



Cisco Nexus Data Broker 組み込み型： 実装クイック スタート ガイド

目次

概要	2
Cisco Nexus Data Broker ソリューションの概要	2
Cisco Nexus Data Broker ソリューションのラボ セットアップ トポロジ	3
Cisco Nexus 3000 シリーズおよび Cisco Nexus 9300 プラットフォーム スイッチの OpenFlow 用 Cisco プラグインの有効化	5
OpenFlow 用 Cisco プラグインのハードウェア サポートの有効化	5
OpenFlow 用 Cisco プラグインのインストールとアクティブ化	6
OpenFlow 用 Cisco プラグインの設定	7
Cisco NX-API モード用 Cisco Nexus 9300、Cisco Nexus 3100 および Cisco Nexus 3200 シリーズ スイッチの設定の有効化	8
Cisco Nexus 3000 シリーズおよび Cisco Nexus 9300 シリーズ スイッチの Cisco Nexus Data Broker 組み込み型ソリューションの有効化	10
Cisco Nexus Data Broker 組み込み型ソリューションのインストールとアクティブ化	10
Cisco Nexus Data Broker 組み込み型ソリューションへのスイッチの接続ステータスの確認	11
最初の Cisco Nexus Data Broker 組み込み型の設定	11
Cisco Nexus Data Broker の設定	12
ポートタイプの設定とモニタリング ツールのマッピング	12
エッジ ポートの設定	13

配信ポートの設定	13
ネットワークトラフィックをマッチングするフィルタの設定	13
まとめ	16
関連情報	16

概要

このドキュメントでは、テスト アクセスポイント(TAP)および Cisco Switched Port Analyzer (SPAN) アグリゲーション用の 1 つの Cisco Nexus 3000 シリーズ スイッチまたは Cisco Nexus 9300 プラットフォーム スイッチを使用した、ネットワークトラフィックの可視性のためのオンスイッチ導入オプションである、Cisco Nexus® Data Broker 組み込み型ソリューションの実装のクイックスタート構成ガイドを示します。このドキュメントには、次の設定手順が含まれます。

- Cisco Nexus 3000 シリーズおよび Cisco Nexus 9300 プラットフォーム スイッチでの OpenFlow 用の Cisco® プラグイン
- Cisco Nexus 3000 シリーズおよび Cisco Nexus 9300 プラットフォーム スイッチでの Cisco Nexus Data Broker アプリケーション
- Cisco Nexus 3000 および Cisco Nexus 9300 シリーズ スイッチでの Cisco NX-API の設定

免責事項:このドキュメントは、製品向けに公開された構成ガイドを置き換えるものではありません。該当する構成ガイドの一覧については、このドキュメントの最後にある「[関連情報](#)」のセクションを参照してください。

Cisco Nexus Data Broker ソリューションの概要

Cisco Nexus Data Broker は、ネットワーク TAP および SPAN アグリゲーション用の 1 つ以上の Cisco Nexus 3000 または 9000 シリーズ スイッチで、専用のマトリックス ネットワークを置き換えます。トラフィックはこの一連の Cisco Nexus 3000 または 9000 シリーズ スイッチに、マトリックス ネットワークの場合と同様に入っていきます。ただし、Cisco Nexus Data Broker アプリケーションでは、トラフィックはフィルタリングされ適切なツールに転送できます。フィルタリング ルールと転送ルールはビジネス ロジックに基づいて動的に変更され、リアルタイムでツールに直接流れるような特有のトラフィック パターンが可能になります。さらに、Cisco Nexus Data Broker は Java および Representational State Transfer (REST) のような共通プログラマブル インターフェイスをサポートするため、ネットワーク オペレータはカバレッジギャップを埋める特有のトラフィックを検出して捕捉するアプリケーションを記述できます。

1 つの Cisco Nexus 3000 シリーズまたは Cisco Nexus 9300 プラットフォーム スイッチをネットワークで使用して、Cisco Nexus Data Broker を実行したいお客様には、組み込みモードを使用してスイッチ自体の Linux コンテナで Cisco Nexus Data Broker を実行するオプションがあります。Cisco Nexus Data Broker 組み込み型ソフトウェアは Cisco Nexus スイッチの Linux コンテナに展開可能なオープン仮想アプライアンス(OVA)として配布されます。このオプションでも次のものを除く Cisco Nexus Data Broker のすべての機能が利用できます。

