Monitoring NetApp Appliances

NetApp Base Pack PowerPack version 104, revision 1

Table of Contents

Chapter 1

Introduction

Overview

This manual describes how to monitor NetApp Data ONTAP environments in SL1 using the *NetApp Base Pack* PowerPack.

The following sections provide an overview of NetApp and the *NetApp Base Pack* 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 NetApp Data ONTAP?

Data ONTAP is the operating system used in NetApp storage disk arrays. It includes two operating modes:

- ***C-Mode***, for clustered environments. C-Mode enables users to bundle multiple, heterogeneous systems into a single cluster and migrate data across the entire cluster.
- ***7-Mode***, for environments with only a single storage controller or two controllers clustered together for high availability.

NOTE: NetApp discontinued support for 7-Mode as of Data ONTAP version 8.3. That version and all subsequent versions support C-Mode only.

What Does the NetApp Base Pack PowerPack Monitor?

The *NetApp Base Pack* PowerPack includes the following features:

- Dynamic Applications that discover, model, and collect data from NetApp storage devices
- Device Classes for each of the NetApp component devices monitored
- Event Policies and corresponding alerts that are triggered when NetApp component devices meet certain status criteria
- Sample Credentials for discovering NetApp component devices
- A device Dashboard that displays information about NetApp clusters

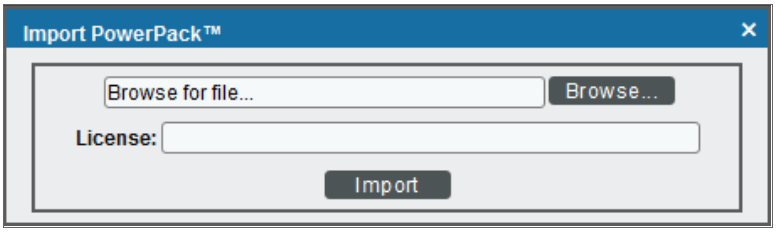
Installing the NetApp Base Pack PowerPack

Before completing the steps in this manual, you must import and install the latest version of the *NetApp Base Pack* PowerPack.

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

To download and install a PowerPack:

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



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

> **NOTE:** If you exit the **PowerPack Installer** modal page 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 page. This page appears when you click the **[Actions]** menu and select *Install PowerPack*.

Chapter 2

Discovering NetApp Devices

Overview

The following sections describe how to configure and discover NetApp appliances for monitoring in SL1 using the *NetApp Base Pack* PowerPack:

Prerequisites for Monitoring NetApp

Before you discover your NetApp appliances in your SL1 system, you must perform the following configuration tasks on each NetApp Appliance you want to discover:

- Configure a user account on the NetApp device that SL1 will use to connect to the NetApp API. The user account must be assigned a role that includes the following allowed capabilities:
    - login-http-admin

- api-system-get-*
- api-aggr-list-info
- api-lun-list-info
- api-volume-list-info
- api-perf-object-get-instances
- api-storage-shelf-environment-list-info
- api-net-config-get-active
- api-vfiler-list-info
- api-disk-list-info
- api-snapshot-list-info

NOTE: For Clustered Data ONTAP 8.3 or later, the documentation for customizing the role of a user account is located in the *Clustered Data ONTAP 8.3 System Administration Guide for Cluster Administrators* in the section titled "Customizing an access-control role to restrict user access to specific commands". To view the guide, go to https://library.netapp.com/ecm/ecm_get_file/ECMP1636037. You can download additional NetApp documentation from the NetApp Support Portal at http://mysupport.netapp.com.

If you are discovering a Clustered Data ONTAP system, the user account you use for the ScienceLogic credential should be given the built-in "readonly" role and access to the "optapi" application. For example:

```
security login create [username] -application ontapi -role readonly -vserver
[clustername]
```

- Determine whether connections to the API on your NetApp device require SSL.
- If you are discovering a NetApp v8 system, you must enable the NetApp multistore license. To do this, execute the following command on your NetApp appliance:

```
options licensed_feature.multistore.enable on
```

Configuring NetApp Credentials

To use the Dynamic Applications in the *NetApp Base Pack* PowerPack, you must first define two or more NetApp credentials in SL1. These credentials allow SL1 to communicate with the NetApp appliances. The *NetApp Base Pack* PowerPack includes templates for the NetApp credentials.

The *NetApp Base Pack* PowerPack includes the following example credentials:

- ***NetApp 7-mode***. This Basic/Snippet type credential allows you to retrieve data from a NetApp 7-Mode appliance.
- ***NetApp w/SSL Option***. This SOAP/XML type credential allows you to retrieve data from a NetApp C-Mode device that uses SSL. In production, most NetApp C-Mode devices use SSL.

- ***NetApp w/SSL Option Off***. This SOAP/XML type credential allows you to retrieve data from a NetApp C-Mode device that does not use SSL.
- ***NetApp w/SSL/TLS Option***. This SOAP/XML type credential allows you to retrieve data from a NetApp C-Mode device that uses TLS.

NOTE: The user account configured for the credential must be assigned a role that includes "login-http-admin" and "api-system-get-*" as allowed capabilities.

In addition, during discovery you will use an SNMP credential to retrieve basic device data from the NetApp devices. You must determine the SNMP Community String for your NetApp devices and then decide whether you need to create a new SNMP credential or can use an existing SNMP credential.

