Utilisation de Traffic Telemetry Appliance (TTA) et de Cisco DNA Center App Assurance : pourquoi et comment

Table des matières

Introduction

Ce document décrit la plate-forme Cisco DNA Traffic Telemetry Appliance (référence Cisco DN-APL-TTA-M) ainsi que la façon d'activer l'assurance des applications dans Cisco DNA Center. Ill permet également de comprendre comment et où le TTA peut être positionné dans un réseau, ainsi que le processus de configuration et de vérification. Cet article traite également des différentes conditions préalables requises.

Conditions préalables

Cisco vous recommande de connaître le fonctionnement de Cisco DNA Center Assurance et de Cisco Application Experience.

Assurance des applications

L'assurance est un moteur d'analyse et de collecte de données réseau polyvalent et en temps réel qui peut augmenter considérablement le potentiel commercial des données réseau. Assurance traite des données d'application complexes et présente les résultats dans les tableaux de bord d'état Assurance pour fournir des informations sur les performances des applications utilisées dans le réseau. Selon l'endroit où les données sont collectées, vous pouvez voir tout ou partie des éléments suivants :

- Nom de l'application
- Débit
- Marques DSCP
- Mesures de performances (latence, gigue et perte de paquets)

En fonction de la quantité de données collectées, Application Assurance peut être catégorisé en deux modèles :

- Application Visibility (AppVis) et
- Expérience des applications (AppX)

Le nom de l'application et le débit sont collectivement appelés mesures quantitatives. Les données des mesures quantitatives proviennent de l'activation de la visibilité sur les applications.

Les marquages DSCP et les mesures de performances (latence, gigue et perte de paquets) sont collectivement appelés mesures qualitatives. Les données pour les mesures qualitatives proviennent de l'activation de l'expérience des applications.

Visibilité sur les applications (AppVis)

Les données de visibilité sur les applications sont collectées à partir des commutateurs exécutant Cisco IOS® XE et des contrôleurs sans fil exécutant AireOS. Pour les commutateurs exécutant Cisco IOS XE, les données de visibilité sur les applications sont collectées à l'aide d'un modèle NBAR prédéfini qui est appliqué de manière bidirectionnelle (entrée et sortie) aux ports de commutation d'accès de couche physique. Pour les contrôleurs sans fil exécutant AireOS, les données de visibilité sur les applications sont collectées au niveau du contrôleur sans fil, puis la télémétrie en continu est utilisée pour transporter ces données vers Cisco DNA Center.

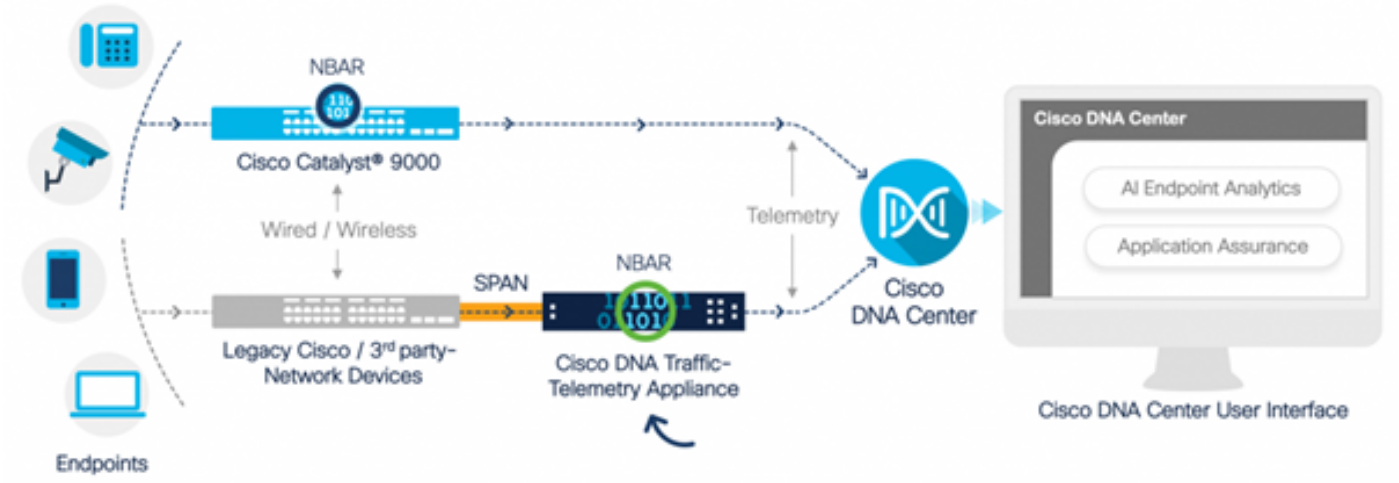
Expérience des applications (AppX)

Les données relatives à l'expérience des applications sont collectées à partir des plates-formes de routeurs Cisco IOS XE, en particulier à l'aide de la fonctionnalité Cisco Performance Monitor

(PerfMon) et des mesures Cisco Application Response Time (ART). Les plates-formes ASR 1000, ISR 4000 et CSR 1000v sont des exemples de plates-formes de routeur. Pour connaître la compatibilité des périphériques avec Cisco DNA Center, reportez-vous à la matrice de compatibilité Cisco DNA Center.

Pourquoi un appareil de télémétrie de trafic ?

Les périphériques filaires et sans fil de la gamme Cisco Catalyst 9000 effectuent une inspection approfondie des paquets (DPI) et fournissent des flux de données pour des services tels que Cisco AI Endpoint Analytics et Application Assurance dans Cisco DNA Center. Mais que se passe-t-il s'il n'y a aucun périphérique de la gamme Catalyst 9000 dans le réseau à partir duquel extraire la télémétrie ? Plusieurs entreprises ont encore une partie de leur infrastructure réseau qui n'a pas été migrée vers les plates-formes de la gamme Cisco Catalyst 9000. La plate-forme Catalyst 9000 génère la télémétrie AppVis, mais pour obtenir des informations AppX supplémentaires, l'appareil de télémétrie de trafic Cisco DNA peut être utilisé pour combler l'écart. L'objectif du TTA est de surveiller le trafic qu'il reçoit via les ports SPAN d'autres périphériques réseau qui n'ont pas la capacité de fournir des données Application Experience à Cisco DNA Center. Étant donné que les périphériques d'infrastructure hérités ne peuvent pas effectuer l'inspection approfondie des paquets requise pour l'analyse avancée, le dispositif de télémétrie du trafic Cisco DNA peut être utilisé pour générer la télémétrie AppX à partir des déploiements existants.



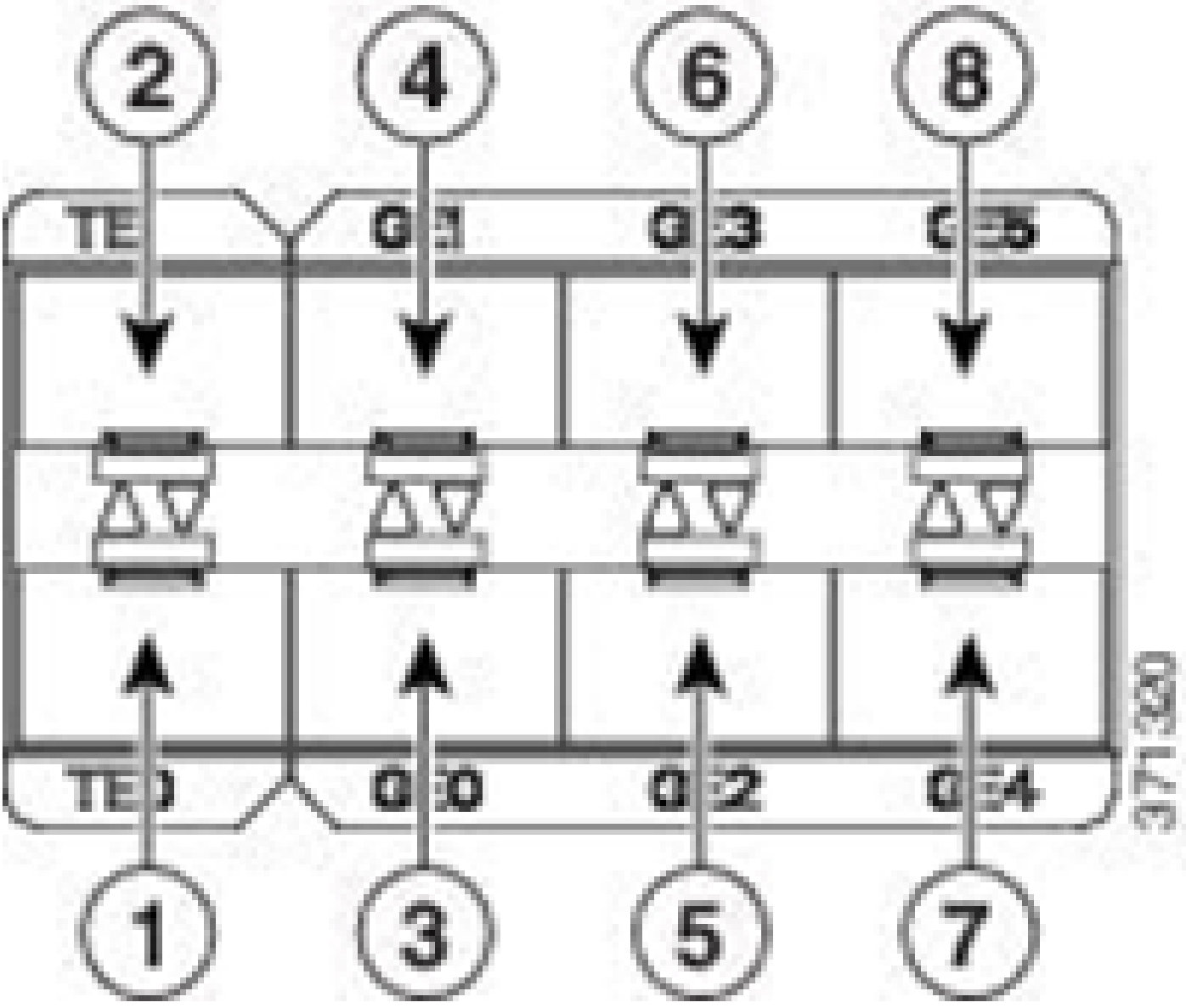
Cisco TTA en action

Détails du périphérique TTA

La plate-forme de capteurs de télémétrie basée sur la plate-forme Cisco IOS XE génère des données de télémétrie à partir du trafic réseau IP mis en miroir à partir de sessions SPAN (Switched Port Analyzer) de commutateurs et de contrôleurs sans fil. L'appliance inspecte des milliers de protocoles à l'aide de la technologie NBAR (Network-Based Application Recognition) afin de produire un flux de télémétrie permettant à Cisco DNA Center d'effectuer des analyses. L'appareil de télémétrie de trafic Cisco DNA peut gérer un trafic à débit soutenu de 20 Gbit/s et inspecter 40 000 sessions de points d'extrémité pour le profilage des périphériques.

L'appareil de télémétrie du trafic Cisco

L'ATT comporte un mélange de liaisons 10 et 10 Gig qui sont utilisées pour l'ingestion de SPAN. Parmi ces ports, Gig0/0/5 est le seul qui peut être configuré avec une adresse IP et utilisé pour communiquer avec Cisco DNA Center. La matrice d'interface est illustrée ci-dessous.



