Traffic Telemetry Appliance (TTA) und Cisco DNA Center App Assurance: die Vorteile

Inhalt

Einleitung

In diesem Dokument werden die Plattform der Cisco DNA Traffic Telemetry Appliance (Cisco Teilenummer DN-APL-TTA-M) sowie die Möglichkeiten zur Anwendungssicherung im Cisco DNA Center beschrieben. IAußerdem wird aufgezeigt, wie und wo die TTA zusammen mit dem Konfigurations- und Verifizierungsprozess in einem Netzwerk positioniert werden kann. In diesem Artikel werden auch die verschiedenen Voraussetzungen behandelt.

Voraussetzungen

Cisco empfiehlt, dass Sie über die Funktionsweise von Cisco DNA Center Assurance and Application Experience Bescheid wissen.

Anwendungssicherheit

Assurance ist eine vielseitig einsetzbare Engine für die Erfassung und Analyse von Netzwerkdaten in Echtzeit, die das Geschäftspotenzial von Netzwerkdaten erheblich steigern kann. Assurance verarbeitet komplexe Anwendungsdaten und stellt die Ergebnisse in Dashboards für die Gewährleistung der Zuverlässigkeit dar, um einen Einblick in die Leistung der im Netzwerk verwendeten Anwendungen zu geben. Je nachdem, wo die Daten erfasst werden, können Sie einige oder alle der folgenden Informationen anzeigen:

- Anwendungsname
- Durchsatz
- DSCP-Markierungen
- Leistungskennzahlen (Latenz, Jitter und Paketverlust)

Je nach Menge der gesammelten Daten kann Application Assurance in zwei Modelle kategorisiert werden:

- Anwendungstransparenz (AppVis) und
- Anwendungserlebnis (AppX)

Anwendungsname und -durchsatz werden zusammen als quantitative Metriken bezeichnet. Die Daten für die quantitativen Metriken werden durch die Aktivierung von Anwendungstransparenz generiert.

DSCP-Markierungen und Leistungsmetriken (Latenz, Jitter und Paketverlust) werden zusammen als qualitative Metriken bezeichnet. Die Daten für die qualitativen Metriken stammen aus der Anwendungserfahrung.

Anwendungstransparenz (AppVIS)

Die Daten zur Anwendungstransparenz werden von Switches mit Cisco IOS® XE und von Wireless-Controllern mit AireOS erfasst. Auf Switches mit Cisco IOS XE werden Daten zur Anwendungstransparenz mithilfe einer vordefinierten NBAR-Vorlage erfasst, die bidirektional (Eingang und Ausgang) auf die Access Switch-Ports der physischen Ebene angewendet wird. Für Wireless-Controller, auf denen AireOS ausgeführt wird, werden Daten zur Anwendungstransparenz am Wireless-Controller erfasst. Diese Daten werden dann mithilfe von Streaming-Telemetrie an das Cisco DNA Center übertragen.

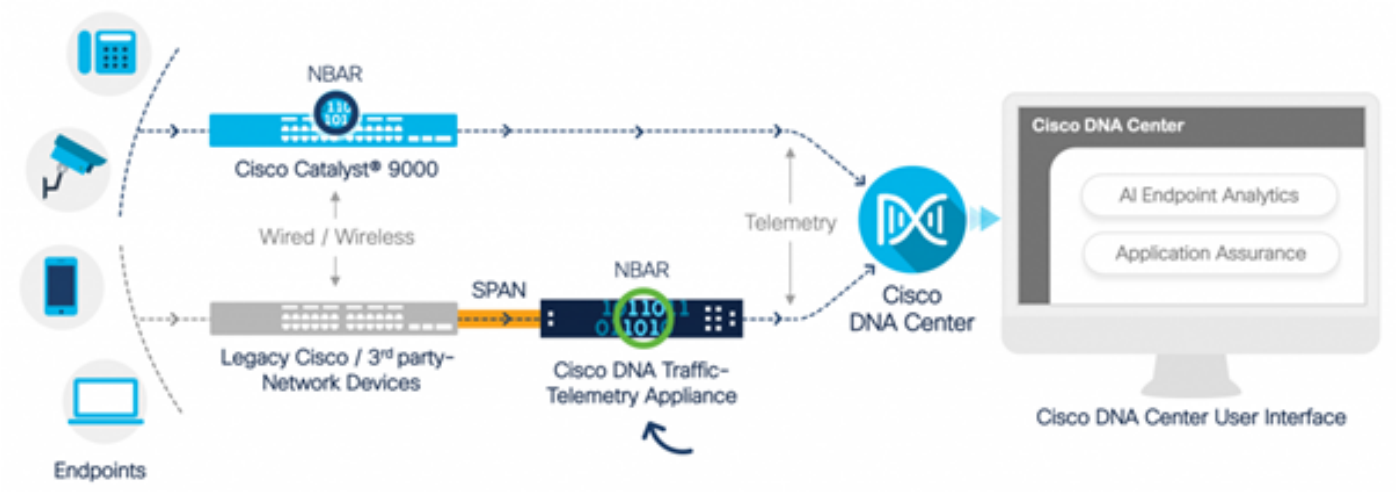
Anwendungserlebnis (AppX)

Die Application Experience-Daten werden von Cisco IOS XE-Routerplattformen erfasst, insbesondere unter Verwendung der Cisco Performance Monitor-Funktion (PerfMon) und der Cisco Application Response Time-Kennzahlen (ART). Beispiele für Routerplattformen sind ASR 1000, ISR 4000 und CSR 1000v. Informationen zur Gerätekompatibilität mit Cisco DNA Center

finden Sie in der [Cisco DNA Center-Kompatibilitätsmatrix.]

Warum eine Traffic Telemetry Appliance?

Die kabelgebundenen und drahtlosen Geräte der Cisco Catalyst Serie 9000 führen eine Deep Packet Inspection (DPI) durch und stellen Datenströme für Services wie Cisco AI Endpoint Analytics und Application Assurance im Cisco DNA Center bereit. Was aber, wenn es im Netzwerk keine Geräte der Catalyst Serie 9000 gibt, aus denen Telemetrie extrahiert werden kann? Einige Unternehmen verfügen noch immer über einen Teil ihrer Netzwerkinfrastruktur, der nicht auf die Plattformen der Cisco Catalyst Serie 9000 migriert wurde. Die Catalyst 9000-Plattform generiert AppVis-Telemetriedaten. Um jedoch zusätzliche Informationen über AppX zu erhalten, kann die Cisco DNA Traffic Telemetry Appliance genutzt werden, um diese Lücke zu schließen. Das Ziel des TTA ist es, den Datenverkehr zu überwachen, den er über SPAN-Ports von anderen Netzwerkgeräten erhält, die nicht in der Lage sind, Application Experience-Daten an das Cisco DNA Center zu übermitteln. Da die älteren Infrastrukturgeräte die für erweiterte Analysen erforderliche Deep Packet Inspection nicht durchführen können, kann die Cisco DNA Traffic Telemetry Appliance verwendet werden, um AppX-Telemetrie aus vorhandenen älteren Bereitstellungen zu generieren.



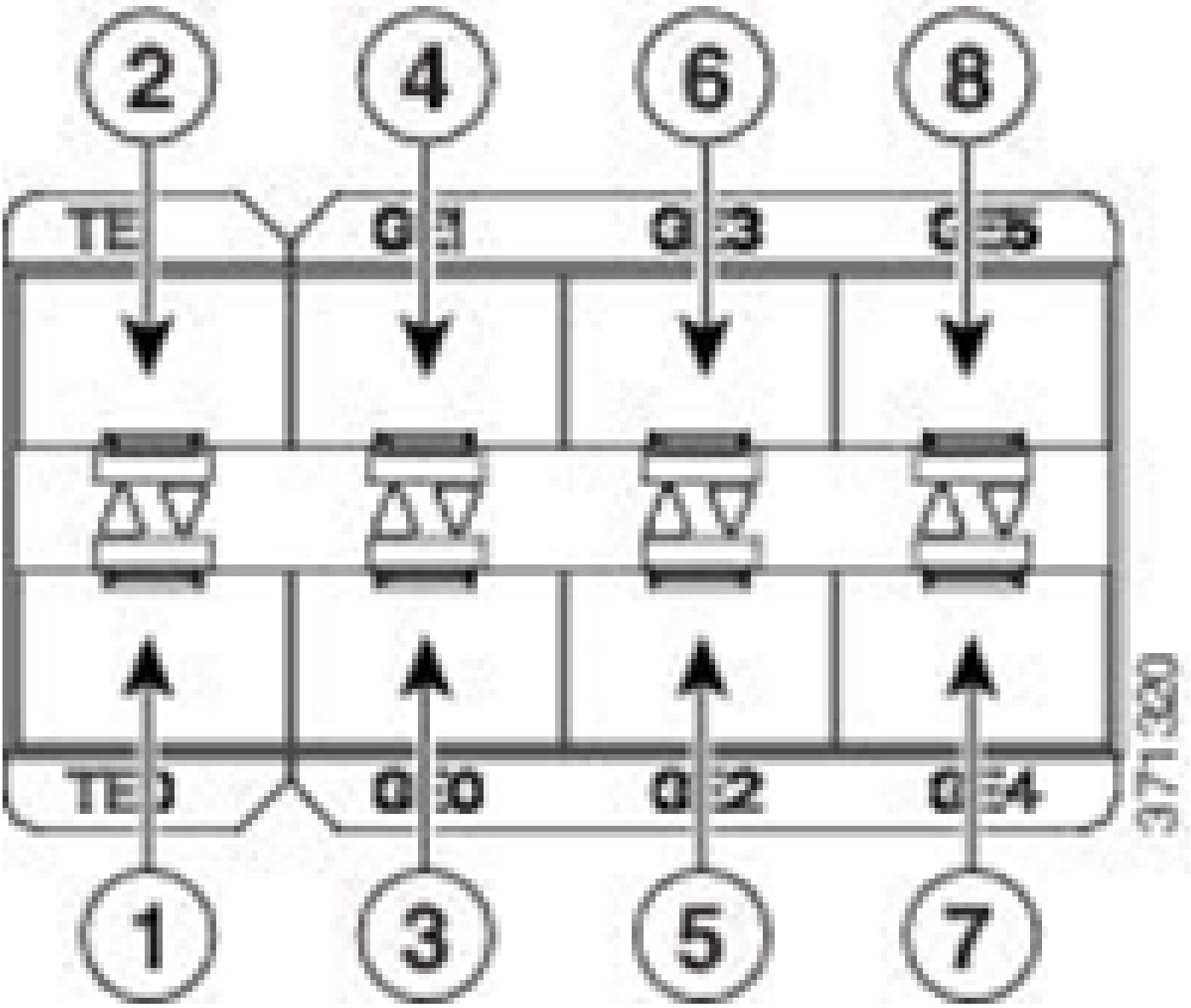
Cisco TTA in Aktion

TTA-Gerätedetails

Die Cisco IOS XE-basierte Telemetriesensor-Plattform generiert Telemetrie aus gespiegeltem IP-Netzwerkverkehr von SPAN-Sitzungen (Switched Port Analyzer) von Switches und Wireless Controllern. Die Appliance überprüft Tausende von Protokollen mithilfe der NBAR-Technologie (Network-Based Application Recognition), um einen Telemetrie-Stream für Analysen im Cisco DNA Center zu erstellen. Die Cisco DNA Traffic Telemetry Appliance kann 20 Gbit/s an Datenverkehr mit anhaltendem Durchsatz verarbeiten und 40.000 Endpunktsitzungen auf Erstellung von Geräteprofilen untersuchen.

Die Cisco Traffic Telemetry Appliance

Der TTA verfügt über eine Mischung aus 10-Gig- und 1-Gig-Verbindungen, die zur SPAN-Aufnahme verwendet werden. Von diesen Ports ist Gig0/0/5 der einzige Port, der mit einer IP-Adresse konfiguriert und für die Kommunikation mit dem Cisco DNA Center verwendet werden kann. Die Schnittstellenmatrix ist unten dargestellt.



