Utilizzo di Traffic Telemetry Appliance (TTA) e Cisco DNA Center App Assurance: il perché e il come

Sommario

- Introduzione
- Prerequisiti
- Application Assurance
  - Visibilità applicazione (AppVis)
  - Esperienza applicazione (AppX)
- Perché un'appliance di telemetria per il traffico?
- Dettagli dispositivo TTA
- Cisco DNA Center - Prerequisiti per la garanzia
- Cluster operativo Cisco DNA Center
- Integrazione tra ISE e Cisco DNA Center
- Requisiti di Cisco DNA Center per la telemetria
  - Pacchetti chiave Cisco DNA Center
  - Cisco DNA Center come Telemetry Collector
  - Cisco AI Cloud
  - Cloud NBAR (Network Based Application Recognition)
  - CBAR (Controller Based Application Recognition) e SD-AVC
  - Microsoft Office 365 Cloud Connector (non necessariamente)
- Implementazione TTA
- Panoramica sul flusso di lavoro TTA
- Distribuzione TTA: diagramma ad alto livello
- Requisiti di licenza e software TTA
- Onboarding TTA e configurazione del giorno 0
- Aggiunta dell'appliance TTA all'inventario di Cisco DNA Center
- configurazione SPAN
- Garanzia raccolta
- Verifica

Introduzione

Questo documento descrive la piattaforma Cisco DNA Traffic Telemetry Appliance (numero di parte Cisco DN-APL-TTA-M) e le modalità di abilitazione di Application Assurance in Cisco DNA Center. IInoltre, fornisce alcune indicazioni su come e dove posizionare il TTA in una rete insieme al processo di configurazione e verifica. Questo articolo affronta anche i vari prerequisiti coinvolti.

Prerequisiti

Cisco raccomanda la conoscenza delle modalità di funzionamento di Cisco DNA Center Assurance e Application Experience.

Application Assurance

Assurance è un motore di raccolta e analisi dei dati di rete multifunzione e in tempo reale in grado di aumentare in modo significativo il potenziale di business dei dati di rete. Assurance elabora dati complessi delle applicazioni e presenta i risultati nei dashboard di integrità Assurance per fornire informazioni dettagliate sulle prestazioni delle applicazioni utilizzate nella rete. A seconda della posizione da cui vengono raccolti i dati, è possibile visualizzare alcuni o tutti gli elementi seguenti:

- Nome applicazione
- Velocità effettiva
- Contrassegni DSCP
- Metriche delle prestazioni (latenza, jitter e perdita di pacchetti)

In base alla quantità di dati raccolti, Application Assurance può essere suddiviso in due modelli:

- Visibilità delle applicazioni (AppVis) e
- Esperienza applicazione (AppX)

Il nome dell'applicazione e il throughput vengono definiti collettivamente metriche quantitative. I dati per le metriche quantitative derivano dall'attivazione di Visibilità applicazione.

Le indicazioni DSCP e le metriche delle prestazioni (latenza, jitter e perdita di pacchetti) sono collettivamente denominate metriche qualitative. I dati per le metriche qualitative derivano dall'attivazione di Esperienza applicazione.

Visibilità applicazione (AppVis)

I dati relativi alla visibilità delle applicazioni vengono raccolti dagli switch con Cisco IOS® XE e dai controller wireless con AireOS. Per gli switch con Cisco IOS XE, i dati di visibilità delle applicazioni vengono raccolti utilizzando un modello NBAR predefinito che viene applicato bidirezionalmente (in entrata e in uscita) alle porte dello switch di accesso al livello fisico. Per i controller wireless che eseguono AireOS, i dati di visibilità delle applicazioni vengono raccolti sul controller wireless e quindi la telemetria di streaming viene utilizzata per trasportare questi dati a Cisco DNA Center.

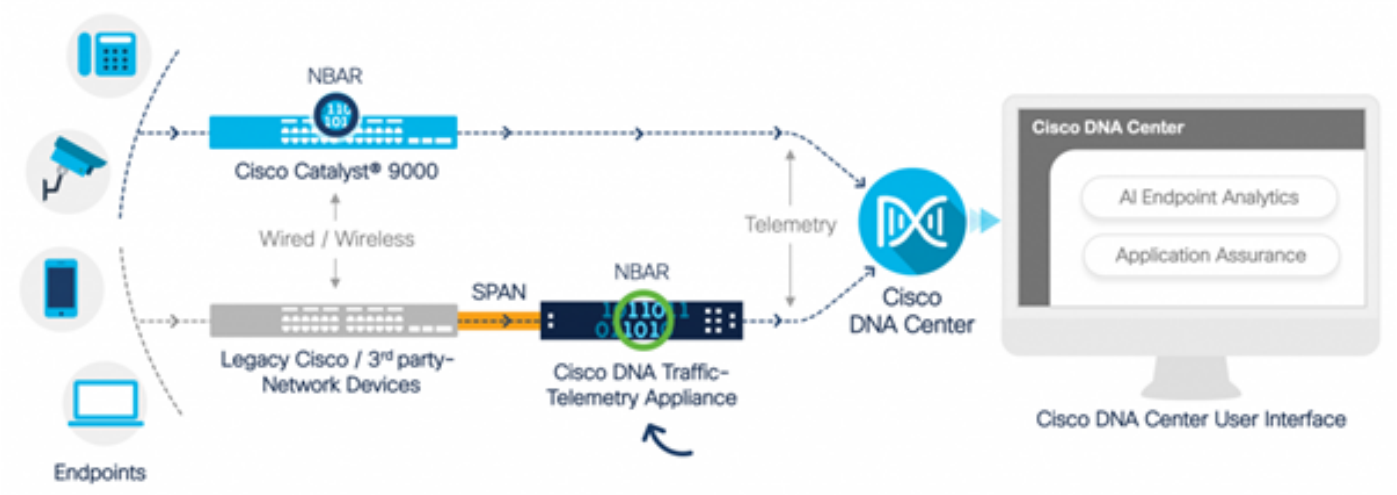
Esperienza applicazione (AppX)

I dati Application Experience vengono raccolti dalle piattaforme router Cisco IOS XE, in particolare utilizzando la funzionalità Cisco Performance Monitor (PerfMon) e le metriche Cisco Application Response Time (ART). Esempi di piattaforme di router includono ASR 1000, ISR 4000 e CSR 1000v. Per la compatibilità dei dispositivi con Cisco DNA Center, vedere la matrice di compatibilità

di Cisco DNA Center.

Perché un'appliance di telemetria per il traffico?

I dispositivi cablati e wireless Cisco Catalyst serie 9000 eseguono un'ispezione approfondita dei pacchetti (DPI) e forniscono flussi di dati per servizi quali Cisco AI Endpoint Analytics e Application Assurance in Cisco DNA Center. E se non ci fossero dispositivi Catalyst serie 9000 nella rete da cui estrarre la telemetria? Molte organizzazioni dispongono ancora di una parte dell'infrastruttura di rete che non è stata migrata alle piattaforme Cisco Catalyst serie 9000. La piattaforma Catalyst 9000 genera telemetria AppVis, ma per ottenere ulteriori informazioni su AppX, è possibile usare Cisco DNA Traffic Telemetry Appliance per colmare il divario. L'obiettivo del TTA è monitorare il traffico che riceve tramite le porte SPAN da altri dispositivi di rete che non hanno la capacità di fornire dati sull'esperienza dell'applicazione a Cisco DNA Center. Poiché i dispositivi dell'infrastruttura legacy non possono eseguire l'ispezione approfondita dei pacchetti richiesta per l'analisi avanzata, Cisco DNA Traffic Telemetry Appliance può essere utilizzata per generare telemetria AppX da installazioni legacy esistenti.



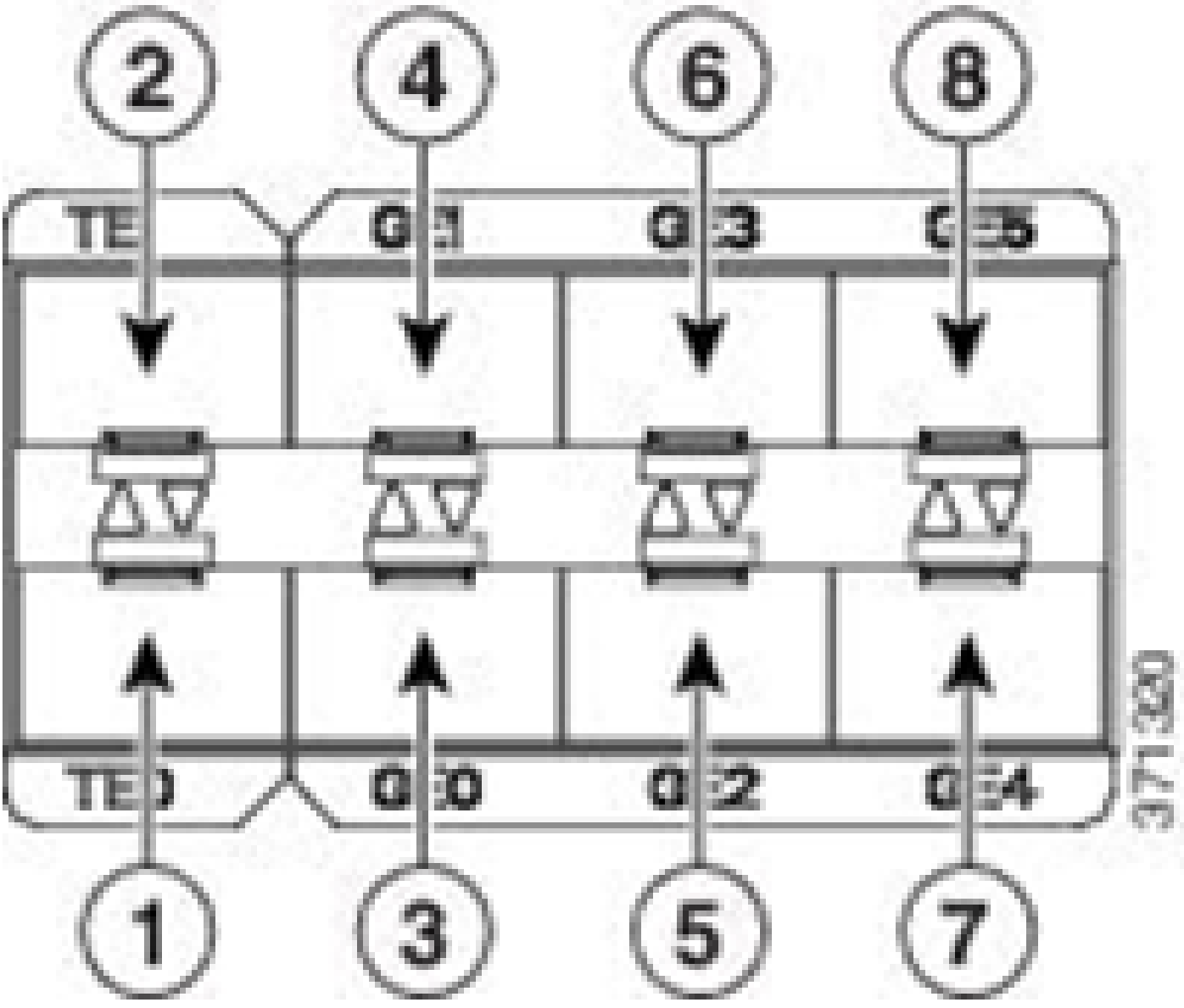
Cisco TTA in azione

Dettagli dispositivo TTA

La piattaforma sensore di telemetria basata su Cisco IOS XE genera telemetria dal traffico di rete IP in mirroring proveniente da sessioni di SPAN (Switched Port Analyzer) di switch e controller wireless. L'appliance controlla migliaia di protocolli utilizzando la tecnologia NBAR (Network-Based Application Recognition) per generare un flusso di telemetria che consente a Cisco DNA Center di eseguire l'analisi. Cisco DNA Traffic Telemetry Appliance è in grado di gestire 20 Gbps di traffico a velocità sostenuta e di ispezionare 40.000 sessioni di endpoint per la profilatura dei dispositivi.

