Monitoring CheckPoint Base Pack

CheckPoint Base Pack PowerPack version 100

Table of Contents

Introduction **3**

What Does the CheckPoint Base Pack PowerPack Monitor? 4

Installing the CheckPoint Base Pack PowerPack 5

Configuration and Discovery **6**

Prerequisites for Monitoring CheckPoint Base Pack 6

Creating an SNMP Credential for CheckPoint Base Pack 7

Verifying Discovery and Dynamic Application Alignment 9

Chapter 1

Introduction

Overview

This manual describes how to monitor CheckPoint devices in SL1 using the "CheckPoint Base Pack" PowerPack.

This chapter covers the following topics:

What Does the CheckPoint Base Pack PowerPack Monitor? 4

Installing the CheckPoint Base Pack PowerPack 5

NOTE: ScienceLogic provides this documentation for the convenience of ScienceLogic customers. Some of the configuration information contained herein pertains to third-party vendor software that is subject to change without notice to ScienceLogic. ScienceLogic makes every attempt to maintain accurate technical information and cannot be held responsible for defects or changes in third-party vendor software. There is no written or implied guarantee that information contained herein will work for all third-party variants. See the End User License Agreement (EULA) for more information.

What Does the CheckPoint Base Pack PowerPack Monitor?

The "CheckPoint Base Pack" PowerPack includes an SNMP credential template that allows SL1 to access a web server on a managed device. The following Dynamic Applications are included in this PowerPack to discover, model, and monitor CheckPoint devices for configuration data and performance metrics:

- CheckPoint FileSystem Inventory
- CheckPoint FileSystem Performance
- CheckPoint: AntiBot
- CheckPoint: AntiSpam
- CheckPoint: AntiVirus
- CheckPoint: Application Control
- CheckPoint: BGP Peers
- Checkpoint: Connections
- CheckPoint: Correlation Unit
- Checkpoint: cpsemd
- CheckPoint: Device
- CheckPoint: GW: Logging
- CheckPoint: HA
- Checkpoint: Memory
- CheckPoint MGR: Gateway
- CheckPoint: MGR: Logs
- CheckPoint: MultiDisk
- CheckPoint: Processor
- Checkpoint: RAID Disks
- Checkpoint: RAID Volumes
- Checkpoint: Sensors
- CheckPoint: SmartEvent Server
- Checkpoint: Stats
- CheckPoint: Temperature
- CheckPoint: ThreatEmulation
- CheckPoint: URLfiltering

Installing the CheckPoint Base Pack PowerPack

Before completing the steps in this manual, you must import and install the latest version of the "CheckPoint Base Pack" PowerPack

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

NOTE: For details on upgrading SL1, see the relevant *SL1 Platform Release Notes*.

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*.

Chapter 2

Configuration and Discovery

Overview

The following sections describe how to configure and discover CheckPoint component devices for monitoring by SL1 using the "CheckPoint Base Pack" PowerPack:

This chapter covers the following topics:

Prerequisites for Monitoring CheckPoint Base Pack 6

Creating an SNMP Credential for CheckPoint Base Pack 7

Verifying Discovery and Dynamic Application Alignment 9

Prerequisites for Monitoring CheckPoint Base Pack

Before you can monitor CheckPoint device components in SL1, you must have the following:

- SL1 version 12.3.1 or later.
- The sample SNMP credential that is already provided with this PowerPack.
- New collector groups and the alignment of message collectors to these collector groups.

