Utilize o Traffic Telemetry Appliance (TTA) e o Cisco DNA Center App Assurance: o porquê e como

Contents

Introdução

Este documento descreve a plataforma do Cisco DNA Traffic Telemetry Appliance (número de peça da Cisco DN-APL-TTA-M) juntamente com como ativar a Garantia de Aplicativo no Cisco DNA Center. IEle também fornece alguma luz sobre como e onde o TTA pode ser posicionado em uma rede juntamente com o processo de configuração e verificação. Este artigo também aborda os vários pré-requisitos envolvidos.

Pré-requisitos

A Cisco recomenda que você tenha conhecimento de como o Cisco DNA Center Assurance and Application Experience funciona.

Garantia de aplicativos

A garantia é um mecanismo de coleta e análise de dados de rede multiuso e em tempo real que pode aumentar significativamente o potencial comercial dos dados de rede. O Assurance processa dados de aplicativos complexos e apresenta os resultados nos painéis de integridade do Assurance para fornecer insight sobre o desempenho dos aplicativos usados na rede. Dependendo de onde os dados são coletados, você poderá ver algumas ou todas as seguintes opções:

- Nome do aplicativo
- Transferência
- Marcações DSCP
- Métricas de desempenho (latência, instabilidade e perda de pacotes)

Com base na quantidade de dados coletados, o Application Assurance pode ser categorizado em dois modelos:

- Visibilidade de aplicativos (AppVis) e
- Experiência de aplicativo (AppX)

Application Name e Throughput são coletivamente chamados de métricas quantitativas. Os dados para as métricas quantitativas vêm da ativação da visibilidade de aplicativos.

As marcações de DSCP e as métricas de desempenho (latência, instabilidade e perda de pacotes) são coletivamente chamadas de métricas qualitativas. Os dados para as métricas qualitativas vêm da habilitação do Application Experience.

Visibilidade do aplicativo (AppVis)

Os dados de visibilidade do aplicativo são coletados de switches que executam o Cisco IOS® XE e de controladores sem fio que executam o AireOS. Para switches que executam o Cisco IOS XE, os dados de visibilidade de aplicativos são coletados usando um modelo NBAR predefinido que é aplicado bidirecionalmente (entrada e saída) às portas do switch de acesso da camada física. Para controladores sem fio que executam o AireOS, os dados de visibilidade de aplicativos são coletados no controlador sem fio e, em seguida, a telemetria de transmissão é usada para transportar esses dados para o Cisco DNA Center.

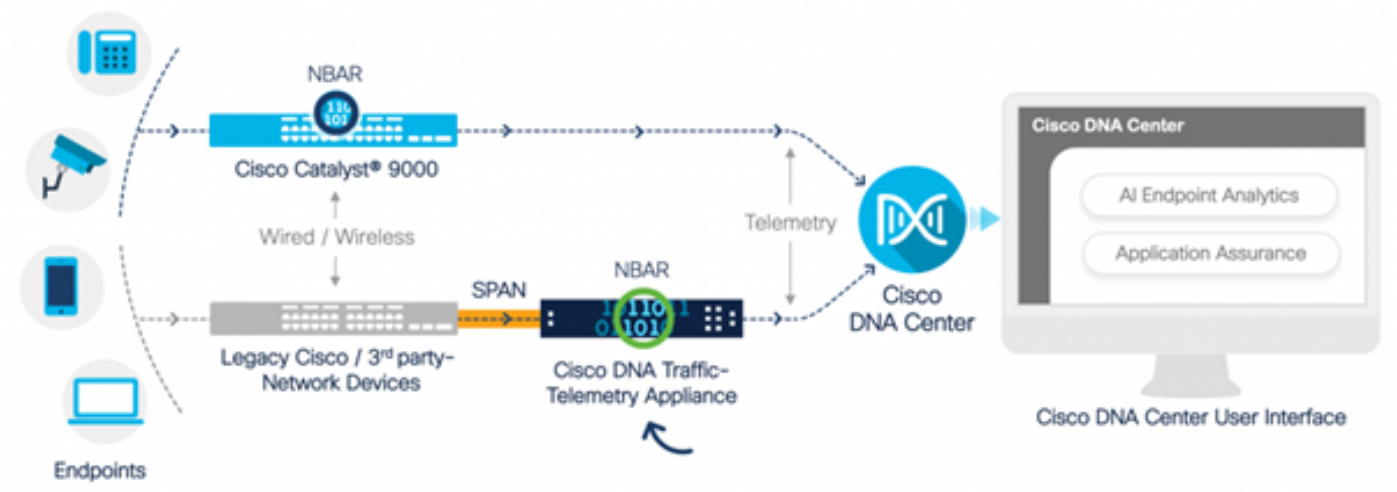
Experiência de aplicativo (AppX)

Os dados do Application Experience são coletados das plataformas do roteador Cisco IOS XE, usando especificamente o recurso Cisco Performance Monitor (PerfMon) e as métricas do Cisco

Application Response Time (ART). Exemplos de plataformas de roteador incluem o ASR 1000, o ISR 4000 e o CSR 1000v. Para obter informações sobre compatibilidade de dispositivos com o Cisco DNA Center, consulte a Matriz de compatibilidade do Cisco DNA Center.

Por que um dispositivo de telemetria de tráfego?

Os dispositivos com e sem fio Cisco Catalyst 9000 Series conduzem inspeção profunda de pacotes (DPI) e fornecem fluxos de dados para serviços como o Cisco AI Endpoint Analytics e o Application Assurance no Cisco DNA Center. Mas e se não houver dispositivos da série Catalyst 9000 na rede para extrair a telemetria? Várias organizações ainda têm uma parte de sua infraestrutura de rede que não foi migrada para as plataformas da série Cisco Catalyst 9000. A plataforma Catalyst 9000 gera a telemetria AppVis, mas para obter insights AppX adicionais, o Cisco DNA Traffic Telemetry Appliance pode ser usado para preencher a lacuna. O objetivo do TTA é monitorar o tráfego que ele recebe através de portas SPAN de outros dispositivos de rede que não têm a capacidade de fornecer dados do Application Experience ao Cisco DNA Center. Como os dispositivos de infraestrutura herdados não podem executar a inspeção profunda de pacotes necessária para análise avançada, o Cisco DNA Traffic Telemetry Appliance pode ser usado para gerar a telemetria AppX a partir de implantações herdadas existentes.



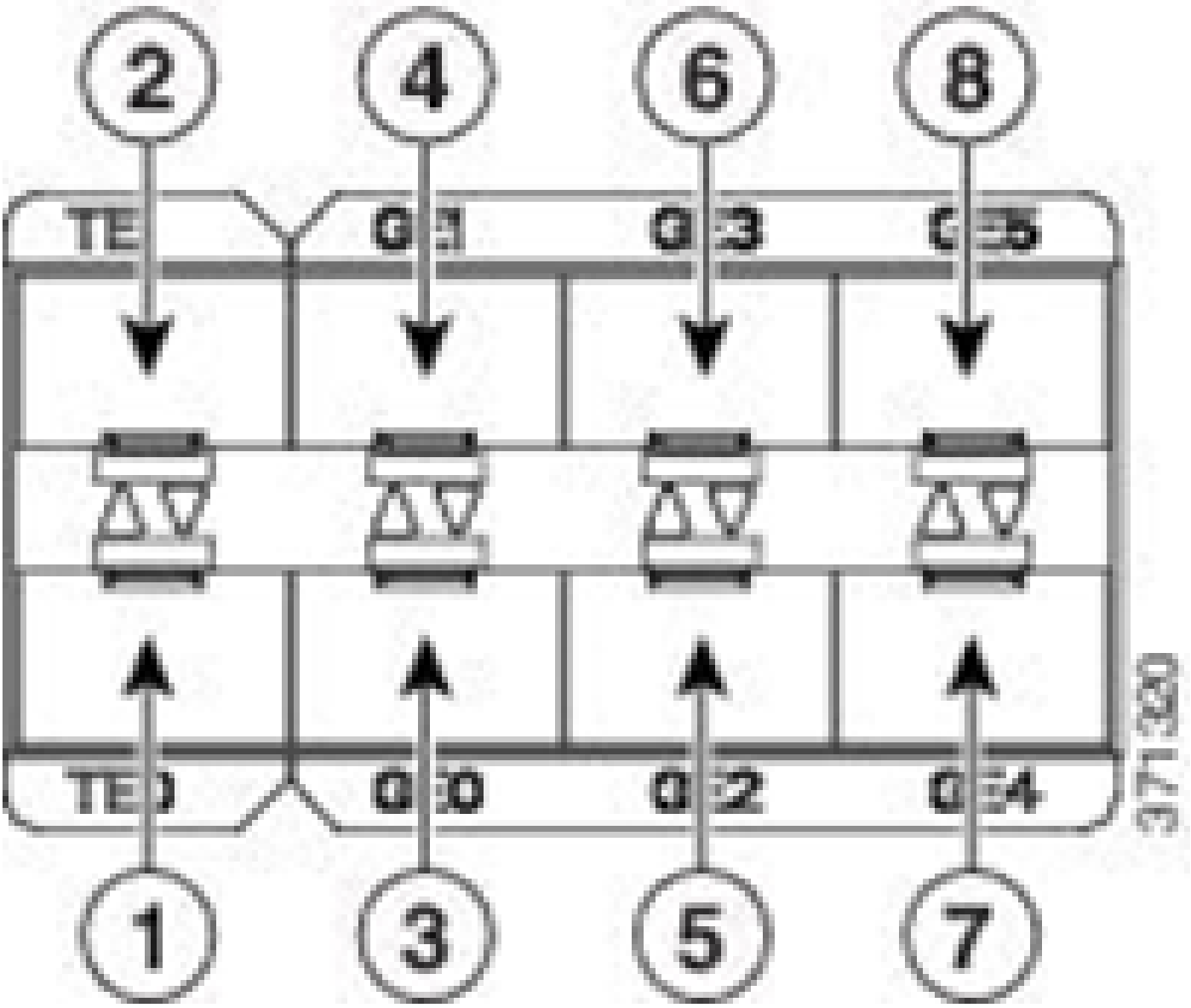
TTA da Cisco em ação

Detalhes do dispositivo TTA

A plataforma de sensor de telemetria baseada no Cisco IOS XE gera a telemetria do tráfego de rede IP espelhado das sessões do Switched Port Analyzer (SPAN) de switches e controladores sem fio. O dispositivo inspeciona milhares de protocolos usando a tecnologia Network-Based Application Recognition (NBAR) para produzir um fluxo de telemetria para que o Cisco DNA Center execute análises. O Cisco DNA Traffic Telemetry Appliance pode lidar com 20 Gbps de tráfego de throughput sustentado e inspecionar 40.000 sessões de endpoint para definição de perfis de dispositivos.

O dispositivo de telemetria de tráfego da Cisco

O TTA tem uma combinação de links de 10 Gig e 1 Gig que são usados para a inclusão de SPAN. Dessas portas, Gig0/0/5 é a única porta que pode ser configurada com um endereço IP e pode ser usada para comunicação com o Cisco DNA Center. A matriz de interface é mostrada abaixo.



Matriz de interface TTA

Matriz de interface TTA			
1	Porta 10 GE SFP+ 0/0/0	5	Porta GE SFP 0/0/2
2	Porta 10 GE SFP+ 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

Pré-requisitos do Cisco DNA Center para garantia

Esta seção destaca as configurações e os pré-requisitos que precisam ser atendidos para que o Cisco DNA Center possa processar a telemetria.