Appliance Cisco Traffic Telemetry

La TTA ha un mix di collegamenti 10-Gig e 1-Gig che sono utilizzati per l'acquisizione SPAN. Di queste porte, Gig0/0/5 è l'unica porta configurabile con un indirizzo IP e può essere utilizzata per comunicare con Cisco DNA Center. La matrice dell'interfaccia è mostrata di seguito.



Matrice interfaccia TTA			
1	10 GE SFP+ porta 0/0/0	5	Porta GE SFP 0/0/2
2	10 GE SFP+ porta 0/0/1	6	Porta GE SFP 0/0/3
3	Porta GE SFP 0/0/0	7	Porta GE SFP 0/0/4
4	Porta GE SFP 0/0/1	8	Porta GE SFP 0/0/5

Cisco DNA Center - Prerequisiti per la garanzia

In questa sezione vengono evidenziati le configurazioni e i prerequisiti da soddisfare prima che Cisco DNA Center possa elaborare la telemetria.

Cluster operativo Cisco DNA Center

È necessario eseguire il provisioning del cluster Cisco DNA Center utilizzato per gestire l'operazione TTA e la telemetria dei processi con i seguenti criteri:

- Gerarchia di rete: La sezione Gerarchia di rete nel flusso di lavoro Progettazione viene utilizzata per definire i diversi campus sito, gli edifici all'interno di tali campus e i singoli piani all'interno di tali edifici e visualizzarli in una mappa del mondo. È necessario configurare la gerarchia del sito o della rete appropriata.
- Impostazioni di rete: la sezione Impostazioni di rete consente di creare impostazioni di rete predefinite comuni che verranno utilizzate dai dispositivi all'interno della rete. Queste impostazioni possono essere applicate in modo globale, nonché a livello di sito, edificio o piano. Immettere le informazioni relative a DNS, nome di dominio, syslog, NTP, fuso orario e banner di accesso in base alle esigenze della distribuzione.
- Credenziali dispositivo: queste credenziali verranno utilizzate per accedere e individuare i dispositivi nella rete, incluso TTA. È necessario configurare Cisco DNA Center con la CLI appropriata e le credenziali SNMP. Insieme a queste credenziali NetConf sono buone da avere.
- Account CCO Cisco: è necessario un account CCO valido per collegare l'appliance e sfruttare le funzionalità di Cisco AI Cloud, scaricare immagini per SWIM e scaricare pacchetti di protocolli per TTA e altri dispositivi.

Integrazione tra ISE e Cisco DNA Center

Cisco Identity Services Engine (ISE) e Cisco DNA Center possono essere integrati per l'automazione delle identità e delle policy. ISE è anche utilizzato per raccogliere informazioni sugli endpoint per sfruttare Cisco AI Endpoint Analytics. PxGrid è usato per implementare l'integrazione tra ISE e Cisco DNA Center.

Di seguito vengono riportati i requisiti di integrazione di Cisco DNA Center e ISE:

- Il servizio pxGrid deve essere abilitato su ISE.
- È necessario abilitare l'accesso in lettura/scrittura a ERS.
- Il certificato di amministrazione ISE deve contenere l'indirizzo IP o il nome di dominio completo (FQDN) di ISE nel campo SAN o nel nome del soggetto.
- Il certificato di sistema Cisco DNA Center deve contenere tutti gli indirizzi IP o gli FQDN di Cisco DNA Center nel nome del soggetto o nel campo SAN.
- Le credenziali ISE ERS Admin verranno utilizzate per stabilire la fiducia nella comunicazione ERS tra ISE e Cisco DNA Center.
- Il nodo pxGrid deve essere raggiungibile da Cisco DNA Center.

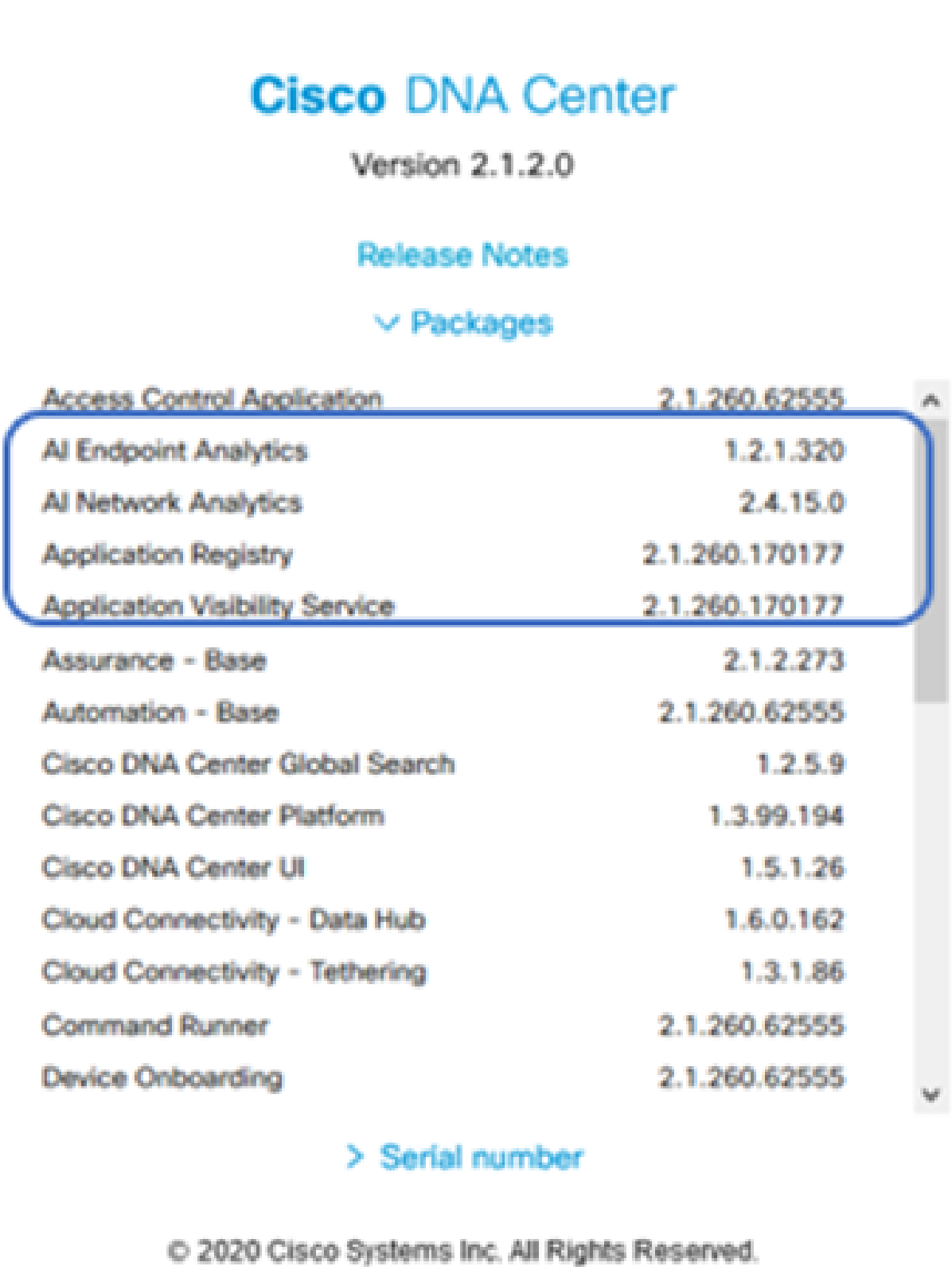
Requisiti di Cisco DNA Center per la telemetria

Per abilitare Application Assurance in Cisco DNA Center è necessario implementare alcuni requisiti. Questi requisiti sono illustrati in dettaglio nelle sezioni seguenti.

Pacchetti chiave Cisco DNA Center

Cisco DNA Center richiede l'installazione di questi tre pacchetti per abilitare e analizzare i dati di telemetria.

- Analisi degli endpoint AI
- Analisi della rete AI
- Servizi di visibilità delle applicazioni



Pacchetti Cisco DNA Center richiesti

Per accedere rapidamente a queste informazioni, fai clic sul link "Informazioni su" sotto l'icona a forma di punto interrogativo nell'angolo in alto a destra della pagina principale di Cisco DNA Center. Se queste applicazioni non sono presenti, è necessario installarle prima di procedere con l'installazione della telemetria. Utilizzare questa guida per installare questi pacchetti in Cisco DNA

Center dal cloud Cisco. [Guida all'aggiornamento di Cisco DNA Center]

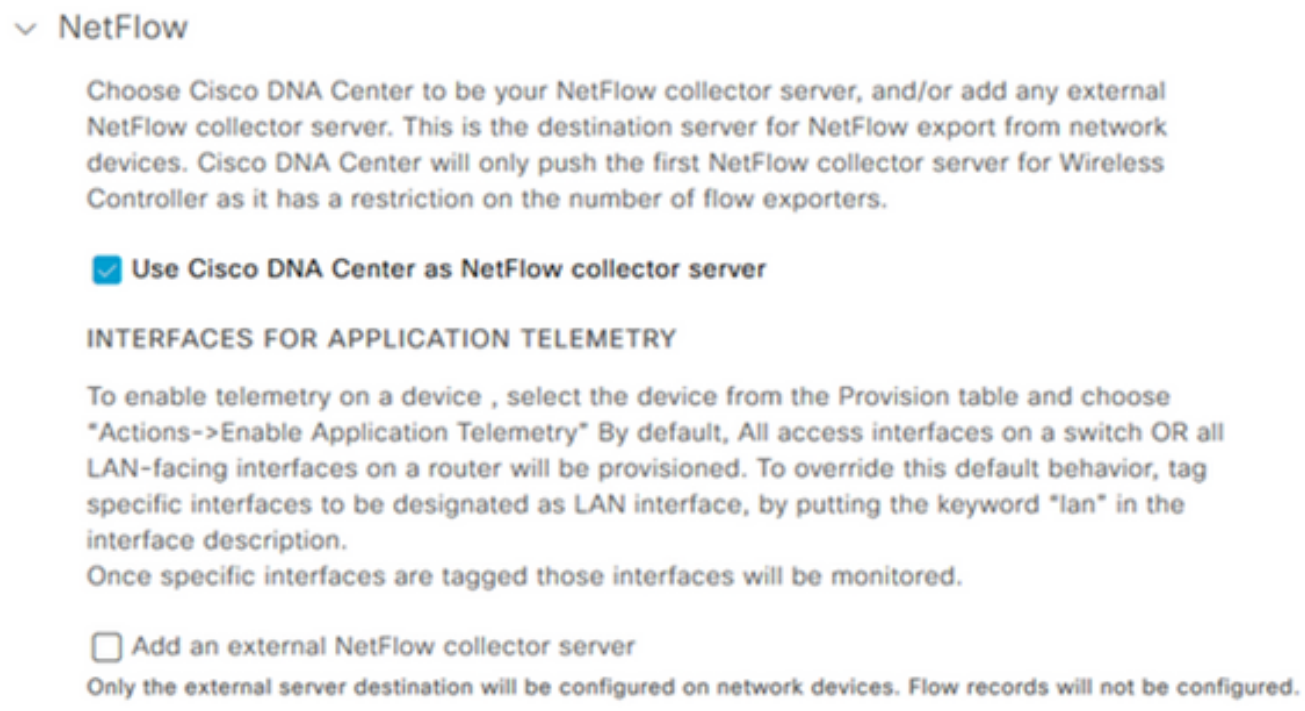
Cisco DNA Center come Telemetry Collector

L'esportazione dei dati NetFlow è il trasporto tecnologico che fornisce i dati di telemetria che verranno inoltrati al Cisco DNA Center per un'analisi approfondita. Per abilitare la raccolta dei dati per l'apprendimento automatico e il ragionamento per l'analisi degli endpoint, NetFlow deve essere esportato in Cisco DNA Center. La TTA è una piattaforma sensore di telemetria utilizzata per generare telemetria dal traffico di rete IP in mirroring e condividerla con Cisco DNA Center per la visibilità di applicazioni ed endpoint.