Creating an SNMP Credential for CheckPoint Base Pack

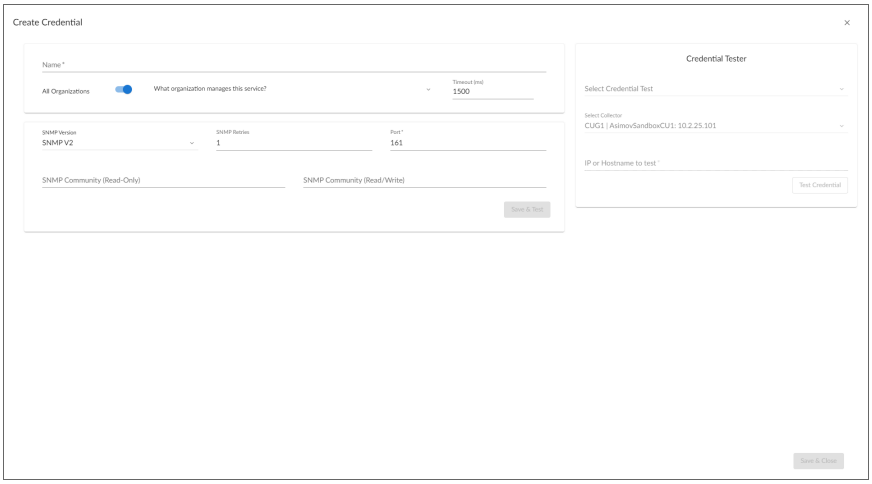
To use the Dynamic Applications in the "CheckPoint Base Pack" PowerPack, you must first define a SNMP credential in SL1. This credential allows SL1 to collect data from your CheckPoint devices.

NOTE: The PowerPack includes an example SNMP credential that you can edit for your own use.

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 **Credentials** page (Manage > Credentials).
2. Click the **[Create New]** button and then select *Create SNMP Credential*. The **Create Credential** modal page appears:



3. Supply values in the following fields:
   - ***Name***. Name of the credential. Can be any combination of alphanumeric characters, up to 64 characters. This is a required field.
   - ***All Organizations***. Toggle on (blue) to align the credential to all organizations, or toggle off (gray) and then select one or more specific organizations from the ***What organization manages this service?*** drop-down field to align the credential with those specific organizations. This field is required.

NOTE: To learn more about credentials and organizations, see the section *Aligning Organizations With a Credential*.

- ***Timeout (ms)***. Time, in milliseconds, after which SL1 will stop trying to communicate with the device. The default value is *1500*.
- ***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.
- ***SNMP Retries***. Number of times SL1 will try to authenticate and communicate with the external device. The default value is *1*.

SNMP V1/V2 Settings

If you selected *SNMP V1* or *SNMP V2* in the ***SNMP Version*** field, complete these fields. These 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.

NOTE: By default, this PowerPack uses a SNMP V2 credential.

- ***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*.
- ***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***. 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 **[Save & Close]**.

> **NOTE:** If you would like to test your credential using the **Credential Tester** panel, click **[Save & Test]**. For detailed instructions on using the **Credential Tester** panel, see the *Using the Credential Tester Panel* section.

Verifying Discovery and Dynamic Application Alignment

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

1. After creating the virtual device and aligning the credential to the template, go to the **Devices** page and click the virtual device you have previously created. From the **Device Investigator** page, click the **[Collections]** tab.
2. All applicable Dynamic Applications for the switch are automatically aligned during discovery and will appear in the **[Collections]** tab.

You should see the following Dynamic Applications aligned to the virtual device:

- CheckPoint FileSystem Inventory
- CheckPoint FileSystem Performance
- CheckPoint: AntiBot
- CheckPoint: AntiSpam
- CheckPoint: AntiVirus
- CheckPoint: Application Control
- CheckPoint: BGP Peers
- Checkpoint: Connections
- CheckPoint: Correlation Unit
- Checkpoint: cpsemd
- CheckPoint: Device
- CheckPoint: GW: Logging

- CheckPoint: HA
- Checkpoint: Memory
- CheckPoint MGR: Gateway
- CheckPoint: MGR: Logs
- CheckPoint: MultiDisk
- CheckPoint: Processor
- Checkpoint: RAID Disks
- Checkpoint: RAID Volumes
- Checkpoint: Sensors
- CheckPoint: SmartEvent Server
- Checkpoint: Stats
- CheckPoint: Temperature
- CheckPoint: ThreatEmulation
- CheckPoint: URLfiltering

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

International: +1-703-354-1010