# Cisco Nexus Dashboard Data Broker 構成ガイド、リリース 3.10.5

**最終更新**：2025 年 10 月 16 日


**シスコシステムズ合同会社**
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

# Trademarks

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS REFERENCED IN THIS DOCUMENTATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. EXCEPT AS MAY OTHERWISE BE AGREED BY CISCO IN WRITING, ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENTATION ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at: https://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html. Cisco product warranty information is available at https://www.cisco.com/c/en/us/products/warranty-listing.html. US Federal Communications Commission Notices are found here https://www.cisco.com/c/en/us/products/us-fcc-notice.html.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability for delay in the delivery or failure to deliver any products or feature roadmap items that may be set forth in this document.

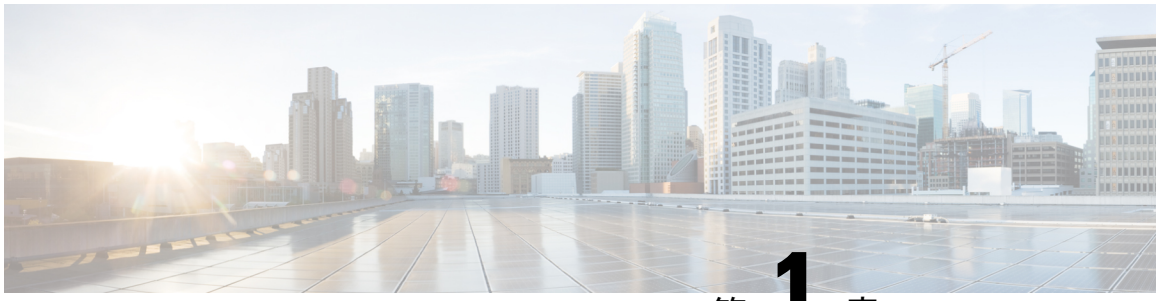
Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners.

Trademarks

The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)



第 1 章

# 概要

この章には、Cisco Nexus Dashboard Data Broker の概要が含まれています。



## Cisco Nexus ダッシュボード Data Broker について

アプリケーショントラフィックに対する可視性は、以前から、セキュリティの維持、トラブルシューティング、コンプライアンス、リソース計画のためのインフラ運用にとって重要でした。テクノロジーの発達と、クラウドベース アプリケーションの増加に伴い、ネットワーク トラフィックの可視性の向上は必須の条件となっています。ネットワーク トラフィックを可視化する従来のアプローチでは、コストがかかり柔軟性に欠けているため、大規模な導入環境のマネージャには負担が大きすぎます。

Cisco Nexus スイッチ ファミリと共に Cisco Nexus Dashboard Data Broker を使用することで、ソフトウェア定義型のプログラム可能なソリューションが実現できます。Switched Port Analyzer（SPAN）またはネットワーク テスト アクセス ポイント（TAP）を使用してネットワーク トラフィックのコピーを集約し、モニタリングと可視化を行います。このパケットブローカリング アプローチは、従来のネットワーク タップやモニタリング ソリューションとは対照的に、シンプルで拡張性とコスト効率に優れたソリューションを実現するもので、セキュリティ、コンプライアンス、およびアプリケーション パフォーマンスのモニタリング ツールを効率的に利用するため大量のビジネスクリティカルなトラフィックをモニタリングする必要のある顧客に適しています。

さまざまな Cisco Nexus スイッチを使用できる柔軟性と、それらを相互接続してスケーラブルなトポロジを形成する機能により、複数の入力 TAP または SPAN ポートからのトラフィックを集約し、トラフィックを複製して、異なるスイッチにわたって接続された複数のモニタリング ツールに転送する機能を提供します。Cisco NX-API エージェントを使用してスイッチと通

