Smart Net Total Care Service

Managed Device List Creation and Maintenance:

Discovery Guidelines and Tips

This document describes how the collector in the Cisco Smart Net Total Care™ Service discovers and gathers data from Cisco devices. It also provides guidelines and tips on how to create the managed device list and credentials that govern data collection. This document addresses both initial deployment and on-going maintenance and operation of the collector.

Introduction

Cisco® Smart Net Total Care Service delivers extensive installed base and contract management, along with foundational technical services, device diagnostics, and alerts for your Cisco products.

The Smart Net Total Care Common Services Platform Collector (CSPC) provides a data-collection mechanism for your network device information. The collector is installed on your network and performs two tasks: device discovery and installed base collection. Once the installed base data is gathered and uploaded to the Cisco data center, it is validated and analyzed with Cisco's deep knowledge base of manufacturing, contract, security, and alerts data. The results are available to network administrators and users in the secure Smart Net Total Care portal.

Figure 1 – The Smart Net Total Care discovery and data collection process

Device Discovery

All Smart Net Total Care collector deployments start by first identifying the Cisco devices that are available in your network. This is accomplished by discovering the available devices. The scope or limits of the network discovery are controlled by you during the configuration of a discovery job. You have several discovery methods to choose from.

During the discovery phase, CSPC first determines the reachability of an element via ICMP (ping). After a successful ICMP reply, the collector uses SNMP to get basic system information from the device. SNMP must be enabled on the target elements for the collector to successfully discover it.

Data Collection

The next step is to collect the detailed device information from the discovered network devices. The Cisco Service for which the collector has been deployed defines what information should be collected from a network element.

CSPC in general uses Simple Network Management Protocol (SNMP), Command Line Interface (CLI) and Simple Object Access Protocol (SOAP) to get different pieces of information from different types of network elements.

Upload to Cisco

Once the information has been collected from the devices, the collector can upload that information to Cisco for further analysis. The upload of collected data is performed over a secure channel.

This document provides guidelines and tips on how to create the credentials and managed device list during the initial deployment, and how to maintain them during ongoing operation of the Smart Net Total Care Service.

Building the Credentials

The credentials stored in the collector are a list of passwords for accessing details on each device.

Credentials are usually defined by protocol for groups of devices (for example, for a family of routers or switches, and for an IP address range or section of the network). Credentials are often periodically changed for security reasons. When credentials are changed for a device, the credentials stored in the collector must also be updated.

Creating and Editing Credentials in the Collector User Interface

Adding or updating credentials is performed through the collector user interface wizard in the **Access Credentials** section. First, select the IP addresses or address ranges of interest. Then enter or modify the credential details for each protocol. Step-by-step details are available in the CSPC Quick Start Guide.

Building the Managed Device List

What is a Managed Device List?

The managed device list is a list of the devices from which the collector will attempt to gather data. You can leverage the collector discovery feature to create the managed device list.

What is Discovery?

Discovery allows you to probe the network using a variety of user-defined methods to find the devices in your network. You can control how deep the discovery should go, to avoid unnecessarily broad network polling. During discovery, the collector will attempt to communicate with a device via SNMP.

Once the initial discovery is complete, you can also schedule discoveries to run at a regular interval to keep the managed device list up to date with changes that occur to the network, thus reducing the need for manually maintaining the device list. Below are the advantages and disadvantages of the network discovery process:

Discovery advantages:

- Can help keep track of device additions and deletions to the network, if run regularly
- Can be scheduled to run at a regular interval

Discovery disadvantages:

- Some discoveries can be time consuming, depending on the size of the customer network and the extent of the scan

Types of Discovery

There are three options for Smart Net Total Care discovery:

Known IP address discovery:

This method uses a list of known IP addresses that you manually enter in the collector user interface.

Protocol-based discovery:

This discovers the network devices by using protocols such as Cisco Discovery Protocol (CDP), and Address Resolution Protocol (ARP) protocols. Data collected from discovered devices is used to find

additional devices in the network. For protocol based discovery, you need to configure the following information:

- Protocol: Such as CDP, ARP, OSPF Neighbors, LLDP, or others
- Hop count: The number of hops the discovery process should traverse
- Seed IP address(s): The list of initial seed device or devices

Scanning a range of addresses:

This method uses SNMP to contact all the IP addresses in the range you specify. You provide the starting IP address and the ending IP address of the range.

Discovery Guidelines and Tips

Discoveries can be time consuming. SNMP timeouts, the number of SNMP community strings used, and WAN latency have the potential to slow down the overall process. In order to have a successful discovery, consider the following general guidelines and tips:

- Before running the discovery, ensure the collector has access to all of the devices to be discovered and that all devices are enabled to respond to the protocols the discovery uses. This includes configuring firewalls and access control lists (ACLs) to allow SNMP requests. Verify SNMP community strings are correct.

  Note: CDP is enabled on IOS devices by default; however, many customers disable CDP for security reasons.

- There is no way to determine if the discovery has reached all the devices on a network. You will still need to know the general quantity of devices on each subnet in order to provide a tangible goal or stopping point.
- If a device does not respond to SNMP then it cannot be discovered. For example, IP phones are not capable of responding to SNMP, thus they cannot communicate directly with Smart Net Total Care. Data on IP phones can be collected from the Cisco Unified Communications Manager to which they are registered. In a similar manner, information from wireless access points is provided through the wireless LAN controller that is managing them.
- If CLI-based discovery is specified, SSH, Telnet or NMAP must be properly configured.
- Before running a discovery, SNMP credentials, such as the read-only community string, must be provided.
- In general, providing more SNMP community strings leads to a longer discovery process. It is good practice to standardize the SNMP community strings in the network to minimize the overall discovery time.