- クラスタリングと高可用性
- ネットワーク TAP または SPAN アグリゲーション用の複数のスイッチの管理

表 1 に、Cisco Nexus Data Broker 組み込み型ソリューションで使用できる主要な機能をまとめます。

表 1 主要な機能

機能	利点
さまざまなポート容量に対応	<ul style="list-style-type: none"> • Data Broker は 1、10、40、および 100 Gbps のポートに対応しています。
TAP および SPAN アグリゲーションのサポート	<ul style="list-style-type: none"> • ポートをモニタリング ツール ポートまたは入力 TAP ポートおよび入力 SPAN ポートとして設定できます。 • エンドデバイス名をトポロジ内で容易に識別できるよう設定できます。
入力ソースの TAP ポートおよび SPAN ポート* をタグ付けする IEEE 802.1 Q-in-Q のサポート	<ul style="list-style-type: none"> • 入力 TAP ポートまたは入力 SPAN ポートごとにトラフィックを VLAN でタグ付けできます。 • エッジ TAP および SPAN ポートの Q-in-Q は、トラフィックの送信元を一意に識別し、実稼働 VLAN 情報を維持することができます。
対称ハッシュまたは対称ロードバランシング*	<ul style="list-style-type: none"> • port-channel リンクにおけるトラフィックのロード バランスのため、レイヤ 3 (IP アドレス) またはレイヤ 3 + レイヤ 4 (プロトコル ポート) に基づいてハッシュを設定できます。 • 大容量トラフィックに対応するため、複数のツール インスタンスにトラフィックを分散できます。
モニタリング対象トラフィックをマッチングするルール	<ul style="list-style-type: none"> • レイヤ 1 からレイヤ 4 の基準に基づいてトラフィックをマッチングできます。 • 必要なトラフィックのみをモニタリング ツールへ送信することで、ツールが不要なトラフィックであふれないようにソフトウェアを設定できます。 • マッチングしたトラフィックに VLAN ID を設定するアクションを設定できます。
HTTP トラフィックのレイヤ 7 モニタリング*	<ul style="list-style-type: none"> • HTTP メソッド (GET、PUT など) でマッチングを行い、そのトラフィックに対して特定のアクションを実行できます。 • この機能により、任意の Websense ツールに送信されるトラフィックの量を削減できます。
マルチプロトコル ラベル スwitチング (MPLS) ラベル ストリッピング* トラフィックの複製と転送	<ul style="list-style-type: none"> • MPLS ラベル ストリッピングを有効にして、MPLS パケットをフィルタリングできます。 • 複数の入力 TAP および SPAN ポートからのトラフィックを集約できます。 • トラフィックを複製して複数のモニタリング ツールに転送するソフトウェアを設定できます。 • これは、any-to-many 転送をサポートする唯一のソリューションです。
タイム スタンプ**	<ul style="list-style-type: none"> • Precision Time Protocol (PTP、IEEE 1588) を使用して、入力時にパケットにタイム スタンプを付けることができます。これにより、ナノ秒単位の精度を実現できます。 • この機能を使用して、法規制へのコンプライアンスおよび高度なトラブルシューティングを目的とした重要なトランザクションのモニタとデータのアーカイブを行うことができます。
パケットの切り捨て**	<ul style="list-style-type: none"> • 指定したバイト数を超えたパケットを切り捨てるようにソフトウェアを設定できます。 • 最小パケット サイズは 64 バイトです。 • ヘッダーは分析とトラブルシューティングの目的でのみ維持できます。 • セキュリティまたはコンプライアンス上の理由から、ペイロードを破棄するようにソフトウェアを設定できます。
エンドツーエンド パスの可視性	<ul style="list-style-type: none"> • このソリューションでは、トラフィック転送ルールごとに、送信元ポートからモニタリング ツールまでのエンドツーエンドのパスが完全に可視化されます。

Cisco Nexus Data Broker ソリューションのラボ セットアップ トポロジ

このソリューションの実装ガイドは、Cisco Nexus Data Broker 組み込み型ソリューションを設定するために必要なステップを示します。次に、ソリューションを設定する前に実装する必要がある前提条件を示します。

- Cisco Nexus Data Broker 組み込み型 zip ファイルを Cisco.com <https://software.cisco.com/download/release.html?mdfid=286281492&softwareid=286281554&release=3.0.0&releind=AVAILABLE&rellifecycle=&reltype=latest&i=rm> からダウンロードします。表 2 を使用してファイルのダウンロード先を選択します。

