トラフィックテレメトリアプライアンス(TTA)とCisco DNA Center App Assuranceを利用する：その理由と方法

内容

はじめに

このドキュメントでは、Cisco DNAトラフィックテレメトリアプライアンス（Cisco部品番号DN-APL-TTA-M）プラットフォームと、Cisco DNA CenterでApplication Assuranceを有効にする方法について説明します。 Iまた、設定および検証プロセスとともに、ネットワーク内でTTAを配置する方法と場所についても説明します。この記事では、関連するさまざまな前提条件についても説明します。

前提条件

Cisco DNA Center AssuranceおよびApplication Experienceの各動作の仕組みに関する知識があることが推奨されます。

アプリケーション保証

Assuranceは、ネットワークデータのビジネス可能性を大幅に高めることができる、多目的のリアルタイムのネットワークデータ収集および分析エンジンです。 Assuranceは、複雑なアプリケーションデータを処理し、その結果をAssuranceヘルスダッシュボードに表示して、ネットワークで使用されているアプリケーションのパフォーマンスに関する洞察を提供します。 データの収集元に応じて、次の一部またはすべてが表示されます。

- アプリケーション名
- スループット
- DSCPマーキング
- パフォーマンスメトリック（遅延、ジッタ、およびパケット損失）

収集されるデータ量に基づいて、Application Assuranceは次の2つのモデルに分類できます。

- Application Visibility(AppVis)および
- アプリケーションエクスペリエンス(AppX)

アプリケーション名とスループットは、まとめて定量的メトリックと呼ばれます。定量的メトリックのデータは、アプリケーションの可視性を有効にすることから得られます。

DSCPマーキングとパフォーマンスメトリック（遅延、ジッタ、およびパケット損失）は、まとめて定性的メトリックと呼ばれます。定性的なメトリックのデータは、アプリケーションエクスペリエンスの実現から得られます。

アプリケーションの可視性(AppVis)

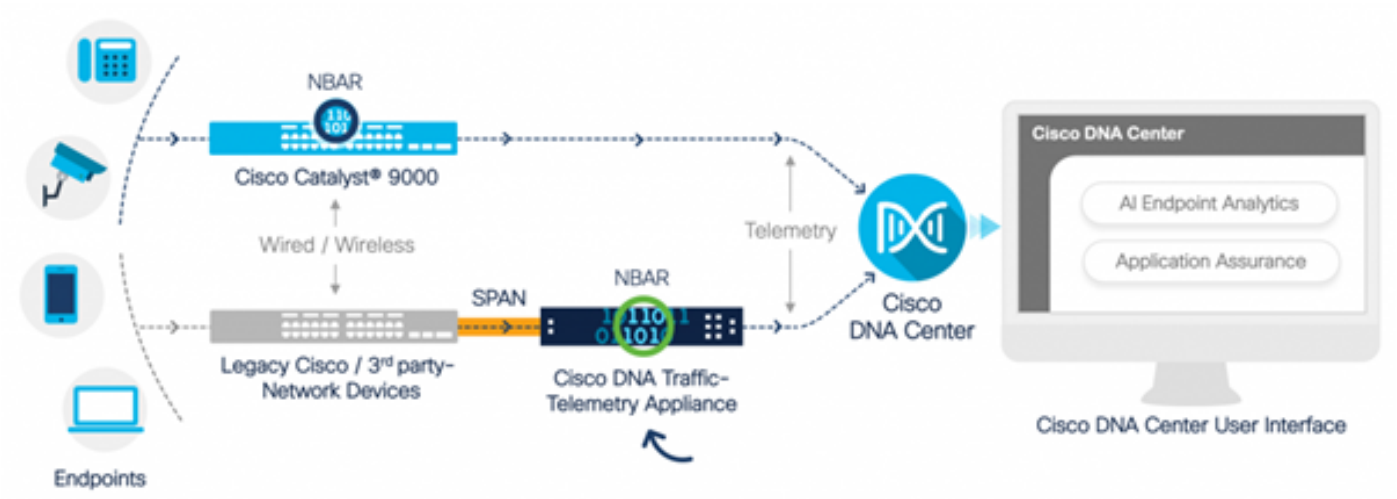
Application Visibilityデータは、Cisco IOS® XEを実行するスイッチおよびAireOSを実行するワイヤレスコントローラから収集されます。 Cisco IOS XEが稼働するスイッチでは、アプリケーションの可視性データは、物理層のアクセススイッチポートに双方向（入力および出力）で適用される事前定義されたNBARテンプレートを使用して収集されます。 AireOSを実行するワイヤレスコントローラの場合、Application Visibilityデータはワイヤレスコントローラで収集され、ストリーミングテレメトリを使用してこのデータがCisco DNA Centerに転送されます。

アプリケーションエクスペリエンス(AppX)

アプリケーションエクスペリエンスデータは、特にCisco Performance Monitor(PerfMon)機能とCisco Application Response Time(ART)メトリックを使用して、Cisco IOS XEルータプラットフォームから収集されます。 ルータプラットフォームの例としては、ASR 1000、ISR 4000、CSR 1000vなどがあります。Cisco DNA Centerとのデバイスの互換性については、『Cisco DNA Center Compatibility Matrix』を参照してください。

トラフィックテレメトリアプライアンスが選ばれる理由

Cisco Catalyst 9000シリーズの有線およびワイヤレスデバイスは、ディープパケットインスペクション(DPI)を実行し、Cisco AI Endpoint AnalyticsやCisco DNA CenterのApplication Assuranceなどのサービスのデータストリームを提供します。 しかし、ネットワークにテレメトリを抽出するCatalyst 9000シリーズデバイスがない場合はどうすればいいですか。 Cisco Catalyst 9000シリーズプラットフォームに移行されていないネットワークインフラストラクチャの一部を依然として所有している組織もあります。 Catalyst 9000プラットフォームはAppVisテレメトリを生成しますが、AppXの洞察をさらに得るために、Cisco DNAトラフィックテレメトリアプライアンスを使用してこのギャップを埋めることができます。TTAの目的は、SPANポートを介して、アプリケーションエクスペリエンスデータをCisco DNA Centerに提供する機能を持たない他のネットワークデバイスから受信するトラフィックを監視することです。 レガシーインフラストラクチャデバイスは、高度な分析に必要なディープパケットインスペクションを実行できないため、Cisco DNAトラフィックテレメトリアプライアンスを使用して、既存のレガシー展開からAppXテレメトリを生成できます。



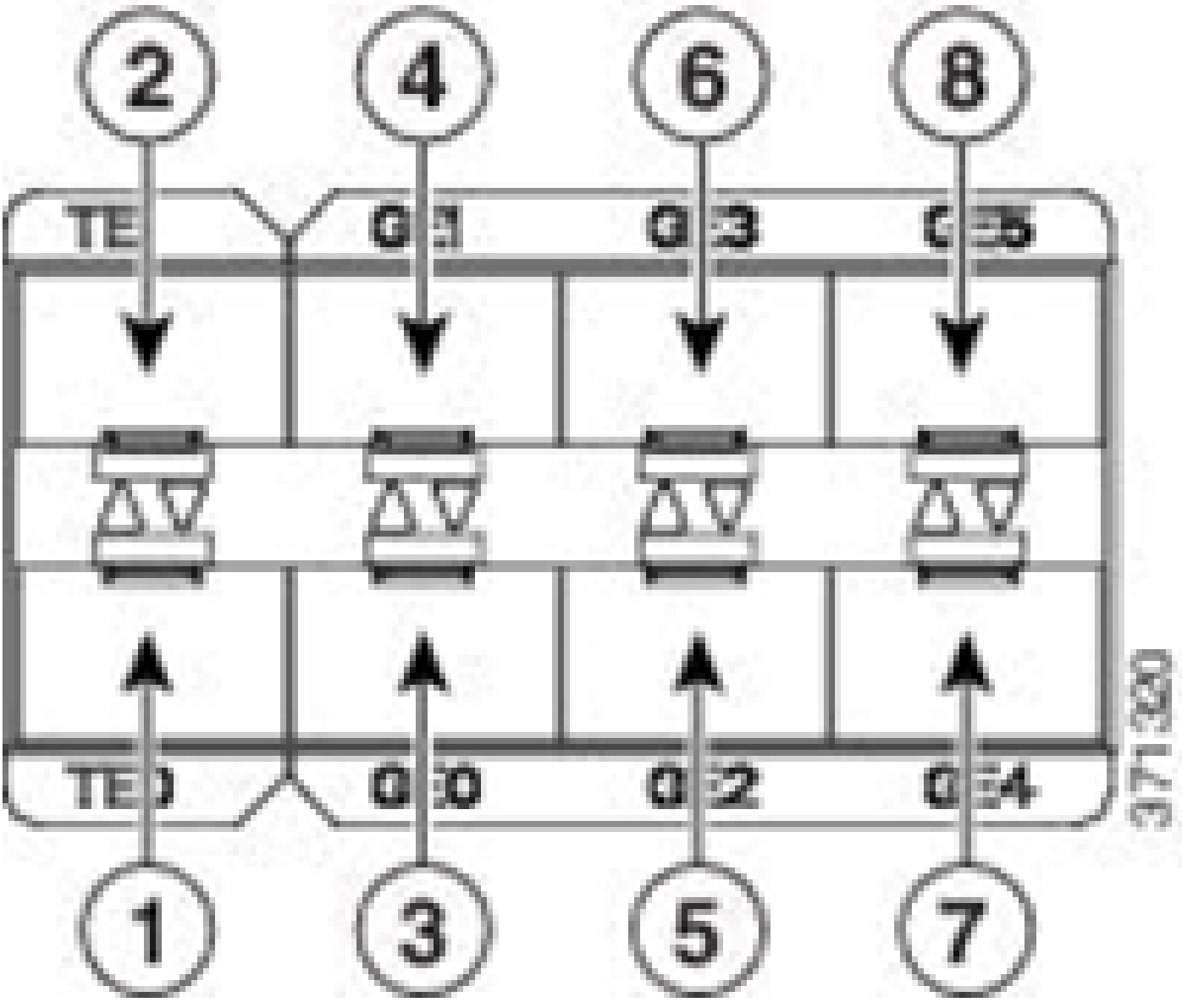
Cisco TTAの動作

TTAデバイスの詳細

Cisco IOS XEベースのテレメトリセンサープラットフォームは、スイッチおよびワイヤレスコントローラのスイッチドポートアナライザ(SPAN)セッションからのミラーリングされたIPネットワークトラフィックからテレメトリを生成します。このアプライアンスは、Network-Based Application Recognition(NBAR)テクノロジーを使用して数千ものプロトコルを検査し、Cisco DNA Center用のテレメトリストリームを生成して分析を行います。Cisco DNAトラフィックテレメトリアプライアンスは、20 Gbpsの持続スループットトラフィックを処理し、40,000のエンドポイントセッションを検査してデバイスプロファイリングを行います。

Ciscoトラフィックテレメトリアプライアンス

TTAには、SPANの取り込みに使用される10-Gigリンクと1-Gigリンクが混在しています。これらのポートのうち、IPアドレスを設定でき、Cisco DNA Centerとの通信に使用できるポートはGig0/0/5だけです。インターフェイスのマトリクスを次に示します。



