

Utilice el dispositivo de telemetría de tráfico (TTA) y Cisco DNA Center App Assurance: el porqué y el cómo

Contenido

[Introducción](#)

[Prerequisites](#)

[Garantía de aplicación](#)

[Visibilidad de la aplicación \(AppVis\)](#)

[Experiencia con las aplicaciones \(AppX\)](#)

[¿Por qué un dispositivo de telemetría de tráfico?](#)

[Detalles del dispositivo TTA](#)

[Requisitos previos para la garantía de Cisco DNA Center](#)

[Clúster de Cisco DNA Center operativo](#)

[Integración de ISE y Cisco DNA Center](#)

[Requisitos de Cisco DNA Center para la telemetría](#)

[Paquetes de claves de Cisco DNA Center](#)

[Cisco DNA Center como recopilador de telemetría](#)

[La nube de IA de Cisco](#)

[La nube de reconocimiento de aplicaciones basadas en la red \(NBAR\)](#)

[CBAR \(reconocimiento de aplicaciones basadas en controlador\) y SD-AVC](#)

[Conector de nube de Microsoft Office 365 \(no es obligatorio\)](#)

[Implementación de TTA](#)

[Descripción general de TTA Workflow](#)

[Implementación de TTA: Diagrama de alto nivel](#)

[Requisitos de licencia y software de TTA](#)

[Incorporación de TTA y configuración de día 0](#)

[Adición del dispositivo TTA al inventario de Cisco DNA Center](#)

[configuración de SPAN](#)

[Garantía recopilada](#)

[Verificación](#)

Introducción

Este documento describe la plataforma Cisco DNA Traffic Telemetry Appliance (número de pieza de Cisco DN-APL-TTA-M) junto con cómo habilitar Application Assurance en Cisco DNA Center. ITambién arroja algo de luz sobre cómo y dónde se puede posicionar el TTA en una red junto con el proceso de configuración y verificación. En este artículo también se abordan los diversos requisitos previos.

Prerequisites

Cisco recomienda que conozca cómo funcionan Cisco DNA Center Assurance y Application Experience.

Garantía de aplicación

Assurance es un motor de análisis y recopilación de datos de red multifuncional y en tiempo real que puede aumentar significativamente el potencial empresarial de los datos de red. Assurance procesa datos de aplicaciones complejas y presenta las conclusiones en los paneles de estado de Assurance para proporcionar información sobre el rendimiento de las aplicaciones utilizadas en la red. Dependiendo de dónde se recopilen los datos, puede ver algunos o todos los elementos siguientes:

- Nombre de aplicación
- Rendimiento de procesamiento
- Marcas DSCP
- Indicadores de rendimiento (latencia, fluctuación y pérdida de paquetes)

En función de la cantidad de datos recopilados, Application Assurance se puede clasificar en dos modelos:

- Visibilidad de la aplicación (AppVis) y
- Experiencia con las aplicaciones (AppX)

El nombre de la aplicación y el rendimiento se conocen colectivamente como métricas cuantitativas. Los datos para las métricas cuantitativas provienen de la habilitación de la Visibilidad de la aplicación.

Las marcas DSCP y las métricas de rendimiento (latencia, fluctuación y pérdida de paquetes) se conocen colectivamente como métricas cualitativas. Los datos para las métricas cualitativas provienen de la habilitación de Application Experience.

Visibilidad de la aplicación (AppVis)

Los datos de visibilidad de la aplicación se recopilan de los switches que ejecutan Cisco IOS® XE y de los controladores inalámbricos que ejecutan AireOS. Para los switches que ejecutan Cisco IOS XE, los datos de visibilidad de la aplicación se recopilan mediante una plantilla NBAR predefinida que se aplica bidireccionalmente (entrada y salida) a los puertos de switch de acceso de capa física. En el caso de los controladores inalámbricos que ejecutan AireOS, los datos de visibilidad de la aplicación se recopilan en el controlador inalámbrico y, a continuación, se utiliza la telemetría de transmisión para transportar estos datos al Cisco DNA Center.

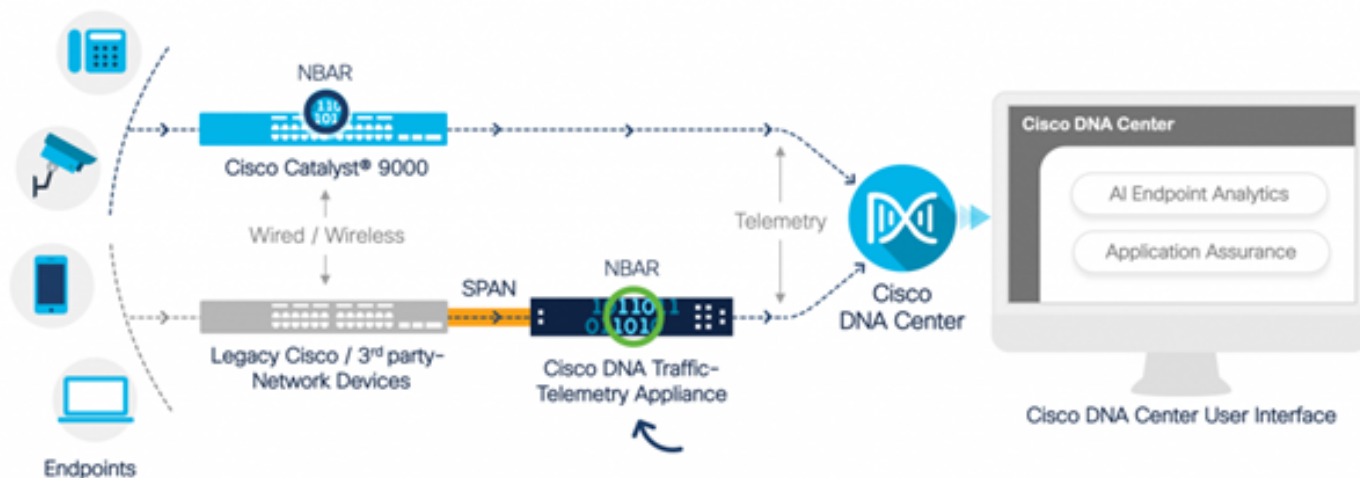
Experiencia con las aplicaciones (AppX)

Los datos de Application Experience se recopilan de las plataformas del router Cisco IOS XE, en

concreto, mediante la función Cisco Performance Monitor (PerfMon) y las métricas de Cisco Application Response Time (ART). Entre los ejemplos de plataformas de router se incluyen ASR 1000, ISR 4000 y CSR 1000v. Para obtener información sobre la compatibilidad de dispositivos con Cisco DNA Center, consulte la [Matriz de compatibilidad de Cisco DNA Center](#).

¿Por qué un dispositivo de telemetría de tráfico?

Los dispositivos por cable e inalámbricos Cisco Catalyst serie 9000 realizan una inspección profunda de paquetes (DPI) y proporcionan flujos de datos para servicios como Cisco AI Endpoint Analytics y Application Assurance en Cisco DNA Center. Pero, ¿qué sucede si no hay dispositivos Catalyst serie 9000 en la red de los que extraer la telemetría? Varias organizaciones aún tienen una parte de su infraestructura de red que no se ha migrado a las plataformas Cisco Catalyst serie 9000. La plataforma Catalyst 9000 genera telemetría de AppVis, pero para obtener información adicional de AppX, el dispositivo de telemetría de tráfico DNA de Cisco se puede utilizar para salvar la brecha. El objetivo de la TTA es supervisar el tráfico que recibe a través de los puertos SPAN de otros dispositivos de red que no tienen la capacidad de proporcionar datos de Application Experience a Cisco DNA Center. Dado que los dispositivos de infraestructura heredados no pueden realizar la inspección profunda de paquetes necesaria para los análisis avanzados, el dispositivo de telemetría de tráfico DNA de Cisco se puede utilizar para generar telemetría de AppX a partir de implementaciones heredadas existentes.



