



Monitoring NetApp Appliances

NetApp Base Pack PowerPack version 102, revision 3

Table of Contents

Introduction	1
What is NetApp Data ONTAP?	1
What Does the NetApp Base Pack PowerPack Monitor?	2
Installing the NetApp Base Pack PowerPack	2
Discovering NetApp Devices	4
Prerequisites for Monitoring NetApp	4
Configuring NetApp Credentials	5
Creating a Credential for 7-Mode	6
Creating a Credential for C-Mode	7
Creating an SNMP Credential	9
Discovering a NetApp Appliance	11
Verifying Discovery and Dynamic Applications	13
Manually Aligning the Dynamic Applications	15
Viewing NetApp Component Devices	17
Relationships with Other Types of Component Devices	18

Introduction

Overview

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

The following sections provide an overview of NetApp and the *NetApp Base Pack PowerPack*:

What is NetApp Data ONTAP?	1
What Does the NetApp Base Pack PowerPack Monitor?	2
Installing the NetApp Base Pack PowerPack	2

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

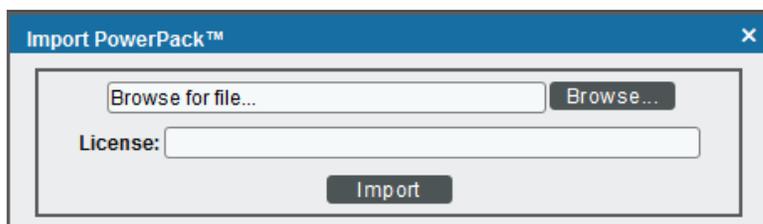
Installing the NetApp Base Pack PowerPack

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*.

Discovering NetApp Devices

Overview

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

<i>Prerequisites for Monitoring NetApp</i>	4
<i>Configuring NetApp Credentials</i>	5
<i>Creating a Credential for 7-Mode</i>	6
<i>Creating a Credential for C-Mode</i>	7
<i>Creating an SNMP Credential</i>	9
<i>Discovering a NetApp Appliance</i>	11
<i>Verifying Discovery and Dynamic Applications</i>	13
<i>Manually Aligning the Dynamic Applications</i>	15
<i>Viewing NetApp Component Devices</i>	17
<i>Relationships with Other Types of Component Devices</i>	18

Prerequisites for Monitoring NetApp

Before you discover your NetApp appliances in your ScienceLogic 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 the platform 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 the ScienceLogic platform. These credentials allow the platform 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 than the other SNMP devices in your network, you must create a new SNMP credential for the NetApp devices.

Creating a Credential for 7-Mode

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

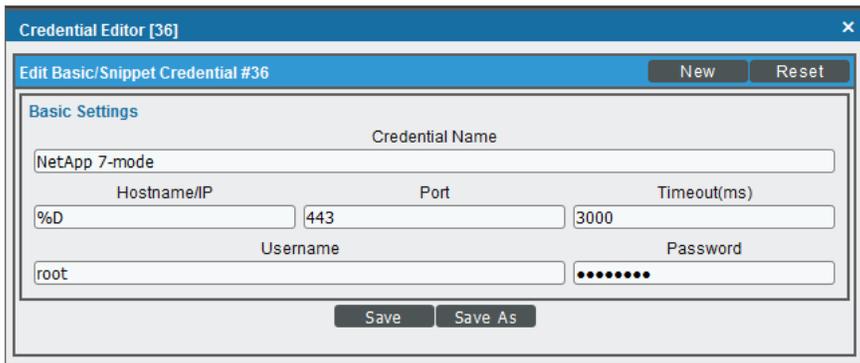
1. Go to the **Credential Management** page (System > Manage > Credentials).