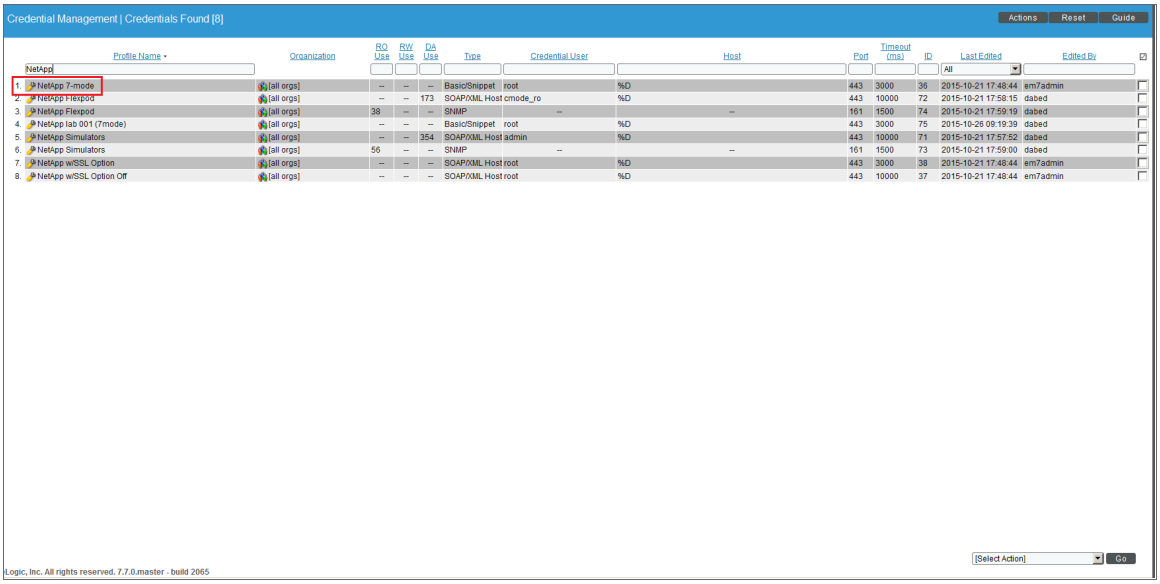
- If your NetApp devices use the same community string as other SNMP devices in your network, you can use an existing SNMP credential during discovery.
- If your NetApp devices use a different SNMP community string that the other SNMP devices in your network, you must create a new SNMP credential for the NetApp devices.

Creating a Credential for 7-Mode

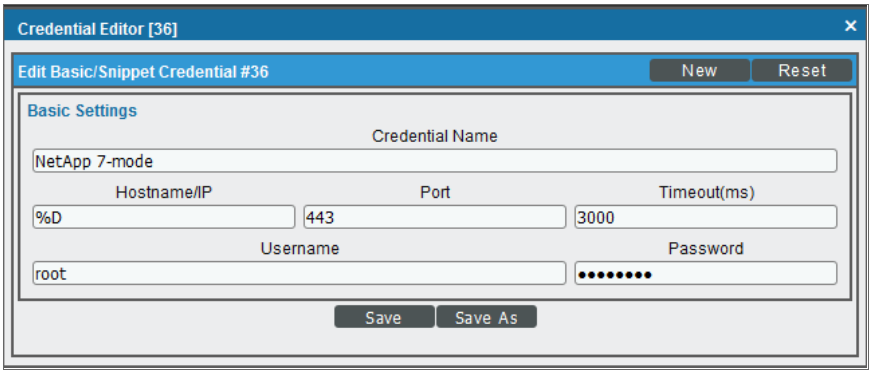
NOTE: If TLS is required for the discovery of a 7-mode NetApp system, the example credential provided will need to be replaced by a SOAP/XML credential, as described in the *Creating a Credential for C-Mode* section. In that case, the ***Embed Value [%1]*** field should be set to *True* and the TLS version should be entered in ***Embed Value [%2]***.

To modify the example credentials for use with your NetApp 7-Mode appliances, perform the following steps:

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



2. Click the wrench icon ( ) for the ***NetApp 7-mode***. The **Credential Editor** modal window appears:



3. Supply values in the following fields:

   - ***Credential Name***. Enter a new name for the credential.
   - ***Username***. Enter the username that SL1 will use to connect to the NetApp appliance.
   - ***Password***. Enter the password for the username you entered in the ***HTTP Auth User*** field.

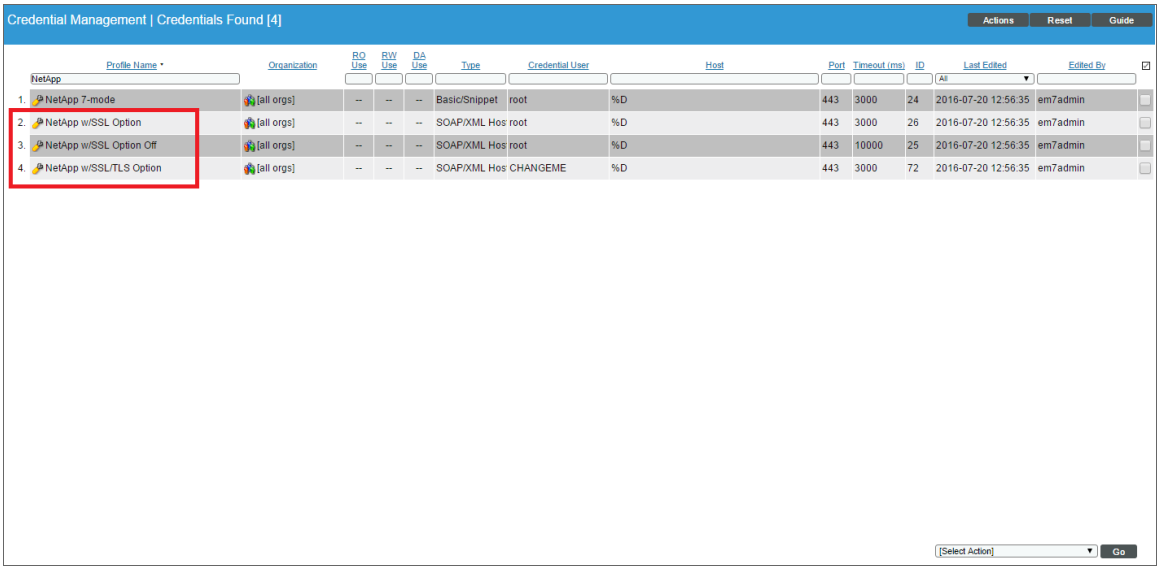
NOTE: The user account configured for the credential must be assigned a role that includes "login-http-admin" and "api-system-get-*" as allowed capabilities.