表 2 Cisco Nexus Data Broker のダウンロード ファイル マトリクス

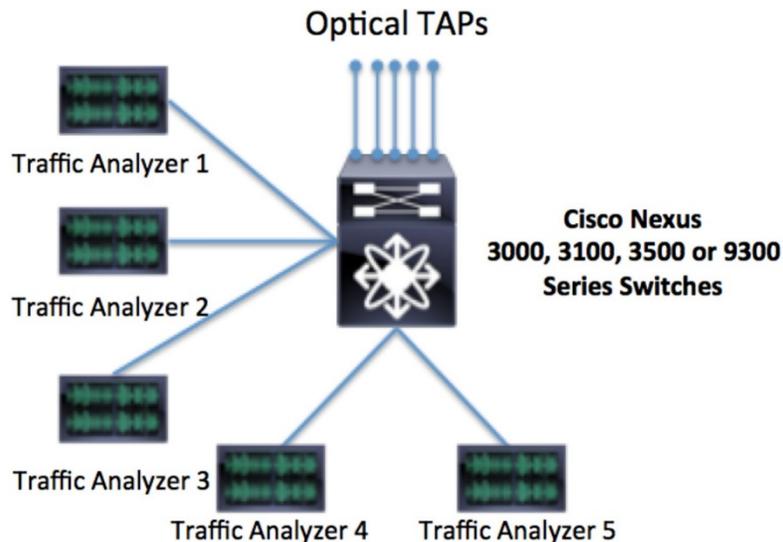
Cisco Nexus スイッチ	Cisco NX-OS バージョン	ダウンロードするファイル
Cisco Nexus 3000 シリーズおよび Cisco Nexus 3100 および 9300 プラットフォーム	OpenFlow モードの Cisco NX-OS リリース 7.0(3) I2(2a)	ndb1000-sw-app-emb-3.0.0-ofa_mmemb-2.1.3-r1-nxos-SPAK9.zip
Cisco Nexus 9300 プラットフォーム Cisco Nexus 3100 シリーズ	Cisco NX-OS リリース 7.0(3) I2 NX-API モード	ndb1000-sw-app-emb-nxapi-3.0.0-k9.zip
Cisco Nexus 3000 および 3500 シリーズ スイッチと Cisco Nexus 3100 プラットフォーム	OpenFlow モードの Cisco NX-OS リリース 6.0(2) X	ndb1000-sw-app-emb-3.0.0-ofa_mmemb-1.1.5-r3-n3000-SPAK9.zip

組み込み型導入モードが OpenFlow の場合:

- Cisco Nexus Data Broker 組み込み型 zip ファイルをディレクトリにコピーして、さらにファイルを取得します。zip ファイルには 2 つの OVA ファイルが含まれています。
- 2 つの OVA ファイルを、Cisco Nexus Data Broker 組み込み型ソリューションが実装される、Cisco Nexus 3000 シリーズまたは Cisco Nexus 9300 プラットフォーム スイッチのブートフラッシュ メモリにコピーします。
- Cisco Nexus スイッチの Cisco NX-OS ソフトウェアをアップグレードします。
 - Cisco Nexus 3000 シリーズおよび Cisco Nexus 3100 プラットフォーム スイッチの場合、次のいずれかを使用します。
 - Cisco NX-OS リリース 6.0(2) U6(3)
 - Cisco NX-OS リリース 7.0(3) I2(2a)
 - Cisco Nexus 3500 シリーズおよび Cisco Nexus 3500-X プラットフォーム スイッチの場合、NX-OS を Cisco NX-OS リリース 6.0(2) A6(5) にアップグレードします。
 - 各 Cisco Nexus 9300 プラットフォーム スイッチの場合、NX-OS を Cisco NX-OS リリース 7.0(3) I2(2a) にアップグレードします。

図 1 に、このドキュメントの設定手順で使われるモニタリング ネットワーク(TAP アグリゲーション)トポロジを示します。5 つの TAP および 5 つのモニタリング デバイス(トラフィック アナライザ)は、Cisco Nexus Data Broker 組み込み型設定を示すために使用される、Cisco Nexus 3000 シリーズまたは Cisco Nexus 9300 プラットフォーム スイッチに接続されます。

図 1 ネットワークトポロジのモニタリング



- Cisco Nexus スイッチのイーサネット ポート 1/10 ~ 1/14 に光 TAP を接続します。
- Cisco Nexus スイッチのイーサネット ポート 1/41 ~ 1/45 にトラフィック アナライザのデバイスを接続します。

Cisco Nexus 3000 シリーズおよび Cisco Nexus 9300 プラットフォーム スイッチの OpenFlow 用 Cisco プラグインの有効化

このセクションは、次の前提条件を満たしていることを前提とします。

- TAP および SPAN アグリゲーション用の各スイッチの場合、NX-OS は推奨バージョンにアップグレードされます。
- OpenFlow エージェントの正しい Cisco プラグインがダウンロードされ、スイッチのブートフラッシュメモリで使用できます。
- マネジメント IP アドレスがスイッチで設定され、スイッチは Cisco Nexus Data Broker ソフトウェアがインストールされるサーバと通信できます。

OpenFlow 用 Cisco プラグインを有効化するプロセスは以下のステップで構成されます。

- OpenFlow 用 Cisco プラグインのハードウェア サポートを有効化します。
- OpenFlow 用 Cisco プラグインをインストールしてアクティブにします。
- OpenFlow 用 Cisco プラグインを設定します。

OpenFlow 用 Cisco プラグインのハードウェア サポートの有効化

ここに示すステップを使用して、OpenFlow 用 Cisco プラグインのサポートを有効にし、補助設定用 Cisco NXAPI を有効にします。Cisco Nexus Data Broker ソリューションの一部である、Cisco Nexus 3000 シリーズまたは Cisco Nexus 9300 プラットフォーム スイッチで、以下のステップを実行する必要があります。導入は、図 1 に示すトポロジを使用します。