- Il traffico di rete viene ricevuto da switch e router tramite mirroring SPAN (Switched Port Analyzer) e inviato alle interfacce di mirroring di Cisco DNA Traffic Telemetry Appliance.
- Cisco DNA Traffic Telemetry Appliance analizza il traffico ricevuto per produrre un flusso di telemetria per Cisco DNA Center.

Per abilitare Cisco DNA Center come collettore di telemetria, attenersi alla seguente procedura.

- In Cisco DNA Center, fare clic su Menu > Design > Network Settings e abilitare la telemetria per Cisco DNA Center per raccogliere NetFlow.



Configurazione di DNAC come NetFlow Collector

Cisco AI Cloud

Cisco AI Network Analytics è un'applicazione all'interno di Cisco DNA Center che sfrutta la potenza dell'apprendimento automatico e del ragionamento automatico per fornire informazioni accurate specifiche per l'installazione della rete, consentendo di risolvere rapidamente i

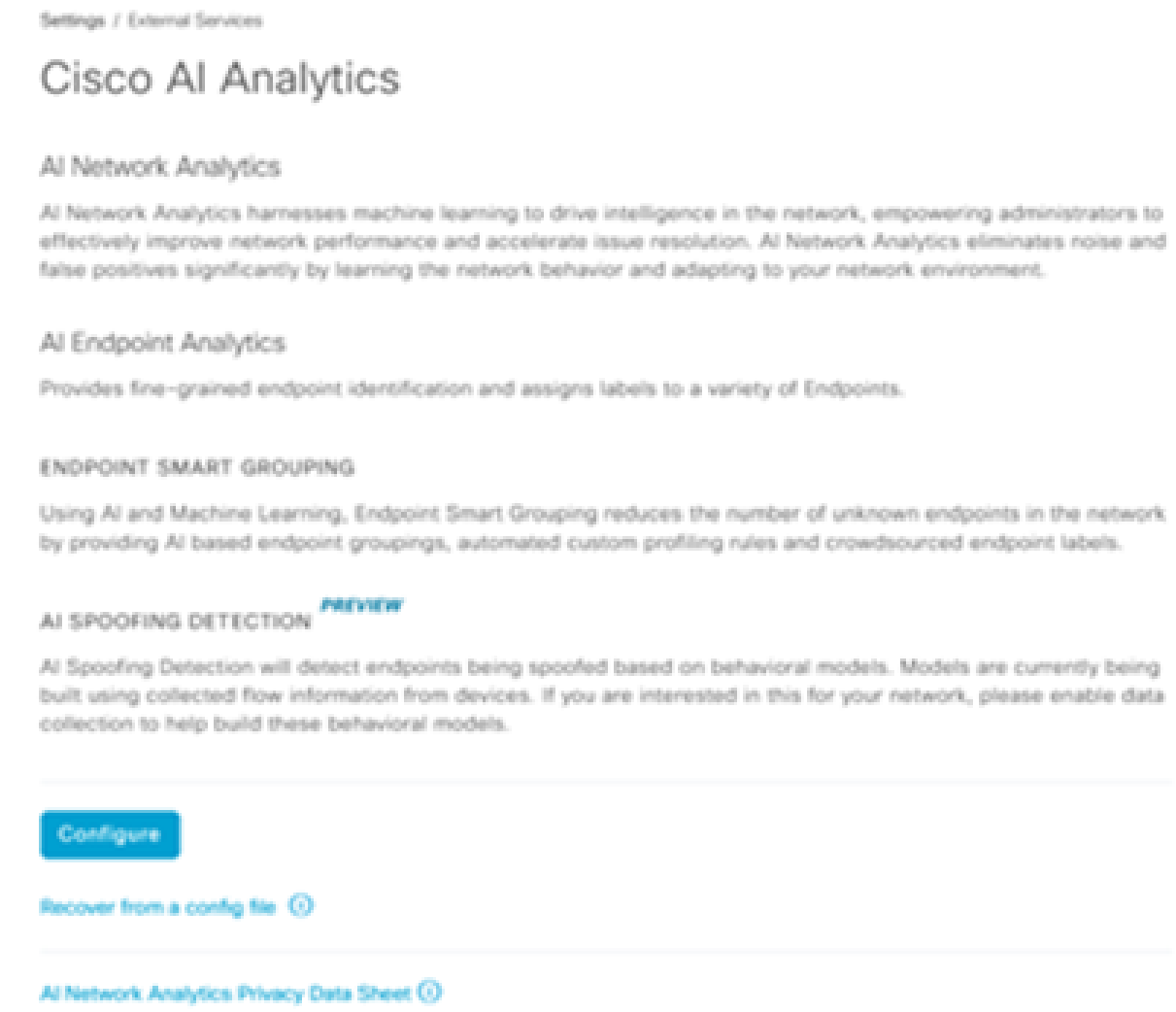
problemi. Le informazioni di rete e telemetria vengono anonimizzate in Cisco DNA Center e quindi inviate tramite un canale crittografato sicuro all'infrastruttura basata su cloud Cisco AI Analytics. Il cloud Cisco AI Analytics esegue il modello di apprendimento automatico con questi dati degli eventi e riporta i problemi e le informazioni generali al Cisco DNA Center. Tutte le connessioni al cloud sono in uscita su TCP/443. Non ci sono connessioni in entrata, il Cisco AI Cloud non avvia alcun flusso TCP verso Cisco DNA Center. I nomi di dominio completi (FQDN) che possono essere utilizzati per consentire l'accesso nel proxy HTTPS e/o nel firewall al momento della scrittura di questo articolo sono:

- https://api.use1.prd.kairos.ciscolabs.com (Stati Uniti orientali)
- https://api.euc1.prd.kairos.ciscolabs.com (regione centrale dell'UE)

L'appliance Cisco DNA Center implementata deve essere in grado di risolvere e raggiungere i vari nomi di dominio su Internet ospitati da Cisco.

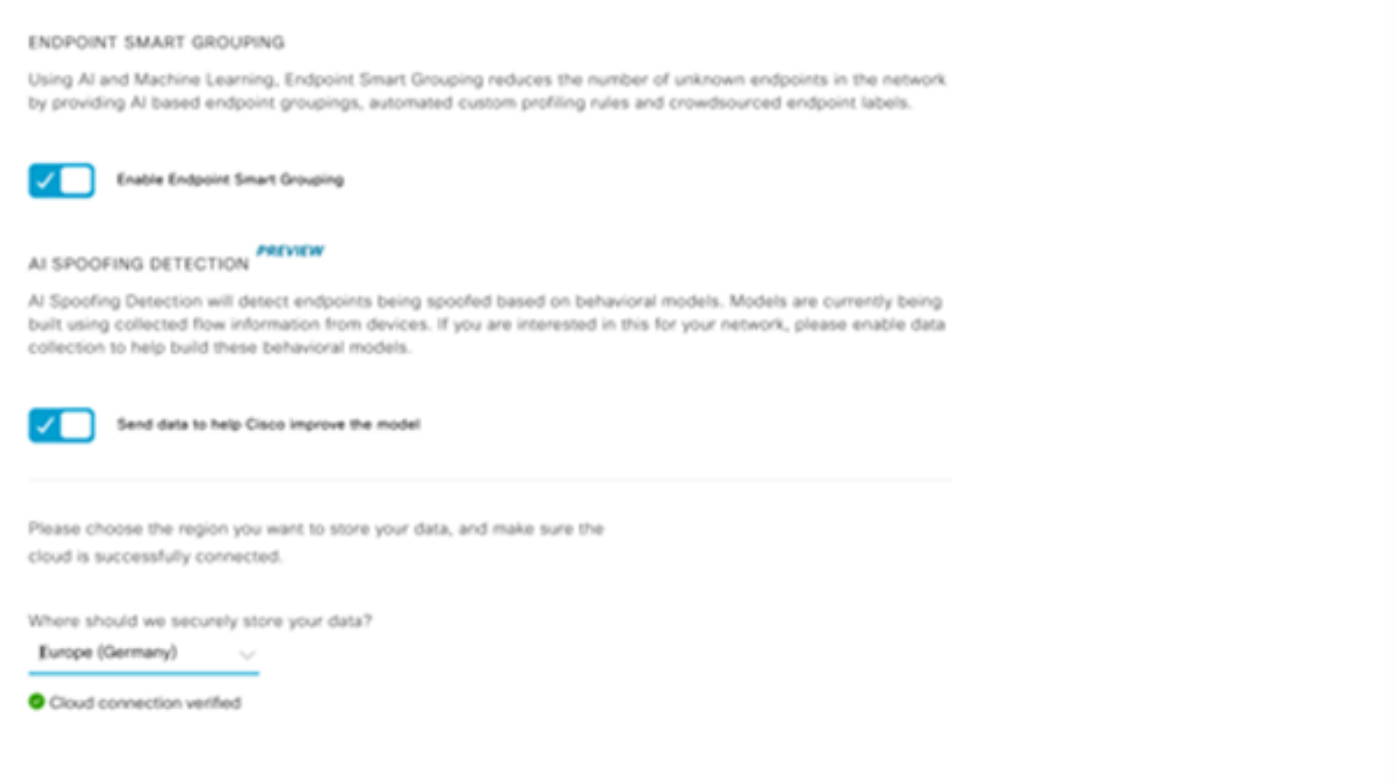
Seguire questi passaggi per collegare Cisco DNA Center al Cisco AI Cloud.

- Per completare la registrazione del cloud AI, andare all'interfaccia Web dell'appliance Cisco DNA Center:
- Passa a Sistema > Impostazioni > Servizi esterni > Cisco AI Analytics
- Fare clic su Configure (Configura) e abilitare l'opzione Endpoint Smart Grouping (Raggruppamento intelligente endpoint) e AI spoof detection (Rilevamento spoof AI).
- Il raggruppamento intelligente degli endpoint utilizza il cloud AI/ML per raggruppare gli endpoint sconosciuti in modo da consentire agli amministratori di etichettare tali endpoint. Ciò è molto utile per ridurre l'incognita della rete.
- Il rilevamento spoof AI consente a Cisco di raccogliere ulteriori informazioni di telemetria/NetFlow e aiuta a modellare l'endpoint.
- Scegliere la posizione più vicina all'area geografica della distribuzione. Una volta completata la verifica della connessione cloud e stabilita la connessione, verrà visualizzata una casella di controllo verde.