Matrice d'interface TTA			
1	Port 10 GE SFP+ 0/0/0	5	Port SFP GE 0/0/2
2	Port 10 GE SFP+ 0/0/1	6	Port SFP GE 0/0/3
3	Port SFP GE 0/0/0	7	Port SFP GE 0/0/4
4	Port SFP GE 0/0/1	8	Port SFP GE 0/0/5

Conditions préalables à l'assurance de Cisco DNA Center

Cette section met en évidence les configurations et les conditions préalables à respecter avant que Cisco DNA Center puisse traiter la télémétrie.

Cluster opérationnel Cisco DNA Center

La grappe Cisco DNA Center utilisée pour gérer la télémétrie TTA et de processus doit être fournie avec les critères suivants :

- Hiérarchie réseau: La section Hiérarchie du réseau du workflow de conception permet de définir différents campus de site, les bâtiments de ces campus et les étages individuels de ces bâtiments et de les afficher sur une carte du monde. La hiérarchie site/réseau appropriée doit être configurée.
- Paramètres réseau: La section Network Settings permet de créer des paramètres réseau par défaut communs qui seront utilisés par les périphériques du réseau. Ces paramètres peuvent être appliqués de manière globale, ainsi qu'au niveau du site, du bâtiment ou de l'étage. Entrez les informations DNS, nom de domaine, syslog, NTP, fuseau horaire et bannière de connexion requises par le déploiement.
- Identifiants des périphériques: Ces informations d'identification seront utilisées pour accéder aux périphériques du réseau, y compris le TTA, et les détecter. Cisco DNA Center doit être configuré avec l'interface de ligne de commande et les identifiants SNMP appropriés. En plus de ces informations d'identification NetConf, il est recommandé de les posséder.
- Compte Cisco CCO : un compte CCO valide est requis pour relier l'appliance et tirer parti des fonctionnalités du cloud Cisco AI, télécharger des images pour SWIM et télécharger des packs de protocoles pour TTA et d'autres périphériques.

Intégration ISE et Cisco DNA Center

Cisco Identity Services Engine (ISE) et Cisco DNA Center peuvent être intégrés pour l'automatisation des politiques et des identités. ISE est également utilisé pour collecter des informations sur les terminaux afin d'exploiter Cisco AI Endpoint Analytics. PxGrid est utilisé pour mettre en oeuvre l'intégration entre ISE et Cisco DNA Center.

Les exigences d'intégration de Cisco DNA Center et ISE sont les suivantes :

- Le service pxGrid doit être activé sur ISE.
- L'accès en lecture/écriture ERS doit être activé.
- Le certificat d'administration ISE doit contenir l'adresse IP ou le nom de domaine complet d'ISE dans le champ du sujet ou du SAN.
- Le certificat système Cisco DNA Center doit contenir toutes les adresses IP ou les noms de domaine complets de Cisco DNA Center dans le champ du nom de l'objet ou du SAN.
- Les informations d'identification d'administrateur ISE ERS seront utilisées pour établir des communications ERS fiables entre ISE et Cisco DNA Center.
- Le noeud pxGrid doit être accessible depuis Cisco DNA Center.

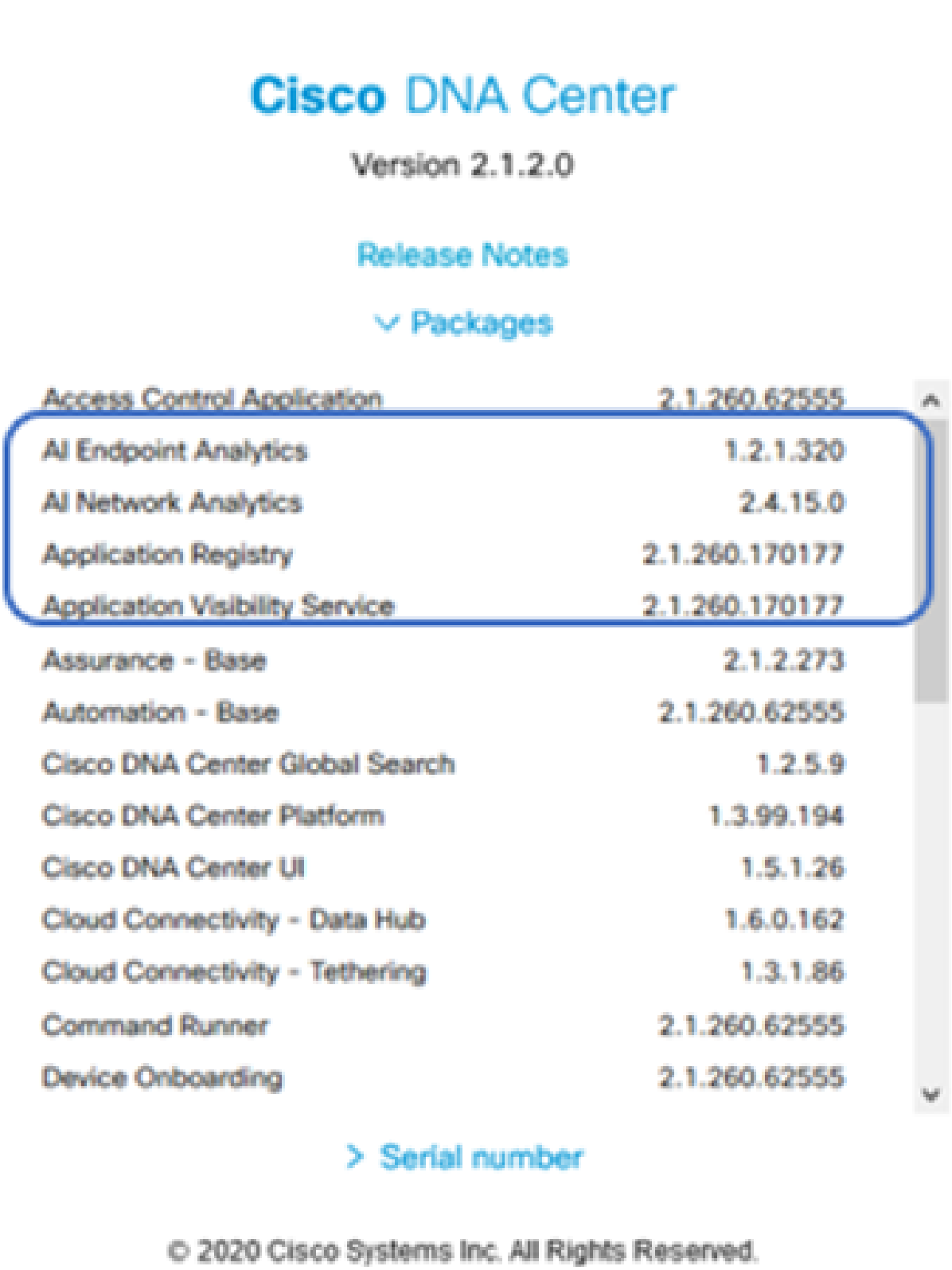
Exigences de Cisco DNA Center en matière de télémétrie

Certaines exigences doivent être mises en oeuvre pour activer l'assurance des applications dans Cisco DNA Center. Ces exigences sont expliquées en détail dans les sections qui suivent.

Packs clés de Cisco DNA Center

Cisco DNA Center nécessite l'installation de ces trois packages afin d'activer et d'analyser les données télémétriques.

- Analyses des terminaux AI
- Analyses réseau AI
- Services de visibilité des applications



Packages Cisco DNA Center requis

Pour accéder rapidement à ces informations, cliquez sur le lien "À propos de" sous l'icône représentant un point d'interrogation dans le coin supérieur droit de la page principale de Cisco DNA Center. Si ces applications sont manquantes, vous devez les installer avant de poursuivre la configuration de la télémétrie. Utilisez ce guide pour installer ces packages dans Cisco DNA

Center à partir du cloud Cisco. Guide de mise à niveau de Cisco DNA Center

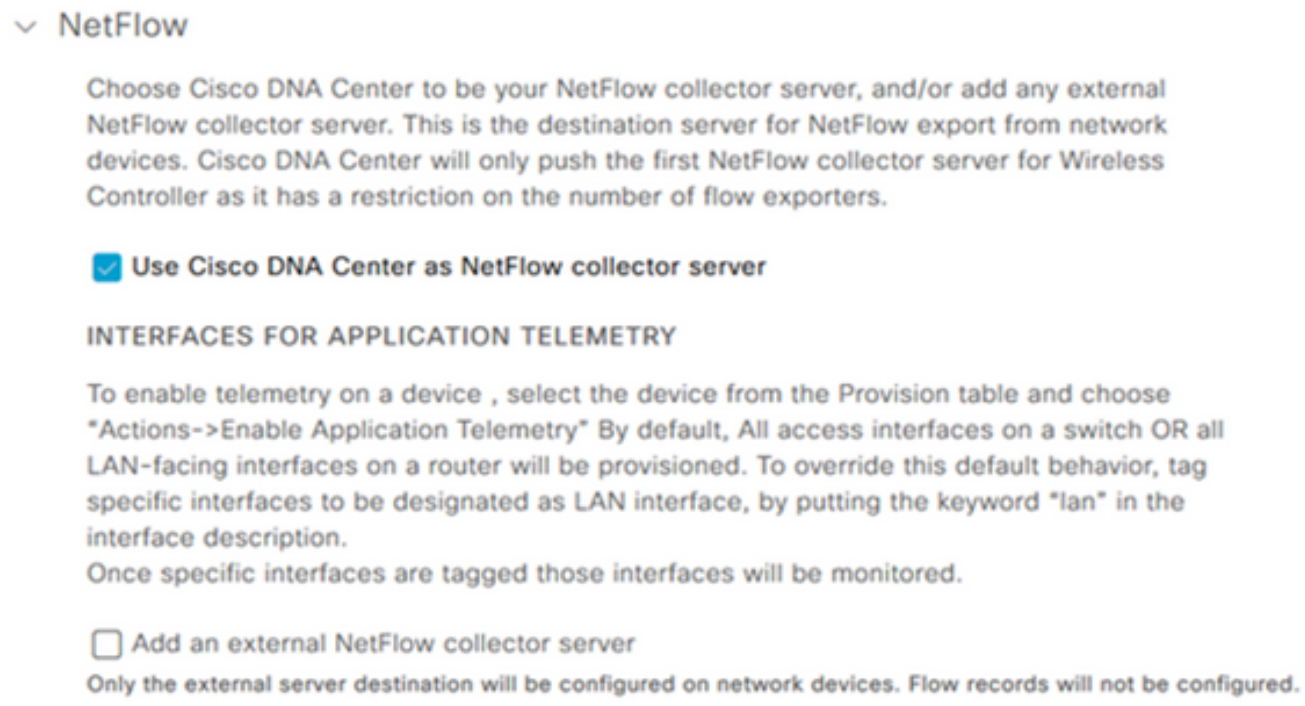
Cisco DNA Center en tant que collecteur de télémétrie

L'exportation de données NetFlow est le transport technologique qui fournit les données télémétriques qui seront transmises à Cisco DNA Center pour une analyse approfondie. NetFlow doit être exporté vers Cisco DNA Center afin de permettre la collecte de données pour l'apprentissage automatique et le raisonnement pour l'analytique des terminaux. TTA est une plate-forme de capteurs de télémétrie qui permet de générer des données télémétriques à partir du trafic réseau IP en miroir et de les partager avec Cisco DNA Center pour une visibilité sur les applications et les terminaux.

- Le trafic réseau est reçu des commutateurs et des routeurs via la mise en miroir SPAN (Switched Port Analyzer) et introduit dans les interfaces de mise en miroir de Cisco DNA Traffic Telemetry Appliance.
- L'appareil de télémétrie de trafic Cisco DNA analyse le trafic reçu pour produire un flux de télémétrie pour Cisco DNA Center.