信する Cisco Nexus Dashboard Data Broker は、トラフィック管理のための高度な機能を提供します。

Cisco Nexus Dashboard Data Broker は、複数の分離された Cisco Nexus Dashboard Data Broker ネットワークの管理サポートを提供します。同じアプリケーションインスタンスを使用して、接続されているとは限らない複数の Cisco Nexus Dashboard Data Broker トポロジを管理できます。たとえば、5か所のデータセンターを運用しており、独立したソリューションをデータセンターごとに導入する場合は、モニタリングネットワークごとに論理パーティション（ネットワークスライス）を作成することで、単一のアプリケーションインスタンスを使用して、独立した5つの導入環境をすべて管理できます。

（注） リリース 3.10.1 から、Cisco Nexus Data Broker（NDB）の名前は、Cisco Nexus Dashboard Data Brokerに変更されました。ただし、GUIおよびインストールフォルダ構造と対応させるため、一部の NDB のインスタンスがこのドキュメントには残されています。NDB/ Nexus Data Broker/ Nexus Dashboard Data Brokerという記述は、相互に交換可能なものとして用いられています。

**Cisco Nexus Dashboard Data Broker の基本の顕著な機能:**

- タップおよびスパン集約向けトポロジ
- すべての機能を実行するための堅牢な Representational State Transfer（REST）API および Web ベースの GUI。
- 複数のモニタリング ツールへの複製と転送機能
- レイヤ 1 からレイヤ 4 の情報に基づいてモニタリング トラフィックを照合するためのルール。
- PTP を使用したタイムスタンプ。
- 指定されたバイト数を超えるパケットの切り捨てによるペイロードの破棄。
- ユーザー定義フィールドを使用した、パケットのカスタム フィルタリング。
- TAP/SPAN 集約ネットワーク状態の変化に適応する機能。
- エンドツーエンドの可視性
- 高可用性。
- ロード バランシング。
- 連続していない複数のネットワークを管理します。
- ACI デバイス/APIC および NX-OS デバイスとの統合。
- トラブルシューティングを容易にするリアルタイムの統計。
- IPv6 によるアプリケーション管理。

- ロールベースのアクセス コントロール（RBAC）などのセキュリティ機能、および認証、許可、アカウンティング（AAA）機能用に RADIUS や TACACS、または LDAP を使用した外部 Active Directory との統合。

**Cisco Nexus Dashboard Data Broker の追加機能のプラットフォーム単位のサポート：**

**表 *1*：サポートされる機能**

| 機能名 | **Cisco Nexus 9300（EX、FX、FX2）**<br>**C93180LC-EX、**<br>**C93180YC-EX、**<br>**C93108TC-EX、**<br>**C93108TC-FX、**<br>**C93180YC-FX、**<br>**C9336C-FX2、**<br>**C93240YC-FX2、**<br>**C93360YC-FX2** |
|---|---|
| ポートチャネル ロードバランシング | Y |
| MPLS ストリッピング | Y |
| MPLS 除去- ラベル | N |
| MPLS フィルタリング | N |
| sFlow | Y |
| PTP/タイムスタンプ | Y |
| Jumbo MTU | Y |
| NetFlow | Y |
| Q-in-Q タグ付け（TAP および SPAN 入力ポート用） | Y |
| スパン宛先 | Y |
| タイムスタンプ機能 | Y |
| パケットの切り捨て | Y |
| タイムスタンプ ストリップ | Y |
| 入力ポート - TAP/SPAN | Y |
| ローカル モニタリング ツール | Y |

| 機能名 | **Cisco Nexus 9300（EX、FX、FX2）**<br>**C93180LC-EX、**<br>**C93180YC-EX、**<br>**C93108TC-EX、**<br>**C93108TC-FX、**<br>**C93180YC-FX、**<br>**C9336C-FX2、**<br>**C93240YC-FX2、**<br>**C93360YC-FX2** |
|---|---|
| リモート モニタリング ツールと ERSPAN サポート | Y |
| リモート送信元 | Y |
| UDF | Y |
| UDF v6 | Y |
| UDE | N |
| ICMPv6 をドロップ | Y |