Cisco TTA en acción

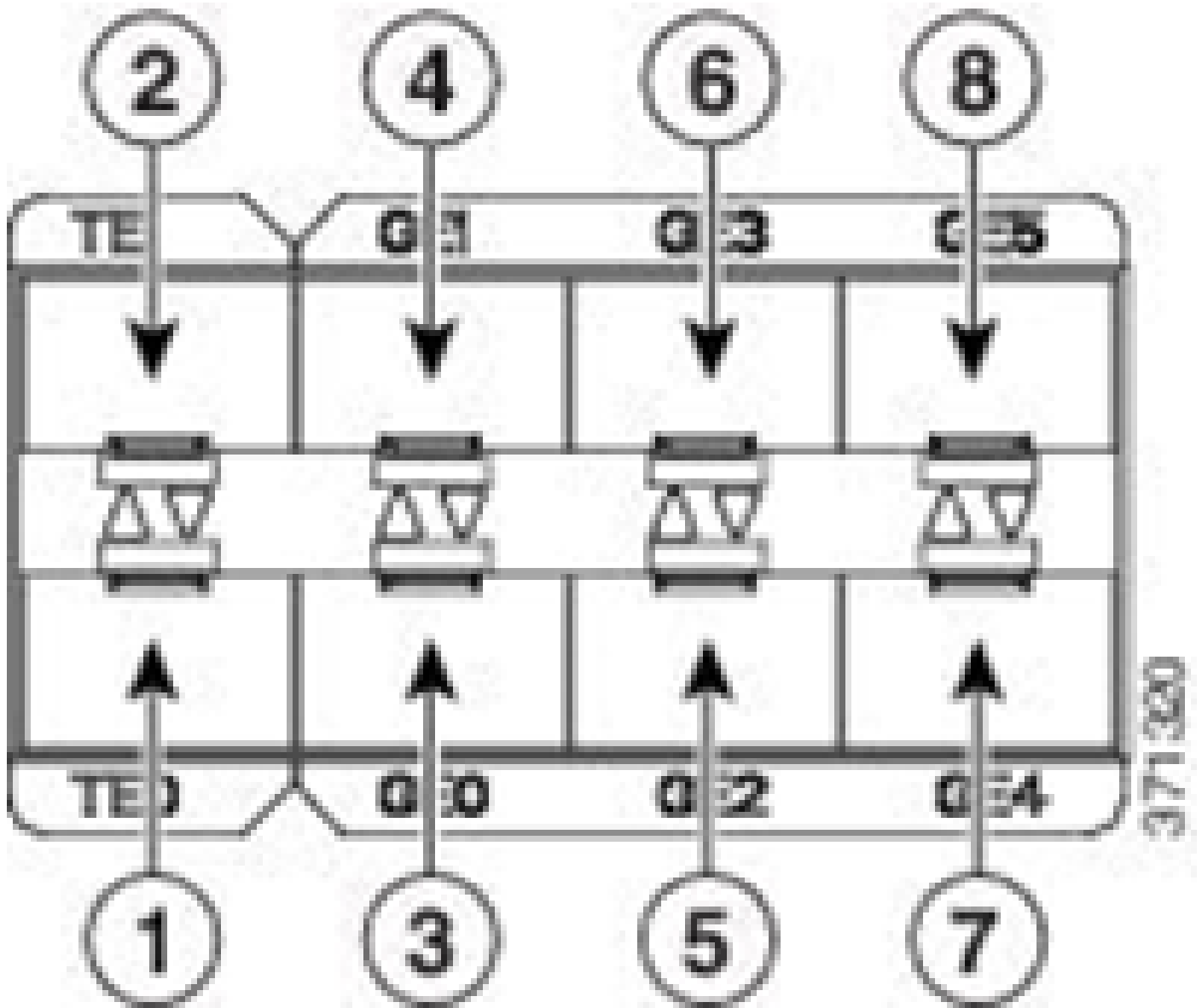
Detalles del dispositivo TTA

La plataforma del sensor de telemetría basada en Cisco IOS XE genera telemetría a partir del tráfico de red IP reflejado de las sesiones de analizador de puerto conmutado (SPAN) de switches y controladores inalámbricos. El dispositivo inspecciona miles de protocolos mediante la tecnología Network-Based Application Recognition (NBAR) para generar un flujo de telemetría para que Cisco DNA Center realice análisis. El dispositivo de telemetría de tráfico DNA de Cisco puede gestionar un tráfico de rendimiento sostenido de 20 Gbps e inspeccionar 40 000 sesiones de terminales para la definición de perfiles de dispositivos.



El dispositivo de telemetría de tráfico de Cisco

El TTA tiene una mezcla de links de 10 Gig y 1 Gig que se utilizan para la ingestión de SPAN. De estos puertos, Gig0/0/5 es el único puerto que se puede configurar con una dirección IP y que se puede utilizar para comunicarse con Cisco DNA Center. La matriz de la interfaz se muestra a continuación.



Matriz de interfaz TTA

Matriz de interfaz TTA	
1 Puerto 10 GE SFP+ 0/0/0	5 Puerto GE SFP 0/0/2
2 Puerto 10 GE SFP+ 0/0/1	6 Puerto GE SFP 0/0/3
3 Puerto GE SFP 0/0/0	7 Puerto GE SFP 0/0/4
4 Puerto GE SFP 0/0/1	8 Puerto GE SFP 0/0/5

Requisitos previos para la garantía de Cisco DNA Center

En esta sección se destacan las configuraciones y los requisitos previos que deben cumplirse antes de que Cisco DNA Center pueda procesar la telemetría.

Clúster de Cisco DNA Center operativo

El clúster de Cisco DNA Center utilizado para administrar la TTA y la telemetría de procesos debe aprovisionarse con estos criterios:

- **Jerarquía de red:** La sección Jerarquía de red del flujo de trabajo de diseño se utiliza para definir distintos campus del sitio, edificios dentro de esos campus y los pisos individuales dentro de esos edificios y mostrarlos en un mapa del mundo. Se debe configurar la jerarquía de red/sitio adecuada.
- **Configuración de red:** La sección Network Settings (Parámetros de red) permite crear parámetros de red predeterminados comunes que utilizarán los dispositivos de la red. Estos ajustes se pueden aplicar de forma global, así como en cada sitio, edificio o planta. Introduzca la información de DNS, nombre de dominio, registro del sistema, NTP, zona horaria e información de inicio de sesión según lo requiera la implementación.
- **Credenciales del dispositivo:** Estas credenciales se utilizarán para acceder y detectar dispositivos en la red, incluida la TTA. Es necesario que Cisco DNA Center esté configurado con las credenciales CLI, WAN y SNMP adecuadas. Junto con estas credenciales de NetConf es bueno tener.
- **Cuenta de Cisco CCO:** se necesita una cuenta de CCO válida para conectar el dispositivo y aprovechar las capacidades de la nube de IA de Cisco, descargar imágenes para SWIM y descargar paquetes de protocolo para TTA y otros dispositivos.

Integración de ISE y Cisco DNA Center

Cisco Identity Services Engine (ISE) y Cisco DNA Center pueden integrarse para la automatización de políticas e identidades. ISE también se utiliza para recopilar información sobre los terminales y aprovechar así Cisco AI Endpoint Analytics. PxGrid se utiliza para implementar la integración entre ISE y Cisco DNA Center.

Los requisitos de integración de Cisco DNA Center e ISE son los siguientes:

- El servicio pxGrid debe estar habilitado en ISE.
- El acceso de lectura/escritura ERS debe estar habilitado.
- El certificado de administración de ISE debe contener la dirección IP o FQDN de ISE en el nombre del sujeto o en el campo SAN.
- El certificado del sistema Cisco DNA Center debe contener todas las direcciones IP o FQDN de Cisco DNA Center en el nombre del sujeto o en el campo SAN.
- Las credenciales de administrador de ISE ERS se utilizarán para establecer con confianza la comunicación ERS entre ISE y Cisco DNA Center.
- El nodo pxGrid debe ser accesible desde Cisco DNA Center.

Requisitos de Cisco DNA Center para la telemetría

Existen requisitos que deben implementarse para habilitar la garantía de aplicaciones en Cisco DNA Center. Estos requisitos se explican con detalle en las siguientes secciones.

Paquetes de claves de Cisco DNA Center

Cisco DNA Center requiere la instalación de estos tres paquetes para habilitar y analizar los datos de telemetría.

- Análisis de terminales de IA
- Análisis de red de IA
- Servicios de visibilidad de aplicaciones

Cisco DNA Center

Version 2.1.2.0

[Release Notes](#)

[v Packages](#)

Access Control Application	2.1.260.62555
AI Endpoint Analytics	1.2.1.320
AI Network Analytics	2.4.15.0
Application Registry	2.1.260.170177
Application Visibility Service	2.1.260.170177
Assurance - Base	2.1.2.273
Automation - Base	2.1.260.62555
Cisco DNA Center Global Search	1.2.5.9
Cisco DNA Center Platform	1.3.99.194
Cisco DNA Center UI	1.5.1.26
Cloud Connectivity - Data Hub	1.6.0.162
Cloud Connectivity - Tethering	1.3.1.86
Command Runner	2.1.260.62555
Device Onboarding	2.1.260.62555

[> Serial number](#)

© 2020 Cisco Systems Inc. All Rights Reserved.