TTAインターフェイスマトリクス			
1	10 GE SFP+ポート0/0/0	5	GE SFPポート0/0/2
2	10 GE SFP+ポート0/0/1	6	GE SFPポート0/0/3
3	GE SFPポート0/0/0	7	GE SFPポート0/0/4
4	GE SFPポート0/0/1	8	GE SFPポート0/0/5

Cisco DNA Center Assuranceの前提条件

このセクションでは、Cisco DNA Centerがテレメトリを処理する前に満たす必要がある設定と前提条件について説明します。

稼働中のCisco DNA Centerクラスタ

TTAおよびプロセステレメトリの管理に使用するCisco DNA Centerクラスタは、次の基準でプロビジョニングする必要があります。

- ネットワーク階層:設計ワークフローの[ネットワーク階層]セクションを使用して、さまざまな外構キャンパス、これらのキャンパス内の建物、およびこれらの建物内の個々の床を定義し、それらを世界地図に表示します。適切なサイト/ネットワーク階層を設定する必要があります。
- ネットワーク設定:Network Settingsセクションでは、ネットワーク内のデバイスで使用される共通のデフォルトネットワーク設定を作成できます。これらの設定は、グローバルな方法で適用することも、サイトごと、建物ごと、またはフロアレベルごとに適用することもできます。導入の必要に応じて、DNS、ドメイン名、syslog、NTP、タイムゾーン、および口グインバナー情報を入力します。
- Device Credentials:これらのクレデンシャルは、TTAを含むネットワーク内のデバイスにアクセスして検出するために使用されます。Cisco DNA Centerには、適切なCLIとSNMPクレデンシャルを設定する必要があります。 このNetConfクレデンシャルとともに使用すると便利です。
- Cisco CCOアカウント：アプライアンスをテストし、Cisco AIクラウドの機能を活用するには、SWIM用のイメージをダウンロードし、TTAおよびその他のデバイス用のプロトコルパックをダウンロードするには、有効なCCOアカウントが必要です。

ISEとCisco DNA Centerの統合

Cisco Identity Services Engine(ISE)とCisco DNA Centerを統合して、アイデンティティとポリシーを自動化できます。 ISEは、Cisco AI Endpoint Analyticsを活用するために、エンドポイントに関する情報を収集するためにも使用されます。 PxGridは、ISEとCisco DNA Center間の統合を実装するために使用されます。

Cisco DNA CenterとISEの統合要件は次のとおりです。

- pxGridサービスをISEで有効にする必要があります。
- ERSの読み取り/書き込みアクセスを有効にする必要があります。
- ISE管理証明書のサブジェクト名またはSANフィールドには、ISEのIPアドレスまたはFQDNが含まれている必要があります。
- Cisco DNA Centerのシステム証明書には、サブジェクト名またはSANフィールドにCisco DNA CenterのすべてのIPアドレスまたはFQDNが含まれている必要があります。
- ISE ERS管理者クレデンシャルは、ISEとCisco DNA Center間のERS通信の信頼確立に使用されます。
- pxGridノードは、Cisco DNA Centerから到達可能である必要があります。

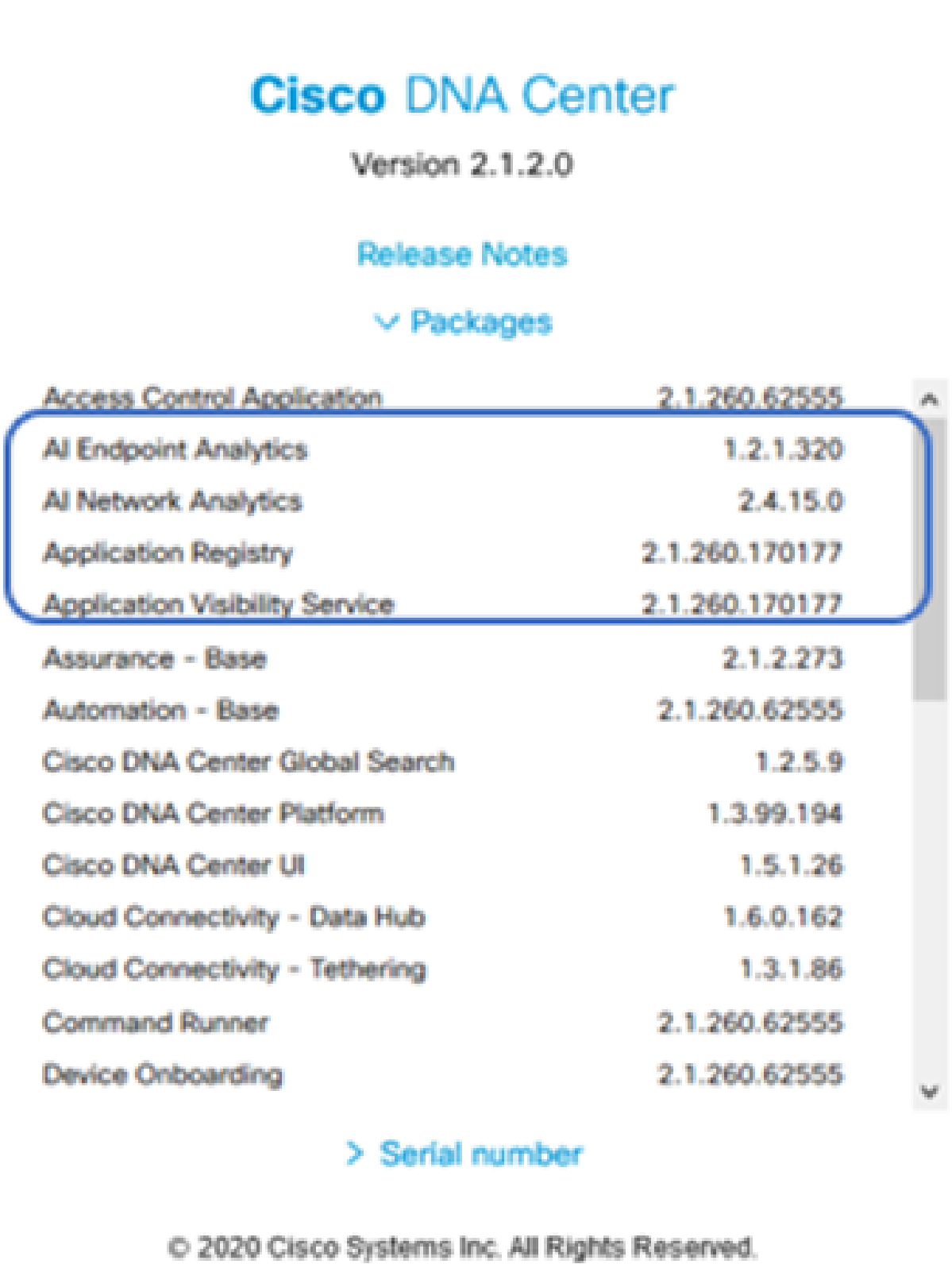
テレメトリのためのCisco DNA Centerの要件

Cisco DNA CenterでApplication Assuranceを有効にするには、実装する必要のある要件があります。これらの要件については、以降のセクションで詳しく説明します。

Cisco DNA Centerキーパッケージ

Cisco DNA Centerでは、テレメトリデータを有効にして分析するために、次の3つのパッケージをインストールする必要があります。

- AIエンドポイント分析
- AIネットワーク分析
- Application Visibilityサービス



必要なCisco DNA Centerパッケージ

この情報にすばやくアクセスするには、Cisco DNA Centerのメインページの右上隅にある疑問符アイコンの下のAboutリンクをクリックします。 これらのアプリケーションが欠落している場合は、テレメトリの設定に進む前にインストールする必要があります。このガイドを使用して、シスコのクラウドからCisco DNA Centerにこれらのパッケージをインストールします。Cisco DNA

Centerアップグレードガイド

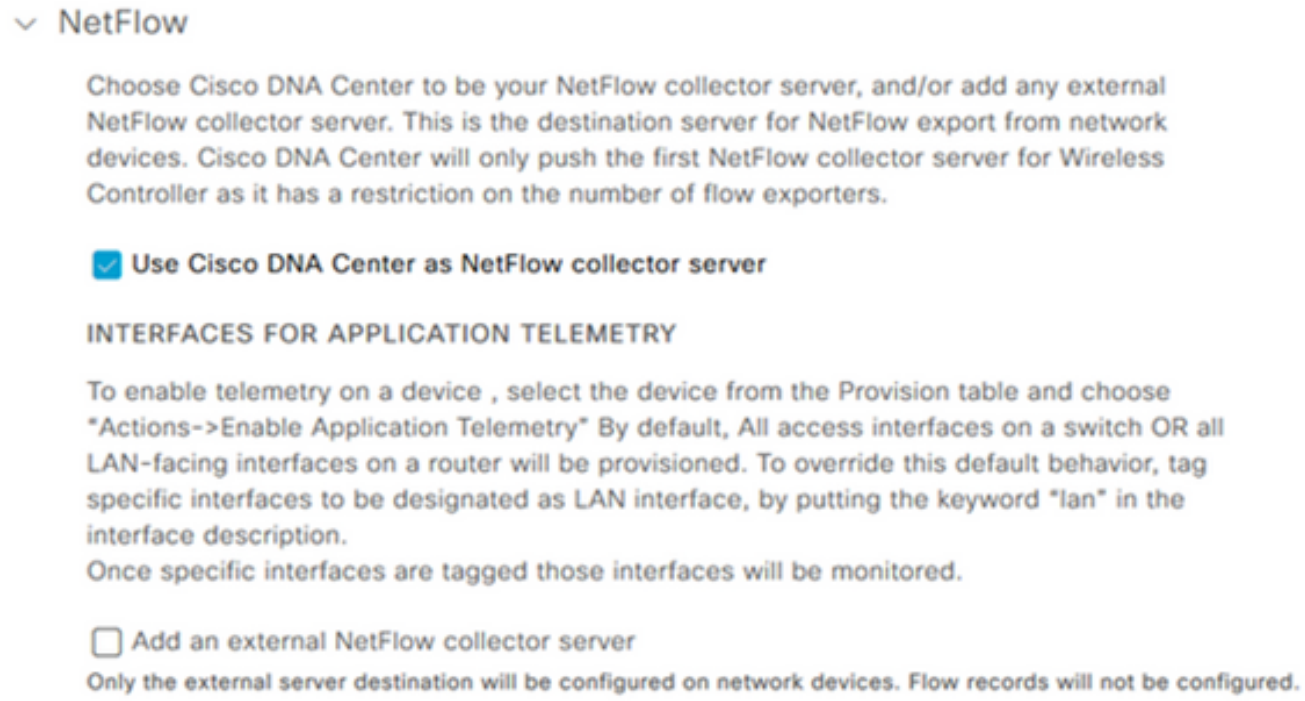
テレメトリコレクタとしてのCisco DNA Center

NetFlowデータエクスポートは、詳細な分析のためにCisco DNA Centerに転送されるテレメトリデータを提供するテクノロジートランスポートです。エンドポイント分析のための機械学習と推論のためのデータ収集を可能にするには、NetFlowをCisco DNA Centerにエクスポートする必要があります。 TTAは、ミラーリングされたIPネットワークトラフィックからテレメトリを生成し、それをアプリケーションおよびエンドポイントの可視性のためにCisco DNA Centerと共有するために使用されるテレメトリセンサープラットフォームです。

