Common Services Platform Collector Overview

Introduction

This document is a high level overview of the Common Services Platform Collector (CSP-C). The intended audience of this document is Cisco personnel and customers. After reading this document, the reader should be able to understand what the CSP-C is and what functions can it perform for different services offered by Cisco. Additionally, the reader should also learn about how the CSP-C keeps data secure in its local storage, and when transmitting the data for further processing.

What is the CSP-C

Common Services Platform Collector, commonly referred to by its acronym CSP-C, is a software package. It is modular and flexible software that can be expanded to enhance its basic functions by use of various additional modules.

You can run CSP-C software on Linux and Windows platforms. Some services within Cisco use the CSP-C on Linux, and other services use it on Windows, based on their needs. The services that have decided to use Linux platform have also opted to make the CSP-C into an appliance by hardening the Linux operating system and then distributing the CSP-C as an appliance along with the hardened Linux.

Highlights

- CSP-C can run on Windows or Linux
- The three main tasks of the CSP-C 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 CSP-C
- Deploying the CSP-C provides resource efficiency and quick addition of other related Cisco Services
Cisco distributes the CSP-C appliance as an ISO to be installed on an x86 server, or as an OVF package for installation on a hypervisor such as VMWare ESX or Microsoft Hyper-V. Figure 1. shows the different software components of the CSP-C.

**Figure 1.** Software Components of the CSP-C

Additional Modules

As mentioned earlier, the CSP-C is a modular software package. Depending on the needs of a particular service, extra modules can be installed within the CSP-C to augment its functionality. Each module is called an “Add On” in CSP-C.

**Why is CSP-C needed**

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

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

**CSP-C Operation**

The CSP-C performs three distinct tasks to enable the services for which it is deployed. These tasks are:

- Network Discovery
- Data Collection
- Data Upload
Network Discovery

Network Discovery is an operation in which the CSP-C finds out 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 discovery job. There are several methods available to crawl through the network segments to find the network elements present. These methods are:

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

During the discovery phase, the CSP-C first determines the reachability of an element via ICMP (ping). After successful ICMP reply, the CSP-C uses SNMP to get basic system information from that element. SNMP must be enabled on the target elements for CSP-C to successfully discover it. During the discovery the CSP-C uses the RFC-1213 MIB to poll for basic system information.

Data Collection

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

Cisco supplies these collection profiles based on the needs of a specific service. Collection profiles can be run on demand, or programmed to run at a later time.

The CSP-C 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.

Cisco maintains a list of commands that a CSP-C can use to collect information from network elements. Contact your Cisco account executive for a copy of this list.

Data Upload

Once the information has been collected from the network elements, the CSP-C can upload that information to Cisco for further analysis. The destination of the information uploaded is dependent upon the service for which the CSP-C is deployed. The upload of collected data is performed over a secure channel. An IPsec tunnel is the preferred method of uploading the data. In case IPsec is not possible, the CSP-C will then use the SSL (HTTPS) to upload the data.

Required credentials

To perform the Network Discovery and Data Collection operations the CSP-C needs the following credentials:

- SNMP Read Only community
- 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 the CSP-C

The CSP-C is placed in a customer’s trusted network segment and collects very sensitive information from the network elements. Security is of utmost importance to Cisco and proper steps have been taken to ensure security in the CSP-C.

Host security

As mentioned earlier, for some services the CSP-C is provided as an appliance that includes the CSP-C 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 operating systems and Cisco internally developed best practices.

Device Credentials

All device passwords and Simple Network Management Protocol (SNMP) community strings are encrypted with an AES-256 key before storage in the local database within the CSP-C. Device credentials stored in the CSP-C are never uploaded to Cisco.

Collected Data

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

Data Masking

Data-masking capability is provided within the CSP-C so that it can hide the sensitive information from being stored locally or uploaded to Cisco. Cisco supplies default set of rules in CSP-C 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 the CSP-C. This functionality enables users to map collected IP addresses and/or hostname fields to different values before being sent to the Cisco data center.

Data Upload

The CSP-C uploads data to Cisco over a secure and encrypted channel. An IPsec tunnel is the preferred method of uploading the data. In cases where IPsec is not possible, the CSP-C will then use SSL (HTTPS) to upload the data.
A Common Collector

As the name implies, the CSP-C 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 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 a CSP-C to meet the needs of different services. However, the network discovery needs to only be run once for all these different services, saving time and bandwidth for customers.

Multiple Services Capability

The CSP-C can be used by multiple services within a customer network. Deploying the CSP-C gives Cisco the ability to turn up additional services quickly, while providing the customer with the benefit of resource efficiency.

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

Figure 2. highlights how the CSP-C can enable different Cisco Services by collecting data from the network and uploading securely to Cisco data center.

Figure 2. Multiple Services Enabled by CSP-C
References

CSP-C Quick Start Guide

CSP-C supported device list