Gebruik de Traffic Telemetry Appliance (TTA) en Cisco DNA Center App Assurance: het waarom en hoe

Inhoud

Inleiding

Dit document beschrijft het Cisco DNA Traffic Telemetry Appliance (Cisco-onderdeelnummer DN-APL-TTA-M) platform samen met hoe u Application Assurance in Cisco DNA Center kunt inschakelen. IHet werpt ook wat licht op hoe en waar de TTA in een netwerk samen met het configuratie- en verificatieproces kan worden geplaatst. Dit artikel gaat ook in op de verschillende voorwaarden waaraan moet worden voldaan.

Voorwaarden

Cisco raadt u aan te weten hoe Cisco DNA Center Assurance en Application Experience werken.

Toepassingsgarantie

Assurance is een multifunctionele, real-time, netwerkgegevensverzameling en analytics engine die het zakelijke potentieel van netwerkgegevens aanzienlijk kan verhogen. Assurance verwerkt complexe toepassingsgegevens en presenteert de bevindingen in Assurance gezondheidsdashboards om inzicht te geven in de prestaties van toepassingen die in het netwerk worden gebruikt. Afhankelijk van de plaats waar de gegevens worden verzameld, kunt u enkele of alle van de volgende punten zien:

- Toepassingsnaam
- Doorvoersnelheid
- DSCP-markeringen
- Prestatiegegevens (latentie, Jitter en pakketverlies)

Op basis van de hoeveelheid verzamelde gegevens kan Application Assurance in twee modellen worden gecategoriseerd:

- Toepassingszichtbaarheid (AppVis) en
- Toepassingservaring (AppX)

Toepassingsnaam en doorvoersnelheid worden gezamenlijk kwantitatieve maatstaven genoemd. Gegevens voor de kwantitatieve maatstaven zijn afkomstig van het inschakelen van Application Visibility.

DSCP-markeringen en -prestatiemetriek (latentie, Jitter en pakketverlies) worden gezamenlijk kwalitatieve metriek genoemd. Gegevens voor de kwalitatieve metriek komen van het toelaten van de Ervaring van de Toepassing.

Toepassingszichtbaarheid (AppVis)

Application Visibility data wordt verzameld van switches met Cisco IOS® XE en van draadloze controllers met AireOS. Voor switches met Cisco IOS XE worden toepassingszichtbaarheidsgegevens verzameld met behulp van een vooraf gedefinieerde NBAR-sjabloon die bidirectioneel (toegang en uitgang) wordt toegepast op de fysieke Layer Access switch-poorten. Voor draadloze controllers waarop AireOS draait, worden de Application Visibility-gegevens verzameld bij de draadloze controller en vervolgens wordt streaming telemetrie gebruikt om deze gegevens naar Cisco DNA Center te transporteren.

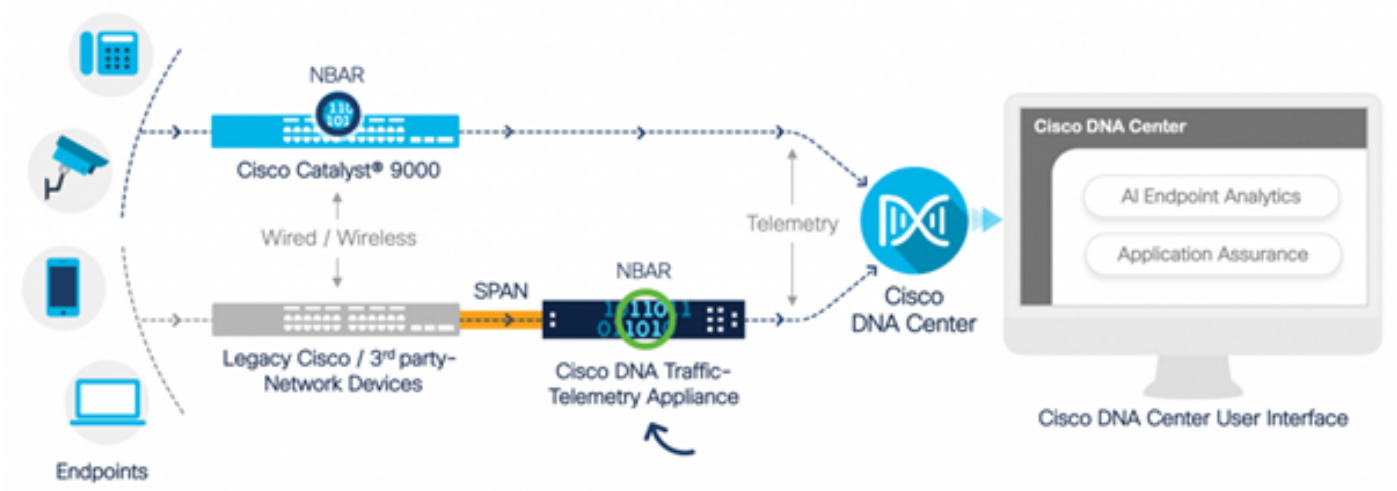
Toepassingservaring (AppX)

Application Experience-gegevens worden verzameld van Cisco IOS XE-routerplatforms, specifiek met behulp van de functie Cisco Performance Monitor (PerfMon) en de Cisco Application

Response Time (ART)-metriek. Voorbeelden van routerplatforms zijn de ASR 1000, ISR 4000 en CSR 1000v. Zie de Cisco DNA Center Compatibility Matrix voor apparaatcompatibiliteit met Cisco DNA Center.

Waarom een Traffic Telemetry-applicatie?

De Cisco Catalyst 9000 Series bekabelde en draadloze apparaten uitvoeren DPI (deep packet inspection) en bieden gegevensstromen voor services zoals Cisco AI Endpoint Analytics en Application Assurance in Cisco DNA Center. Maar wat als er geen Catalyst 9000 Series apparaten in het netwerk zijn om telemetrie uit te halen? Verschillende organisaties hebben nog steeds een deel van hun netwerkinfrastructuur die niet is gemigreerd naar de platforms van Cisco Catalyst 9000 Series. Het Catalyst 9000-platform genereert AppVis-telemetrie, maar om extra AppX-inzichten te krijgen, kan de Cisco DNA Traffic Telemetry-applicatie worden gebruikt om de kloof te overbruggen. Het doel van de TTA is om het verkeer te controleren dat het via SPAN-poorten ontvangt van andere netwerkapparaten die niet de mogelijkheid hebben om Application Experience-gegevens aan Cisco DNA Center te leveren. Aangezien de bestaande infrastructurele apparaten de grondige pakketinspectie niet kunnen uitvoeren die voor geavanceerde analyses vereist is, kan de Cisco DNA Traffic Telemetry Applicatie worden gebruikt om AppX-telemetrie te genereren uit bestaande legacy-implementaties.



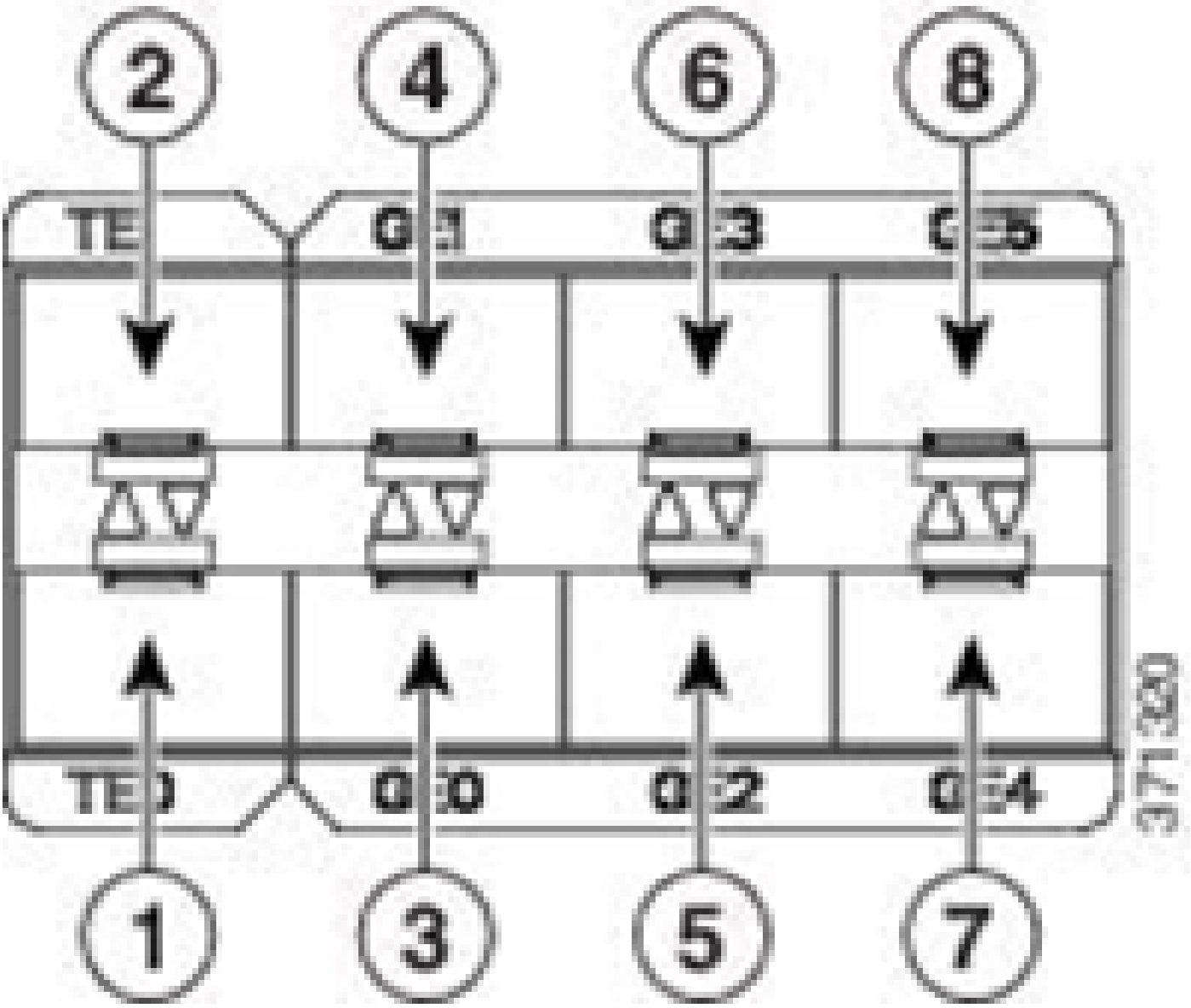
Cisco TTA in actie

TTA-apparaatgegevens

Het op Cisco IOS XE gebaseerde telemetriesensorplatform genereert telemetrie van gespiegeld IP-netwerkverkeer via Switched Port Analyzer (SPAN) sessies van switches en draadloze controllers. Het apparaat inspecteert duizenden protocollen met de NBAR-technologie (Network-Based Application Recognition) om een telemetriestroom te produceren die Cisco DNA Center kan gebruiken voor het uitvoeren van analyses. De Cisco DNA Traffic Telemetry Applicatie kan 20 Gbps duurzaam doorvoerverkeer verwerken en 40.000 endpointsessies controleren op apparaatprofilering.

De Cisco Traffic Telemetry-applicatie

De TTA heeft een mix van 10-Gig en 1-Gig links die worden gebruikt voor SPAN-inname. Van deze poorten is Gig0/0/5 de enige poort die met een IP-adres kan worden geconfigureerd en die kan worden gebruikt voor communicatie met Cisco DNA Center. De interfacematrix wordt hieronder getoond.