Credential Management | Credentials Found [8]

NetApp	Profile Name	Organization	RO Use	RW Use	DA Use	Type	Credential User	Host	Exp	Timeout (min)	ID	Last Edited	Edited By
1	NetApp 7-mode	[all orgs]	--	--	--	BasicSnmpet	root	%D	443	3000	36	2015-10-21 17:48:44	em7admin
2	NetApp Flexpod	[all orgs]	--	--	173	SOAP/XML Host cmode_ro	%D		443	10000	72	2015-10-21 17:58:15	dabed
3	NetApp Flexpod	[all orgs]	38	--	--	SNMP	--	--	161	1500	74	2015-10-21 17:59:19	dabed
4	NetApp lab 001 (7-mode)	[all orgs]	--	--	--	BasicSnmpet	root	%D	443	3000	75	2015-10-26 09:19:39	dabed
5	NetApp Simulators	[all orgs]	--	--	354	SOAP/XML Host admin	%D		443	10000	71	2015-10-21 17:57:52	dabed
6	NetApp Simulators	[all orgs]	56	--	--	SNMP	--	--	161	1500	73	2015-10-21 17:59:00	dabed
7	NetApp w/SSL Option	[all orgs]	--	--	--	SOAP/XML Host root	%D		443	3000	38	2015-10-21 17:48:44	em7admin
8	NetApp w/SSL Option Off	[all orgs]	--	--	--	SOAP/XML Host root	%D		443	10000	37	2015-10-21 17:48:44	em7admin

Logic, Inc. All rights reserved. 7.7.0.master - build 2065

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



The screenshot shows a 'Credential Editor' window with the following fields and values:

Field	Value
Credential Name	NetApp 7-mode
Hostname/IP	%D
Port	443
Timeout(ms)	3000
Username	root
Password	••••••••

3. Supply values in the following fields:

- **Credential Name**. Enter a new name for the credential.
- **Username**. Enter the username that the platform 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:

Profile Name	Organization	RO Use	RW Use	DA Use	Type	Credential User	Host	Port	Timeout (ms)	ID	Last Edited	Edited By
1. NetApp 7-mode	[all orgs]	--	--	--	BasicSnippet	root	%D	443	3000	24	2016-07-20 12:56:35	em7admin
2. NetApp w/SSL Option	[all orgs]	--	--	--	SOAP/XML Hos	root	%D	443	3000	26	2016-07-20 12:56:35	em7admin
3. NetApp w/SSL Option Off	[all orgs]	--	--	--	SOAP/XML Hos	root	%D	443	10000	25	2016-07-20 12:56:35	em7admin
4. NetApp w/SSL/TLS Option	[all orgs]	--	--	--	SOAP/XML Hos	CHANGEME	%D	443	3000	72	2016-07-20 12:56:35	em7admin

- If you want the platform 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 the platform 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 the platform 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.
- **HTTP Auth User.** Type the username that the platform 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 the platform to use SSL or TLS when connecting to the NetApp device. Type "False" if you do not want the platform to use SSL or TLS when connecting to the NetApp device.
- **Embed Value [%2].** Type "TLSv1.0" if you want the platform to use TLS when connecting to the NetApp device. Otherwise, keep this field blank.

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 the ScienceLogic platform to access SNMP data on a managed device. The platform 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).