表 *2:* サポートされている機能（続き）

| 機能名 | **Cisco Nexus 9300（EX、FX）**<br>**C9504、**<br>**C9508、**<br>**C9516** | **Cisco Nexus 9364C、9332C** | **Cisco Nexus 9300-GX**<br>**93600CD-GX**<br>**9364C-GX**<br>**9316D-GX** |
|---|---|---|---|
| ポートチャネル ロードバランシング | Y | Y | Y |
| MPLS ストリッピング | N | N | Y |
| MPLS 除去- ラベル | N | N | N |
| MPLS フィルタリング | N | N | N |
| sFlow | Y | Y | Y |
| PTP/タイムスタンプ | Y | Y | Y |
| Jumbo MTU | Y | Y | Y |
| NetFlow | Y | N | Y |

| 機能名 | Cisco Nexus 9300（EX、FX）<br>C9504、<br>C9508、<br>C9516 | Cisco Nexus 9364C、9332C | Cisco Nexus 9300-GX<br>93600CD-GX<br>9364C-GX<br>9316D-GX |
|---|---|---|---|
| Q-in-Q タグ付け（TAP および SPAN 入力ポート用） | Y | Y | Y |
| スパン宛先 | Y | Y | Y |
| タイムスタンプ機能 | Y | Y | Y |
| パケットの切り捨て | Y | Y | Y |
| タイムスタンプ ストリップ | Y | Y | Y |
| 入力ポート - TAP/SPAN | Y | Y | Y |
| ローカル モニタリング ツール | Y | Y | Y |
| リモート モニタリング ツールと ERSPAN サポート | Y | Y | Y |
| リモート送信元 | Y | N | Y |
| UDF | Y | Y | Y |
| UDF v6 | Y | Y | Y |
| UDE | Y | N | N |
| ICMPv6 をドロップ | Y | Y | Y |

（注） 上記の表に示されている Cisco Nexus シリーズ スイッチが推奨されます。これらの各スイッチでサポートされている NX-OS バージョンについては、各リリースの *Cisco Nexus Dashboard Data Broker* リリース ノートの相互運用性マトリックスの表を参照してください。Cisco Nexus Dashboard Data Broker リリースノートのリストは次のとおりです。

**Cisco Nexus シリーズ スイッチの制限**：

表 *3:* 制限事項

| Cisco Nexus シリーズ スイッチ | 制限事項 |
|---|---|
| 9364C-GX、93600CD-GX、9316D-GX | • 入力ポートの QinQ VLAN の範囲は 2 ～ 509 です。<br>• MPLS ラベル ストリップの設定後に QinQ VLAN を追加することはできません。 |

# Cisco Nexus シリーズ スイッチの前提条件

Cisco Nexus Dashboard Data Broker は、Cisco Nexus 3000、3100、3200、および 9000 シリーズ スイッチでサポートされています。ソフトウェアを展開する前に、次のことを行う必要があります。

- スイッチにログインするための管理者権限があることを確認してください。
- スイッチ（mgmt0）の管理インターフェイスに、**show running-config interface mgmt0** コマンドを使用して設定された IP アドレスがあることを確認します。
- スイッチがマルチ スパニング ツリー（MST）モードであることを確認します。**spanning-tree mode mst** コマンドを使用して、スイッチで MST モードをイネーブルにできます。
- VLAN フィルタリングをサポートするために、タップ アグリゲーションおよびインライン モニタリング リダイレクションのために Cisco Nexus Dashboard Data Broker で使用される VLAN 範囲をデータベースに追加します。たとえば、VLAN 範囲は <1-3967> です。
- すべての VLAN でスパニング ツリー プロトコルが無効になっていることを確認します。**no spanning-tree vlan 1-3967** を使用して、すべての VLAN でスパニング ツリーを無効にすることができます。
- NXOS バージョン 9.2(1) を使用した最初の Nexus Dashboard Data Broker 展開の場合、**feature nxapi** および **nxapi http port 80** コマンドが NDB デバイスで構成されていることを確認します。NDB デバイスを NXOS バージョン I7(x) から 9.2(1) にアップグレードする場合、**feature nxapi** および **nxapi http port 80** 構成は必要ありません。