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

Creating a Credential for C-Mode

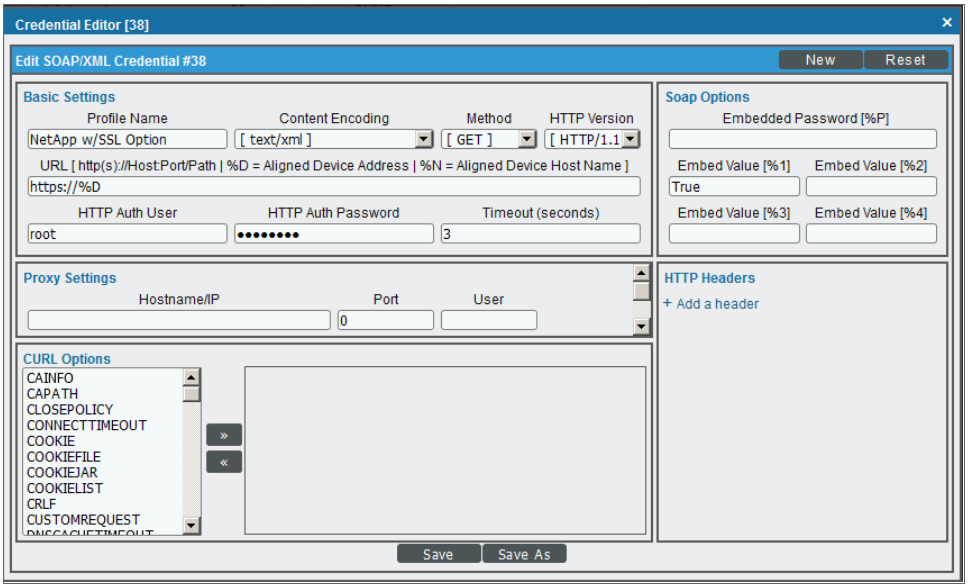
To modify the example credentials for use with your NetApp C-Mode appliances, perform the following steps:

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



   - If you want SL1 to use SSL when connecting to the NetApp device, click the wrench icon () for the ***NetApp w/SSL Option*** credential.
   - If you do not want SL1 to use SSL or TLS when connecting to the NetApp device, click the wrench icon () for the ***NetApp w/SSL Option Off*** credential.
   - If you want SL1 to use TLS when connecting to the NetApp device, click the wrench icon () for the ***NetApp w/SSL/TLS Option*** credential.

The **Credential Editor** modal window appears:



3. Supply values in the following fields:

   - ***Profile Name***. Type a new name for the credential.
   - ***URL***. Use the provided value of "https://%D".
   - ***HTTP Auth User***. Type the username that SL1 will use to connect to the NetApp appliance.
   - ***HTTP Auth Password***. Type the password for the username you entered in the ***HTTP Auth User*** field.
   - ***Embed Value [%1]***. Type "True" if you want SL1 to use SSL or TLS when connecting to the NetApp device, or if you are discovering a 7-mode NetApp system in which TLS is required. Type "False" if you do not want SL1 to use SSL or TLS when connecting to the NetApp device.
   - ***Embed Value [%2]***. Type one of the following, depending on the version of TLS you use, if you want SL1 to use TLS when connecting to the NetApp device: "TLSv1.0", "TLSv1.1", or "TLSv1.2". Otherwise, keep this field blank.
   - ***Port***. If SL1 is running in FIPS-compliant mode, set the port to 80.

NOTE: The user account configured for the credential must be assigned a role that includes "login-http-admin" and "api-system-get-*" as allowed capabilities.