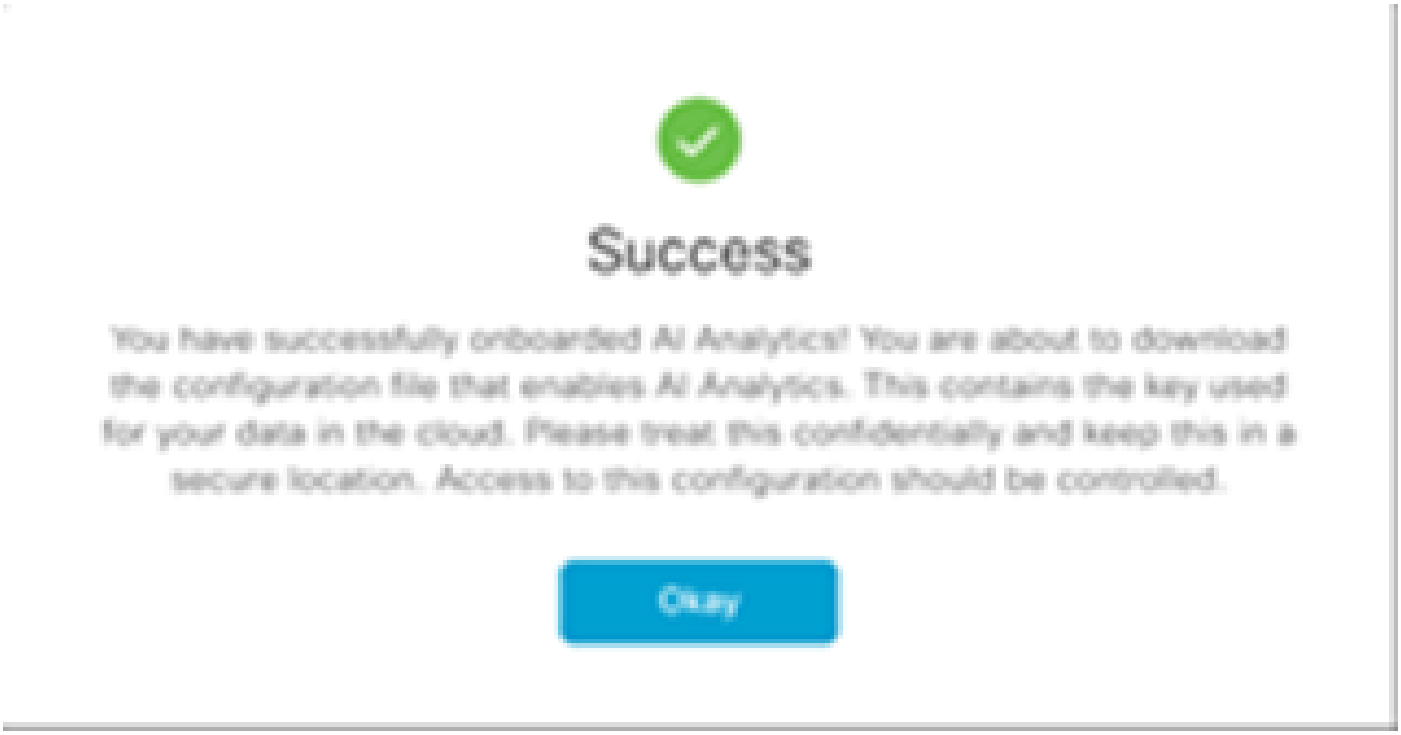
Configurazione dell'interfaccia utente grafica di Cisco AI Analytics

- Se la connessione non riesce, controllare le impostazioni proxy in Cisco DNA Center dalla pagina System > Settings > System Configuration > Proxy config se viene utilizzato un proxy. È inoltre consigliabile controllare le regole del firewall che potrebbero bloccare la comunicazione.



Verifica connessione cloud Cisco AI/ML

- Accettare l'accordo Cisco per il cloud universale per abilitare l'analisi dell'IA.
- A questo punto l'onboarding sarà completato e verrà visualizzata una finestra di dialogo che indica che ciò è come mostrato.



Finestra di dialogo Operazioni riuscite dopo la registrazione

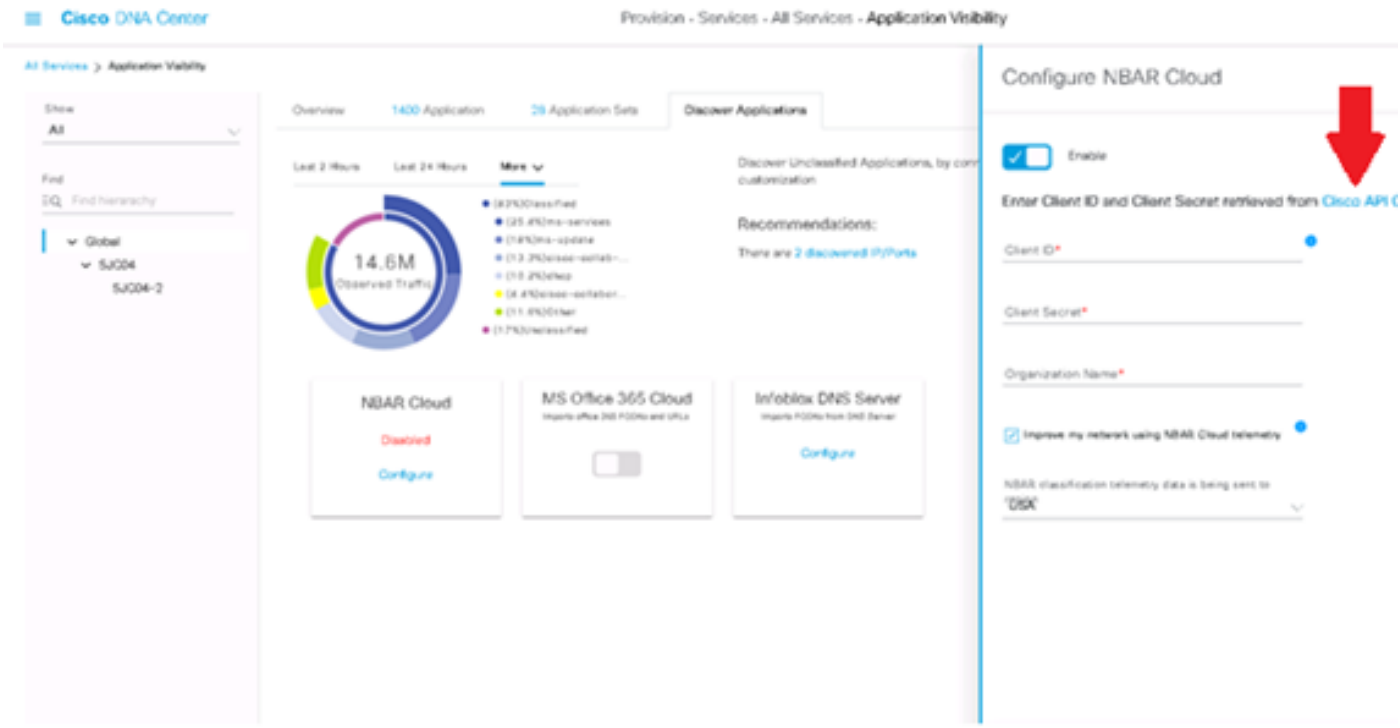
Cloud NBAR (Network Based Application Recognition)

L'appliance di telemetria e la piattaforma Catalyst 9000 raccolgono i metadati dell'endpoint utilizzando l'ispezione approfondita dei pacchetti dei flussi e applicano il riconoscimento delle applicazioni basato sulla rete (NBAR) per determinare i protocolli e le applicazioni utilizzati nella rete. Cisco DNA Center dispone di un pacchetto di protocollo NBAR incorporato che può essere aggiornato. I dati di telemetria possono essere inviati al cloud Cisco NBAR per ulteriori analisi e per rilevare firme di protocollo sconosciute. Affinché ciò avvenga, l'appliance Cisco DNA Center deve essere collegata al cloud. Network-Based Application Recognition (NBAR) è un motore di riconoscimento avanzato delle applicazioni sviluppato da Cisco che utilizza diverse tecniche di classificazione e può aggiornare facilmente le regole di classificazione.

Per collegare Cisco DNA Center al Cisco NBAR Cloud, attenersi alla seguente procedura.

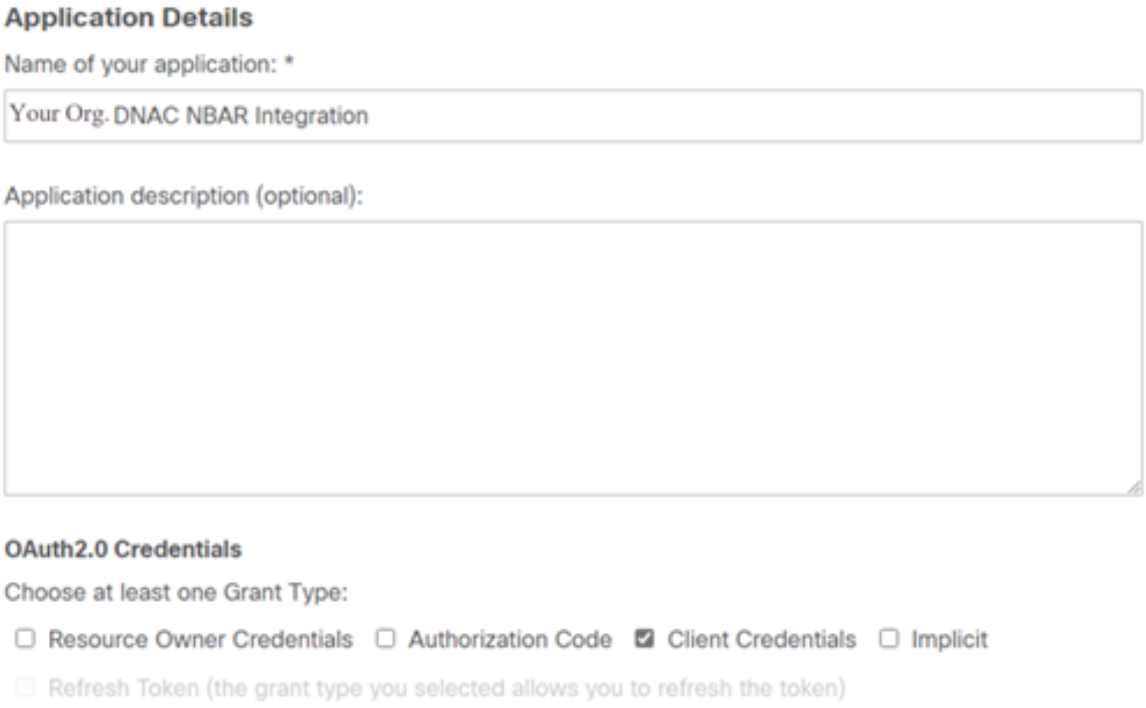
- Dall'interfaccia utente di Cisco DNA Center, selezionare Provisioning > Services > Application Visibility (Servizi > Visibilità applicazioni). Fare clic su Configura in NBAR Cloud per aprire un pannello. Abilitare il servizio.
- Se si dispone di ID client, segreto client e nome organizzazione, assegnare loro nomi univoci a seconda dell'organizzazione e utilizzare.
- Al momento della scrittura l'unica regione di NBAR Cloud attualmente disponibile è negli Stati Uniti; altre regioni potrebbero diventare disponibili in futuro. Selezionare quello nelle preferenze di distribuzione e salvarlo.

Per ottenere le credenziali ID client e segreto client, fare clic sul collegamento "Cisco API Console" per aprire un portale. Effettua l'accesso con l'ID CCO appropriato, crea una nuova app, seleziona le opzioni corrispondenti al cloud NBAR e completa il modulo. Una volta completato, otterrai un ID client e un segreto. Fate riferimento alla figura riportata di seguito.



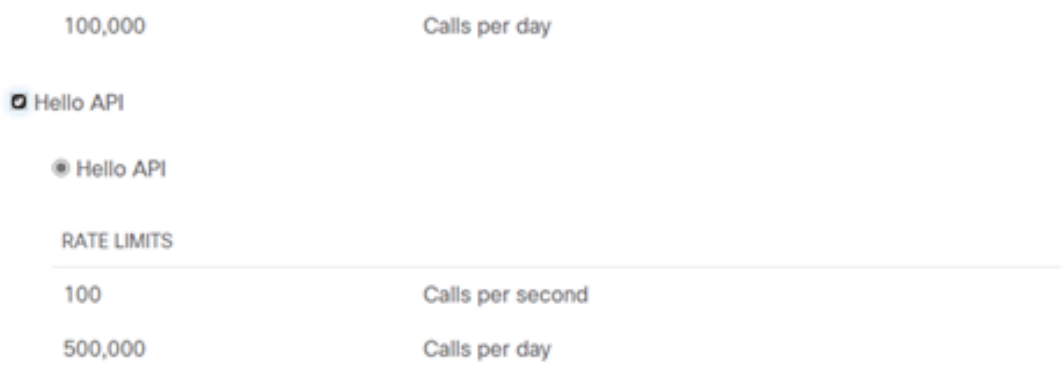
Cisco API Link to Retrieve Client ID and Secret

Queste immagini illustrano le opzioni utilizzate per la registrazione nel cloud NBAR.