Paquetes de Cisco DNA Center requeridos

Una manera rápida de acceder a esta información es hacer clic en el enlace "Acerca de" debajo del icono de signo de interrogación en la esquina superior derecha de la página principal de Cisco DNA Center. Si faltan estas aplicaciones, deben instalarse antes de continuar con la configuración de telemetría. Utilice esta guía para instalar estos paquetes en Cisco DNA Center

desde la nube de Cisco. [Guía de actualización de Cisco DNA Center](#)

Cisco DNA Center como recopilador de telemetría

La exportación de datos de NetFlow es el transporte de tecnología que proporciona los datos de telemetría que se reenviarán a Cisco DNA Center para un análisis en profundidad. Para permitir la recopilación de datos para el aprendizaje automatizado y el razonamiento para el análisis de terminales, NetFlow debe exportarse a Cisco DNA Center. El TTA es una plataforma de sensores de telemetría que se utiliza para generar telemetría a partir del tráfico de red IP reflejado y compartirla con Cisco DNA Center para obtener visibilidad de terminales y aplicaciones.

- El tráfico de red se recibe de los switches y routers a través de la duplicación del analizador de puertos conmutados (SPAN) y se introduce en las interfaces de duplicación del dispositivo de telemetría de tráfico DNA de Cisco.
- Cisco DNA Traffic Telemetry Appliance analiza el tráfico recibido para generar un flujo de telemetría para Cisco DNA Center.

Para activar Cisco DNA Center como recopilador de telemetría, realice estos pasos.

- En Cisco DNA Center, haga clic en Menu > Design > Network Settings y habilite la telemetría para que Cisco DNA Center recopile NetFlow.

NetFlow

Choose Cisco DNA Center to be your NetFlow collector server, and/or add any external NetFlow collector server. This is the destination server for NetFlow export from network devices. Cisco DNA Center will only push the first NetFlow collector server for Wireless Controller as it has a restriction on the number of flow exporters.

Use Cisco DNA Center as NetFlow collector server

INTERFACES FOR APPLICATION TELEMETRY

To enable telemetry on a device , select the device from the Provision table and choose "Actions->Enable Application Telemetry" By default, All access interfaces on a switch OR all LAN-facing interfaces on a router will be provisioned. To override this default behavior, tag specific interfaces to be designated as LAN interface, by putting the keyword "lan" in the interface description.

Once specific interfaces are tagged those interfaces will be monitored.

Add an external NetFlow collector server

Only the external server destination will be configured on network devices. Flow records will not be configured.

Configuración de DNAC como Recopilador de NetFlow

La nube de IA de Cisco

Cisco AI Network Analytics es una aplicación de Cisco DNA Center que aprovecha el potencial del aprendizaje automatizado y el razonamiento automatizado para proporcionar información

precisa específica para la implementación de su red, lo que le permite resolver problemas rápidamente. La información de red y telemetría se anonimiza en Cisco DNA Center y, a continuación, se envía a través de un canal cifrado seguro a la infraestructura basada en la nube de Cisco AI Analytics. La nube de Cisco AI Analytics ejecuta el modelo de aprendizaje automatizado con estos datos del evento y devuelve los problemas y la información general a Cisco DNA Center. Todas las conexiones a la nube son salientes en TCP/443. No hay conexiones entrantes, la nube de IA de Cisco no inicia ningún flujo TCP hacia Cisco DNA Center. Los nombres de dominio completos (FQDN) que se pueden utilizar para permitir el acceso al proxy o firewall HTTPS en el momento de escribir este artículo son:

- <https://api.use1.prd.kairos.ciscolabs.com> (región este de EE. UU.)
- <https://api.euc1.prd.kairos.ciscolabs.com> (Región Central de la UE)

El dispositivo Cisco DNA Center implementado debe ser capaz de resolver y alcanzar los diversos nombres de dominio en Internet que se alojan en Cisco.

Siga estos pasos para conectar Cisco DNA Center a la nube de IA de Cisco.

- Vaya a la interfaz de usuario web del dispositivo Cisco DNA Center para completar el registro en la nube de IA:
- Desplácese hasta System > Settings > External Services > Cisco AI Analytics
- Haga clic en Configure y habilite la opción Endpoint Smart Grouping and AI spoof detection.
- Endpoint Smart Grouping utiliza la nube AI/ML para agrupar los terminales desconocidos con el fin de ayudar a los administradores a etiquetar dichos terminales. Esto es muy útil para reducir las incógnitas netas en la red.
- La detección de simulación de IA ayudará a Cisco a recopilar información adicional de NetFlow/telemetría y a modelar el terminal.
- Elija la ubicación más cercana a la región geográfica de la implementación. Una vez que se haya completado la verificación de la conexión a la nube y la conexión se haya realizado correctamente, aparecerá una casilla de verificación verde.

Cisco AI Analytics

AI Network Analytics

AI Network Analytics harnesses machine learning to drive intelligence in the network, empowering administrators to effectively improve network performance and accelerate issue resolution. AI Network Analytics eliminates noise and false positives significantly by learning the network behavior and adapting to your network environment.

AI Endpoint Analytics

Provides fine-grained endpoint identification and assigns labels to a variety of Endpoints.

ENDPOINT SMART GROUPING

Using AI and Machine Learning, Endpoint Smart Grouping reduces the number of unknown endpoints in the network by providing AI based endpoint groupings, automated custom profiling rules and crowdsourced endpoint labels.

AI SPOOFING DETECTION **PREVIEW**

AI Spoofing Detection will detect endpoints being spoofed based on behavioral models. Models are currently being built using collected flow information from devices. If you are interested in this for your network, please enable data collection to help build these behavioral models.

[Configure](#)

[Recover from a config file](#) ⓘ

[AI Network Analytics Privacy Data Sheet](#) ⓘ

Configuración de la GUI de Cisco AI Analytics

- Si la conexión es incorrecta, verifique la configuración de proxy en Cisco DNA Center desde la página System > Settings > System Configuration > Proxy config si se está utilizando un proxy. También es recomendable comprobar las reglas del firewall que puedan estar bloqueando esta comunicación.

ENDPOINT SMART GROUPING

Using AI and Machine Learning, Endpoint Smart Grouping reduces the number of unknown endpoints in the network by providing AI based endpoint groupings, automated custom profiling rules and crowdsourced endpoint labels.

Enable Endpoint Smart Grouping

AI SPOOFING DETECTION PREVIEW

AI Spoofing Detection will detect endpoints being spoofed based on behavioral models. Models are currently being built using collected flow information from devices. If you are interested in this for your network, please enable data collection to help build these behavioral models.

Send data to help Cisco improve the model

Please choose the region you want to store your data, and make sure the cloud is successfully connected.

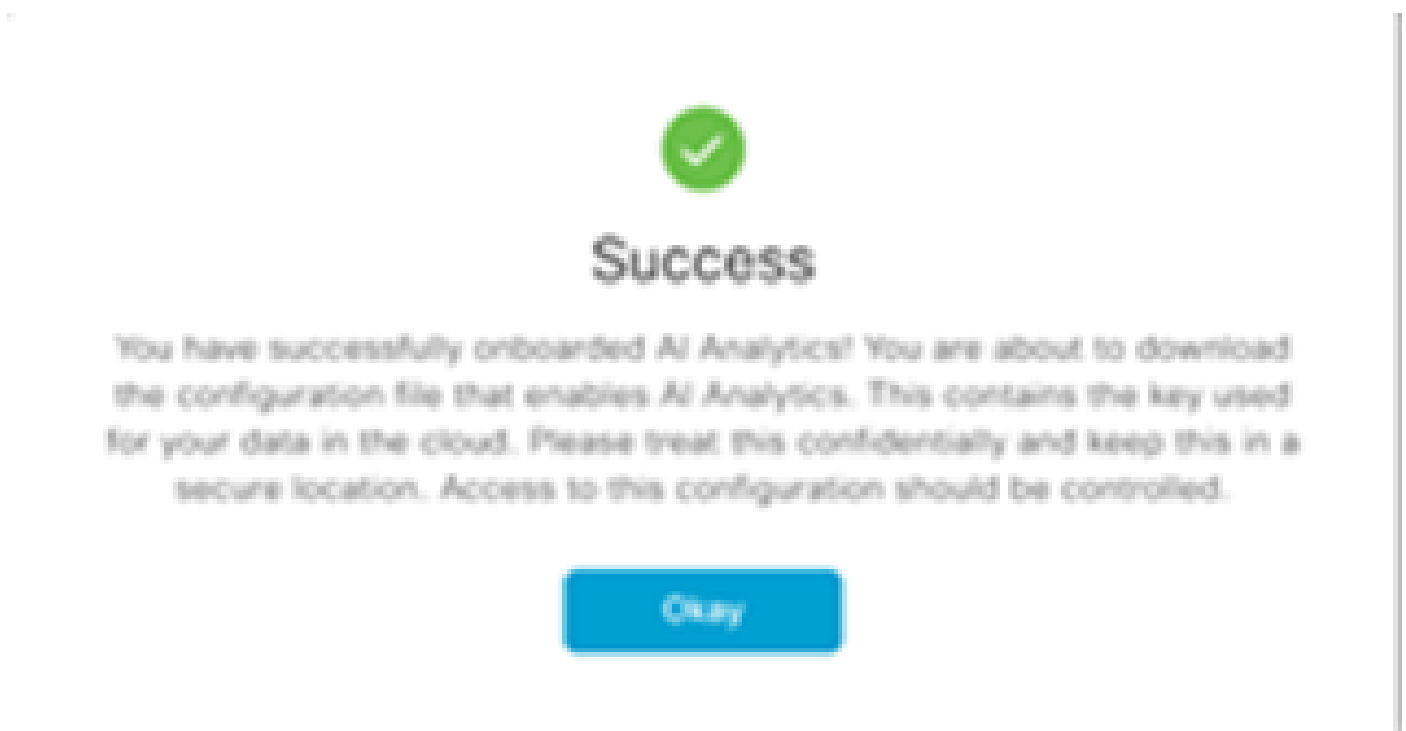
Where should we securely store your data?

