Monitoring SNMP-Enabled Devices

SL1 version 10.1.4, revision 1

Table of Contents

Introduction 3

What is SNMP? 3

What is Net-SNMP? 4

Why Should I Use Net-SNMP? 4

Basic SNMP Terminology 5

PowerPacks for Monitoring SNMP-Enabled Devices 7

Importing and Installing a PowerPack 8

Viewing the Contents of a PowerPack 9

Credentials 11

Creating Credentials for Monitoring SNMP-Enabled Devices 11

Discovery 14

Discovering SNMP-Enabled Devices 14

Dynamic Application and Device Class Alignment 15

How Does SL1 Align Dynamic Applications During Discovery? 16

How Does SL1 Align Device Classes During Discovery? 17

Chapter

1

Introduction

Overview

This manual describes how to monitor SNMP-enabled devices with SL1 using SNMP-based PowerPacks.

The following sections provide an overview of SNMP and the PowerPacks that you can use for Monitoring SNMP-Enabled Devices:

This chapter covers the following topics:

What is SNMP? 3

What is Net-SNMP? 4

Basic SNMP Terminology 5

PowerPacks for Monitoring SNMP-Enabled Devices 7

Importing and Installing a PowerPack 8

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 SNMP?

Simple Network Management Protocol (SNMP) is a set of standard protocols for managing diverse computer hardware and software within a TCP/IP network. SNMP is the most common protocol used by network monitoring and management applications to exchange information between devices. SL1 uses this protocol and other protocols to collect availability, performance, and configuration information.

SNMP uses a server-client structure.

- Clients are called ***agents***. Devices and software that run SNMP are agents. For the purposes of this document, Net-SNMP is the agent.
- The server is called the ***management system***. SL1 is the management system.

Typically, ***agents***:

- Implement the SNMP protocol on the device.
- Store data points as defined by the Management Information Base (MIB) file.
- Can asynchronously signal an event to the manager.

Typically, a ***management system***:

- Uses the SNMP Protocol.
- Queries agents.
- Receives responses (data points) from agents.
- Acknowledges asynchronous events from agents.

Most enterprise-level network hardware is configured for SNMP and can be SNMP-enabled. Many enterprise software applications are also SNMP-compliant. When SNMP is running on a device, it uses a standard format to collect and store data about the device and/or software. For example, SNMP might collect information on each network interface and the traffic on each interface. SL1 can then query the device to retrieve the stored data.

What is Net-SNMP?

Net-SNMP is a suite of applications used to implement SNMP. Net-SNMP is an agent. Standard Net-SNMP includes the SNMP daemon and a suite of client utilities. Net-SNMP can be run on any supported operating system, and SL1 will then be able communicate with and collect data from the device.

Why Should I Use Net-SNMP?

- Net-SNMP is an open-source application. It is free to use and distribute.
- Because Net-SNMP is widely used, there are many user groups and support forums for the product.

NOTE: Although ScienceLogic does not directly support the Net-SNMP agent, this document will get you started on the installation and configuration tasks for Net-SNMP. For detailed documentation on Net-SNMP, see the Net-SNMP website.

- Net-SNMP includes source and pre-compiled objects for all major flavors or UNIX and Linux as well as a number of other operating systems.

- Net-SNMP is an ***extensible*** agent. Generally, SNMP agents can retrieve only data that has been defined in a MIB file. In most cases, a hardware or software manufacturer creates the MIB file and then ships the MIB file with the product. Net-SNMP allows users to add values to the MIB file and retrieve values from scripts, programs, and files.
- Net-SNMP is a natural fit with SL1's Dynamic Applications. Using Net-SNMP and dynamic applications, users can create reports, coupled graphs, and events based on the data points that are most useful to them.

Basic SNMP Terminology

This section defines some basic SNMP terminology. You should be familiar with the following terminology before installing and configuring Net-SNMP:

- ***SNMP (Simple Network Management Protocol)***. A set of standard protocols for managing diverse computer hardware and software within a TCP/IP network. SNMP is the most common network protocol used by network monitoring and management applications to exchange management information between devices. SL1 uses this protocol and other protocols to collect availability, performance, and configuration information.

  SNMP uses a server-client structure. Clients are called agents. Devices and software that run SNMP are agents. The server is called the management system. SL1 is the management system.

  Most enterprise-level network hardware is configured for SNMP and can be SNMP-enabled. Many enterprise software applications are also SNMP-compliant. When SNMP is running on a device, it uses a standard format to collect and store data about the device and/or software. For example, SNMP might collect information on each network interface and the traffic on each interface. SL1 can then query the device to retrieve the stored data.