- ネットワークトラフィックは、スイッチドポートアナライザ(SPAN)ミラーリングを介してスイッチおよびルータから受信され、Cisco DNAトラフィックテレメトリアプライアンスのミラーリングインターフェイスに送られます。
- Cisco DNAトラフィックテレメトリアプライアンスは、受信したトラフィックを分析して、Cisco DNA Centerのテレメトリストリームを生成します。

Cisco DNA Centerをテレメトリコレクタとして有効にするには、次の手順を実行します。

- Cisco DNA Centerで、Menu > Design > Network Settingsの順にクリックし、Cisco DNA Centerのテレメトリを有効にしてNetFlowを収集します。



NetFlowコレクタとしてのDNACの設定

Cisco AIクラウド

Cisco AI Network Analyticsは、Cisco DNA Center内のアプリケーションであり、機械学習とマシン推論の機能を活用して、ネットワーク展開に固有の正確な洞察を提供します。これにより、問

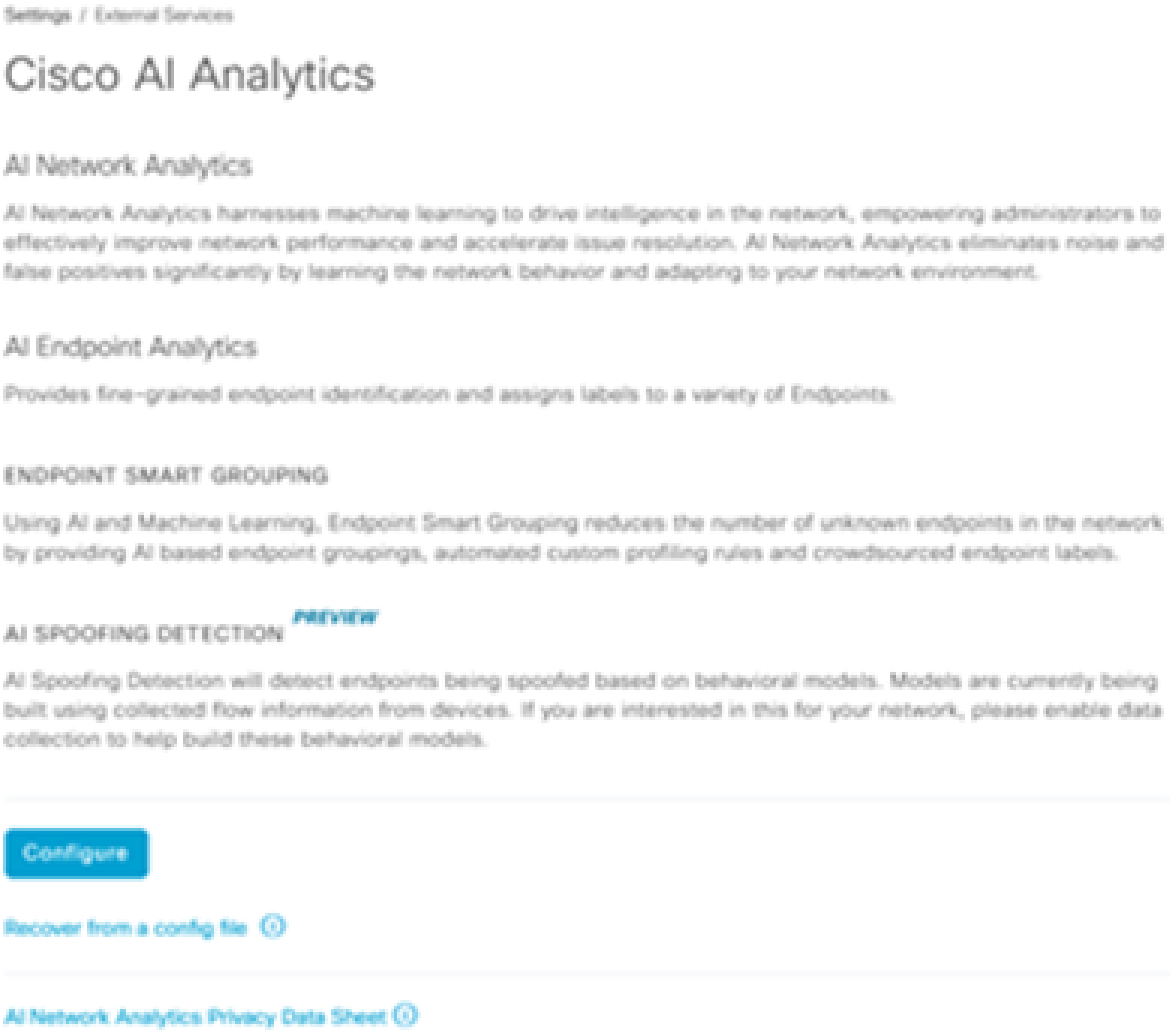
題のトラブルシューティングを迅速に行うことができます。 ネットワークおよびテレメトリ情報は、Cisco DNA Centerで匿名化され、セキュアな暗号化チャネルを通じてCisco AI Analyticsクラウドベースインフラストラクチャに送信されます。Cisco AI Analyticsクラウドは、このイベントデータを使用して機械学習モデルを実行し、問題と全体的な洞察をCisco DNA Centerに返します。 クラウドへのすべての接続は、TCP/443で送信されます。インバウンド接続はなく、Cisco AI CloudはCisco DNA CenterへのTCPフローを開始しません。 この記事の作成時点でHTTPSプロキシやファイアウォールで許可するために使用できる完全修飾ドメイン名(FQDN)は次のとおりです。

- https://api.use1.prd.kairos.ciscolabs.com（米国東部）
- https://api.euc1.prd.kairos.ciscolabs.com（EU中央地域）

導入されたCisco DNA Centerアプライアンスは、シスコがホストするインターネット上のさまざまなドメイン名を解決して到達できる必要があります。

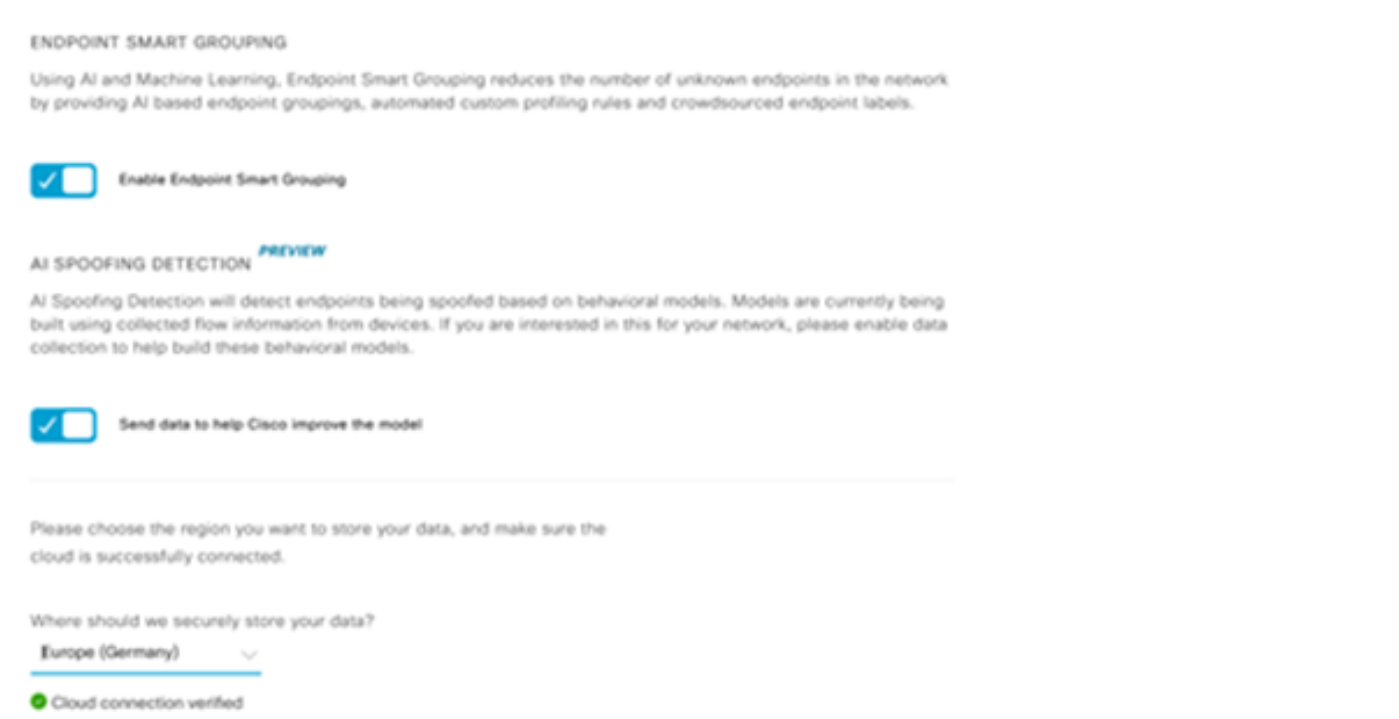
次の手順に従って、Cisco DNA CenterをCisco AI Cloudにテザーします。

- Cisco DNA CenterアプライアンスのWeb UIに移動し、AIクラウドの登録を完了します。
- 移動先 [システム] > [設定] > [外部サービス] > [Cisco AI Analytics]
- Configureをクリックし、Endpoint Smart Grouping and AI spoof detection optionを有効にします。
- Endpoint Smart Groupingは、AI/MLクラウドを使用して不明なエンドポイントをクラスタリングし、管理者がそれらのエンドポイントにラベルを付けるのを支援します。これは、ネットワーク内の正味の未知数を減らすのに非常に役立ちます。
- AIスプーフィング検出は、シスコが追加のNetFlow/テレメトリ情報を収集し、エンドポイントのモデリングに役立ちます。
- 展開する地域に最も近い場所を選択します。クラウド接続の検証が完了し、接続が成功すると、緑色のチェックボックスが表示されます。



