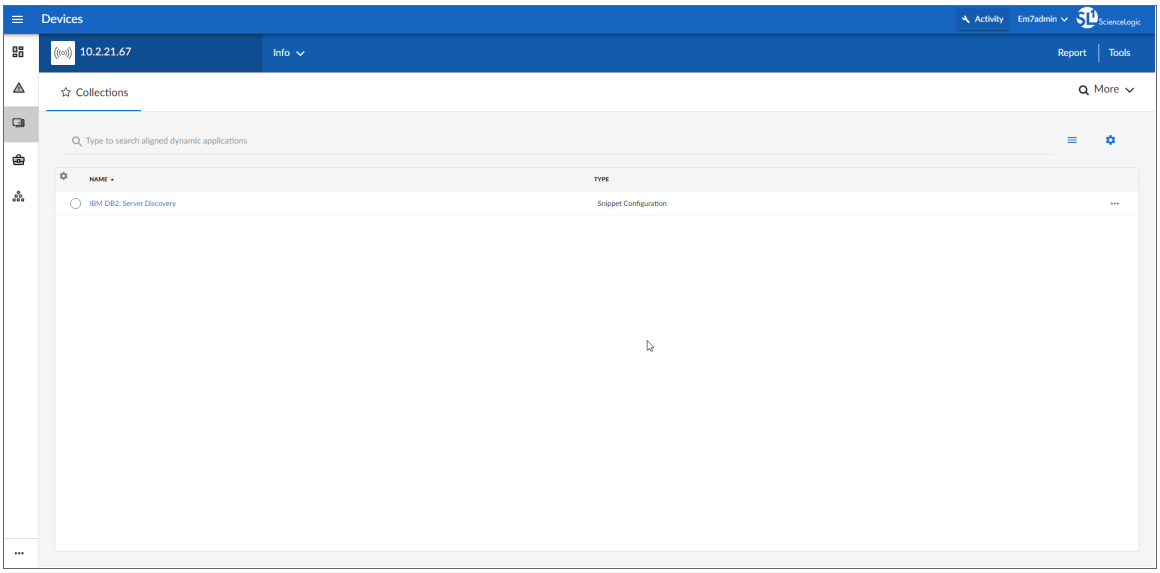
1. After discovery has completed, go to the **Discovery Logs** page (Devices > Discovery Sessions > click the Actions button ··· for that session > click Show Logs) and click on the IP address of the device. If you are in the SL1 classic user interface, click the device icon for the IBM Db2 device ( ). From the **Device Investigator** page for the IBM Db2 device, or the **Device Properties** page if you are in the SL1 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:

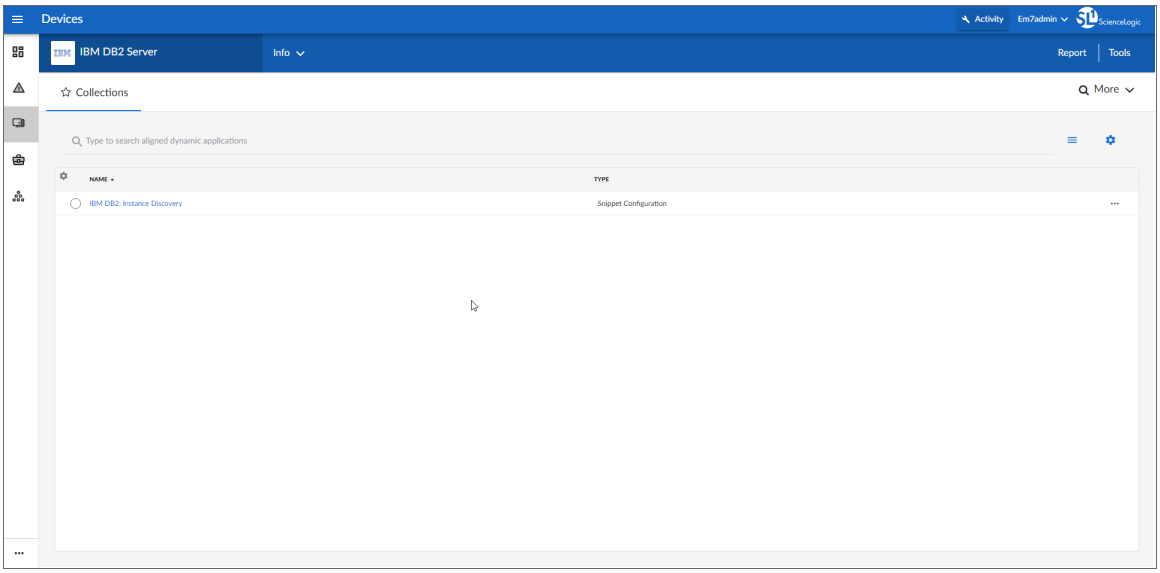
You should see the following Dynamic Application aligned to the root device:

- IBM DB2: Server Discovery



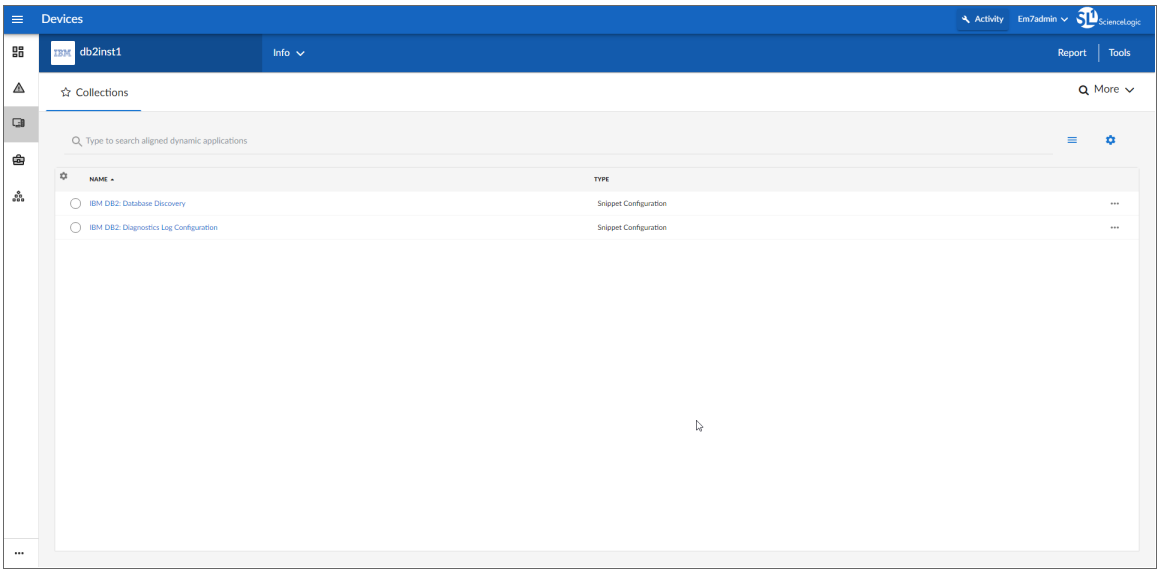
You should see the following Dynamic Application aligned to the Db2 server:

- IBM DB2: Instance Discovery



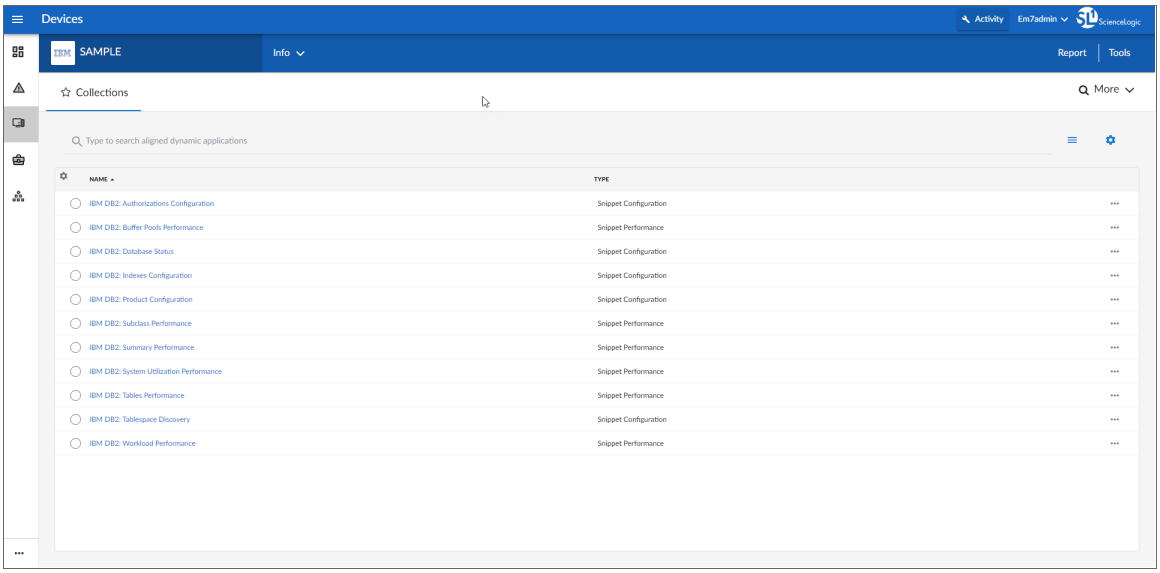
You should see the following Dynamic Application aligned to the Db2 instance:

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



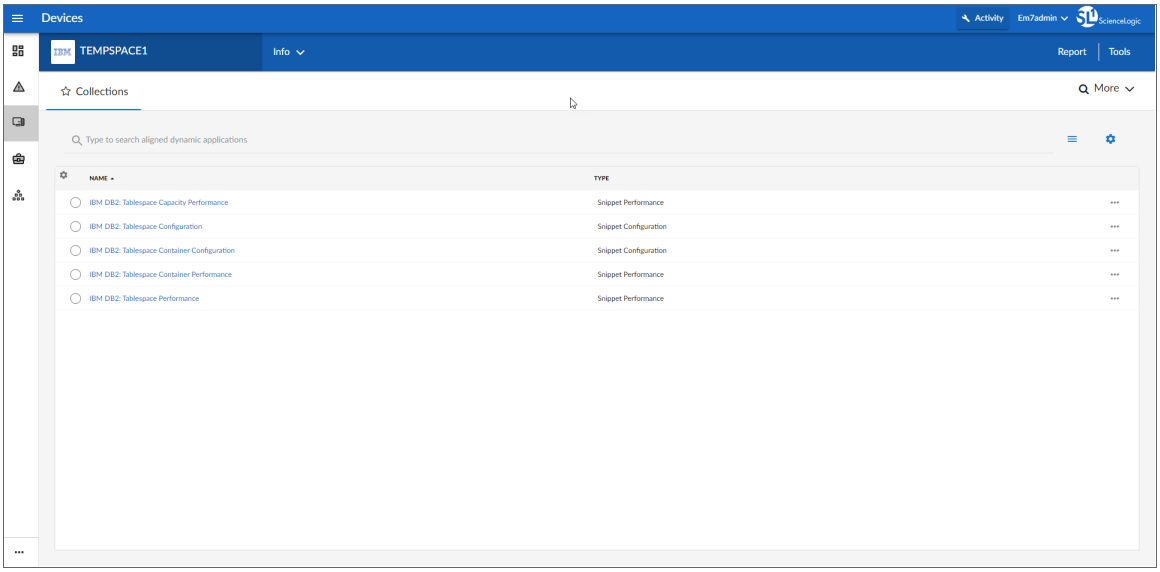
You should see some or all of the following Dynamic Applications aligned to the Db2 database:

- 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



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

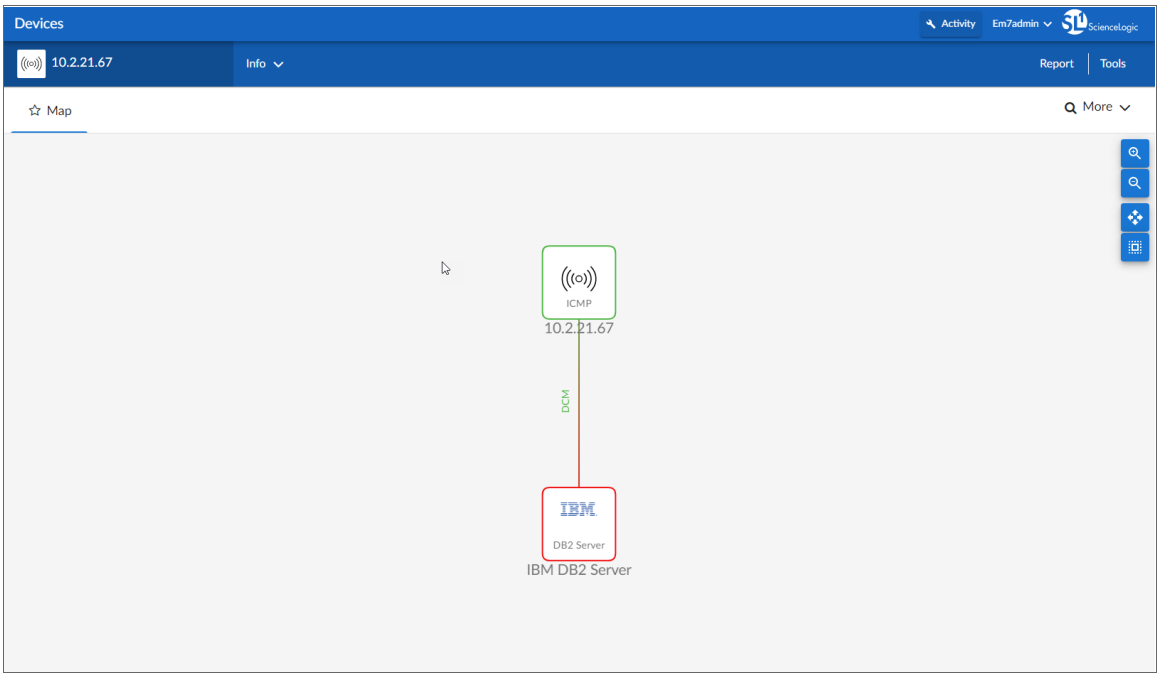


NOTE: The *IBM Db2* PowerPack uses db2ilist to discover all Db2 instances, but the Dynamic Applications will be aligned to only the instances specified in the SOAP/XML credential headers.