Cluster operacional do Cisco DNA Center

O cluster do Cisco DNA Center usado para gerenciar o TTA e processar a telemetria deve ser provisionado com estes critérios:

- Hierarquia de rede: A seção Hierarquia da rede no fluxo de trabalho de projeto é usada para definir diferentes campi do local, edifícios dentro desses campi e os andares individuais dentro desses edifícios e exibi-los em um mapa mundial. A hierarquia de site/rede apropriada deve ser configurada.
- Configurações de rede: A seção Network Settings permite a criação de configurações de rede padrão comuns que serão usadas pelos dispositivos na rede. Essas configurações podem ser aplicadas de maneira global, por local, edifício ou andar. Insira informações de DNS, nome de domínio, syslog, NTP, fuso horário e banner de login conforme exigido pela implantação.
- Credenciais do dispositivo: Essas credenciais serão usadas para acessar e descobrir dispositivos na rede, incluindo o TTA. É necessário que o Cisco DNA Center seja configurado com as credenciais apropriadas de CLI e SNMP. Juntamente com essas credenciais da NetConf, é bom ter.
- Conta CCO da Cisco: uma conta CCO válida é necessária para conectar o dispositivo e aproveitar os recursos do Cisco AI Cloud, fazer download de imagens para SWIM e fazer download de pacotes de protocolo para TTA e outros dispositivos.

Integração do ISE e do Cisco DNA Center

O Cisco Identity Services Engine (ISE) e o Cisco DNA Center podem ser integrados para automação de identidade e política. O ISE também é usado para coletar informações sobre os endpoints para aproveitar a Análise de endpoint de IA da Cisco. O PxGrid é usado para implementar a integração entre o ISE e o Cisco DNA Center.

Os requisitos de integração do Cisco DNA Center e do ISE são os seguintes:

- o serviço pxGrid deve ser habilitado no ISE.
- O acesso de leitura/gravação ERS deve estar habilitado.
- O certificado de administrador do ISE deve conter o endereço IP ou o FQDN do ISE no nome do assunto ou no campo SAN.
- O certificado do sistema Cisco DNA Center deve conter todos os endereços IP ou FQDNs do Cisco DNA Center no nome do assunto ou no campo SAN.
- As credenciais de administrador ERS do ISE serão usadas para estabelecer uma relação de confiança da comunicação ERS entre o ISE e o Cisco DNA Center.
- O nó pxGrid deve estar acessível a partir do Cisco DNA Center.

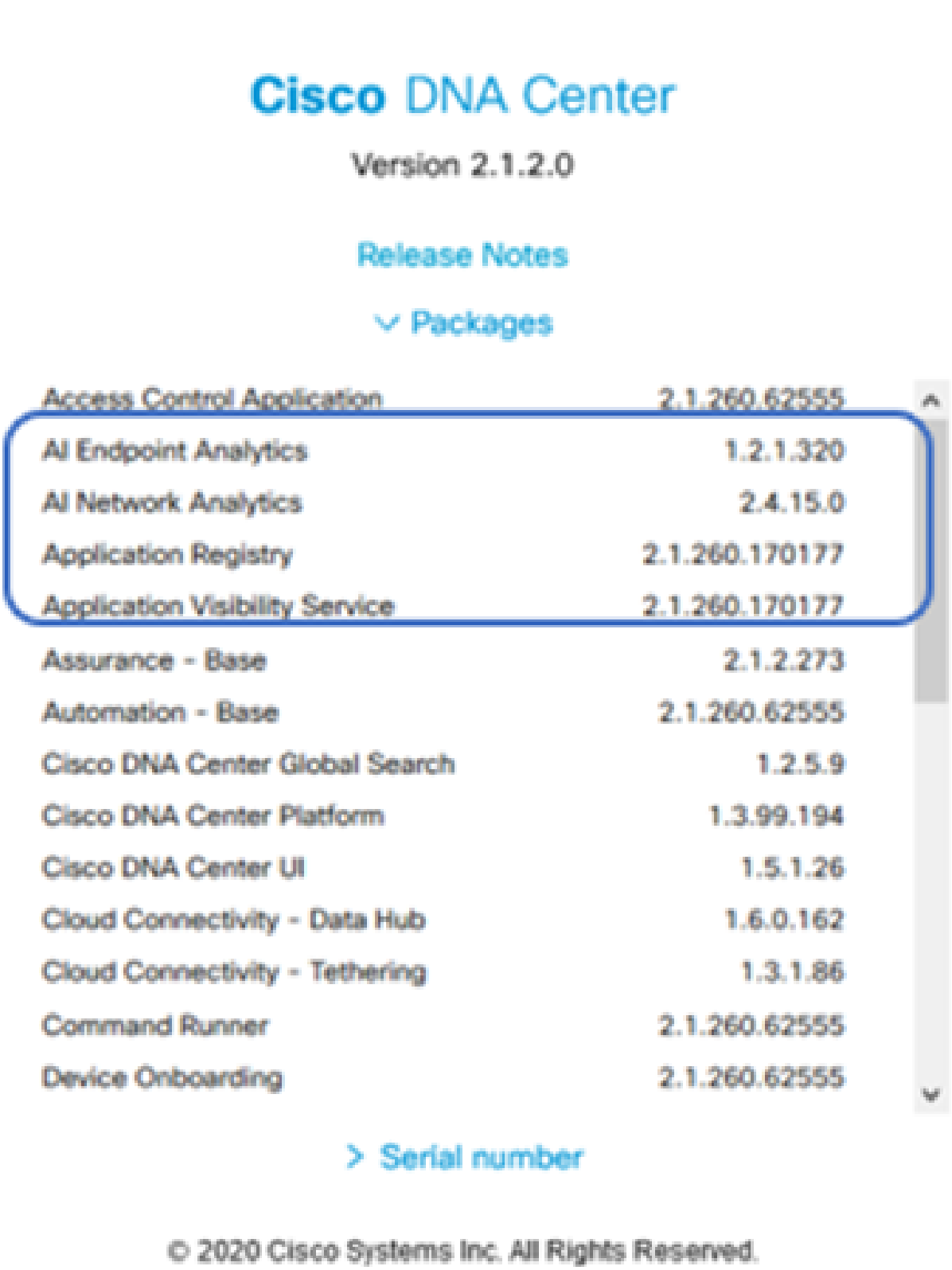
Requisitos do Cisco DNA Center para telemetria

Há requisitos que devem ser implementados para ativar a Garantia de Aplicativos no Cisco DNA Center. Esses requisitos são explicados em detalhes nas seções a seguir.

Pacotes de chaves do Cisco DNA Center

O Cisco DNA Center requer que esses três pacotes sejam instalados para permitir e analisar os dados de telemetria.

- Análise de endpoint de IA
- Análise de rede de IA
- Serviços de visibilidade de aplicativos



Pacotes do Cisco DNA Center necessários

Uma forma rápida de acessar essas informações é clicar no link "Sobre", abaixo do ícone de ponto de interrogação, no canto superior direito da página principal do Cisco DNA Center. Se esses aplicativos estiverem ausentes, eles precisarão ser instalados antes de prosseguir com a configuração de telemetria. Use este guia para instalar esses pacotes no Cisco DNA Center a

partir da nuvem da Cisco. Guia de atualização do Cisco DNA Center

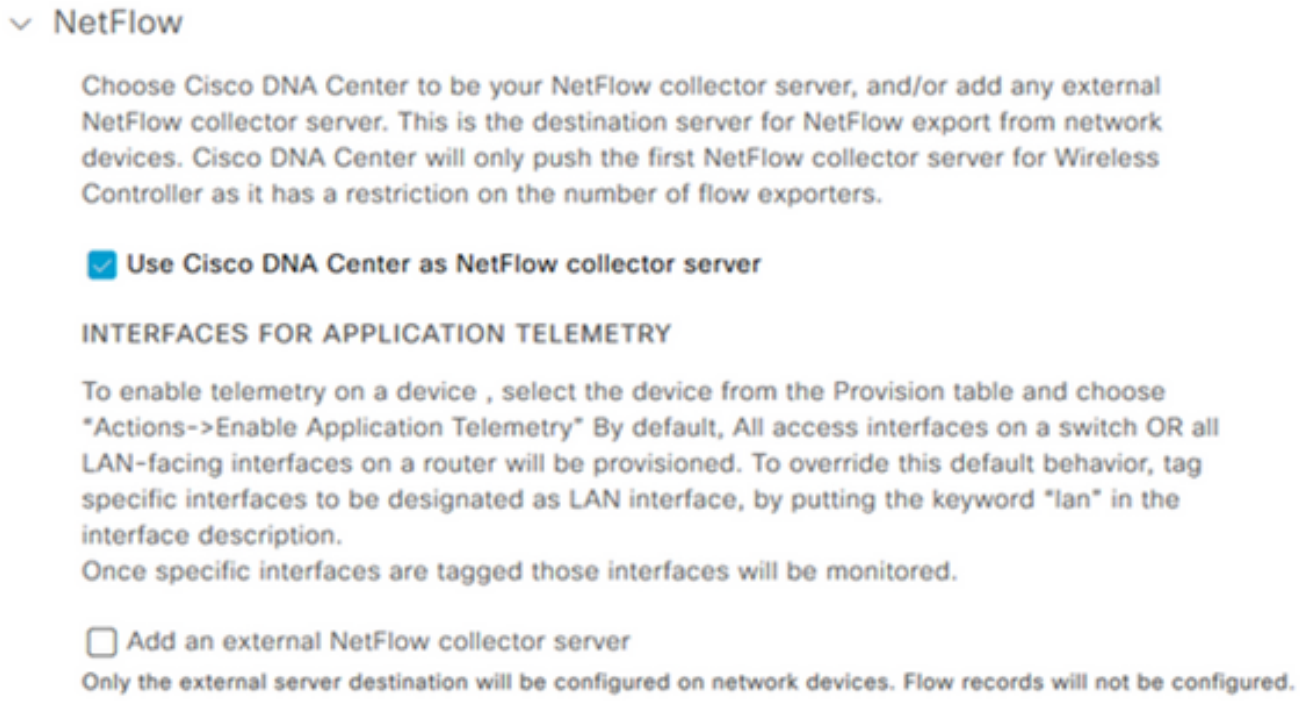
Cisco DNA Center como o coletor de telemetria

A exportação de dados do NetFlow é o transporte de tecnologia que fornece os dados de telemetria que serão encaminhados ao Cisco DNA Center para análise detalhada. Para permitir a coleta de dados para aprendizagem automática e raciocínio para análise de endpoint, o NetFlow precisa ser exportado para o Cisco DNA Center. O TTA é uma plataforma de sensor de telemetria usada para gerar telemetria a partir de tráfego de rede IP espelhado e compartilhá-la com o Cisco DNA Center para visibilidade de aplicativos e endpoints.

- O tráfego de rede é recebido de switches e roteadores através do espelhamento do Switched Port Analyzer (SPAN) e alimentado nas interfaces de espelhamento do Cisco DNA Traffic Telemetry Appliance.
- O Cisco DNA Traffic Telemetry Appliance analisa o tráfego recebido para produzir um fluxo de telemetria para o Cisco DNA Center.

Para ativar o Cisco DNA Center como o coletor de telemetria, siga estas etapas.