TTA-Schnittstellenmatrix

TTA-Schnittstellenmatrix			
1	10 GE SFP+ Port 0/0/0	5	GE SFP-Port 0/0/2
2	10 GE SFP+ Port 0/0/1	6	GE SFP-Port 0/0/3
3	GE SFP-Port 0/0/0	7	GE SFP-Port 0/0/4
4	GE SFP-Port 0/0/1	8	GE SFP-Port 0/0/5

Cisco DNA Center - Voraussetzungen für Assurance

In diesem Abschnitt werden die Konfigurationen und Voraussetzungen beschrieben, die erfüllt werden müssen, bevor das Cisco DNA Center die Telemetrie verarbeiten kann.

Operativer Cisco DNA Center Cluster

Für das zur Verwaltung der TTA und der Prozesstelemetrie verwendete Cisco DNA Center-Cluster müssen die folgenden Kriterien erfüllt sein:

- Netzwerkhierarchie: Im Abschnitt "Netzwerkhierarchie" des Design-Workflows werden verschiedene Campus-Standorte, Gebäude innerhalb dieser Standorte und die einzelnen Stockwerke innerhalb dieser Gebäude definiert und auf einer Weltkarte dargestellt. Die entsprechende Standort-/Netzwerkhierarchie muss konfiguriert werden.
- Netzwerkeinstellungen: Im Abschnitt "Netzwerkeinstellungen" können allgemeine Standard-Netzwerkeinstellungen erstellt werden, die von den Geräten im Netzwerk verwendet werden. Diese Einstellungen können global angewendet werden, aber auch standort-, gebäude- oder ebenerdig. Geben Sie DNS, Domänennamen, Syslog, NTP, Zeitzone und Anmeldebanner-Informationen gemäß den Anforderungen der Bereitstellung ein.
- Geräteanmeldedaten: Diese Anmeldeinformationen werden für den Zugriff auf und die Erkennung von Geräten im Netzwerk einschließlich des TTA verwendet. Cisco DNA Center muss mit der entsprechenden CLI und SNMP-Anmeldeinformationen konfiguriert werden. Zusammen mit dieser NetConf Anmeldeinformationen sind gut zu haben.
- Cisco CCO-Konto: Ein gültiges CCO-Konto ist erforderlich, um die Appliance zu binden und die Funktionen der Cisco AI Cloud zu nutzen, Images für SWIM herunterzuladen und Protokollpakete für TTA und andere Geräte herunterzuladen.

ISE und Cisco DNA Center-Integration

Die Cisco Identity Services Engine (ISE) und das Cisco DNA Center können zur Identitäts- und Richtlinienautomatisierung integriert werden. Die ISE dient außerdem dazu, Informationen über die Endgeräte zu sammeln und so Cisco AI Endpoint Analytics zu nutzen. PxGrid wird zur Implementierung der Integration zwischen der ISE und dem Cisco DNA Center verwendet.

Für die Integration von Cisco DNA Center und ISE gelten folgende Anforderungen:

- Der pxGrid-Dienst muss auf der ISE aktiviert sein.
- ERS-Lese-/Schreibzugriff muss aktiviert sein.
- Das ISE-Admin-Zertifikat muss die IP-Adresse oder den FQDN der ISE entweder im Antragstellernamen oder im SAN-Feld enthalten.
- Das Cisco DNA Center-Systemzertifikat muss alle IP-Adressen oder FQDNs des Cisco DNA Center im Betreffnamen- oder SAN-Feld enthalten.
- Die ISE ERS-Administratoranmeldeinformationen werden für die vertrauenswürdige Einrichtung der ERS-Kommunikation zwischen der ISE und dem Cisco DNA Center verwendet.
- Der pxGrid-Knoten muss vom Cisco DNA Center aus erreichbar sein.

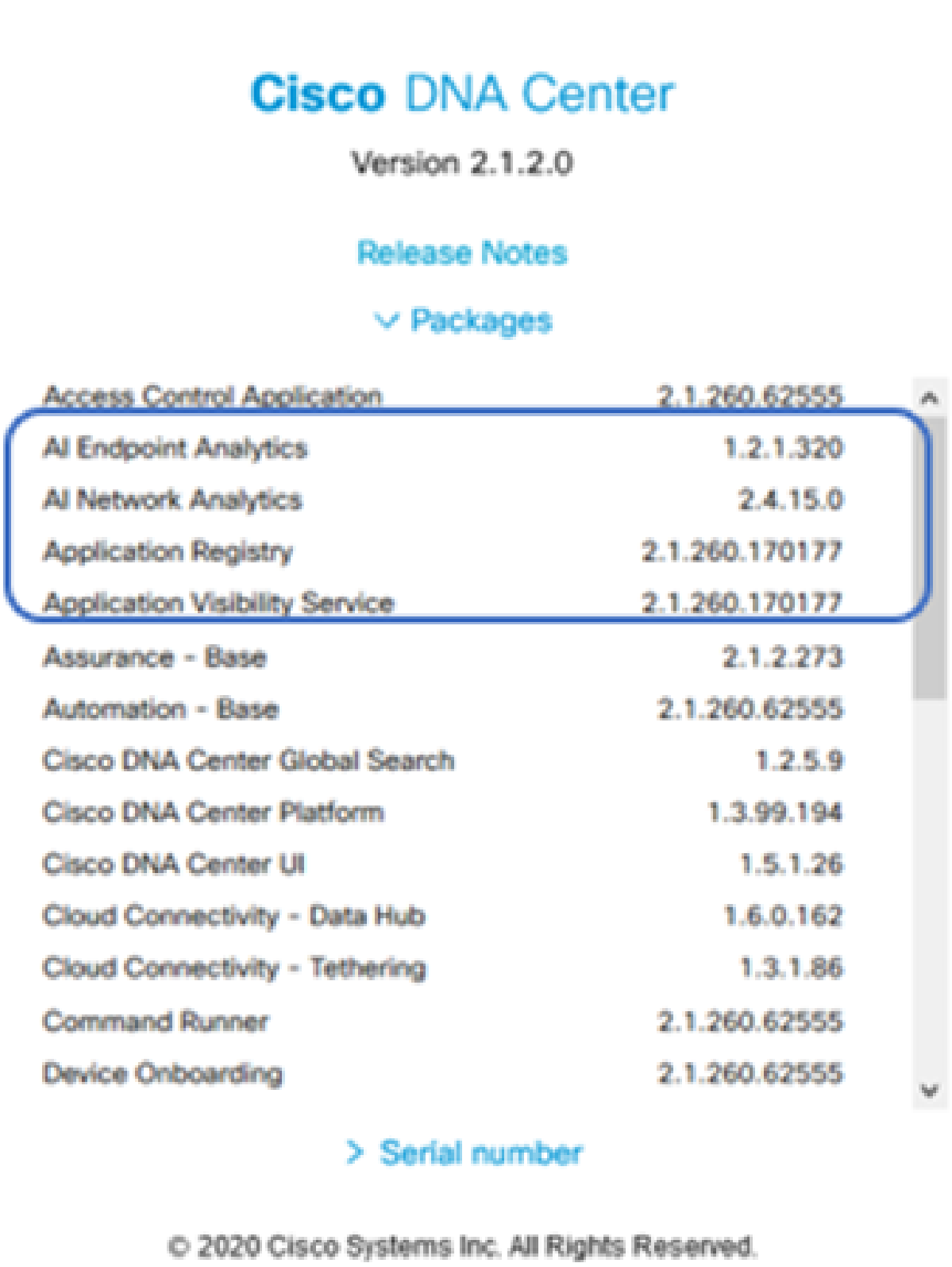
Cisco DNA Center-Anforderungen für Telemetrie

Es gibt Anforderungen, die implementiert werden müssen, um Application Assurance im Cisco DNA Center zu ermöglichen. Diese Anforderungen werden in den folgenden Abschnitten ausführlich erläutert.

Schlüsselpakete für Cisco DNA Center

Für Cisco DNA Center müssen diese drei Pakete installiert sein, damit Telemetriedaten analysiert werden können.

- AI-Endgeräteanalysen
- AI-Netzwerkanalysen
- Anwendungstransparenz-Services



Erforderliche Cisco DNA Center-Pakete

Um schnell auf diese Informationen zuzugreifen, klicken Sie auf den Link "About" (Über) unter dem Fragezeichen-Symbol oben rechts auf der Hauptseite von Cisco DNA Center. Wenn diese Anwendungen fehlen, müssen sie installiert werden, bevor mit dem Telemetrie-Setup fortgefahren werden kann. Verwenden Sie dieses Handbuch, um diese Pakete über die Cisco Cloud im Cisco

DNA Center zu installieren. [Cisco DNA Center Upgrade-Leitfaden]

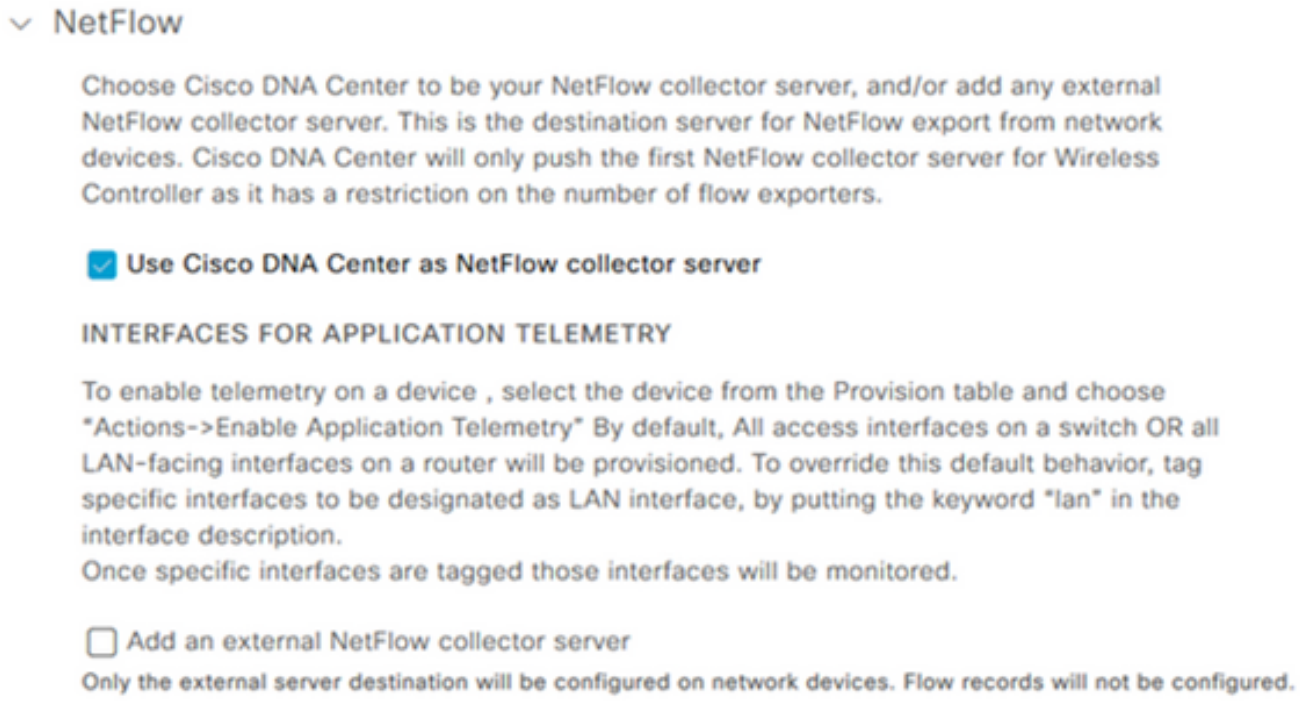
Cisco DNA Center als Telemetriesammler

Der NetFlow-Datenexport ist der Technologietransport, der die Telemetriedaten bereitstellt, die zur eingehenden Analyse an Cisco DNA Center weitergeleitet werden. NetFlow muss in das Cisco DNA Center exportiert werden, um Datenerfassung für maschinelles Lernen und das logische Denken für Endpunktanalysen zu ermöglichen. Die TTA ist eine Telemetriesensor-Plattform, die Telemetriedaten aus gespiegeltem IP-Netzwerkverkehr generiert und für Anwendungs- und Endgeräte-Transparenz an das Cisco DNA Center weitergibt.