- ***SNMP Tree***. SNMP uses a tree structure. The first few branches of the tree are organizational and do not apply to specific manufacturers and device. The starting point for all device or application info is:
  - 1.3.6.1.4.1.vendor_number
  - For details on SNMP tree structure, see the SMI Network Management Private Enterprise Codes.
  - For an overview of the entire SNMP tree, see http://www3.rad.com/networks/applications/snmp/main.htm.

- ***MIB (Management Information Base)***. A collection of objects that can be monitored by a network management system (in this case, SL1). The objects are organized hierarchically and stored in a MIB file. SNMP requires a standardized format for each MIB file. This standardized format allows SL1 to gather data on any device where SNMP is enabled. A MIB file is usually associated with a manufacturer and a device. Some companies use a single MIB that contains information on all their products; some manufacturers create a separate MIB for each product.
- ***OID (Object ID)***. OIDs are the numeric IDs that are used in the SNMP tree. OIDs are used to define manufacturers, devices, and the characteristics of devices. OIDs are defined and organized in MIB files.
- In SL1, the ***root OID*** (sometimes called the vendor number) refers to the unique number assigned to each manufacturer. Each root OID is registered with IANA. For example, the root OID for American Power Conversion (APC) Corporation is 1.3.6.1.4.1.318. APC can then create and organize OIDs under this root OID. For example:

- 1.3.6.1.4.1.318 is the root OID for American Power Conversion Corporation.
- 1.3.6.1.4.1.318.1 could mean "all products". APC could then define unique IDs under “all products”.
- 1.3.6.1.4.1.318.1.1 could mean "hardware".
- 1.3.6.1.4.1.318.1.2 could mean "software".

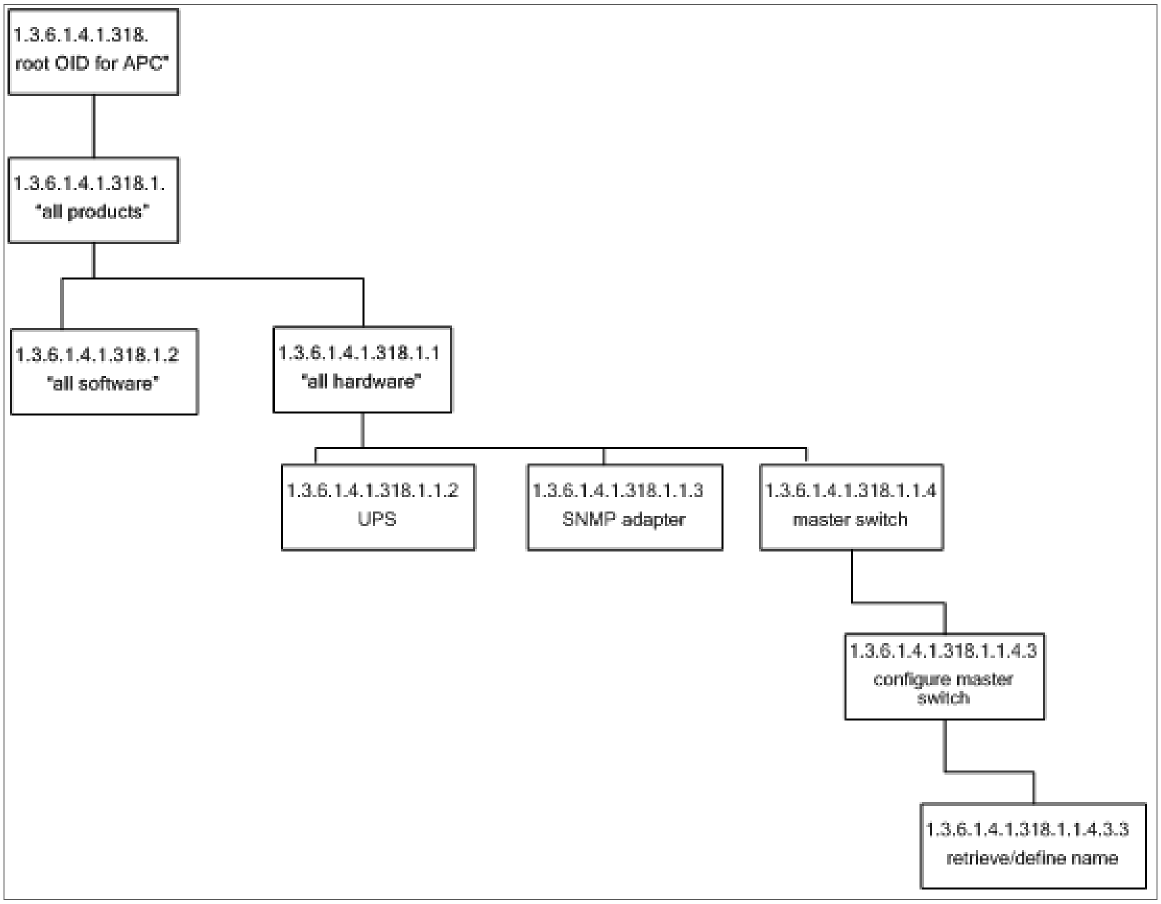
All the OIDs that occur under 1.3.6.1.4.1.318.1.1 would be mapped to types of hardware, for example:

- 1.3.6.1.4.1.318.1.1.2 could mean "UPS".
- 1.3.6.1.4.1.318.1.1.3 could mean "SNMP adapter".
- 1.3.6.1.4.1.318.1.1.4 could mean "master switch".

All the OIDs that occur under each type of hardware (UPS, SNMP adapter, master switch) would be mapped to specific parameters that can be monitored and controlled through SNMP commands. For example:

- 1.3.6.1.4.1.318.1.1.4.3 could mean "configuration settings for master switch".
- 1.3.6.1.4.1.318.1.1.4.3.3 could mean "retrieve or define name for master switch".

The section of the SNMP tree for our example would look like this:



PowerPacks for Monitoring SNMP-Enabled Devices

The following PowerPacks contain SNMP Dynamic Applications and device classes, and can be used to monitor SNMP-enabled devices with SL1:

- Alteon Base Pack
- APC Base Pack
- Aruba Base Pack
- Avocent Base Pack
- Avocent ACS Pack
- Blue Coat Base Pack
- BlueCat Base Pack
- Brocade Base Pack
- Cisco: Base Pack
- Cisco: IPSLA
- Cisco: TelePresence: Endpoints
- Cisco: TelePresence: Infrastructure
- Cisco Unity Pack
- Citrix Base Pack
- Coyote Point Base Pack
- Data Pull Support
- Dell OM Base Pack
- Dell OpenManage Old Base Pack
- Dell PowerConnect Base Pack
- Dell PowerVault Base Pack
- Enterasys Base Pack
- Extreme Base Pack
- Force 10 Base Pack
- Fortinet Base Pack
- Foundry Base Pack
- Generic Switch/Router MIB Support
- Google Base Pack
- H3C Base Pack
- Hitachi Base Pack
- HP-ISM Base Pack
- HP Pro Curve Base Pack

- HP-UX Base Pack
- Juniper Base Pack
- Liebert Base Pack
- LifeSize Endpoint
- MIB-2 Base Pack
- Net-SNMP Base Pack
- Netscreen Base Pack
- Nokia Base Pack
- Polycom Infrastructure
- Polycom Endpoint
- Printer Base Pack
- Riverbed Base Pack
- UCD-SNMP Base Pack

You can find and download PowerPacks on the ScienceLogic Support Site.

Importing and Installing a PowerPack

To perform the steps in this manual, you must first download, import, and install the appropriate PowerPack for the SNMP-enabled devices that you want to monitor.

To view a list of all installed PowerPacks, go to the **PowerPack Manager** page (System > Manage > PowerPacks).

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.)

IMPORTANT: The minimum required MySQL version is 5.6.0.

To download and install the PowerPack:

1. Search for and download the PowerPack from the **PowerPacks** page (Product Downloads > PowerPacks & SyncPacks) at the ScienceLogic Support Site.
2. In SL1, go to the **PowerPacks** page (System > Manage > PowerPacks).
3. Click the **[Actions]** button and choose *Import PowerPack*. The **Import PowerPack** dialog box appears.
4. Click **[Browse]** and navigate to the PowerPack file from step 1.

5. Select the PowerPack file and click **[Import]**. The **PowerPack Installer** modal displays a list of the PowerPack contents.
6. Click **[Install]**. The PowerPack is added to the **PowerPacks** page.

NOTE: If you exit the **PowerPack Installer** modal without installing the imported PowerPack, the imported PowerPack will not appear in the **PowerPacks** page. However, the imported PowerPack will appear in the **Imported PowerPacks** modal. This page appears when you click the **[Actions]** menu and select *Install PowerPack*.