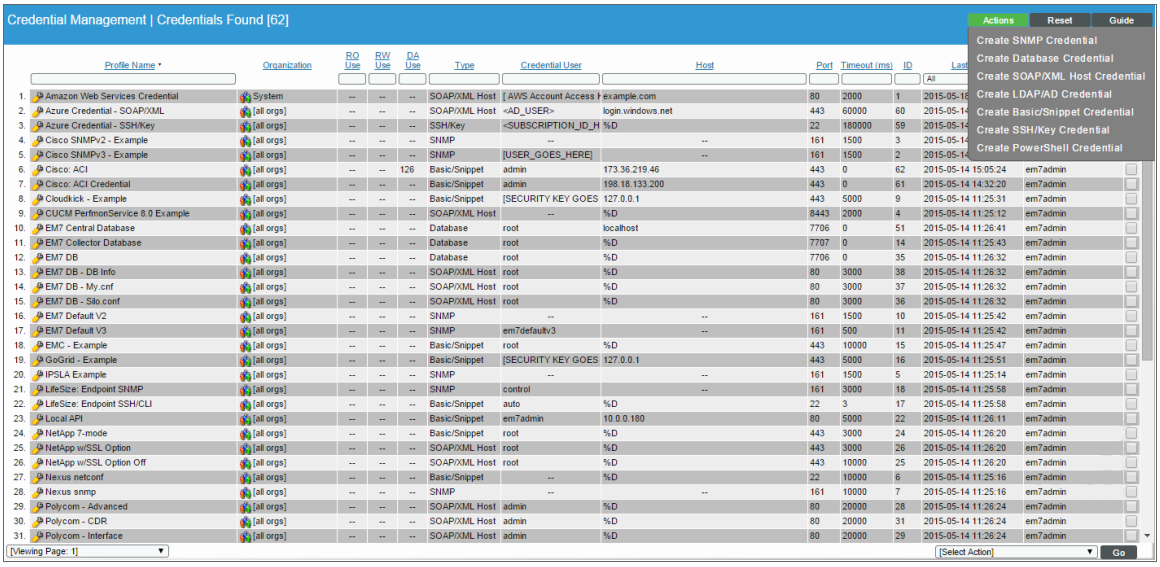
4. Click the **[Save As]** button.

Creating an SNMP Credential

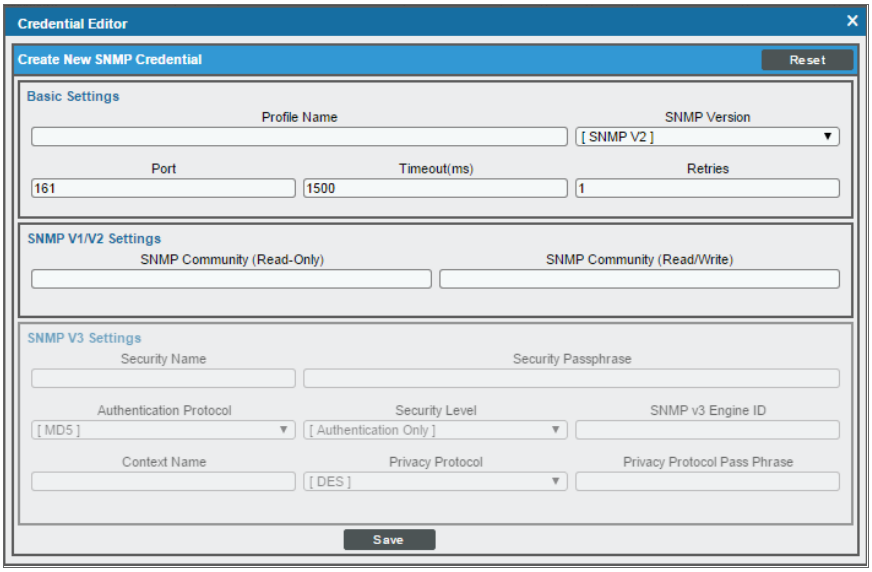
SNMP Credentials (called "community strings" in earlier versions of SNMP) allow SL1 to access SNMP data on a managed device. SL1 uses SNMP credentials to perform discovery, run auto-discovery, and gather information from SNMP Dynamic Applications.

To create an SNMP credential:

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



2. Click the **[Actions]** button and select *Create SNMP Credential*. The **Credential Editor** page appears.



3. Supply values in the following fields:
    - ***Profile Name***. Name of the credential. Can be any combination of alphanumeric characters. This field is required.
    - ***SNMP Version***. SNMP version. Choices are *SNMP V1*, *SNMP V2*, and *SNMP V3*. The default value is *SNMP V2*. This field is required.
    - ***Port***. The port SL1 will use to communicate with the external device or application. The default value is *161*. This field is required.
    - ***Timeout (ms)***. Time, in milliseconds, after which SL1 will stop trying to communicate with the SNMP device. The default value is *1500*. This field is required.
    - ***Retries***. Number of times SL1 will try to authenticate and communicate with the external device. The default value is *1*. This field is required.

    SNMP V1/V2 Settings

    These fields appear if you selected *SNMP V1* or *SNMP V2* in the ***SNMP Version*** field. Otherwise, these fields are grayed out.

    - ***SNMP Community (Read Only)***. The SNMP community string (password) required for read-only access of SNMP data on the remote device or application. For SNMP V1 and SNMP V2 credentials, you must supply a community string, either in this field or in the ***SNMP Community (Read/Write)*** field.
    - ***SNMP Community (Read/Write)***. The SNMP community string (password) required for read and write access of SNMP data on the remote device or application. For SNMP V1 and SNMP V2 credentials, you must supply a community string, either in this field or in the ***SNMP Community (Read Only)*** field.

    SNMP V3 Settings

    These fields appear if you selected *SNMP V3* in the ***SNMP Version*** field. Otherwise, these fields are grayed out.

    - ***Security Name***. Name for SNMP authentication. This field is required.
    - ***Security Passphrase***. Password to authenticate the credential. This value must contain at least 8 characters. This value is required if you use a ***Security Level*** that includes authentication.
    - ***Authentication Protocol***. Select an authentication algorithm for the credential. Choices are MD5 or SHA. The default value is *MD5*. This field is required.
    - ***Security Level***. Specifies the combination of security features for the credentials. This field is required. Choices are:
        - *No Authentication / No Encryption*.
        - *Authentication Only*. This is the default value.
        - *Authentication and Encryption*.
    - ***SNMP v3 Engine ID***. The unique engine ID for the SNMP agent you want to communicate with. (SNMPv3 authentication and encryption keys are generated based on the associated passwords and

the engine ID.) This field is optional.