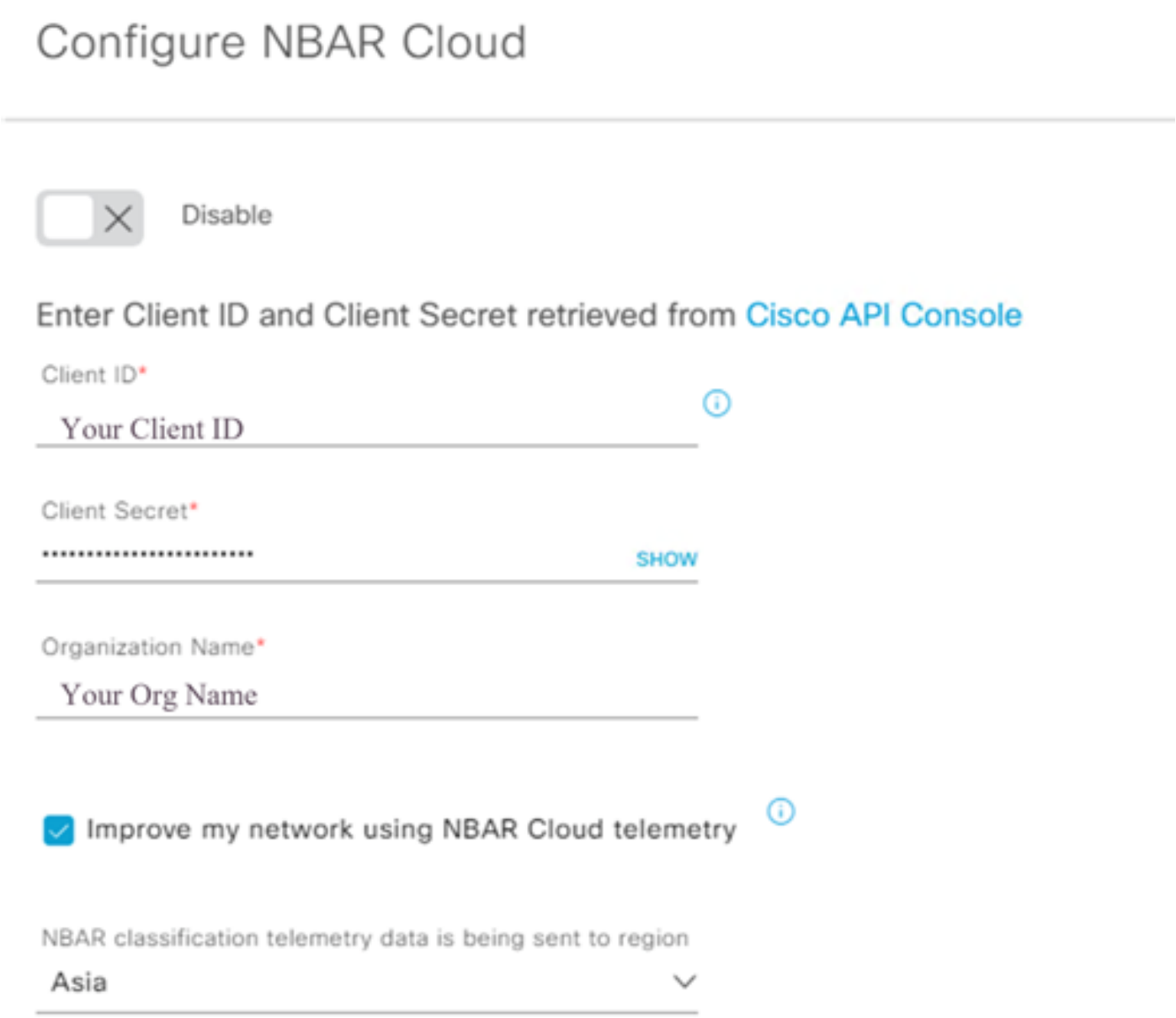
Dettagli app cloud NBAR

- Utilizzare questa immagine come riferimento durante il completamento dei dettagli della richiesta API.



Dettagli API app

- Immettere l'ID client e il segreto ottenuti dal portale Cisco in Cisco DNA Center.



Configurazione di ID e segreto client su DNAC

CBAR (Controller Based Application Recognition) e SD-AVC

La tecnologia CBAR viene utilizzata per classificare migliaia di applicazioni di rete, applicazioni sviluppate internamente e traffico di rete generico. Consente a Cisco DNA Center di ottenere informazioni sulle applicazioni utilizzate dinamicamente nell'infrastruttura di rete. CBAR aiuta a mantenere aggiornata la rete identificando nuove applicazioni man mano che la loro presenza sulla rete continua ad aumentare e consente gli aggiornamenti ai pacchetti di protocollo. Se la visibilità delle applicazioni viene persa da un'applicazione all'altra a causa di pacchetti di protocolli obsoleti, è possibile che si verifichino una classificazione errata e un successivo inoltro. Ciò causerà non solo buchi di visibilità all'interno della rete, ma anche problemi di accodamento o

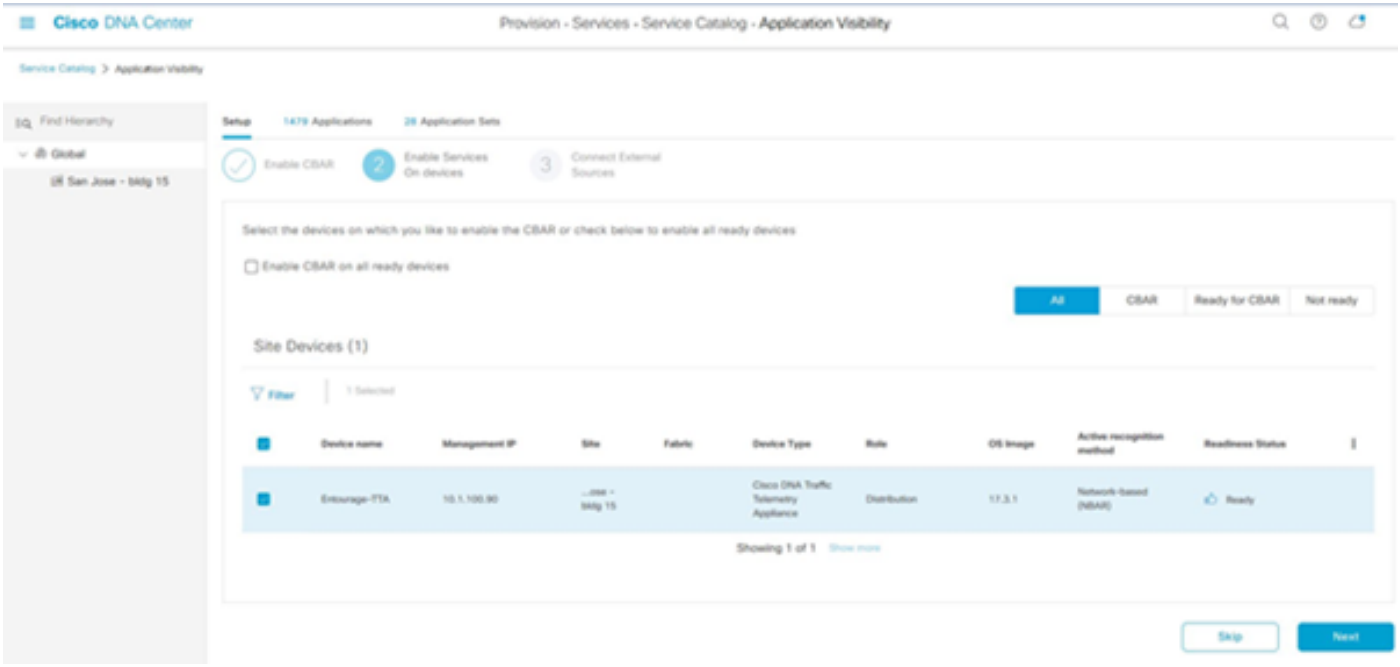
inoltro non corretti. CBAR risolve questo problema consentendo il push dei pacchetti di protocollo aggiornati attraverso la rete.

Il software Cisco AVC (SD-AVC) è un componente di Cisco Application Visibility and Control (AVC). Funge da servizio di rete centralizzato che opera con specifici dispositivi collegati in una rete. Il formato SD-AVC supporta inoltre la visualizzazione di DPI dei dati dell'applicazione. Tra le caratteristiche e i vantaggi offerti da SD-AVC vi sono:

- Riconoscimento coerente delle applicazioni a livello di rete su tutta la rete
- Migliore riconoscimento delle applicazioni in ambienti di routing simmetrici e asimmetrici
- Migliore riconoscimento del primo pacchetto
- Aggiornamento del Protocol Pack a livello di rete
- Dashboard SD-AVC sicuro basato su browser su HTTPS per il monitoraggio delle funzionalità e delle statistiche SD-AVC e per la configurazione degli aggiornamenti del Protocol Pack in tutta la rete

Per attivare CBAR per i dispositivi rilevanti, procedere come segue.

- Andare al menu del Cisco DNA Center, Provisioning > Visibilità delle applicazioni. OSPF (Open Shortest Path First) la prima volta che viene aperta la pagina Visibilità applicazione, all'utente verrà visualizzata una configurazione guidata illustrata di seguito.
- Dopo aver individuato i dispositivi in Cisco DNA Center per ciascun sito, selezionare il dispositivo su cui attivare CBAR e procedere con il passaggio successivo.