How to Run a Discovery

Detailed instructions on how to run a discovery process are available on the Smart Net Total Care portal in the Add Devices, Credentials and Run Collection How-To video for customer administrators and in the CSPC User Guide.

Maintaining the Managed Device List

Your managed device list must be maintained and kept up to date with changes that occur in the network. You have the responsibility to maintain the managed device list during ongoing collection and maintenance.

Generally, there are four types of changes that need to be addressed:

- Credential changes
- Removed devices
- Added devices
- Moved devices

If previously managed devices are removed from your network, the CSPC will not automatically delete them. They will instead be marked as “unreachable” until you manually delete them from the CSPC.

You have a couple of options for keeping the managed device list up to date:

- Updating the managed device list with information from a network management system.

  If you maintain an up-to-date device list in your network management system, such as Cisco Prime LMS, you can export the device list from the network management system and load it into the collector. Refer to the Updating the Collector Managed Device List How-To videos for customer administrators for detailed instructions.

- Schedule discoveries to run on a regular basis.

  If you do not have an up-to-date device list in your network management system, you can schedule discoveries to run at a regular interval to keep the managed device list up to date. Discovery can be scheduled weekly, monthly, or quarterly. You can also schedule discoveries on a specific day or time. As part of the discovery process, you must correct credential changes and any access issues between the collector and the devices in the network, such as ACLs and firewall changes, which may occur periodically.

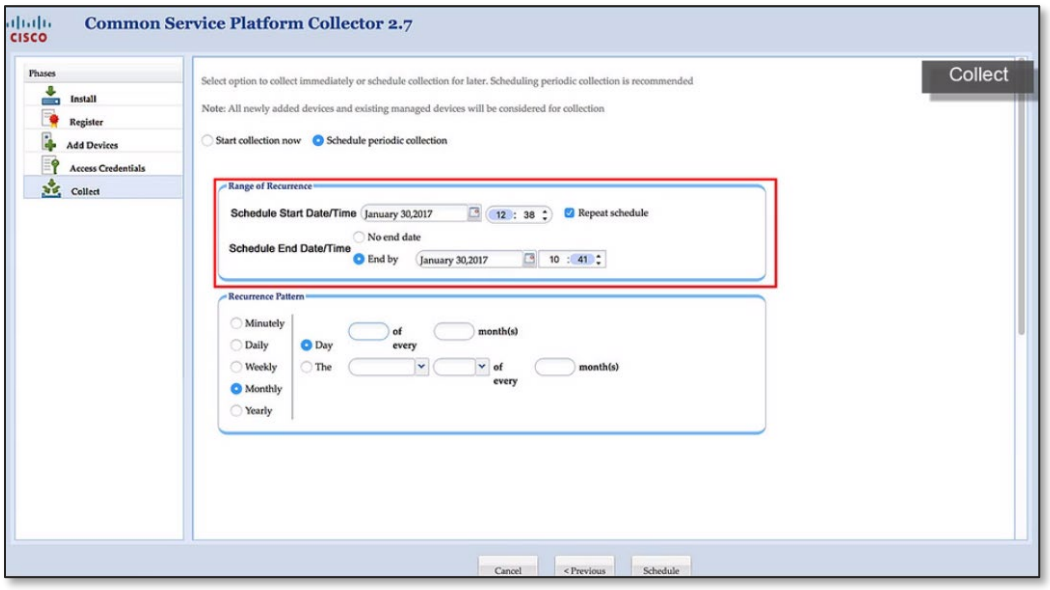

Figure 2 – scheduling regular discovery

.

Things to Consider

No collector can guarantee that it will discover, collect data from, and report on every device on your network. There may be several reasons for this:

- Not all devices are discoverable. The CSPC collector uses SNMP for discovery and basic collection. If your device does not support SNMP, or you have not enabled SNMP on the device, it won't be found and no data will be collected.
- Devices that are behind a company firewall or are in other secure segments of your network will not be discovered.
- Discovery and collection processes may time out because the device is busy with other activities and does not respond within the time allotted. Therefore, data from an active device may not be collected.
- The Smart Net Total Care portal may not report on all the devices that the collector gathers. Additional processing is required for the portal to analyze and display the data from the collector. For example, newly released Cisco devices or device updates may take some time to be supported by the portal software..
- You may not want to discover all the devices on all the segments of your network. You can control and limit the range of collection. There are several ways to do this, but if you choose to limit discovery, the devices not included in the range you specify will not be discovered and no device data will be collected for them.
- You must provide the necessary credentials for the protocols you choose to use for discovery and collection. To maximize the effectiveness of the Smart Net Total Care Service, the device list and credentials must be maintained and kept up to date with changes that occur in your network. If you change credentials on your network devices, you must update the information in the collector.

- Devices must be attached to your network and operational to be discovered. If you have spares that are not powered on or not connected to your network but that you consider as part of your inventory, they will not be included in the portal inventory reports.

Summary

Cisco Smart Net Total Care Service provides valuable information about your installed base and contracts that can help you improve risk management, resolve problems quickly, and reduce operating expenses. The managed device list and credentials that provide this valuable data must be created and kept up-to-date. You should review the material in this application note and decide on the methods that work best for your company and network.

Resources

Refer to these resources for details about Smart Net Total Care discovery and maintenance:

How To video – Add Devices, Credentials and Run Collection

How To video – Updating the Collector Managed Device List

CSPC Quick Start Guide

CSPC User Guide

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA 09/20