TTA-interfacematrix

TTA-interfacematrix			
1	10 GE SFP+ poort 10/100/2000	5	GE SFP-poort 20/10/2
2	10 GE SFP+ poort 10/10/2010	6	GE SFP-poort 20/10/3
3	GE SFP-poort 10/10/10	7	GE SFP-poort 10/10/4
4	GE SFP-poort 10/10/1	8	GE SFP-poort 20/10/5

Cisco DNA Center-vereisten voor garantie

Deze sectie beschrijft de configuraties en vereisten waaraan moet zijn voldaan voordat Cisco DNA Center telemetrie kan verwerken.

Operationeel Cisco DNA Center-cluster

Het Cisco DNA Center-cluster dat wordt gebruikt voor het beheer van de TTA en de procestelemetrie moet met deze criteria zijn uitgerust:

- Netwerkhiërarchie: De sectie van de Netwerkhiërarchie binnen het Ontwerpwerkschema wordt gebruikt om verschillende plaatscampussen, gebouwen binnen die campussen, en de individuele vloeren binnen die gebouwen te bepalen en hen te tonen op een wereldkaart. De juiste site/netwerkhiërarchie moet worden geconfigureerd.
- Netwerkinstellingen: In het gedeelte Netwerkinstellingen kunt u algemene standaardinstellingen voor het netwerk maken die worden gebruikt door de apparaten binnen het netwerk. Deze instellingen kunnen zowel op een globale manier als per site, gebouw of vloerniveau worden toegepast. Voer DNS, domeinnaam, syslog, NTP, tijdzone en loginbanner in zoals vereist door de implementatie.
- Apparaatreferenties: Deze referenties worden gebruikt om apparaten in het netwerk te openen en te ontdekken, inclusief de TTA. Het is vereist dat Cisco DNA Center wordt geconfigureerd met de juiste CLI- en SNMP-referenties. Samen met deze NetConf geloofsbrieven zijn goed om te hebben.
- Cisco CCO-account: Er is een geldige CCO-account vereist om het apparaat te verbinden en de mogelijkheden van de Cisco AI Cloud te benutten, afbeeldingen voor SWIM te downloaden en protocolpakketten voor TTA en andere apparaten te downloaden.

ISE- en Cisco DNA Center-integratie

Cisco Identity Services Engine (ISE) en Cisco DNA Center kunnen worden geïntegreerd voor automatisering van identiteit en beleid. ISE wordt ook gebruikt om informatie te verzamelen over de endpoints om gebruik te maken van Cisco AI Endpoint Analytics. PxGrid wordt gebruikt om de integratie tussen ISE en Cisco DNA Center te implementeren.

De vereisten voor Cisco DNA Center en ISE-integratie volgen:

- PxGrid-service moet zijn ingeschakeld op ISE.
- De ERS Read/Write-toegang moet zijn ingeschakeld.
- Het ISE-beheercertificaat moet het IP-adres of FQDN van ISE bevatten in de onderwerpnaam of in het SAN-veld.
- Het Cisco DNA Center-systeemcertificaat moet alle IP-adressen of FQDN’s van Cisco DNA Center in de onderwerpnaam of in het SAN-veld bevatten.
- De referenties van ISE ERS Admin worden gebruikt voor het instellen van vertrouwen in de ERS-communicatie tussen ISE en Cisco DNA Center.
- De pxGrid-knooppunt moet bereikbaar zijn via Cisco DNA Center.

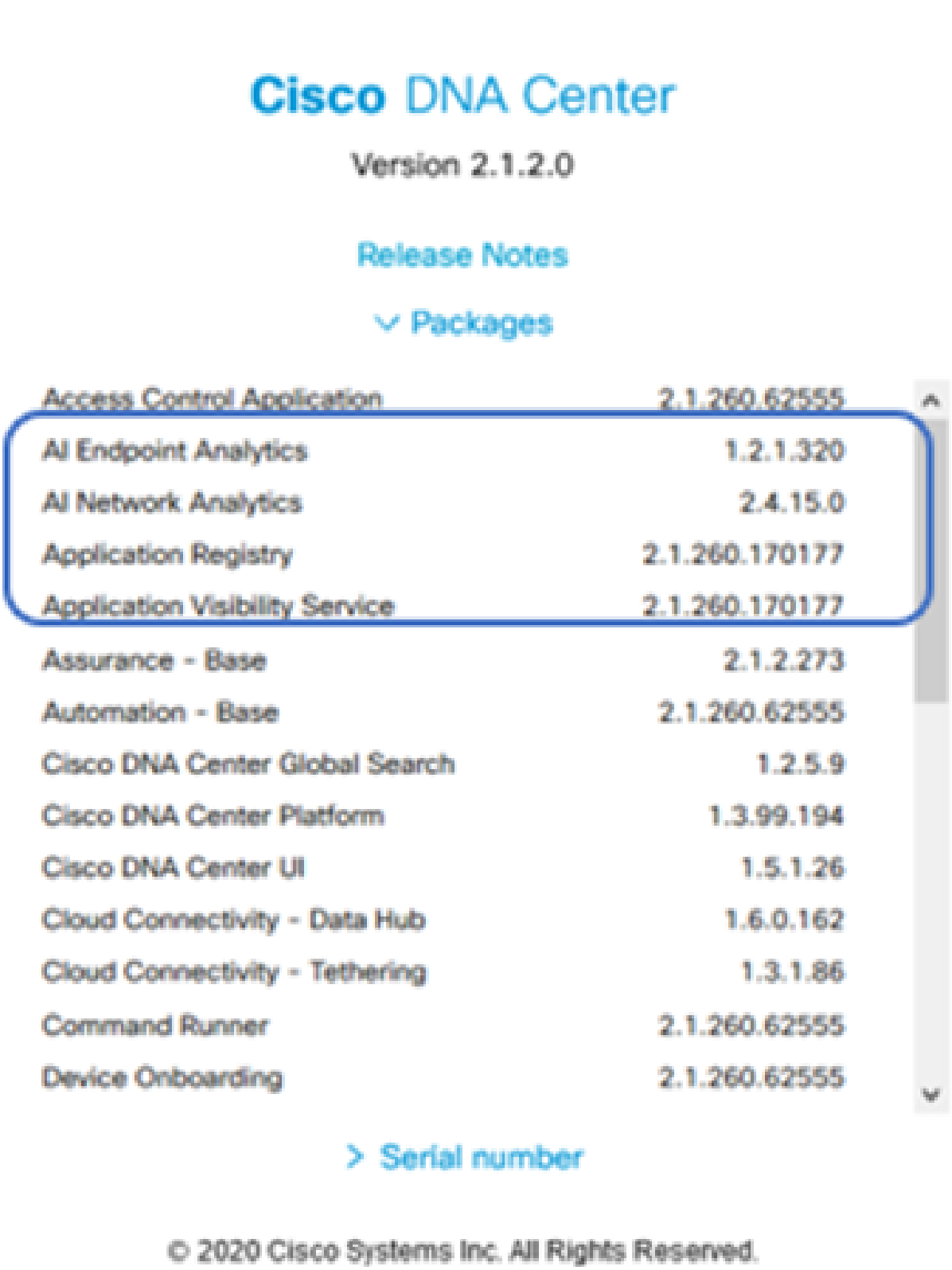
Cisco DNA Center-vereisten voor telemetrie

Er zijn vereisten die moeten worden geïmplementeerd om Application Assurance in Cisco DNA Center mogelijk te maken. Deze vereisten worden in detail toegelicht in de volgende paragrafen.

Cisco DNA Center-sleutelpakketten

Cisco DNA Center vereist dat deze drie pakketten worden geïnstalleerd om telemetriegegevens in te schakelen en te analyseren.

- AI-endpointanalyse
- AI-netwerkanalyse
- Toepassingszichtservices



Cisco DNA Center-pakketten vereist

Een snelle manier om toegang tot deze informatie te krijgen, is door op de link "Over" te klikken onder het pictogram voor het vraagteken rechtsboven op de hoofdpagina van het Cisco DNA Center. Als deze toepassingen ontbreken, moeten deze zijn geïnstalleerd voordat u de telemetrieprocedure doorvoert. Gebruik deze handleiding om deze pakketten in Cisco DNA Center

te installeren vanuit de Cisco-cloud. Gids voor upgrade van Cisco DNA Center

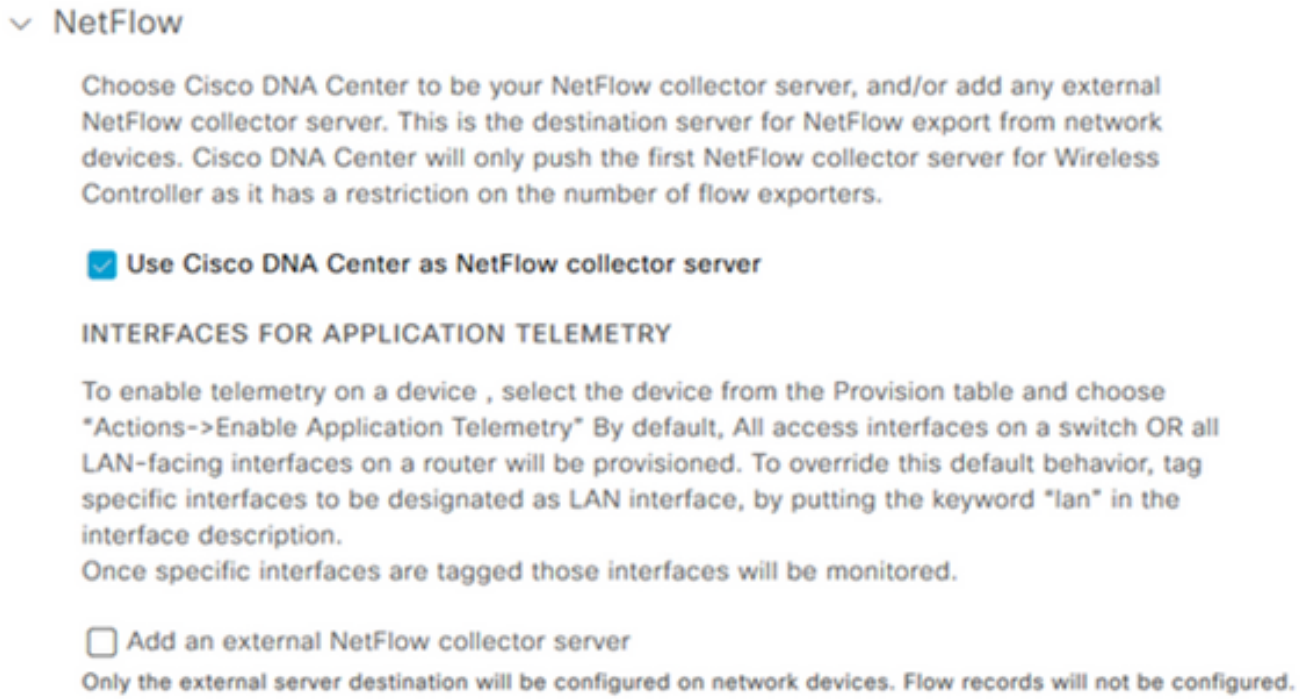
Cisco DNA Center als telemetrieverzamelaar

NetFlow-gegevensexport is het technologietransport dat de telemetriegegevens biedt die naar Cisco DNA Center worden doorgestuurd voor een diepgaande analyse. Om gegevensverzameling voor machine learning en redeneren voor endpointanalyses mogelijk te maken, moet NetFlow worden geëxporteerd naar Cisco DNA Center. TTA is een platform van de telemetriesensor dat wordt gebruikt om telemetrie van weerspiegeld IP netwerkverkeer te produceren en het te delen met het Centrum van Cisco DNA voor toepassing en endpointzicht.

- Het netwerkverkeer wordt ontvangen van switches en routers via Switched Port Analyzer (SPAN)-mirroring en ingevoerd in de Cisco DNA Traffic Telemetry Applicatie-mirroring interfaces.
- De Cisco DNA Traffic Telemetry Applicatie analyseert het ontvangen verkeer om een telemetriestroom voor Cisco DNA Center te produceren.