Profile Name	Organization	BO Use	RW Use	DA Use	Type	Credential User	Host	Port	Timeout (ms)	ID	Last
1. Amazon Web Services Credential	System	--	--	--	SOAP/XML Host	AWS Account Access	example.com	80	2000	1	2015-05-16
2. Azure Credential - SOAP/XML	[all orgs]	--	--	--	SOAP/XML Host	<AD_USER>	login.windows.net	443	60000	60	2015-05-14
3. Azure Credential - SSH/Key	[all orgs]	--	--	--	SSH/Key	<SUBSCRIPTION_ID_H %D		22	180000	59	2015-05-14
4. Cisco SNMPv2 - Example	[all orgs]	--	--	--	SNMP	--	--	161	1500	3	2015-05-14
5. Cisco SNMPv3 - Example	[all orgs]	--	--	--	SNMP	{USER_GOES_HERE}		161	1500	2	2015-05-14
6. Cisco: ACI	[all orgs]	--	--	126	Basic/Snippet	admin	173.36.219.46	443	0	62	2015-05-14 15:05:24
7. Cisco: ACI Credential	[all orgs]	--	--	--	Basic/Snippet	admin	198.18.133.200	443	0	61	2015-05-14 14:32:20
8. Cloudkick - Example	[all orgs]	--	--	--	Basic/Snippet	{SECURITY KEY GOES	127.0.0.1	443	5000	9	2015-05-14 11:25:31
9. GUCM PerimeterService 8.0 Example	[all orgs]	--	--	--	SOAP/XML Host	--	%D	8443	2000	4	2015-05-14 11:25:12
10. EM7 Central Database	[all orgs]	--	--	--	Database	root	localhost	7706	0	51	2015-05-14 11:28:41
11. EM7 Collector Database	[all orgs]	--	--	--	Database	root	%D	7707	0	14	2015-05-14 11:25:43
12. EM7 DB	[all orgs]	--	--	--	Database	root	%D	7706	0	35	2015-05-14 11:28:32
13. EM7 DB - DB info	[all orgs]	--	--	--	SOAP/XML Host	root	%D	80	3000	38	2015-05-14 11:28:32
14. EM7 DB - My.cnf	[all orgs]	--	--	--	SOAP/XML Host	root	%D	80	3000	37	2015-05-14 11:28:32
15. EM7 DB - Ssl.cnf	[all orgs]	--	--	--	SOAP/XML Host	root	%D	80	3000	36	2015-05-14 11:28:32
16. EM7 Default V2	[all orgs]	--	--	--	SNMP	--	--	161	1500	10	2015-05-14 11:25:42
17. EM7 Default V3	[all orgs]	--	--	--	SNMP	em7default3	--	161	500	11	2015-05-14 11:25:42
18. EMC - Example	[all orgs]	--	--	--	Basic/Snippet	root	%D	443	10000	15	2015-05-14 11:25:47
19. GoGrid - Example	[all orgs]	--	--	--	Basic/Snippet	{SECURITY KEY GOES	127.0.0.1	443	5000	16	2015-05-14 11:25:51
20. IP-SLA Example	[all orgs]	--	--	--	SNMP	--	--	161	1500	5	2015-05-14 11:25:14
21. LifeSize - Endpoint SNMP	[all orgs]	--	--	--	SNMP	control	--	161	3000	16	2015-05-14 11:25:58
22. LifeSize - Endpoint SSH/CLI	[all orgs]	--	--	--	Basic/Snippet	auto	%D	22	3	17	2015-05-14 11:25:58
23. Local API	[all orgs]	--	--	--	Basic/Snippet	em7admin	193.0.0.180	80	5000	22	2015-05-14 11:28:11
24. NetApp 7-mode	[all orgs]	--	--	--	Basic/Snippet	root	%D	443	3000	24	2015-05-14 11:28:20
25. NetApp w/SSL Option	[all orgs]	--	--	--	SOAP/XML Host	root	%D	443	3000	26	2015-05-14 11:28:20
26. NetApp w/SSL Option Off	[all orgs]	--	--	--	SOAP/XML Host	root	%D	443	10000	25	2015-05-14 11:28:20
27. Nexus netconf	[all orgs]	--	--	--	Basic/Snippet	--	%D	22	10000	6	2015-05-14 11:25:16
28. Nexus snmp	[all orgs]	--	--	--	SNMP	--	--	161	10000	7	2015-05-14 11:25:16
29. Polycm - Advanced	[all orgs]	--	--	--	SOAP/XML Host	admin	%D	80	20000	28	2015-05-14 11:28:24
30. Polycm - CDR	[all orgs]	--	--	--	SOAP/XML Host	admin	%D	80	20000	31	2015-05-14 11:28:24
31. Polycm - interface	[all orgs]	--	--	--	SOAP/XML Host	admin	%D	80	20000	29	2015-05-14 11:28:24