- No Cisco DNA Center, clique em Menu > Design > Network Settings e habilite a telemetria para o Cisco DNA Center coletar o NetFlow.



Configuração do DNAC como um coletor NetFlow

A Cisco AI Cloud

O Cisco AI Network Analytics é um aplicativo do Cisco DNA Center que aproveita o poder do aprendizado de máquina e do raciocínio de máquina para fornecer insights precisos que são

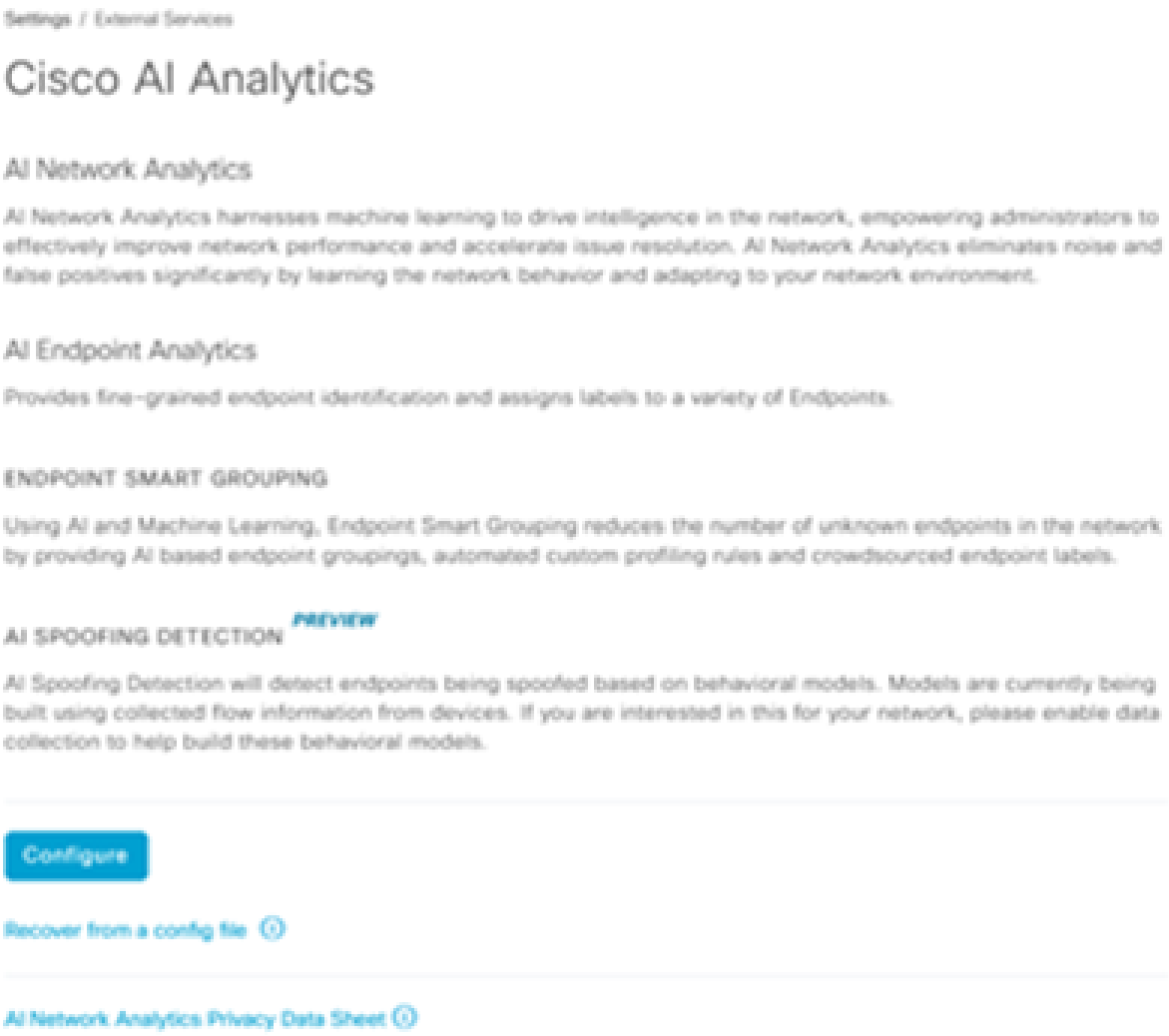
específicos para sua implantação de rede, o que permite que você solucione problemas rapidamente. As informações de rede e telemetria são anonimizadas no Cisco DNA Center e, em seguida, enviadas por meio de um canal criptografado seguro para a infraestrutura baseada em nuvem do Cisco AI Analytics. A nuvem do Cisco AI Analytics executa o modelo de aprendizagem automática com esses dados de evento e traz os problemas e as percepções gerais de volta para o Cisco DNA Center. Todas as conexões com a nuvem são de saída no TCP/443. Não há conexões de entrada, o Cisco AI Cloud não inicia nenhum fluxo de TCP em direção ao Cisco DNA Center. Os nomes de domínio totalmente qualificados (FQDN) que podem ser usados para permitir acesso ao proxy HTTPS e/ou firewall no momento em que este artigo é escrito são:

- https://api.use1.prd.kairos.ciscolabs.com (Região Leste dos EUA)
- https://api.euc1.prd.kairos.ciscolabs.com (Região Central da UE)

O dispositivo Cisco DNA Center implantado deve ser capaz de resolver e acessar os vários nomes de domínio na Internet que são hospedados pela Cisco.

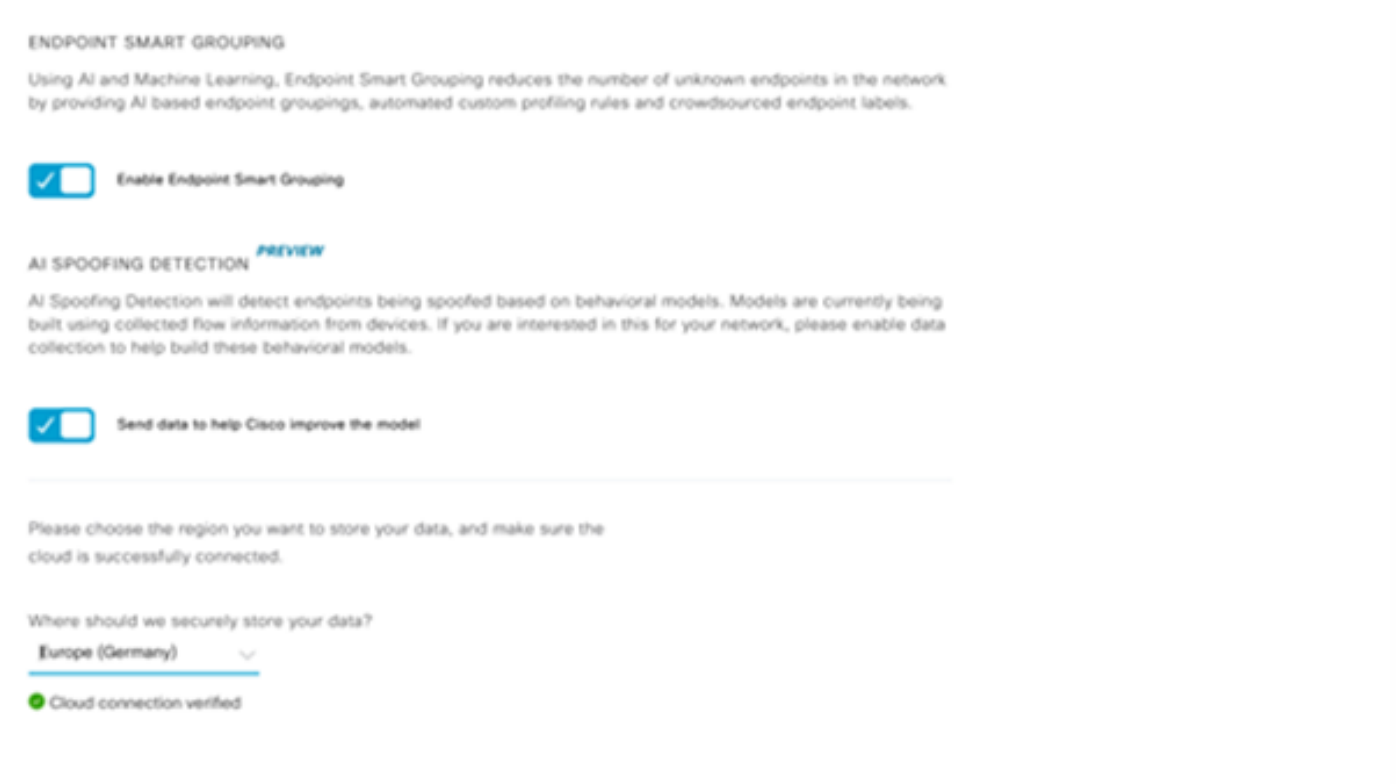
Siga estas etapas para conectar o Cisco DNA Center ao Cisco AI Cloud.

- Vá para a interface do usuário da Web do dispositivo Cisco DNA Center para concluir o registro do AI Cloud:
- Navegue até Sistema > Configurações > Serviços externos > Cisco AI Analytics
- Clique em Configure e ative a opção Endpoint Smart Grouping and AI spoof detection.
- O Agrupamento inteligente de endpoints usa a nuvem AI/ML para agrupar endpoints desconhecidos para ajudar os administradores a rotular esses endpoints. Isso é muito útil para reduzir a rede desconhecida na rede.
- A detecção de spoof de IA ajudará a Cisco a reunir informações adicionais de NetFlow/telemetria e a modelar o endpoint.
- Escolha o local mais próximo da região geográfica da implantação. Depois que a verificação da conexão em nuvem for feita e a conexão for bem-sucedida, você verá uma caixa de seleção verde.



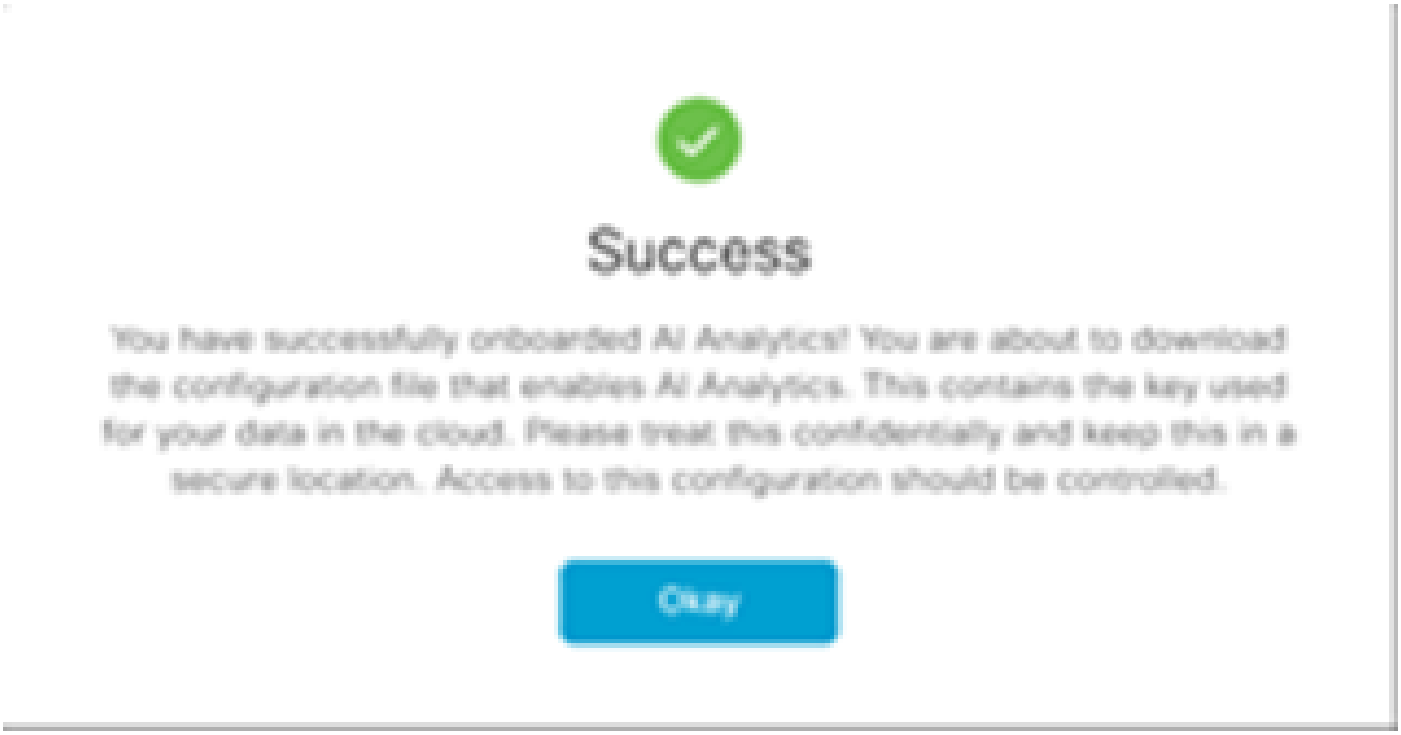
Configuração da GUI do Cisco AI Analytics