Voltooi deze stappen om Cisco DNA Center als telemetrieverzamelaar in te schakelen.

- In Cisco DNA Center klikt u op Menu > Design > Network Settings en schakelt u telemetrie in voor Cisco DNA Center om NetFlow te verzamelen.



DNAC configureren als NetFlow Collector

De Cisco AI-cloud

Cisco AI Network Analytics is een toepassing binnen Cisco DNA Center die gebruik maakt van de kracht van machine learning en machine redelijk redeneren om nauwkeurige inzichten te bieden

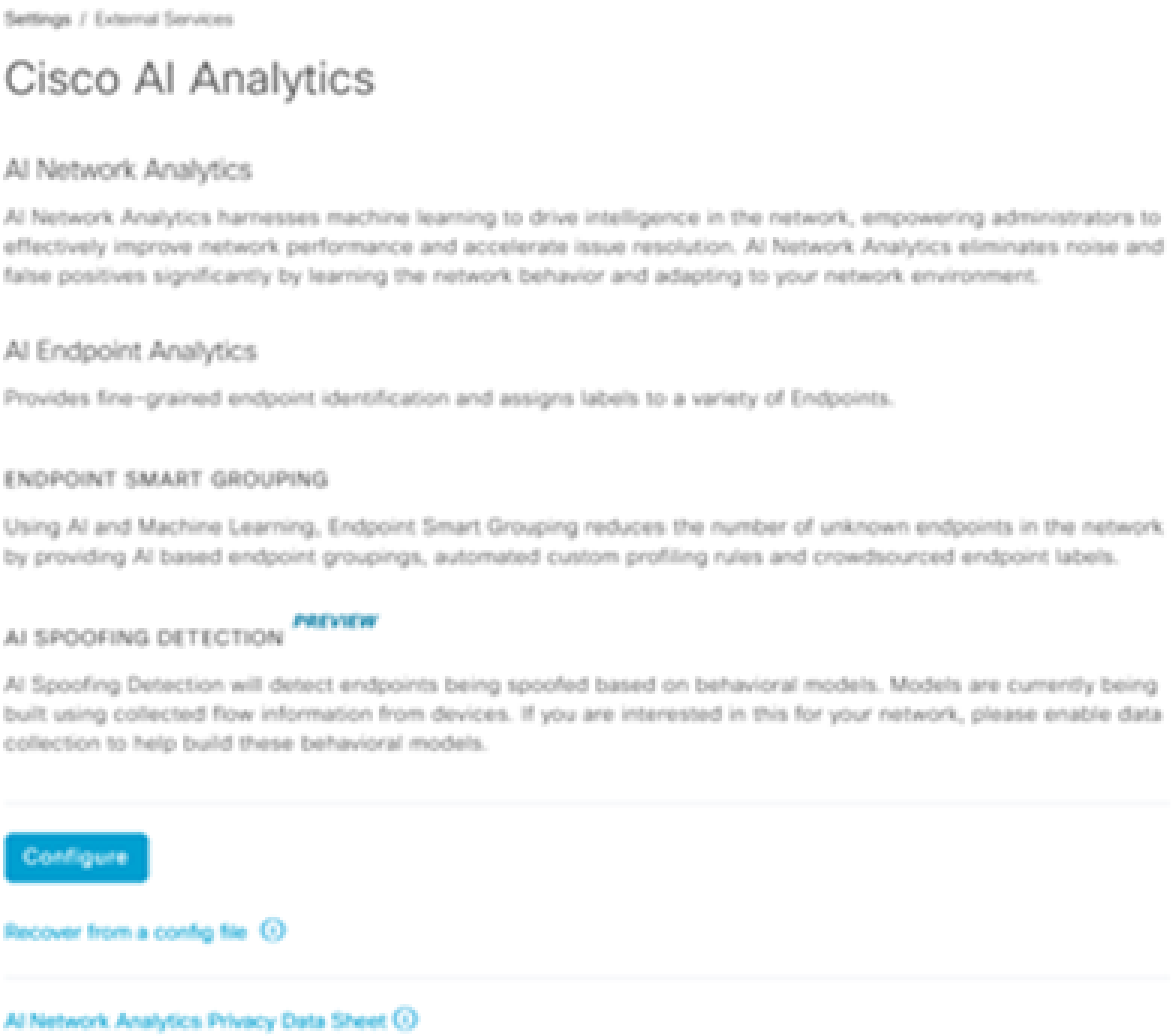
die specifiek zijn voor uw netwerkimplementatie, waardoor u snel problemen kunt oplossen. Network- en telemetriegegevens worden geanonimiseerd in Cisco DNA Center en vervolgens via een veilig versleuteld kanaal naar de op Cisco AI Analytics gebaseerde infrastructuur in de cloud verzonden. De Cisco AI Analytics cloud voert het machine learning model uit met deze gebeurtenisgegevens en brengt de problemen en algemene inzichten terug naar Cisco DNA Center. Alle verbindingen met de cloud zijn uitgaand op TCP/443. Er zijn geen inkomende verbindingen, de Cisco AI Cloud initieert geen TCP-stromen naar Cisco DNA Center. Volledig gekwalificeerde domeinnamen (FQDN) die kunnen worden gebruikt om in de HTTPS-proxy en/of firewall toe te staan op het moment dat dit artikel wordt geschreven, zijn:

- https://api.use1.prd.kairos.ciscolabs.com (US East Region)
- https://api.euc1.prd.kairos.ciscolabs.com (centrale regio van de EU)

De geïmplementeerde Cisco DNA Center-applicatie moet de verschillende domeinnamen op het internet die worden gehost door Cisco, kunnen oplossen en bereiken.

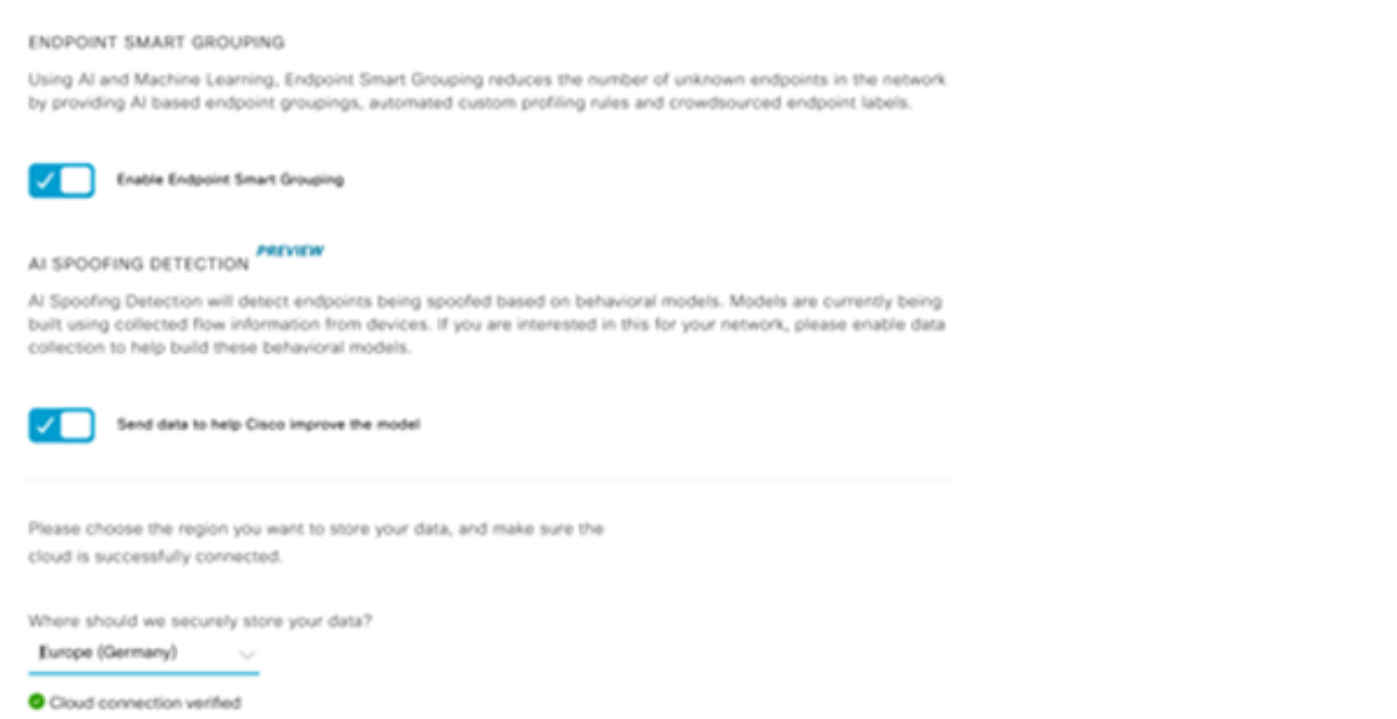
Volg deze stappen om Cisco DNA Center aan de Cisco AI-cloud te koppelen.

- Ga naar de gebruikersinterface van het Cisco DNA Center-apparaat om de AI-cloudregistratie te voltooien:
- Naar navigeren Systeem > Instellingen > Externe services > Cisco AI Analytics
- Klik op Configureren en inschakelen van de optie voor Slimme Groepering van Endpoint en de optie voor detectie van AI-nep.
- Endpoint Smart Grouping maakt gebruik van de AI/ML-cloud om onbekende endpoints te clusteren om beheerders te helpen bij het labelen van die endpoints. Dit is zeer nuttig om de netto-onbekenden in het netwerk te verminderen.
- AI-spookdetectie zal Cisco helpen om aanvullende NetFlow/telemetrie-informatie te verzamelen en helpt bij de modellering van het endpoint.
- Kies de dichtstbijzijnde locatie bij de geografische regio van de implementatie. Zodra de verificatie van de cloudverbinding is uitgevoerd en de verbinding succesvol is, ziet u een groen selectievakje.



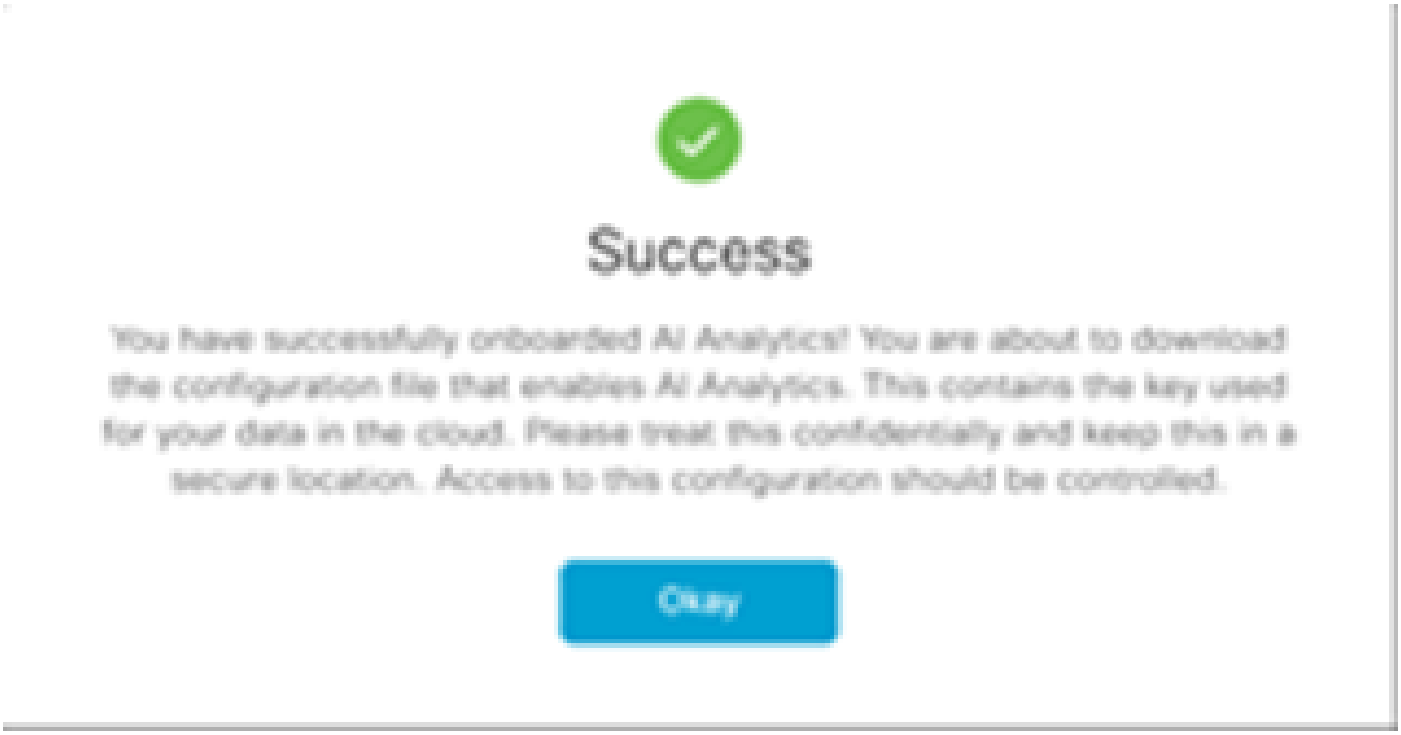
Cisco AI-analyse GUI configureren

- Als de verbinding niet succesvol is, controleer dan de proxy-instellingen in Cisco DNA Center vanaf de pagina System > Settings > System Configuration > Proxy config als er een proxy wordt gebruikt. Het is ook een goed idee om alle firewallregels te controleren die deze communicatie zouden kunnen blokkeren.