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

The screenshot shows a window titled "Credential Editor" with a sub-header "Create New SNMP Credential". The window contains three main sections of settings:

- Basic Settings:** Includes a text field for "Profile Name", a dropdown for "SNMP Version" (currently set to "[SNMP V2]"), a text field for "Port" (161), a text field for "Timeout(ms)" (1500), and a text field for "Retries" (1).
- SNMP V1/V2 Settings:** Includes two text fields: "SNMP Community (Read-Only)" and "SNMP Community (Read/Write)".
- SNMP V3 Settings:** Includes text fields for "Security Name" and "Security Passphrase", a dropdown for "Authentication Protocol" (set to "[MD5]"), a dropdown for "Security Level" (set to "[Authentication Only]"), a text field for "SNMP v3 Engine ID", a text field for "Context Name", a dropdown for "Privacy Protocol" (set to "[DES]"), and a text field for "Privacy Protocol Pass Phrase".

Buttons for "Reset" (top right) and "Save" (bottom center) are visible.

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 the platform 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 the platform will stop trying to communicate with the SNMP device. The default value is *1500*. This field is required.
- **Retries.** Number of times the platform 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 the ScienceLogic platform.

NOTE: When you define a SNMP Credential, the ScienceLogic platform 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).

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

The screenshot shows the 'Discovery Session Editor' window with the following sections:

- Identification Information:** Name: NetApp 9.1 CMode Sim; Description: (empty).
- IP and Credentials:**
 - IP Address/Hostname Discovery List:** 10.2.5.25
 - SNMP Credentials:** List includes EM7 Default V3, IPSLA Example, LifeSize: Endpoint SNMP, [NetApp - Cmode Sim SNMP], NetApp Flexpod, Nexus snmp, SNMP Public V1, SNMP Public V2, VMware_vCenter55 snmp.
 - Other Credentials:** List includes Dell EMC: Isilon SOAP, Dell EMC: Isilon SOAP ADMIN, Dell EMC: Isilon SOAP Example, EM7 DB - DB Info, EM7 DB - My.cnf, EM7 DB - Silo.conf, [Netapp - Cmode Sim], NetApp Flexpod, NetApp Sim.
- Detection and Scanning:**
 - Initial Scan Level: [System Default (recommended)]
 - Scan Throttle: [System Default (recommended)]
 - Port Scan All IPs: [System Default (recommended)]
 - Port Scan Timeout: [System Default (recommended)]
 - Detection Method & Port: [Default Method], UDP: 161 SNMP, TCP: 1 - tcpmux, TCP: 2 - compressnet, TCP: 3 - compressnet, TCP: 5 - rje, TCP: 7 - echo, TCP: 9 - discard, TCP: 11 - systat, TCP: 13 - daytime, TCP: 17 - qotd, TCP: 18 - msp.
 - Interface Inventory Timeout (ms): 600000
 - Maximum Allowed Interfaces: 10000
 - Bypass Interface Inventory:
- Basic Settings:**
 - Discover Non-SNMP:
 - Model Devices:
 - DHCP:
 - Duplication Protection:
 - Collection Server PID: 5
 - Organization: [NetApp - Cmode 9.1 Sim]
 - Add Devices to Device Group(s): None Servers
 - Apply Device Template: [Choose a Template]

Buttons at the bottom: Save, Save As, Log All (checked).