Europe (Germany)

Cloud connection verified

Verificación de la conexión a la nube Cisco AI/ML

- Acepte el Acuerdo de nube universal de Cisco para habilitar el análisis de IA.
- En este momento, la incorporación se habrá completado y se mostrará un cuadro de diálogo que indica esto, como se muestra.



Cuadro de diálogo Satisfactorio tras la inscripción

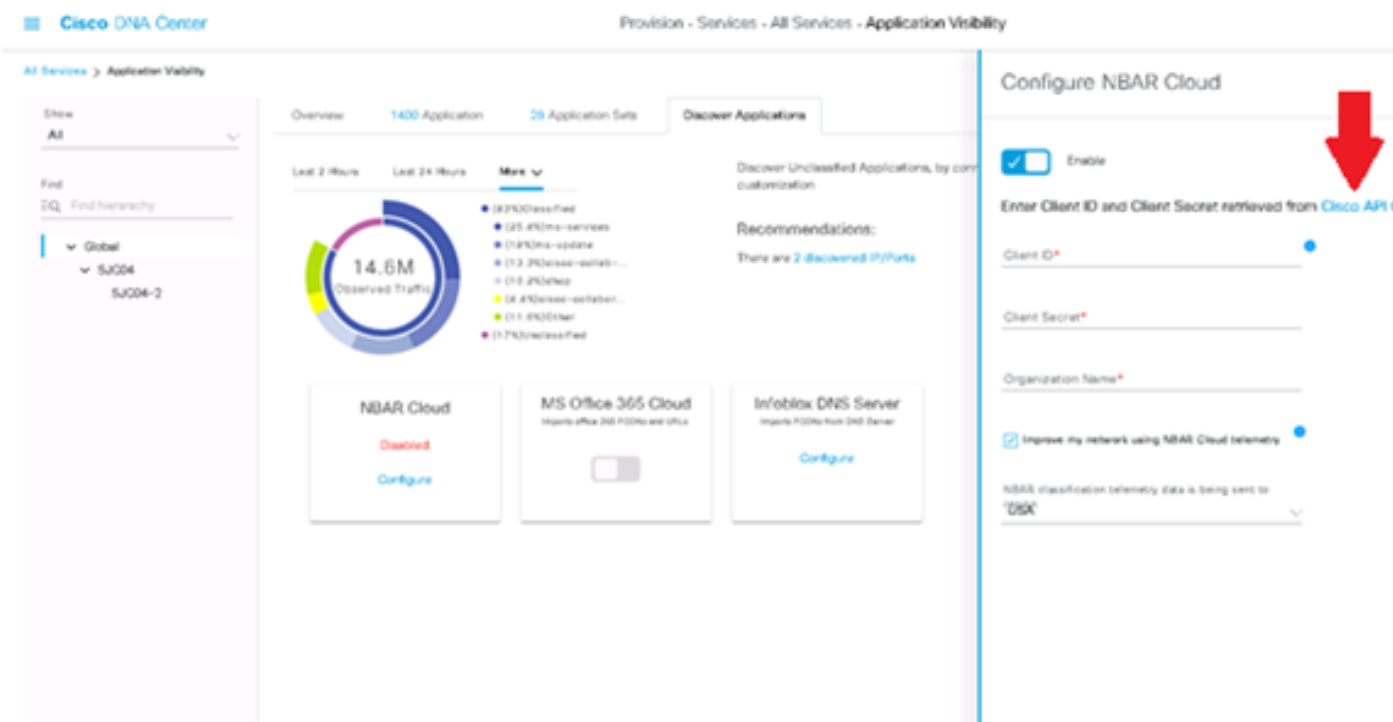
La nube de reconocimiento de aplicaciones basadas en la red (NBAR)

El dispositivo de telemetría y la plataforma Catalyst 9000 recopilan metadatos de terminales mediante una inspección profunda de paquetes de flujos de paquetes y aplican el reconocimiento de aplicaciones basadas en red (NBAR) para determinar qué protocolos y aplicaciones se utilizan en la red. Cisco DNA Center cuenta con un paquete de protocolos NBAR integrado que se puede actualizar. Los datos de telemetría se pueden enviar a la nube de Cisco NBAR para realizar análisis adicionales y detectar firmas de protocolo desconocidas. Para que esto ocurra, el dispositivo Cisco DNA Center debe estar vinculado a la nube. Network-Based Application Recognition (NBAR) es un motor de reconocimiento de aplicaciones avanzado desarrollado por Cisco que utiliza varias técnicas de clasificación y puede actualizar fácilmente sus reglas de clasificación.

Para vincular Cisco DNA Center a la nube de Cisco NBAR, realice estos pasos.

- En la interfaz de usuario de Cisco DNA Center, vaya a Provisioning > Services > Application Visibility. Haga clic en Configurar en Nube NBAR y se abrirá un panel. Active el servicio.
- Si tiene la ID de cliente, el secreto de cliente y el nombre de la organización, asígneles nombres exclusivos en función de la organización y el uso.
- En el momento de redactar este documento, la única región de la nube de NBAR disponible actualmente se encuentra en EE. UU.; es posible que haya más regiones disponibles en el futuro. Seleccione la opción en las preferencias de implementación y guárdela.

Para obtener la ID de cliente y las credenciales de Client Secret, haga clic en el enlace "Cisco API Console" (Consola de API de Cisco) para abrir un portal. Inicie sesión con la ID de CCO adecuada, cree una nueva aplicación, seleccione las opciones correspondientes a la nube de NBAR y complete el formulario. Una vez completado, obtendrá un ID de cliente y un secreto. Consulte la figura que se muestra a continuación.



Enlace de la API de Cisco para recuperar la ID y el secreto del cliente

Estas imágenes muestran las opciones que se utilizan para registrarse en la nube de NBAR.

Application Details

Name of your application: *

Your Org. DNAC NBAR Integration

Application description (optional):

OAuth2.0 Credentials

Choose at least one Grant Type:

- Resource Owner Credentials Authorization Code Client Credentials Implicit
- Refresh Token (the grant type you selected allows you to refresh the token)

Detalles de la aplicación NBAR Cloud

- Utilice esta imagen como referencia mientras completa los detalles de la solicitud de la API.

100,000	Calls per day
<input checked="" type="radio"/> Hello API	
<input type="radio"/> Hello API	
RATE LIMITS	
100	Calls per second
500,000	Calls per day

Detalles de API de aplicaciones

- Introduzca la ID de cliente y el secreto obtenidos del portal de Cisco en Cisco DNA Center.

Configure NBAR Cloud

× Disable

Enter Client ID and Client Secret retrieved from [Cisco API Console](#)

Client ID*

Your Client ID ⓘ

Client Secret*

.....