次に、Cisco Nexus 3000 シリーズまたは Cisco Nexus 9300 プラットフォーム スイッチで動作する必要がある設定コマンドを示します。

Cisco Nexus 3000、3100、3200、3500 シリーズおよび 9300 プラットフォーム スイッチのコマンド

- **enable**
- **configure terminal**
- **spanning-tree mode mst**
- **vlan 1-3967**
- **no spanning-tree vlan 1-3967**

スイッチが Cisco Nexus 3000 シリーズまたは Cisco Nexus 3100 プラットフォームの場合：

- **hardware profile openflow**
- **hardware profile tcam region qos 0**
- **hardware profile tcam region racl 0**
- **hardware profile tcam region vacl 0**
- **hardware profile tcam region ifacl 1024 double-wide**

スイッチが Cisco Nexus 3500 シリーズの場合：

- **hardware profile tcam region qos 0**
- **hardware profile tcam region racl 0**
- **hardware profile tcam region vacl 0**
- **hardware profile tcam region ifacl 1024 double-wide**
- **hardware profile forwarding-mode openflow-hybrid**

スイッチが Cisco Nexus 3200 シリーズの場合：

- **hardware access-list tcam region e-racl 0**
- **hardware access-list tcam region span 0**
- **hardware access-list tcam region redirect 0**
- **hardware access-list tcam region vpc-convergence 0**
- **hardware access-list tcam region racl-lite 256**
- **hardware access-list tcam region l3qos-intra-lite 0**
- **hardware access-list tcam region ifacl 256 double-wide**
- **hardware access-list tcam region openflow 256**

スイッチが Cisco Nexus 9300 プラットフォームの場合：

- **hardware access-list tcam region qos 0**
- **hardware access-list tcam region vacl 0**
- **hardware access-list tcam region racl 0**
- **hardware access-list tcam region vpc-convergence 0**
- **hardware access-list tcam region ifacl 1024 double-wide**
- **hardware access-list tcam region openflow 512**

- **exit**
- **copy running-config startup-config**
- **reload**

OpenFlow 用 Cisco プラグインのインストールおよび有効化

OpenFlow 用 Cisco プラグインをインストールして有効化にするには、以下のステップに従います。この例では、OpenFlow OVA ファイル名が ofa_mmemb-1.1.5-r3-n3000-SPA-k9.ova で、Cisco 3000 シリーズ スイッチのブートフラッシュメモリにダウンロードされ、使用できると仮定しています。

- **enable**
- **virtual-service install name ofa package bootflash: ofa_mmemb-1.1.5-r3-n3000-SPA- k9.ova**

次の **show** コマンドを使用して、virtual-service インストールのステータスを確認します。

- **show virtual-service list**

仮想サービスのステータスが [Installed] として表示されるようになった後で、サービスをアクティブにするには、次のコマンドを実行します。

- **configure terminal**
- **virtual-service ofa**
- **activate**
- **end**
- **copy running-config startup-config**

show virtual-service list コマンドを使用して、サービス ステータスが [Activated] に変更されたことを確認します。この変更プロセスには最大 2 分かかります。

OpenFlow 用 Cisco プラグインの設定

OpenFlow 用 Cisco プラグインを設定するには、OpenFlow ポートを設定し、Cisco Nexus Data Broker の IP アドレスを指定し、論理スイッチと OpenFlow ポートを関連付ける必要があります。

OpenFlow 用に有効化されるすべてのポートはトランクポートとして設定される必要があります。次に示す設定コマンドは、OpenFlow 対応インターフェイスのいずれにも存在する必要があります(複数のインターフェイスを同時に設定できるあらゆるインターフェイス範囲を使用します)。

Cisco Nexus 3000、3100 シリーズと 3500 シリーズおよび Cisco Nexus 3200 と Cisco Nexus 9300 プラットフォーム スイッチのコマンド

- **enable**
- **configure terminal**
- **interface Ethernet 1/10-14, Ethernet1/41-45**
- **switchport**
- **switchport mode trunk**
- **no shutdown**
- **end**
- **copy running-config startup-config**

OpenFlow 論理スイッチを設定するには、Cisco Nexus Data Broker 組み込み型の IP アドレスとポート情報を指定し、OpenFlow 対応ポートを含める必要があります。Cisco Nexus Data Broker 組み込み型の設定では、Cisco Nexus 3000 シリーズ スイッチ管理インターフェイスの IP アドレスを Cisco Nexus Data Broker IP アドレスとして使用します。この設定例では、10.10.10.10 が Cisco Nexus 3000 シリーズ スイッチのインターフェイス IP アドレスであると仮定します。

Cisco Nexus 3000 および 3100 シリーズと Cisco 3200 および Cisco Nexus 9300 プラットフォーム スイッチのコマンド

- **OpenFlow**
- **switch 1**
- **pipeline 201**
- **controller ipv4 10.10.10.10 port 6653 vrf management security none**
- **of-port interface ethernet1/10**
- **of-port interface ethernet1/11**
- **of-port interface ethernet1/12**
- **of-port interface ethernet1/13**
- **of-port interface ethernet1/14**
- **of-port interface ethernet1/41**
- **of-port interface ethernet1/42**
- **of-port interface ethernet1/43**
- **of-port interface ethernet1/44**
- **of-port interface ethernet1/45**
- **end**
- **copy running-config startup-config**