- Se a conexão não for bem-sucedida, verifique as configurações de proxy no Cisco DNA Center na página System > Settings > System Configuration > Proxy config se um proxy estiver sendo usado. Também é uma boa ideia verificar quaisquer regras de firewall que possam estar bloqueando essa comunicação.



Verificação de conexão em nuvem Cisco AI/ML

- Aceite o contrato universal de nuvem da Cisco para ativar a análise de IA.
- Neste ponto, a integração estará concluída e uma caixa de diálogo indicando isso será exibida como mostrado.



Caixa de diálogo de êxito após a inscrição

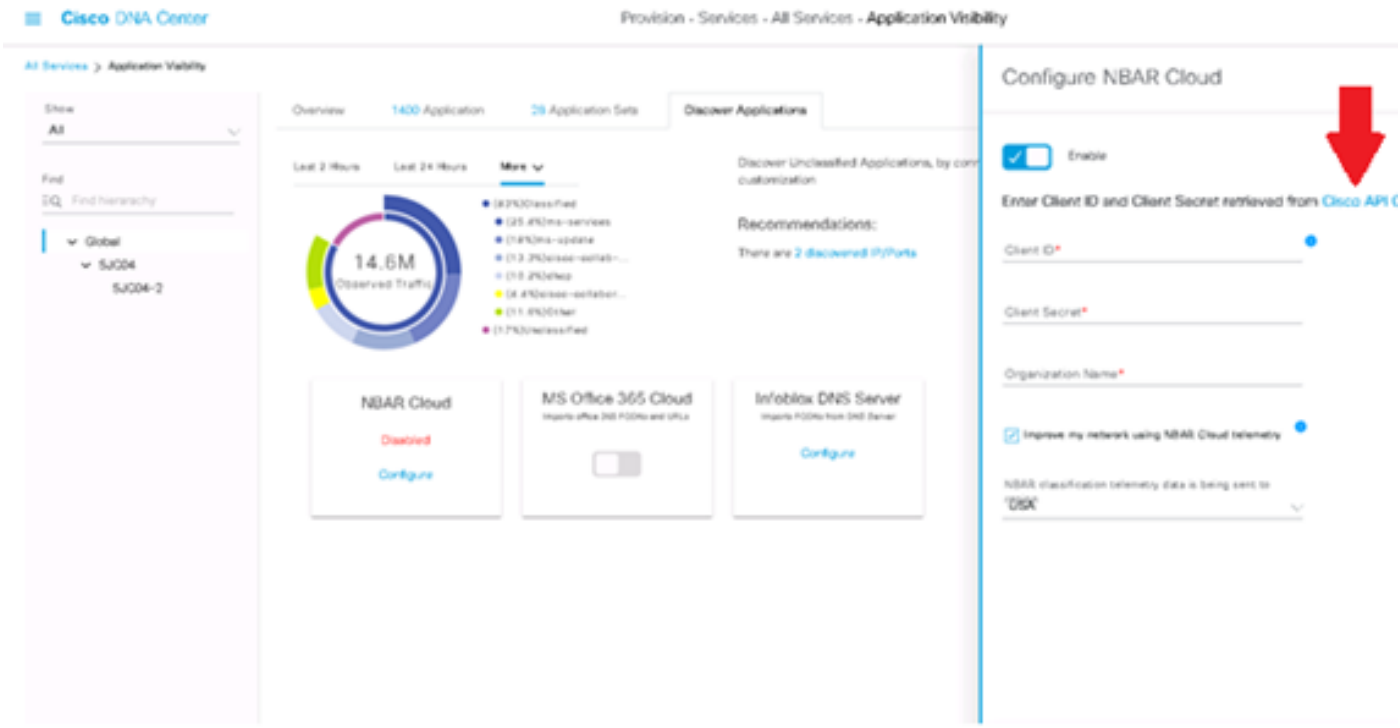
A nuvem de reconhecimento de aplicativos baseados em rede (NBAR)

O Telemetry Appliance e a plataforma Catalyst 9000 coletam metadados de endpoint usando a inspeção profunda de pacotes de fluxos de pacotes e aplicam o Network Based Application Recognition (NBAR) para determinar quais protocolos e aplicativos estão sendo utilizados na rede. O Cisco DNA Center tem um pacote de protocolo NBAR integrado que pode ser atualizado. Os dados de telemetria podem ser enviados para a nuvem do Cisco NBAR para análise adicional e para detecção de assinaturas de protocolos desconhecidos. Para que isso aconteça, o dispositivo do Cisco DNA Center precisa estar limitado à nuvem. O Network-Based Application Recognition (NBAR) é um mecanismo avançado de reconhecimento de aplicativos desenvolvido pela Cisco que utiliza várias técnicas de classificação e pode atualizar facilmente suas regras de classificação.

Para conectar o Cisco DNA Center à nuvem do Cisco NBAR, siga estas etapas.

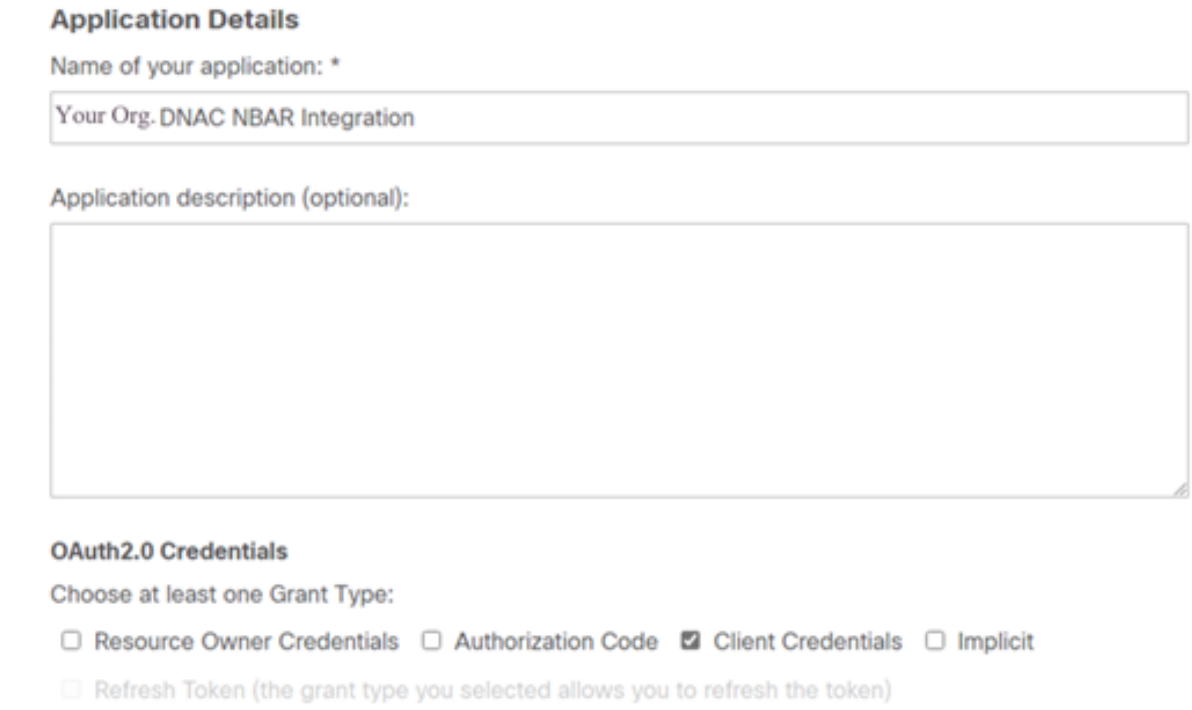
- Na interface do usuário do Cisco DNA Center, vá para Provision > Services > Application Visibility. Clique em Configurar em Nuvem NBAR e um painel será aberto. Ative o serviço.
- Se você tiver a ID do cliente, o segredo do cliente e o nome da empresa, atribua a eles nomes exclusivos, dependendo da organização e do uso.
- No momento em que escrevemos, a única região de nuvem NBAR atualmente disponível está nos EUA; mais regiões podem se tornar disponíveis no futuro. Selecione o que está nas preferências de implantação e salve-o.

Para obter as credenciais de ID do cliente e Segredo do cliente, clique no link "Cisco API Console", isso abrirá um portal. Faça login com a ID CCO apropriada, crie um novo aplicativo, selecione as opções correspondentes à nuvem NBAR e preencha o formulário. Depois de concluído, você obterá uma ID de cliente e um segredo. Consulte a figura mostrada abaixo.



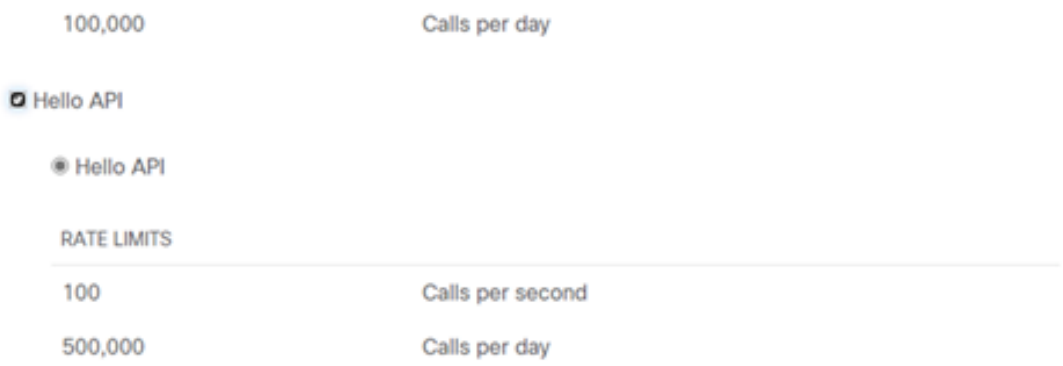
Link da API da Cisco para recuperar a ID e o segredo do cliente

Essas imagens demonstram as opções usadas para registrar na nuvem NBAR.