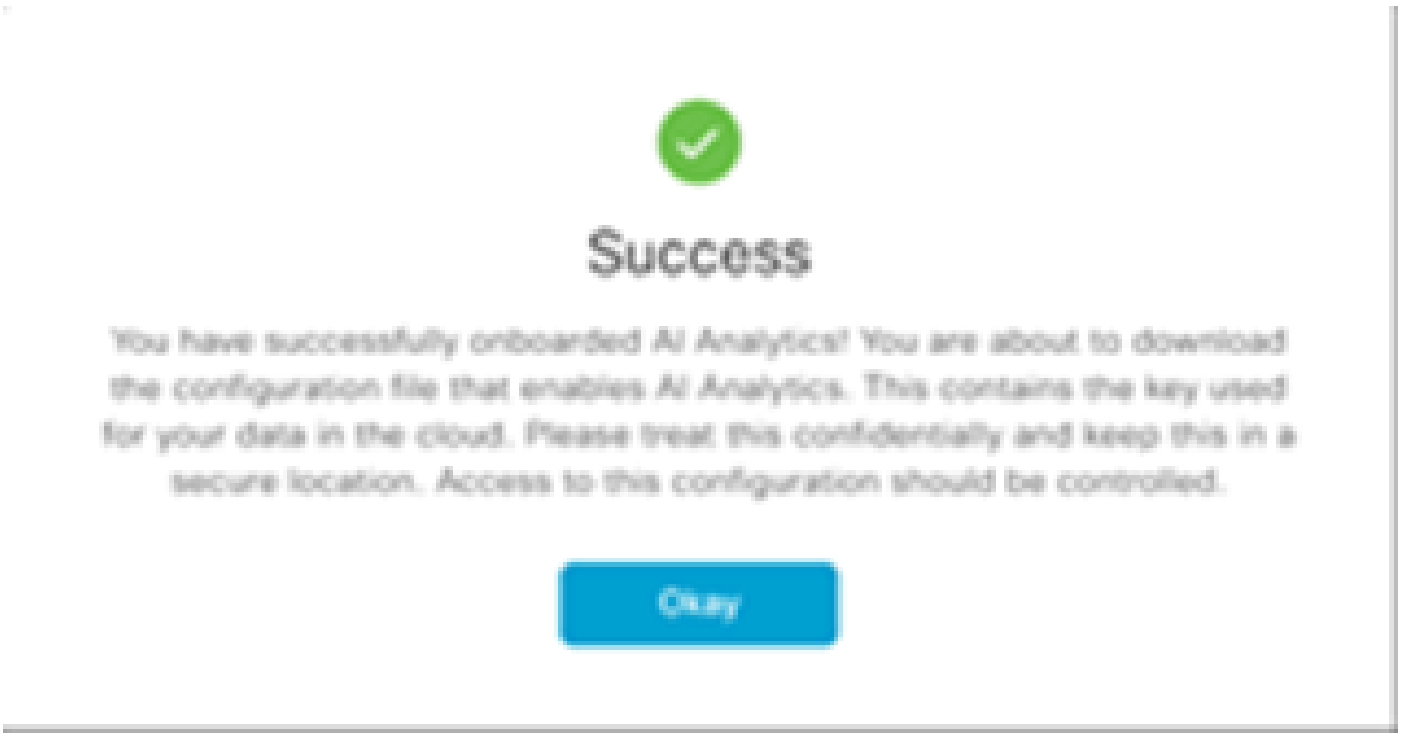
Cisco AI Analytics GUIの設定

- 接続が失敗した場合は、プロキシが使用されているかどうかをSystem > Settings > System Configuration > Proxy configページからCisco DNA Centerのプロキシ設定を確認します。また、この通信をブロックしている可能性があるファイアウォールルールを確認することも推奨されます。



Cisco AI/MLクラウド接続の検証

- Cisco Universal Cloud Agreementに同意してAI Analyticsを有効にします。
- この時点でオンボーディングが完了し、次に示すようにダイアログボックスが表示されます。



登録後の成功ダイアログボックス

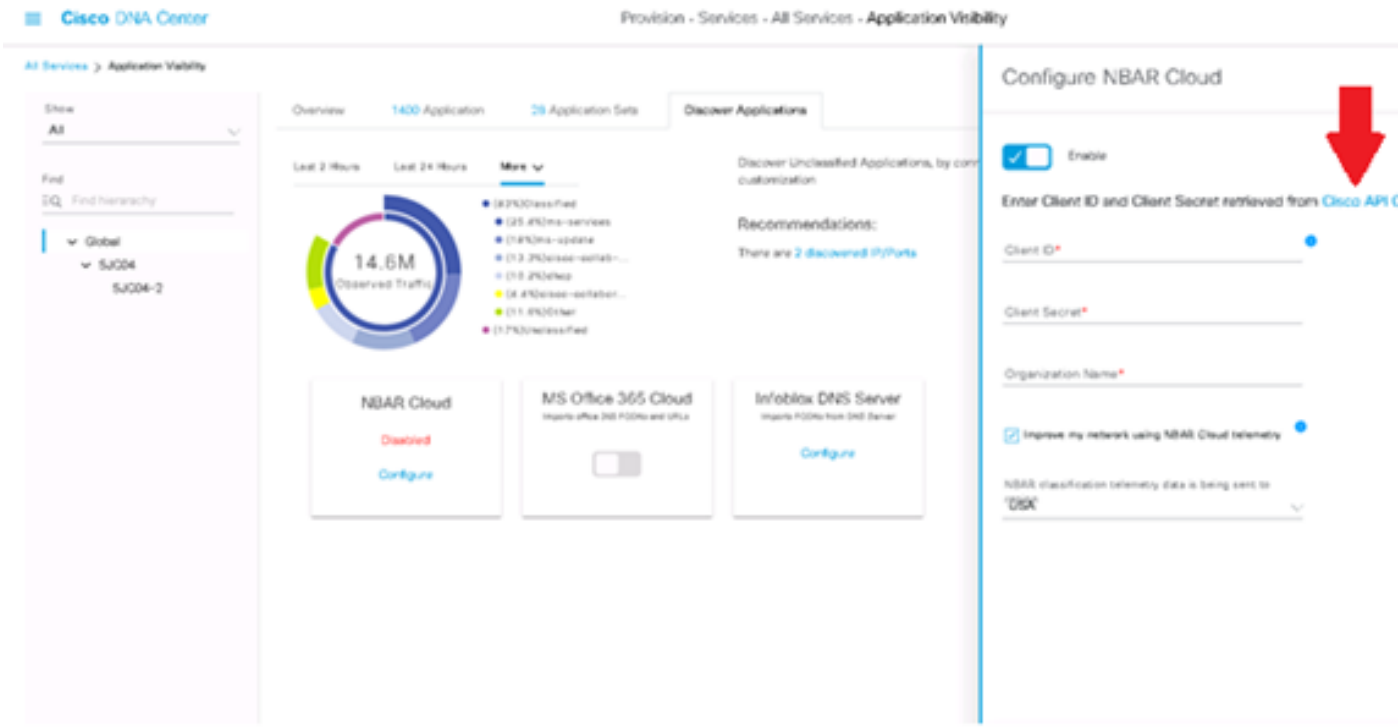
Network Based Application Recognition(NBAR)クラウド

テレメトリアプライアンスとCatalyst 9000プラットフォームは、パケットフローのディープパケットインスペクションを使用してエンドポイントメタデータを収集し、Network Based Application Recognition(NBAR)を適用して、ネットワークで使用されているプロトコルとアプリケーションを判別します。Cisco DNA Centerには、更新可能なNBARプロトコルパックが組み込まれています。テレメトリデータをCisco NBARクラウドに送信して、追加の分析や未知のプロトコルシグニチャの検出を行うことができます。 これを実現するには、Cisco DNA Centerアプライアンスをクラウドに接続する必要があります。Network-Based Application Recognition(NBAR)は、シスコが開発した高度なアプリケーション認識エンジンで、複数の分類技術を使用し、分類ルールを簡単に更新できます。

Cisco DNA CenterをCisco NBARクラウドに接続するには、次の手順を実行します。

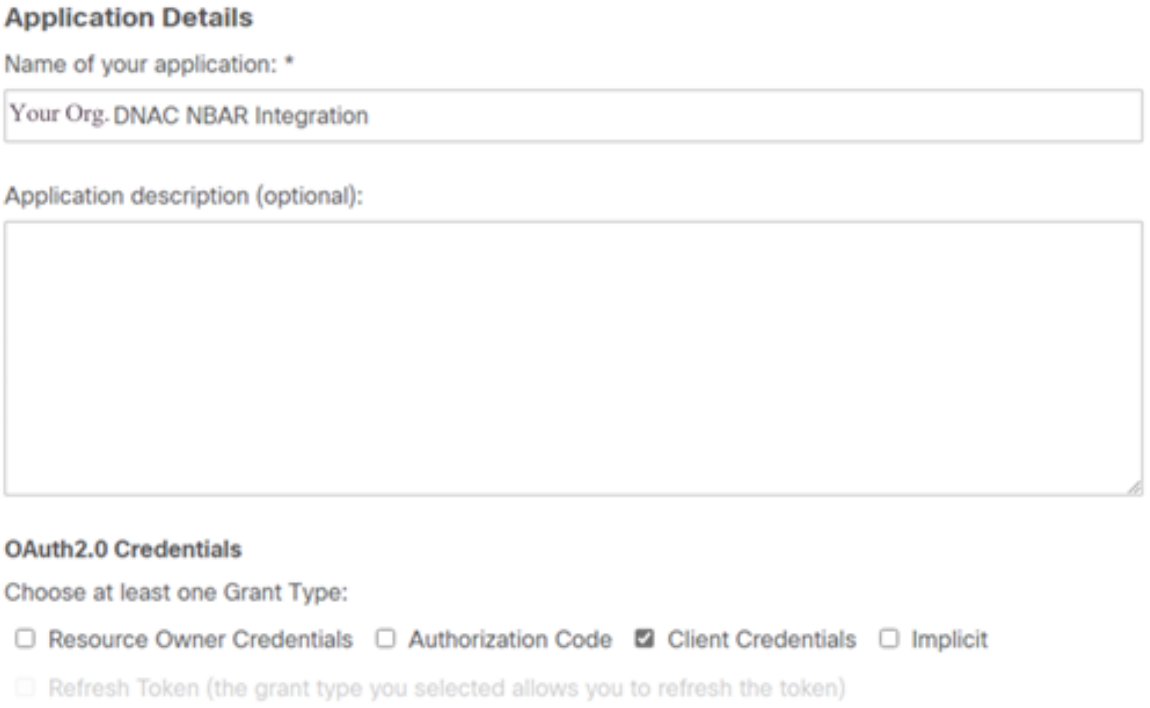
- Cisco DNA CenterのUIで、Provision > Services > Application Visibilityの順に選択します。NBAR Cloudの下のConfigureをクリックすると、パネルが開きます。サービスを有効にします。
- クライアントID、クライアントシークレット、組織名がある場合は、組織や用途に応じて一意の名前を付けてくださいを参照。
- 現時点で利用可能なNBARクラウドのリージョンは米国のみであり、今後さらに多くのリージョンが利用可能になる可能性があります。展開設定で選択して保存します。

クライアントIDとクライアントシークレットのクレデンシャルを取得するには、「Cisco API Console」リンクをクリックします。ポータルが開きます。適切なCCO IDでログインし、新しいアプリケーションを作成し、NBARクラウドに対応するオプションを選択して、フォームに入力します。完了すると、クライアントIDとシークレットが表示されます。次の図を参照してください。