Cisco Nexus 3500 シリーズ スイッチのコマンド

- **OpenFlow**
- **switch 1**
- **default-miss cascade drop**
- **pipeline 203**
- **controller ipv4 10.10.10.10 port 6653 vrf management security none**
- **of-port interface ethernet1/10**
- **of-port interface ethernet1/11**
- **of-port interface ethernet1/12**
- **of-port interface ethernet1/13**
- **of-port interface ethernet1/14**
- **of-port interface ethernet1/41**
- **of-port interface ethernet1/42**
- **of-port interface ethernet1/43**
- **of-port interface ethernet1/44**
- **of-port interface ethernet1/45**
- **end**

copy running-config startup-config

Cisco NX-API モードでの Cisco Nexus 9300、Cisco Nexus 3100 および Cisco Nexus 3200 シリーズ スイッチの設定の有効化

このセクションは、TAP および SPAN アグリゲーション用の NX-API モードでの Cisco Nexus 9300 プラットフォーム スイッチで組み込みオプションを使用するときのみ適用されます。

このセクションは、次の前提条件を満たしていることを前提とします。

- Cisco Nexus 9300 プラットフォームと Cisco Nexus 3100 シリーズ スイッチの場合、NX-OS は Cisco NX-OS リリース 7.0 (3) I2 (2a) にアップグレードされます。
- マネジメント IP アドレスがスイッチで設定され、スイッチは Cisco Nexus Data Broker サーバと通信できます。

Cisco Nexus 9300 プラットフォーム スイッチと Cisco Nexus Data Broker を使用する前に、次のものを設定する必要があります。

- Link Layer Discovery Protocol (LLDP) および NX-API 機能を有効化し、各スイッチに VLAN を作成します。
- ternary content-addressable memory (TCAM) を設定します。
- 設定を保存し、スイッチをリロードします。

各スイッチでの LLDP および Cisco NX-API の有効化

Cisco Nexus 9300 プラットフォームで LLDP および NX-API 機能を有効にし、VLAN を作成するには、各スイッチで次に示す設定を使用します。

- **enable**
- **configure terminal**
- **feature lldp**
- **feature nxapi**
- **spanning-tree mode mst**
- **vlan 1-3967**
- **no spanning-tree vlan 1-3967**
- **end**
- **copy running-config startup-config**

TCAM の設定

Cisco Nexus 9300 プラットフォームと Cisco Nexus 3100 シリーズおよび Cisco Nexus 3200 シリーズ スイッチの TCAM 割り当てを再設定するには、各スイッチで次に示すコマンドを使用します。これらのコマンドは IP アクセスリストおよび MAC アクセスリストに対して割り当てます。

注: TCAM の再設定を有効にするには、スイッチを再起動する必要があります。プロセス全体の最後にスイッチを再起動します。

- **enable**
 - **configure terminal**
- スイッチが Cisco Nexus 3000 シリーズまたは Cisco Nexus 3100 プラットフォームの場合：
- **hardware profile tcam region qos 0**
 - **hardware profile tcam region racl 0**
 - **hardware profile tcam region vacl 0**
 - **hardware profile tcam region ifacl 1024 double-wide**

スイッチが Cisco Nexus 3200 シリーズの場合：

- **hardware access-list tcam region e-racl 0**
- **hardware access-list tcam region span 0**
- **hardware access-list tcam region redirect 0**
- **hardware access-list tcam region vpc-convergence 0**
- **hardware access-list tcam region racl-lite 256**
- **hardware access-list tcam region l3qos-intra-lite 0**
- **hardware access-list tcam region ifacl 512**
- **hardware access-list tcam region mac-ifacl 256**

スイッチが Cisco Nexus 9300 および Cisco Nexus 3164 スイッチの場合：

- **hardware access-list tcam region qos 0**

- **hardware access-list tcam region vacl 0**
- **hardware access-list tcam region racl 0**
- **hardware access-list tcam region redirect 0**
- **hardware access-list tcam region vpc-convergence 0**
- **hardware access-list tcam region ifacl 1024 double-wide**
- **hardware access-list tcam region mac-ifacl 512**
- **end**

設定の保存およびスイッチのリロード

ハードウェア TCAM の設定変更を有効にするには、すべてのスイッチを再起動する必要があります。設定を保存し、スイッチをリロードするには、以下のステップに従います。

- **enable**
- **copy running-config startup-config**
- **reload**

Cisco 3000 シリーズおよび Cisco Nexus 9300 シリーズ スイッチでの Cisco Nexus Data Broker 組み込み型ソリューションの有効化