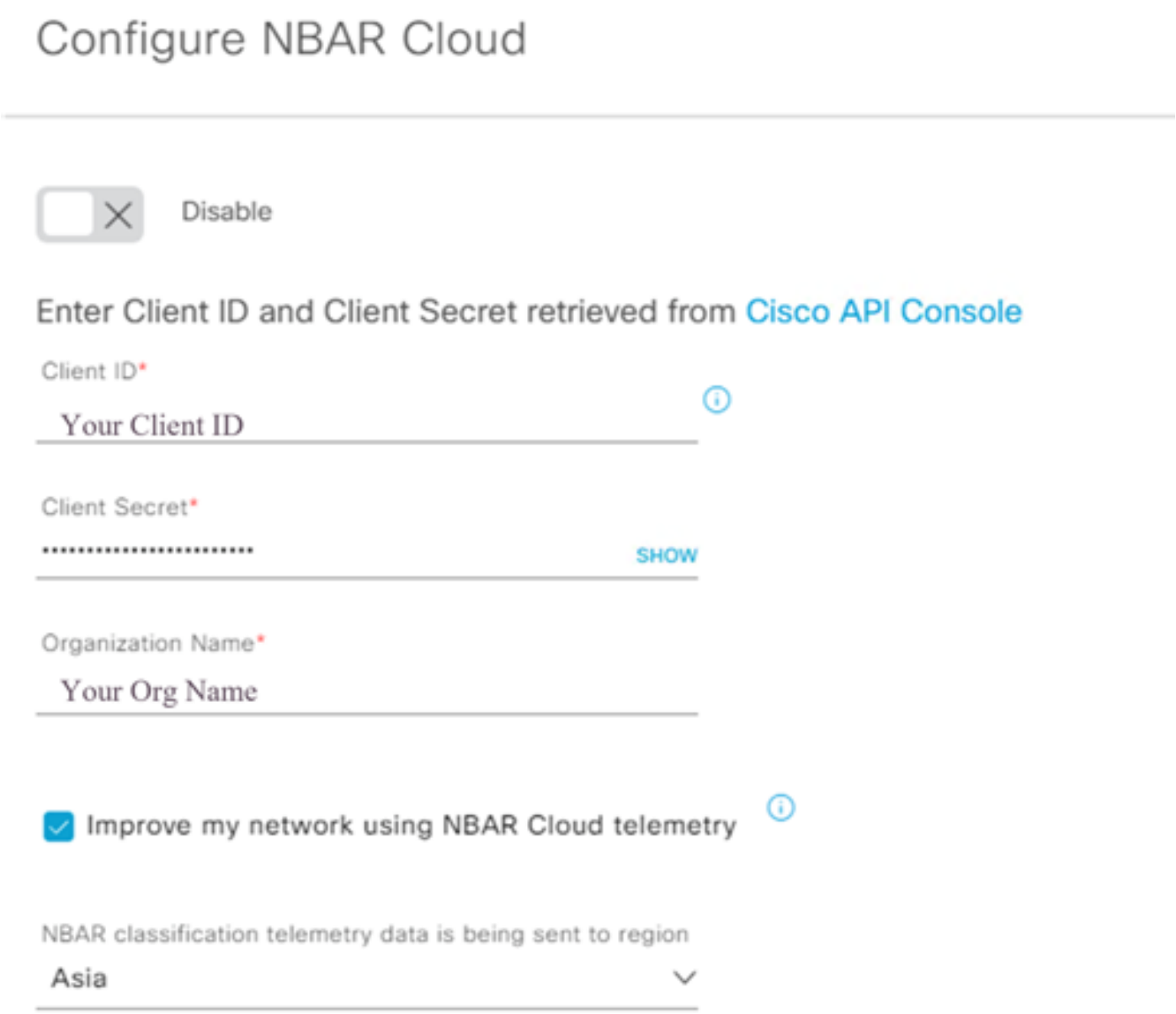
Detalhes do aplicativo de nuvem NBAR

- Use esta imagem como referência ao concluir os detalhes da solicitação de API.



Detalhes da API do Aplicativo

- Insira a ID do cliente e o segredo obtidos no portal Cisco no Cisco DNA Center.



Configurando ID e segredo do cliente no DNAC

CBAR (reconhecimento de aplicativo baseado em controlador) e SD-AVC

O CBAR é usado para classificar milhares de aplicativos de rede, aplicativos internos e tráfego de rede geral. Ele permite que o Cisco DNA Center aprenda dinamicamente sobre os aplicativos usados na infraestrutura de rede. O CBAR ajuda a manter a rede atualizada, identificando novos aplicativos à medida que sua presença na rede continua a aumentar e permite atualizações para pacotes de protocolo. Se a visibilidade do aplicativo for perdida de ponta a ponta por meio de pacotes de protocolo desatualizados, poderá ocorrer uma categorização incorreta e um encaminhamento subsequente. Isso causará não apenas buracos de visibilidade na rede, mas também problemas incorretos de enfileiramento ou encaminhamento. O CBAR resolve esse

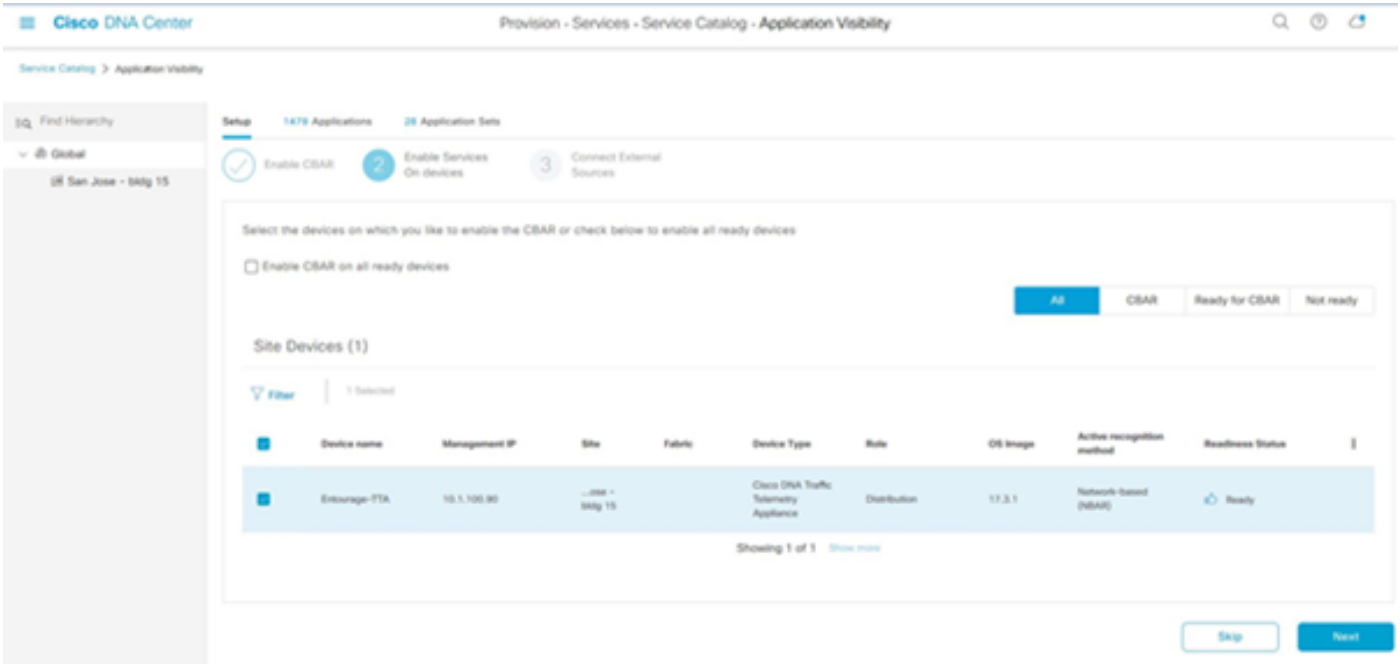
problema permitindo que pacotes de protocolo atualizados sejam enviados pela rede.

O Cisco Software-Defined AVC (SD-AVC) é um componente do Cisco Application Visibility and Control (AVC). Ele funciona como um serviço de rede centralizado operando com dispositivos participantes específicos em uma rede. O SD-AVC também auxilia no DPI dos dados do aplicativo. Alguns dos recursos e benefícios atuais fornecidos pelo SD-AVC incluem:

- Reconhecimento de aplicativos em nível de rede consistente na rede
- Melhor reconhecimento de aplicativos em ambientes de roteamento simétricos e assimétricos
- Reconhecimento de primeiro pacote aprimorado
- Atualização do pacote de protocolos no nível da rede
- Painel SD-AVC baseado em navegador seguro sobre HTTPS para monitorar a funcionalidade e as estatísticas SD-AVC, e para configurar atualizações do Pacote de Protocolo em toda a rede

Para ativar o CBAR para dispositivos relevantes, siga estas etapas.

- Vá para o menu do Cisco DNA Center, Provisionar > Visibilidade do aplicativo. O na primeira vez que a página Application Visibility for aberta, o usuário receberá um assistente de configuração mostrado abaixo.
- Depois de descobrir os dispositivos no Cisco DNA Center para cada site, selecione o dispositivo para ativar o CBAR e continue com a próxima etapa.



Ativando o CBAR no dispositivo

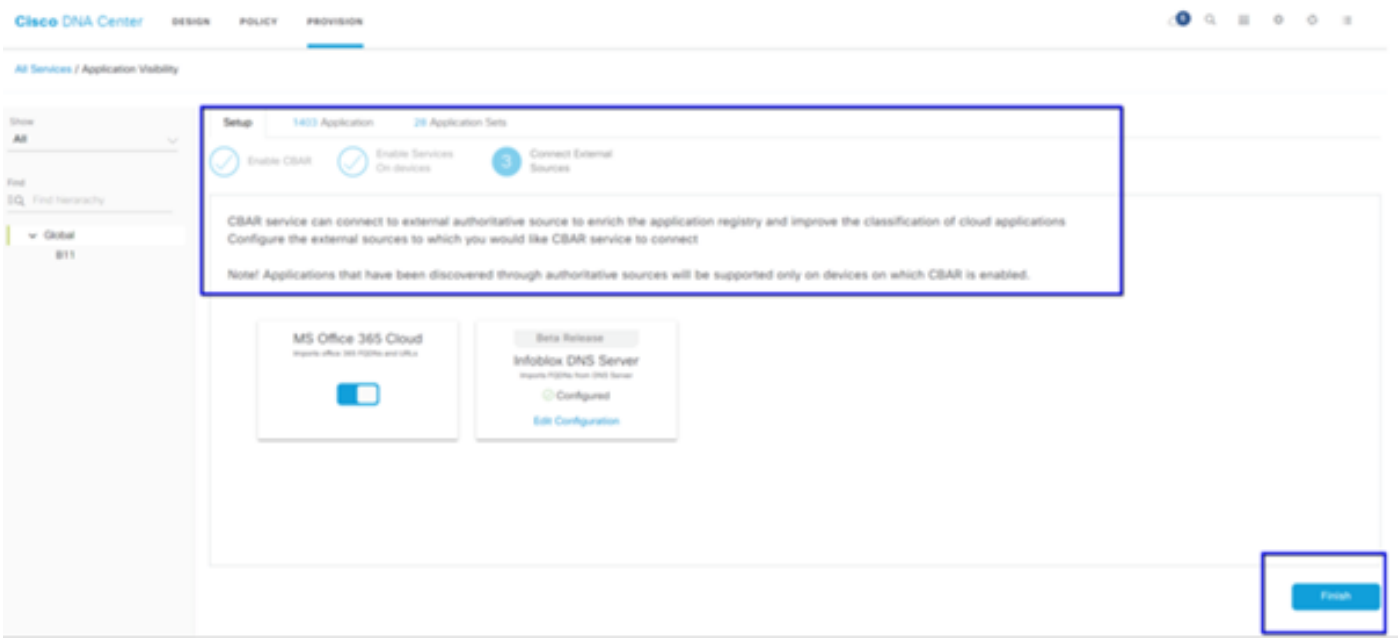
Conector de Nuvem do Microsoft Office 365 (não obrigatório)