- Netzwerkverkehr wird von Switches und Routern über SPAN-Spiegelung (Switched Port Analyzer) empfangen und in die Schnittstellen der Cisco DNA Traffic Telemetry Appliance zur Spiegelung eingespeist.
- Die Cisco DNA Traffic Telemetry Appliance analysiert den empfangenen Datenverkehr und erstellt einen Telemetrie-Stream für das Cisco DNA Center.

Führen Sie diese Schritte aus, um Cisco DNA Center als Telemetriesammler zu aktivieren.

- Klicken Sie im Cisco DNA Center auf Menu > Design > Network Settings, und aktivieren Sie Telemetrie für Cisco DNA Center, um NetFlow zu erfassen.



Konfigurieren von DNAC als NetFlow-Collector

Die Cisco KI Cloud

Cisco AI Network Analytics ist eine Anwendung im Cisco DNA Center, die maschinelles Lernen und maschinelles Denken nutzt, um genaue Einblicke zu erhalten, die spezifisch für Ihre

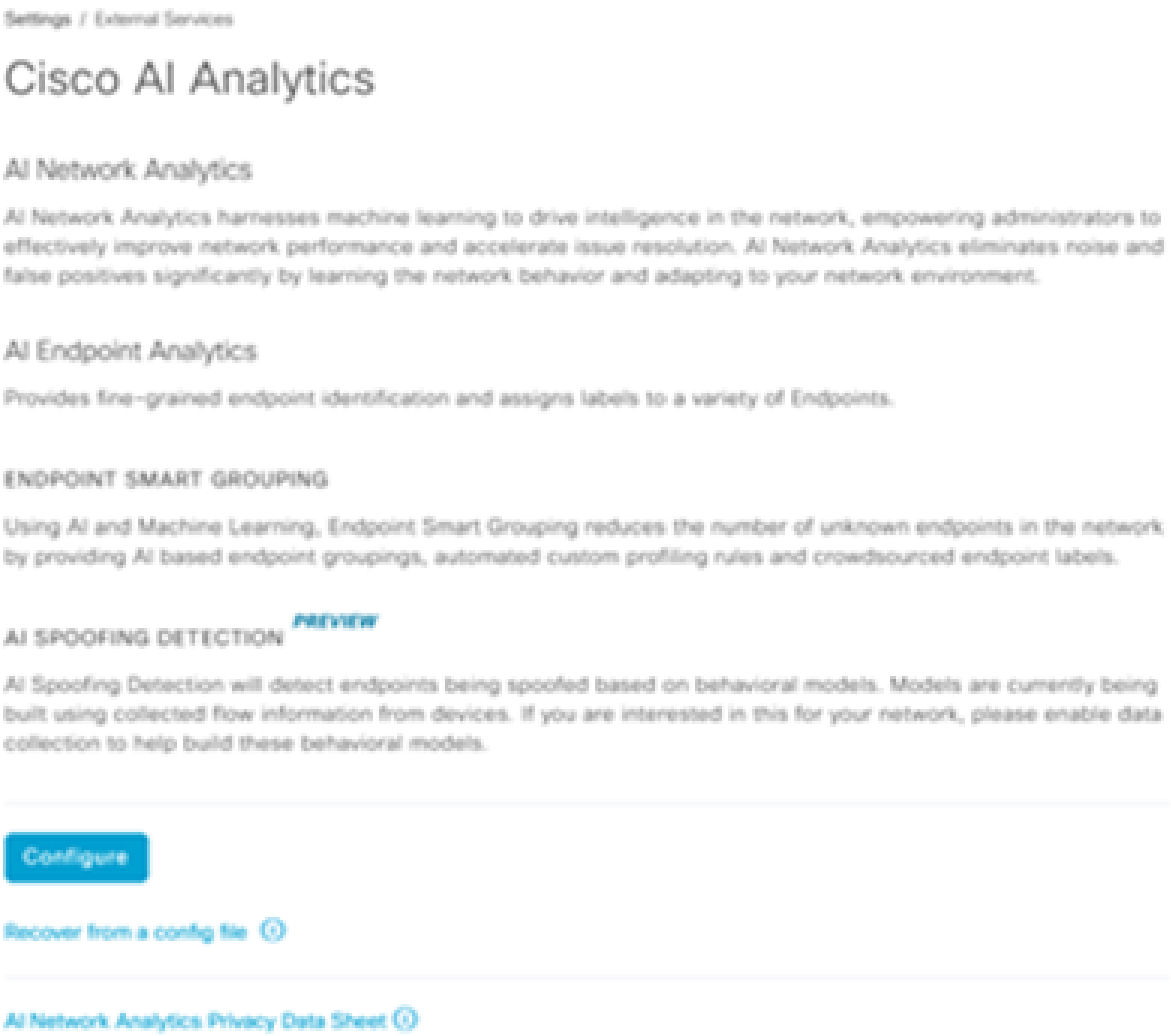
Netzwerkbereitstellung sind, sodass Sie Probleme schnell beheben können. Netzwerk- und Telemetrieinformationen werden im Cisco DNA Center anonymisiert und dann über einen sicheren verschlüsselten Kanal an die Cloud-basierte Infrastruktur von Cisco AI Analytics gesendet. Die Cisco AI Analytics-Cloud führt das maschinelle Lernmodell mit diesen Ereignisdaten aus und bringt die Probleme und allgemeinen Erkenntnisse zurück ins Cisco DNA Center. Alle Cloud-Verbindungen erfolgen ausgehend über TCP/443. Es gibt keine eingehenden Verbindungen. Die Cisco AI Cloud initiiert keine TCP-Flows zum Cisco DNA Center. FQDN (Fully Qualified Domain Names), die zum Zeitpunkt der Erstellung dieses Artikels im HTTPS-Proxy und/oder in der Firewall zugelassen werden können, sind:

- https://api.use1.prd.kairos.ciscolabs.com (Ostregion der USA)
- https://api.euc1.prd.kairos.ciscolabs.com (EU-Zentralregion)

Die bereitgestellte Cisco DNA Center-Appliance muss in der Lage sein, die verschiedenen von Cisco gehosteten Domänennamen im Internet aufzulösen und zu erreichen.

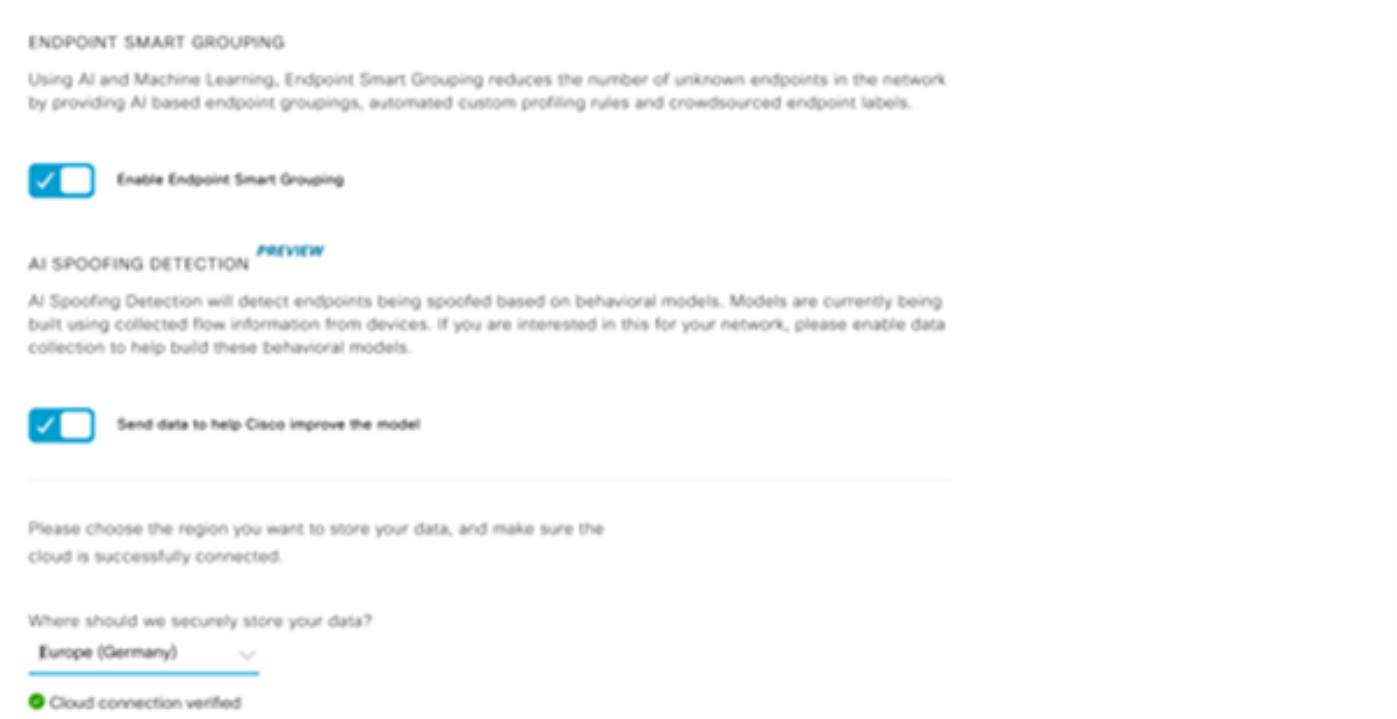
Befolgen Sie diese Schritte, um das Cisco DNA Center mit der Cisco AI Cloud zu verbinden.

- Besuchen Sie die Web-UI der Cisco DNA Center Appliance, um die KI Cloud-Registrierung abzuschließen:
- Navigieren Sie zu System > Einstellungen > Externe Dienste > Cisco AI Analytics
- Klicken Sie auf Konfigurieren, und aktivieren Sie die Option Endpoint Smart Grouping and AI spoof detection.
- Die intelligente Endpunktgruppierung verwendet die AI/ML-Cloud zum Clustern unbekannter Endpunkte, um Administratoren bei der Kennzeichnung dieser Endpunkte zu helfen. Dies ist sehr nützlich, um die Unbekannten im Netzwerk zu reduzieren.
- Die Erkennung von KI-Spoofing unterstützt Cisco beim Sammeln zusätzlicher NetFlow/Telemetrieinformationen und hilft bei der Modellierung des Endgeräts.
- Wählen Sie den Standort aus, der der geografischen Region der Bereitstellung am nächsten kommt. Nach der Überprüfung der Cloud-Verbindung und der erfolgreichen Herstellung der Verbindung wird ein grünes Kontrollkästchen angezeigt.