Viewing the Contents of a PowerPack

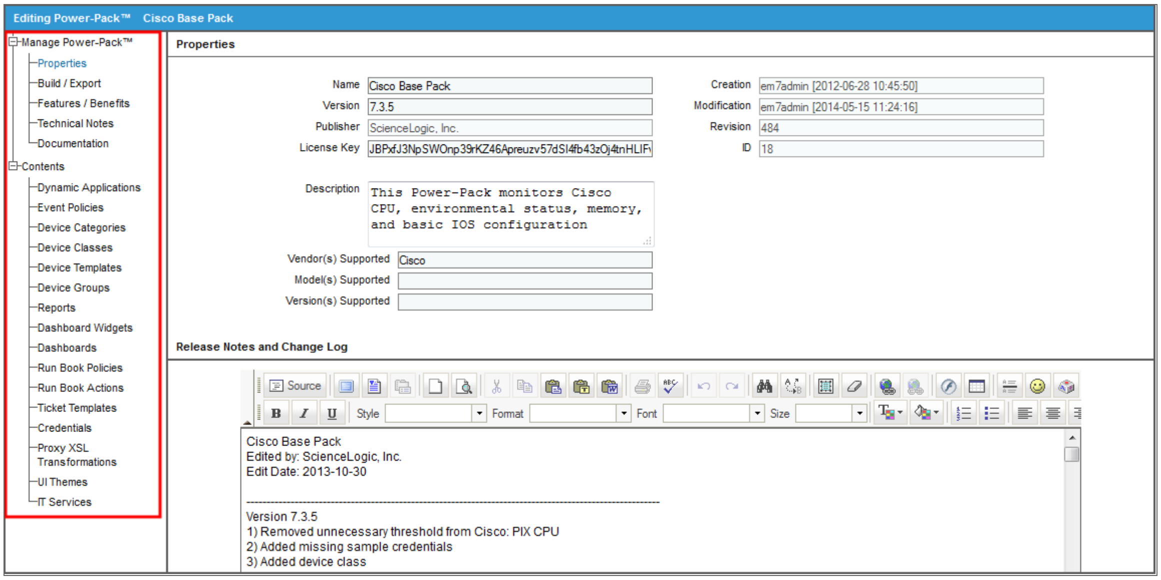
PowerPacks consist of one or more of the following:

- Dynamic Applications
- Event policies
- Device categories
- Device classes
- Device templates
- Device groups
- Reports
- Dashboard Widgets
- Dashboards
- Run book policies
- Run book actions
- Ticket templates
- Credentials
- Proxy XML transformations
- UI themes
- IT service policies

To view the contents of a PowerPack:

1. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).
2. Click the wrench icon (🔧) next to the desired PowerPack to view the **PowerPack Properties** page.

3. In the left NavBar, select the type of content you want to view.



Properties

Name: Cisco Base Pack
Version: 7.3.5
Publisher: ScienceLogic, Inc.
License Key: JBPxfJ3NpSWOnp39rKZ46Apreuzv57dSI4fb43zOj4tnHLIF

Creation: em7admin [2012-06-28 10:45:50]
Modification: em7admin [2014-05-15 11:24:16]
Revision: 484
ID: 18

Description: This Power-Pack monitors Cisco CPU, environmental status, memory, and basic IOS configuration

Vendor(s) Supported: Cisco
Model(s) Supported:
Version(s) Supported:

Release Notes and Change Log

Cisco Base Pack
Edited by: ScienceLogic, Inc.
Edit Date: 2013-10-30

Version 7.3.5
1) Removed unnecessary threshold from Cisco: PIX CPU
2) Added missing sample credentials
3) Added device class

NOTE: The entries under **Contents** are dependent upon your Access Hooks. An entry appears only if you have been granted an Access Key that contains the Access Hook that allows you to view the content-type in SL1. For example, the ***Dynamic Applications*** entry will appear under the **Contents** link only if you have permission to view the list of Dynamic Applications in the **Dynamic Applications Manager** page (System > Manage > Applications) in SL1.

Chapter

2

Credentials

Overview

The following section describes how to create credentials for monitoring SNMP-enabled devices:

This chapter covers the following topics:

Creating Credentials for Monitoring SNMP-Enabled Devices 11

Creating Credentials for Monitoring SNMP-Enabled Devices

To monitor SNMP-enabled devices with SL1, you must first create an SNMP credential.

SNMP Credentials 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*.
    - ***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*.
- ***Retries***. Number of times SL1 will try to authenticate and communicate with the external device. The default value is *1*.