このセクションは、次の前提条件を満たしていることを前提とします。

- Cisco Nexus 3000 シリーズと Cisco Nexus 9300 プラットフォーム スイッチで、Cisco Nexus Data Broker 組み込み型 OVA ファイルがダウンロードされ、ブートフラッシュ メモリで使用できること。
- 管理 IP アドレスが Cisco Nexus 3000 シリーズ スイッチで設定されていること。
- Cisco Nexus 3000 シリーズまたは Cisco Nexus 9300 プラットフォーム スイッチで、ブートフラッシュ メモリに少なくとも 700 MB の空き領域があること。

Cisco Nexus Data Broker 組み込み型ソリューションのインストールとアクティブ化

Cisco Nexus 3000 シリーズまたは Cisco Nexus 9300 プラットフォーム スイッチで Cisco Nexus Data Broker 組み込み型ソリューションをインストールおよびアクティブ化するには、以下のステップに従います。この例では、Cisco Nexus Data Broker 組み込み型ファイルが `ndb1000-sw-app-emb-k9-3.0.0.ova` で、Cisco Nexus スイッチのブートフラッシュ メモリにダウンロードされ、使用できると仮定しています。

Cisco Nexus 3000、3100 シリーズと 3500 シリーズおよび Cisco Nexus 3200 と Cisco Nexus 9300 プラットフォーム スイッチのコマンド

- **enable**
- **virtual-service install name ndbemb package bootflash: ndb1000-sw-app-emb-k9-3.0.0.ova**

次の **show** コマンドを使用して、**virtual-service** インストールのステータスを確認します。

- **show virtual-service list**

仮想サービスのステータスが [Installed] として表示されるようになった後で、サービスをアクティブにするには、次のコマンドを実行します。

- **configure terminal**
- **virtual-service ndbemb**
- **activate**
- **end**
- **copy running-config startup-config**

show virtual-service list コマンドを使用して、サービス ステータスが [Activated] に変更されたことを確認します。この変更プロセスには最大 2 分かかります。

Cisco Nexus Data Broker 組み込み型ソリューションへのスイッチの接続ステータスの確認

このステップは Cisco Nexus Data Broker 組み込み型オプションが OpenFlow モードで使用されるときにのみ適用されます。

スイッチが Cisco Nexus Data Broker インスタンスに接続できることを確認するには、次に示す **show** コマンドを使用します。スイッチが Cisco Nexus Data Broker に正常に接続されると、[Connected] ステータスが [Yes] として表示されます。

- **show openflow switch 1 controllers**
- **show openflow switch 1 controllers stats**

最初の Cisco Nexus Data Broker 組み込み型の設定

このセクションでは、Cisco Nexus Data Broker アプリケーションが動作していると仮定します。次のサポート対象ブラウザのいずれかを使用して Cisco Nexus Data Broker Web GUI を起動します (<https://10.10.10.10:8443/monitor> を参照)。

- Firefox 18.0 以降
- Google Chrome 24.0 以降

この設定例では、Cisco Nexus Data Broker 埋め込み型アプリケーションが、管理 IP アドレスが 10.10.10.10 の Cisco Nexus 3000 シリーズ スイッチで実行しています。

デフォルトのクレデンシャルを使用して GUI にログインします。

- ユーザ名: admin
- パスワード: admin

Cisco NX-API モードでの Cisco Nexus 9300、Cisco Nexus 3100 および Cisco Nexus 3200 プラットフォーム スイッチでのデバイス検出

上部の [Administration] タブをクリックして管理画面に移動します。

ユーザ名とパスワードを入力し、接続モードを NX-API に設定するには、Cisco Nexus 9300、Cisco Nexus 3100 および Cisco Nexus 3200 プラットフォーム スイッチを編集する必要があります。

- [Cisco Nexus Data Broker Administration] ページで、[Devices] をクリックします。
- [Devices] で、[Device Connections] タブをクリックします。

- Cisco Nexus 9300、3100 または 3200 シリーズ スイッチはすでに使用できます。
- [Edit] ボタンをクリックします。
- ポップアップ ウィンドウで次の情報を入力します。
 - Username: Cisco Nexus Data Broker がスイッチに接続するのに使用する必要があるログイン ユーザ名
 - Password: スイッチのパスワード
 - Connection Type: NX-API
- [Edit Device Connection] をクリックして設定を保存します。

Cisco Nexus Data Broker の設定

Cisco Nexus Data Broker の設定は以下のステップで構成されます。

- ポートタイプを設定しモニタリング ツールをマッピングします。
- トラフィックをマッチングするフィルタを設定します。
- さまざまなモニタリング ツールへトラフィックを転送するためのポリシーを設定します。

<https://10.10.10.10:8443/monitor> で Cisco Nexus Data Broker GUI にアクセスします

ポートタイプの設定とモニタリング ツールのマッピング

Cisco Nexus Data Broker では、次のようなさまざまなポートタイプを設定できます。

- エッジポート (SPAN または光 TAP)
- 配信ポート

エッジポートは、トラフィックがモニタリング ネットワークに入るときの入力ポートです。通常は、ネットワーク TAP または SPAN ポートです。Cisco Nexus Data Broker は次のエッジポートをサポートします。