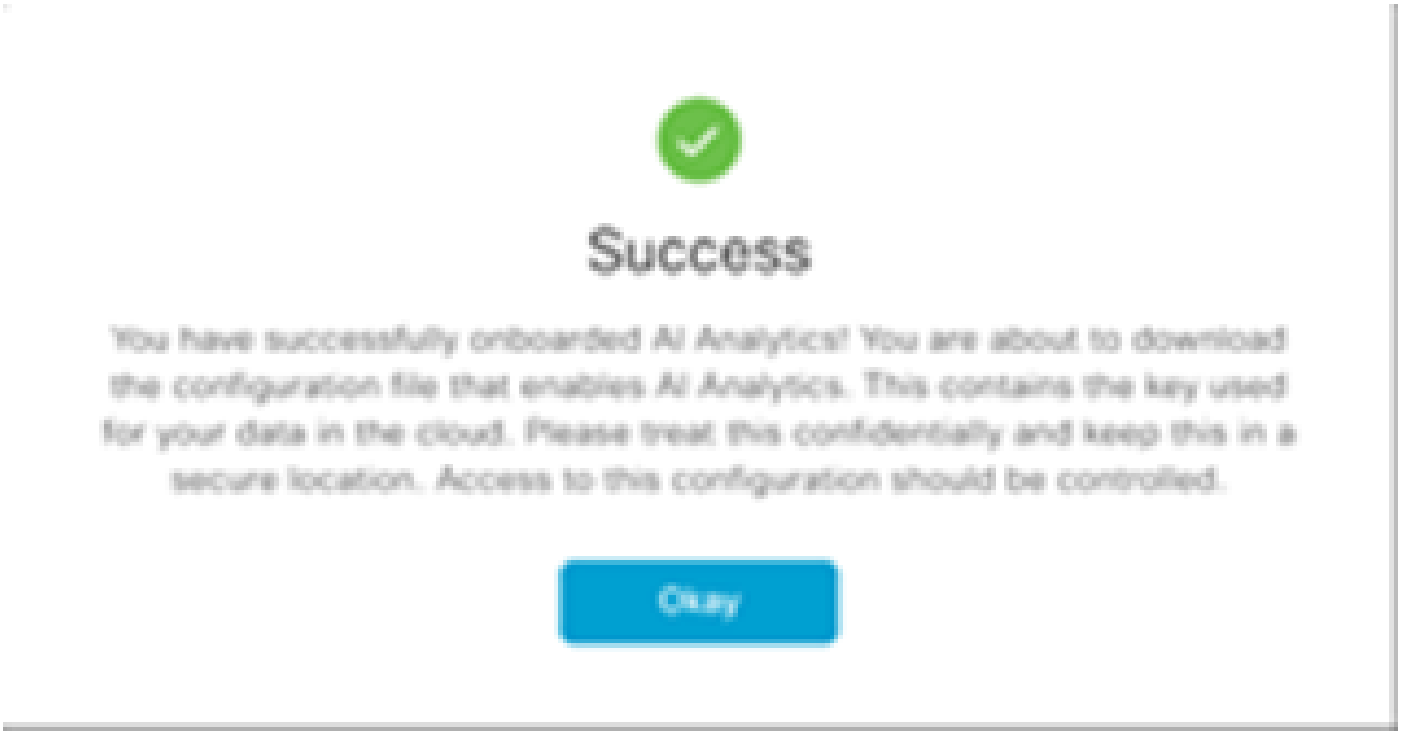
Konfigurieren der Benutzeroberfläche von Cisco AI Analytics

- Wenn die Verbindung fehlschlägt, überprüfen Sie die Proxy-Einstellungen in Cisco DNA Center auf der Seite System > Settings > System Configuration > Proxy config (System > Einstellungen > Systemkonfiguration > Proxy-Konfiguration), ob ein Proxy verwendet wird. Es ist auch empfehlenswert, alle Firewall-Regeln zu überprüfen, die diese Kommunikation blockieren könnten.



Überprüfung der Cisco AI/ML Cloud-Verbindung

- Akzeptieren Sie das Cisco Universal Cloud Agreement, um KI-Analysen zu ermöglichen.
- An diesem Punkt ist die Integration abgeschlossen, und ein entsprechendes Dialogfeld wird angezeigt.



Dialogfeld "Erfolg" nach der Registrierung

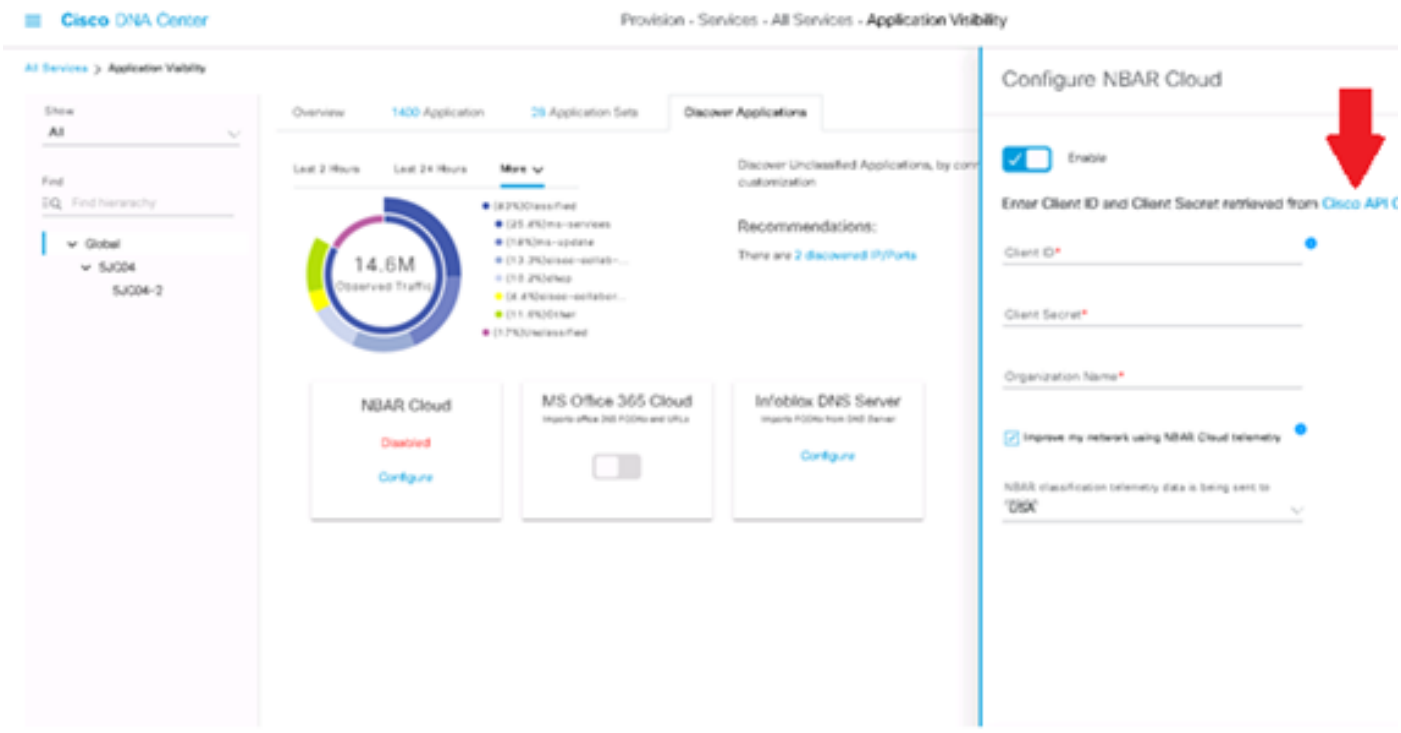
Die Network Based Application Recognition (NBAR) Cloud

Die Telemetrie-Appliance und die Catalyst 9000-Plattform erfassen Endpunkt-Metadaten mithilfe von Deep Packet Inspection der Paketflüsse und wenden Network Based Application Recognition (NBAR) an, um zu bestimmen, welche Protokolle und Anwendungen im Netzwerk verwendet werden. Cisco DNA Center verfügt über ein integriertes NBAR-Protokollpaket, das aktualisiert werden kann. Die Telemetriedaten können zur weiteren Analyse und zur Erkennung unbekannter Protokollsignaturen an die Cisco NBAR-Cloud gesendet werden. Um dies zu erreichen, muss die Cisco DNA Center-Appliance an die Cloud gebunden werden. Network-Based Application Recognition (NBAR) ist eine von Cisco entwickelte Engine zur erweiterten Anwendungserkennung, die verschiedene Klassifizierungsverfahren nutzt und Klassifizierungsregeln leicht aktualisieren kann.

Führen Sie diese Schritte aus, um das Cisco DNA Center an die Cisco NBAR Cloud anzubinden.

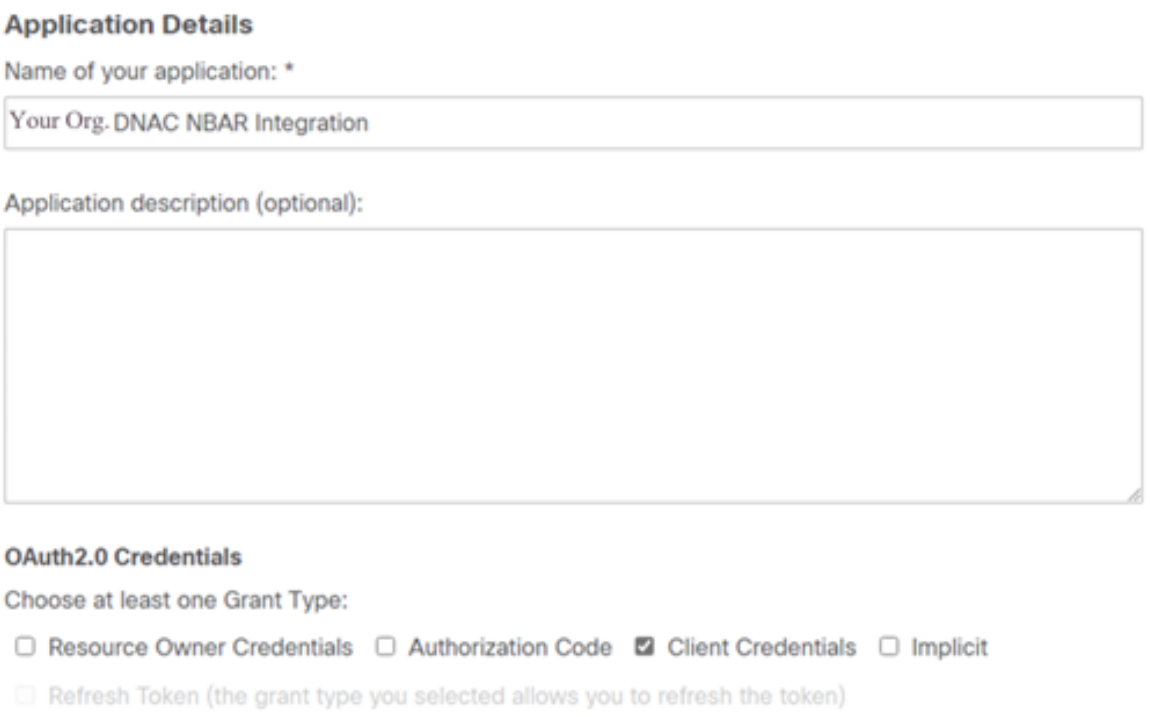
- Gehen Sie auf der Benutzeroberfläche von Cisco DNA Center zu Bereitstellung > Dienste > Anwendungstransparenz. Klicken Sie unter NBAR Cloud auf Konfigurieren, um ein Fenster zu öffnen. Aktivieren Sie den Dienst.
- Wenn Sie die Client-ID, den Client-Schlüssel und den Organisationsnamen haben, geben Sie diesen je nach Organisation eindeutige Namen, und verwenden Sie.
- Zum Zeitpunkt der Erstellung dieses Dokuments ist die einzige NBAR Cloud-Region derzeit in den USA verfügbar. In Zukunft werden möglicherweise weitere Regionen verfügbar sein. Wählen Sie in den Bereitstellungseinstellungen die Option aus, und speichern Sie sie.

Um die Client-ID und die Client Secret-Anmeldeinformationen abzurufen, klicken Sie auf den Link "Cisco API Console". Daraufhin wird ein Portal geöffnet. Melden Sie sich mit der entsprechenden CCO-ID an, erstellen Sie eine neue App, wählen Sie die Optionen für die NBAR-Cloud aus, und füllen Sie das Formular aus. Nach Abschluss dieses Vorgangs erhalten Sie eine Client-ID und einen Schlüssel. Siehe nachstehende Abbildung.