- Enter values in the following fields:
 - IP Address Discovery List.** Enter the IP address for the NetApp appliance. This can be the IP address for a single filer appliance List or the IP address for a cluster.
 - SNMP Credential.** Select an SNMP credential to use with the NetApp appliance.
 - Other Credentials.** Select the credential that you configured in the previous section.
- 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.
- Click the **[Save]** button and then close the **Discovery Session Editor** window.
- 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.
- The **Discovery Session** window will be displayed.
- 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 the ScienceLogic platform 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:

The screenshot shows the 'Dynamic Application Collections' page for a NetApp device. The top navigation bar includes tabs for Close, Properties, Thresholds, Collections (selected), Monitors, and Schedule. Below this are sub-tabs for Logs, Toolbox, Interfaces, Relationships, Tickets, Redirects, Notes, and Attributes. The main content area displays device details for 'KNT_ONTAP_91.qa.sciencelogic.local', including its IP address (10.2.5.25 | 201), class (NetApp), organization (Netapp 9x Cmode), and collection mode (Active). A table lists 17 dynamic applications with columns for ID, Poll Frequency, Type, and Credential. The applications include various configurations and performance snippets for the NetApp C-Mode cluster. At the bottom, there is a '[Select Action]' dropdown and a 'Go' button, and a 'Save' button is located below the table.

Dynamic Application	ID	Poll Frequency	Type	Credential
+ Cisco IPSLA Configuration	722	60 mins	Snippet Configuration	Default SNMP Credential
+ Host Resource: Configuration	17	15 mins	Snippet Configuration	Default SNMP Credential
+ NetApp: Cache C-Mode	2143	15 mins	Snippet Configuration	NetApp 9.1 Sim
+ NetApp: Cache vServer Node C-Mode	2179	15 mins	Snippet Configuration	NetApp 9.1 Sim
+ NetApp: Cluster Configuration C-Mode	2177	15 mins	Snippet Configuration	NetApp 9.1 Sim
+ NetApp: Cluster Logical Interface Config C-Mode	2092	15 mins	Snippet Configuration	NetApp 9.1 Sim
+ NetApp: Cluster Logical Interface Stats C-Mode	2180	5 mins	Snippet Performance	NetApp 9.1 Sim
+ NetApp: Cluster Performance C-Mode	2178	5 mins	Snippet Performance	NetApp 9.1 Sim
+ NetApp: Disk Count C-Mode	2175	15 mins	Snippet Configuration	NetApp 9.1 Sim
+ NetApp: Hardware Count C-Mode	2156	1440 mins	Snippet Configuration	NetApp 9.1 Sim
+ NetApp: System C-Mode	2154	1440 mins	Snippet Configuration	NetApp 9.1 Sim
+ NetApp: Topology Cache C-Mode	2140	15 mins	Snippet Configuration	NetApp 9.1 Sim
+ NetApp: Volume LUN Config Cache C-Mode	2176	5 mins	Snippet Configuration	NetApp 9.1 Sim
+ NetApp: vServer Data Discovery C-Mode	2167	5 mins	Snippet Configuration	NetApp 9.1 Sim
+ NetApp: vServer Node Discovery C-Mode	2157	5 mins	Snippet Configuration	NetApp 9.1 Sim

- NetApp: Cache C-Mode
- 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:

Dynamic Application	ID	Poll Frequency	Type	Credential
+ NetApp: Aggregate Discovery 7-Mode	588	5 mins	Snippet Configuration	NetApp 7mode test
+ NetApp: Cache 7-Mode	572	15 mins	Snippet Configuration	NetApp 7mode test
+ NetApp: Cache Queue Stats 7-Mode	599	5 mins	Snippet Performance	NetApp 7mode test
+ NetApp: CIFS Stats 7-Mode	588	5 mins	Snippet Performance	NetApp 7mode test
+ NetApp: Cluster Configuration C-Mode	1236	15 mins	Snippet Configuration	NetApp 7mode test
+ NetApp: Cluster Performance C-Mode	1237	5 mins	Snippet Performance	NetApp 7mode test
+ NetApp: Disk Config 7-Mode	592	15 mins	Snippet Configuration	NetApp 7mode test
+ NetApp: Disk Stats 7-Mode	585	5 mins	Snippet Performance	NetApp 7mode test
+ NetApp: Ethernet Interface Config 7-Mode	591	15 mins	Snippet Configuration	NetApp 7mode test
+ NetApp: FCP Stats 7-Mode	589	5 mins	Snippet Performance	NetApp 7mode test
+ NetApp: Hardware Config 7-Mode	593	1440 mins	Snippet Configuration	NetApp 7mode test
+ NetApp: iSCSI Stats 7-Mode	587	5 mins	Snippet Performance	NetApp 7mode test
+ NetApp: Network Stats 7-Mode	586	5 mins	Snippet Performance	NetApp 7mode test
+ NetApp: NFSv3 Stats 7-Mode	581	5 mins	Snippet Performance	NetApp 7mode test
+ NetApp: NFSv4 Stats 7-Mode	582	5 mins	Snippet Performance	NetApp 7mode test
+ NetApp: NVRAM Stats 7-Mode	584	5 mins	Snippet Performance	NetApp 7mode test
+ NetApp: Processor Stats 7-Mode	597	5 mins	Snippet Performance	NetApp 7mode test
+ NetApp: RAID Stats 7-Mode	596	5 mins	Snippet Performance	NetApp 7mode test
+ NetApp: Readahead Stats 7-Mode	598	5 mins	Snippet Performance	NetApp 7mode test
+ NetApp: System 7-Mode	602	1440 mins	Snippet Configuration	NetApp 7mode test
+ NetApp: System Stats 7-Mode	583	5 mins	Snippet Performance	NetApp 7mode test
+ NetApp: Temperature 7-Mode	600	5 mins	Snippet Performance	NetApp 7mode test
+ NetApp: Topology Cache 7-Mode	567	15 mins	Snippet Configuration	NetApp 7mode test
+ NetApp: Traditional Volume Discovery 7-Mode	601	5 mins	Snippet Configuration	NetApp 7mode test
+ NetApp: vFiler Config 7-Mode	590	5 mins	Snippet Configuration	NetApp 7mode test
+ NetApp: vFiler Stats 7-Mode	594	5 mins	Snippet Performance	NetApp 7mode test
+ NetApp: WAFL Stats 7-Mode	595	5 mins	Snippet Performance	NetApp 7mode test
+ System Uptime: sysUptime	931	5 mins	SNMP Configuration	Default SNMP Credential

- NetApp: Aggregate Discovery 7-Mode
- NetApp: Cache 7-Mode
- NetApp: Cache Queue Stats 7-Mode
- NetApp: CIFS Stats 7-Mode
- NetApp: Cluster Configuration C-Mode
- NetApp: Cluster Performance C-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

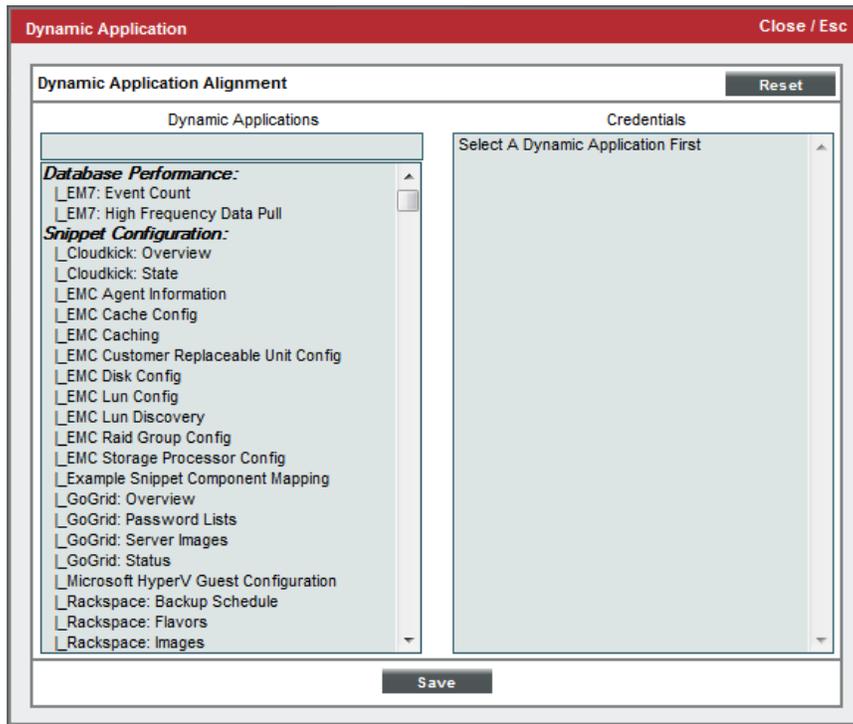
4. If one or more of these Dynamic Applications are not automatically aligned with each NetApp device, follow the instructions in the section on [Manually Aligning the Dynamic Applications](#).