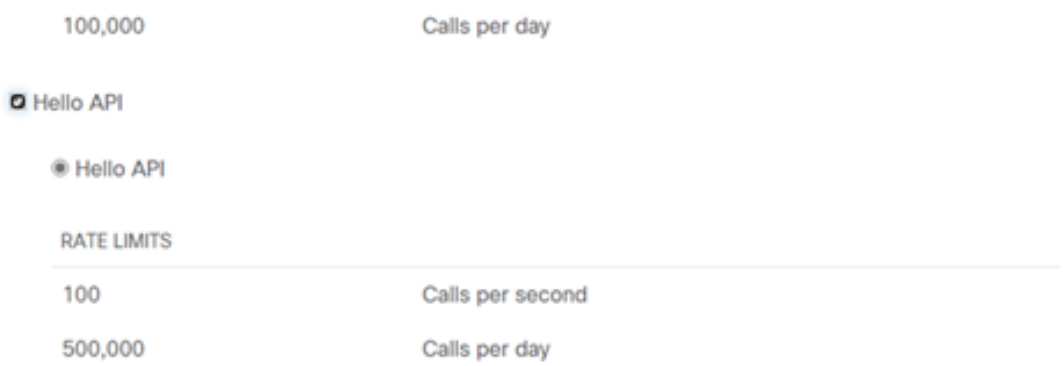
クライアントIDとシークレットを取得するためのCisco APIリンク

次の図は、NBARクラウドへの登録に使用されるオプションを示しています。



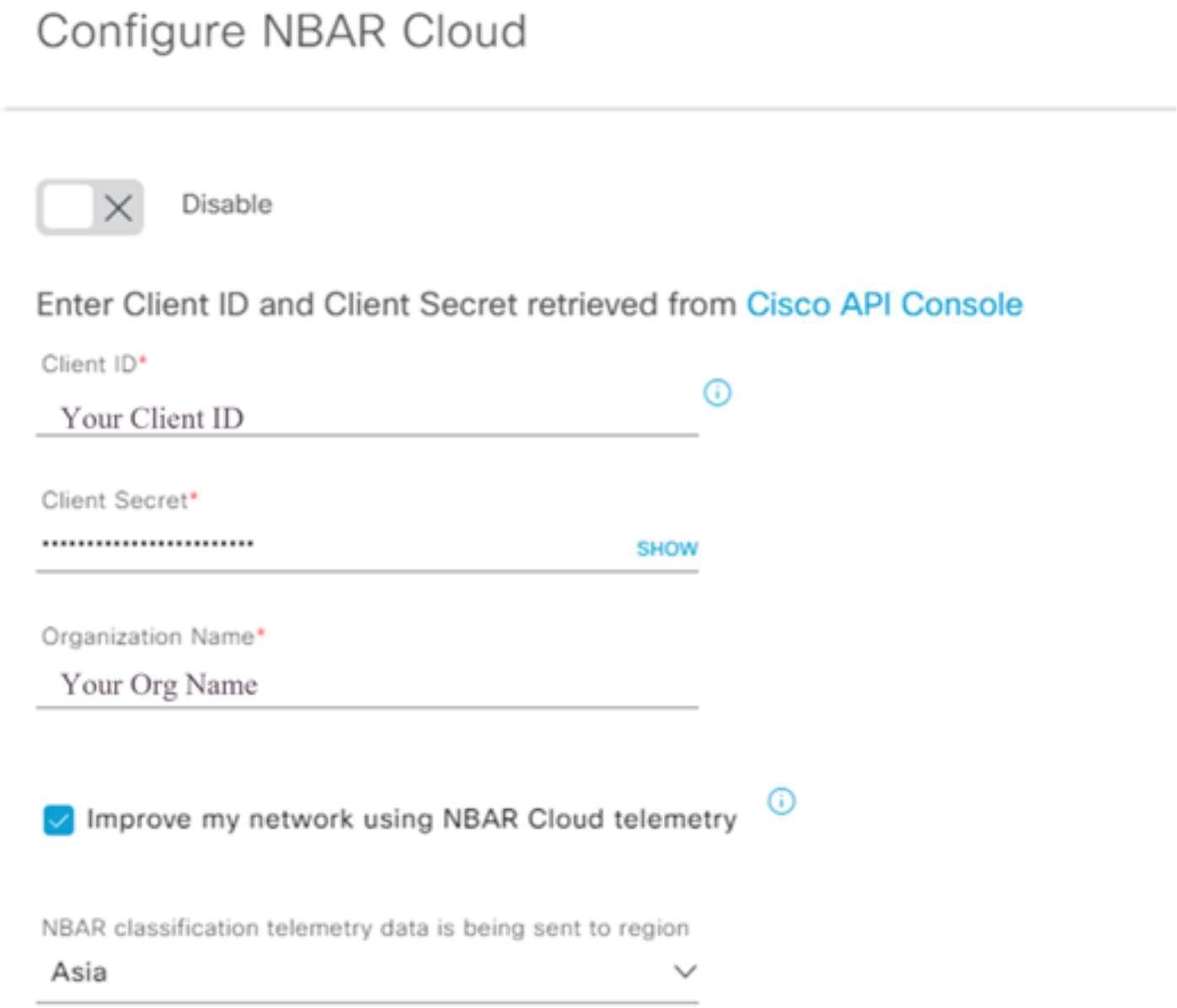
NBARクラウドアプリの詳細

- API要求の詳細を入力する際は、この図を参照用として使用してください。



アプリケーションAPIの詳細

- シスコポータルから取得したクライアントIDとシークレットをCisco DNA Centerに入力します。



DNACでのクライアントIDとシークレットの設定

CBAR(Controller Based Application Recognition)およびSD-AVC

CBARは、何千ものネットワークアプリケーション、自社開発アプリケーション、および一般的なネットワークトラフィックを分類するために使用されます。これにより、Cisco DNA Centerはネットワークインフラストラクチャで使用されるアプリケーションについて動的に学習できます。CBARは、ネットワーク上に存在する新しいアプリケーションが増加し続けていることを特定し、プロトコルパックの更新を可能にすることで、ネットワークを最新の状態に保つのに役立ちます。古いプロトコルパックによってアプリケーションの可視性がエンドツーエンドで失われると、誤った分類が行われ、その後の転送が発生する可能性があります。これにより、ネットワーク内の可視性のホールが発生するだけでなく、キューイングや転送の問題も発生します。

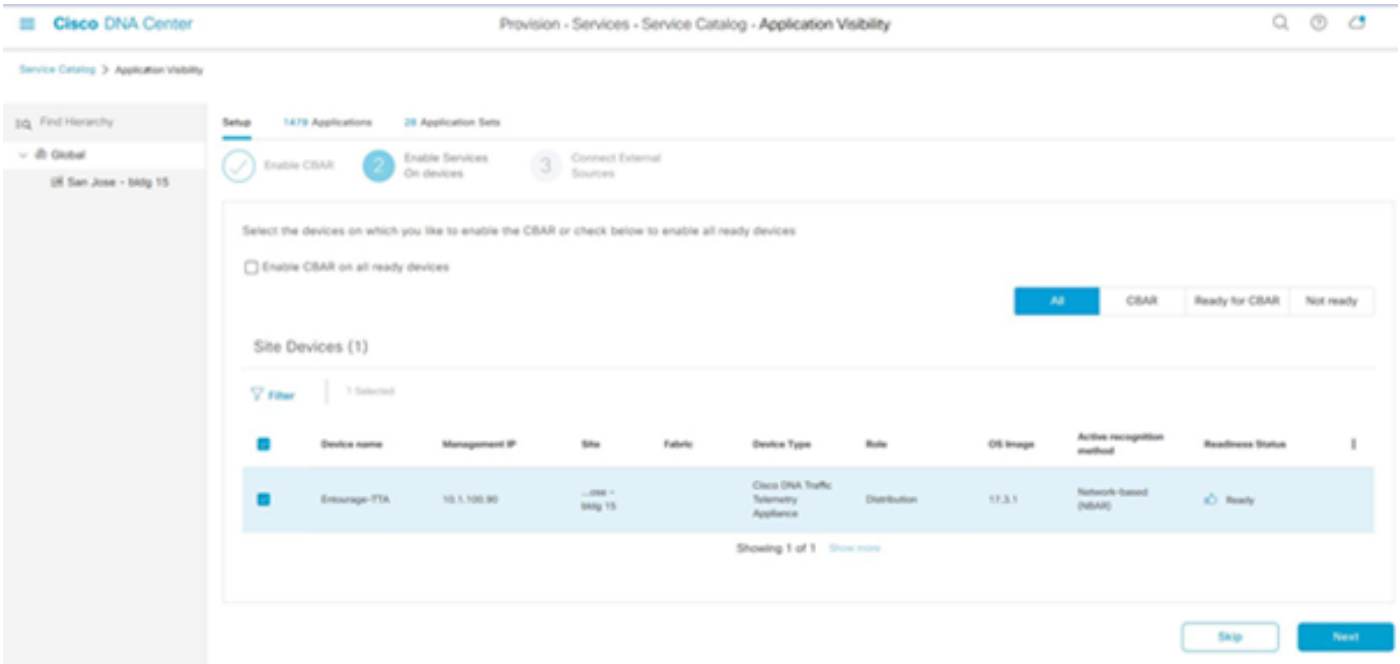
CBARは、更新されたプロトコルパックをネットワーク全体にプッシュできるようにすることで、この問題を解決します。

Cisco Software-Defined AVC(SD-AVC)は、Cisco Application Visibility and Control(AVC)のコンポーネントです。ネットワーク内の特定の参加デバイスで動作する集中型ネットワークサービスとして機能するSD-AVCは、アプリケーションデータのDPIにも役立ちます。SD-AVCの現在の機能と利点には次のようなものがあります。

- ネットワーク全体で一貫したネットワークレベルのアプリケーション認識
- 対称および非対称ルーティング環境におけるアプリケーション認識の向上
- 改善された最初のパケット認識
- ネットワークレベルでのProtocol Packの更新
- SD-AVCの機能と統計情報を監視し、Protocol Packのアップデートをネットワーク全体で設定するための、ブラウザベースのSD-AVCダッシュボード（HTTPS経由）

関連するデバイスに対してCBARを有効にするには、次の手順を実行します。

- Cisco DNA Centerのメニューの**Provision** > **Application Visibility**に移動します。 「アプリケーションの表示/非表示ページを初めて開くと、次に示す設定ウィザードが表示されます。
- 各サイトのCisco DNA Centerでデバイスを検出した後、CBARを有効にするデバイスを選択し、次の手順に進みます。



デバイスでのCBARの有効化

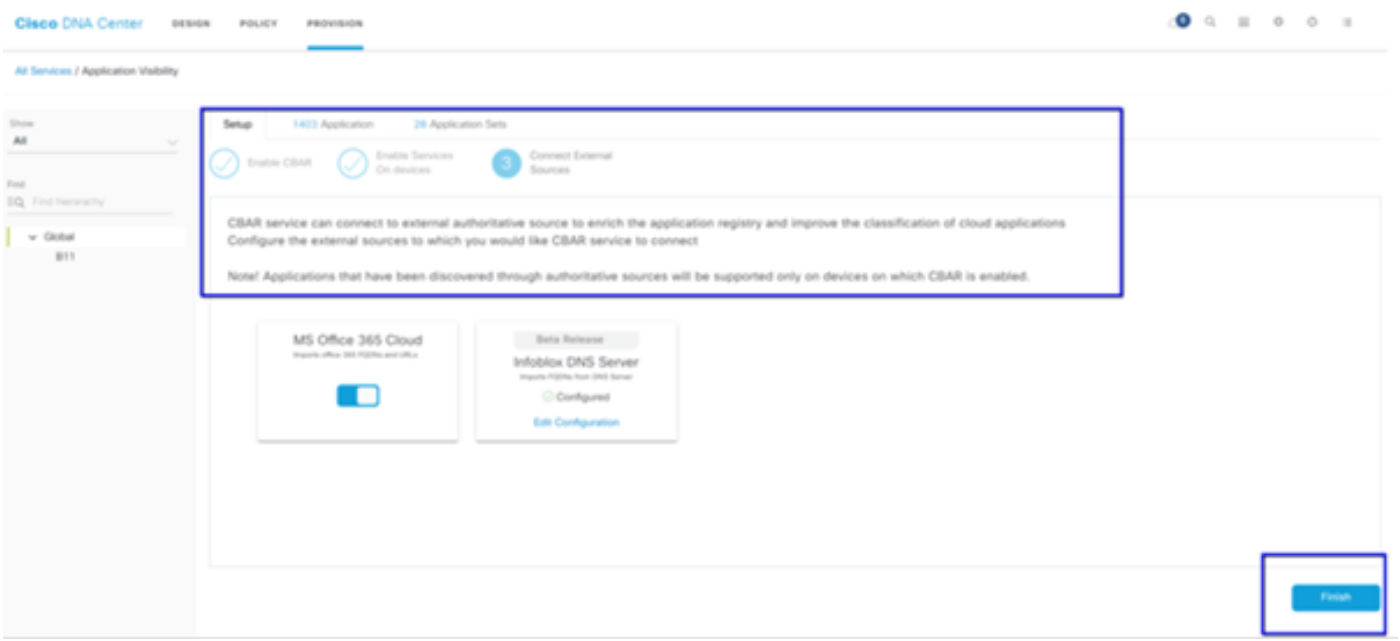
Microsoft Office 365 Cloud Connector（必須ではありません）