Pour activer Cisco DNA Center en tant que collecteur de télémétrie, procédez comme suit.

- Dans Cisco DNA Center, cliquez sur Menu > Design > Network Settings et activez la télémétrie pour que Cisco DNA Center collecte NetFlow.



Configuration de DNAC en tant que collecteur NetFlow

Le cloud Cisco AI

Cisco AI Network Analytics est une application de Cisco DNA Center qui tire parti de la puissance

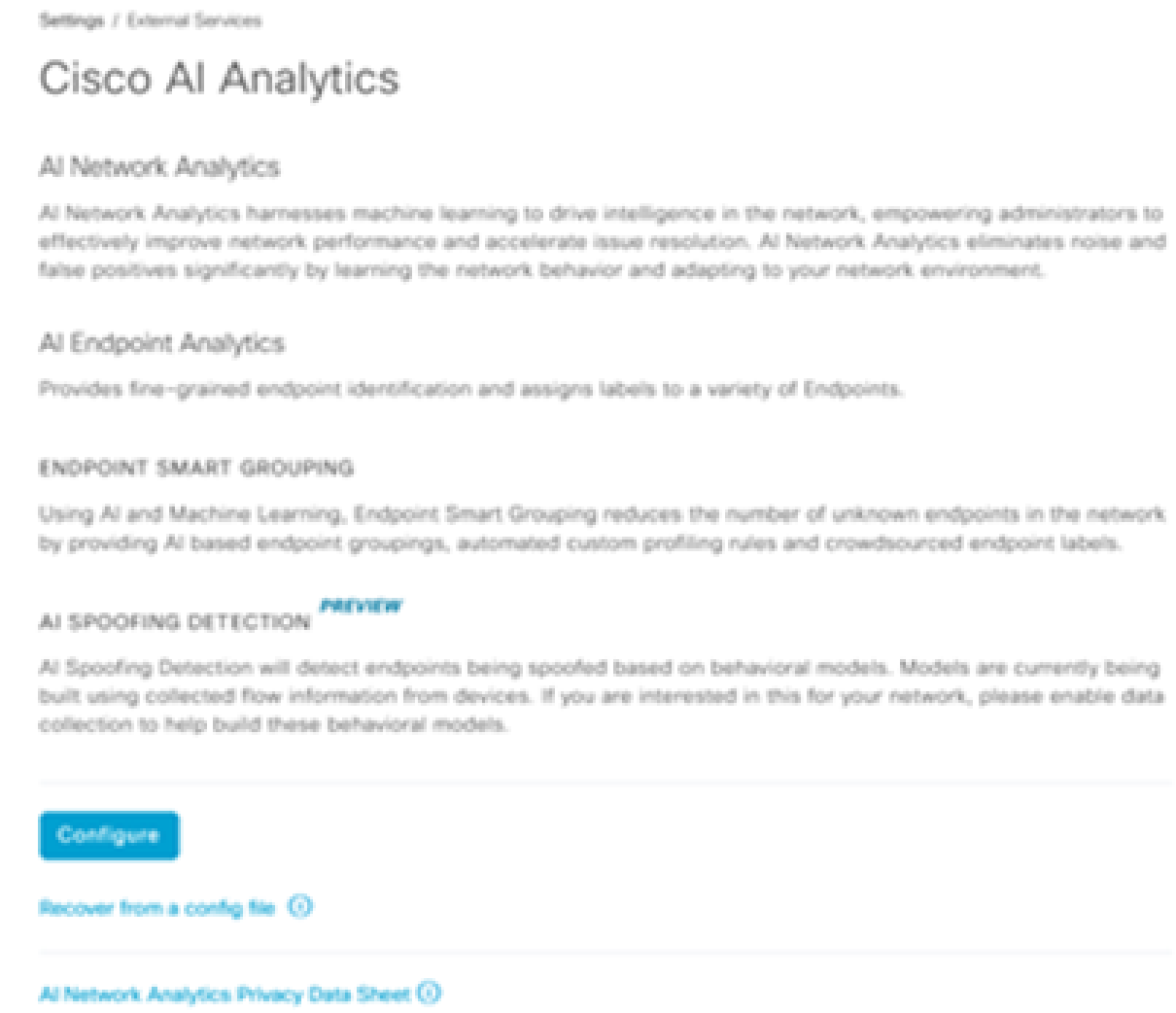
de l'apprentissage automatique et du raisonnement automatique pour fournir des informations précises spécifiques à votre déploiement réseau, ce qui vous permet de résoudre rapidement les problèmes. Les informations de réseau et de télémétrie sont anonymisées dans Cisco DNA Center, puis envoyées via un canal chiffré sécurisé à l'infrastructure cloud Cisco AI Analytics. Le cloud Cisco AI Analytics utilise le modèle d'apprentissage automatique avec ces données d'événement et renvoie les problèmes et les informations générales à Cisco DNA Center. Toutes les connexions au cloud sont sortantes sur TCP/443. Il n'y a aucune connexion entrante, le cloud Cisco AI n'initie aucun flux TCP vers Cisco DNA Center. Les noms de domaine complets (FQDN) qui peuvent être utilisés pour autoriser dans le proxy HTTPS et/ou le pare-feu au moment de la rédaction de cet article sont :

- https://api.use1.prd.kairos.ciscolabs.com (Région Est des États-Unis)
- https://api.euc1.prd.kairos.ciscolabs.com (Région centrale de l'UE)

L'appliance Cisco DNA Center déployée doit être en mesure de résoudre et d'atteindre les différents noms de domaine sur Internet qui sont hébergés par Cisco.

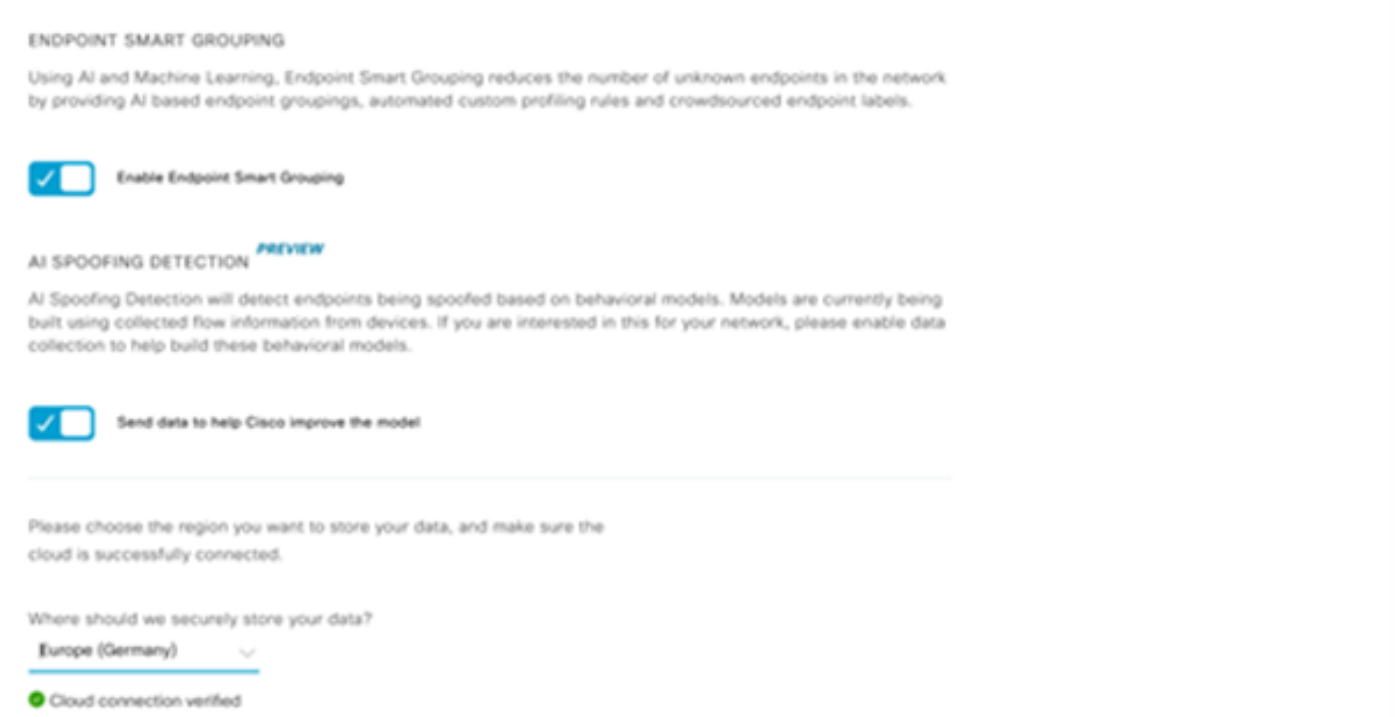
Procédez comme suit pour relier Cisco DNA Center au cloud Cisco AI.

- Accédez à l'interface utilisateur Web de l'appliance Cisco DNA Center pour terminer l'enregistrement du cloud AI :
- Naviguez jusqu'à Système > Paramètres > Services externes > Cisco AI Analytics
- Cliquez sur Configure et activez l'option Endpoint Smart Grouping and AI spoof detection.
- Le regroupement intelligent des terminaux utilise le cloud AI/ML pour regrouper les terminaux inconnus afin d'aider les administrateurs à étiqueter ces terminaux. Cela est très utile pour réduire les inconnues du réseau.
- La détection des usurpations d'IA aidera Cisco à recueillir des informations NetFlow/télémétriques supplémentaires et à modéliser le terminal.
- Choisissez l'emplacement le plus proche de la région géographique du déploiement. Une fois la vérification de la connexion au cloud effectuée et la connexion établie, une case à cocher verte s'affiche.



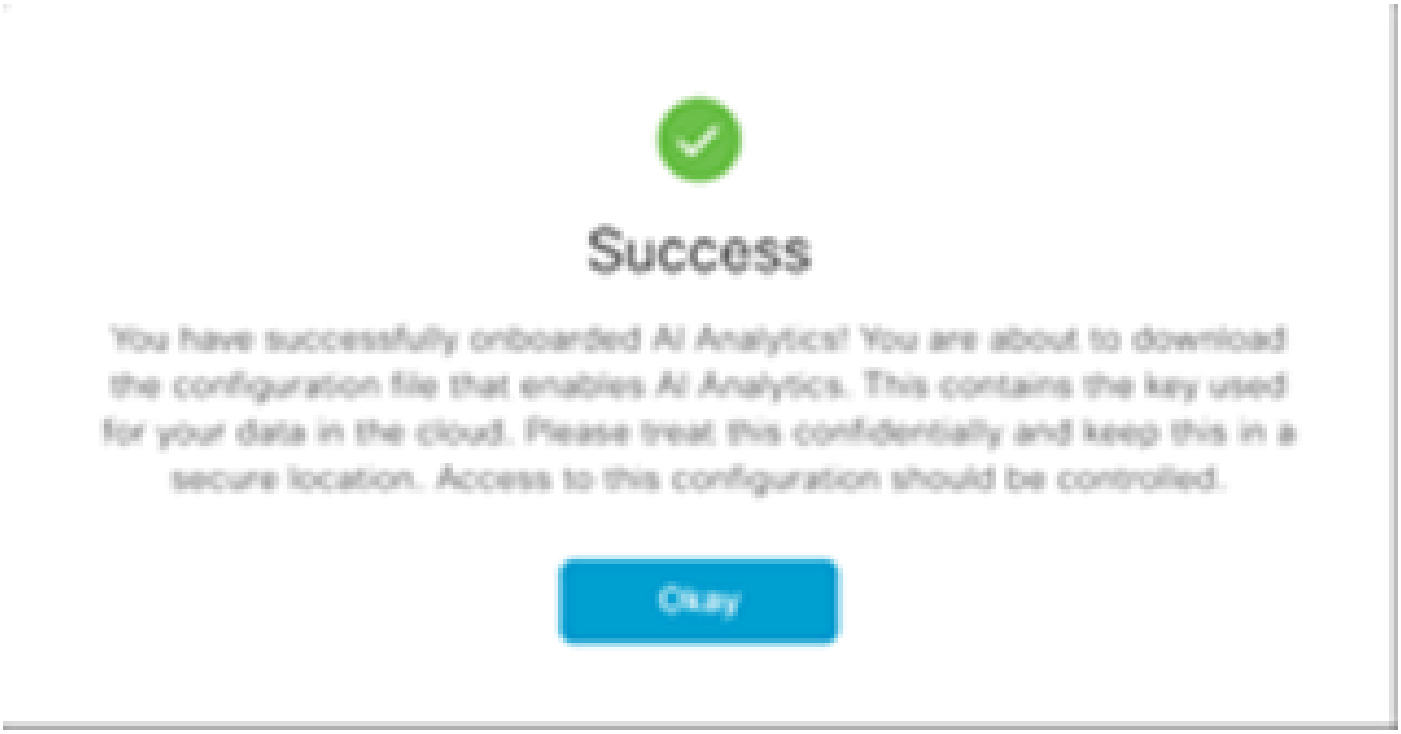
Configuration de l'interface Cisco AI Analytics