- TAP ポート: 物理 TAP のワイヤに接続された着信トラフィック用のエッジポート
- SPAN ポート: SPAN 宛先として設定されるアップストリームスイッチに接続された着信トラフィック用のエッジポート

注: [Edge-Tap] または [Edge-SPAN] オプションは、Cisco Nexus Data Broker アプリケーション内での分類専用です。これらは、トラフィックのフィルタリングおよび転送に影響せず、ネットワーク構成の変更を必要としません。

必要に応じて、入力ソースポートと VLAN を関連付けることもできます。送信元ポートに着信するすべてのパケットは VLAN ID でタグ付けされ、入力ポートの特定に使用できます。

配信ポートはトラフィックがモニタ ネットワークを出るとき出力ポートです。これらの出力ポートは、外部モニタリングおよび分析ツールに接続されます。Cisco Nexus Data Broker のモニタリング デバイスを設定するときに、名前とアイコンを関連付けた後、スイッチとスイッチが接続されているポートに関連付けることができます。

設定されたデバイスは、[Devices] タブの [Monitor Devices] テーブルに表示されます。アイコンとそれをノードに接続する直線がトポロジ図に表示されます。

エッジポートの設定

次の設定例では、各 Cisco Nexus スイッチに 5 つの TAP ポートがあります。Cisco Nexus スイッチのエッジ TAP ポートを設定するためのステップを次に示します。

トポロジ図で、Cisco Nexus 3000 または 3500 シリーズまたは Cisco Nexus 3100 プラットフォーム スイッチをクリックしてポートを設定します。

イーサネット ポート 1/10 ~ 1/14 に対し次に示すステップを繰り返します。

- ノードのポートのリストで、ポート(たとえば、ethernet1/10)に対し [Click to Configure] をクリックします。
- [Select a Port Type] ドロップダウン リストをクリックし、[Edge-Tap] を選択します。
- (オプション)エッジ TAP ポートの説明を入力します。
- (オプション)入力ソース ポートを特定するには、VLAN ID を入力します。
- [Submit] をクリックします

エッジ TAP ポートを設定した後で、左ペインの上部の [Back] ボタン(青色でハイライト)をクリックします。

配信ポートの設定

次に示す設定例では、合計で 5 つのモニタリング ツール(Traffic Analyzer)を使用します。次にスイッチとポートにモニタリング ツールをマッピングするステップを示します。

トポロジ図で、Cisco Nexus 3000 または 3500 シリーズまたは Cisco Nexus 3100 プラットフォーム スイッチをクリックしてポートを設定します。

イーサネット ポート 1/41 ~ 1/45 に対し次に示すステップを繰り返します。

- ノードのポートリストで、イーサネット ポート 1/41 に対し [Click to Configure] をクリックします。
- [Add Monitoring Device] をクリックします。
- [Add Device] ダイアログボックスで、次の操作を実行します。
 - デバイス名を入力します。
 - スイッチ名を選択します
 - 接続されるポートを選択します
 - モニタリング デバイスに使用するアイコンを選択します。
 - [Submit] をクリックします。

エッジ TAP ポートを設定した後で、左ペインの上部の [Back] ボタン(青色でハイライト)をクリックします。

ネットワークトラフィックをマッチングするフィルタの設定

トラフィックをフィルタリングするために Cisco Nexus Data Broker によって使用されるレイヤ 2、レイヤ 3、およびレイヤ 4 基準を定義するためにフィルタが使用されます。フィルタで基準に一致するトラフィックは、モニタリング デバイスが接続された配信ポートにルーティングされます。

設定例では、特定の宛先 IP アドレスへのすべての FTP トラフィックをマッチングするために別のフィルタを作成する場合、次のステップを使用します。

- 左側のペインで [Filters] をクリックし、[Add Filter] をクリックします。
- [Add Filter] ダイアログボックスで、次を指定します。
 - Name : Match-FTP
 - Layer 3 – Destination IP Address : 10.17.44.3
 - Layer 3 – Protocol : TCP
 - Layer 4 – Destination Port : FTP (Data)
 その他の値はデフォルト設定のままにします。
- [Add Filter] をクリックします。

設定例では、特定の宛先 IP アドレスの特定の IP サブネットへのすべてのユーザ データグラム プロトコル (UDP) のトラフィックをマッチングするために別のフィルタを作成する場合、次のステップを使用します。

- 左側のペインで [Filters] をクリックし、[Add Filter] をクリックします。
- [Add Filter] ダイアログボックスで、次を指定します。
 - Name : Match-UDP
 - Bidirectional: このオプションを選択します。
 - Layer 3 – Source IP Address : 22.22.22.0/24
 - Layer 3 – Destination IP Address : 10.17.44.13
 - Layer 3 – Protocol : UDP
 - Layer 4 – Destination Port : [Enter Destination Port] オプションを選択し、**53** をテキスト ボックスに入力します。
 その他の値はデフォルト設定のままにします。
- [Add Filter] をクリックします。