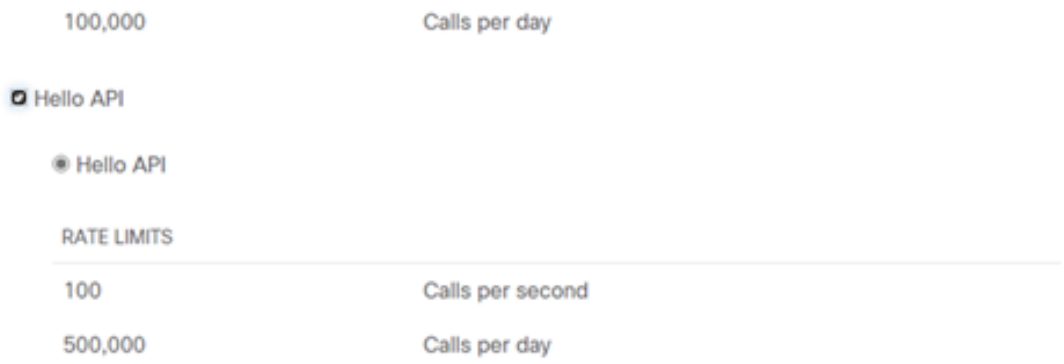
Cisco API-Link zum Abrufen der Client-ID und des geheimen Schlüssels

Diese Images zeigen die Optionen für die Registrierung in der NBAR-Cloud.



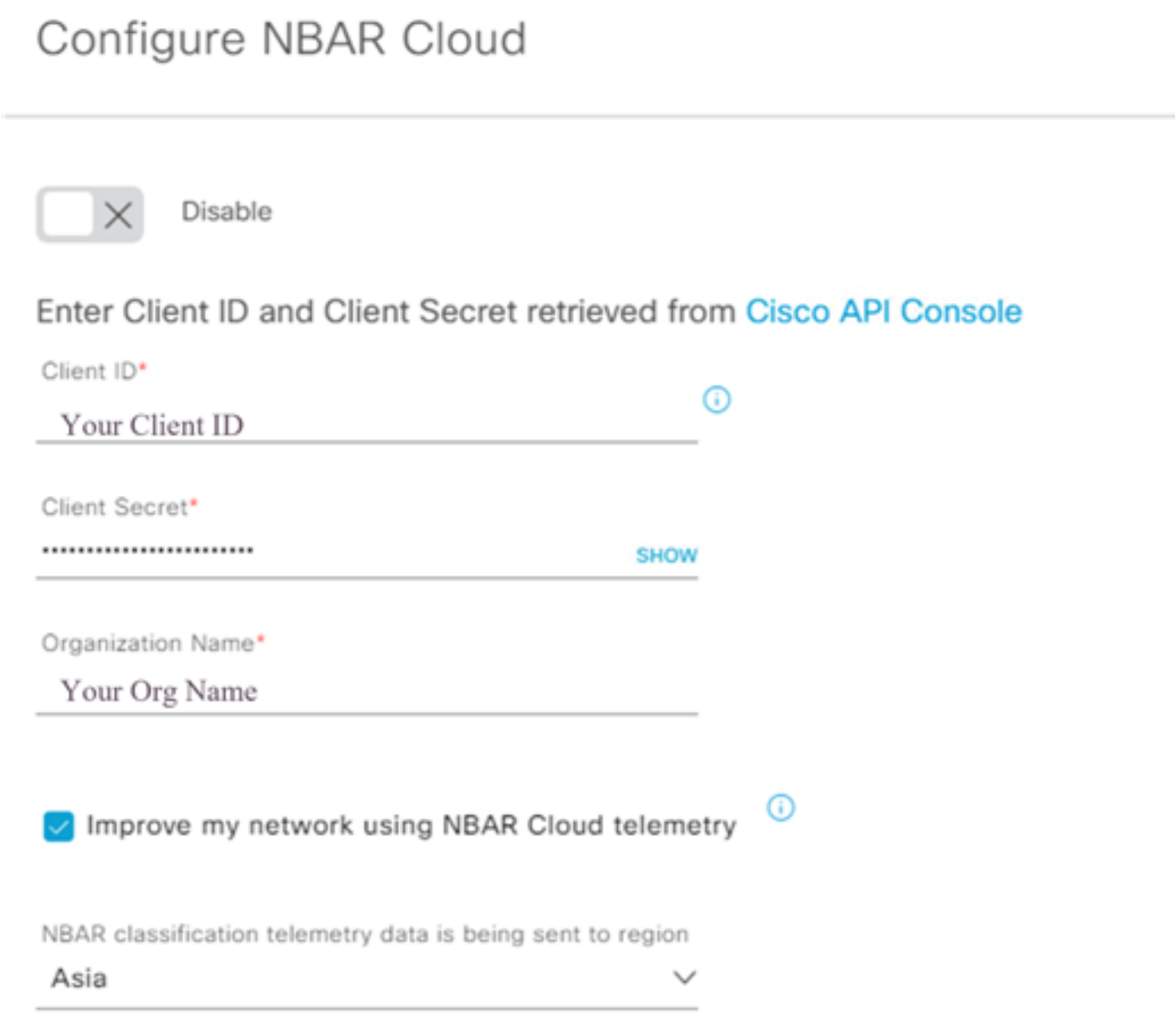
Details der NBAR Cloud-Anwendung

- Verwenden Sie dieses Bild als Referenz, während Sie die Details der API-Anforderung vervollständigen.



API-Details für Anwendungen

- Geben Sie die Client-ID und den geheimen Schlüssel aus dem Cisco Portal in Cisco DNA Center ein.



Client-ID und Schlüssel auf DNAC konfigurieren

CBAR (Controller-basierte Anwendungserkennung) und SD-AVC

CBAR wird zur Klassifizierung Tausender Netzwerkanwendungen, privater Anwendungen und des allgemeinen Netzwerkverkehrs verwendet. So kann das Cisco DNA Center Informationen zu Anwendungen erhalten, die dynamisch in der Netzwerkinfrastruktur verwendet werden. CBAR hilft, das Netzwerk auf dem neuesten Stand zu halten, indem es neue Anwendungen identifiziert, deren Präsenz im Netzwerk weiter zunimmt, und ermöglicht Aktualisierungen von Protokollpaketen. Wenn die Anwendungstransparenz aufgrund veralteter Protokollpakete verloren geht, kann es zu einer fehlerhaften Kategorisierung und anschließenden Weiterleitung kommen. Dies führt nicht nur zu Sichtbarkeitslücken im Netzwerk, sondern auch zu falschen

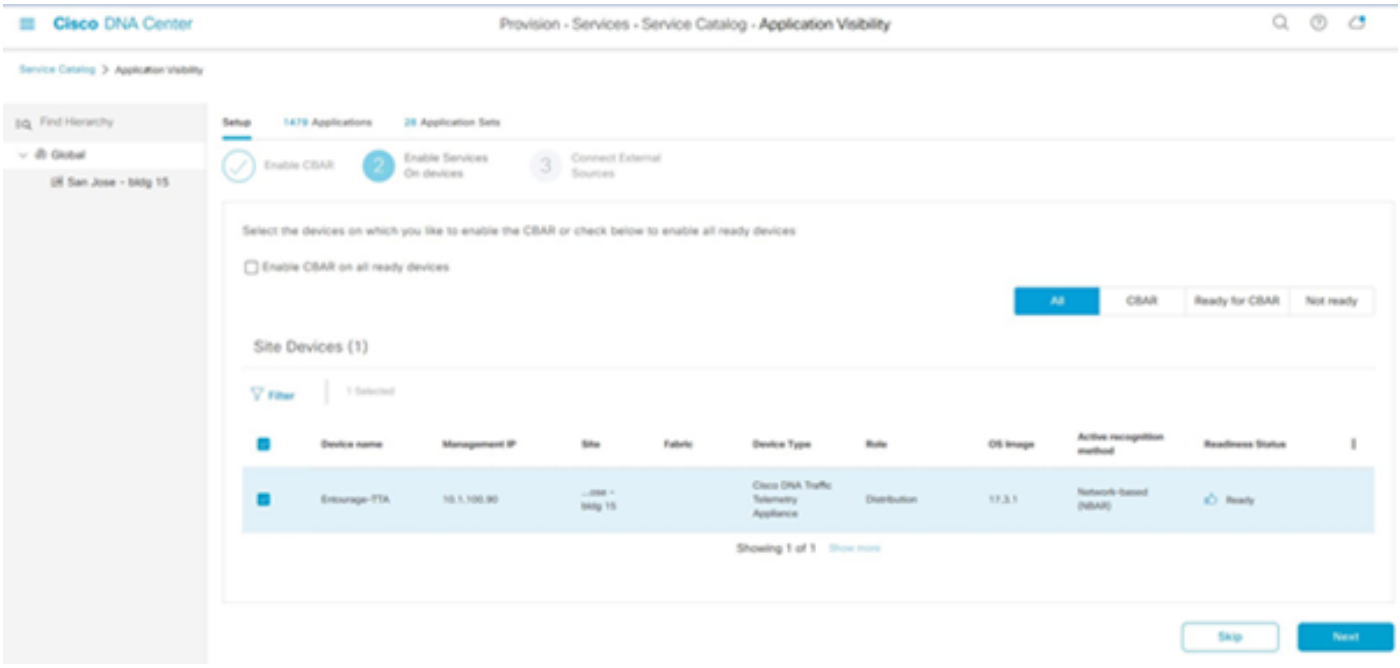
Warteschlangen- oder Weiterleitungsproblemen. CBAR löst dieses Problem, indem es die Bereitstellung aktualisierter Protokollpakete im gesamten Netzwerk ermöglicht.

Cisco Software-Defined AVC (SD-AVC) ist eine Komponente von Cisco Application Visibility and Control (AVC). Er fungiert als zentralisierter Netzwerkservice, der mit bestimmten teilnehmenden Geräten in einem Netzwerk arbeitet. SD-AVC unterstützt auch das DPI der Anwendungsdaten. Zu den aktuellen Funktionen und Vorteilen von SD-AVC gehören:

- Erkennung von Anwendungen auf Netzwerkebene konsistent im gesamten Netzwerk
- Verbesserte Anwendungserkennung in symmetrischen und asymmetrischen Routing-Umgebungen
- Verbesserte erste Paketerkennung
- Protokollpaket-Update auf Netzwerkebene
- Sicheres browserbasiertes SD-AVC-Dashboard über HTTPS zur Überwachung der SD-AVC-Funktionen und -Statistiken sowie zur Konfiguration von Protokollpaket-Updates im gesamten Netzwerk

Führen Sie die folgenden Schritte aus, um CBAR für relevante Geräte zu aktivieren.

- Gehen Sie zum Menü von Cisco DNA Center unter Provisioning > Application Visibility. Die Fehlermeldung Wenn die Seite "Application Visibility" (Anwendungstransparenz) zum ersten Mal geöffnet wird, wird dem Benutzer der unten gezeigte Konfigurationsassistent angezeigt.
- Nachdem Sie die Geräte für jeden Standort im Cisco DNA Center erkannt haben, wählen Sie das Gerät aus, auf dem CBAR aktiviert werden soll, und fahren Sie mit dem nächsten Schritt fort.