Cisco AI/ML-cloudverbindingsverificatie

- Accepteer de Universal Cloud-overeenkomst van Cisco om AI-analyse mogelijk te maken.
- Op dit punt is het instappen voltooid en wordt een dialoogvenster weergegeven dat dit aangeeft.



Dialoogvenster Succes na inschrijving

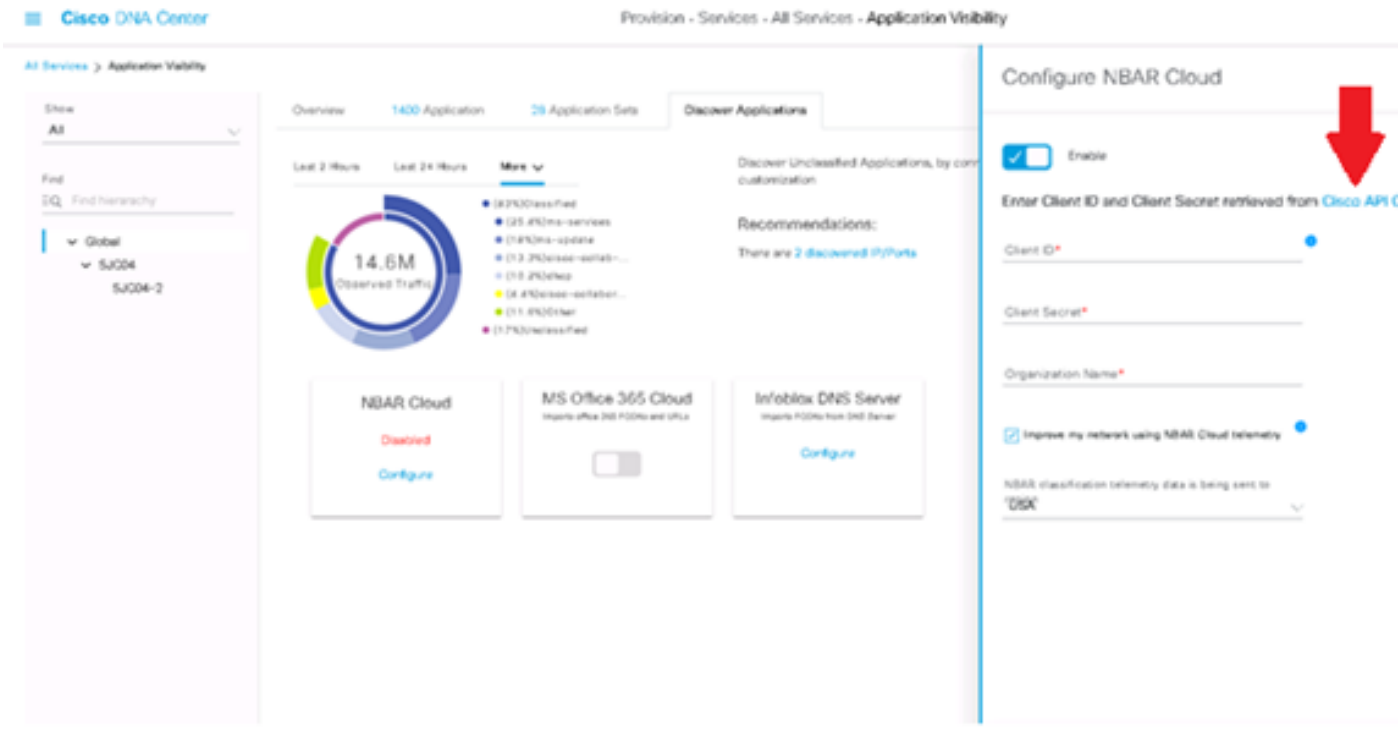
De Network Based Application Recognition (NBAR)-cloud

De telemetrie-applicatie en het Catalyst 9000-platform verzamelen endpointmetagegevens met behulp van diepe pakketinspectie van pakketstromen en passen Network Based Application Recognition (NBAR) toe om te bepalen welke protocollen en toepassingen in het netwerk worden gebruikt. Cisco DNA Center heeft een ingebouwd NBAR-protocolpakket dat kan worden bijgewerkt. De telemetriegegevens kunnen naar de Cisco NBAR-cloud worden verzonden voor aanvullende analyse en voor het detecteren van onbekende protocolhandtekeningen. Hiervoor moet het Cisco DNA Center-apparaat zijn aangesloten op de cloud. Network-Based Application Recognition (NBAR) is een geavanceerde applicatie-herkenningsengine die is ontwikkeld door Cisco en die gebruikmaakt van verschillende classificatietechnieken, en die de classificatieregels eenvoudig kan bijwerken.

Voltooi deze stappen om Cisco DNA Center aan de Cisco NBAR Cloud te koppelen.

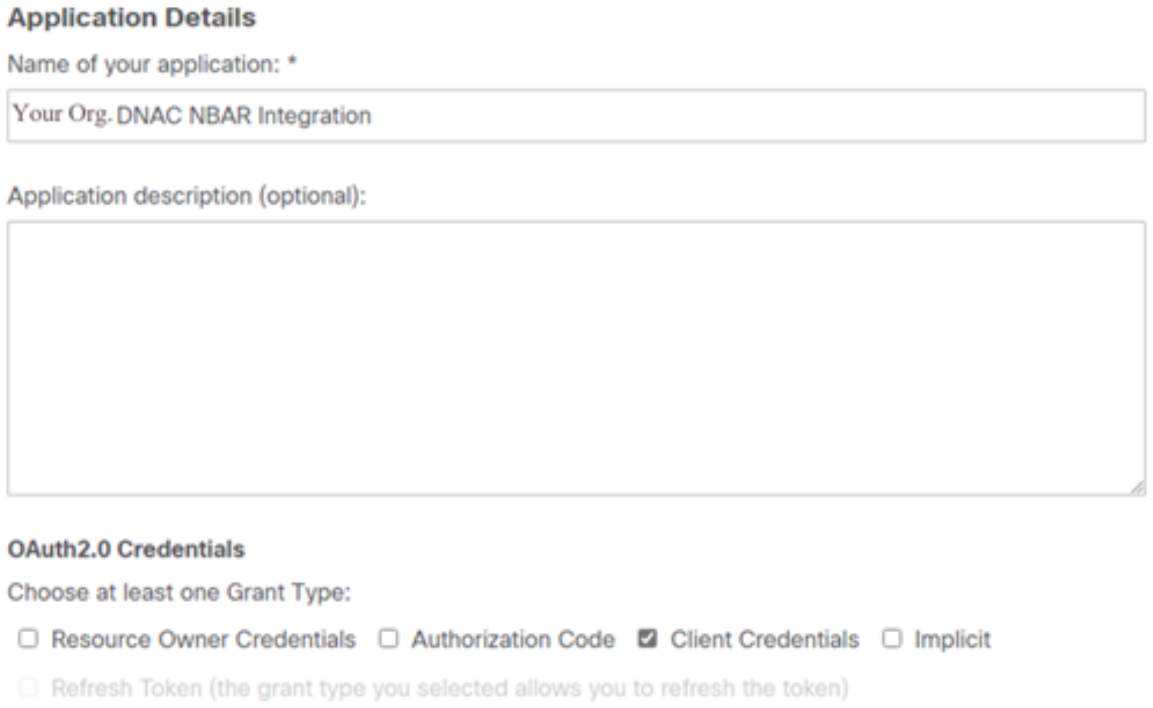
- Ga vanuit de gebruikersinterface van Cisco DNA Center naar Provision > Services > Application Visibility. Klik op Configureren onder NBAR Cloud en er wordt een paneel geopend. Schakel de service in.
- Als u de klant-ID, het clientgeheim en de organisatienaam heeft, geef ze dan unieke namen, afhankelijk van de organisatie en het gebruik.
- Op het moment van schrijven is de enige NBAR Cloud-regio die momenteel beschikbaar is in de VS; in de toekomst kunnen meer regio's beschikbaar komen. Selecteer in implementatievoorkeuren en sla deze op.

Klik op de koppeling "Cisco API Console" om de referenties voor client-id en clientgeheim op te halen. Hierdoor wordt een portal geopend. Aanmelden met de juiste CCO-id, een nieuwe app maken, de opties selecteren die overeenkomen met NBAR-cloud en het formulier invullen. Als je klaar bent, krijg je een klant-ID en geheim. Raadpleeg de onderstaande afbeelding.



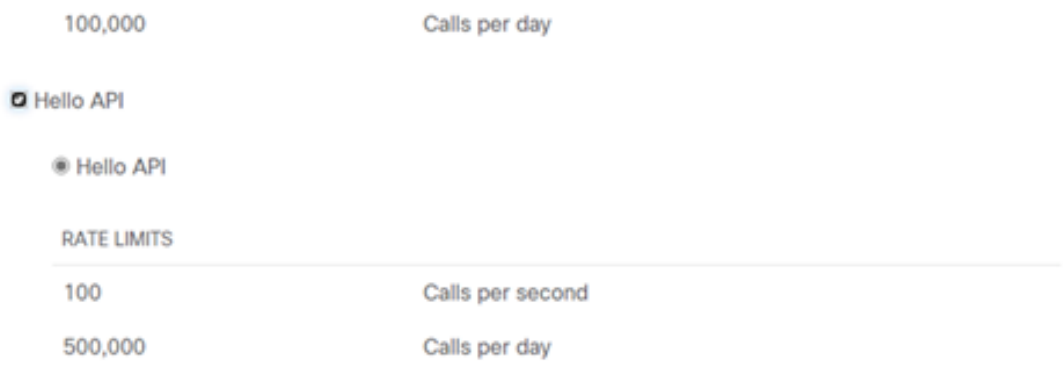
Cisco API Link naar client-id en geheim ophalen

Deze afbeeldingen tonen de opties die worden gebruikt voor registratie in de NBAR-cloud.