Cisco Nexus シリーズ スイッチで NX-API モードを実行するには、次の前提条件を参照してください。

（注） IPv6 機能の前提条件であるハードウェア コマンドは、**hardware access-list tcam region ipv6-ifacl 512 double-wide** です。

（注） TCAM構成は、必要なフィルタのタイプに基づいています。ネットワーク要件に基づいて、特定のリージョンから複数のTCAMエントリを設定できます。たとえば、*ing-ifacl* は、N93180YC-Eの場合にMAC、IPv4、IPv6フィルタに対応するTCAMリージョンです。この領域から複数のTCAMを設定して、より多くのフィルタリングACL TCAMエントリに適合させることができます。

| デバイス モデル | NX-API モード |
|---|---|
| Cisco Nexus 3000 シリーズ スイッチ | プロンプトで次のコマンドを入力します。<br>• **# hardware profile tcam region qos 0**<br>• **# hardware profile tcam region racl 0**<br>• **# hardware profile tcam region vacl 0**<br>• **# hardware profile tcam region ifacl 1024 double-wide**<br>• **# hardware access-list tcam region mac-ifacl 512**<br>• **#feature nxapi**<br>• **#feature lldp** |
| Cisco Nexus 3164Q、3132Q スイッチ | プロンプトで次のコマンドを入力します。<br>• **# hardware profile tcam region qos 0**<br>• **# hardware profile tcam region racl 0**<br>• **# hardware profile tcam region vacl 0**<br>• **# hardware profile tcam region ifacl 1024 double-wide**<br>• **# hardware access-list tcam region mac-ifacl 512**<br>• **#feature nxapi**<br>• **#feature lldp** |
| Cisco Nexus 3172 シリーズ スイッチ | **hardware profile mode tap-aggregation** [**l2drop**] CLI コマンドを使用して、タップ集約を有効にし、VLAN タギングに必要なエントリをインターフェイステーブルに予約します。l2dropオプションは、タップ インターフェイス上でIP以外のトラフィック入力をドロップします。 |

| デバイス モデル | NX-API モード |
| --- | --- |
| Cisco Nexus 3200 シリーズ スイッチ | プロンプトで次のコマンドを入力します。<br>• **# hardware access-list tcam region e-racl 0**<br>• **# hardware access-list tcam region span 0**<br>• **# hardware access-list tcam region redirect 0**<br>• **# hardware access-list tcam region vpc-convergence 0**<br>• **# hardware access-list tcam region racl-lite 256**<br>• **# hardware access-list tcam region l3qos-intra-lite 0**<br>• **# hardware access-list tcam region ifacl 256 double-wide**<br>• **# hardware access-list tcam region mac-ifacl 512**<br>• **# hardware access-list tcam region ipv6-ifacl 256**<br>• **#feature nxapi**<br>• **#feature lldp** |

| デバイス モデル | NX-API モード |
| --- | --- |
| Cisco Nexus 9300 シリーズ スイッチ | プロンプトで次のコマンドを入力します。<br>• **# hardware access-list tcam region qos 0**<br>• **# hardware access-list tcam region vacl 0**<br>• **# hardware access-list tcam region racl 0**<br>• **# hardware access-list tcam region redirect 0**<br>• **# hardware access-list tcam region vpc-convergence 0**<br>• **#hardware access-list tcam region ifacl 1024 double-wide**<br>• **# hardware access-list tcam region mac-ifacl 512**<br>• **# hardware access-list tcam region ipv6-ifacl 512**<br>• **#feature nxapi**<br>• **#feature lldp**<br>• **#system dot1q-tunnel transit** |