[SHOW](#)

Organization Name*

Your Org Name

Improve my network using NBAR Cloud telemetry ⓘ

NBAR classification telemetry data is being sent to region

Asia ▾

Configuración de ID de cliente y secreto en DNAC

CBAR (reconocimiento de aplicaciones basadas en controlador) y SD-AVC

CBAR se utiliza para clasificar miles de aplicaciones de red, aplicaciones domésticas y tráfico de red general. Permite a Cisco DNA Center obtener información dinámica sobre las aplicaciones utilizadas en la infraestructura de red. CBAR ayuda a mantener actualizada la red identificando nuevas aplicaciones a medida que aumenta su presencia en la red y permite actualizaciones de los paquetes de protocolos. Si se pierde la visibilidad de la aplicación de extremo a extremo a través de paquetes de protocolos obsoletos, se puede producir una categorización incorrecta y el reenvío posterior. Esto no solo provocará agujeros de visibilidad dentro de la red, sino también problemas incorrectos de envío o colocación en cola. CBAR resuelve ese problema permitiendo

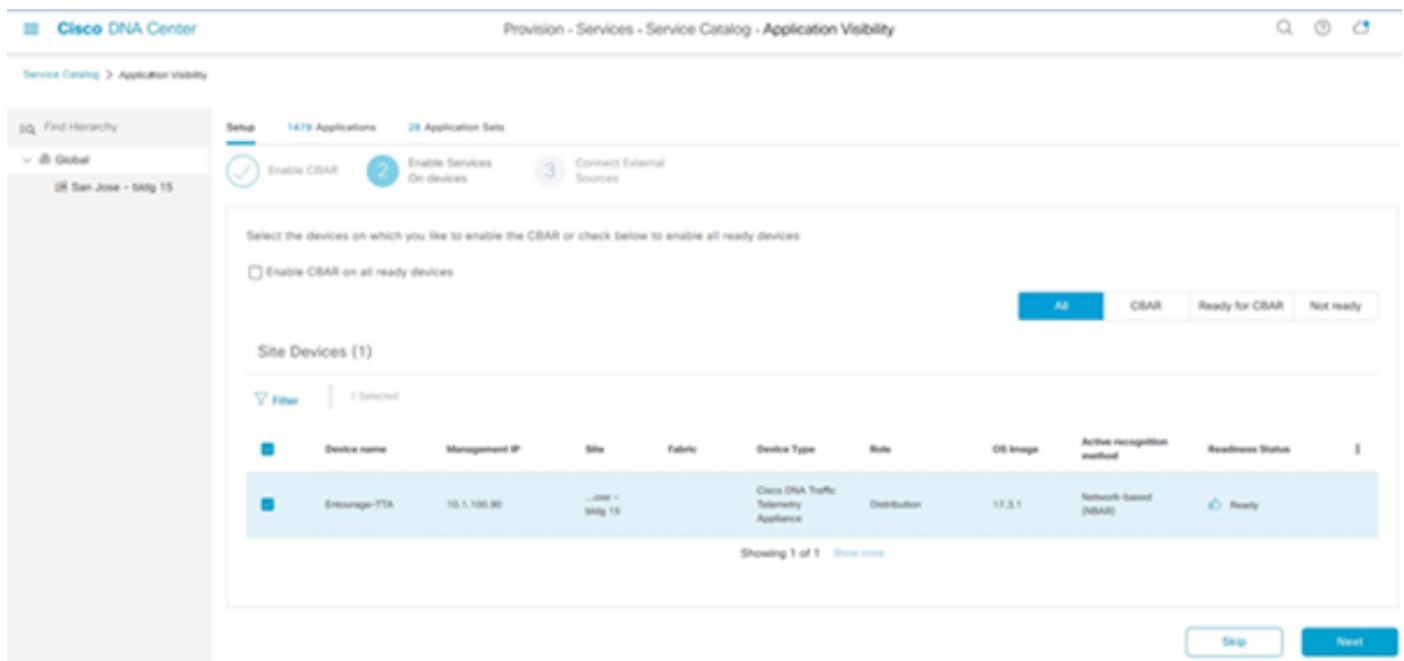
que los paquetes de protocolos actualizados se envíen a través de la red.

Cisco Software-Defined AVC (SD-AVC) es un componente de Cisco Application Visibility and Control (AVC). Funciona como un servicio de red centralizado que funciona con dispositivos participantes específicos en una red. SD-AVC también ayuda en DPI de los datos de la aplicación. Algunas de las funciones y ventajas actuales que ofrece SD-AVC son:

- Reconocimiento uniforme de aplicaciones en toda la red
- Reconocimiento de aplicaciones mejorado en entornos de routing simétricos y asimétricos
- Reconocimiento mejorado del primer paquete
- Actualización del paquete de protocolos en el nivel de red
- Proteja el panel SD-AVC basado en navegador a través de HTTPS para supervisar la funcionalidad y las estadísticas de SD-AVC, así como para configurar actualizaciones de paquetes de protocolos en toda la red

Para activar CBAR para los dispositivos relevantes, siga estos pasos.

- Vaya al menú de Cisco DNA Center, Provisión > Visibilidad de la aplicación. La primera vez que se abra la página Visibilidad de la aplicación, se mostrará al usuario un asistente de configuración que se muestra a continuación.
- Después de detectar los dispositivos en Cisco DNA Center para cada sitio, seleccione el dispositivo en el que desea activar CBAR y continúe con el siguiente paso.



Habilitación de CBAR en el dispositivo

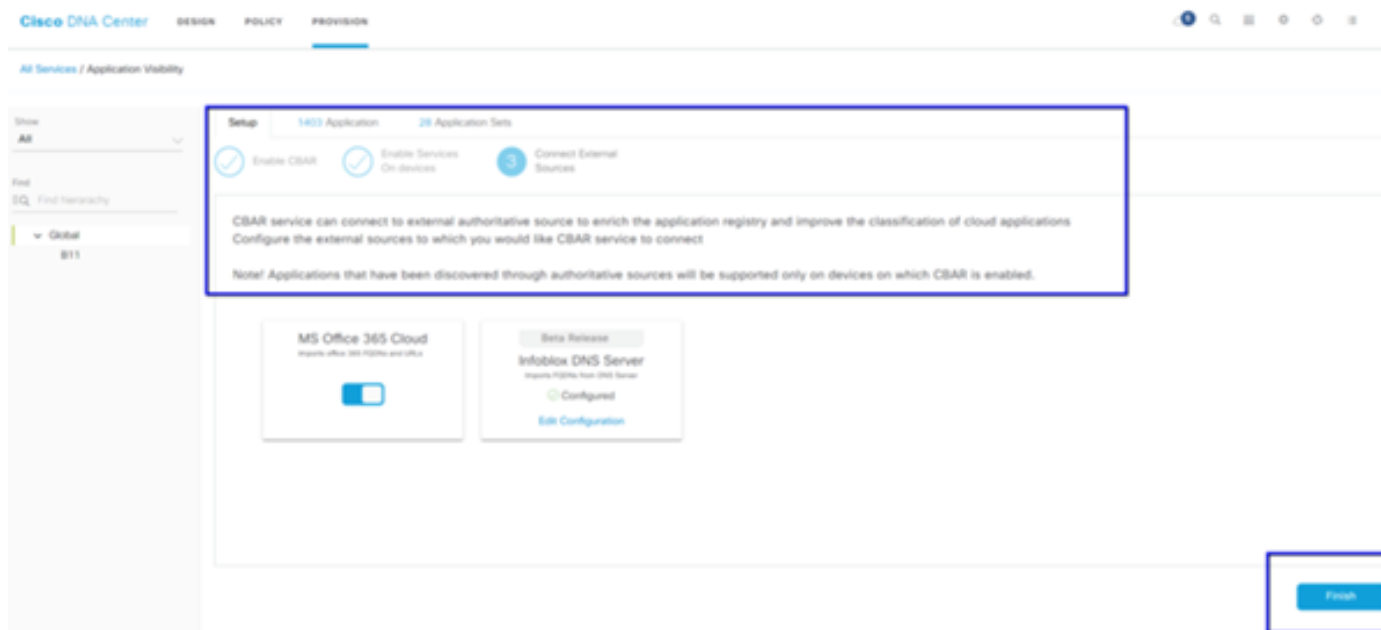
Conector de nube de Microsoft Office 365 (no es obligatorio)

Cisco DNA Center se puede integrar directamente con la fuente RSS de Microsoft para garantizar que el reconocimiento de aplicaciones para Office 365 se ajuste a la guía publicada. Esta integración se conoce como el conector de nube de Microsoft Office 365 en Cisco DNA Center. Es conveniente que esta opción se implemente si el usuario está ejecutando aplicaciones de

Microsoft Office 365 en la red. La integración con Microsoft Office 365 no es un requisito y, si no está habilitada, solo afectará a la capacidad de Cisco DNA Center para procesar y clasificar los datos del host de Microsoft Office 365. Cisco DNA Center ya tiene incorporado el reconocimiento de aplicaciones de Microsoft Office 365, pero al integrarse directamente con el proveedor de aplicaciones, Cisco DNA Center puede obtener información precisa y actualizada sobre los bloques de propiedad intelectual y las URL que utiliza actualmente el conjunto de aplicaciones de Microsoft Office 365.