Aktivieren von CBAR auf dem Gerät

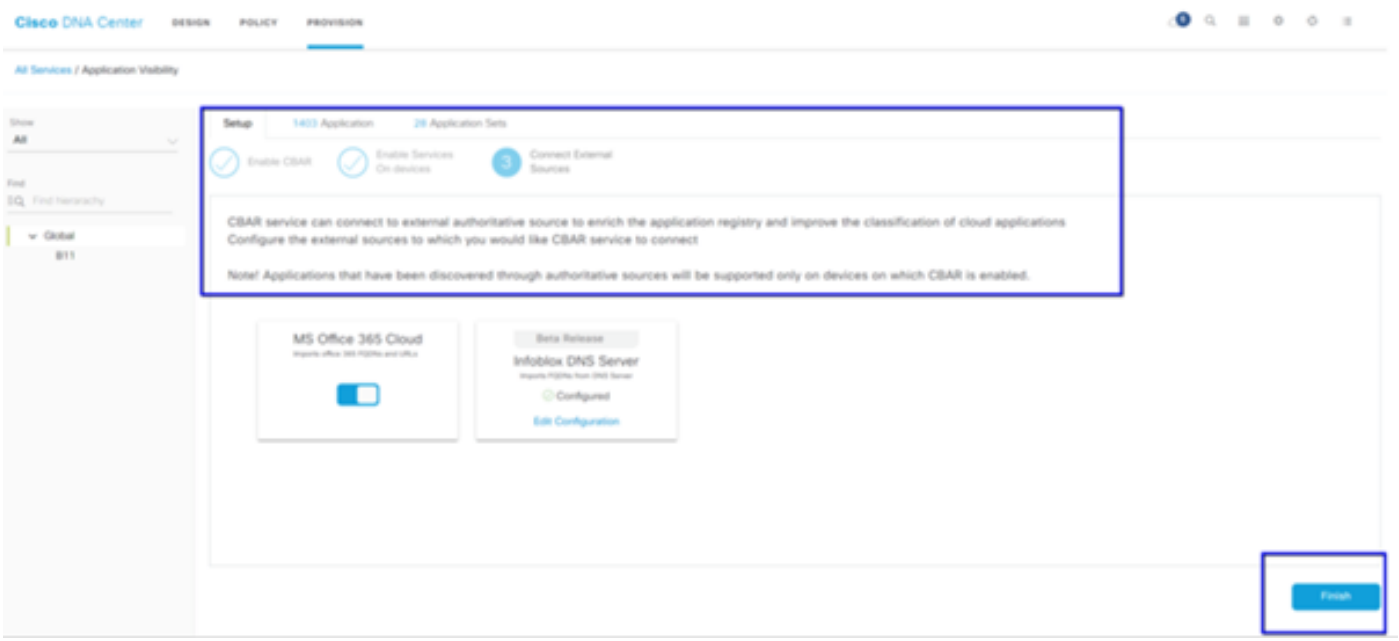
Microsoft Office 365 Cloud Connector (kein Pflichtprogramm)

Cisco DNA Center kann direkt in den Microsoft RSS-Feed integriert werden, um sicherzustellen,

dass die Anwendungserkennung für Office 365 mit den veröffentlichten Richtlinien übereinstimmt. Diese Integration wird im Cisco DNA Center als Microsoft Office 365 Cloud Connector bezeichnet. Es empfiehlt sich, diese Funktion bereitzustellen, wenn der Benutzer Microsoft Office 365-Anwendungen im Netzwerk ausführt. Die Integration mit Microsoft Office 365 ist nicht erforderlich. Ist diese Option nicht aktiviert, kann Cisco DNA Center Hostdaten von Microsoft Office 365 nur verarbeiten und klassifizieren. Im Cisco DNA Center ist die Erkennung von Microsoft Office 365-Anwendungen bereits integriert. Durch die direkte Integration mit dem Anwendungsanbieter kann Cisco DNA Center jedoch aktuelle und präzise Informationen zu den aktuellen geistigen Eigentumsblöcken und URLs abrufen, die von der Microsoft Office 365-Suite verwendet werden.

Um Cisco DNA Center in die Microsoft Office 365 Cloud zu integrieren, befolgen Sie diese Schritte.

- Klicken Sie auf das Menü-Symbol, und wählen Sie Provisioning > Services > Application Visibility.
- Klicken Sie auf Anwendungen suchen
- Klicken Sie auf die MS Office 365 Cloud-Umschaltfläche, um Cisco DNA Center in die Microsoft Office 365 Cloud zu integrieren.

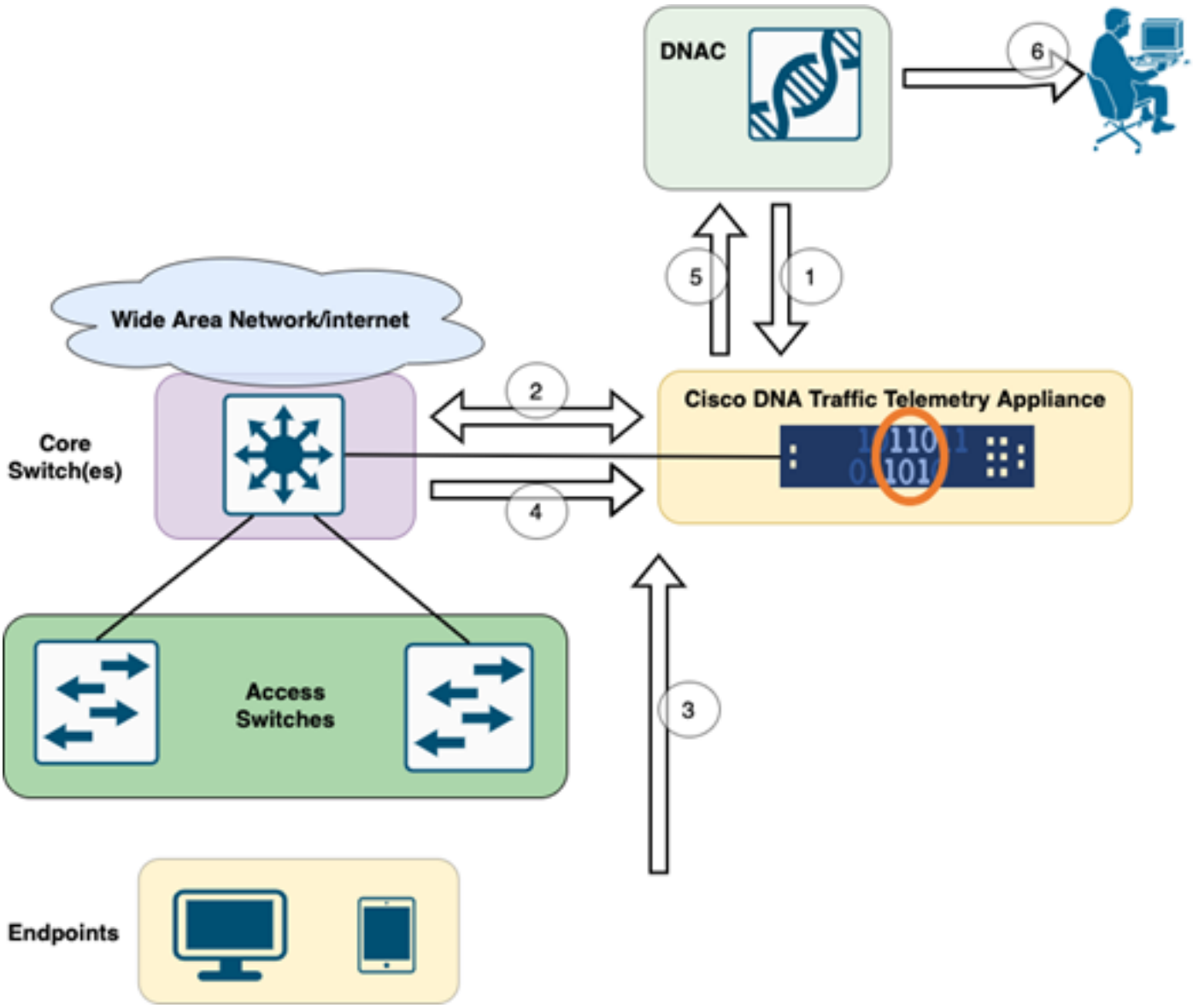


MS O365 Cloud-Integration

TTA-Implementierung

In diesem Abschnitt werden die erforderlichen Schritte zur Implementierung der TTA in einem Netzwerk beschrieben.

Übersicht über TTA-Workflow



TTA-zu-DNAC-Workflow

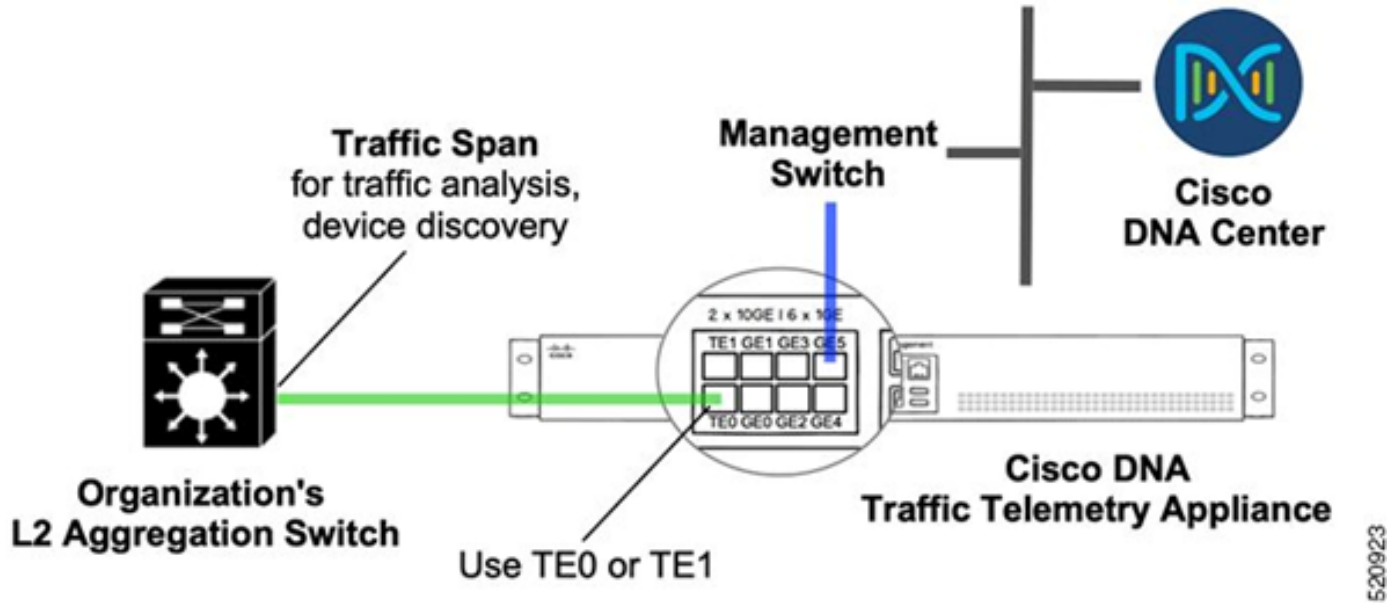
Die in diesem Diagramm hervorgehobenen Schritte beschreiben den Prozess- und Telemetriestrom zwischen TTA und Cisco DNA Center. Diese Schritte sind hier näher ausgeführt.

1. Die Cisco Traffic Telemetry Appliance ist entweder mit dem Aggregation Switch des Standorts oder dem Core-Switch der Netzwerkinfrastruktur verbunden. Über diese Verbindung kann die Appliance Datenverkehrsdaten von verschiedenen Access Switches im Netzwerk empfangen.
2. Die Cisco Traffic Telemetry Appliance ist in das Cisco DNA Center als Netzwerkmanagement-Plattform integriert. Diese Integration ermöglicht die nahtlose Kommunikation und den Datenaustausch zwischen der Appliance und dem Cisco DNA Center.
3. Wenn Benutzerdatenverkehr durch das Netzwerk fließt, wird er auf die Cisco Traffic Telemetry Appliance verteilt oder gespiegelt. Das bedeutet, dass eine Kopie des Netzwerkverkehrs zu Überwachungs- und Analysezwecken an die Appliance gesendet wird, während der ursprüngliche Datenverkehr seinen normalen Pfad fortsetzt.
4. Die Cisco Traffic Telemetry Appliance erfasst und verarbeitet die empfangenen Verkehrsdaten. Es extrahiert relevante Informationen aus dem gespiegelten Datenverkehr,

z. B. Paketebenendetails, Flussstatistiken und Leistungsmetriken.

