Common Services Platform Collector Overview

Updated November 2021

Contents

Introduction

This document provides a high-level overview of the Cisco® Common Services Platform Collector (CSPC). Afterreading this document, you should be able to understand what functions it can perform. Additionally, you will learn how the CSPC keeps data secure in its local storage, and when transmitting the data for further processing.

Highlights

- The three main tasks of CSPC are network discovery, data collection, and data upload
- Security is of utmost importance to Cisco, and proper steps have been taken to ensure security in CSPC
- Deploying CSPC provides resource efficiency and the quick addition of other related Cisco services

What is the CSPC?

Common Services Platform Collector (CSPC) is a software package. It is modular and flexible software that canbe expanded to enhance its basic functions by use of various additional modules.

You can run CSPC software on Linux and Windows platforms. Some services within Cisco use the CSPC on Linux, and other services use it on Windows, based on their requirements. CSPC for Linux is made into an appliance by hardening the Linux operating system and then distributing CSPC as an appliance along with thehardened Linux.

Cisco distributes CSPC software as an OVA package for installation on a hypervisor such as VMWare ESX, or asan ISO image to be installed on an x86 server for Microsoft Hyper-V. Figure 1 shows the different software components of CSPC.

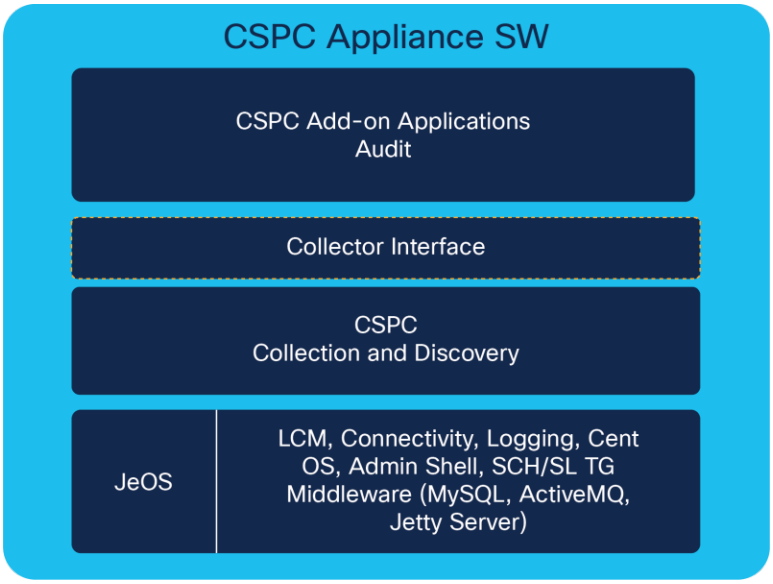

Figure 1.
CSPC software components

Additional modules

CSPC is a modular software package. Depending on the needs of a particular service, extra modules can beinstalled within CSPC to augment its functionality. Each module is called an “add-on” in CSPC.

Why is CSPC needed?

CSPC’s basic function is to discover the network elements and collect information from those elements. Anetwork element is any manageable logical entity on the network. A physical device can have one or morenetwork elements. Conversely, a network element can span across more than one physical device.

The information collected from network elements by CSPC is then transferred to the respective service portals.Cisco Smart Services are Software-as-a-Service (SaaS) types of services offered through a web portal. The portal uses the information uploaded by CSPC, along with Cisco intellectual capital, to generate different typesof assessments, reports, and recommendations.

CSPC operation

CSPC performs three distinct tasks to enable the services for which it is deployed. These tasks include:

- Network discovery
- Data collection
- Data upload

Network discovery

Network discovery is an operation in which CSPC discovers what devices are present in a network segment. The scope or limits of the network discovery are controlled by the user during the configuration of a discoveryjob. There are several methods available to crawl through network segments to find the network elements present. These methods include:

- Known IP addresses
- A range of IP addresses
- Layer 2/3 neighbors up to 15 hops

During the discovery phase, CSPC first determines the reachability of an element via Internet Control MessageProtocol (ICMP); ping). After a successful ICMP reply, CSPC uses Simple Network Management Protocol (SNMP) to get basic system information from that element. SNMP must be enabled on the target elements for CSPC to successfully discover them. During the discovery, CSPC uses the RFC-1213 MIB to poll for basic system information.

Data collection

Data collection is an operation in which CSPC collects specific information from a discovered network element.The Cisco service for which the collector has been deployed defines what information is collected from a network element. These definitions of what should be collected from what type of device are referred to as collection profiles in CSPC.

Cisco supplies these collection profiles based on the needs of a specific service. Collection profiles can be runon demand, or they can be programmed to run on a regular schedule.

CSPC uses SNMP, Command-Line Interface (CLI), and Simple Object Access Protocol (SOAP) to get differentpieces of information from different types of network elements.

Cisco maintains a list of commands that CSPC uses for a particular service to collect information from networkelements.

Data upload

Once the information has been collected from the network elements, CSPC uploads that information to Ciscofor further analysis. The destination of the information uploaded is dependent upon the service for which the CSPC is deployed. The upload of collected data is performed over a secure channel.

Required credentials

To perform the network discovery and data collection operations, CSPC needs the following credentials:

- SNMP read-only community string
- Telnet or SSH credentials
- HTTP or HTTPS credentials

Not every device needs to be accessed via CLI or SOAP; however, SNMP is required for all devices.