Para integrar Cisco DNA Center con la nube de Microsoft Office 365, siga estos pasos.

- Haga clic en el icono Menú y seleccione Provisionamiento > Servicios > Visibilidad de la aplicación
- Haga clic en Detectar aplicaciones
- Haga clic en el botón de alternancia MS Office 365 Cloud para integrar Cisco DNA Center con Microsoft Office 365 Cloud.

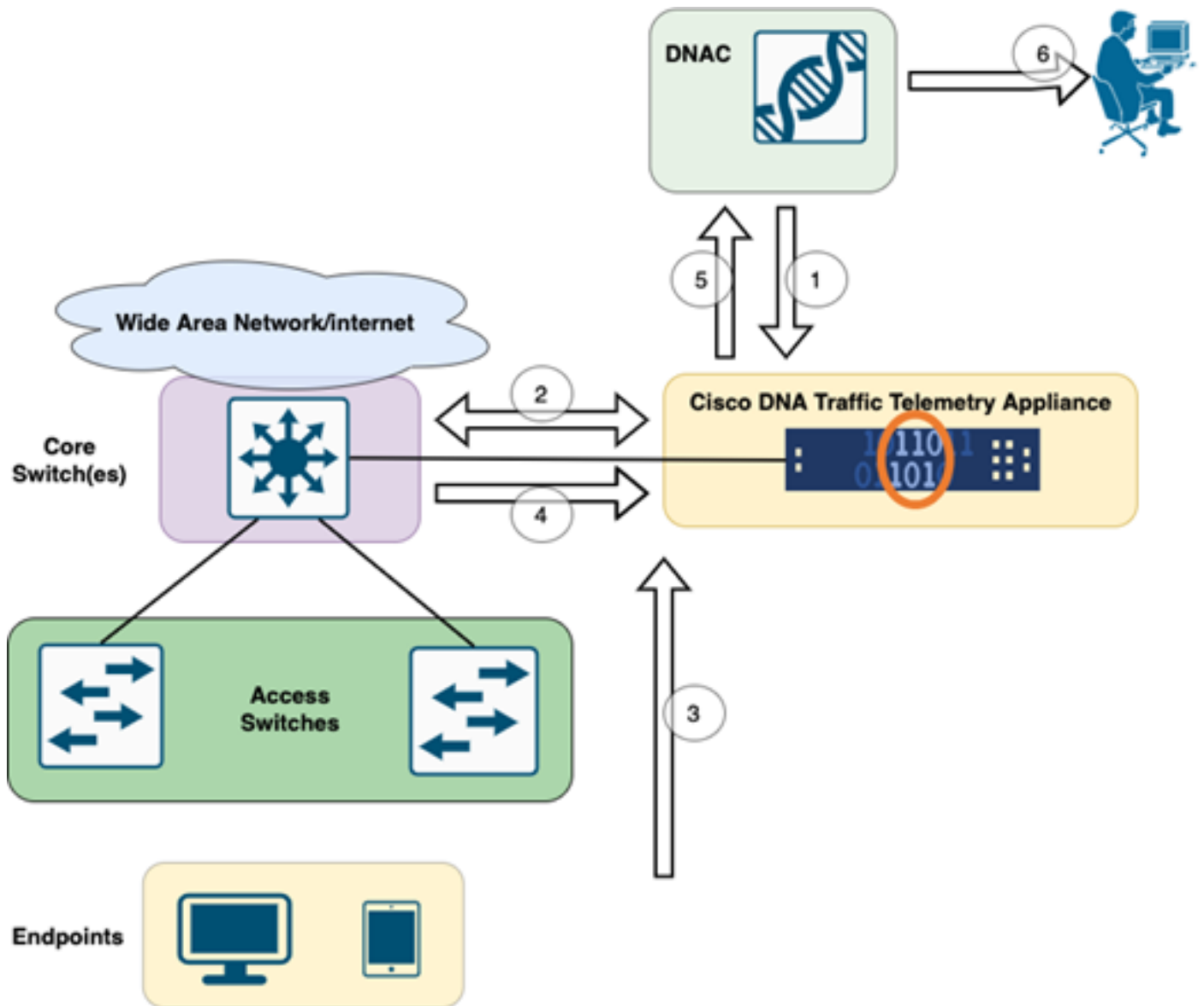


Integración de la nube MS O365

Implementación de TTA

En esta sección se explican los pasos necesarios para implementar TTA en una red.

Descripción general de TTA Workflow



Flujo de trabajo de TTA a DNAC

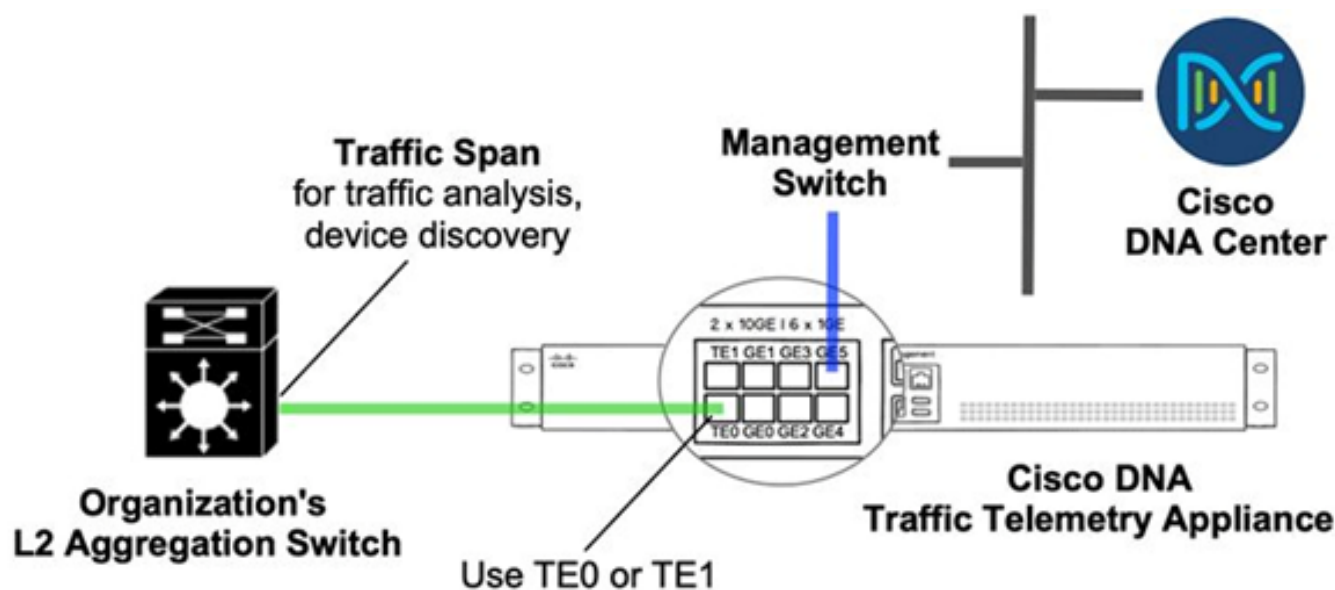
Los pasos resaltados en este diagrama describen el proceso y el flujo de telemetría entre TTA y Cisco DNA Center. Estas medidas se explican con más detalle.

1. El dispositivo de telemetría de tráfico de Cisco está conectado al switch de agregación de sitios o al switch principal dentro de la infraestructura de red. Esta conexión permite al dispositivo recibir datos de tráfico de varios switches de acceso de la red.
2. Cisco Traffic Telemetry Appliance se integra con Cisco DNA Center, que actúa como plataforma de gestión de redes. Esta integración permite una comunicación y un intercambio de datos fluidos entre el dispositivo y Cisco DNA Center.
3. A medida que el tráfico de usuarios fluye a través de la red, se expande o se duplica en el dispositivo de telemetría de tráfico de Cisco. Esto significa que se envía una copia del tráfico de red al dispositivo con fines de supervisión y análisis, mientras que el tráfico original continúa su ruta normal.
4. El dispositivo de telemetría de tráfico de Cisco recopila y procesa los datos de tráfico recibidos. Extrae información relevante, como detalles de nivel de paquete, estadísticas de flujo y métricas de rendimiento, del tráfico reflejado.
5. La información de telemetría procesada se envía a continuación desde el dispositivo de

telemetría de tráfico de Cisco al centro de DNA de Cisco. Esta comunicación permite a Cisco DNA Center recibir información y actualizaciones en tiempo real sobre los patrones de tráfico de la red, el rendimiento de las aplicaciones y las anomalías.