| デバイス モデル | NX-API モード |
|---|---|
| Cisco Nexus 9200、9300-EX、9336C-FX2、93240YC-FX2、およびN9K-C93360YC-FX2 スイッチ | プロンプトで次のコマンドを入力します。<br>• **#hardware access-list tcam region ing-l2-span-filter 0**（Cisco Nexus 93108 シリーズ スイッチのみ）<br>• **#hardware access-list tcam region ing-l3-span-filter 0**（Cisco Nexus 93108 シリーズ スイッチのみ）<br>• **# hardware access-list tcam region ing-racl 0**<br>• **hardware access-list tcam region ing-l3-vlan-qos 0**<br>• **# hardware access-list tcam region egr-racl 0**<br>• **# hardware access-list tcam region ing-ifacl 1024**<br>• **#feature nxapi**<br>• **#feature lldp**<br>• **#system dot1q-tunnel transit**<br>（注）<br>このコマンドは、Nexus 9200 スイッチではサポートされません。 |
| Cisco Nexus 9500-EX および 9500-FX シリーズ スイッチ（9504、9508、および 9516） | プロンプトで次のコマンドを入力します。<br>• **# hardware access-list tcam region ing-racl 0**<br>• **# hardware access-list tcam region ing-l3-vlan-qos 0**<br>• **# hardware access-list tcam region egr-racl 0**<br>• **# hardware access-list tcam region ing-ifacl 1024**<br>• **#feature nxapi**<br>• **#hardware acl tap-agg**<br>• **#feature lldp**<br>• **#system dot1q-tunnel transit** |

| デバイス モデル | NX-API モード |
|---|---|
| Cisco Nexus 9300-GX シリーズ スイッチ | プロンプトで次のコマンドを入力します。<br>• **# hardware access-list tcam region ing-racl 0**<br>• **# hardware access-list tcam region ing-l3-vlan-qos 0**<br>• **# hardware access-list tcam region egr-racl 0**<br>• **# hardware access-list tcam region ing-ifacl 1024**<br>• **#feature nxapi**<br>• **#hardware acl tap-agg**<br>• **#feature lldp**<br>• **#system dot1q-tunnel transit** |

# サポートされる Web ブラウザ

次の Web ブラウザが Nexus Dashboard Data Broker に対してサポートされています。

- Firefox 85.0 以降のバージョン。
- Chrome 88.0 以降のバージョン
- Microsoft Edge 88.0 以降のバージョン。

（注） 互換性のないブラウザを使用すると、リリース 3.10 の GUI 表示の問題が発生する可能性があります。

（注） ブラウザで JavaScript を有効にします。

# システム要件

次の表に展開サイズごとのシステム要件を示します：

表 *4:* 展開サイズごとのシステム要件

| 説明 | 小規模 | 中規模 | 大規模 |
|---|---|---|---|
| CPU（仮想または物理） | 6コア | 12 コア | 18 コア |
| メモリ | 8 GB RAM | 16 GB RAM | 24 GB の RAM |
| TAP および SPAN 集約のスイッチ数 | 最大 25 台のスイッチ | 最大 50 台のスイッチ | 75～100 台のスイッチ |
| ハードディスク | データ ブローカー ソフトウェアがインストールされているパーティションで最小 40 GB の空き領域が使用可能なこと。 | | |
| オペレーティング システム | Java をサポートする最近の 64 ビット Linux ディストリビューション。できれば Ubuntu、Fedora、または Red Hat が望ましい。 | | |
| その他 | Java 仮想マシン 1.8 | | |

# 注意事項と制約事項

Cisco Nexus Dashboard Data Broker は、Java 仮想マシン（JVM）で実行されます。Java ベースのアプリケーションとして、Cisco Nexus Dashboard Data Broker は任意の x86 サーバで実行できます。最適な結果を得るためには、次の点を推奨します。