Cisco DNA CenterをMicrosoft RSSフィードと直接統合することで、Office 365のアプリケーション認識を公開されているガイダンスに合わせることができます。この統合は、Cisco DNA CenterではMicrosoft Office 365 Cloud Connectorと呼ばれます。ユーザがネットワークでMicrosoft Office 365アプリケーションを実行している場合は、これを導入することをお勧めします。 Microsoft Office 365との統合は必須ではありません。統合を有効にしない場合、Cisco DNA

CenterによるMicrosoft Office 365ホストデータの処理および分類機能にのみ影響します。 Cisco DNA CenterにはすでにMicrosoft Office 365 Application Recognitionが組み込まれていますが、アプリケーションプロバイダーと直接統合することで、Microsoft Office 365スイートで使用されている現在の知的財産ブロックとURLに関する最新かつ正確な情報を入手できます。

Cisco DNA CenterをMicrosoft Office 365 Cloudと統合するには、次の手順を実行します。

- メニューアイコンをクリックし、Provision > Services > Application Visibilityの順に選択します
- Discover Applicationsをクリックします。
- Cisco DNA CenterをMicrosoft Office 365クラウドと統合するには、MS Office 365クラウドの切り替えボタンをクリックします。

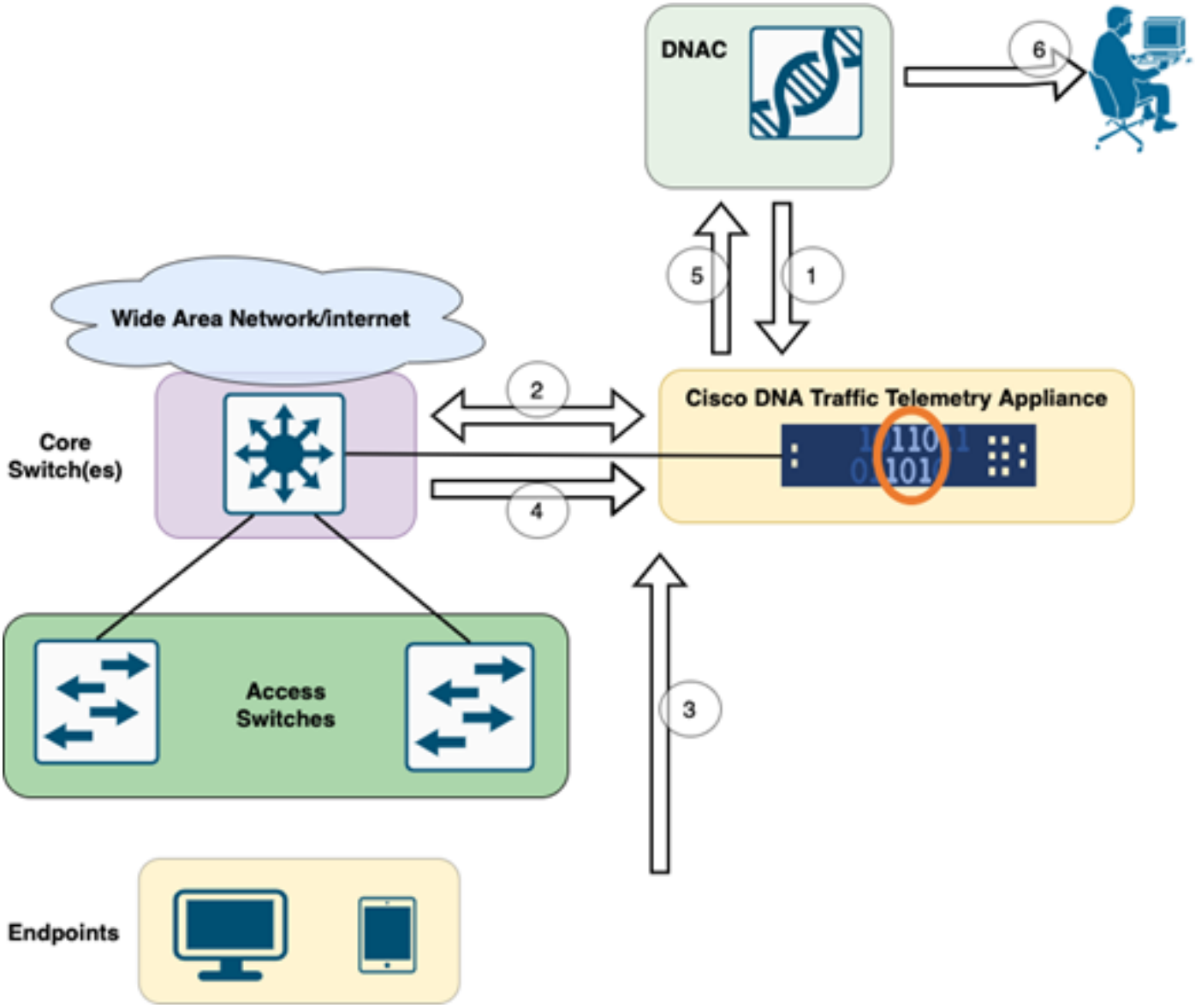


MS O365クラウド統合

TTAの実装

このセクションでは、ネットワークにTTAを実装するために必要な手順について説明します。

TTAワークフローの概要



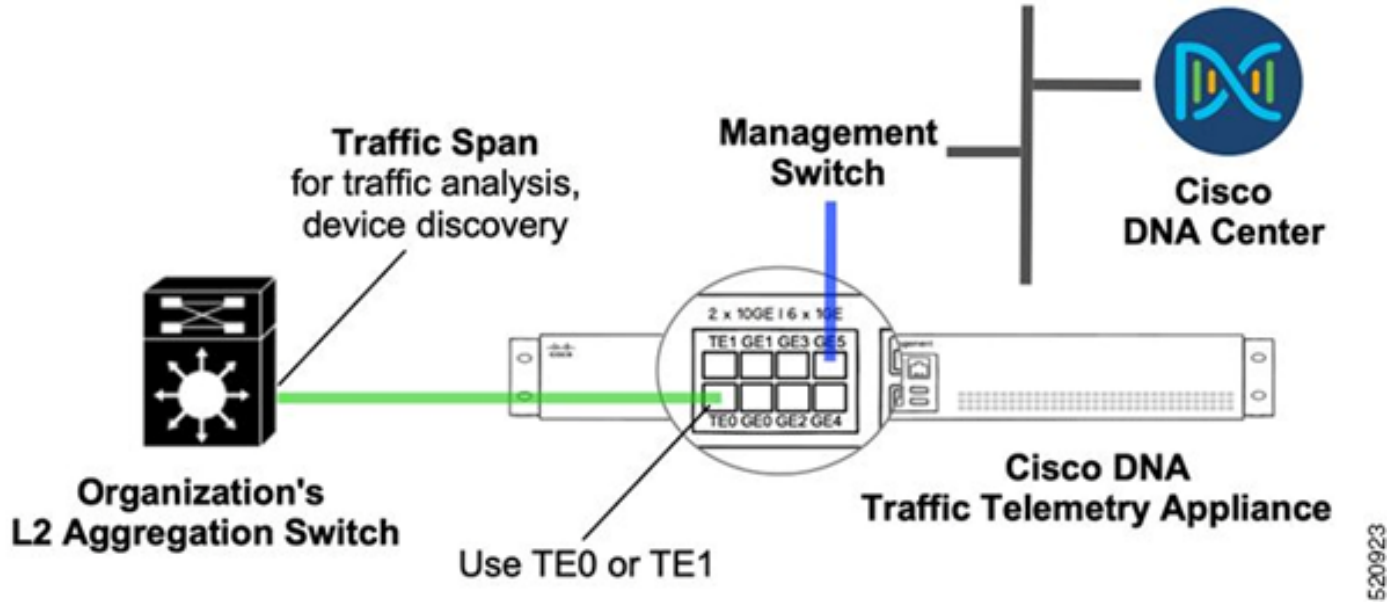
TTAからDNACへのワークフロー

この図で強調表示されている手順は、TTAとCisco DNA Center間のプロセスとテレメトリフローの概要を示しています。 ここでは、これらの手順について詳しく説明します。

1. Ciscoトラフィックテレメトリアプライアンスは、ネットワークインフラストラクチャ内のサイト集約スイッチまたはコアスイッチのいずれかに接続されます。この接続により、アプライアンスはネットワーク内のさまざまなアクセススイッチからトラフィックデータを受信できます。
2. Ciscoトラフィックテレメトリアプライアンスは、ネットワーク管理プラットフォームとして機能するCisco DNA Centerと統合されています。この統合により、アプライアンスとCisco DNA Center間のシームレスな通信とデータ交換が可能になります。
3. ユーザトラフィックがネットワークを通過する際には、Ciscoトラフィックテレメトリアプライアンスにスパニングまたはミラーリングされます。つまり、ネットワークトラフィックのコピーがモニタリングと分析の目的でアプライアンスに送信され、元のトラフィックは通常のパスを維持します。
4. Ciscoトラフィックテレメトリアプライアンスは、受信したトラフィックデータを収集して処理します。パケットレベルの詳細、フロー統計情報、パフォーマンスメトリックなどの関連情報を、ミラーリングされたトラフィックから抽出します。

5. 処理されたテレメトリ情報は、Ciscoトラフィックテレメトリアプライアンスから Cisco DNA Centerに送信されます。この通信により、Cisco DNA Centerは、ネットワークのトラフィックパターン、アプリケーションパフォーマンス、異常に関するリアルタイムの洞察と更新を受け取ることができます。
6. Cisco DNA Centerによって生成されたテレメトリの洞察は、ネットワーク管理者に有益な情報を提供します。Cisco DNA Centerのインターフェイスを使用して、収集されたデータの表示と分析、ネットワークの健全性とアプリケーションパフォーマンスの可視化、潜在的な問題の特定、およびネットワークの最適化とトラブルシューティングに関する情報に基づいた決定を行うことができます。

TTAの導入：概要図



TTAの導入：概要

上の図は、TTAをネットワークに接続する方法を示しています。10-Gigおよび1-Gigインターフェイスは、ラインレートでのSPANの取り込みに使用できます。Gi0/0/5インターフェイスは、Cisco DNA Centerとの通信、オーケストレーション、およびCisco DNA Centerへのテレメトリ情報の転送に使用されます。このインターフェイスは、SPANの取り込みに使用できません。