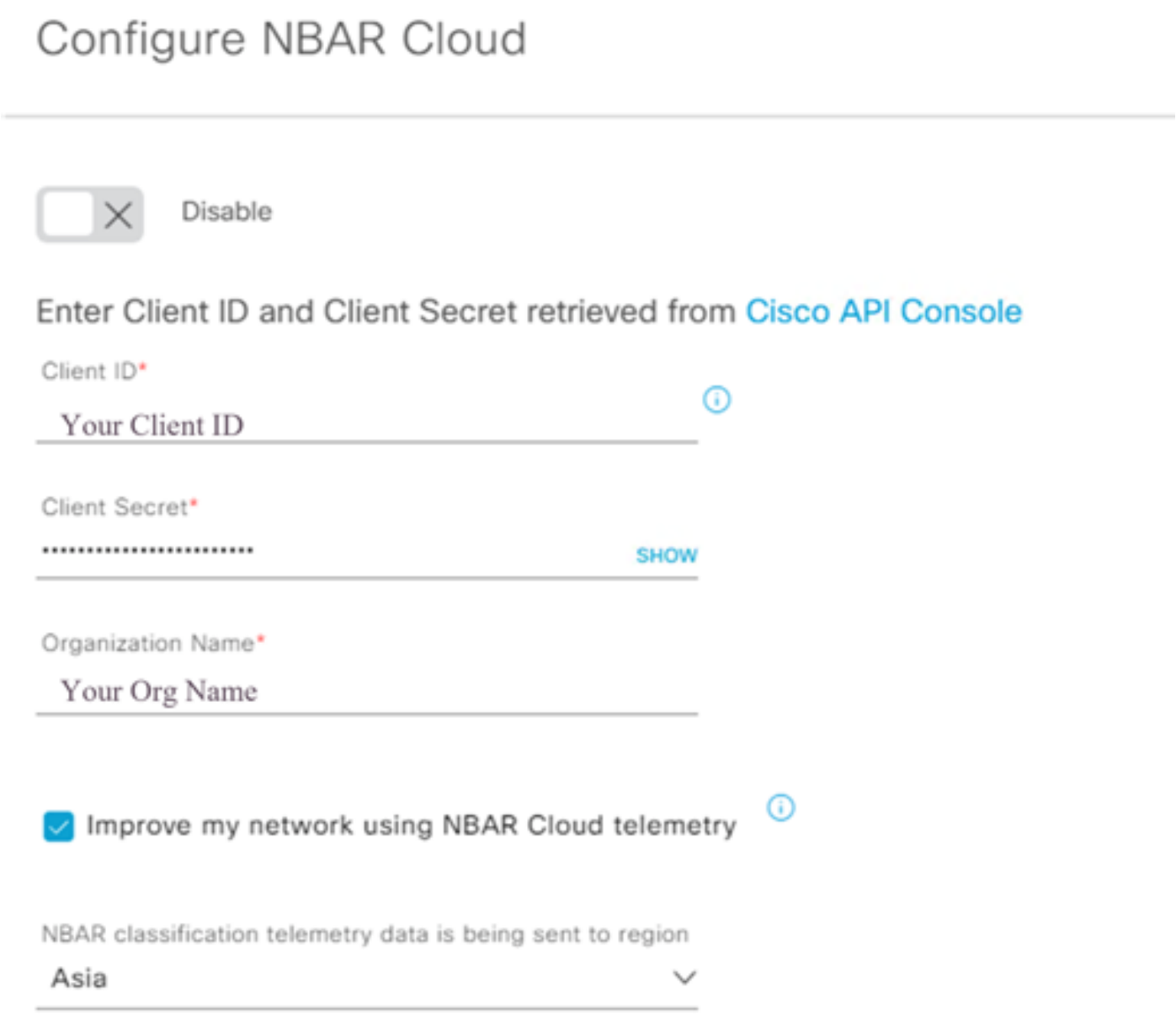
Details van NBAR Cloud App

- Gebruik deze afbeelding als referentie bij het invullen van de details van de API-aanvraag.



API-gegevens voor toepassingen

- Voer de client-id en het geheim in dat via het Cisco-portal is verkregen naar Cisco DNA Center.



Client ID en geheim configureren op DNAC

CBAR (Controller-gebaseerde toepassingsherkenning) en SD-AVC

CBAR wordt gebruikt voor de classificatie van duizenden netwerktoepassingen, zelfgemaakte toepassingen en algemeen netwerkverkeer. Hiermee kan Cisco DNA Center op dynamische wijze informatie verkrijgen over toepassingen die op de netwerkinfrastructuur worden gebruikt. CBAR helpt om het netwerk up-to-date te houden door nieuwe toepassingen te identificeren aangezien hun aanwezigheid op het netwerk blijft toenemen en updates aan protocolpakketten toestaat. Als Application Visibility van end-to-end verloren gaat door verouderde protocolpakketten, kan onjuiste categorisering en verder doorsturen voorkomen. Dit veroorzaakt niet alleen zichtbaarheidsgaten in het netwerk, maar ook onjuiste wachtrijen of doorsturen van problemen. CBAR lost dat probleem

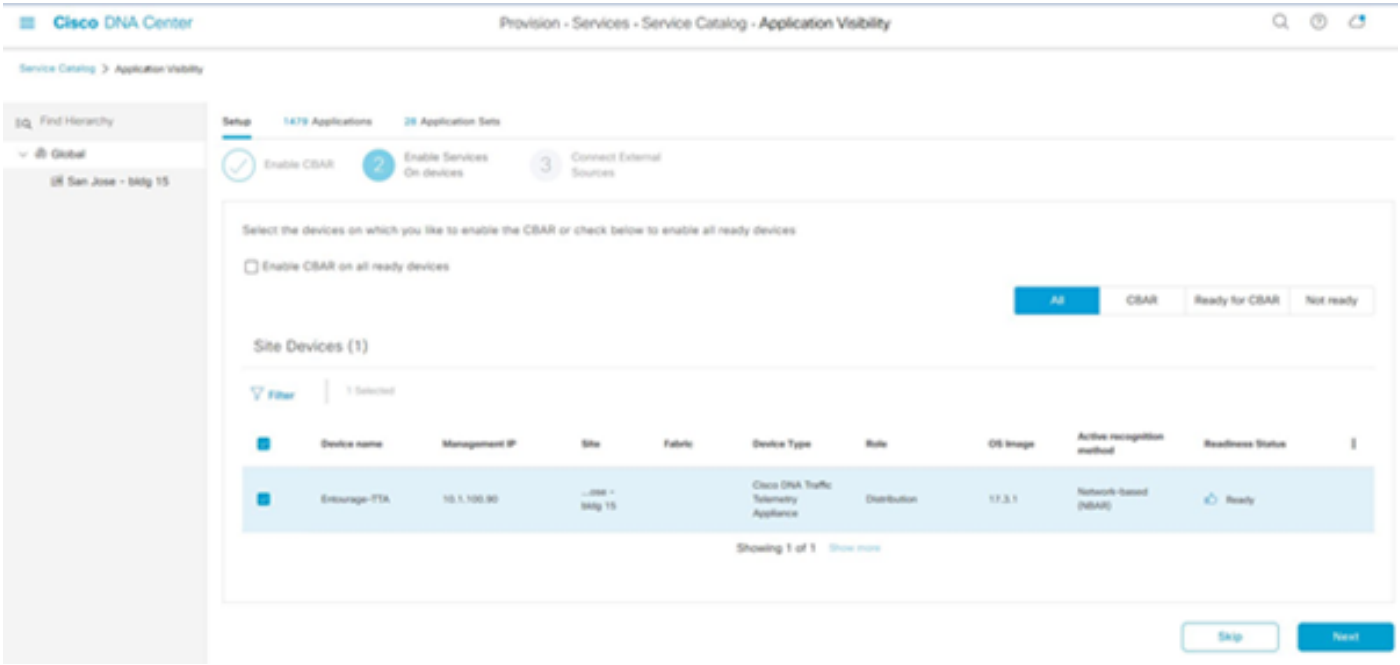
op door bijgewerkte protocolpakketten toe te staan om over het netwerk worden geduwd.

Cisco Softwaregedefinieerde AVC (SD-AVC) is een onderdeel van Cisco Application Visibility and Control (AVC). Het functioneert als een gecentraliseerde netwerkdienst die met specifieke deelnemende apparaten in een netwerk werkt. SD-AVC helpt ook bij DPI van de toepassingsgegevens. Enkele van de huidige functies en voordelen van SD-AVC omvatten:

- Toepassingsherkenning op netwerkniveau die consistent is in het netwerk
- Verbeterde toepassingsherkenning in symmetrische en asymmetrische routeringsomgevingen
- Verbeterde eerste pakketherkenning
- Bijwerken van het Protocolpakket op netwerkniveau
- Beveiligd op browser gebaseerde SD-AVC dashboard via HTTPS voor het monitoren van SD-AVC functionaliteit en statistieken, en voor het configureren van protocolpack updates voor het hele netwerk

Volg deze stappen om CBAR in te schakelen voor de relevante apparaten.

- Ga naar het menu van Cisco DNA Center, Provision > Application Visibility. Het De eerste keer dat de pagina Toepassingszichtbaarheid wordt geopend, wordt de gebruiker weergegeven met een configuratiewizard die hieronder wordt weergegeven.
- Nadat u de apparaten in Cisco DNA Center voor elke site hebt gedetecteerd, selecteert u het apparaat waarop CBAR is ingeschakeld en gaat u verder met de volgende stap.



CBAR op apparaat inschakelen

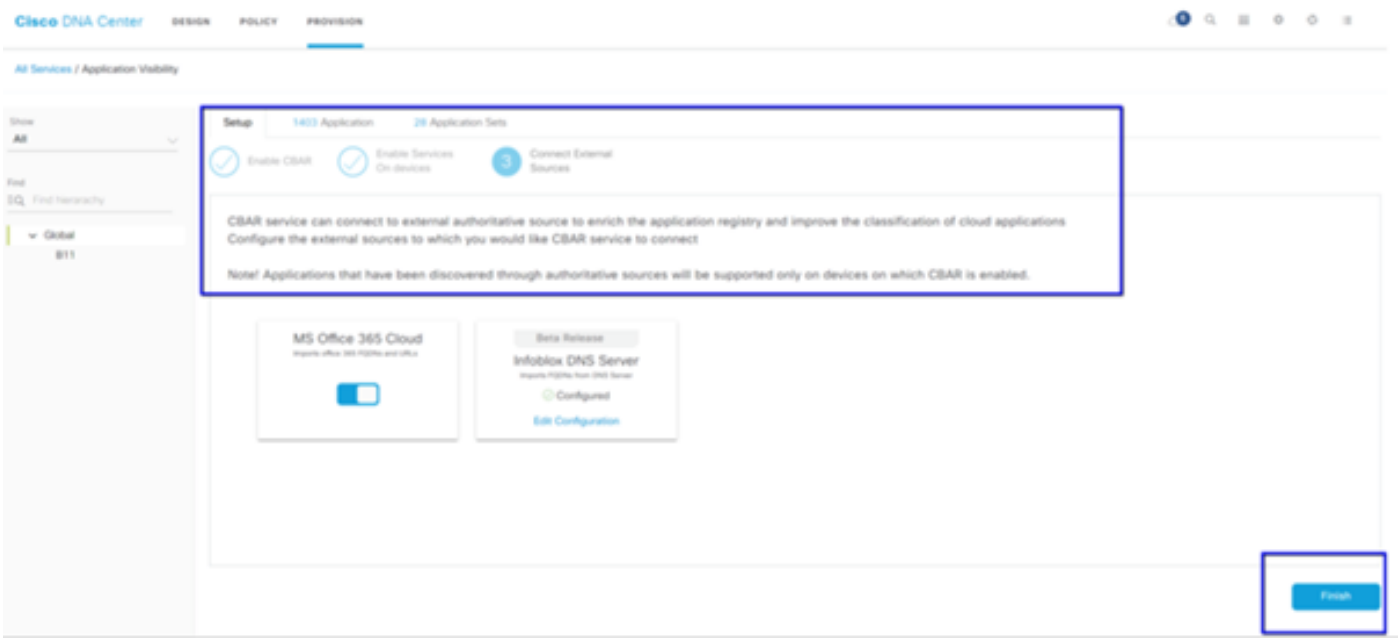
Microsoft Office 365 Cloud Connector (niet verplicht)

Cisco DNA Center kan rechtstreeks met de Microsoft RSS-feed worden geïntegreerd om ervoor te zorgen dat de herkenning van toepassingen voor Office 365 is afgestemd op de gepubliceerde richtlijnen. Deze integratie wordt in Cisco DNA Center de Microsoft Office 365 Cloud Connector

genoemd. Het is een goede zaak dat dit is geïmplementeerd als de gebruiker Microsoft Office 365-toepassingen in het netwerk gebruikt. Integratie met Microsoft Office 365 is geen vereiste en als deze niet is ingeschakeld, heeft dit alleen gevolgen voor de capaciteit van Cisco DNA Center om Microsoft Office 365-hostgegevens te verwerken en te classificeren. Cisco DNA Center heeft Microsoft Office 365 applicatie herkenning ingebouwd, maar door rechtstreeks te integreren met de applicatie provider kan Cisco DNA Center bijgewerkte en nauwkeurige informatie krijgen over de huidige intellectuele eigendom blokken en URL's die gebruikt worden door de Microsoft Office 365 suite.