Attivazione di CBAR sul dispositivo

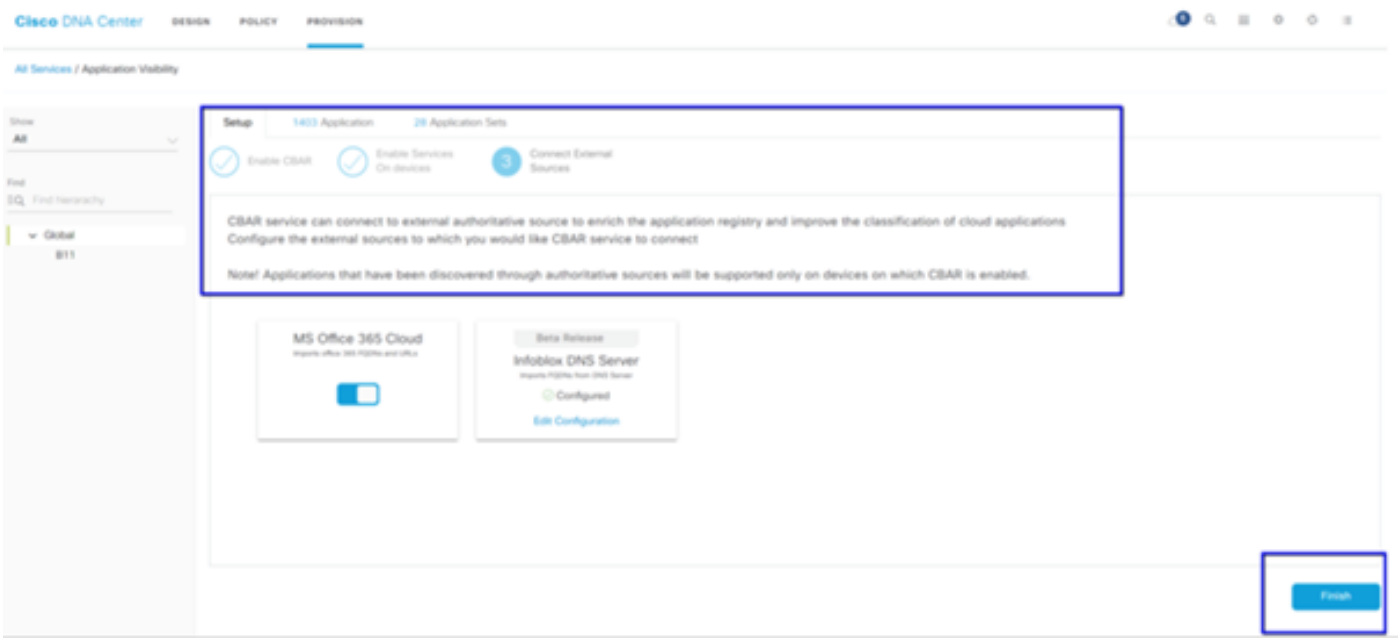
Microsoft Office 365 Cloud Connector (non necessariamente)

Cisco DNA Center può essere integrato direttamente con il feed RSS Microsoft per garantire che il riconoscimento delle applicazioni per Office 365 sia in linea con le linee guida pubblicate. Questa integrazione è nota come Microsoft Office 365 Cloud Connector in Cisco DNA Center. È

consigliabile implementare questa funzionalità se l'utente esegue applicazioni di Microsoft Office 365 nella rete. L'integrazione con Microsoft Office 365 non è un requisito e se non abilitata influirà solo sulla capacità di Cisco DNA Center di elaborare e classificare i dati host di Microsoft Office 365. Cisco DNA Center dispone già del riconoscimento delle applicazioni di Microsoft Office 365 integrato, ma, integrandosi direttamente con il provider di applicazioni, Cisco DNA Center può ottenere informazioni aggiornate e precise sui blocchi di proprietà intellettuale e sugli URL attualmente utilizzati dalla suite Microsoft Office 365.

Per integrare Cisco DNA Center con Microsoft Office 365 Cloud, attenersi alla seguente procedura.

- Fare clic sull'icona Menu e scegliere Provisioning > Servizi > Visibilità applicazione
- Fare clic su Individua applicazioni
- Fare clic sull'interruttore Cloud di MS Office 365 per integrare Cisco DNA Center con Microsoft Office 365 Cloud.

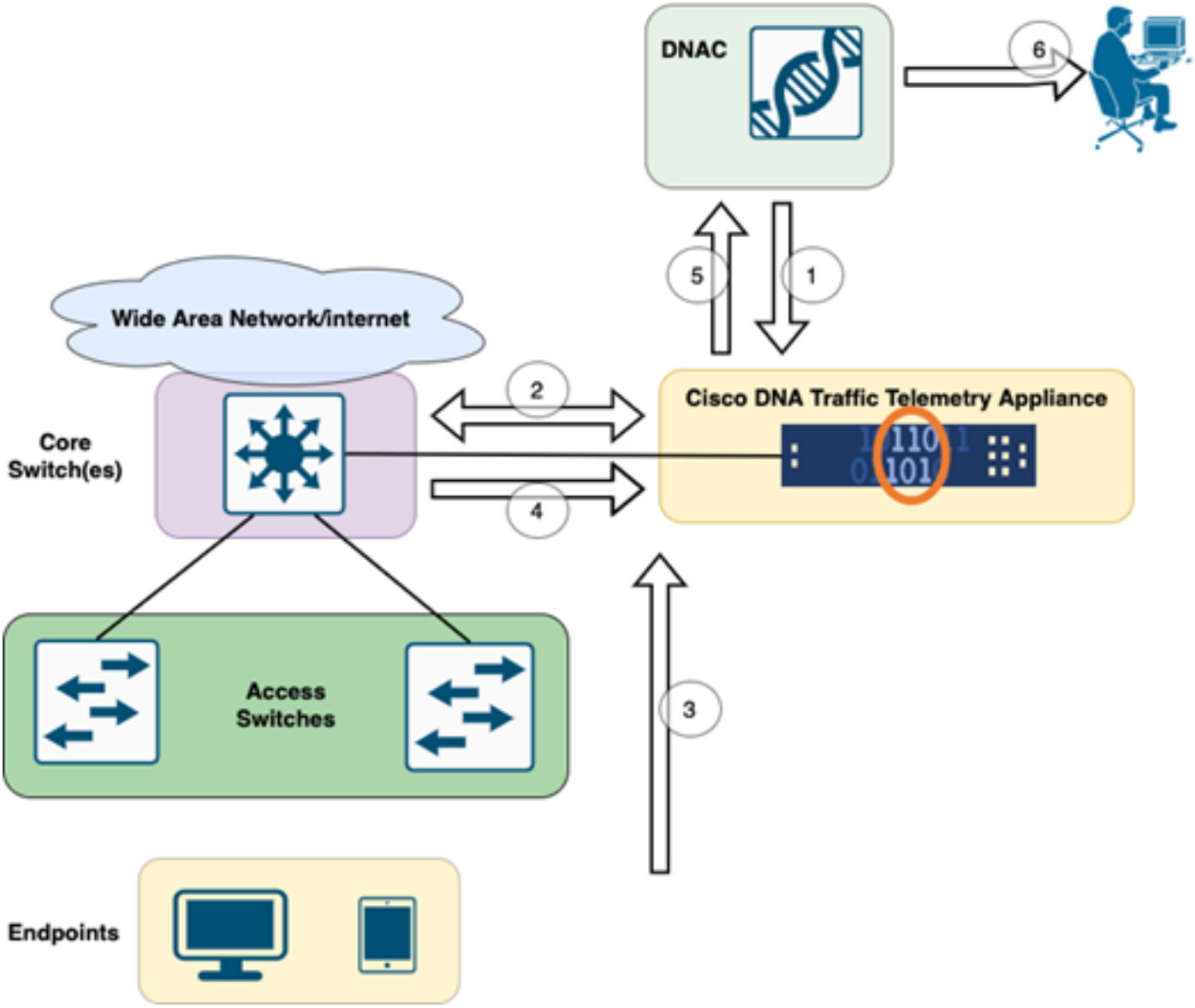


Integrazione cloud MS O365

Implementazione TTA

In questa sezione vengono illustrati i passaggi necessari per implementare l'interfaccia TTA in una rete.

Panoramica sul flusso di lavoro TTA



Flusso di lavoro da TTA a DNAC

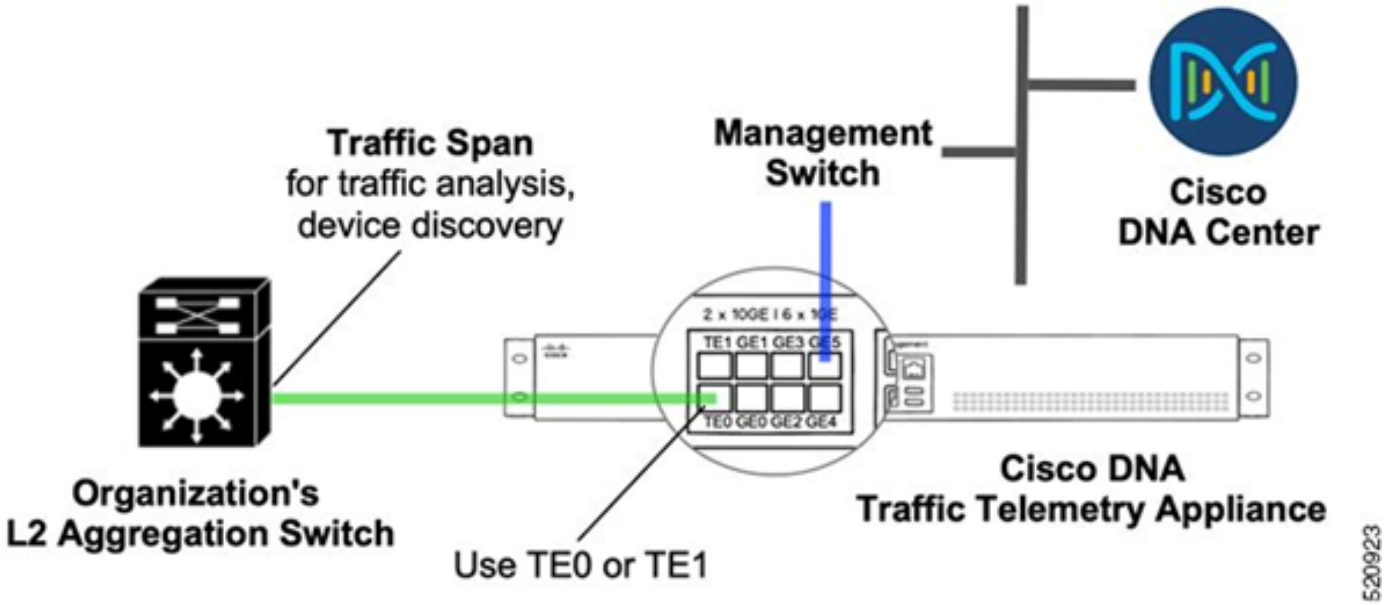
Le fasi evidenziate in questo diagramma delineano il processo e il flusso di telemetria tra TTA e Cisco DNA Center. In questo caso, i passaggi sono illustrati in dettaglio.

1. L'appliance Cisco Traffic Telemetry è collegata allo switch di aggregazione dei siti o allo switch principale all'interno dell'infrastruttura di rete. Questa connessione consente all'accessorio di ricevere i dati relativi al traffico da vari switch di accesso nella rete.
2. L'appliance Cisco Traffic Telemetry è integrata con Cisco DNA Center, che funge da piattaforma di gestione della rete. Questa integrazione consente una comunicazione e uno scambio di dati senza interruzioni tra l'accessorio e Cisco DNA Center.
3. Quando il traffico degli utenti attraversa la rete, viene eseguito lo spanning o il mirroring su Cisco Traffic Telemetry Appliance. Il traffico di rete viene quindi inviato all'accessorio per il monitoraggio e l'analisi, mentre il traffico originale continua il suo normale percorso.
4. L'appliance Cisco Traffic Telemetry raccoglie ed elabora i dati sul traffico ricevuti. Estrae le informazioni rilevanti, ad esempio i dettagli a livello di pacchetto, le statistiche di flusso e le metriche delle prestazioni, dal traffico con mirroring.
5. Le informazioni di telemetria elaborate vengono quindi inviate dal dispositivo di telemetria del traffico Cisco al Cisco DNA Center. Questa comunicazione consente a Cisco DNA Center di

ricevere informazioni e aggiornamenti in tempo reale sui modelli di traffico, le prestazioni delle applicazioni e le anomalie della rete.

6. Le informazioni di telemetria generate da Cisco DNA Center forniscono informazioni preziose agli amministratori di rete. Possono utilizzare l'interfaccia di Cisco DNA Center per visualizzare e analizzare i dati raccolti, ottenere visibilità sullo stato della rete e sulle prestazioni delle applicazioni, identificare potenziali problemi e prendere decisioni informate per l'ottimizzazione e la risoluzione dei problemi di rete.

Distribuzione TTA: diagramma ad alto livello



Distribuzione TTA: livello alto

Il diagramma precedente mostra come è possibile connettere TTA nella rete. Le interfacce 10-Gig e 1-Gig possono essere utilizzate per l'acquisizione SPAN a velocità di linea. L'interfaccia Gi0/0/5 viene usata per la comunicazione con Cisco DNA Center, per l'orchestrazione e per l'inoltro di informazioni di telemetria a Cisco DNA Center; questa interfaccia NON PUÒ essere usata per l'acquisizione di SPAN.