SNMP V1/V2 Settings

These fields appear if you selected *SNMP V1* or *SNMP V2* in the ***SNMP Version*** field. The fields are inactive if you selected SNMP V3.

- ***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. These fields are inactive if you selected SNMP V1 or SNMP V2.

- ***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. This field is required. Choices are:

    - *MD5*. This is the default value.
    - *SHA*
    - *SHA-224*
    - *SHA-256*
    - *SHA-384*
    - *SHA-512*

NOTE: The *SHA* option is SHA-128.

- ***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. This field is required. Choices are:
    - *DES*. This is the default value.
    - *AES-128*
    - *AES-192*
    - *AES-256*
    - *AES-256-C*. This option is for discovering Cisco devices only.
  - ***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 an SNMP Credential, SL1 automatically aligns the credential with all organizations of which you are a member.

Chapter 3

Discovery

Overview

The following sections describe how to discover SNMP-enabled devices:

This chapter covers the following topics:

Discovering SNMP-Enabled Devices *14*

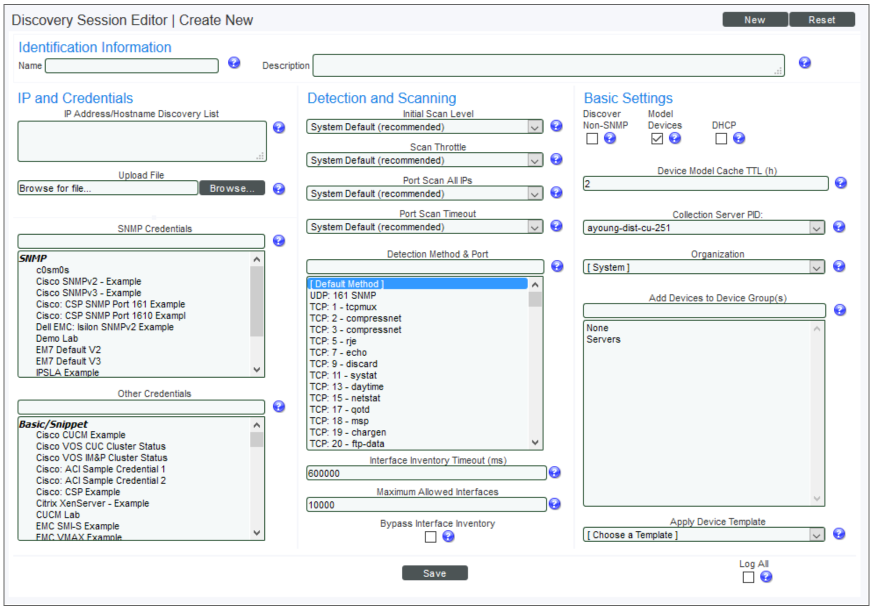
Dynamic Application and Device Class Alignment *15*

Discovering SNMP-Enabled Devices

To discover a SNMP-enabled device:

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

3. The **Discovery Session Editor** page appears. In the **Discovery Session Editor** page, supply values in the following fields:



Discovery Session Editor | Create New

Identification Information

Name

Description

IP and Credentials

IP Address/Hostname Discovery List

Upload File: Browse for file...

SNMP Credentials

SNMP
- c0sm0s
- Cisco SNMPv2 - Example
- Cisco SNMPv3 - Example
- Cisco: CSP SNMP Port 161 Example
- Cisco: CSP SNMP Port 1610 Exampl
- Dell EMC: Isilon SNMPv2 Example
- Demo Lab
- EM7 Default V2
- EM7 Default V3
- IPSLA Example

Other Credentials

Basic/Snippet
- Cisco CUCM Example
- Cisco VOS CUC Cluster Status
- Cisco VOS IM&P Cluster Status
- Cisco: ACI Sample Credential 1
- Cisco: ACI Sample Credential 2
- Cisco: CSP Example
- Citrix XenServer - Example
- CUCM Lab
- EMC SMI-S Example
- EMC VMAX Example

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: 15 - netstat
- TCP: 17 - qotd
- TCP: 18 - msp
- TCP: 19 - chargen
- TCP: 20 - ftp-data

Interface Inventory Timeout (ms): 600000

Maximum Allowed Interfaces: 10000

Bypass Interface Inventory ☐

Basic Settings

Discover Non-SNMP ☐ Model Devices ☑ DHCP ☐

Device Model Cache TTL (h): 2

Collection Server PID: ayoung-dist-cu-251

Organization: [System]

Add Devices to Device Group(s)
- None
- Servers

Apply Device Template: [Choose a Template]

Log All ☐

- *Name*. Enter a name for the discovery session. This name is displayed in the list of discovery sessions in the **Discovery Control Panel** page.
- *IP Address/Hostname Discovery List*. Provide a list of the IP addresses or fully qualified domain names of the SNMP-enabled devices you want to discover.
- *SNMP Credentials*. Select the SNMP credentials you created for the SNMP-enabled devices. You can select multiple credentials in this field.