Volg deze stappen voor het integreren van Cisco DNA Center met Microsoft Office 365 Cloud.

- Klik op het pictogram Menu en kies Provisioning > Services > Toepassingszichtbaarheid
- Klik op Toepassingen opsporen
- Klik op de knop MS Office 365 Cloud om Cisco DNA Center in de Microsoft Office 365 Cloud te integreren.

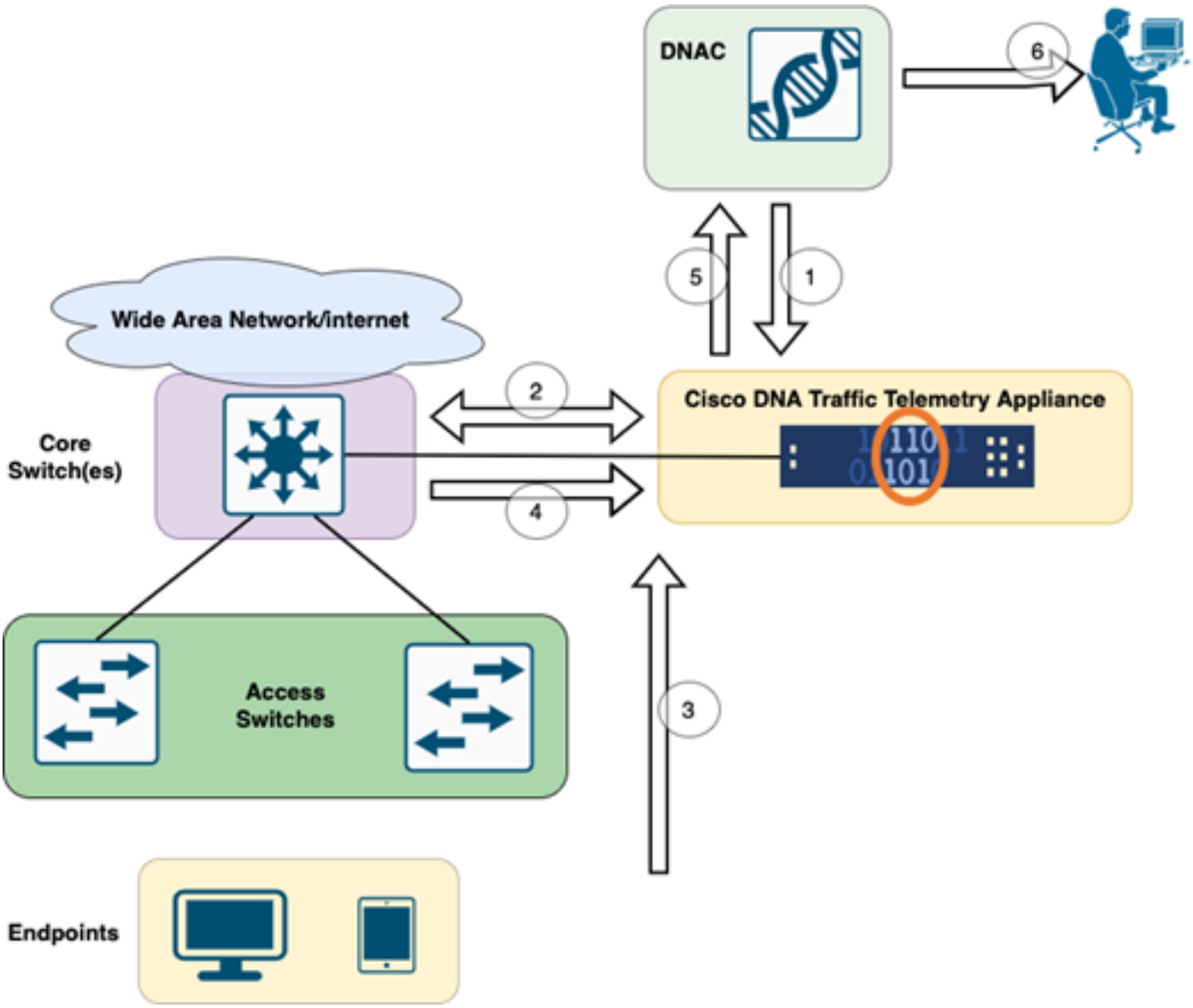


MS O365 cloudintegratie

TTA-implementatie

In dit deel worden de stappen beschreven die nodig zijn om TTA in een netwerk te implementeren.

TTA Workflow - Overzicht



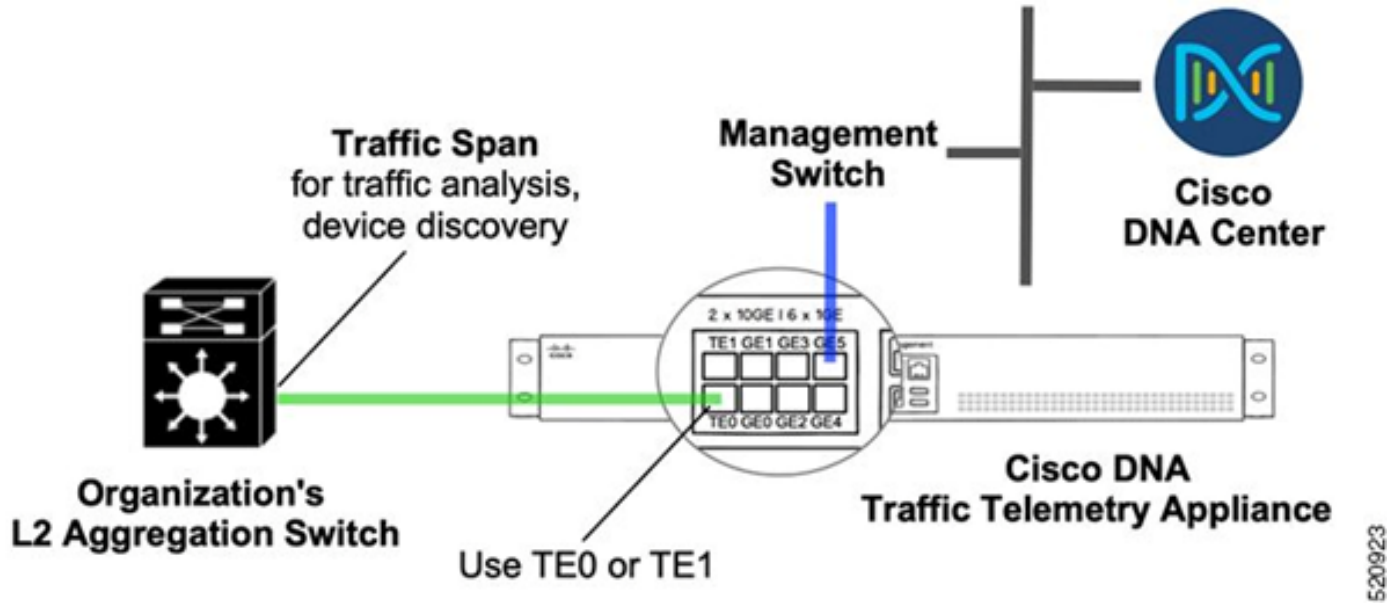
TTA naar DNAC Workflow

De stappen die in dit diagram worden gemarkeerd, geven een overzicht van het proces en de telemetriestroom tussen TTA en Cisco DNA Center. Hier worden deze stappen verder uitgewerkt.

1. De Cisco Traffic Telemetry Applicatie is aangesloten op de site aggregation switch of de core switch binnen de netwerkinfrastructuur. Dankzij deze aansluiting kan het apparaat verkeersgegevens ontvangen van verschillende switches die toegang hebben tot het netwerk.
2. De Cisco Traffic Telemetry Applicatie is geïntegreerd met Cisco DNA Center, dat fungeert als netwerkbeheerplatform. Deze integratie maakt naadloze communicatie en gegevensuitwisseling tussen het apparaat en Cisco DNA Center mogelijk.
3. Aangezien gebruikersverkeer door het netwerk stroomt, wordt het overspannen of gespiegeld aan de Cisco Traffic Telemetry Applicatie. Dit betekent dat een kopie van het netwerkverkeer naar het apparaat wordt verzonden voor controle- en analysedoeleinden, terwijl het oorspronkelijke verkeer op het normale pad blijft.
4. De Cisco Traffic Telemetry Applicatie verzamelt en verwerkt de ontvangen verkeersgegevens. Het haalt relevante informatie, zoals pakketniveau-details, stroomstatistieken, en prestatiesmetriek, uit het gespiegelde verkeer.

5. De verwerkte telemetrie-informatie wordt vervolgens van de Cisco Traffic Telemetry Appliance naar Cisco DNA Center verzonden. Deze communicatie maakt het mogelijk voor Cisco DNA Center om real-time inzichten en updates te ontvangen over de verkeerspatronen, toepassingsprestaties en afwijkingen van het netwerk.
6. De telemetrie-inzichten die door Cisco DNA Center worden gegenereerd, bieden waardevolle informatie aan netwerkbeheerders. Ze kunnen de interface van Cisco DNA Center gebruiken om de verzamelde gegevens te bekijken en analyseren, inzicht te verkrijgen in de prestaties van het netwerk op het gebied van gezondheid en toepassingen, potentiële problemen te identificeren en geïnformeerde beslissingen te nemen voor netwerkoptimalisatie en probleemoplossing.

TTA-implementatie: diagram op hoog niveau



TTA-implementatie: hoog niveau

In het bovenstaande schema is aangegeven hoe TTA in het netwerk kan worden aangesloten. De 10-Gig- en 1-Gig-interfaces kunnen worden gebruikt voor de opname van SPAN tegen lijnsnelheid. De Gi0/0/5 interface wordt gebruikt voor communicatie met Cisco DNA Center, voor orkestratie en voor het doorsturen van telemetrie-inzichten naar Cisco DNA Center; deze interface KAN NIET worden gebruikt voor SPAN-inname.