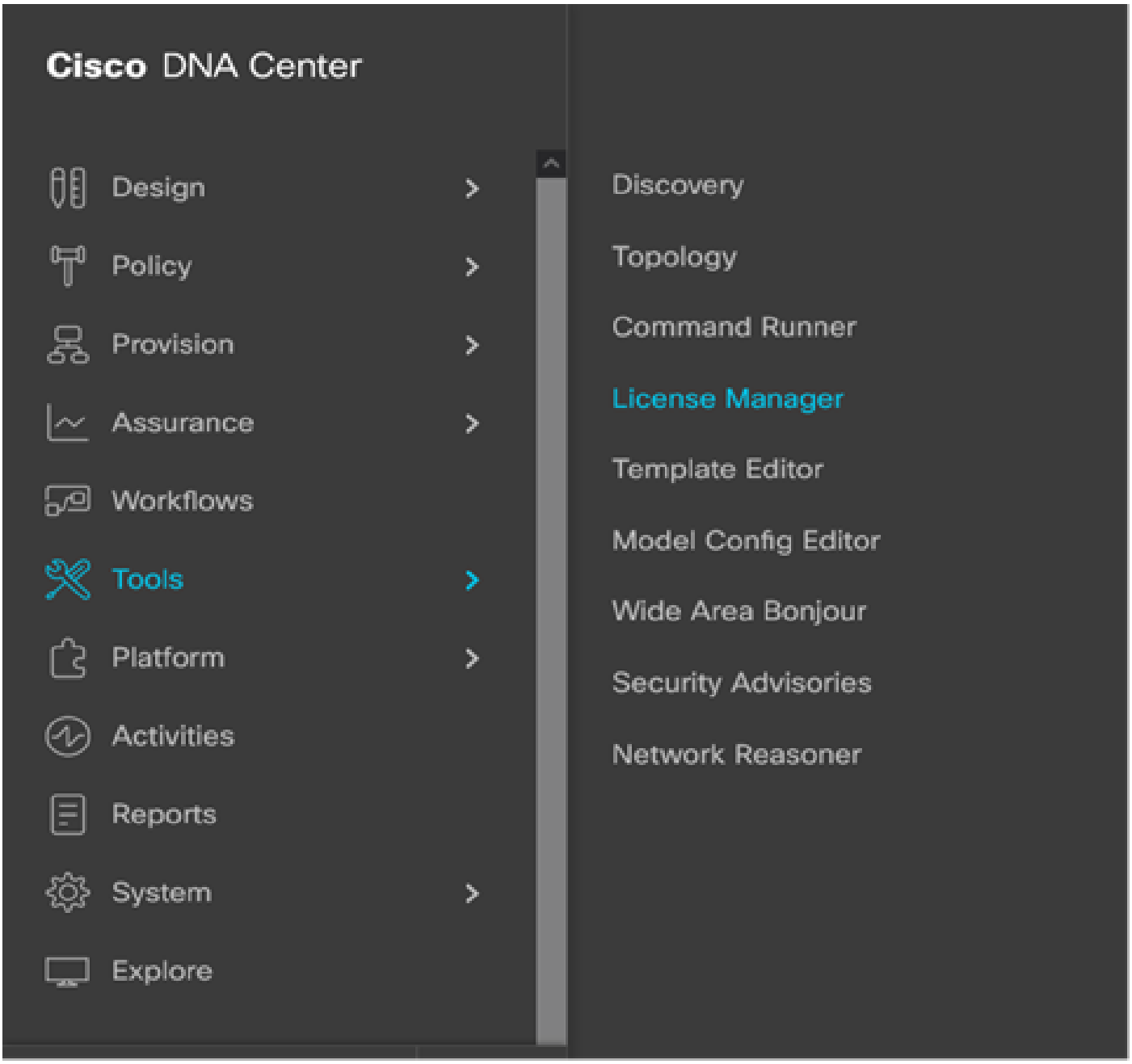
Requisiti di licenza e software TTA

Le appliance TTA installate nella rete saranno fondamentali per fornire informazioni di telemetria sui dati utente e sugli endpoint utente. Per distribuire correttamente la soluzione, è necessario soddisfare questi requisiti.

- Il TTA deve essere configurato con una configurazione iniziale di bootstrap in modo che possa essere individuato da Cisco DNA Center (configurazione bootstrap TTA)
- L'appliance TTA deve essere integrata in Cisco DNA Center in modo da poter essere gestita da Cisco DNA Center (aggiunta di un dispositivo di telemetria all'inventario di Cisco DNA Center)
- È necessario installare la licenza corretta sulla licenza dell'appliance TTA (TTA)

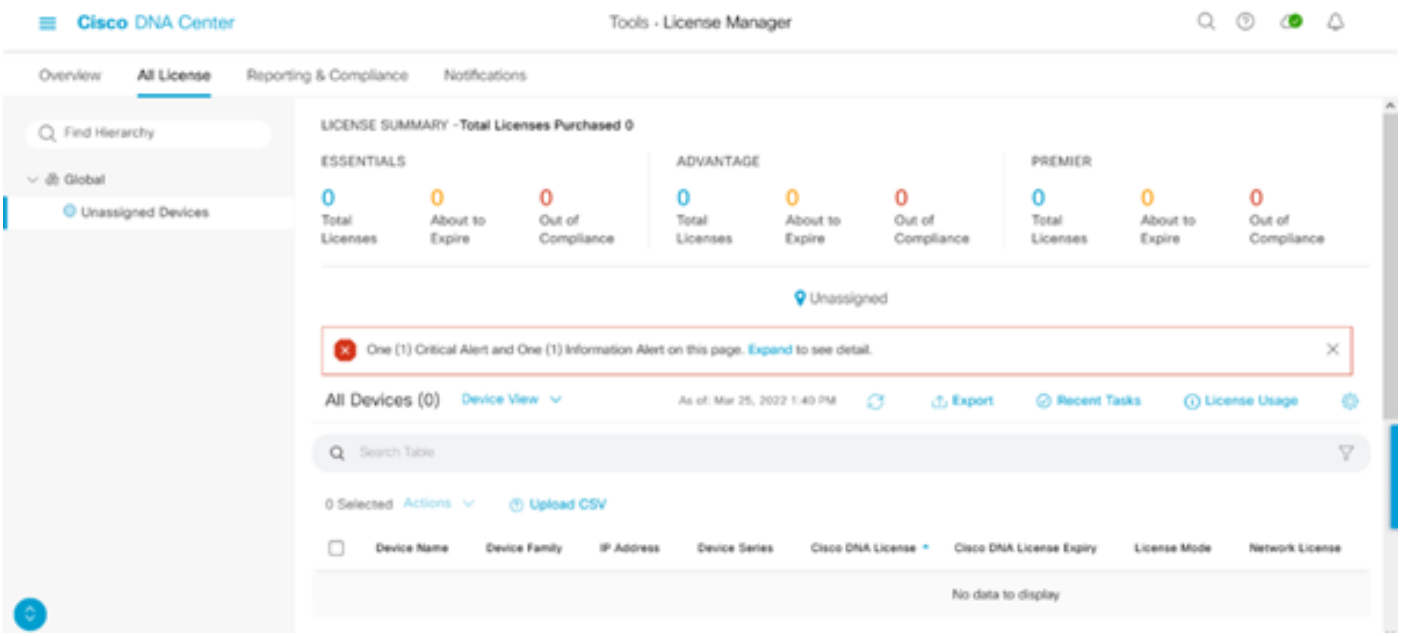
L'accessorio supporta un solo sistema operativo e richiede la Cisco DNA TTA Advantage License per raccogliere dati di telemetria. Non è necessaria una licenza per le funzionalità (ad esempio IP Base o Servizi IP avanzati) o un pacchetto di licenze perpetuo (ad esempio Network Essentials o Network Advantage).

Per gestire le licenze in Cisco DNA Center, passare a Gestione licenze selezionando Strumenti > Gestione licenze dal menu a discesa di Cisco DNA Center facendo clic sull'icona Menu



License Manager su DNAC

- Passare alla pagina Tutte le licenze ; l'aspetto sarà simile a quello dell'immagine. In questa pagina l'amministratore può gestire le licenze dei dispositivi di rete come quelle del TTA.



Pagina Tutte le licenze su DNAC

Onboarding TTA e configurazione del giorno 0

Per facilitare il rilevamento e l'onboarding dell'appliance TTA da parte di Cisco DNA Center, è necessario configurare i comandi bootstrap sugli appliance TTA del sito. Con la configurazione bootstrap in uso, l'interfaccia TTA sarà rilevabile dal dashboard di Cisco DNA Center. Di seguito sono riportati gli elementi di configurazione del giorno 0 per un accessorio TTA. Una volta installato il dispositivo nella gerarchia dei siti, l'appliance TTA erediterà gli elementi di configurazione rimanenti da Cisco DNA Center.

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

ip route 0.0.0.0 0.0.0.0 x.x.x.y
username dna privilege 15 algorithm-type scrypt secret
```

```
enable secret
```

```
service password-encryption
ip domain name <domain name>
ip ssh version 2
line vty 0 15
login local
transport input ssh
transport preferred none
```

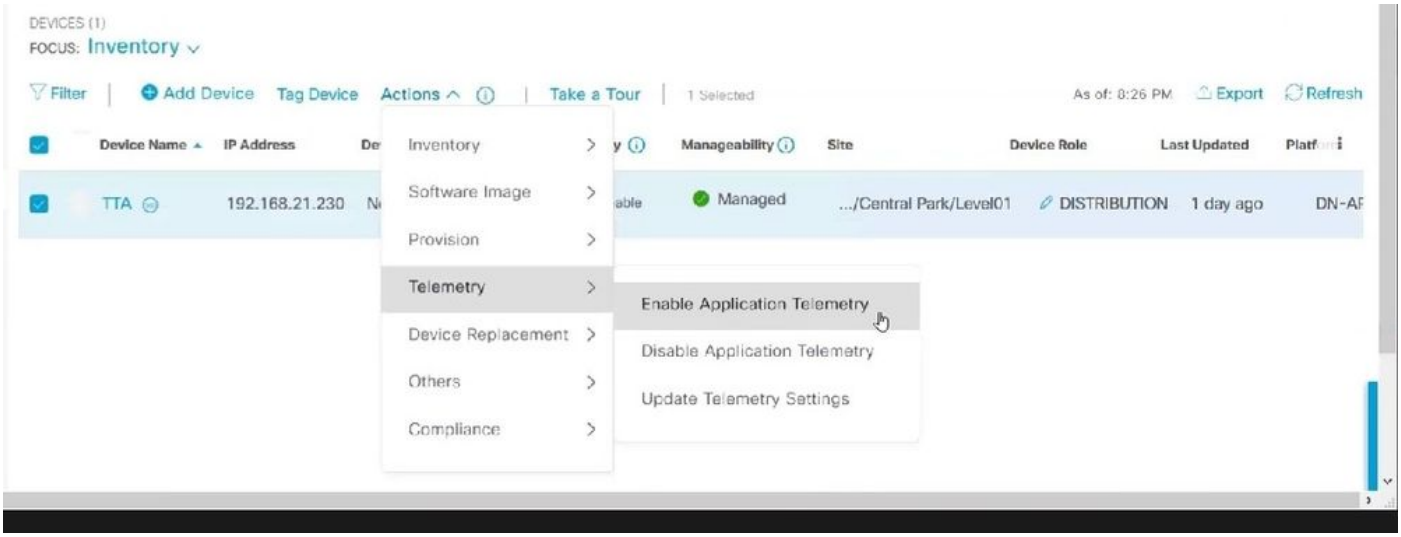
```
ip ssh source-interface GigabitEthernet0/0/5

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

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

Una volta configurati questi elementi sul TTA, possono essere rilevati da Cisco DNA Center.