O Cisco DNA Center pode ser integrado diretamente com o feed RSS da Microsoft para garantir que o reconhecimento de aplicativos para o Office 365 esteja de acordo com as orientações publicadas. Essa integração é conhecida como Microsoft Office 365 Cloud Connector no Cisco

DNA Center. É recomendável ter esse recurso implantado se o usuário estiver executando aplicativos do Microsoft Office 365 na rede. A integração com o Microsoft Office 365 não é um requisito e, se não estiver habilitada, afetará apenas a capacidade do Cisco DNA Center de processar e classificar dados de host do Microsoft Office 365. O Cisco DNA Center já tem o reconhecimento de aplicativos do Microsoft Office 365 integrado, mas ao integrar-se diretamente com o provedor de aplicativos, o Cisco DNA Center pode obter informações atualizadas e precisas sobre os blocos de propriedade intelectual atuais e URLs utilizados pelo conjunto do Microsoft Office 365.

Para integrar o Cisco DNA Center à nuvem do Microsoft Office 365, siga estas etapas.

- Clique no ícone Menu e escolha Provisionar > Serviços > Visibilidade do aplicativo
- Clique em Discover Applications (Descobrir aplicativos)
- Clique no botão de alternância MS Office 365 Cloud para integrar o Cisco DNA Center com a nuvem do Microsoft Office 365.

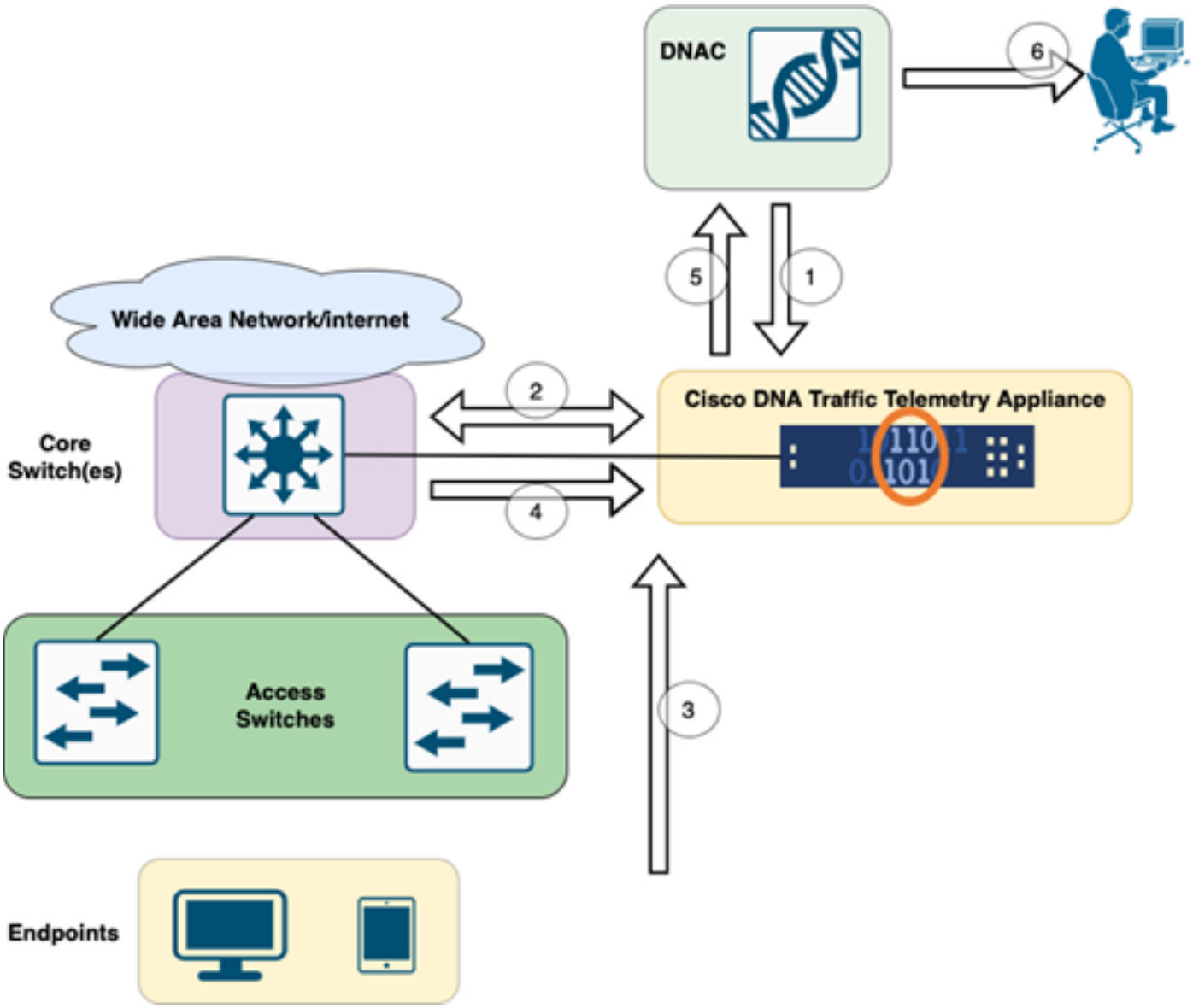


Integração de nuvem MS O365

Implementação de TTA

Esta seção aborda as etapas necessárias para implementar o TTA em uma rede.

Visão Geral do Fluxo de Trabalho TTA



Fluxo de trabalho de TTA para DNAC

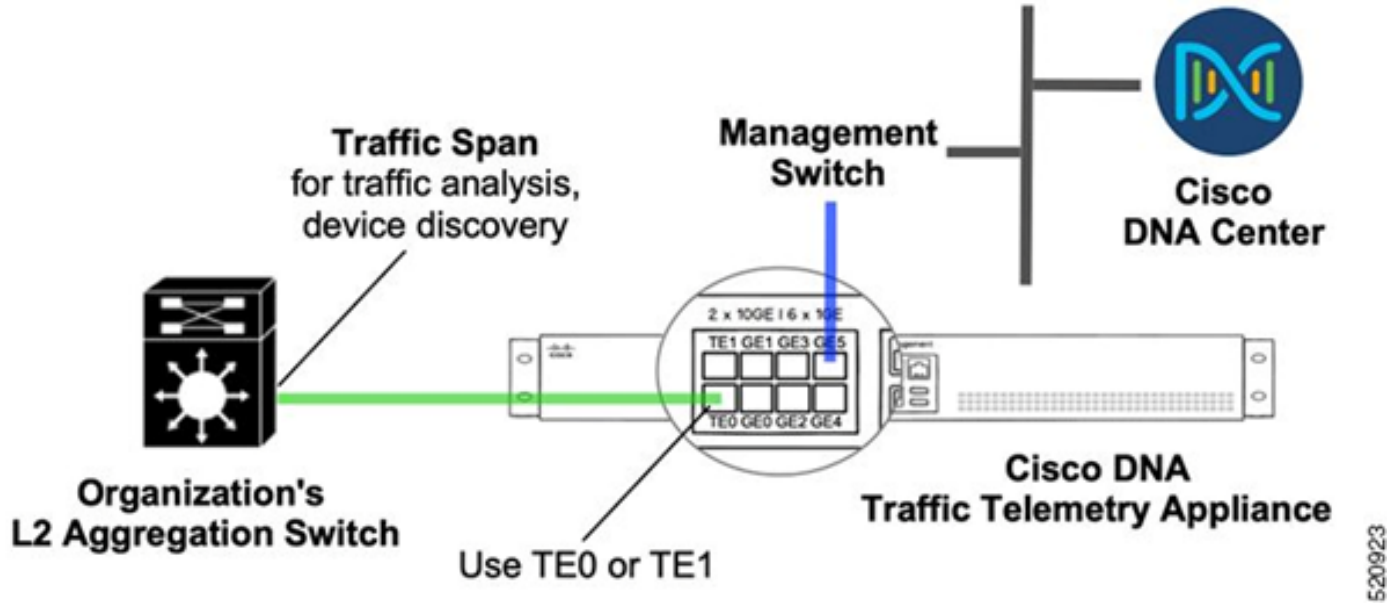
As etapas destacadas neste diagrama descrevem o processo e o fluxo de telemetria entre o TTA e o Cisco DNA Center. Aqui, essas etapas são desenvolvidas com mais detalhes.

1. O Cisco Traffic Telemetry Appliance está conectado ao switch de agregação de site ou ao switch central na infraestrutura de rede. Essa conexão permite que o equipamento receba dados de tráfego de vários switches de acesso na rede.
2. O Cisco Traffic Telemetry Appliance integra-se ao Cisco DNA Center, que serve como plataforma de gerenciamento de rede. Essa integração permite a comunicação e a troca de dados sem interrupções entre o dispositivo e o Cisco DNA Center.
3. À medida que o tráfego do usuário flui pela rede, ele é estendido ou espelhado para o Cisco Traffic Telemetry Appliance. Isso significa que uma cópia do tráfego de rede é enviada ao dispositivo para fins de monitoramento e análise, enquanto o tráfego original continua seu caminho normal.
4. O Cisco Traffic Telemetry Appliance coleta e processa os dados de tráfego recebidos. Ele extrai informações relevantes, como detalhes em nível de pacote, estatísticas de fluxo e métricas de desempenho, do tráfego espelhado.
5. As informações de telemetria processadas são enviadas do Cisco Traffic Telemetry

Appliance para o Cisco DNA Center. Essa comunicação permite que o Cisco DNA Center receba informações e atualizações em tempo real sobre os padrões de tráfego, o desempenho de aplicativos e as anomalias da rede.

6. Os insights de telemetria gerados pelo Cisco DNA Center fornecem informações valiosas aos administradores de rede. Eles podem usar a interface do Cisco DNA Center para visualizar e analisar os dados coletados, obter visibilidade sobre a integridade e o desempenho dos aplicativos da rede, identificar possíveis problemas e tomar decisões conscientes para otimização e solução de problemas da rede.

Implantação do TTA: Diagrama de alto nível



Implantação do TTA: alto nível

O diagrama acima descreve como o TTA pode ser conectado na rede. As interfaces de 10 Gig e 1 Gig podem ser usadas para a inclusão de SPAN na taxa de linha. A interface Gi0/0/5 é usada para comunicação com o Cisco DNA Center, para orquestração e para o encaminhamento de insights de telemetria para o Cisco DNA Center; essa interface NÃO PODE ser usada para a inclusão de SPAN.