6. La información de telemetría generada por Cisco DNA Center proporciona información valiosa a los administradores de red. Pueden utilizar la interfaz de Cisco DNA Center para ver y analizar los datos recopilados, obtener visibilidad del estado de la red y del rendimiento de las aplicaciones, identificar posibles problemas y tomar decisiones fundamentadas para la optimización y la resolución de problemas de la red.

Implementación de TTA: Diagrama de alto nivel



Implementación de TTA: alto nivel

El diagrama anterior muestra cómo se puede conectar TTA en la red. Las interfaces de 10 Gig y 1 Gig se pueden utilizar para la ingestión de SPAN a velocidad de línea. La interfaz Gi0/0/5 se utiliza para la comunicación con Cisco DNA Center, para la orquestación y para reenviar información de telemetría a Cisco DNA Center; esta interfaz NO se puede utilizar para la ingestión de SPAN.

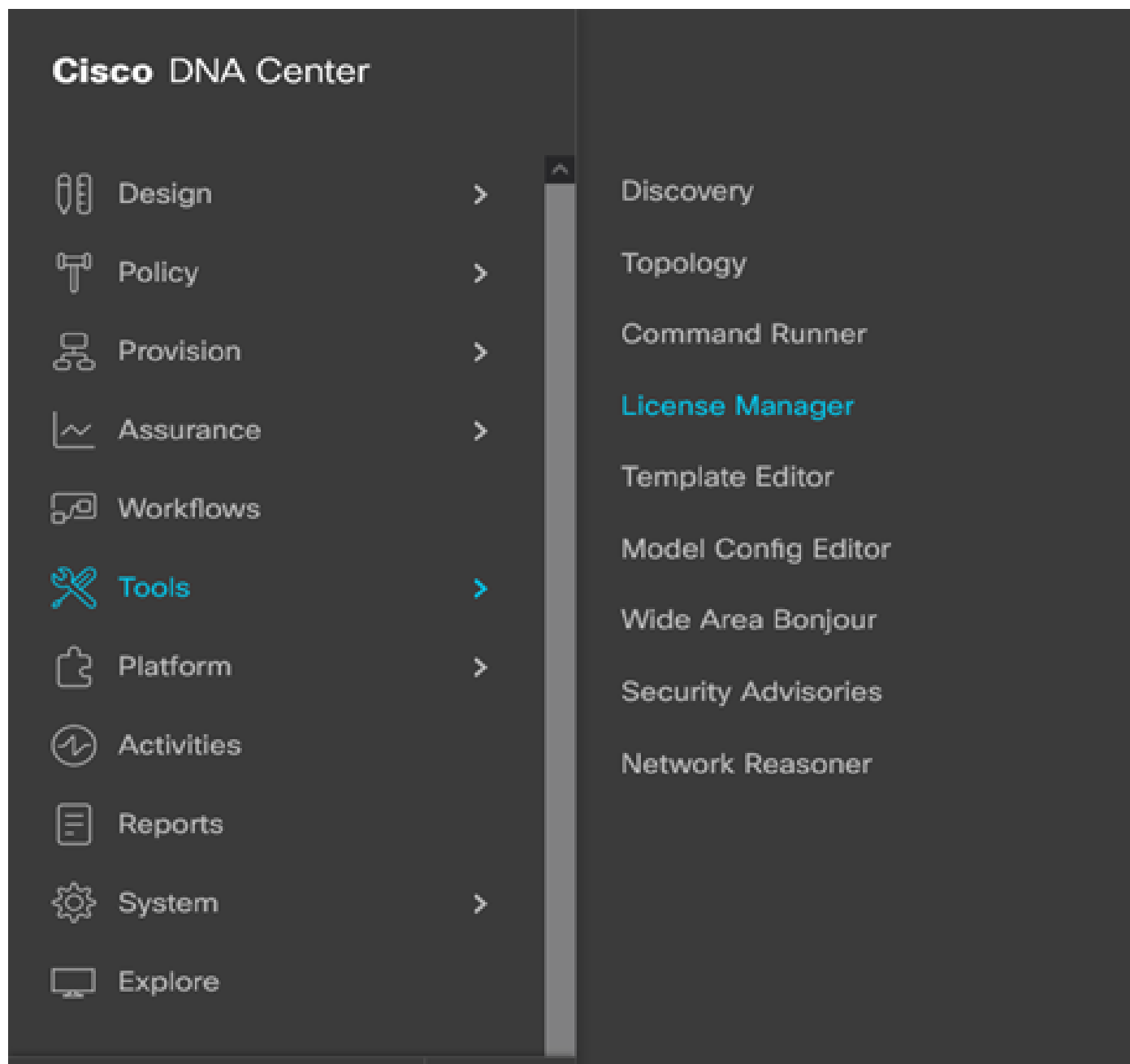
Requisitos de licencia y software de TTA

Los dispositivos TTA implementados en la red serán cruciales para proporcionar información de telemetría sobre los datos de los usuarios y los terminales de estos. Para implementar correctamente la solución, deben cumplirse estos requisitos.

- El TTA debe configurarse con una configuración de bootstrap inicial para que Cisco DNA Center (TTA Bootstrap Configuration) pueda detectarlo
- El dispositivo de TTA debe estar incorporado en Cisco DNA Center para que Cisco DNA Center pueda gestionarlo (agregando el cuadro de telemetría al inventario de Cisco DNA Center)
- Es necesario instalar la licencia correcta en la TTA (licencia del dispositivo TTA)

El dispositivo admite un solo sistema operativo y requiere la licencia Cisco DNA TTA Advantage para recopilar la telemetría. No se necesita una licencia de funciones (como Base IP o Servicios IP avanzados) ni un paquete de licencias perpetuas (como Network Essentials o Network Advantage).

Para administrar licencias en Cisco DNA Center, desplácese hasta el administrador de licencias. Para ello, vaya a Herramientas > Administrador de licencias en el menú desplegable Cisco DNA Center haciendo clic en el icono Menú



Administrador de licencias en DNAC

- Navegue hasta la página All License; tendrá un aspecto similar a esta imagen. En esta página, el administrador puede administrar licencias de dispositivos de red como la de la TTA.

Página Todas las licencias en DNAC

Incorporación de TTA y configuración de día 0

Para facilitar la detección e incorporación del dispositivo TTA por parte de Cisco DNA Center, hay comandos de bootstrap que se deben configurar en los dispositivos TTA del sitio. Con la configuración de bootstrap en su lugar, el TTA se podrá detectar desde el panel de Cisco DNA Center. A continuación se muestran los elementos de configuración de día 0 para un dispositivo TTA. Una vez que el dispositivo se incorpora a la jerarquía del sitio, el dispositivo TTA heredará los elementos de configuración restantes de Cisco DNA Center.

```
hostname TTA
interface GigabitEthernet0/0/5
description ***** Management Interface *****
ip address x.x.x.x <SUBNET MASK>
negotiation auto
cdp enable

ip route 0.0.0.0 0.0.0.0 x.x.x.y
username dna privilege 15 algorithm-type scrypt secret
.
.
.
enable secret
.
.
.
service password-encryption
ip domain name <domain name>
ip ssh version 2
line vty 0 15
login local
transport input ssh
transport preferred none
```

```
ip ssh source-interface GigabitEthernet0/0/5
```

```
aaa new-model  
aaa authentication login default local  
aaa authorization exec default local
```