5. Die verarbeiteten Telemetrieinformationen werden dann von der Cisco Traffic Telemetry Appliance an das Cisco DNA Center gesendet. Mit dieser Kommunikation erhält das Cisco DNA Center Echtzeit-Informationen und -Updates zu Datenverkehrsmustern, der Anwendungsleistung und Anomalien im Netzwerk.
6. Die vom Cisco DNA Center generierten Telemetrie-Erkenntnisse liefern wertvolle Informationen für Netzwerkadministratoren. Sie können die Schnittstelle von Cisco DNA Center nutzen, um die erfassten Daten anzuzeigen und zu analysieren, Einblicke in den Netzwerkzustand und die Anwendungsleistung zu erhalten, potenzielle Probleme zu identifizieren und fundierte Entscheidungen für die Netzwerkoptimierung und Fehlerbehebung zu treffen.

TTA-Bereitstellung: Allgemeines Diagramm



TTA-Bereitstellung: Allgemein

Das obige Diagramm zeigt, wie TTA im Netzwerk verbunden werden kann. Die 10-Gig- und 1-Gig-Schnittstellen können zur SPAN-Aufnahme mit Leitungsgeschwindigkeit verwendet werden. Die Gi0/0/5-Schnittstelle wird für die Kommunikation mit Cisco DNA Center, für die Orchestrierung und für die Weiterleitung von Telemetrie-Erkenntnissen an Cisco DNA Center verwendet. Diese Schnittstelle KANN NICHT für die SPAN-Erfassung verwendet werden.

TTA-Software- und Lizenzierungsanforderungen

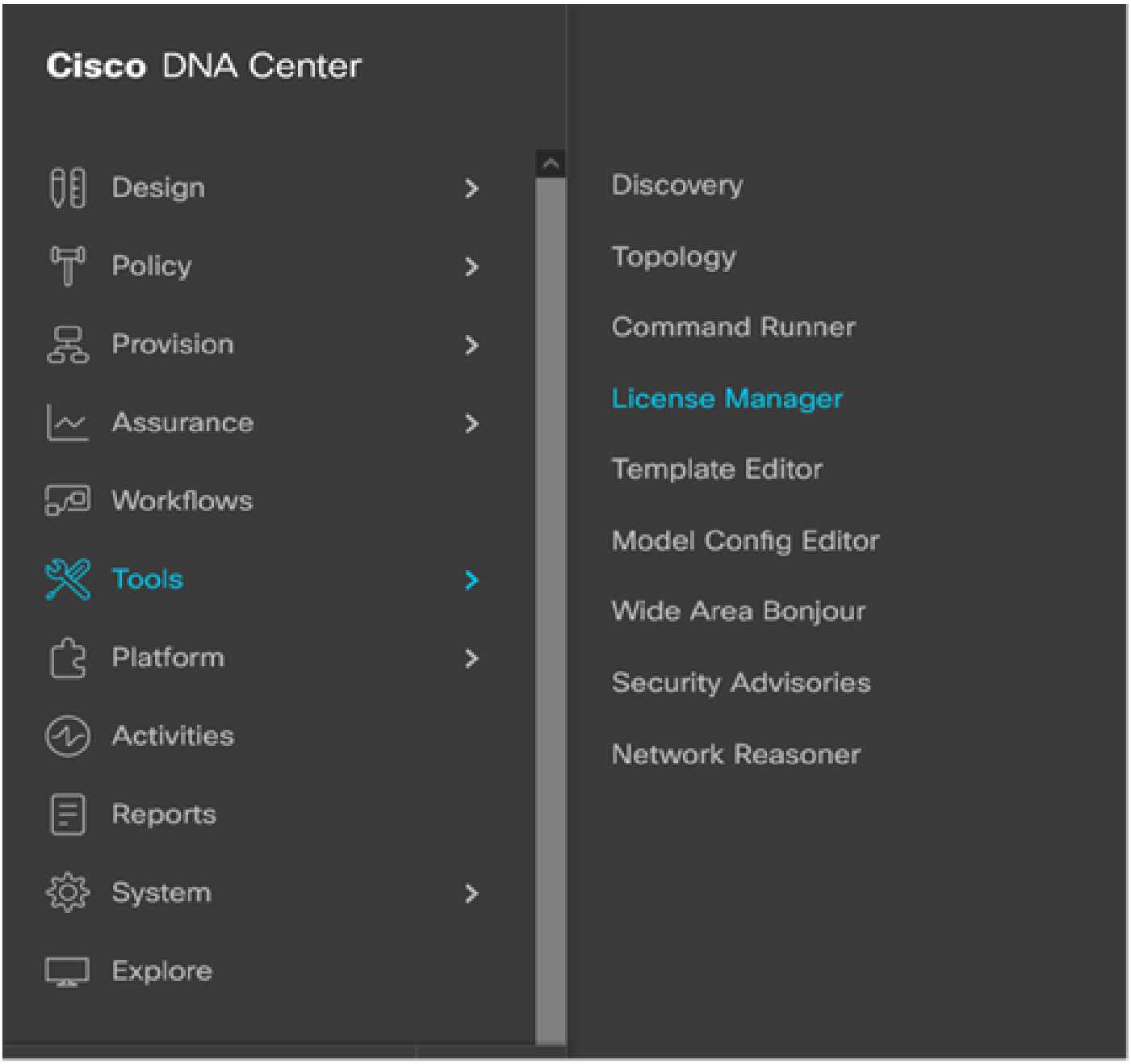
TTA-Appliances, die im Netzwerk bereitgestellt werden, sind von entscheidender Bedeutung für die Bereitstellung von Telemetriedaten zu Benutzerdaten und Benutzerendpunkten. Um die Lösung erfolgreich bereitstellen zu können, müssen diese Anforderungen erfüllt sein.

- TTA muss mit einer anfänglichen Bootstrap-Konfiguration konfiguriert werden, damit sie vom Cisco DNA Center erkannt werden kann (TTA-Bootstrap-Konfiguration)
- Die TTA-Appliance muss in das Cisco DNA Center integriert werden, damit sie vom Cisco

DNA Center verwaltet werden kann (Hinzufügen der Telemetriekarte zum Cisco DNA Center-Inventar)
- Die richtige Lizenz muss auf der TTA (TTA Appliance-Lizenz) installiert werden.

Die Appliance unterstützt nur ein Betriebssystem und erfordert die Cisco DNA TTA Advantage-Lizenz zum Erfassen von Telemetriedaten. Es ist keine Funktionslizenz (wie IP Base oder Advanced IP Services) oder ein unbefristetes Lizenzpaket (wie Network Essentials oder Network Advantage) erforderlich.

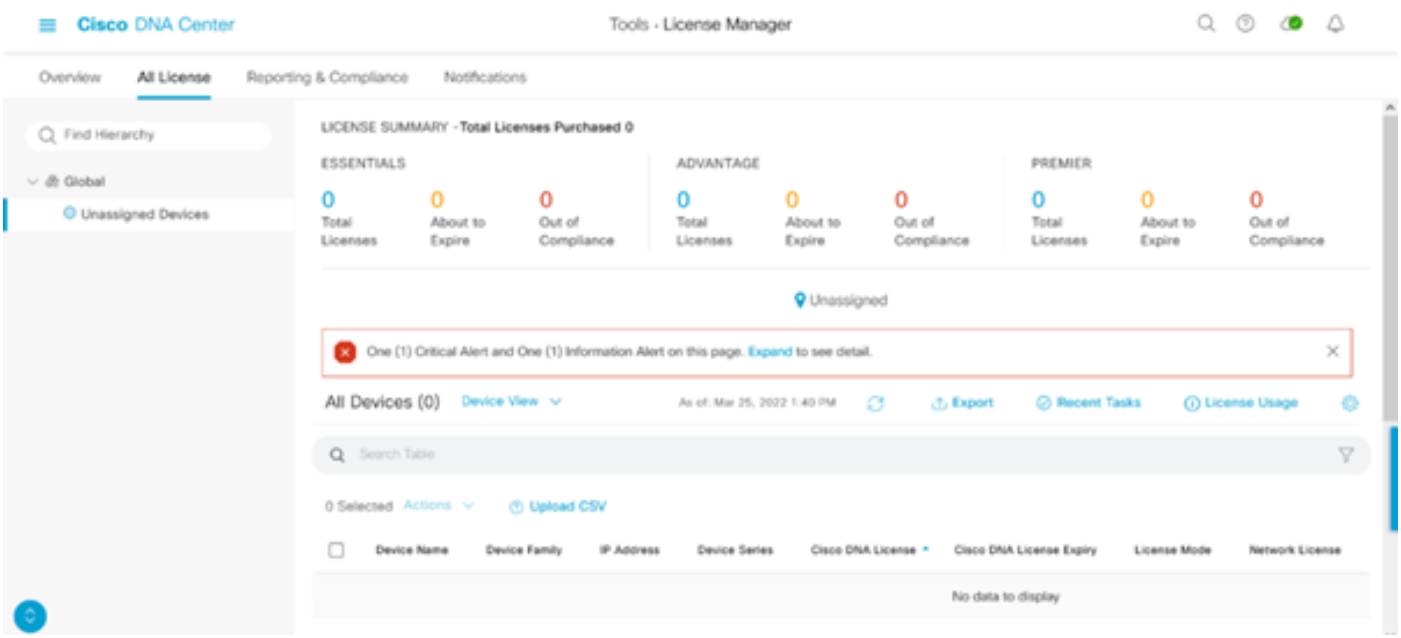
Um Lizenzen im Cisco DNA Center zu verwalten, navigieren Sie zum Lizenzmanager, indem Sie im Dropdown-Menü von Cisco DNA Center auf Tools > License Manager klicken.



Lizenzmanager auf DNAC

- Navigieren Sie zur Seite All License (Alle Lizenzen). Diese sieht ähnlich aus wie in diesem Bild. Auf dieser Seite kann der Administrator Lizenzen für Netzwerkgeräte wie die des TTA

verwalten.



Alle Lizenzen auf DNAC

TTA-Onboarding und Day-0-Konfiguration

Um die Erkennung und Integration der TTA-Appliance durch Cisco DNA Center zu erleichtern, müssen auf den TTA-Appliances des Standorts Bootstrap-Befehle konfiguriert werden. Nach der Bootstrap-Konfiguration ist der TTA über das Dashboard von Cisco DNA Center sichtbar. Nachfolgend sind die Day-0-Konfigurationselemente für eine TTA-Appliance aufgeführt. Sobald das Gerät in die Standorthierarchie integriert wurde, übernimmt die TTA-Appliance die übrigen Konfigurationselemente von 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
```

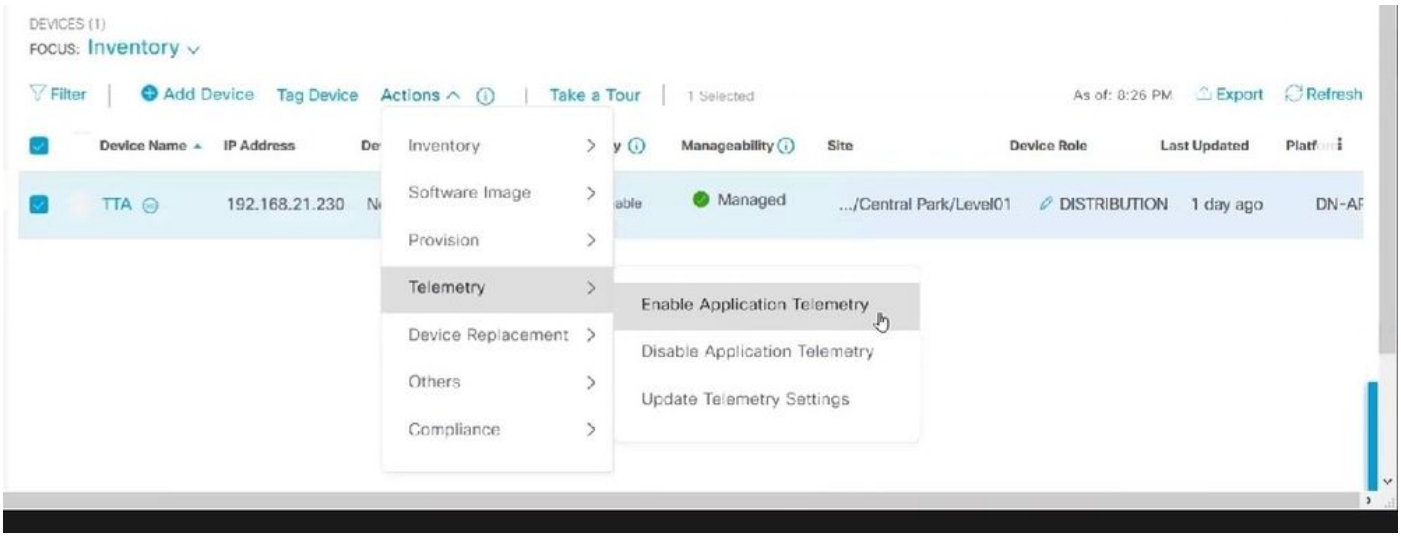
```
login local
transport input ssh
transport preferred none
ip ssh source-interface GigabitEthernet0/0/5