4. Optionally, supply values in the other fields in this page. For a description of the fields in this page, see the ***Discovery & Credentials*** manual.
5. Click **[Save]**.
6. The **Discovery Control Panel** page will refresh. Click the lightning bolt icon (⚡) for the discovery session you just created.
7. In the pop-up window, click **[OK]**. The page displays the progress of the discovery session.

Dynamic Application and Device Class Alignment

SL1 automatically aligns the correct device class and Dynamic Applications to each device during discovery.

The following sections describe how SL1 aligns Dynamic Applications and device classes.

How Does SL1 Align Dynamic Applications During Discovery?

Most Dynamic Applications include a discovery object. A discovery object enables SL1 to determine which devices to align with a Dynamic Application.

During discovery, SL1:

1. Searches the list of Dynamic Applications.
2. If a Dynamic Application includes a discovery object, SL1 adds that Dynamic Application to the list of Dynamic Applications to try to align during discovery.
3. For each Dynamic Application that includes a discovery object, SL1 checks the current discovery session for an appropriate credential. For example, for each database Dynamic Application, SL1 would look for one or more database credentials that have been selected for the discovery session.
4. For each discovered device, both those that support SNMP and those that don't, discovery tries to determine which Dynamic Applications to align. For each discovered device, SL1 tries to align each Dynamic Application in the list of Dynamic Applications to try during discovery. For each Dynamic Application in the list, SL1 tries to connect to each device with each of the appropriate credentials (until SL1 finds a working credential) and then tries to find the discovery object. If SL1 is able to connect to a device with one of the credentials and can then retrieve the discovery object, SL1 will align the Dynamic Application with the device.

NOTE: SL1 also includes more sophisticated logic that allows you to define multiple discovery objects, validate the value of the discovery object, and to align the Dynamic Application if a discovery object is not available. However, the most common use of a discovery object is as described above (discovery object exists).

5. If discovery aligns a Dynamic Application with a device, immediately after discovery completes SL1 will start the first collection from that device using the aligned Dynamic Application. This step is not performed for Dynamic Applications that meet all of the following three criteria:
    - Has a collection frequency of 1 minute, 2 minutes, 3 minutes or 5 minutes.
    - Does not have component mapping enabled (does not discover component devices).
    - Is aligned with a component device.

NOTE: During discovery, SL1 tries each SNMP credential specified in the discovery session on each discovered device, to determine if SL1 can collect SNMP details from the device. Later in the discovery session, during alignment of Dynamic Applications, discovery again tries each SNMP credential specified in the discovery session. If one of the SNMP credentials times out three times ***without any response***, discovery will stop trying to use that SNMP credential to align SNMP Dynamic Applications. Note that "no response" means that a device did not respond at all. Note that if a device reports that "no OID was found" or "the end of the OID tree was reached", these are considered a legitimate response and would not cause SL1 to abandon the credential.

How Does SL1 Align Device Classes During Discovery?

Device classes determine:

- How devices are represented in the user interface
- Whether the device is a physical device or a virtual device
- How managed devices are discovered with the discovery tool

The **Device Class Editor** page (System > Customize > Device Classes) allows advanced administrators to define new or legacy device classes in SL1 and to customize properties of existing device classes.

Most TCP/IP-compliant devices have an internally-defined class ID, called the System Object ID and abbreviated to SysObjectID. This SysObjectID is an SNMP OID defined by the manufacturer. Each manufacturer specifies a SysObjectID for each different hardware model. In SL1, each SNMP device class is associated with a SysObjectID. During initial discovery, SL1 searches each device for the SysObjectID and assigns each device to the appropriate device class.

SL1 also includes device classes for devices that do not support SNMP. These device classes are associated with values returned by nmap. SL1 runs nmap against each device during discovery.

The following sections describe the types of device classes used in SL1.

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. For more information, see https://sciencelogic.com/company/legal.

ScienceLogic

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

International: +1-703-354-1010