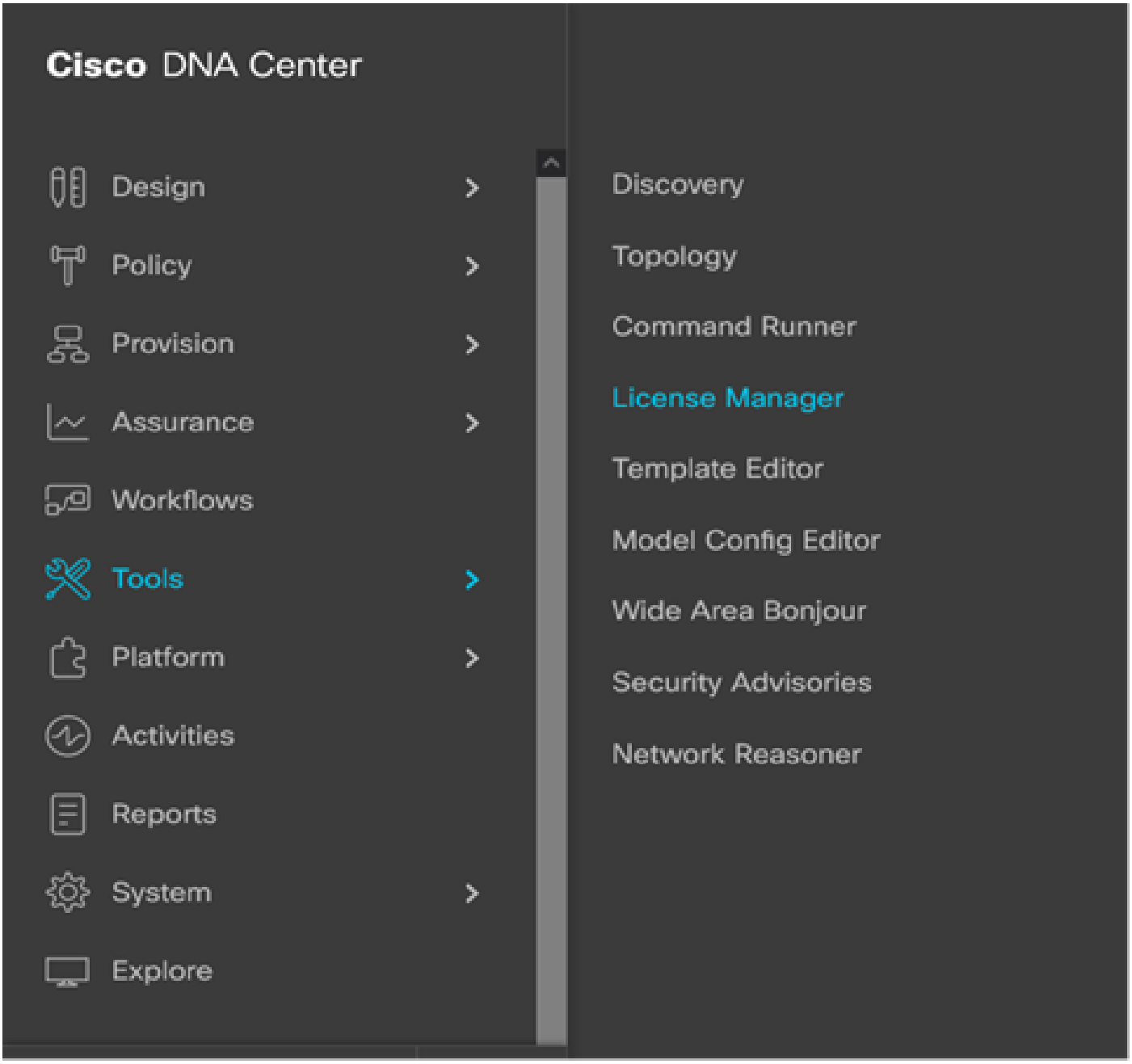
Software TTA e requisitos de licenciamento

Os dispositivos TTA implantados na rede serão cruciais para fornecer insights de telemetria sobre os dados do usuário e endpoints do usuário. Para implantar a solução com êxito, esses requisitos devem ser atendidos.

- O TTA deve ser configurado com uma configuração inicial de bootstrap para que possa ser descoberto pelo Cisco DNA Center (Configuração de bootstrap do TTA)
- O dispositivo TTA precisa ser integrado ao Cisco DNA Center para que possa ser gerenciado pelo Cisco DNA Center (Adicionando caixa de telemetria ao inventário do Cisco DNA Center)
- A licença correta precisa ser instalada no TTA (licença do dispositivo TTA)

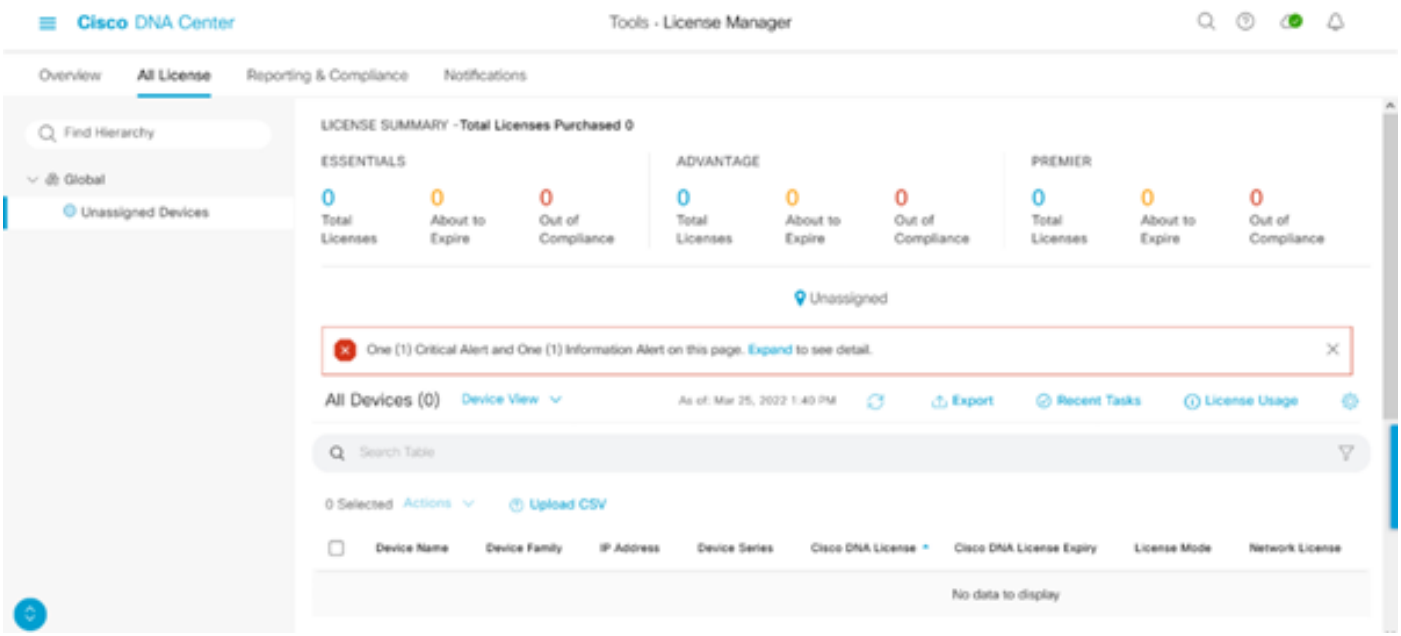
O dispositivo oferece suporte a apenas um sistema operacional e exige a licença Cisco DNA ATA Advantage para coletar telemetria. Não há necessidade de uma licença de recurso (como IP Base ou Advanced IP Services) ou um pacote de licenciamento perpétuo (como Network Essentials ou Network Advantage).

Para gerenciar licenças no Cisco DNA Center, navegue até o gerenciador de licenças navegando até Ferramentas > Gerenciador de licenças no menu suspenso do Cisco DNA Center clicando no ícone Menu



Gerenciador de licença em DNAC

- Navegue até a página All License; ela será semelhante a esta imagem. Nesta página, o administrador pode gerenciar licenças de dispositivos de rede como a do TTA.



Página Todas as Licenças no DNAC

Integração de TTA e configuração de dia 0

Para facilitar a descoberta e a integração do dispositivo TTA pelo Cisco DNA Center, há comandos de bootstrap que devem ser configurados nos dispositivos TTA do site. Com a configuração de bootstrap implementada, o TTA poderá ser descoberto no painel do Cisco DNA Center. A seguir estão itens de configuração de dia 0 para um dispositivo TTA. Depois que o dispositivo for integrado à hierarquia do site, o dispositivo TTA herdará os itens de configuração restantes do 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
```

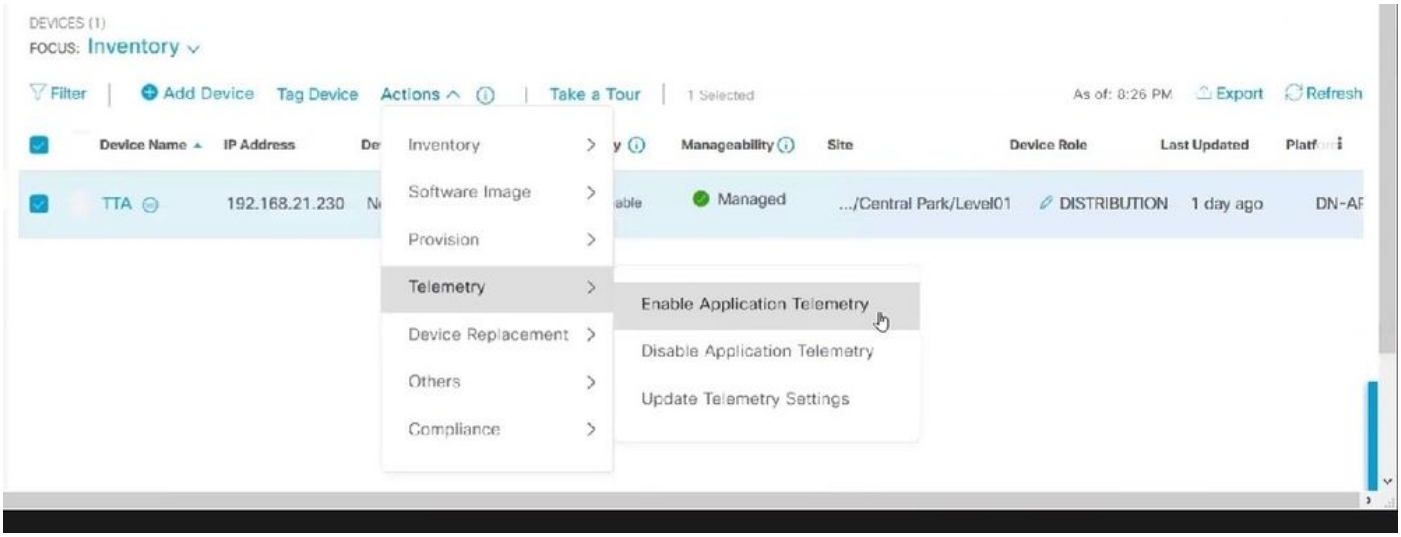
```
ip ssh source-interface GigabitEthernet0/0/5