- Si la connexion échoue, vérifiez les paramètres de proxy dans Cisco DNA Center à partir de la page System > Settings > System Configuration > Proxy config si un proxy est utilisé. Il est également conseillé de vérifier les règles de pare-feu susceptibles de bloquer cette communication.



Vérification de la connexion au cloud Cisco AI/ML

- Acceptez l'accord Cisco Universal Cloud pour activer AI Analytics.
- À ce stade, l'intégration est terminée et une boîte de dialogue s'affiche, comme illustré.



Boîte de dialogue Réussite après l'inscription

Le cloud NBAR (Network Based Application Recognition)

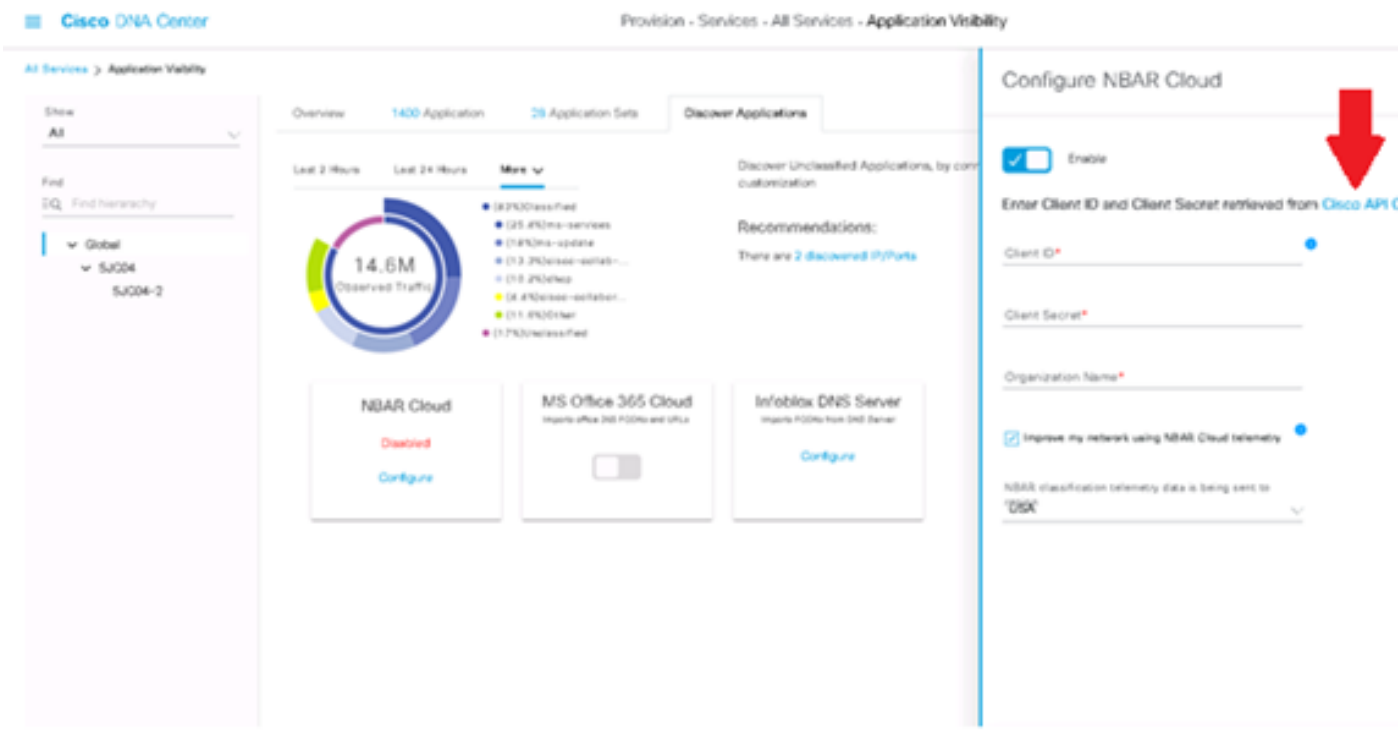
L'appareil de télémétrie et la plate-forme Catalyst 9000 collectent des métadonnées de point

d'extrémité à l'aide d'une inspection approfondie des flux de paquets et appliquent la reconnaissance d'application basée sur le réseau (NBAR) pour déterminer quels protocoles et quelles applications sont utilisés sur le réseau. Cisco DNA Center intègre un pack de protocoles NBAR qui peut être mis à jour. Les données de télémétrie peuvent être envoyées au nuage Cisco NBAR pour une analyse supplémentaire et pour la détection de signatures de protocole inconnues. Pour ce faire, l'appliance Cisco DNA Center doit être connectée au cloud. Network-Based Application Recognition (NBAR) est un moteur avancé de reconnaissance des applications développé par Cisco qui utilise plusieurs techniques de classification et peut facilement mettre à jour ses règles de classification.

Pour relier Cisco DNA Center au cloud Cisco NBAR, procédez comme suit.

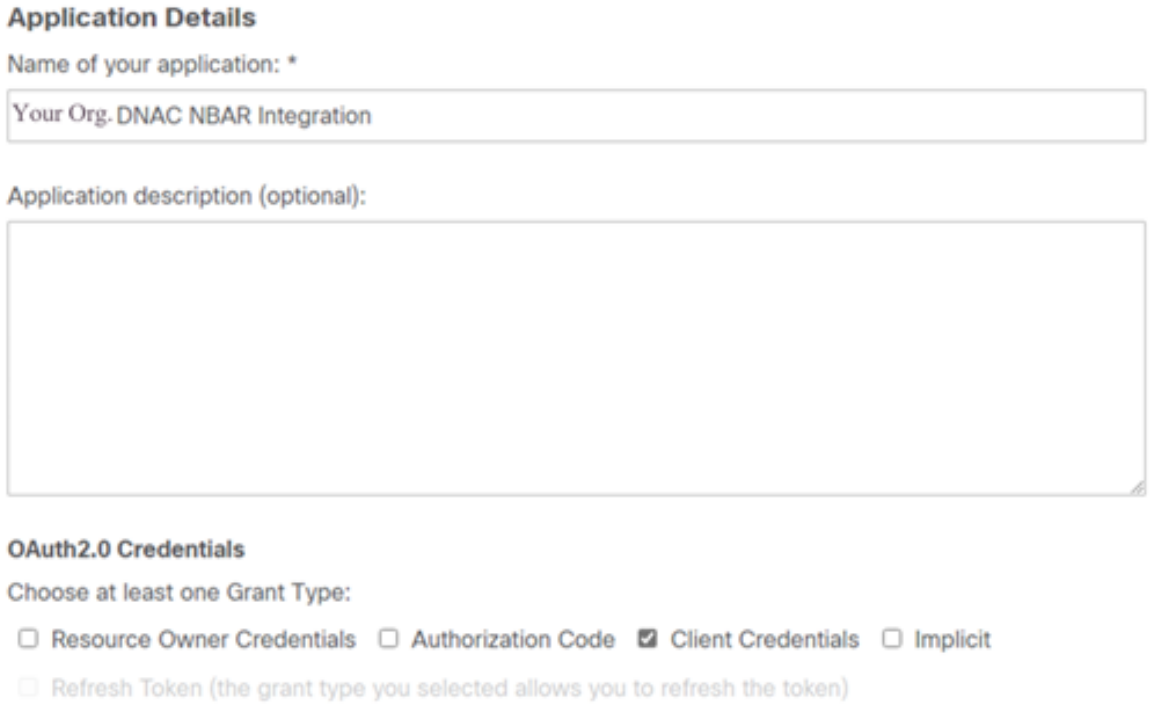
- Dans l'interface utilisateur de Cisco DNA Center, accédez à Provisionner > Services > Application Visibility. Cliquez sur Configure sous NBAR Cloud et un panneau s'ouvre. Activez le service.
- Si vous avez l'ID client, le secret client et le nom de l'entreprise, veuillez leur donner des noms uniques selon l'entreprise et l'utilisation.
- Au moment de la rédaction du présent rapport, la seule région NBAR Cloud actuellement disponible se trouve aux États-Unis ; d'autres régions pourraient être disponibles à l'avenir. Sélectionnez celui dans les préférences de déploiement et enregistrez-le.

Pour obtenir l'ID client et les informations d'identification du secret client, cliquez sur le lien « Cisco API Console », ce qui ouvre un portail. Connectez-vous avec l'ID CCO approprié, créez une nouvelle application, sélectionnez les options correspondant au cloud NBAR et remplissez le formulaire. Une fois terminé, vous obtiendrez un ID client et un code secret. Reportez-vous à la figure ci-dessous.



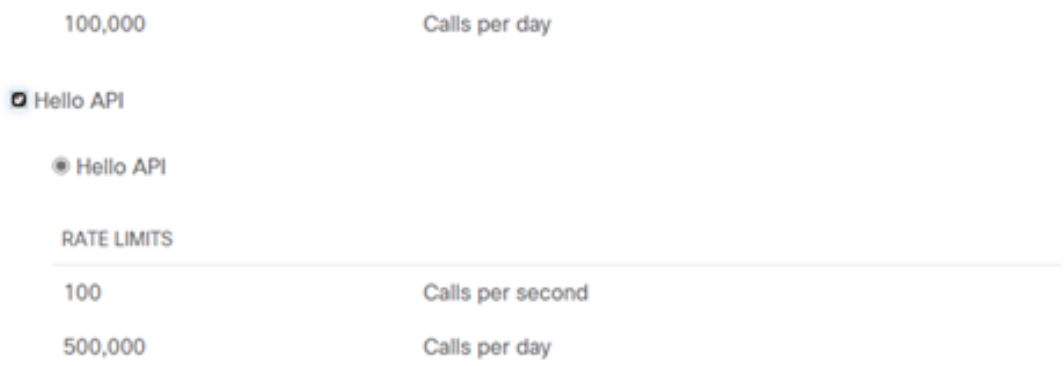
Lien de l'API Cisco pour récupérer l'ID et le secret client

Ces images illustrent les options utilisées pour l'enregistrement sur le cloud NBAR.