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.

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



- In the **Dynamic Applications** field, select the Dynamic Application you want to align.
- In the **Credentials** field, select the credential *you created for this NetApp appliance*.
- Click the **[Save]** button.
- Repeat steps 2-5 for the remaining Dynamic Applications to align with the C-mode or 7-Mode NetApp appliance.
- 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:

Collection Object *	Cid	Found	Collecting	Edited By	
Aggregate Name	s_21634	yes	yes	--	📊
Discovery Object	s_21635	no	yes	--	📊

- 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.

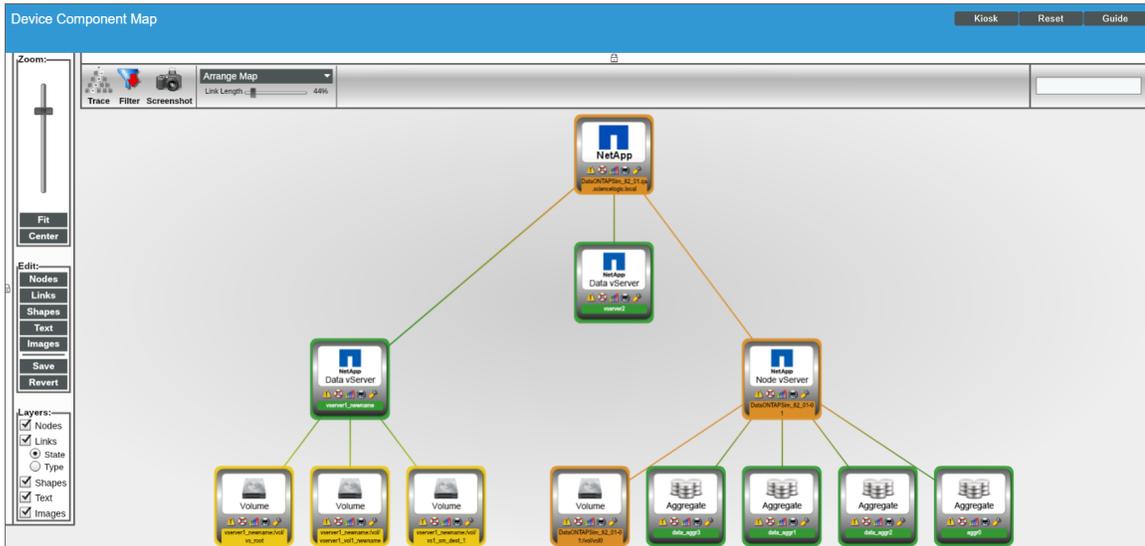
Viewing NetApp Component Devices

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 the ScienceLogic platform 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 (+):