TTA-software- en licentievereisten

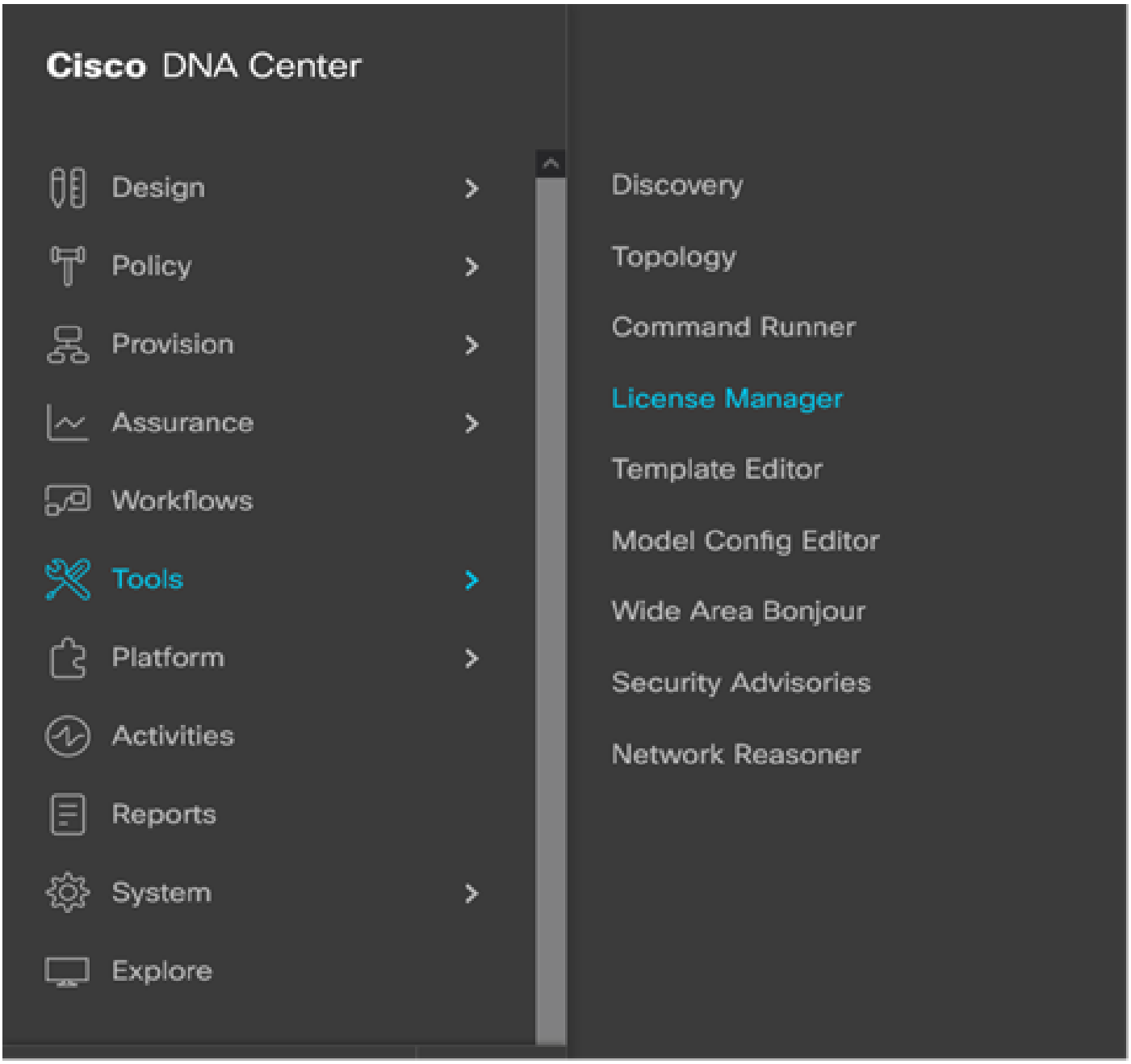
TTA-apparaten die in het netwerk worden geïmplementeerd, zijn van cruciaal belang voor het verschaffen van telemetrie-inzichten in gebruikersgegevens en gebruikerseindpunten. Om de oplossing met succes te kunnen implementeren moet aan deze vereisten worden voldaan.

- TTA moet worden geconfigureerd met een initiële bootstrap-configuratie zodat het kan worden ontdekt door Cisco DNA Center (TTA Bootstrap Configuration)
- Het TTA-apparaat moet worden opgeslagen in Cisco DNA Center zodat het kan worden beheerd door Cisco DNA Center (Telemetry Box toevoegen aan Cisco DNA Center

Inventory)
- De juiste licentie moet op de TTA (TTA-applicatie-licentie) worden geïnstalleerd

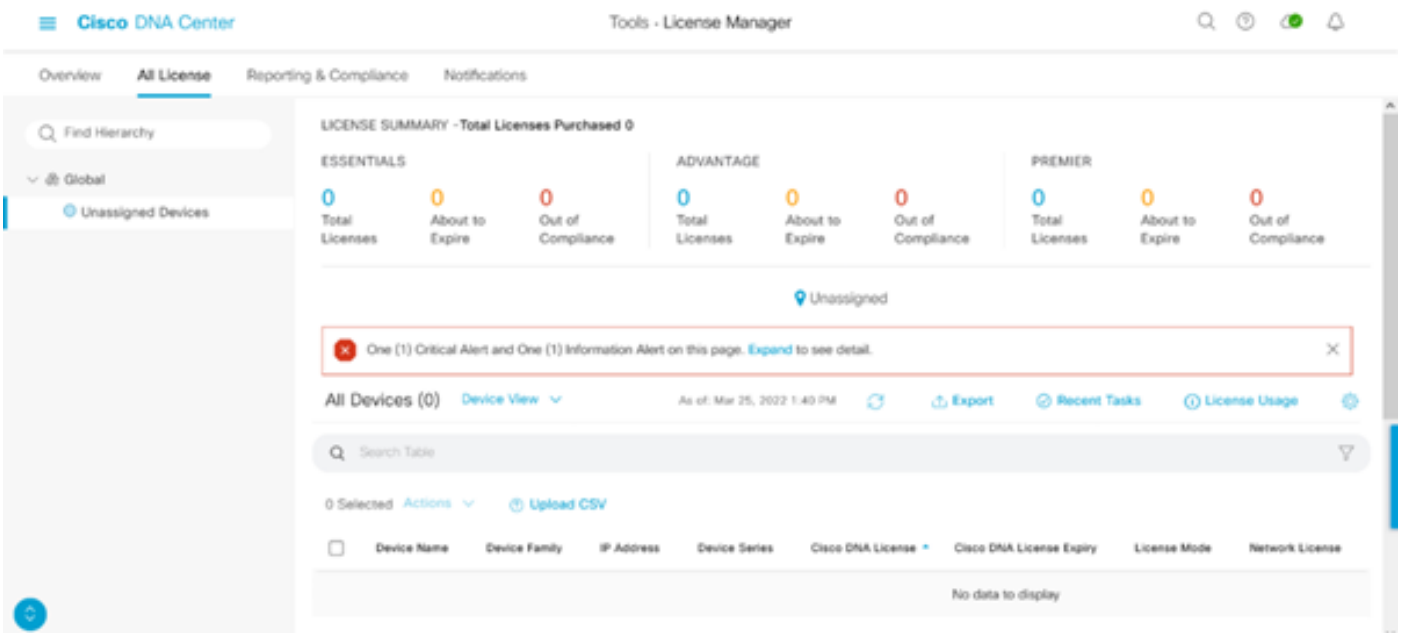
Het apparaat ondersteunt slechts één besturingssysteem en hiervoor is de Cisco DNA TTA Advantage License vereist om telemetrie te verzamelen. Er is geen behoefte aan een functielicentie (zoals IP-basis of geavanceerde IP-services) of een eeuwigdurend licentiepakket (zoals Network Essentials of Network Advantage).

Als u licenties in Cisco DNA Center wilt beheren, navigeert u naar de licentiemanager door naar Tools > Licentiebeheer te navigeren in het uitrolmenu van Cisco DNA Center door op het pictogram Menu te klikken



Licentiebeheer op DNAC

- Navigeer naar de pagina Alle licenties en het lijkt op deze afbeelding. Op deze pagina kan de beheerder netwerkapparaatlicenties beheren zoals die van de TTA.



Alle licentiepagina op DNAC

TTA-onboarding en dag-0 configuratie

Om de detectie en het aan boord gaan van het TTA-apparaat door Cisco DNA Center te vergemakkelijken, zijn er bootstrap-opdrachten die op de TTA-apparaten van de site moeten worden geconfigureerd. Als de laarzentrekkerconfiguratie is geïnstalleerd, kan de TTA worden gedetecteerd via het dashboard van Cisco DNA Center. Hieronder vindt u dag-0 configuratie-items voor een TTA-apparaat. Als het apparaat eenmaal is opgenomen in de sitehiërarchie, erft het TTA-apparaat de resterende configuratie-onderdelen van 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
```

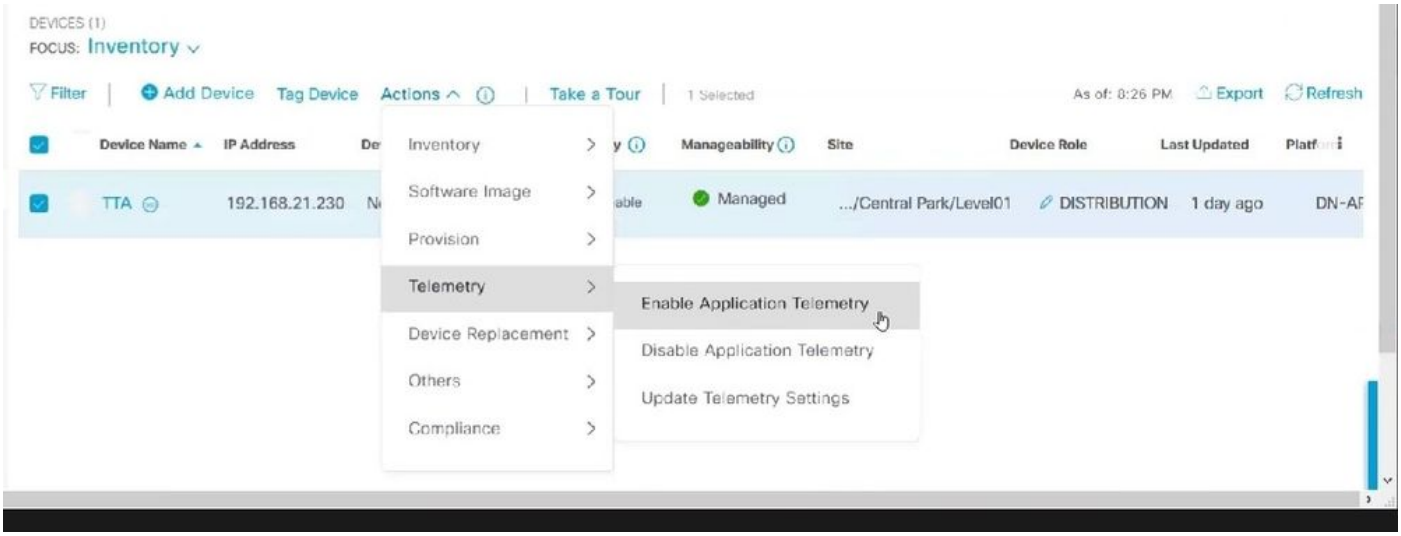
```
ip ssh source-interface GigabitEthernet0/0/5