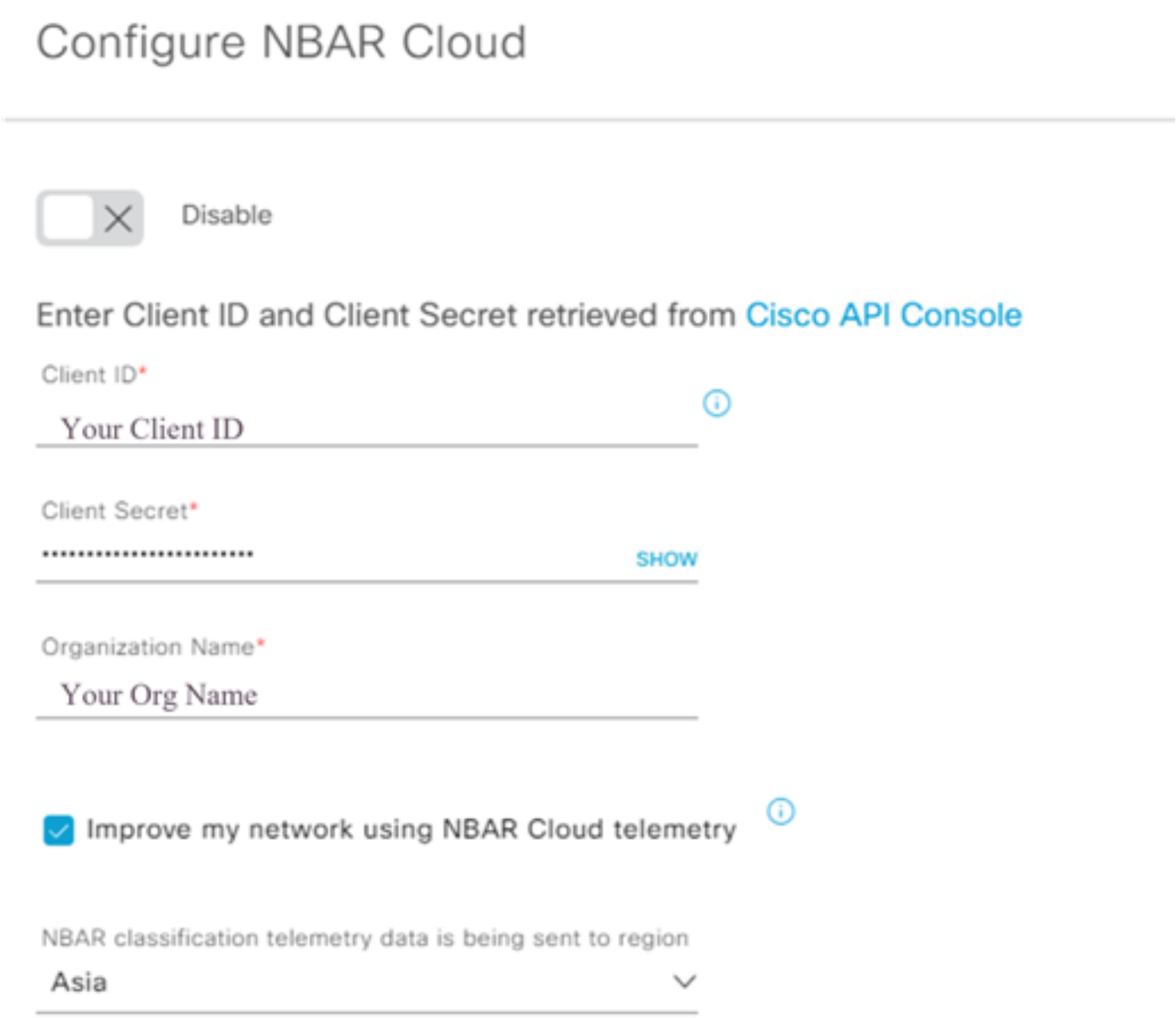
Détails de l'application cloud NBAR

- Utilisez cette image comme référence lors de l'exécution des détails de la demande d'API.



Détails API des applications

- Saisissez l'ID et le secret client obtenus à partir du portail Cisco dans Cisco DNA Center.



Configuration de l'ID et du secret client sur DNAC

CBAR (Controller Based Application Recognition) et SD-AVC

Le CBAR est utilisé pour classer des milliers d'applications réseau, d'applications développées en interne et le trafic réseau général. Il permet à Cisco DNA Center d'en savoir plus sur les applications utilisées sur l'infrastructure réseau de manière dynamique. Le CBAR permet de maintenir le réseau à jour en identifiant les nouvelles applications à mesure que leur présence sur le réseau continue à augmenter et en permettant les mises à jour des packs de protocoles. Si la visibilité des applications est perdue de bout en bout par le biais de packs de protocoles obsolètes, une catégorisation incorrecte et un transfert ultérieur peuvent se produire. Cela entraînera non seulement des trous de visibilité dans le réseau, mais également des problèmes

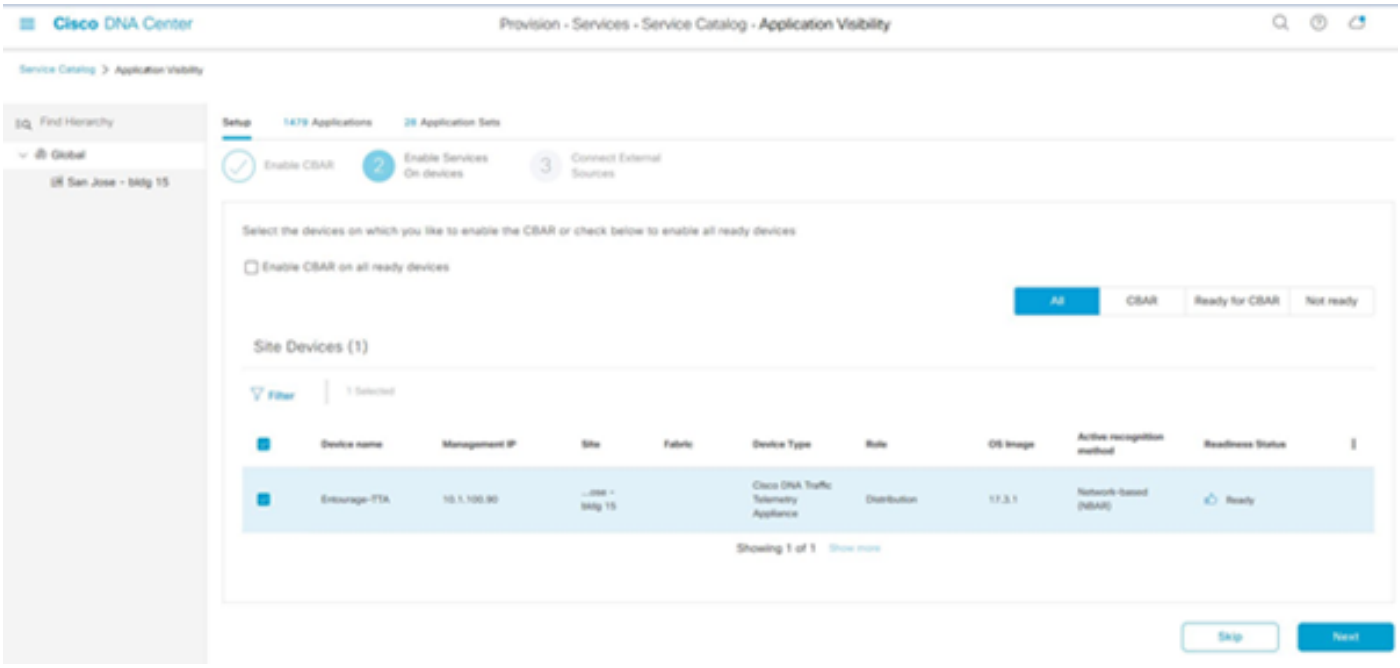
de mise en file d'attente ou de transfert incorrects. Le protocole CBAR résout ce problème en permettant la diffusion de packs de protocoles mis à jour sur le réseau.

Cisco Software-Defined AVC (SD-AVC) est un composant de Cisco Application Visibility and Control (AVC). Il fonctionne comme un service réseau centralisé fonctionnant avec des périphériques spécifiques participant à un réseau. SD-AVC aide également à la résolution en PPP des données d'application. Parmi les fonctionnalités et avantages actuels offerts par SD-AVC, citons :

- Reconnaissance des applications au niveau du réseau cohérente sur l'ensemble du réseau
- Meilleure reconnaissance des applications dans les environnements de routage symétrique et asymétrique
- Reconnaissance améliorée du premier paquet
- Mise à jour du pack de protocoles au niveau du réseau
- Tableau de bord SD-AVC sécurisé basé sur navigateur sur HTTPS pour la surveillance des fonctionnalités et des statistiques SD-AVC, et pour la configuration des mises à jour du pack de protocoles sur l'ensemble du réseau

Pour activer le CBAR pour les périphériques concernés, procédez comme suit.

- Accédez au menu de Cisco DNA Center, Provisionner > Visibilité des applications. Les Lors de la première ouverture de la page Visibilité sur les applications, un assistant de configuration s'affiche ci-dessous.
- Après avoir détecté les périphériques dans Cisco DNA Center pour chaque site, sélectionnez le périphérique sur lequel activer CBAR et passez à l'étape suivante.



Activation de CBAR sur le périphérique

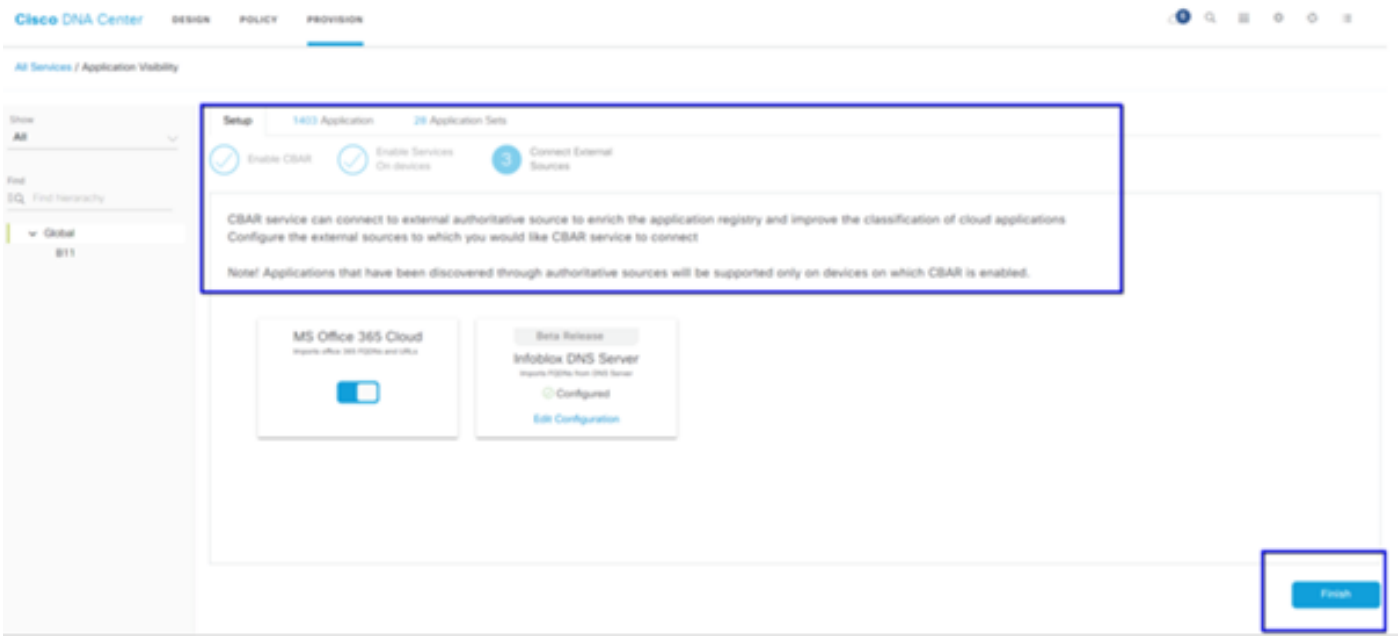
Connecteur cloud Microsoft Office 365 (non obligatoire)

Cisco DNA Center peut être intégré directement au flux RSS de Microsoft pour garantir que la

reconnaissance des applications pour Office 365 s'aligne sur les conseils publiés. Cette intégration est appelée Microsoft Office 365 Cloud Connector dans Cisco DNA Center. Il est recommandé de déployer cette fonctionnalité si l'utilisateur exécute des applications Microsoft Office 365 sur le réseau. L'intégration à Microsoft Office 365 n'est pas obligatoire et si elle n'est pas activée, elle affectera uniquement la capacité de Cisco DNA Center à traiter et à classer les données d'hôte Microsoft Office 365. Cisco DNA Center intègre déjà la reconnaissance des applications Microsoft Office 365, mais en s'intégrant directement au fournisseur d'applications, Cisco DNA Center peut obtenir des informations précises et mises à jour sur les blocs de propriété intellectuelle et les URL utilisés par la suite Microsoft Office 365.