- ***Context Name***. A context is a mechanism within SNMPv3 (and AgentX) that allows you to use parallel versions of the same MIB objects. For example, one version of a MIB might be associated with SNMP Version 2 and another version of the same MIB might be associated with SNMP Version 3. For SNMP Version 3, specify the context name in this field. This field is optional.
- ***Privacy Protocol***. The privacy service encryption and decryption algorithm. Choices are *DES* or *AES*. The default value is *DES*. This field is required.
- ***Privacy Protocol Passphrase***. Privacy password for the credential. This field is optional.

4. Click the **[Save]** button to save the new SNMP credential.
5. Repeat steps 1-4 for each SNMP-enabled device in your network that you want to monitor with SL1.

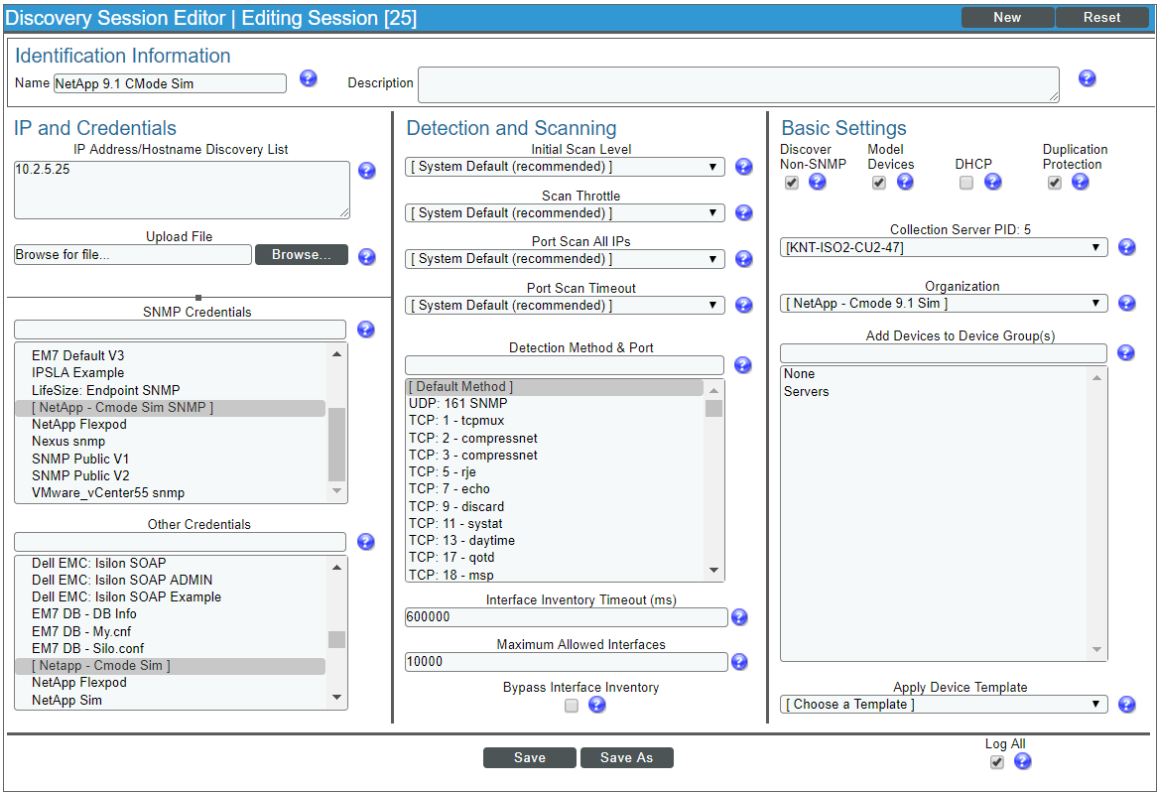
NOTE: When you define a SNMP Credential, SL1 automatically aligns the credential with all organizations of which you are a member.

Discovering a NetApp Appliance

To create and run a discovery session that will discover a NetApp appliance, perform the following steps:

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

2. Click the **[Create]** button to create a new discovery session. The **Discovery Session Editor** window appears:



3. Enter values in the following fields:

   - ***IP Address Discovery List***. Enter the IP address for the NetApp appliance. This can be the address for a single filer (in the case of 7-mode) or the IP address for a cluster (in the case of clustered Data ONTAP).
   - ***SNMP Credential***. Select an SNMP credential to use with the NetApp appliance.
   - ***Other Credentials***. Select the credential that you configured in the previous section.