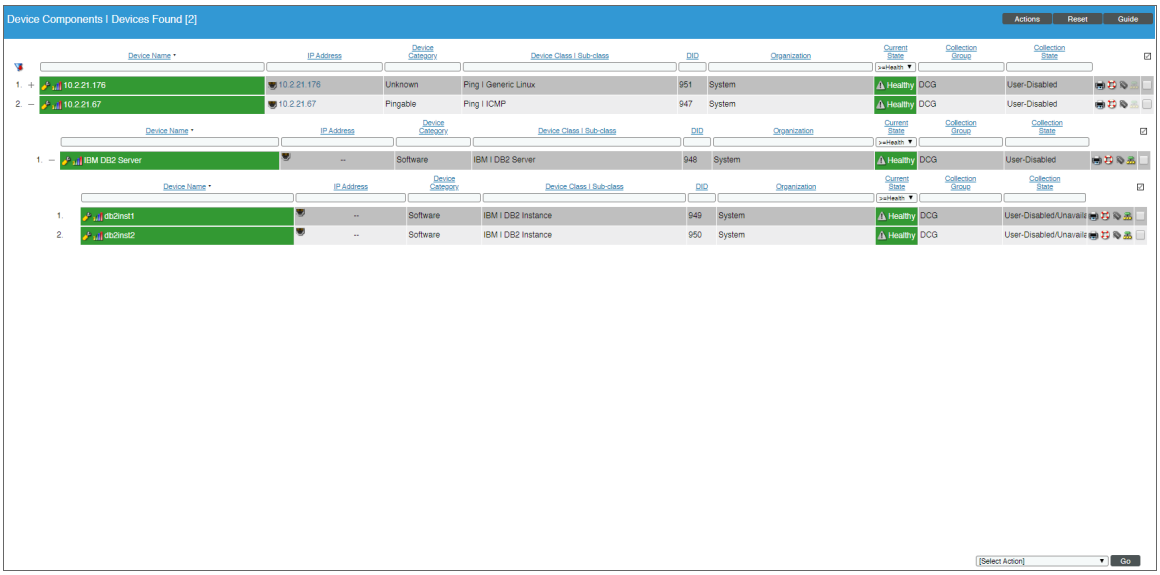
Viewing IBM Db2 Component Devices

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

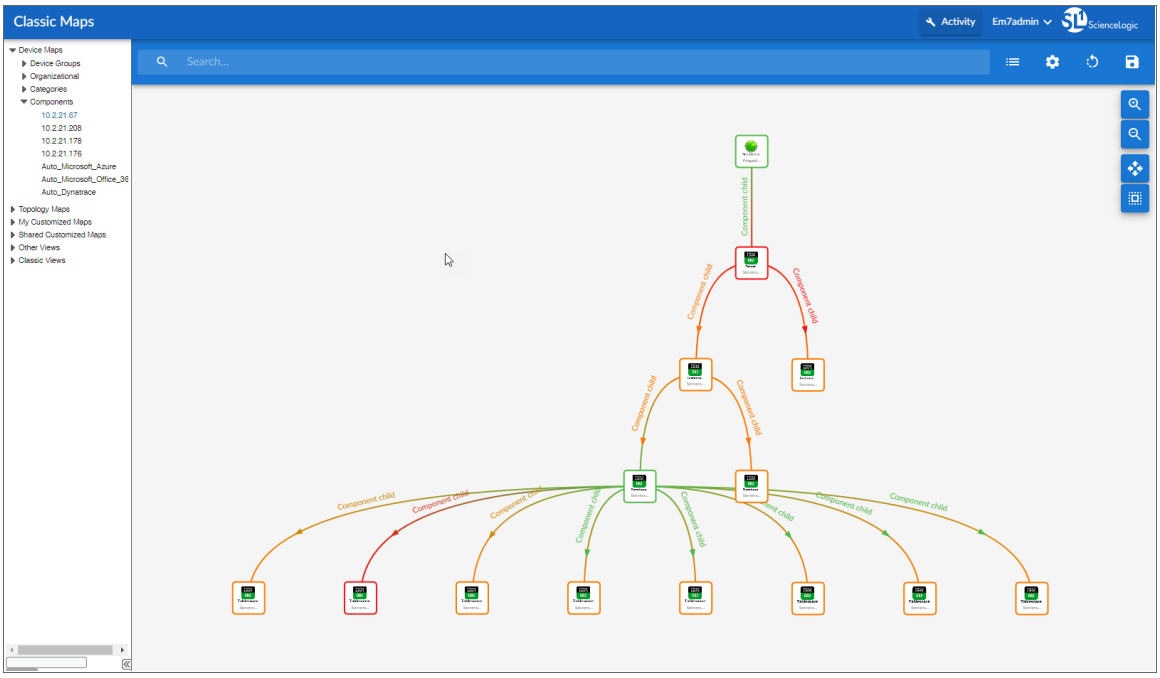
- The **Device Investigator** Map page (click **Map** in the **Device Investigator** page) displays a map of a particular device and all of the devices with which it has parent-child relationships. Double-clicking any of the listed devices reloads the page to make the selected device the primary device:



- The **Device Components** page (Devices > Device Components) displays a list of all root devices and component devices discovered by SL1 in an indented view, so you can easily view the hierarchy and relationships between child devices, parent devices, and root devices. To view the component devices associated with 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. 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 ***Maps*** manual.



Chapter 3

IBM Db2 Dashboards

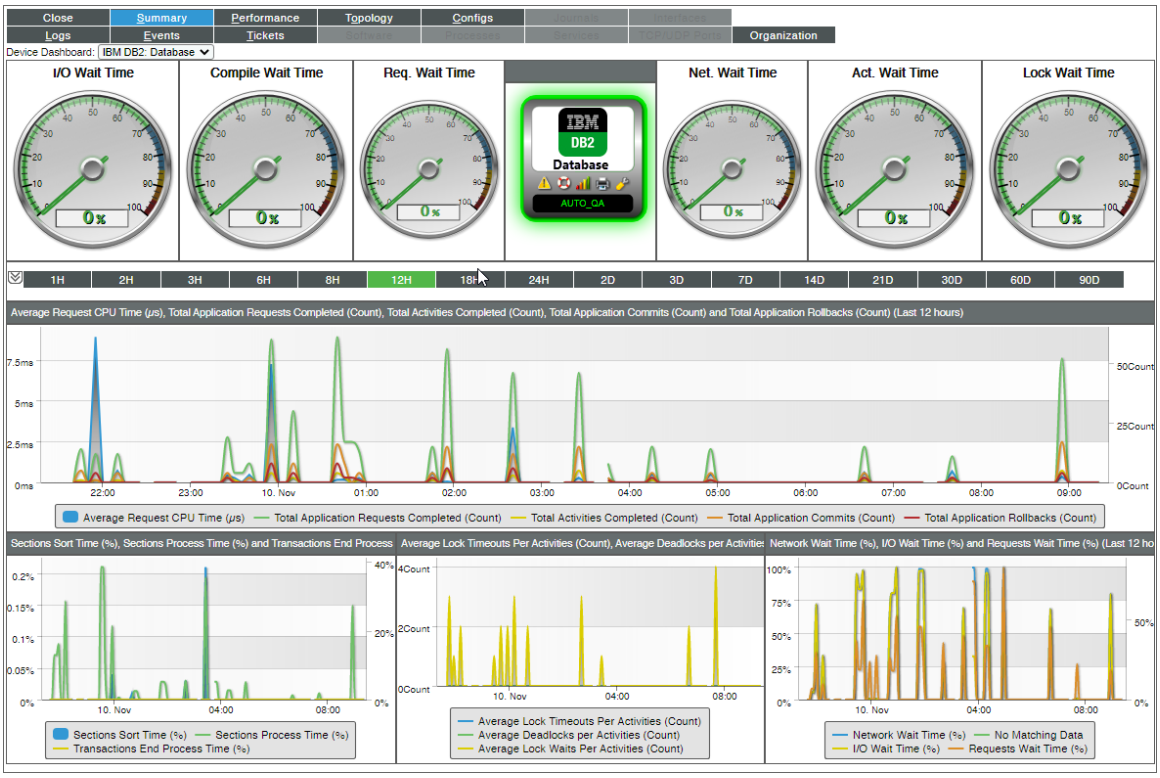
Overview

The following section describes the device dashboard that is included in the *IBM: Db2* PowerPack:

Device Dashboard

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

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 (%)

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