Pour intégrer Cisco DNA Center à Microsoft Office 365 Cloud, procédez comme suit.

- Cliquez sur l'icône Menu et choisissez Provisionnement > Services > Application Visibility
- Cliquez sur Découvrir les applications
- Cliquez sur le bouton bascule Cloud MS Office 365 pour intégrer Cisco DNA Center au cloud Microsoft Office 365.

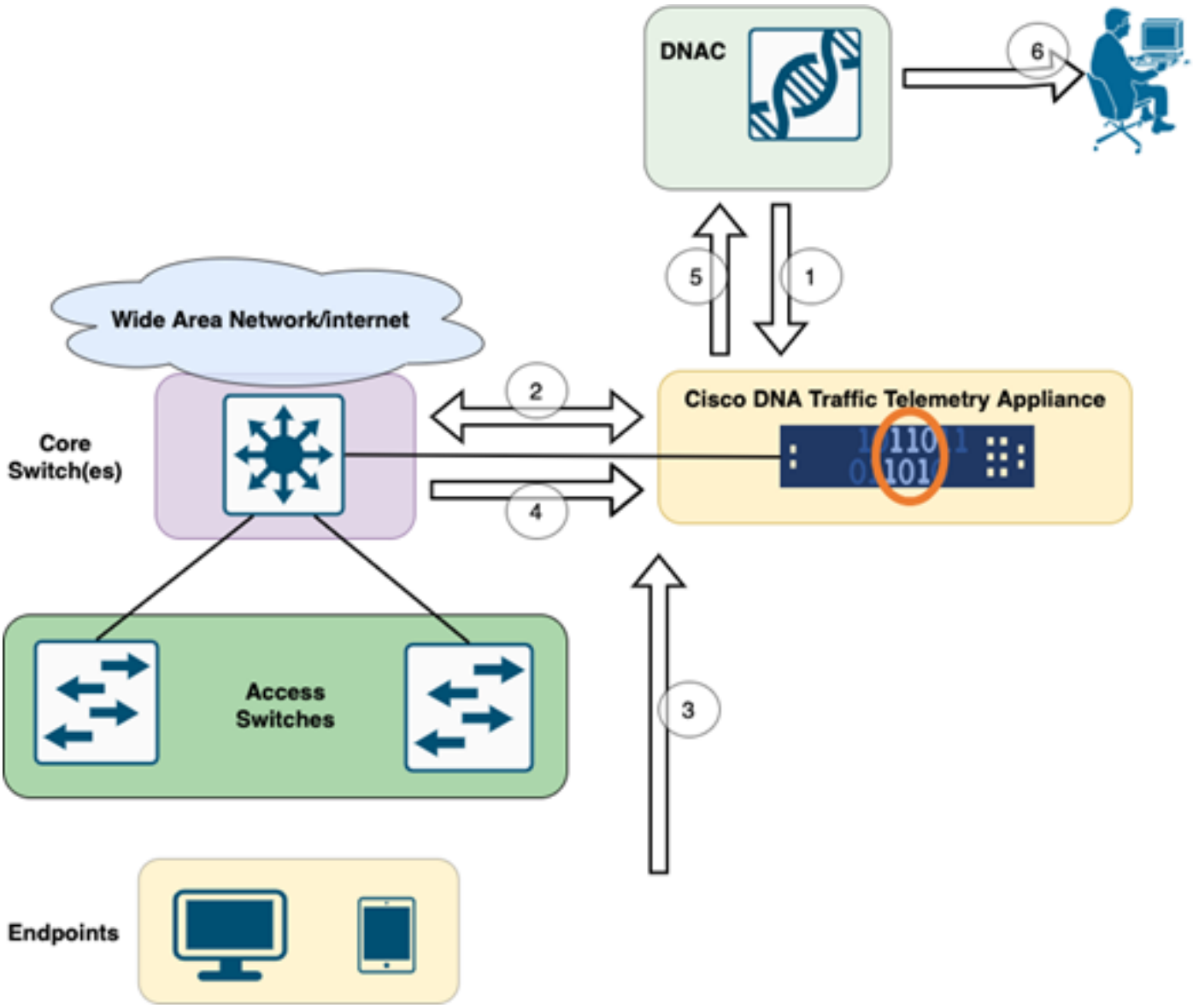


Intégration cloud MS O365

Implémentation TTA

Cette section décrit les étapes nécessaires à la mise en oeuvre de la fonction TTA dans un réseau.

Présentation du workflow TTA



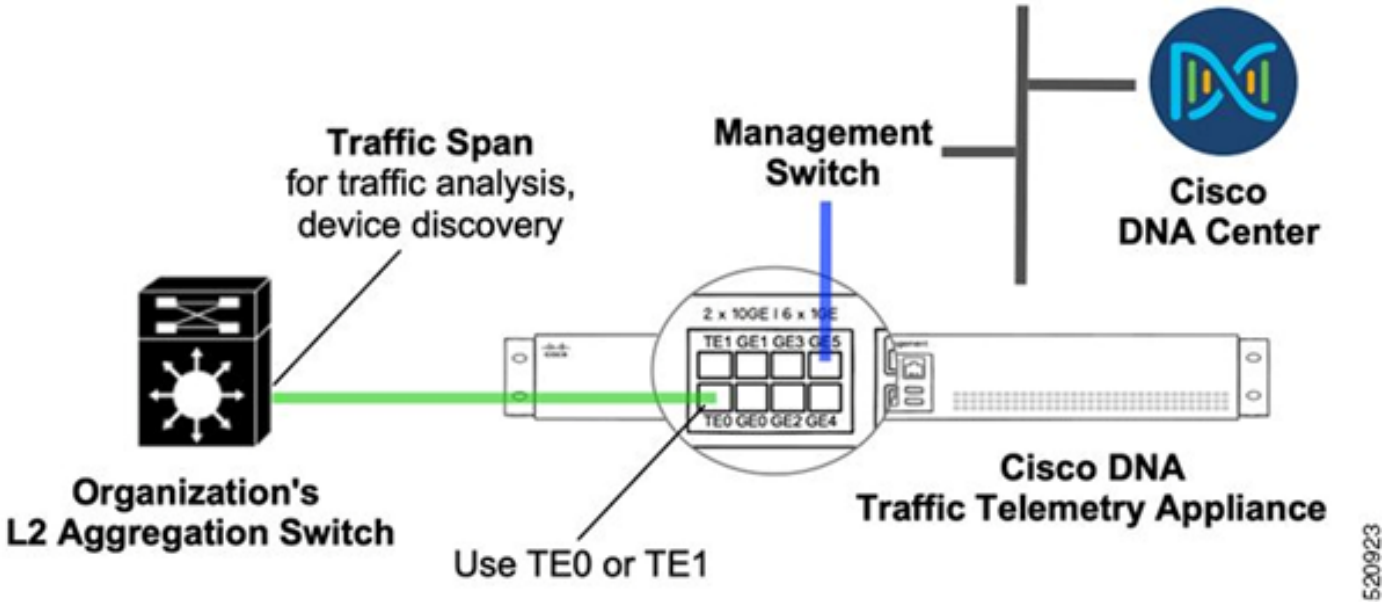
Workflow TTA vers DNAC

Les étapes mises en évidence dans ce schéma décrivent le processus et le flux télémétrique entre TTA et Cisco DNA Center. Ces étapes sont décrites plus en détail.

1. L'appareil de télémétrie du trafic Cisco est connecté au commutateur d'agrégation de site ou au commutateur principal au sein de l'infrastructure réseau. Cette connexion permet à la solution matérielle-logicielle de recevoir des données de trafic provenant de divers commutateurs d'accès du réseau.
2. Cisco Traffic Telemetry Appliance est intégré à Cisco DNA Center, qui sert de plate-forme de gestion du réseau. Cette intégration permet une communication et un échange de données transparents entre l'appliance et Cisco DNA Center.
3. À mesure que le trafic utilisateur circule sur le réseau, il est étendu ou mis en miroir sur l'appareil de télémétrie de trafic Cisco. Cela signifie qu'une copie du trafic réseau est envoyée à l'appliance à des fins de surveillance et d'analyse, tandis que le trafic d'origine continue son chemin normal.
4. L'appareil de télémétrie du trafic Cisco collecte et traite les données de trafic reçues. Il extrait du trafic mis en miroir les informations pertinentes, telles que les détails au niveau des paquets, les statistiques de flux et les mesures de performances.

5. Les informations de télémétrie traitées sont ensuite envoyées de Cisco Traffic Telemetry Appliance à Cisco DNA Center. Cette communication permet à Cisco DNA Center de recevoir en temps réel des informations et des mises à jour sur les modèles de trafic, les performances des applications et les anomalies du réseau.
6. Les informations télémétriques générées par Cisco DNA Center fournissent des informations précieuses aux administrateurs réseau. Ils peuvent utiliser l'interface de Cisco DNA Center pour visualiser et analyser les données collectées, obtenir une visibilité sur l'état du réseau et les performances des applications, identifier les problèmes potentiels et prendre des décisions éclairées pour l'optimisation et le dépannage du réseau.

Déploiement TTA : schéma de haut niveau



Déploiement TTA : haut niveau

Le schéma ci-dessus montre comment TTA peut être connecté au réseau. Les interfaces 10 Gig et 1 Gig peuvent être utilisées pour la réception SPAN à la vitesse de ligne. L'interface Gi0/0/5 est utilisée pour la communication avec Cisco DNA Center, pour l'orchestration et pour la transmission des informations télémétriques à Cisco DNA Center ; cette interface NE PEUT PAS être utilisée pour l'acquisition de la fonctionnalité SPAN.