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
```

Zodra deze items zijn geconfigureerd op de ATA, kan deze worden ontdekt door Cisco DNA Center.

De TTA-applicatie toevoegen aan de inventaris van Cisco DNA Center

Om de TTA te kunnen gebruiken, moet Cisco DNA Center het TTA-apparaat detecteren en beheren. Zodra de TTA is aangesloten op Cisco DNA Center kan deze vervolgens worden beheerd vanuit Cisco DNA Center. Voordat we het TTA-apparaat ontdekken, moeten we ervoor zorgen dat de complete site-hiërarchie is ingesteld voor de site. Daarna gaan we verder met het toevoegen van het TTA-apparaat onder de specifieke site hiërarchie door deze stappen te volgen van de pagina Menu > Provision > Devices > Inventory om het apparaat toe te voegen aan een site.

1. Geef de gebruikersnaam/het wachtwoord (CLI) en SNMP-community op die nodig zijn om verbinding met het apparaat te maken en om het wachtwoord in te schakelen. Wacht totdat het apparaat is toegevoegd voordat u verder gaat.
2. Controleer de naam van het apparaat, de familie (netwerkbeheer in het geval van TTA), Reachability - Reachable, Manageable, de Rol van het apparaat - Distributie. Het apparaat zal in eerste instantie 'niet-conform' zijn, maar als de status volledig is ingesteld, zal deze veranderen.
3. Zodra de TTA is aangesloten, zal Cisco DNA Center configuratiesjablonen doordrukken om deze te configureren met geavanceerde telemetriefuncties.



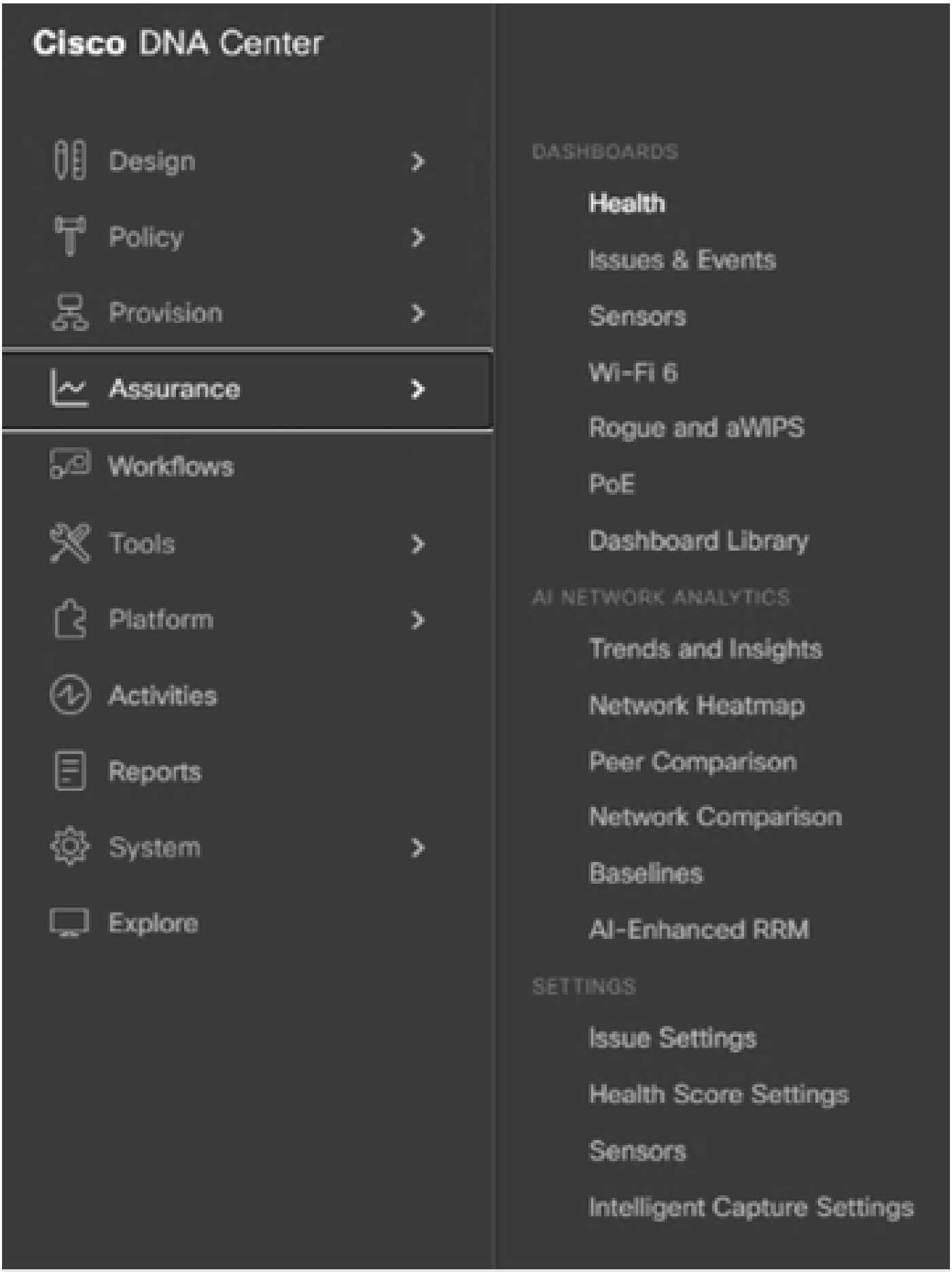
SPAN-configuratie

Afhankelijk van de hardwaremogelijkheden van de kern-switch kan de SPAN-sessie worden geconfigureerd om een groep VLAN's of interfaces te configureren voor de interface die is aangesloten op de TTA. Hier wordt een voorbeeldconfiguratie gegeven.

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

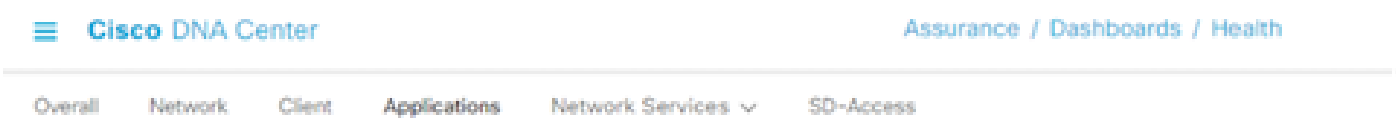
Verzameld vertrouwen

Om toegang te krijgen tot de Assurance-gegevens die zijn verzameld met de geïnstalleerde Traffic Telemetry-applicatie, ga naar de Assurance-sectie en klik op Health.

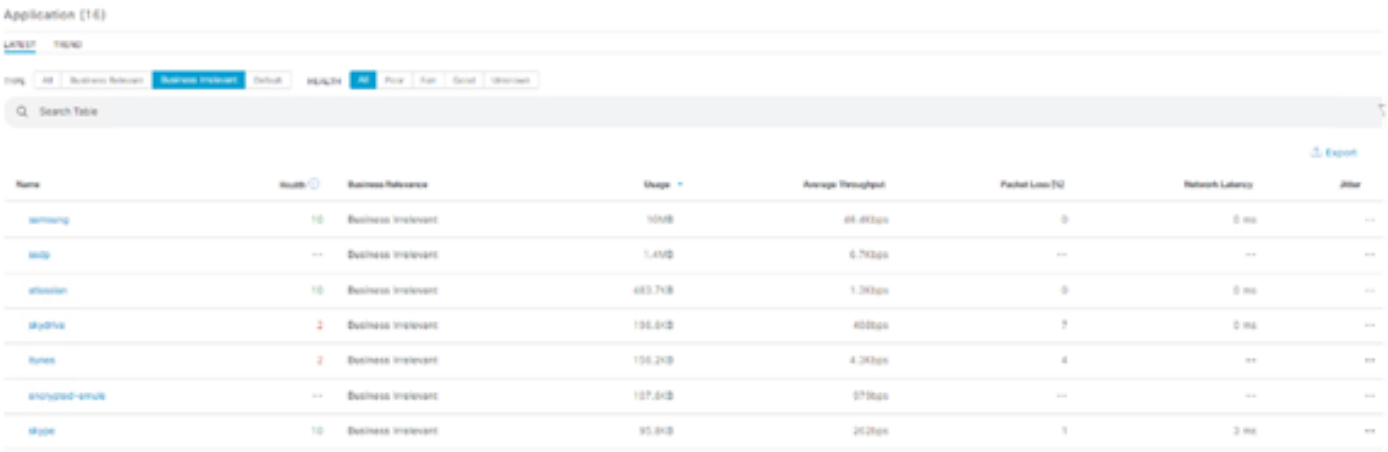


Navigeren naar App Assurance

Kies Toepassingen, en u vindt een uitgebreid overzicht van toepassingsgegevens, met inbegrip van latentie en jitter die door TTA worden gevangen die op het specifieke toepassingstype wordt gebaseerd.

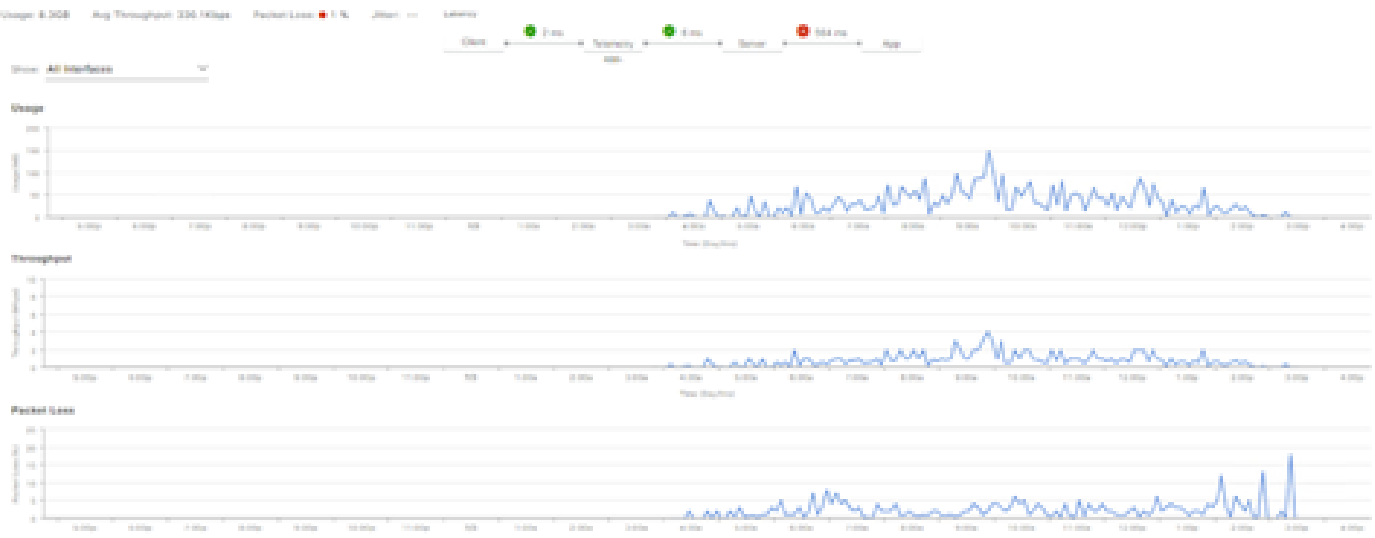


Navigeren naar Application Assurance



Gedetailleerde gebruikersinterface voor Application Assurance

Voor een gedetailleerdere analyse kunnen gebruikers individuele toepassingen verkennen door op de specifieke toepassing te klikken en de Exporteur te selecteren om de Traffic Telemetry Applicatie te zijn en specifieke maatstaven onderzoeken zoals Gebruik, Doorvoersnelheid en Packet Loss-gegevens, Clientnetwerklatentie, servernetwerklatentie en toepassingsserverlatentie.



Voorbeeld: Toepassingsgegevens Pt.1

Voorbeeld: Toepassingsgegevens Pt.2

Verifiëren

1. Controleer na het inschakelen van CBAR of de SD-AVC (Application Visibility Control)-service op het apparaat is ingeschakeld door u aan te melden bij de Cisco Traffic Telemetry Appliance en deze CLI-opdracht uit te voeren. De uitvoer is gelijk aan deze steekproef die het IP-adres van de controller aangeeft en de status van de verbinding.

```
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. Gebruik de opdracht "toon licentiesamenvatting" op de CLI van de TTA om de relevante details van de apparaatlicentie te controleren.

```
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. Controleer of de SPAN-sessie correct is geconfigureerd op de kern/aggregatie-switch.

```
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. Zodra TTA met succes is geleverd, zullen deze opdrachten naar het apparaat worden (of zijn) geduwd.

```
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
```

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.