Security in CSPC

CSPC is placed in a customer's trusted network segment and collects inventory and configuration informationfrom the network elements. Security is of utmost importance to Cisco and proper steps have been taken to ensure security in CSPC.

Host security

As mentioned earlier, for some services CSPC is provided as an appliance that includes CSPC application software and the Linux operating system. The Linux operating system is hardened by removing any unnecessary services and by blocking general-purpose computing operations. The operating system is hardened according to the United States National Security Administration (NSA) guidelines for Linux operatingsystems and Cisco internally developed best practices.

Device credentials

All device passwords and SNMP community strings are encrypted with an AES-256 key before storage in thelocal database within CSPC. Device credentials stored in CSPC are never uploaded to Cisco.

Collected data

Collected data from network elements is stored in the local SQL database. The collected data is not storedencrypted, but a robust set of masking operations exists such that any portion of the data collected from adevice can be masked before insertion into the CSPC database or before upload to Cisco.

Data masking

A data-masking capability is provided within CSPC so that it can hide sensitive information being stored locallyor uploaded to Cisco. Cisco supplies a default set of rules in CSPC to mask credentials, certificates, and other common sensitive fields. Users can enhance these rules if desired.

Data privacy

Data privacy is another capability that enhances the existing, end-to-end security features of CSPC. This functionality enables users to map collected IP addresses and/or hostname fields to different values before theyare sent to the Cisco data center.

Data upload

CSPC uploads data to Cisco over a secure and encrypted channel. An IPsec tunnel is the preferred method ofuploading the data. In cases where IPsec is not possible, CSPC will then use SSL (HTTPS) to upload the data.

A common collector

As the name implies, CSPC is a collector that can be used by different services. These services range from support to optimize to operate. Not only can the same software be used by different services, but if a customer has multiple services, they can use the same collector to collect data for the different services. The data collected for a support service is mainly the installed base information, whereas an optimize service would require feature configurations and the like. Different collection jobs are programmed in CSPC to meet the needsof different services. However, network discovery needs to be run only once for all these different services, saving time and bandwidth for customers.

Multiple services capability

CSPC can be used by multiple services within a customer network. Deploying CSPC gives Cisco the ability toturn up additional services quickly, while providing the customer with the benefit of resource efficiency.

A CSPC can be loaded up with the extra add-ons that a customer might need at a later time. Processed and finished reports are available only in service portals, and access to those portals is controlled via registration. Therefore, having a CSPC at a customer site with extra add-ons does not enable the customer to use servicesfor which they are not entitled.

Figure 2 highlights how CSPC can enable different Cisco services by collecting data from the network andsecurely uploading that data to the Cisco data center.

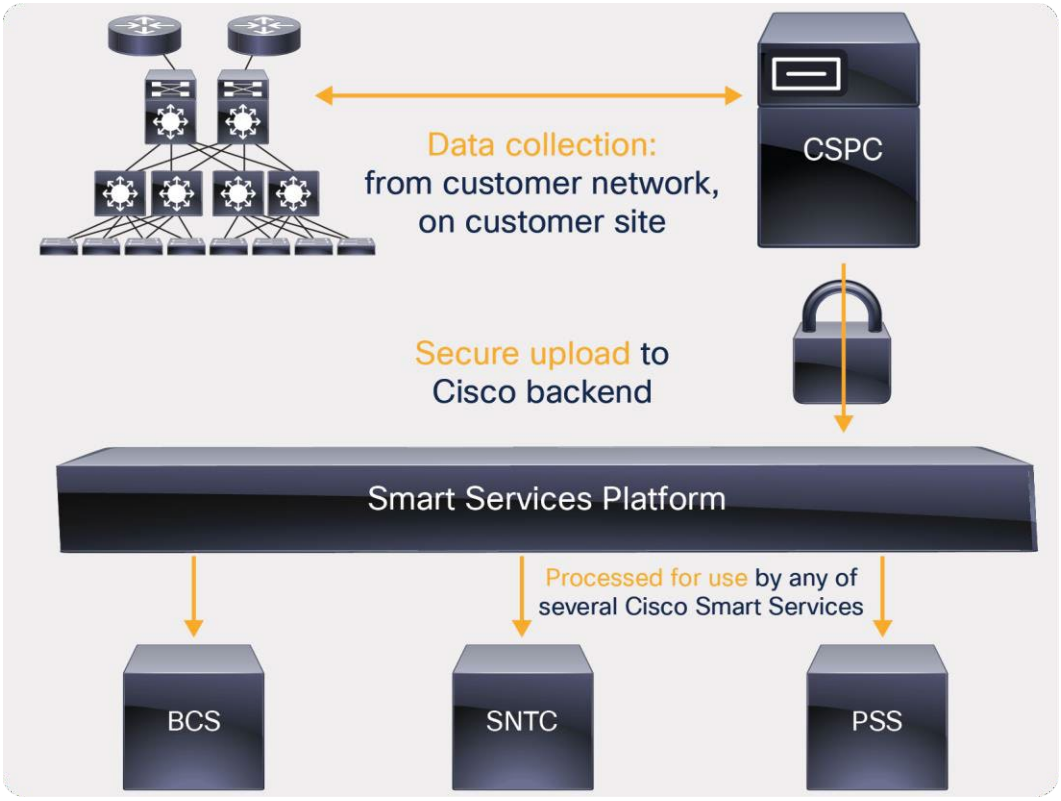

Figure 2.
Multiple services enabled by CSPC

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 **https://www.cisco.com/go/offices**.

Printed in USA C11-744792-00 11/21