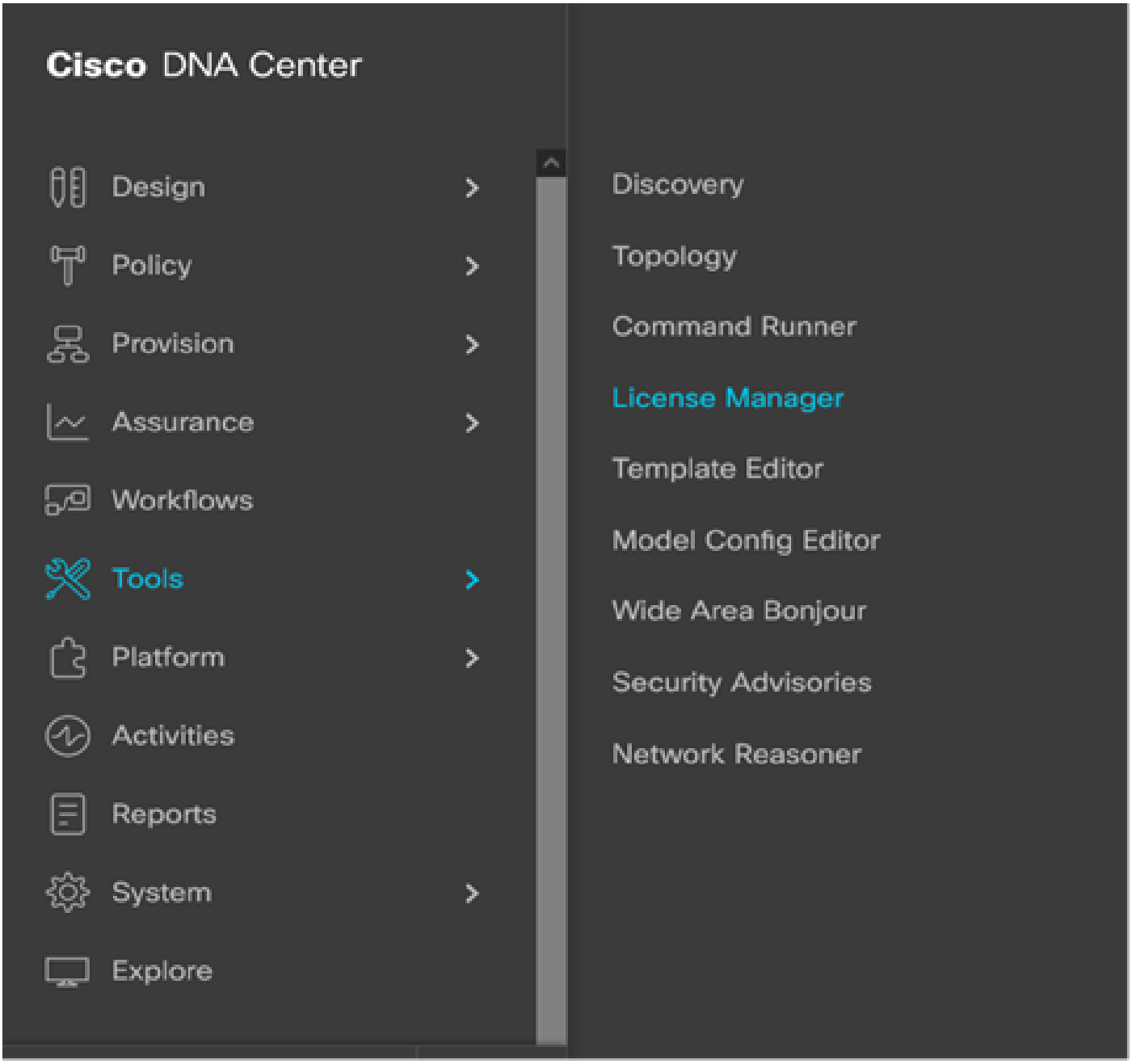
Logiciels et conditions de licence TTA

Les appliances TTA déployées sur le réseau seront essentielles pour fournir des informations télémétriques sur les données et les terminaux des utilisateurs. Pour réussir le déploiement de la solution, ces conditions doivent être remplies.

- TTA doit être configuré avec une configuration d'amorçage initiale afin qu'il puisse être découvert par Cisco DNA Center (configuration d'amorçage TTA)
- L'appliance TTA doit être intégrée à Cisco DNA Center pour pouvoir être gérée par Cisco DNA Center (ajout d'un boîtier de télémétrie à l'inventaire Cisco DNA Center)
- La licence appropriée doit être installée sur le TTA (TTA Appliance License)

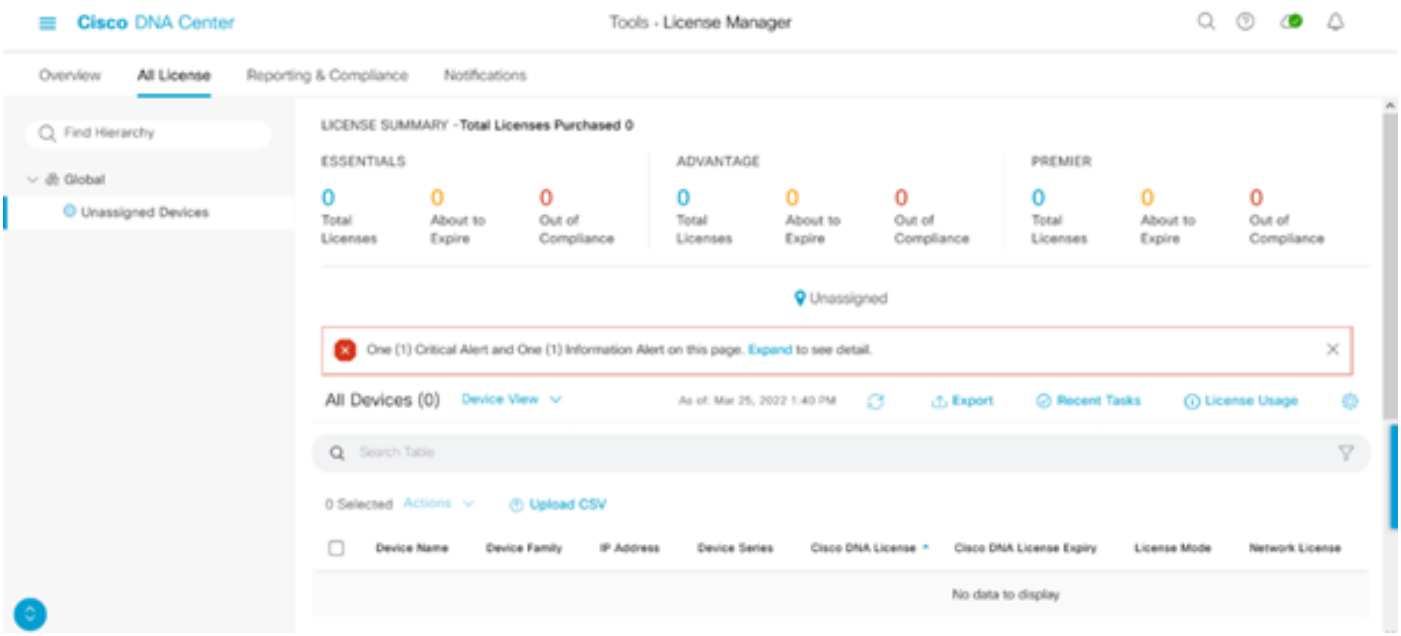
L'appliance ne prend en charge qu'un seul système d'exploitation et nécessite la licence Cisco DNA TTA Advantage pour collecter les données télémétriques. Il n'est pas nécessaire de disposer d'une licence de fonction (telle qu'IP Base ou Advanced IP Services) ou d'un package de licence perpétuelle (tel que Network Essentials ou Network Advantage).

Pour gérer les licences dans Cisco DNA Center, accédez au gestionnaire de licences en sélectionnant Tools > License Manager dans le menu déroulant de Cisco DNA Center en cliquant sur l'icône Menu



License Manager sur DNAC

- Accédez à la page All License ; elle ressemblera à cette image. Sur cette page, l'administrateur peut gérer les licences de périphériques réseau comme celles de l'ATT.



Page Toutes les licences sur DNAC

Intégration TTA et configuration du jour 0

Pour faciliter la découverte et l'intégration de l'appliance TTA par Cisco DNA Center, des commandes bootstrap doivent être configurées sur les appliances TTA du site. Une fois la configuration bootstrap en place, le TTA sera détectable à partir du tableau de bord de Cisco DNA Center. Les éléments de configuration du jour 0 pour un appareil TTA sont les suivants. Une fois le périphérique intégré à la hiérarchie du site, l'appliance TTA hérite des éléments de configuration restants 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
```

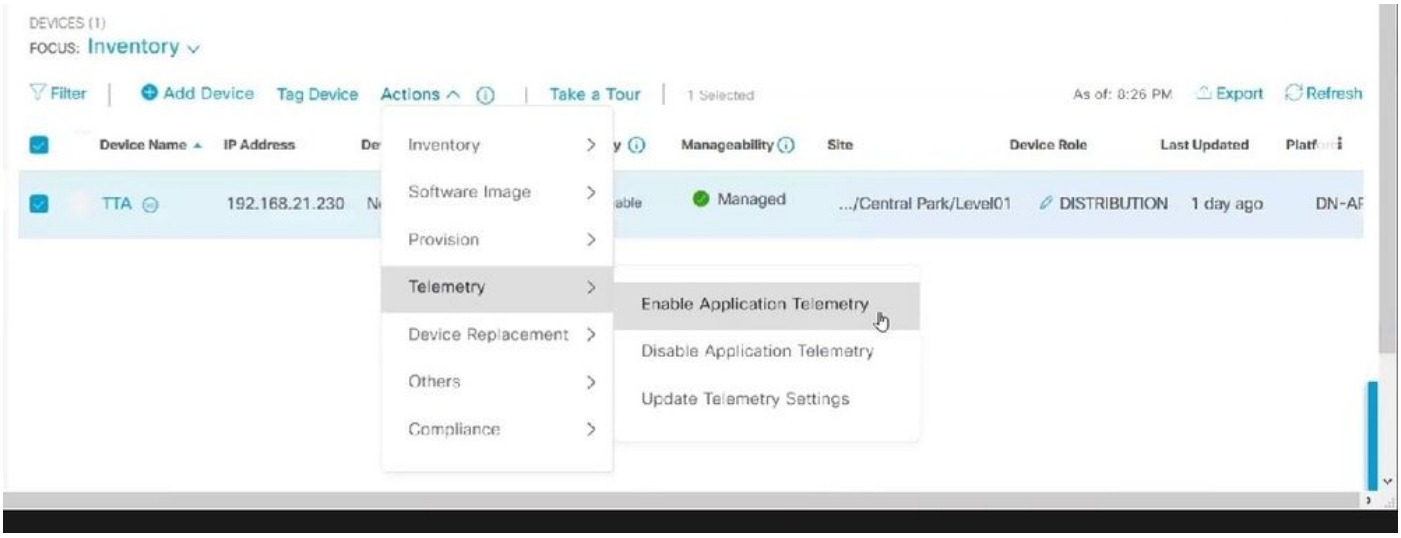
```
ip ssh source-interface GigabitEthernet0/0/5