TTAソフトウェアおよびライセンス要件

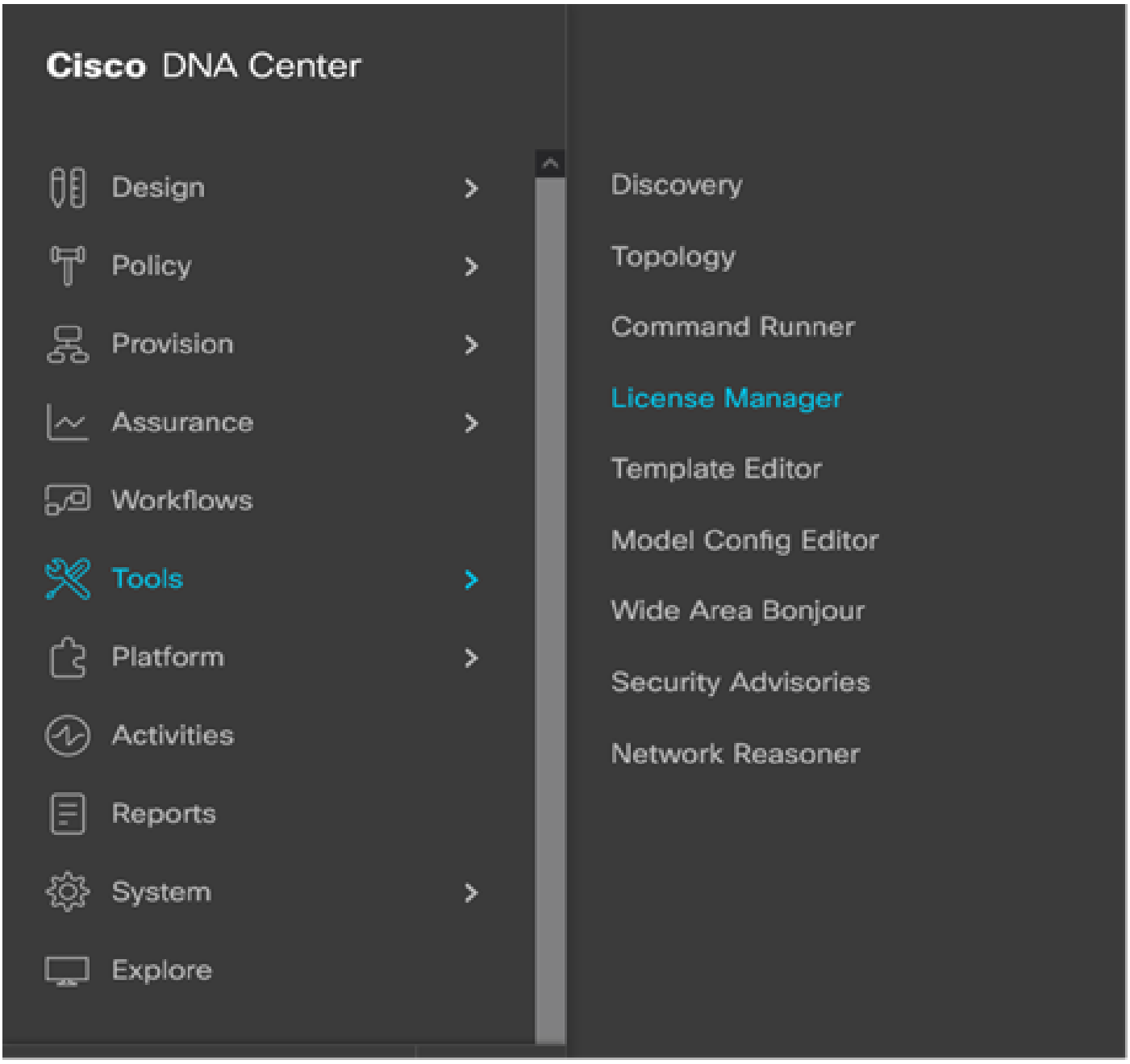
ネットワークに導入されたTTAアプライアンスは、ユーザデータとユーザエンドポイントに関するテレメトリの洞察を提供するために不可欠です。ソリューションを正常に導入するには、これらの要件を満たす必要があります。

- Cisco DNA Center（TTAブートストラップ設定）で検出できるように、TTAを初期ブートストラップ設定で設定する必要があります
- TTAアプライアンスをCisco DNA Centerにオンボーディングして、Cisco DNA Centerで管理できるようにする必要があります（Cisco DNA Centerインベントリへのテレメトリボックスの追加）
- 正しいライセンスをTTA（TTAアプライアンスのライセンス）にインストールする必要があ

ります

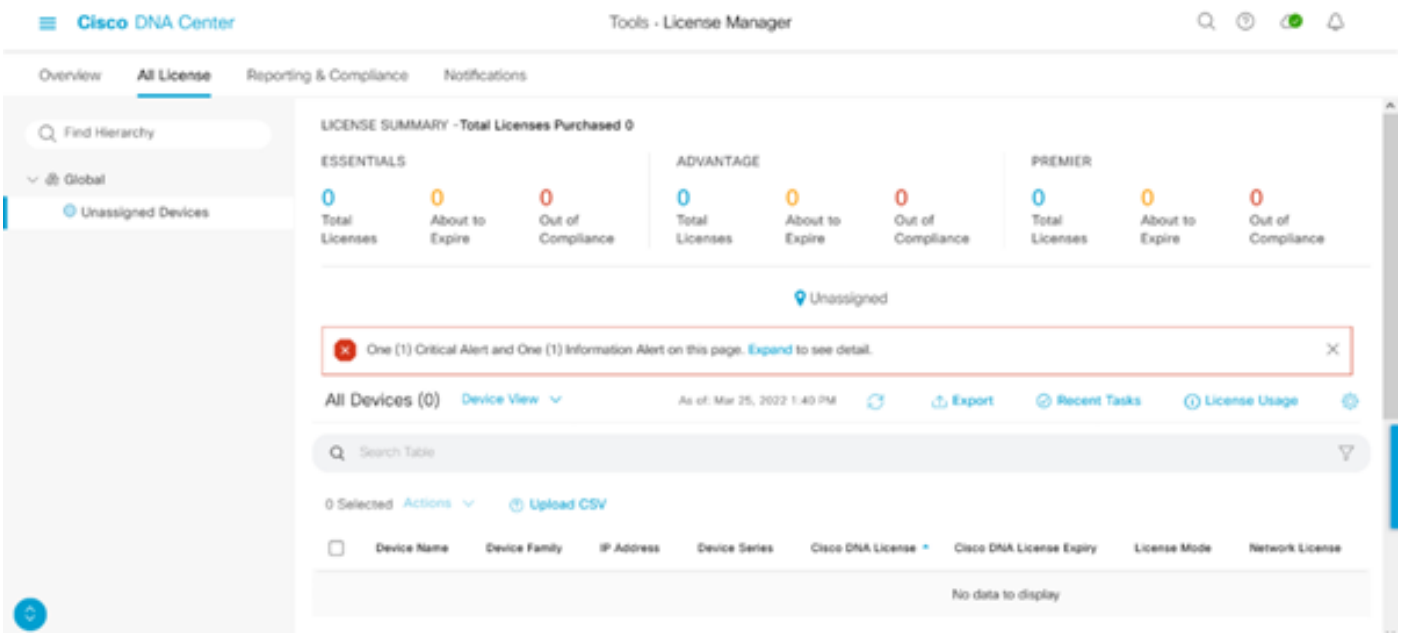
このアプライアンスは1つのオペレーティングシステムのみをサポートし、テレメトリを収集するにはCisco DNA TTA Advantageライセンスが必要です。 フィーチャライセンス（IP BaseやAdvanced IP Servicesなど）や永久ライセンスパッケージ（Network EssentialsやNetwork Advantageなど）は必要ありません。

Cisco DNA Centerでライセンスを管理するには、メニューアイコンをクリックして、Cisco DNA Centerのドロップダウンメニューから**Tools > License Manager**に移動し、ライセンスマネージャに移動します



DNACのLicense Manager

- All Licenseページに移動します。次の図のようになります。このページでは、管理者はTTAと同様にネットワークデバイスライセンスを管理できます。



DNACのすべてのライセンスページ

TTAオンボーディングおよびDay-0設定

Cisco DNA CenterによるTTAアプライアンスの検出とオンボーディングを容易にするために、サイトのTTAアプライアンスで設定する必要があるブートストラップコマンドがあります。ブートストラップの設定が完了すると、Cisco DNA Centerのダッシュボードから TTAを検出できるようになります。TTAアプライアンスの0日目の設定項目を次に示します。 デバイスがサイト階層にオンボーディングされると、TTAアプライアンスはCisco DNA Centerから残りの設定項目を継承します。

```
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
```

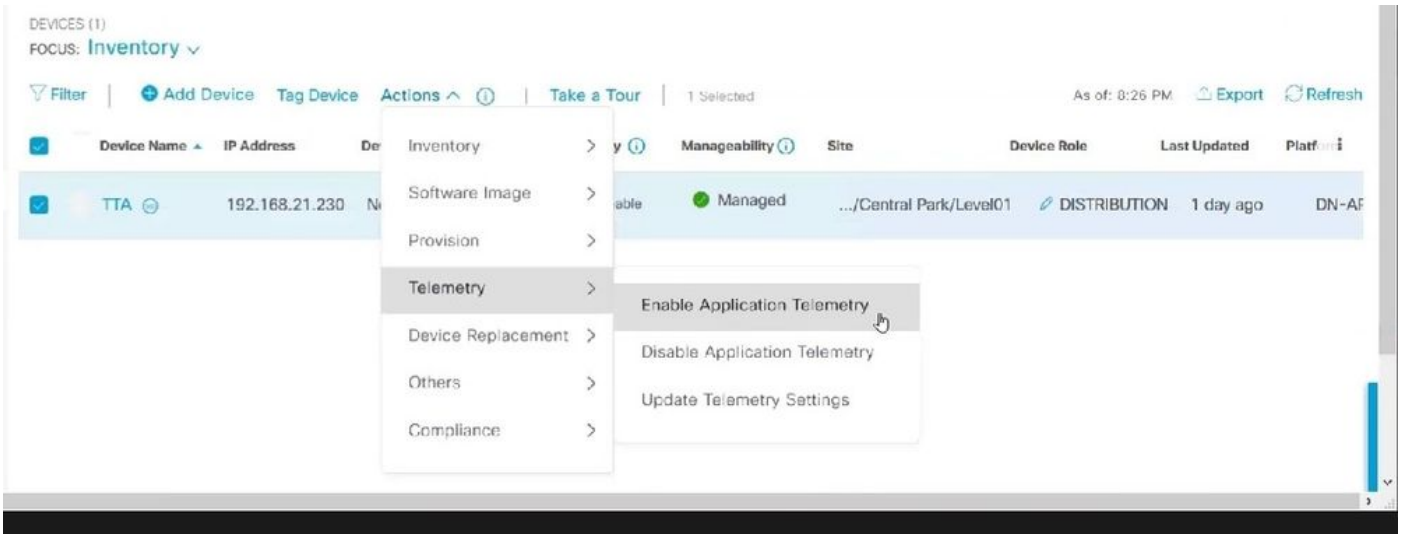
```
ip ssh source-interface GigabitEthernet0/0/5

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
```