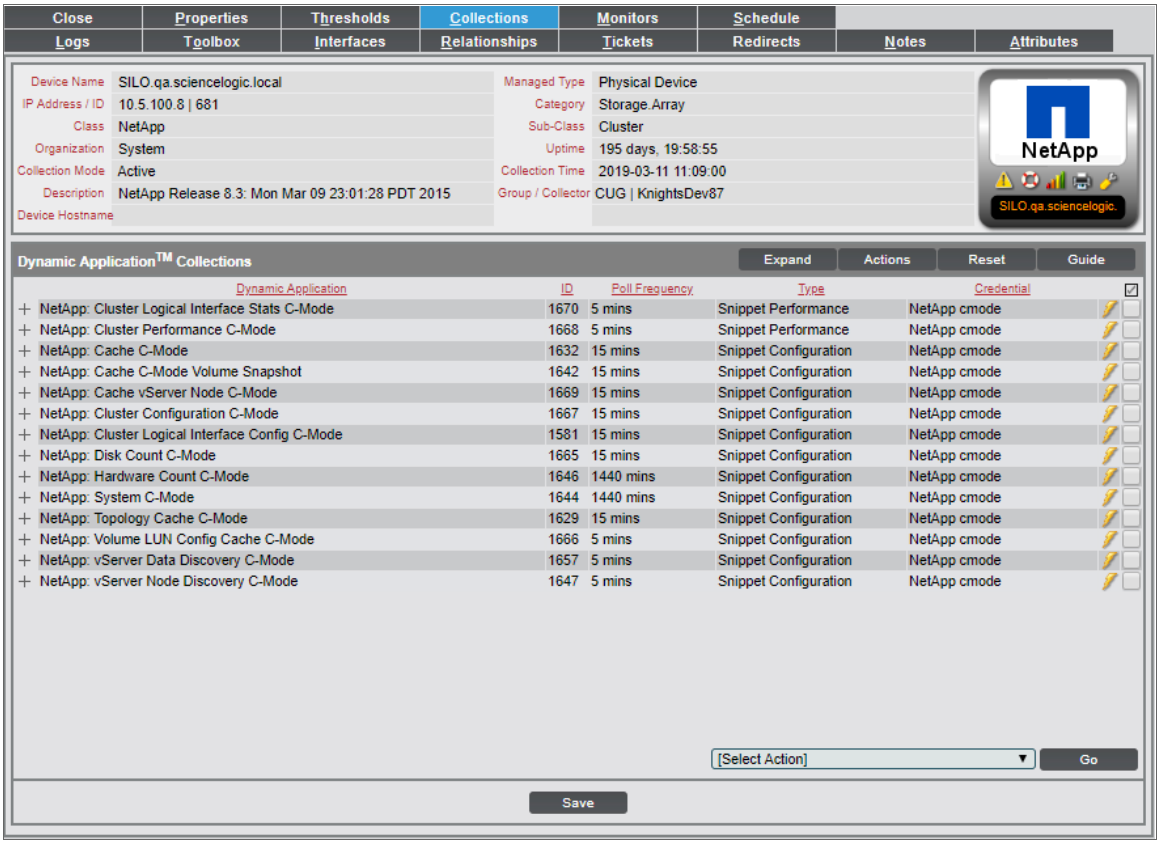
4. You can enter values in the other fields on this page, but are not required to and can simply accept the default values. For more information about the other fields on this page, see the ***Discovery & Credentials*** manual.
5. Click the **[Save]** button and then close the **Discovery Session Editor** window.
6. The discovery session you created will appear at the top of the **Discovery Control Panel** page. Click its lightning-bolt icon ( ) to run the discovery session.
7. The **Discovery Session** window will be displayed.
8. When the NetApp appliance is discovered, click its device icon ( ) to view the **Device Properties** page for the NetApp appliance.

Verifying Discovery and Dynamic Applications

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

> **NOTE:** It can take several minutes after discovery for Dynamic Applications to appear on the **Dynamic Application Collections** page. If the specified Dynamic Applications do not appear on this page, try clicking the **[Reset]** button.

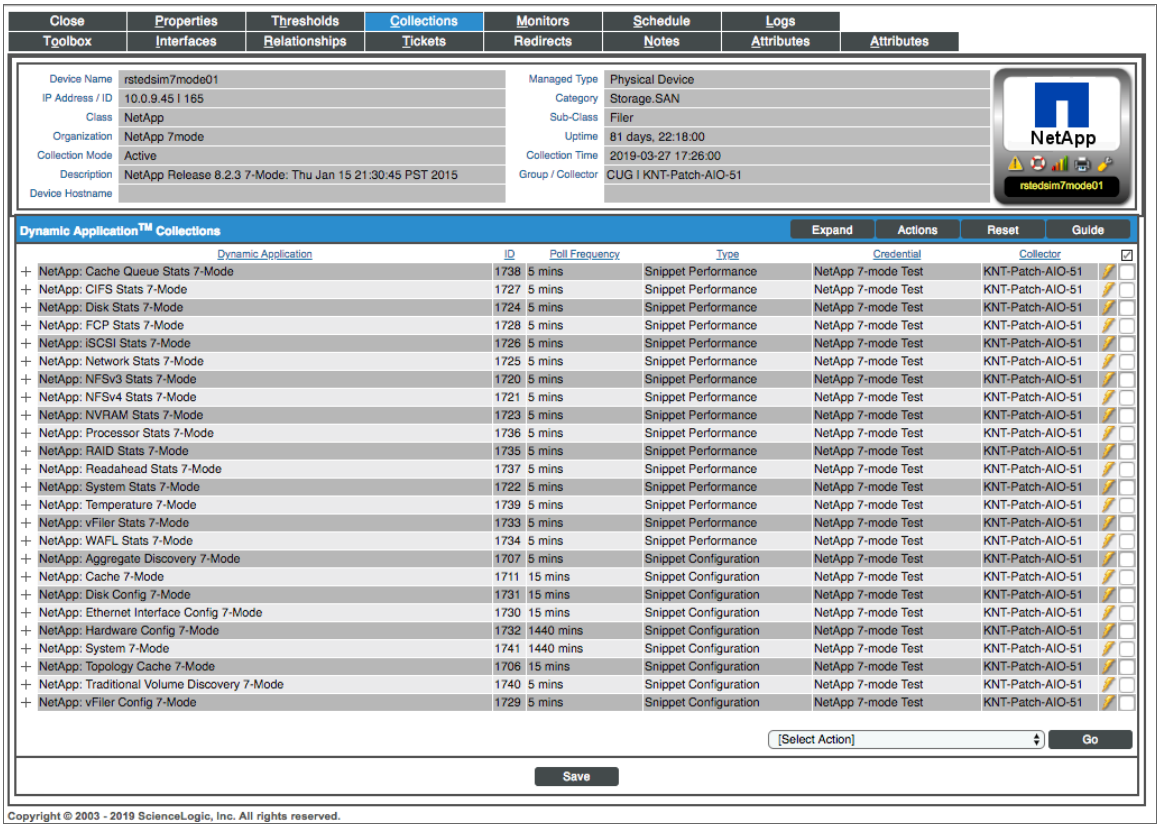
1. From the **Device Properties** page for the NetApp appliance, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
2. If the NetApp appliance is a C-Mode device, the following Dynamic Applications should be displayed in the list of Dynamic Applications aligned to the NetApp appliance:



- NetApp: Cache C-Mode
- NetApp: Cache C-Mode Volume Snapshot
- NetApp: Cache vServer Node C-Mode
- NetApp: Cluster Configuration C-Mode

- NetApp: Cluster Logical Interface Config C-Mode
- NetApp: Cluster Logical Interface Stats C-Mode
- NetApp: Cluster Performance C-Mode
- NetApp: Disk Count C-Mode
- NetApp: Hardware Count C-Mode
- NetApp: System C-Mode
- NetApp: Topology Cache C-Mode
- NetApp: Volume LUN Config Cache C-Mode
- NetApp: vServer Data Discovery C-Mode
- NetApp: vServer Node Discovery C-Mode

3. If the NetApp appliance is a 7-Mode device, the following Dynamic Applications should be displayed in the list of Dynamic Applications aligned to the NetApp appliance:



- NetApp: Aggregate Discovery 7-Mode
- NetApp: Cache 7-Mode
- NetApp: Cache Queue Stats 7-Mode
- NetApp: CIFS Stats 7-Mode

- NetApp: Disk Config 7-Mode
- NetApp: Disk Stats 7-Mode
- NetApp: Ethernet Interface Config 7-Mode
- NetApp: FCP Stats 7-Mode
- NetApp: Hardware Config 7-Mode
- NetApp: iSCSI Stats 7-Mode
- NetApp: Network Stats 7-Mode
- NetApp: NFSv3 Stats 7-Mode
- NetApp: NFSv4 Stats 7-Mode
- NetApp: NVRAM Stats 7-Mode
- NetApp: Processor Stats 7-Mode
- NetApp: RAID Stats 7-Mode
- NetApp: Readahead Stats 7-Mode
- NetApp: System 7-Mode
- NetApp: System Stats 7-Mode
- NetApp: Temperature 7-Mode
- NetApp: Topology Cache 7-Mode
- NetApp: Traditional Volume Discovery 7-Mode
- NetApp: vFiler Config 7-Mode
- NetApp: vFiler Stats 7-Mode
- NetApp: WAFL Stats 7-Mode

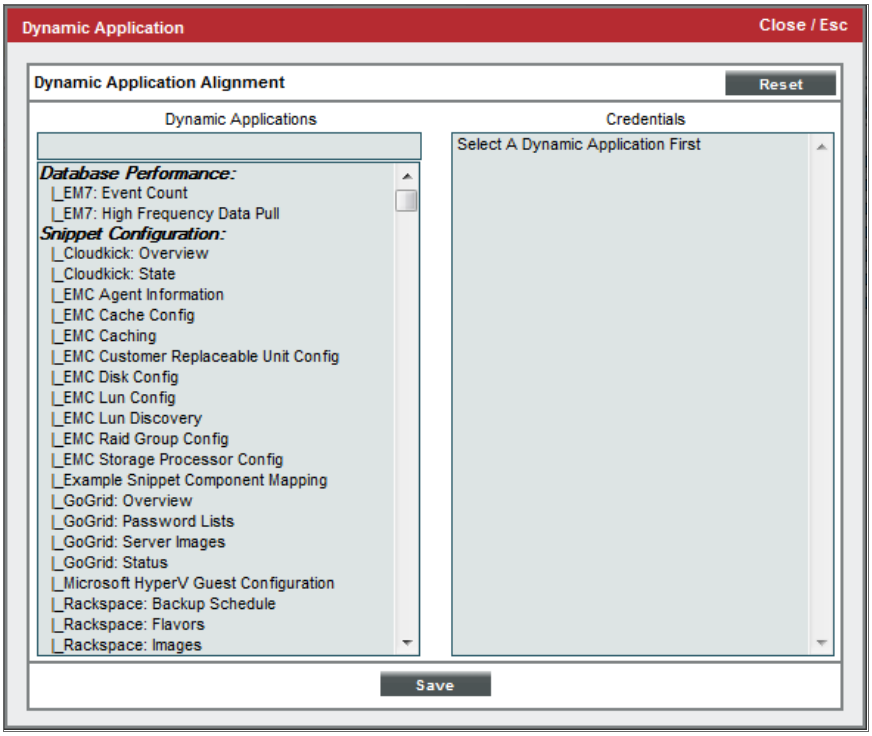
4. If one or more of these Dynamic Applications are not automatically aligned with each NetApp device, follow the instructions in the section on *Manually Aligning the Dynamic Applications*.