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
```

Une fois que ces éléments sont configurés sur le TTA, ils peuvent être détectés par Cisco DNA Center.

Ajout de l'appliance TTA à l'inventaire de Cisco DNA Center

Pour tirer parti du TTA, Cisco DNA Center doit détecter et gérer l'appliance TTA. Une fois que le TTA est intégré à Cisco DNA Center, il peut être géré à partir de Cisco DNA Center. Avant de découvrir l'appliance TTA, nous devons nous assurer que la hiérarchie complète du site est en place. Ensuite, nous allons ajouter l'appliance TTA sous la hiérarchie de site spécifique en suivant ces étapes à partir de la page Menu > Provisionner > Périphériques > Inventaire pour ajouter le périphérique à un site.

1. Fournissez le nom d'utilisateur/mot de passe (CLI) et la communauté SNMP nécessaires pour se connecter au périphérique et au mot de passe enable. Attendez que le périphérique soit ajouté avant de continuer.
2. Vérifiez le nom du périphérique, la famille (gestion du réseau en cas de TTA), l'accessibilité - accessible, gérable, le rôle du périphérique - distribution. Le périphérique sera initialement « Non conforme », mais une fois entièrement provisionné, son état changera.
3. Une fois le TTA intégré, Cisco DNA Center diffuse des modèles de configuration pour le configurer avec des fonctions de télémétrie avancées.



Découverte TTA et activation de la télémétrie des applications

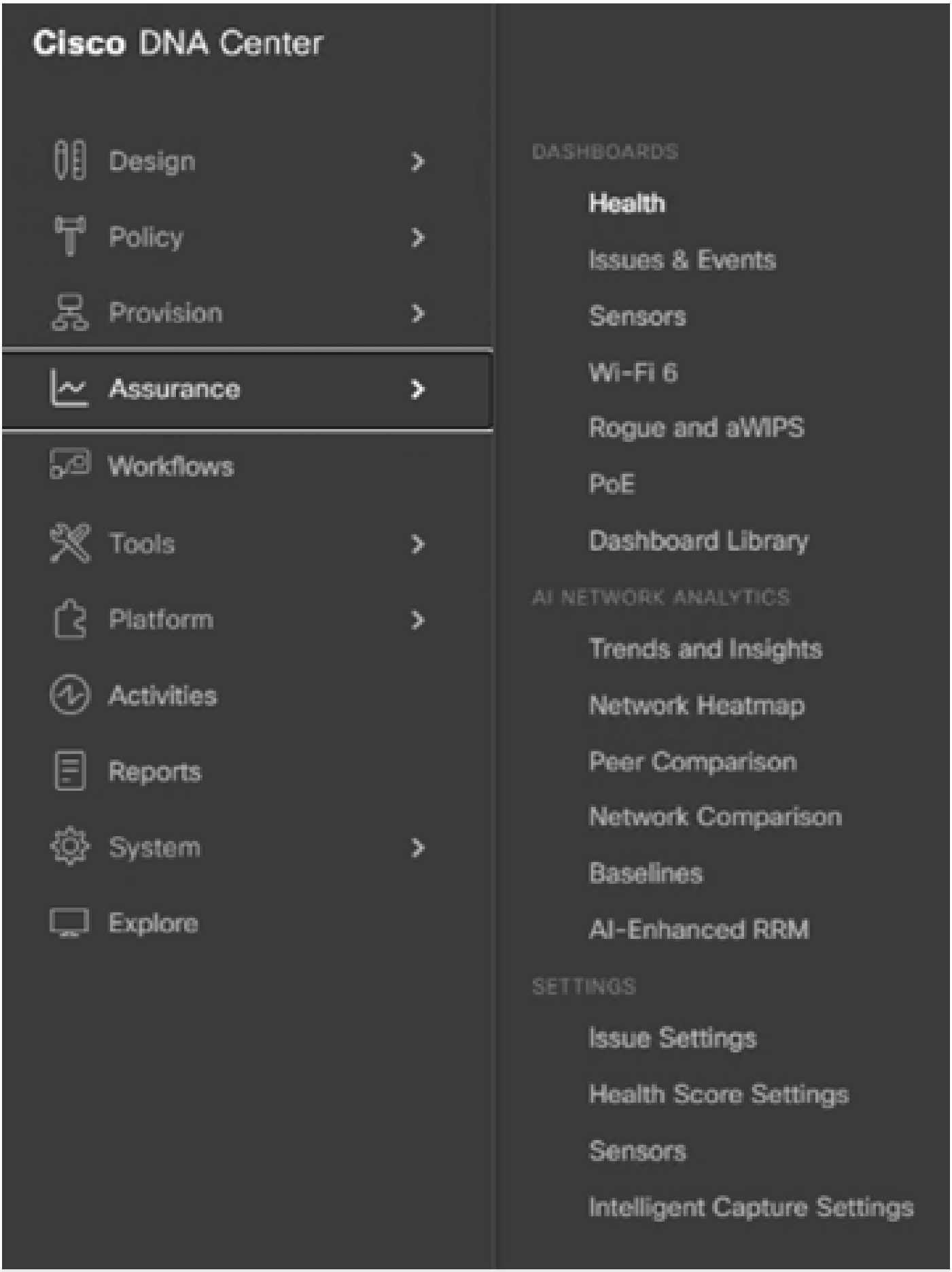
Configuration SPAN

En fonction des capacités matérielles du commutateur principal, la session SPAN peut être configurée pour effectuer une analyse SPAN d'un groupe de VLAN ou d'une ou plusieurs interfaces vers l'interface connectée à la TTA. Un exemple de configuration est fourni ici.

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

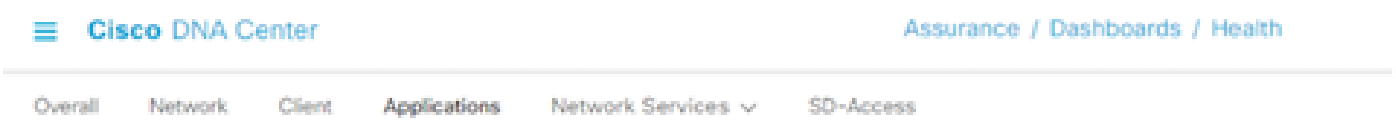
Assurance collectée

Pour accéder aux données d'assurance collectées à partir de l'appareil de télémétrie du trafic installé, accédez à la section Assurance et cliquez sur Health.

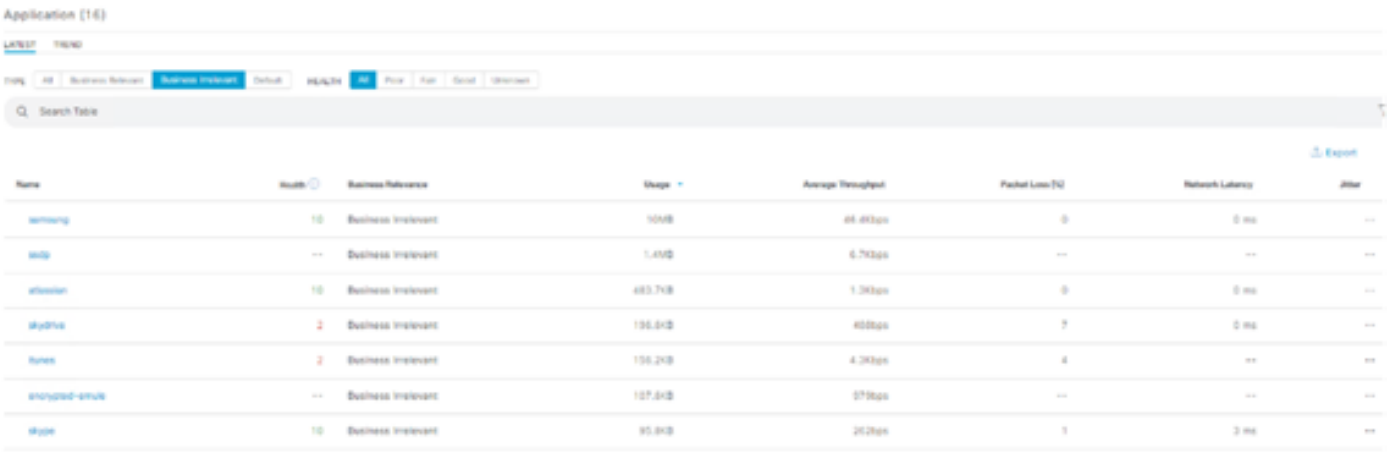


Navigation vers App Assurance

Choisissez Applications, et vous trouverez une vue d'ensemble complète des données d'application, y compris la latence et la gigue capturées par le TTA en fonction du type d'application spécifique.

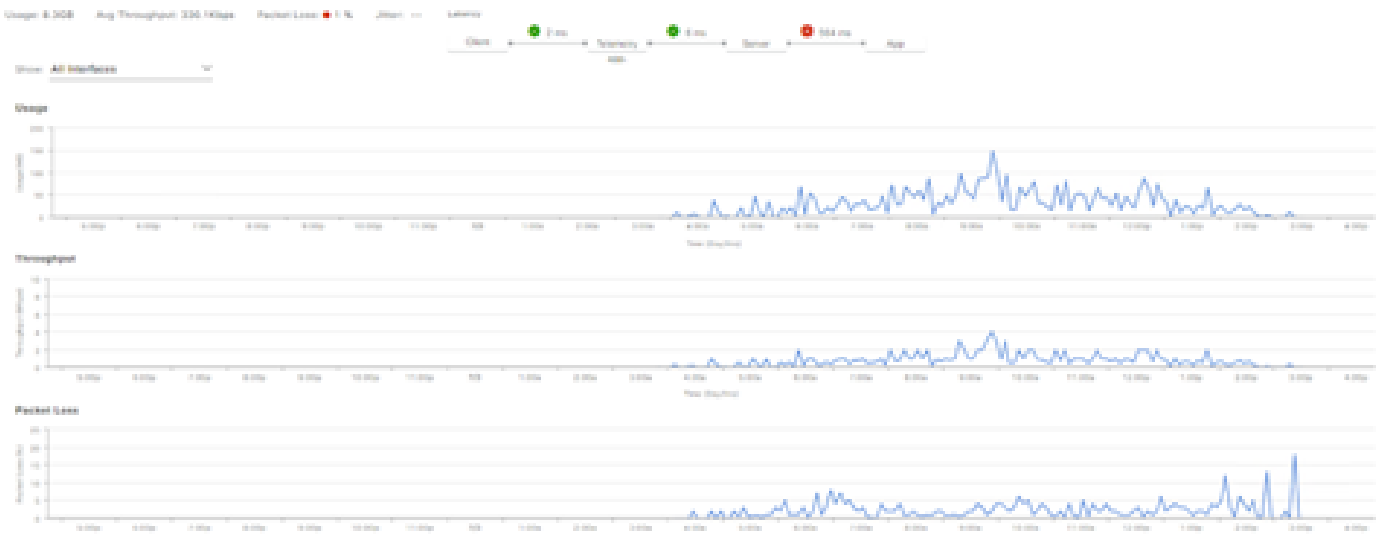


Accès à Application Assurance



Interface utilisateur d'assurance application détaillée

Pour une analyse plus détaillée, les utilisateurs peuvent explorer des applications individuelles en cliquant sur l'application spécifique et en sélectionnant l'exportateur comme appliance de télémétrie du trafic et examiner des mesures spécifiques telles que l'utilisation, le débit et les données de perte de paquets, la latence du réseau client, la latence du réseau serveur et la latence du serveur d'applications.



Exemple : Caractéristiques D'Application Pt.1

Exemple : Caractéristiques D'Application Pt.2

Vérifier

1. Après avoir activé CBAR, vérifiez que le service SD-AVC (Application Visibility Control) est activé sur le périphérique en vous connectant à Cisco Traffic Telemetry Appliance et en exécutant cette commande CLI. Le résultat sera similaire à cet exemple indiquant l'adresse IP du contrôleur et l'état connecté.

```
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. Utilisez la commande « show license summary » dans l'interface de ligne de commande de l'ATT pour vérifier les détails pertinents de la licence de périphérique.

```
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. Vérifiez que la session SPAN a été correctement configurée sur le commutateur principal/d'agrégation.

```
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. Une fois le TTA configuré avec succès, ces commandes seront (ou ont été) envoyées au périphérique.

```
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
```

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.