これらの項目をTTAに設定すると、Cisco DNA Centerで検出できるようになります。

Cisco DNA CenterのインベントリへのTTAアプライアンスの追加

TTAを活用するには、Cisco DNA CenterがTTAアプライアンスを検出して管理する必要があります。TTAがCisco DNA Centerにオンボーディングされると、Cisco DNA Centerから管理できるようになります。 TTAアプライアンスを検出する前に、サイトの階層全体がサイトに適していることを確認する必要があります。その後、Menu > Provision > Devices > Inventoryページで次の手順に従って、特定のサイト階層の下にTTAアプライアンスを追加し、サイトにデバイスを追加します。

1. デバイスへの接続に必要なユーザ名/パスワード(CLI)とSNMPコミュニティ、およびイネーブルパスワードを入力します。続行する前に、デバイスが正常に追加されるまで待ちます。
2. デバイス名、ファミリ（TTAの場合はネットワーク管理）、到達可能性 – 到達可能、管理可能、デバイスロール – ディストリビューションを確認します。デバイスは最初は「非準拠」ですが、完全にプロビジョニングされるとステータスが変わります。
3. TTAがオンボーディングされると、Cisco DNA Centerは設定テンプレートをプッシュして、高度なテレメトリ機能を設定します。



TTAの検出とアプリケーションテレメトリの有効化

SPAN Configuration

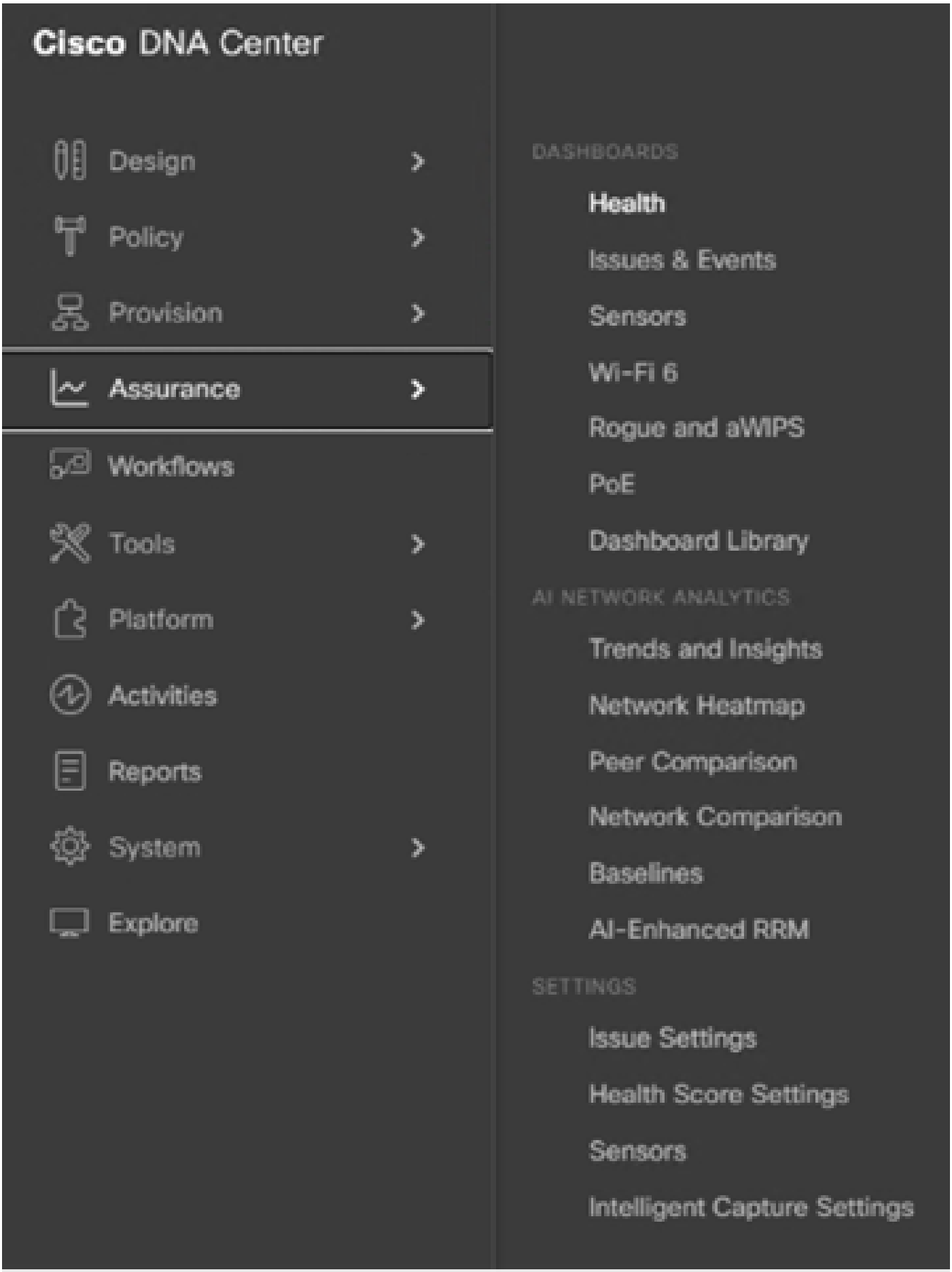
コアスイッチのハードウェア機能に応じて、VLANのグループまたはインターフェイスをTTAに接

続されたインターフェイスにSPANするようにSPANセッションを設定できます。設定例を次に示します。

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

アシュアランスの収集

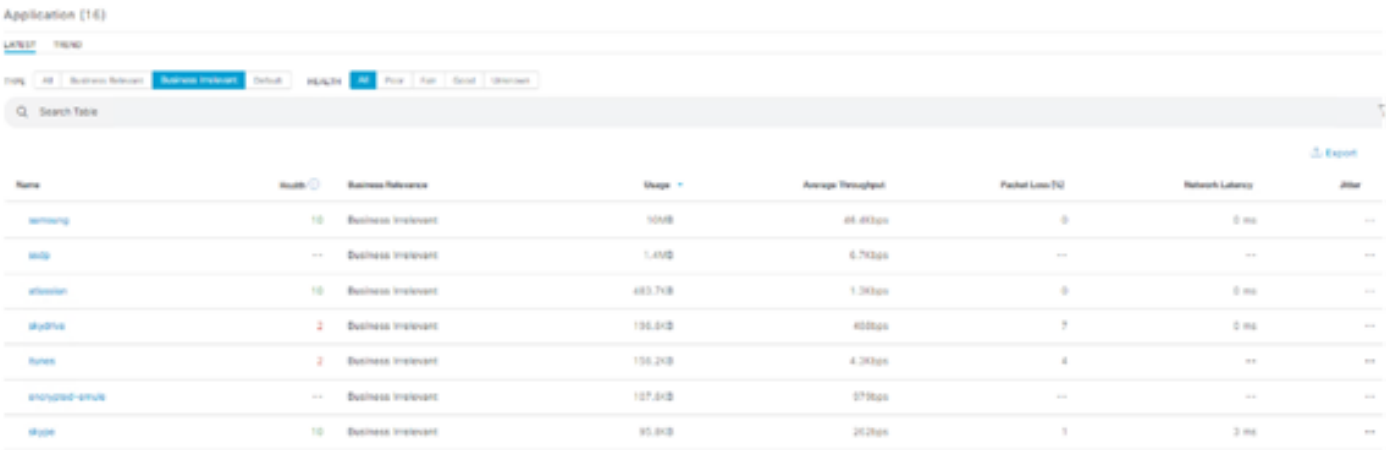
インストール済みのトラフィックテレメトリアプライアンスから収集された保証データにアクセスするには、保証セクションに移動し、健全性をクリックします。



App Assuranceへの移動

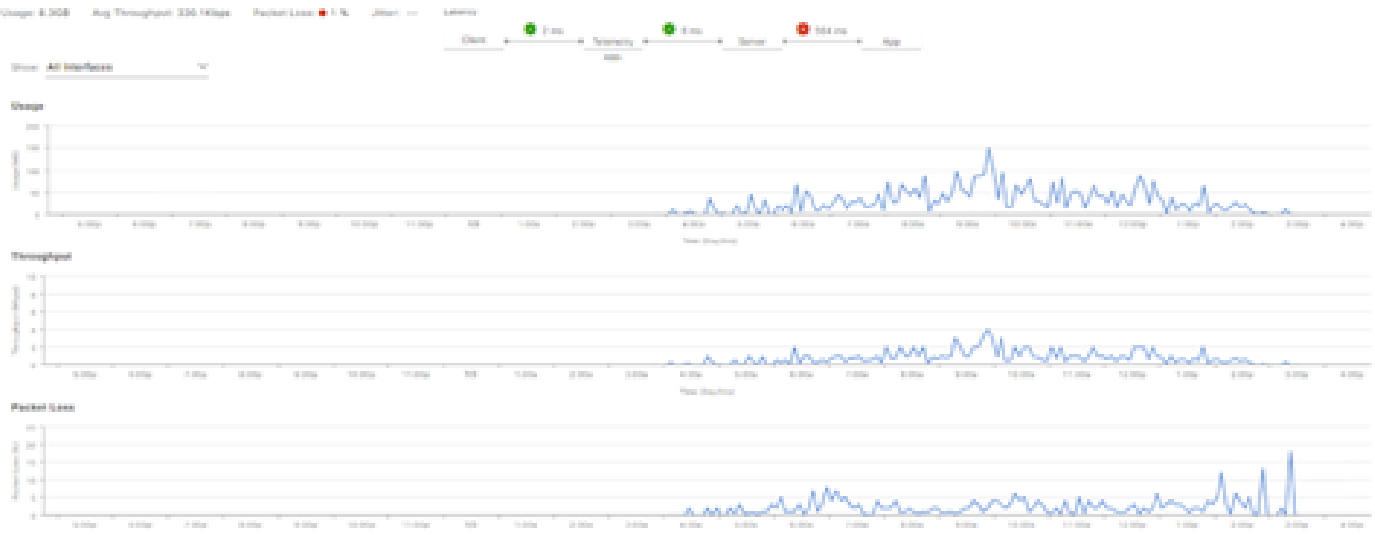
Applicationsを選択すると、特定のアプリケーションタイプに基づいてTTAによってキャプチャされた遅延やジッタなど、アプリケーションデータの包括的な概要が表示されます。

Application Assuranceへの移動



詳細なApplication Assurance UI

より詳細な分析を行うには、特定のアプリケーションをクリックし、トラフィックテレメトリアプライアンスとしてエクスポータを選択して個々のアプリケーションを調べ、使用状況、スループット、パケット損失データ、クライアントネットワーク遅延、サーバネットワーク遅延、アプリケーションサーバ遅延などの特定のメトリックを調べます。



例：申請事項Pt.1

例：申請事項Pt.2

確認

1. CBARを有効にした後、Ciscoトラフィックテレメトリアプライアンスにログインして次のCLIコマンドを実行し、デバイスでSD-AVC(Application Visibility Control)サービスが有効になっていることを確認します。出力は次の例と同様で、コントローラのIPアドレスとステータスがconnectedであることを示します。

```
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. TTAのCLIで「show license summary」コマンドを使用して、関連するデバイスライセンスの詳細を確認します。

```
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.コア/アグリゲーションスイッチでSPANセッションが正しく設定されていることを確認します。

```
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. TTAが正常にプロビジョニングされると、これらのコマンドがデバイスにプッシュ（またはプッシュ）されます。

```
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
```

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。