Aggiunta dell'appliance TTA all'inventario di Cisco DNA Center

Per sfruttare il TTA, Cisco DNA Center deve individuare e gestire l'appliance TTA. Una volta incorporato nel Cisco DNA Center, il TTA può essere gestito da Cisco DNA Center. Prima di individuare l'appliance TTA, è necessario verificare che la gerarchia dei siti sia completa per il sito. Successivamente, si procederà all'aggiunta dell'accessorio TTA nella gerarchia di siti specifica seguendo questi passaggi dalla pagina Menu > Provisioning > Dispositivi > Inventario per aggiungere il dispositivo a un sito.

1. Fornire il nome utente/password (CLI) e la community SNMP necessari per connettersi al dispositivo e la password di abilitazione. Attendere il completamento dell'aggiunta del dispositivo prima di continuare.
2. Verificare il nome del dispositivo, la famiglia (gestione di rete in caso di TTA), la raggiungibilità - raggiungibile, gestibile, il ruolo del dispositivo - distribuzione. Inizialmente il dispositivo sarà "Non conforme", ma una volta eseguito il provisioning completo lo stato cambia.
3. Una volta che la TTA è stata integrata, Cisco DNA Center spingerà i modelli di configurazione per configurarla con funzioni di telemetria avanzate.



TTA Discovery e abilitazione della telemetria delle applicazioni

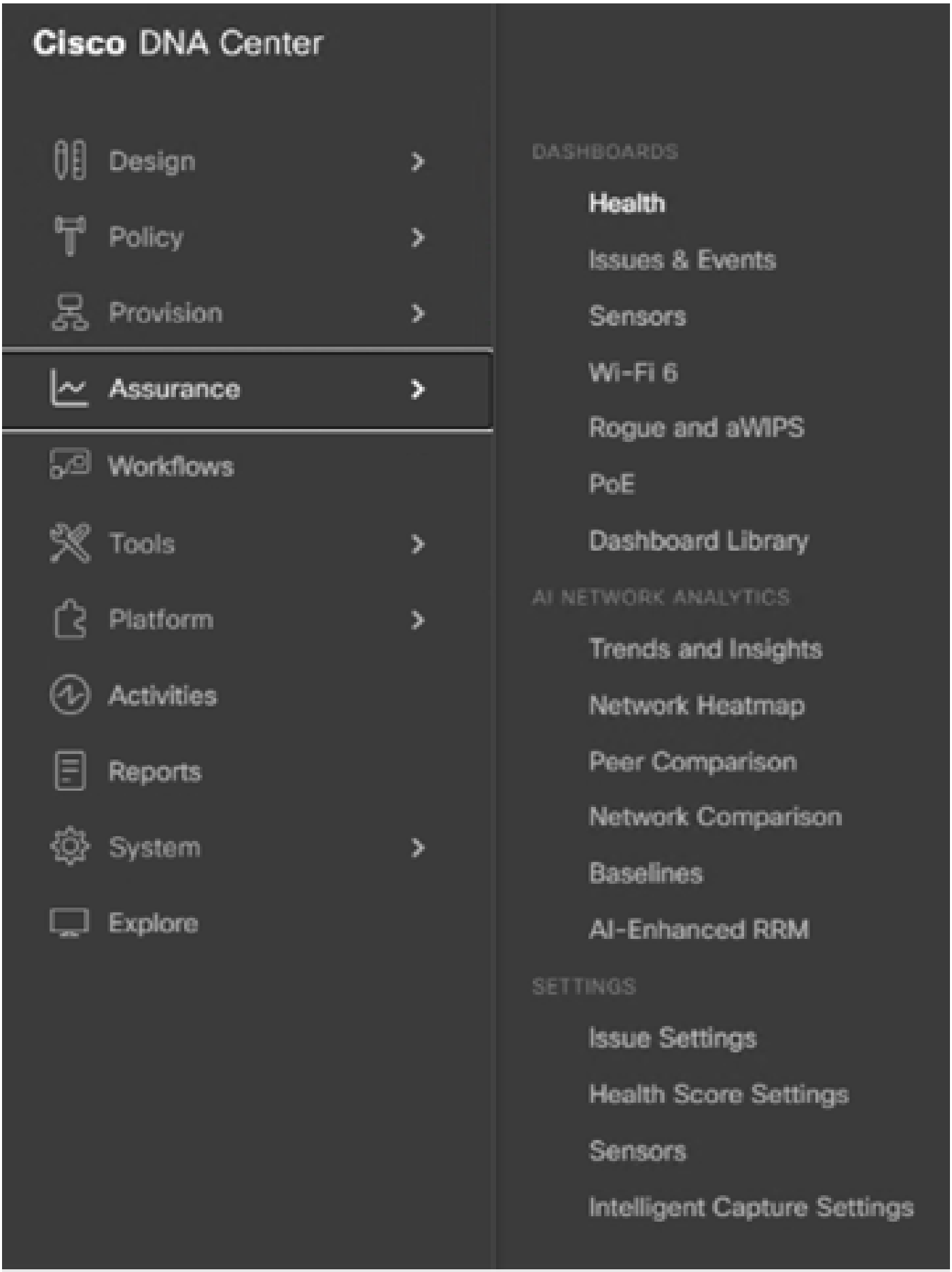
configurazione SPAN

A seconda delle funzionalità hardware dello switch core, la sessione SPAN può essere configurata in modo da SPAN di un gruppo di VLAN o interfacce sull'interfaccia collegata al TTA. Di seguito è riportato un esempio di configurazione.

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

Garanzia raccolta

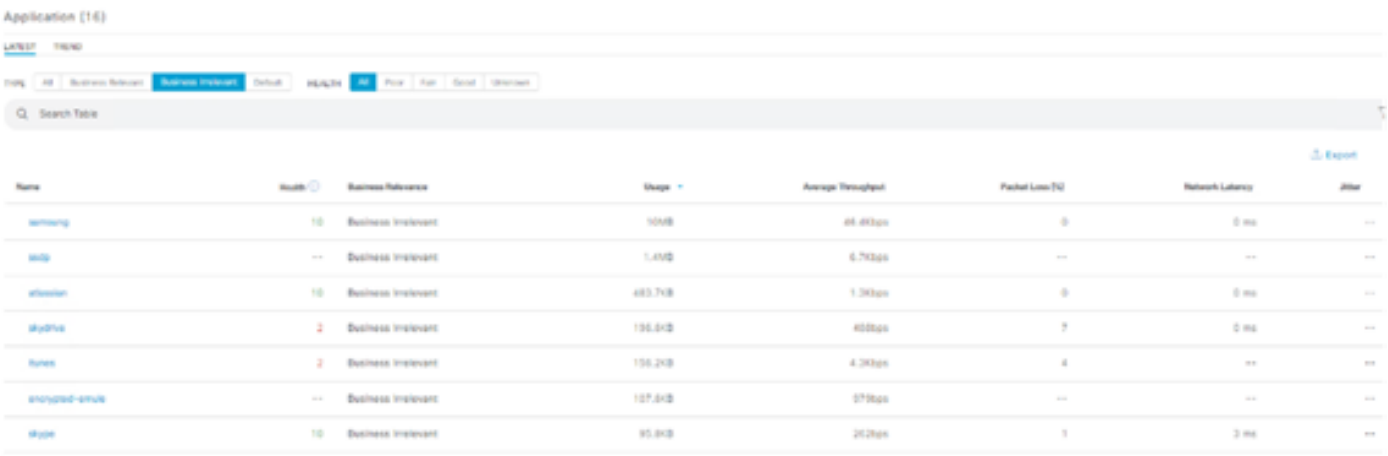
Per accedere ai dati Assurance raccolti dall'accessorio di telemetria del traffico installato, andare alla sezione Assurance e fare clic su Integrità.



Passaggio a App Assurance

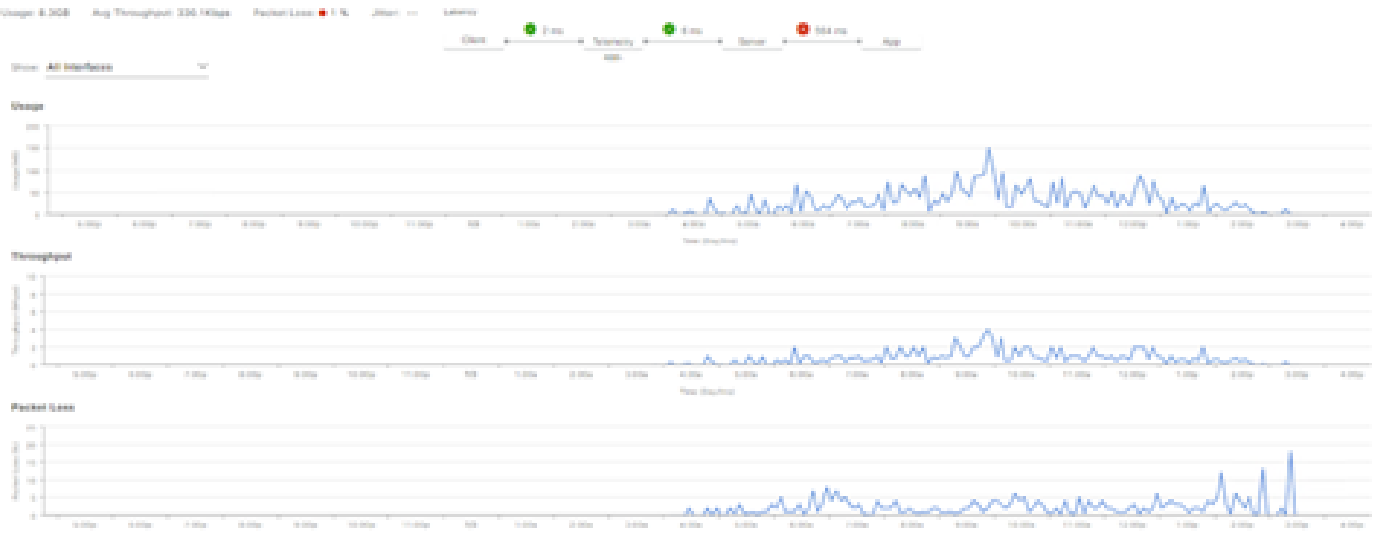
Scegliere Applicazioni per ottenere una panoramica completa dei dati dell'applicazione, inclusi latenza e jitter acquisiti dall'agente di trasferimento dati in base al tipo di applicazione specifico.

Passaggio ad Application Assurance



Interfaccia utente Application Assurance dettagliata

Per un'analisi più dettagliata, gli utenti possono esplorare singole applicazioni facendo clic sull'applicazione specifica e selezionando l'utilità di esportazione come appliance di telemetria del traffico ed esaminare metriche specifiche quali l'utilizzo, il throughput e i dati di perdita di pacchetti, la latenza della rete client, la latenza della rete del server e la latenza del server applicazioni.



Esempio: Dettagli Dell'Applicazione Pt.1

Esempio: Dettagli Dell'Applicazione Pt.2

Verifica

1. Dopo aver abilitato CBAR, verificare che il servizio SD-AVC (Application Visibility Control) sia abilitato sul dispositivo accedendo a Cisco Traffic Telemetry Appliance ed eseguendo questo comando CLI. L'output sarà simile a questo esempio e indicherà l'indirizzo IP del controller e lo stato connesso.

```
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. Usare il comando "show license summary" sulla CLI del TTA per controllare i dettagli della licenza del dispositivo.

```
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. Verificare che la sessione SPAN sia stata configurata correttamente sul commutatore core/aggregazione.

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

4. Una volta completato il provisioning della TTA, questi comandi verranno (o sono stati) trasferiti al dispositivo.

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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).