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
```

Sobald diese Elemente für den TTA konfiguriert wurden, kann er vom Cisco DNA Center erkannt werden.

Hinzufügen der TTA-Appliance zum Inventar von Cisco DNA Center

Um die TTA nutzen zu können, muss Cisco DNA Center die TTA-Appliance erkennen und verwalten. Sobald der TTA in Cisco DNA Center integriert ist, kann er über das Cisco DNA Center verwaltet werden. Bevor die TTA-Appliance erkannt wird, müssen wir sicherstellen, dass die vollständige Standorthierarchie für den Standort vorhanden ist. Danach fahren wir fort, die TTA-Appliance unter der spezifischen Standorthierarchie hinzuzufügen, indem wir die folgenden Schritte auf der Seite Menu > Provision > Devices > Inventory (Menü > Geräte > Bestand) ausführen, um das Gerät einem Standort hinzuzufügen.

1. Geben Sie den Benutzernamen/das Kennwort (CLI) und die SNMP-Community an, die für die Verbindung mit dem Gerät und die Aktivierung des Kennworts erforderlich sind. Warten Sie, bis das Gerät erfolgreich hinzugefügt wurde, bevor Sie fortfahren.
2. Überprüfen Sie den Gerätenamen, die Produktfamilie (Netzwerkmanagement bei TTA), Erreichbarkeit - Erreichbar, Verwaltbar, Geräterolle - Verteilung. Das Gerät ist zunächst nicht konform, nach der vollständigen Bereitstellung ändert sich der Status jedoch.
3. Sobald das TTA integriert ist, überträgt Cisco DNA Center Konfigurationsvorlagen, um erweiterte Telemetriefunktionen zu konfigurieren.



TTA-Erkennung und Aktivierung von Anwendungstelemetrie

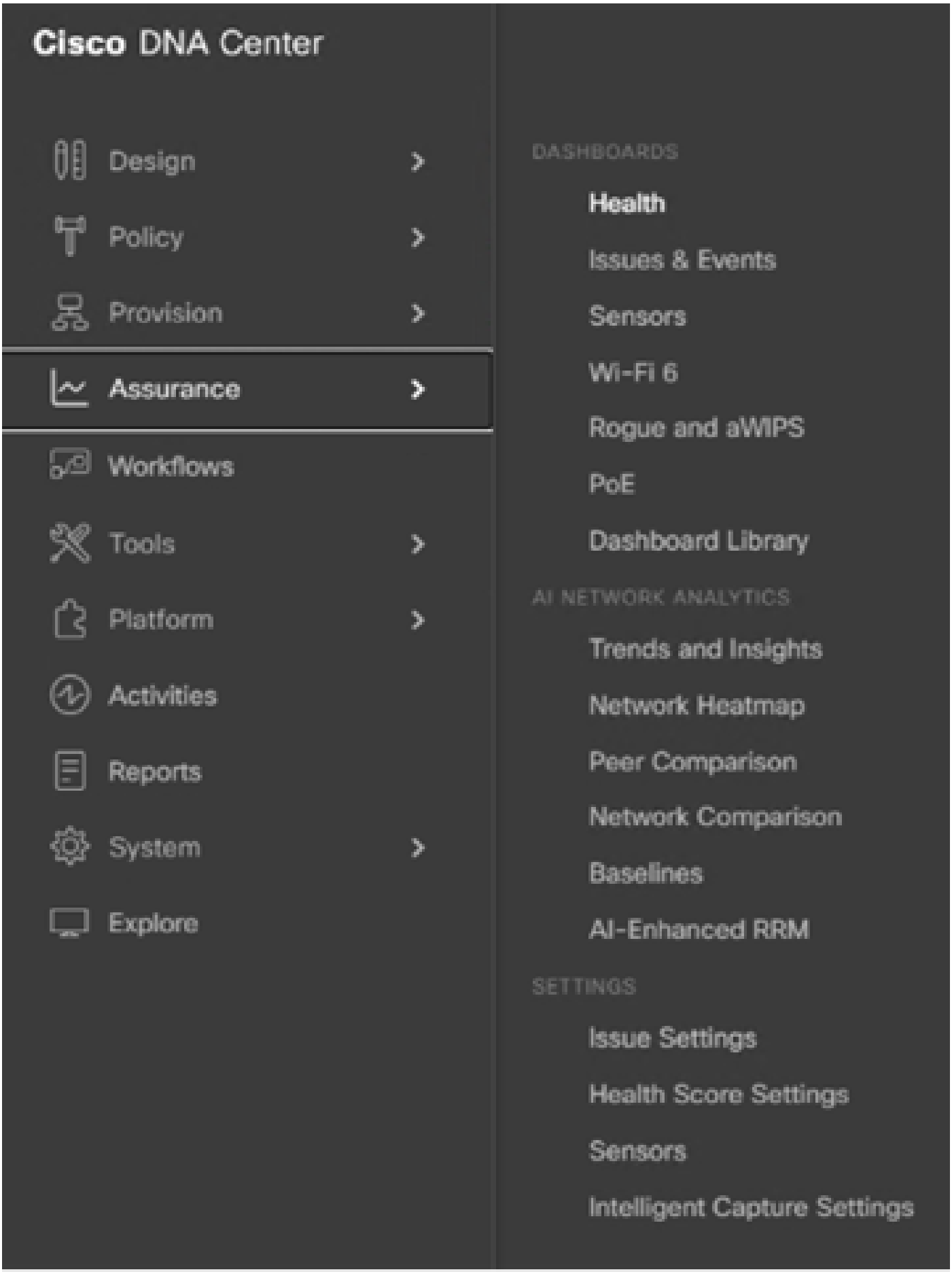
SPAN-Konfiguration

Abhängig von den Hardwarefunktionen des Core-Switches kann die SPAN-Sitzung so konfiguriert werden, dass sie eine Gruppe von VLANs oder eine oder mehrere Schnittstellen mit der mit dem TTA verbundenen Schnittstelle SPAN verbindet. Eine Beispielkonfiguration ist hier angegeben.

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

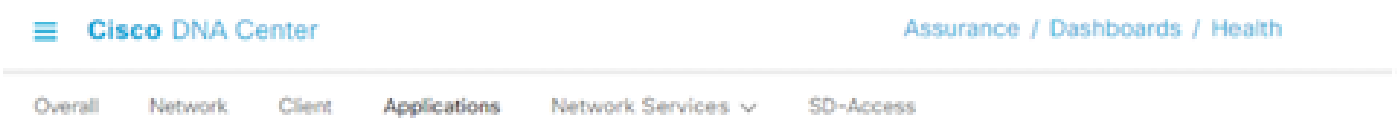
Gesicherte Informationen

Um auf die von der installierten Traffic Telemetry Appliance erfassten Assurance-Daten zuzugreifen, gehen Sie zum Abschnitt Assurance, und klicken Sie auf Health (Integrität).

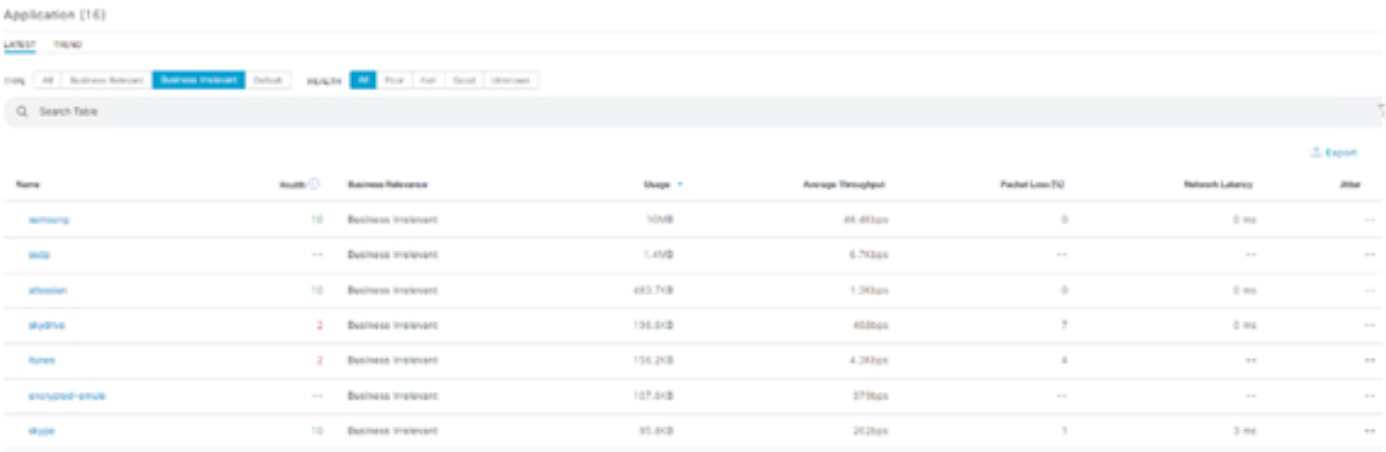


Navigieren zu Anwendungssicherheit

Wählen Sie Applications (Anwendungen) aus, und Sie erhalten einen umfassenden Überblick über Anwendungsdaten, einschließlich Latenz und Jitter, die vom TTA basierend auf dem jeweiligen Anwendungstyp erfasst werden.



Navigieren zu Application Assurance



Detaillierte Benutzeroberfläche für Application Assurance

Für eine detailliertere Analyse können Benutzer einzelne Anwendungen erkunden, indem sie auf die jeweilige Anwendung klicken und den Exporter auswählen, der die Traffic Telemetry Appliance bilden soll. Anschließend können sie bestimmte Metriken untersuchen, z. B. Nutzung, Durchsatz und Paketverlust-Daten, Client-Netzwerklatenz, Server-Netzwerklatenz und Anwendungsserverlatenz.

Beispiel: Anwendungsangaben PT.1

Beispiel: Anwendungsangaben PT.2

Überprüfung

1. Nachdem Sie CBAR aktiviert haben, überprüfen Sie, ob der SD-AVC-Service (Application Visibility Control) auf dem Gerät aktiviert ist, indem Sie sich bei der Cisco Traffic Telemetry Appliance anmelden und diesen CLI-Befehl ausführen. Der Ausgang entspricht in etwa diesem Beispiel und zeigt die IP-Adresse des Controllers sowie den Status "Verbunden" an.

```
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. Verwenden Sie den Befehl "show license summary" in der CLI des TTA, um die entsprechenden Gerätelizenzdetails zu überprüfen.

```
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. Überprüfen Sie, ob die SPAN-Sitzung auf dem Kern-/Aggregations-Switch ordnungsgemäß konfiguriert wurde.

```
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. Sobald die TTA erfolgreich bereitgestellt wurde, werden diese Befehle an das Gerät gesendet (oder wurden gesendet).

```
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
```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.