接続を使用してフィルタとモニタリング ツールを関連付けます。接続が設定されるときに、Cisco Nexus スイッチは一致するトラフィックを宛先モニタリング ツールに転送するようにプログラムされます。Cisco Nexus Data Broker は次をサポートします。

- **Multipoint-to-Multipoint (MP2MP) 転送**: MP2MP 転送パス オプションによって、SPAN または TAP トラフィックがモニタリング ネットワークに入るときの入力エッジポート、および出力配信ポートの両方が定義されます。Cisco Nexus Data Broker は配信ポートを使用して、その入力ポートから 1 つ以上のデバイスにトラフィックを転送します。
- **Any-to-Multipoint (A2MP) 転送パス オプション**: A2MP 転送パス オプションによって、モニタ ネットワークの入力エッジポートは不明ですが、出力配信ポートは定義されます。Cisco Nexus Data Broker はルート ノードから他のすべてのノードへのループフリー転送パスを Single-Source Shortest Path (SSSP) アルゴリズムを使用して自動的に計算します。

設定例では、Traffic Analyzer-1、Traffic Analyzer-3、および Traffic Analyzer-5 へのすべてのインターフェイストラフィックを転送する場合、次のステップを使用します。

- 左側のペインで [Connections] をクリックします。
- [New Connection] をクリックし、新しいルールを作成するための次のパラメータを使用します。
 - Connection Name: ルールに **Match-all** という名前を付けます。
 - Select Filter: ドロップダウン リストから [Default-Match-All] を選択します。
 - Select Destination Devices: [Traffic Analyzer 1]、[Traffic Analyzer 3] および [Traffic Analyzer 5] を選択します。
 - Select Source Node: ドロップダウン リストから [NX-SW-1] を選択します。
 - Select Source Port: ドロップダウン リストから [Ethernet1/10] を選択します。
 - [Add Source Port] ボタンをクリックします。
 - Select Source Port: ドロップダウン リストから [Ethernet1/11] を選択します。
 - [Add Source Port] ボタンをクリックします。
 - Select Source Port: ドロップダウン リストから [Ethernet1/12] を選択します。
 - [Add Source Port] ボタンをクリックします。

[Submit] をクリックします。

設定例では、Traffic Analyzer-2 および Traffic Analyzer-4 へのすべての UDP トラフィックを転送する場合、次のステップを使用します。

- 左側のペインで [Connections] をクリックします。
- [New Connection] をクリックし、新しいルールを作成するための次のパラメータを使用します。
 - Connection Name: ルールに **Match-UDP** という名前を付けます。
 - Select Filter: ドロップダウン リストから [Match-UDP] を選択します。
 - Select Destination Devices: [Traffic Analyzer 2] および [Traffic Analyzer 4] を選択します。
 - Select Source Node: デフォルト設定を使用します。
 - Select Source Port: デフォルト設定を使用します。
- [Submit] をクリックします。

各ルールの実際の traffic-forwarding パスを表示するには、接続名をクリックします。

この時点で、スイッチの 2 つのエッジポートが、適用されたフィルタに従ってトラフィックを受信していることを確認します。Cisco Nexus Data Broker Management UI の [Troubleshoot] タブを使用してフローの詳細を確認します。

- 左側のペインで [Statistics] をクリックします。
- ドロップダウン ボックスからスイッチ名を選択します
- デフォルトでフローの統計情報のページが表示されます
- [Flows] タブの横にある [Ports] タブをクリックして、ポートの統計情報に移動できます。

まとめ

Cisco Nexus スイッチを備えた Cisco Nexus Data Broker は、ネットワークトラフィックのモニタリングと可視化のために、拡張性があり、コスト効率のよい、効率的なインフラストラクチャを提供できます。ハイブリッドモードで動作する Cisco Nexus スイッチファミリの機能により、ハードウェアの設備投資なしで投資から新たな価値を得ることができます。顧客は少数のポートをモニタリング専用にすることができ、それらのポートは Cisco Nexus Data Broker によって制御されます。残りのすべてのポートはローカル制御プレーンで管理し続けることができ、実稼働トラフィックに使用できます。このアプローチにより、インフラストラクチャへの大幅な変更なしで、顧客が既存のデータセンター ネットワークに新しい機能を導入できるようになります。

詳細情報

詳細については、次の各項を参照してください。

- OpenFlow 用 Cisco プラグインの構成ガイド：
<http://www.cisco.com/en/US/docs/switches/datacenter/sdn/configuration/openflow-agent-nxos.html>
- Cisco Nexus Data Broker 構成ガイド：
<http://www.cisco.com/c/en/us/support/cloud-systems-management/nexus-data-broker/products-installation-and-configuration-guides-list.html>
- Cisco Nexus 9000 シリーズ スイッチ構成ガイド：
http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/system_management/configuration/guide/b Cisco Nexus 9000 Series NX-OS System Management Configuration Guide 7x.html