White paper
Cisco public

Cisco Operational Insights Collector

Efficient and Versatile Data Collection

September 2023

Contents

Introduction

Operational Insights Collector (OIC) is a powerful network data collection application that enables Cisco® to collect relevant data. The data collected by OIC is used to support Operational Insights reporting and other related services. Cisco engineers rely on accurate and up-to-date reporting to help them make better recommendations to Cisco customers.

Basic architecture

OIC provides connection support for third-party Network Management Systems (NMS) and Cisco Business Entity (BE) controllers. The data are then exported to the Cisco cloud through a secured API.

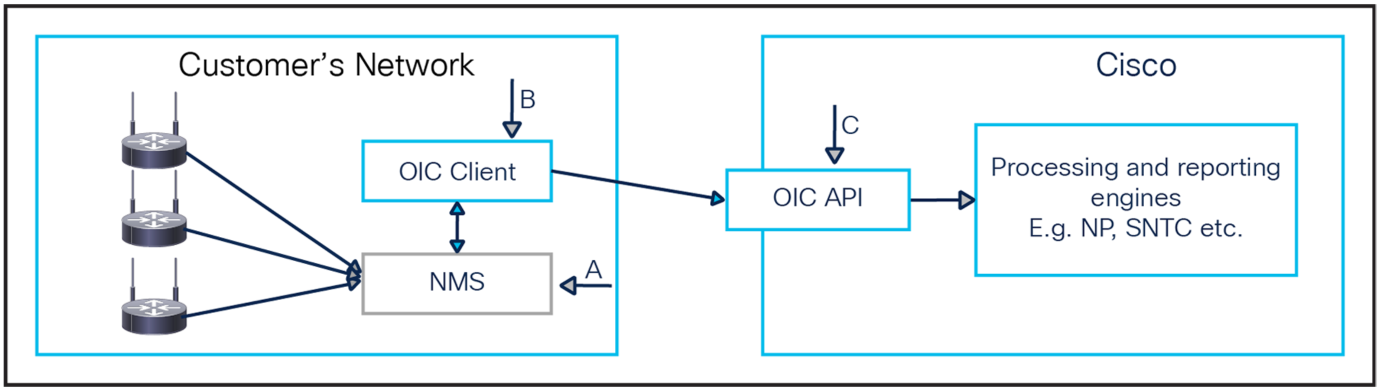

Figure 1.
OIC architecture

OIC leverages a Network Management System ("A" on Figure 1) or Cisco controllers, already installed on the network, to collect the data. It is a full software solution, made of two main components:

- **Client side ("B" on Figure 1):** An OIC Client application is installed on the customer's network. It is responsible for collecting the data through an NMS or a Cisco BE controller.
- **Backend side ("C" on Figure 1):** OIC exposes an API to let a client push the collected data to the Cisco cloud. The data are then formatted and routed to provide reports.

Customers using a non supported NMS or who want to own the collection process end to end can use the OIC Software Development Kit (SDK). The OIC SDK enables customers to develop and use custom software connections to upload their data through the OIC API.

Deployment model

OIC is flexible and can be deployed in either of the following ways:

- **Standalone application:** OIC can run by itself. This is usually possible if the NMS covers the whole network.
- **Parallel deployment:** OIC can be deployed in parallel to an existing implementation of Common Services Platform Collector (CSPC), if CSPC does not cover all technologies (like EPNM, ACI®, SD-WAN, etc.).

Operating model

OIC is designed to adapt to the customer's environment and can support multiple connection mechanisms. This allows Cisco to choose the operating models that best suit the customer's needs and infrastructure.

- **Network Management Systems:** One of the connection mechanisms supported by OIC is NMS. OIC can connect to popular NMS solutions such as SolarWinds, Science Logic, and HPNA. This allows customers to use their existing NMS to collect and transmit data to the OIC, streamlining the data collection process.
- **Cisco Business Entity Controllers:** OIC supports Cisco BE controllers such as APIC, ACI, and EPNM. By connecting to BE controllers, OIC can collect data from Cisco devices directly.
- **Software Development Kit:** In addition to these operating models, OIC also offers SDK. The SDK allows customers to develop and use custom software connections to the OIC API to push data to Cisco. This is particularly useful for customers that do not have third-party NMS or Cisco BE controllers, as it enables them to collect and transmit data to the OIC using their own software.

Security with OIC

Security is of the utmost importance to Cisco, and proper steps have been taken to ensure security in OIC.

Device credentials

OIC does not need to collect customer's device credentials, adding an immediate level of security to the customer's network.

Data masking

OIC has the capability to mask data so that it can hide sensitive information. Cisco supplies a default set of rules in OIC to mask credentials, certificates, and other common sensitive fields. In addition, OIC collects the IP addresses of the customer's devices, and these will be masked to address a customer's security and privacy concerns.

Collected data

The data collected by OIC primarily depend on the NMS in picture. However, OIC broadly collects the following data from the customer's NMS/Cisco controllers:

- Show commands via command line interface
- SNMP data
- Config data

The data collected by OIC are not stored by the OIC backend, but are sent straight to the consuming engine within Cisco using authentication/authorization – TLS 1.2-based security used for the transport protocol.

The following are the geo locations for current storage at Cisco:

- EMEA data -> EMEA NetProfile
- US and APJC data -> US NetProfile

It should be noted that only the passwords for OIC applications are encrypted in the config file. There is no other encryption, as OIC does not store any other data. Additionally, only the Cisco engineer who created the Company Key has access to that customer’s data.

Software security

OIC is Cisco Secure Development Lifecycle (CSDL) approved. CSDL is a Cisco process that reviews software for security risks, data privacy, and third-party licensing compliance.

OIC has undergone stringent security reviews, as code quality and dependencies were analyzed throughout the development process. More details on CSDL are available here.

OIC has undergone the following scans:

- BAVA
- Corona
- BlackDuck
- CSE
- SonarQube scans

Installing OIC

OIC supports multiple deployment options, such as Docker, VM, multi-OS, and more.

The customer must provision a user account that has access to the NMS/Cisco controller to integrate OIC with it.

The customer must also ensure connectivity from OIC to NMS and from OIC to the Cisco backend for flow of data, using the following ports: port 443 – api.cisco.com and cxd.cisco.com.

Benefits of OIC

Overall, OIC offers a lot of advantages, including:

- **Better coverage:** OIC enables data collection from Cisco technology not currently served by CSPC, such as ACI, SD WAN, and EPNM.
- **Reduced security concerns:** OIC collects data from NMS without "touching" customer devices. Customers need not share their device credentials and have complete visibility into what data are collected and when.
- **Faster time to value:** OIC can be deployed and become operational in days. Upgrading to the latest OIC version takes less than an hour.
- **Less resource consumption:** OIC reduces customer involvement by removing the need for security audits and hardware maintenance.

For more information, please contact us at astools-support-techleads@cisco.com.

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

C11-3666058-00 09/23