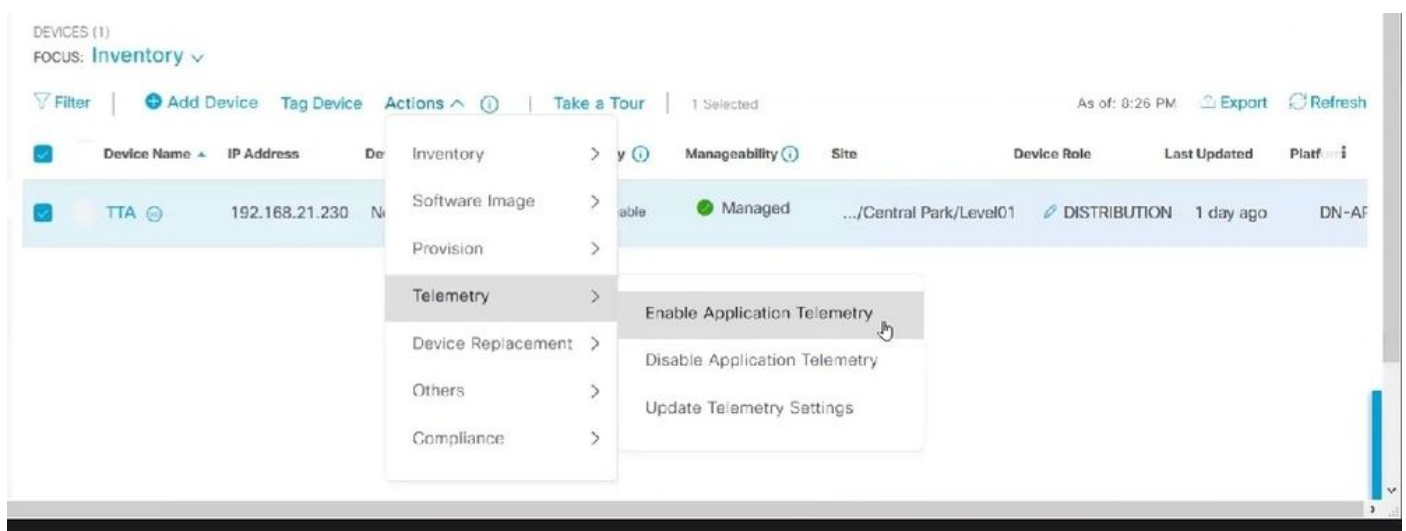
```
**SNMPv2c or SNMPv3 paramters as applicable**  
snmp-server community <string> RO  
snmp-server community <string> RW
```

Una vez que estos elementos se configuran en el TTA, Cisco DNA Center puede descubrirlo.

Adición del dispositivo TTA al inventario de Cisco DNA Center

Para aprovechar la TTA, Cisco DNA Center necesita descubrir y gestionar el dispositivo TTA. Una vez que la TTA se incorpora al Cisco DNA Center, se puede gestionar desde Cisco DNA Center. Antes de descubrir el dispositivo TTA, debemos asegurarnos de que se ha establecido la jerarquía de sitios completa para el sitio. Después de esto, continuaremos agregando el dispositivo TTA bajo la jerarquía específica del sitio siguiendo estos pasos desde la página Menu > Provisioning > Devices > Inventory para agregar el dispositivo a un sitio.

1. Proporcione el nombre de usuario/contraseña (CLI) y la comunidad SNMP necesarios para conectarse al dispositivo y la contraseña de habilitación. Espere hasta que el dispositivo se haya agregado correctamente antes de continuar.
2. Compruebe el nombre del dispositivo, la familia (administración de red en caso de TTA), la disponibilidad (accesible), la capacidad de gestión y la función del dispositivo (distribución). Inicialmente, el dispositivo será "No conforme"; sin embargo, una vez que se haya provisionado por completo, el estado cambiará.
3. Una vez que el TTA esté incorporado, Cisco DNA Center insertará plantillas de configuración para configurarlo con funciones de telemetría avanzadas.



Detección de TTA y habilitación de la telemetría de aplicaciones

configuración de SPAN

Dependiendo de las capacidades de hardware del switch principal, la sesión SPAN se puede configurar para SPAN en un grupo de VLAN o interfaces a la interfaz conectada al TTA. Aquí se proporciona un ejemplo de configuración.

```
Switch#configure terminal
Switch(config)#monitor session 1 source vlan|interface rx|tx|both
Switch(config)#monitor session 1 destination interface intx/y/z
```

Garantía recopilada

Para acceder a los datos de Assurance recopilados desde el dispositivo de telemetría de tráfico instalado, vaya a la sección Assurance y haga clic en Health (Estado).

Cisco DNA Center

 Design >

 Policy >

 Provision >

 Assurance >

 Workflows

 Tools >

 Platform >

 Activities

 Reports

 System >

 Explore

DASHBOARDS

Health

Issues & Events

Sensors

Wi-Fi 6

Rogue and aWIPS

PoE

Dashboard Library

AI NETWORK ANALYTICS

Trends and Insights

Network Heatmap

Peer Comparison

Network Comparison

Baselines

AI-Enhanced RRM

SETTINGS

Issue Settings

Health Score Settings

Sensors

Intelligent Capture Settings

Elija Aplicaciones y encontrará una descripción general completa de los datos de la aplicación, incluida la latencia y la fluctuación capturadas por el TTA en función del tipo de aplicación específico.

The screenshot shows the Cisco DNA Center Assurance / Dashboards / Health page. The navigation bar includes Overall, Network, Client, Applications, Network Services, and SD-Access. The main content area is titled "Application Assurance" and displays a table of applications. The table has columns for Name, Health, Business Relevance, Usage, Average Throughput, Packet Loss (%), Network Latency, and Jitter. The applications listed are: Learning, Web, Amazon, YouTube, Zoom, Microsoft-Exchange, and Mail.

Name	Health	Business Relevance	Usage	Average Throughput	Packet Loss (%)	Network Latency	Jitter
Learning	10	Business Important	10MB	46.4Kbps	0	0 ms	--
Web	--	Business Important	1.4MB	6.7Kbps	--	--	--
Amazon	10	Business Important	483.7KB	1.3Kbps	0	0 ms	--
YouTube	2	Business Important	156.6KB	458bps	2	0 ms	--
Zoom	2	Business Important	156.2KB	4.2Kbps	4	--	--
Microsoft-Exchange	--	Business Important	107.6KB	278bps	--	--	--
Mail	10	Business Important	95.6KB	252bps	1	2 ms	--

UI de Application Assurance detallada

Para obtener un análisis más detallado, los usuarios pueden explorar aplicaciones individuales haciendo clic en la aplicación específica y seleccionando el exportador que será el dispositivo de telemetría de tráfico. Además, pueden examinar métricas específicas como los datos de uso, rendimiento y pérdida de paquetes, latencia de red de cliente, latencia de red de servidor y latencia de servidor de aplicaciones.



Ejemplo: Datos de la aplicación Pt.1



Ejemplo: Datos de la aplicación Pt.2

Verificación

1. Después de habilitar CBAR, verifique que el servicio SD-AVC (Application Visibility Control) esté habilitado en el dispositivo iniciando sesión en Cisco Traffic Telemetry Appliance y ejecutando este comando CLI. El resultado será similar a este ejemplo, indicando la dirección IP del controlador y el estado como conectado.

```
Cisco-TTA#sh avc sd-service info summary
Status: CONNECTED
Device ID: Cisco-TTA
Device segment name: AppRecognition
Device address: <TTA IP Address>
Device OS version: 17.03.01
Device type: DN-APL-TTA-M
Active controller:
Type : Primary
IP : <Cisco DNA Center IP Address>
Status: Connected
Version : 4.0.0
```

2. Utilice el comando "show license summary" en la CLI de la TTA para verificar los detalles de licencia de dispositivo relevantes.

```
Device# show license summary
Smart Licensing is ENABLED
License Reservation is ENABLED
```

```
Registration:
Status: REGISTERED - SPECIFIC LICENSE RESERVATION
Export-Controlled Functionality: ALLOWED
```

License Authorization:
Status: AUTHORIZED - RESERVED

License Usage:

License	Entitlement tag	Count	Status

Cisco_DNA_TTA_Advantage	(DNA_TTA_A)	1	AUTHORIZED

3. Verifique que la sesión SPAN se haya configurado correctamente en el switch de núcleo/agregación.

```
AGG_SWITCH#show monitor session 1
Session 1
-----
Type : Local Session
Source VLANs : 300-320
RX Only :
Destination Ports : TenGigx/y/z
Encapsulation : Native
Ingress : Disabled
```

4. Una vez que el TTA se ha provisionado correctamente, estos comandos se enviarán (o se han enviado) al dispositivo.

```
avc sd-service
segment AppRecognition
controller
address <Cisco DNA Center IP Address>
.....
!
flow exporter <Cisco DNA Center IP Address>
destination <Cisco DNA Center IP Address>
!
crypto pki trustpoint DNAC-CA
.....
!
performance monitor context tesseract profile application-assurance
exporter destination <Cisco DNA Center IP Address> source GigabitEthernet0/0/5 transport udp port 6007
....
!
All interfaces must have
ip nbar protocol-discovery
performance monitor context tesseract
```

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).