Manually Aligning the Dynamic Applications

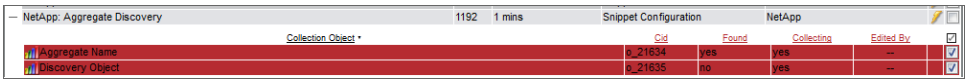
If the Dynamic Applications have not been automatically aligned, you can align them manually:

1. From the **Device Properties** page for the NetApp appliance, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.

2. Click the **[Action]** button and then click *Add Dynamic Application*. The **Dynamic Application Alignment** page appears:



3. In the ***Dynamic Applications*** field, select the Dynamic Application you want to align.
4. In the ***Credentials*** field, select the credential *you created for this NetApp appliance*.
5. Click the **[Save]** button.
6. Repeat steps 2-5 for the remaining Dynamic Applications to align with the C-mode or 7-Mode NetApp appliance.
7. After aligning the Dynamic Applications, click the **[Reset]** button and then click the plus icon (+) for the Dynamic Application. If collection for the Dynamic Application was successful, the graph icons ( ) for the Dynamic Application are enabled:

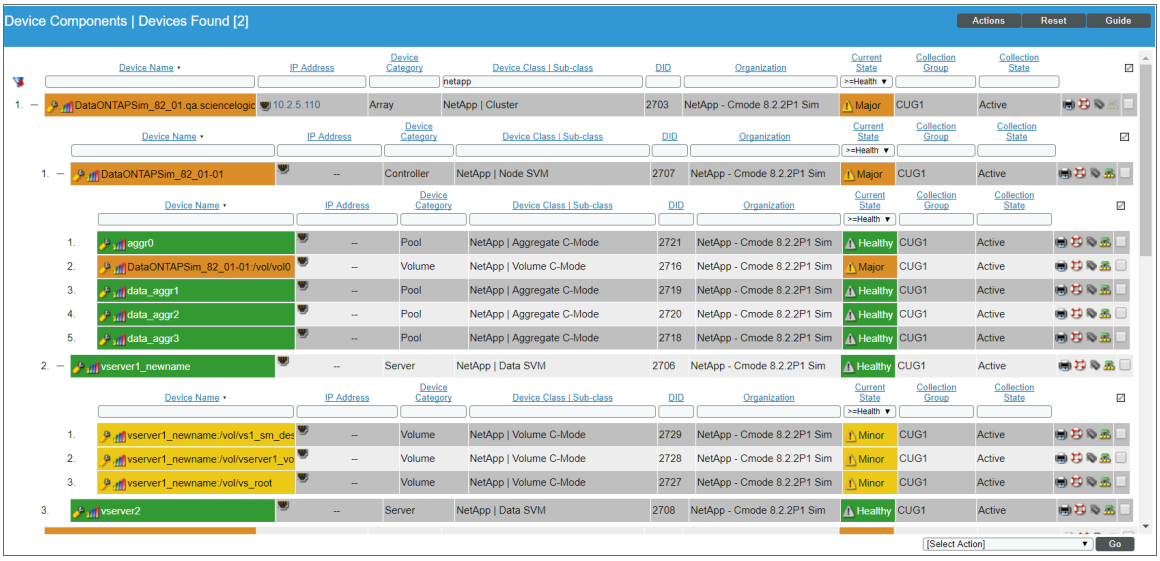


8. Click a graph icon ( ) to view the collected data. The **Configuration Report** page will display the number of components of each type and the total number of components managed by the NetApp appliance.

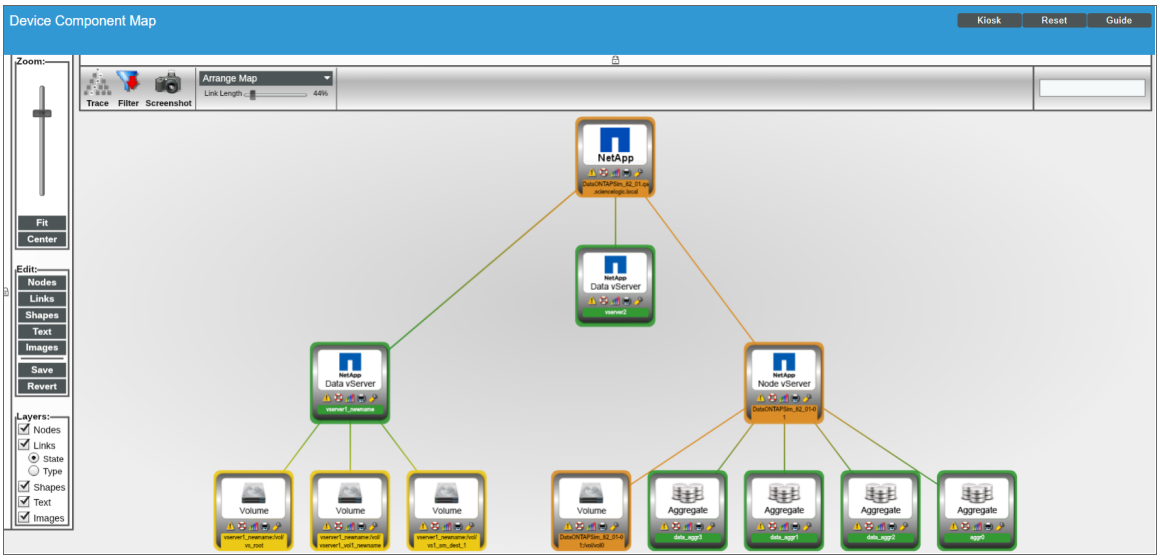
Viewing NetApp Component Devices

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

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



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



Relationships with Other Types of Component Devices

SL1 can automatically build relationships between NetApp component devices and other associated devices. If you discover a vCenter device using the Dynamic Applications in the *VMware: vSphere Base Pack* PowerPack, SL1 will automatically create relationships between NetApp LUNs and VMware Datastores, where appropriate.

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