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
```

Depois que esses itens forem configurados no TTA, ele poderá ser descoberto pelo Cisco DNA Center.

Adicionando o dispositivo TTA ao inventário do Cisco DNA Center

Para aproveitar o TTA, o Cisco DNA Center precisa descobrir e gerenciar o dispositivo TTA. Depois que o TTA é integrado ao Cisco DNA Center, ele pode ser gerenciado a partir do Cisco DNA Center. Antes de descobrir o dispositivo TTA, precisamos garantir que a hierarquia de site completa esteja em vigor para o site. Depois disso, continuaremos adicionando o dispositivo TTA sob a hierarquia de site específica seguindo estas etapas da página Menu > Provisionar > Dispositivos > Inventário para adicionar o dispositivo a um site.

1. Forneça o nome de usuário/senha (CLI) e a comunidade SNMP necessária para se conectar ao dispositivo e a senha de ativação. Aguarde até que o dispositivo seja adicionado com êxito antes de continuar.
2. Verifique o nome do dispositivo, a família (gerenciamento de rede no caso de TTA), a acessibilidade - alcançável, gerenciável, função do dispositivo - distribuição. O dispositivo será inicialmente "Não compatível", no entanto, quando totalmente provisionado, o status mudará.
3. Quando o TTA estiver integrado, o Cisco DNA Center enviará modelos de configuração para configurá-lo com funções avançadas de telemetria.



Detecção de TTA e habilitação de telemetria de aplicativos

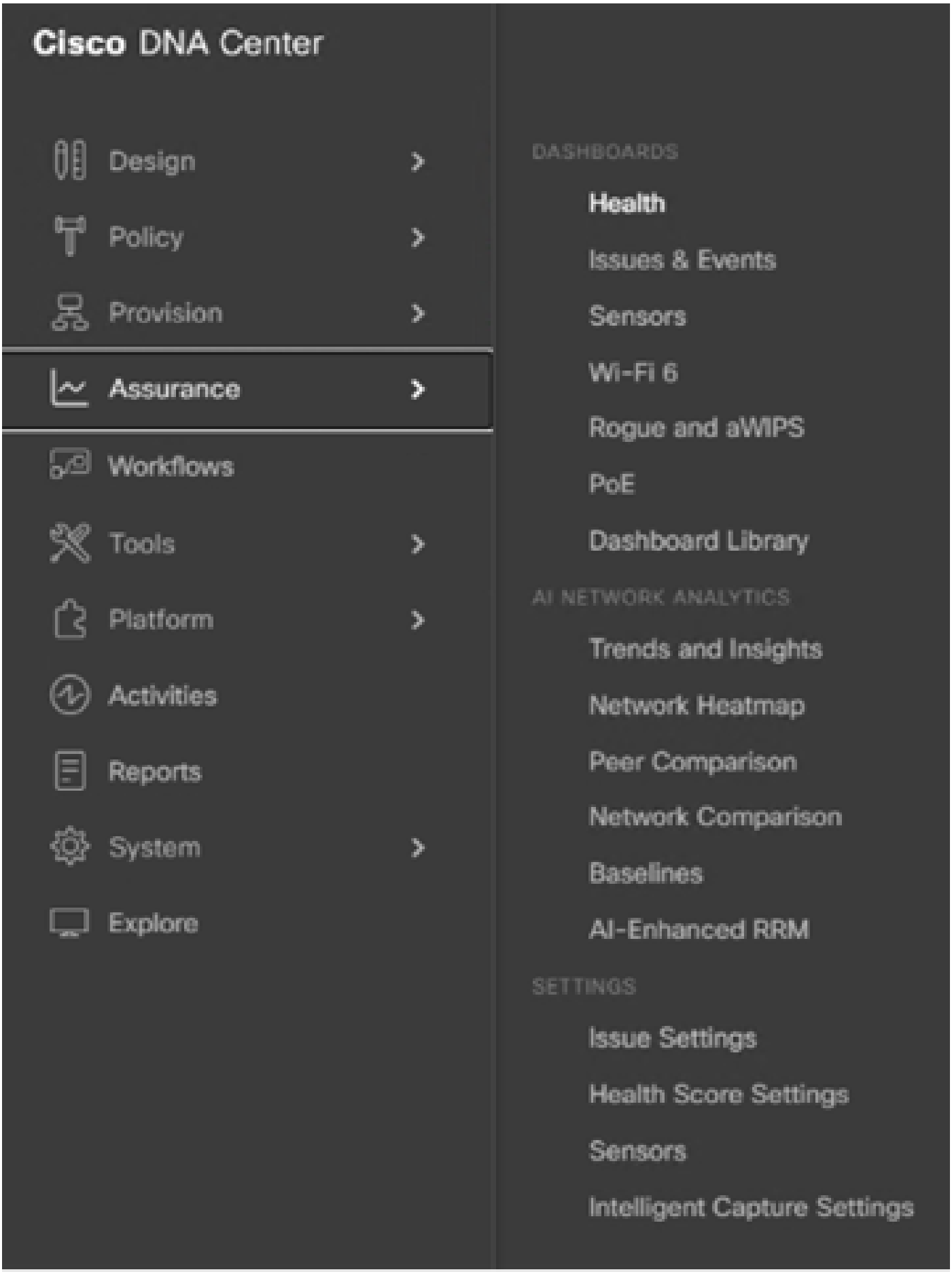
configuração de SPAN

Dependendo das capacidades de hardware do switch principal, a sessão de SPAN pode ser configurada para SPAN em um grupo de VLANs ou interface(s) à interface conectada ao TTA. Um exemplo de configuração é fornecido aqui.

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

Garantia coletada

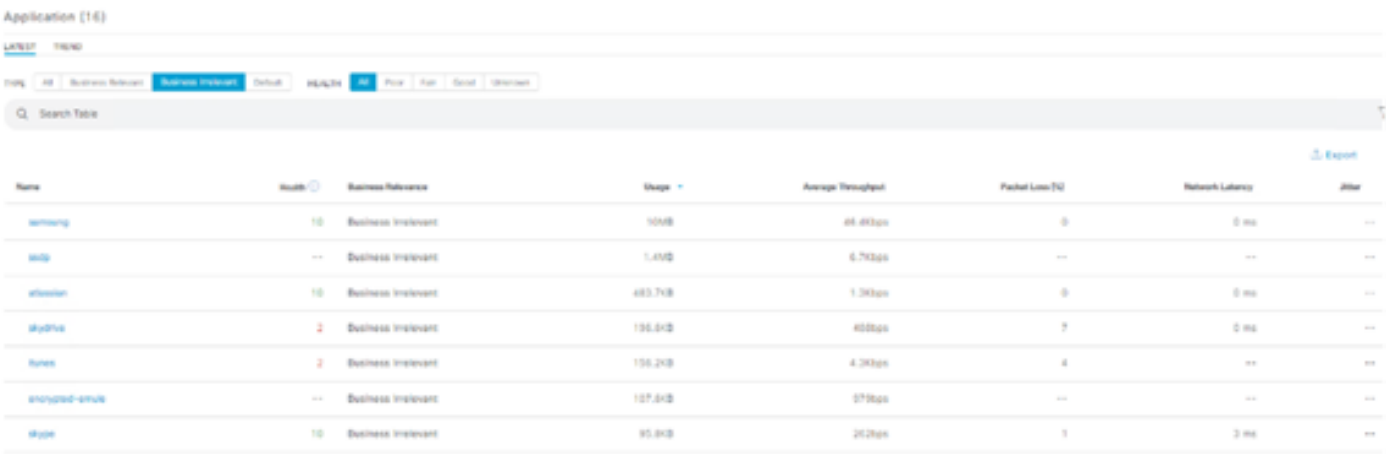
Para acessar os dados de garantia coletados do Traffic Telemetry Appliance instalado, vá para a seção Garantia e clique em Saúde.



Navegação para o App Assurance

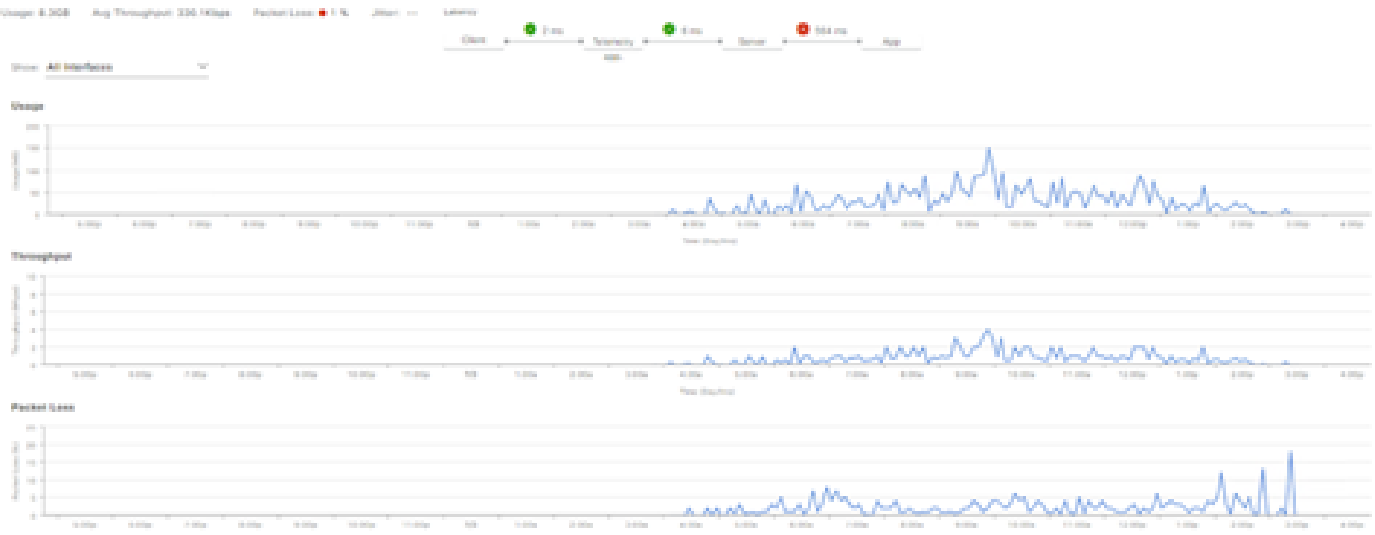
Escolha Aplicativos e você encontrará uma visão geral abrangente dos dados do aplicativo, incluindo latência e jitter capturados pelo TTA com base no tipo de aplicativo específico.

Navegação para o Application Assurance



Interface de usuário de Garantia de Aplicativo Detalhada

Para obter uma análise mais detalhada, os usuários podem explorar aplicativos individuais clicando no aplicativo específico e selecionando o Exportador como o Dispositivo de telemetria de tráfego e examinando métricas específicas, como dados de uso, throughput e perda de pacotes, latência de rede do cliente, latência de rede do servidor e latência do servidor de aplicativos.



Exemplo: Informações De Aplicação Pt.1

Exemplo: Informações De Aplicação Pt.2

Verificar

1. Após ativar o CBAR, verifique se o serviço SD-AVC (Application Visibility Control) está ativado no dispositivo efetuando login no Cisco Traffic Telemetry Appliance e executando este comando CLI. A saída será semelhante a esta amostra, indicando o endereço IP do controlador e o status como conectado.

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

2. Use o comando "show license summary" na CLI do TTA para verificar os detalhes relevantes da licença do 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. Verifique se a sessão de SPAN foi configurada corretamente no switch central/de agregação.

```
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. Quando o TTA for provisionado com êxito, esses comandos serão (ou foram) enviados ao 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
```

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.