Device Name	IP Address	Device Category	Device Class Sub-class	DID	Organization	Current State	Collection Group	Collection State
1. - DataONTAPSim_82_01 qa sciencelogic	10.2.5.110	Array	NetApp Cluster	2703	NetApp - Cmode 8.2.2P1 Sim	Major	CUG1	Active
1. - DataONTAPSim_82_01-01	--	Controller	NetApp Node SVM	2707	NetApp - Cmode 8.2.2P1 Sim	Major	CUG1	Active
1. aggr0	--	Pool	NetApp Aggregate C-Mode	2721	NetApp - Cmode 8.2.2P1 Sim	Healthy	CUG1	Active
2. DataONTAPSim_82_01-01/vol/vol0	--	Volume	NetApp Volume C-Mode	2716	NetApp - Cmode 8.2.2P1 Sim	Major	CUG1	Active
3. data_aggr1	--	Pool	NetApp Aggregate C-Mode	2719	NetApp - Cmode 8.2.2P1 Sim	Healthy	CUG1	Active
4. data_aggr2	--	Pool	NetApp Aggregate C-Mode	2720	NetApp - Cmode 8.2.2P1 Sim	Healthy	CUG1	Active
5. data_aggr3	--	Pool	NetApp Aggregate C-Mode	2718	NetApp - Cmode 8.2.2P1 Sim	Healthy	CUG1	Active
2. - vsriver1_newname	--	Server	NetApp Data SVM	2706	NetApp - Cmode 8.2.2P1 Sim	Healthy	CUG1	Active
1. vsriver1_newname/vol/vs1_sm_des	--	Volume	NetApp Volume C-Mode	2729	NetApp - Cmode 8.2.2P1 Sim	Minor	CUG1	Active
2. vsriver1_newname/vol/vsriver1_vo	--	Volume	NetApp Volume C-Mode	2728	NetApp - Cmode 8.2.2P1 Sim	Minor	CUG1	Active
3. vsriver1_newname/vol/vs_root	--	Volume	NetApp Volume C-Mode	2727	NetApp - Cmode 8.2.2P1 Sim	Minor	CUG1	Active
3. vsriver2	--	Server	NetApp Data SVM	2708	NetApp - Cmode 8.2.2P1 Sim	Healthy	CUG1	Active

- 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. The ScienceLogic platform 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

The ScienceLogic platform 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, the platform will automatically create relationships between NetApp LUNs and VMware Datastores, where appropriate.

© 2003 - 2018, ScienceLogic, Inc.

All rights reserved.

LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

ALL INFORMATION AVAILABLE IN THIS GUIDE IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED. SCIENCELOGIC™ AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT.

Although ScienceLogic™ has attempted to provide accurate information on this Site, information on this Site may contain inadvertent technical inaccuracies or typographical errors, and ScienceLogic™ assumes no responsibility for the accuracy of the information. Information may be changed or updated without notice. ScienceLogic™ may also make improvements and / or changes in the products or services described in this Site at any time without notice.

Copyrights and Trademarks

ScienceLogic, the ScienceLogic logo, and EM7 are trademarks of ScienceLogic, Inc. in the United States, other countries, or both.

Below is a list of trademarks and service marks that should be credited to ScienceLogic, Inc. The ® and ™ symbols reflect the trademark registration status in the U.S. Patent and Trademark Office and may not be appropriate for materials to be distributed outside the United States.

- ScienceLogic™
- EM7™ and em7™
- Simplify IT™
- Dynamic Application™
- Relational Infrastructure Management™

The absence of a product or service name, slogan or logo from this list does not constitute a waiver of ScienceLogic's trademark or other intellectual property rights concerning that name, slogan, or logo.

Please note that laws concerning use of trademarks or product names vary by country. Always consult a local attorney for additional guidance.

Other

If any provision of this agreement shall be unlawful, void, or for any reason unenforceable, then that provision shall be deemed severable from this agreement and shall not affect the validity and enforceability of any remaining provisions. This is the entire agreement between the parties relating to the matters contained herein.

In the U.S. and other jurisdictions, trademark owners have a duty to police the use of their marks. Therefore, if you become aware of any improper use of ScienceLogic Trademarks, including infringement or counterfeiting by third parties, report them to Science Logic's legal department immediately. Report as much detail as possible about the misuse, including the name of the party, contact information, and copies or photographs of the potential misuse to: legal@sciencelogic.com



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

International: +1-703-354-1010