- 両方とも JDK の一部である JConsole と VisualVM は、トラブルシューティングのために推奨される追加です（必須ではありません）。
- Cisco Nexus Dashboard Data Broker によるリンク ディスカバリで予測不能な動作を避けるために、トポロジ内の複数のスイッチに同じ名前を構成しないでください。
- 次の特殊文字は、ポート定義、ポート グループ、接続、リダイレクト、モニタリング デバイス、およびサービス ノードの説明フィールドでは使用できません。アポストロフィ（'）、より小さい（<）、より大きい（>）、二重引用符（"）、バックスラッシュ（\）、縦棒（|）、および疑問符（?）。
- スイッチでドメイン名が有効になっていると、LLDP ネイバーの変更が反映されず、その特定のスイッチのリンクが削除されます。この問題を回避するには、LLDP 機能を無効にしてから、**no feature lldp** CLI コマンドおよび **feature lldp** CLI コマンドをそれぞれ使用して再度有効にします。
- Cisco Nexus 9000 シリーズ スイッチが NX-API モードで 7.0(3)I4(1) 以降のバージョンを使用しており、フローが VLAN ファイラーを使用してインストールされている場合、デバイスは IP アクセス リストを通過させ、レイヤ 2 パケット上での照合を行いません。

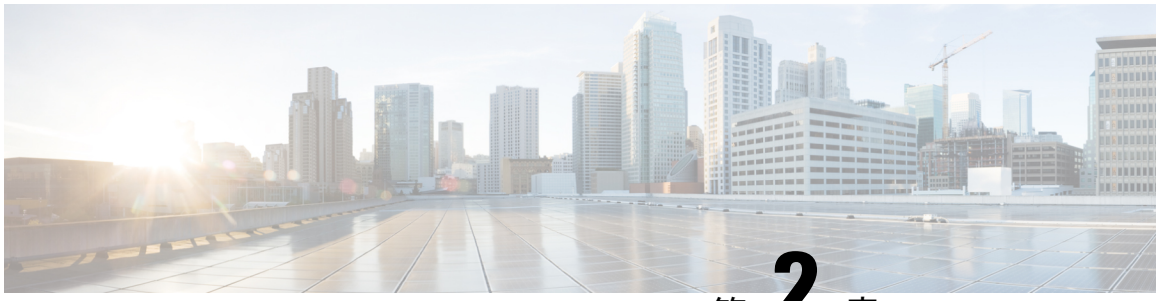
# ファイル名マトリックス

Cisco Nexus Dashboard Data Broker のファイル名マトリックス：

| 展開のモード | NXOS イメージ | モード | ファイル名 |
|---|---|---|---|
| 組み込み | 9.3(1)～9.3(5) | NXAPI | `ndb1000-sw-app-emb-k9-release-number.zip` |
| 集中型 | 9.3(1)～9.3(5) | NXAPI | `ndb1000-sw-app-k9-release-number.zip` |

# 相互運用性マトリクス

相互運用性マトリクスについては、*Cisco Nexus Dashboard Data Broker* リリース ノート、リリース *3.10.1* を参照してください。



第 2 章

# Cisco Nexus Dashboard Data Broker へのログインと管理

この章では、Cisco Nexus Dashboard Data Broker へのログインと管理、および GUI の概要について詳しく説明します。

リリース 3.10.1 から、Cisco Nexus Data Broker（NDB）の名前は、Cisco Nexus Dashboard Data Brokerに変更されました。ただし、GUIおよびインストール フォルダ構造と対応させるため、一部の NDB のインスタンスがこのドキュメントには残されています。NDB/ Nexus Data Broker/ Nexus Dashboard Data Brokerという記述は、相互に交換可能なものとして用いられています。



## 高可用性クラスタの構成

Cisco Nexus Dashboard Data Broker は、最大 5 台のコントローラによるアクティブ/アクティブモードの高可用性クラスタリングをサポートします。Cisco Nexus Dashboard Data Broker で高可用性クラスタリングを使用するには、Cisco Nexus Dashboard Data Broker の各インスタンスの `config.ini` ファイルを編集する必要があります。

NDDB リリース 3.10.4 は、3 ノードクラスタのみをサポートします。

スプリットブレイン シナリオの場合、3 ノード クラスタは次のように処理されます。

クラスタの正常性は黄色であると表示します。クラスタを動作状態にするには、少なくとも 2 つのノードが稼働し、クラスタ内で接続されている必要があります。そうでない場合、クラスタノードは非動作状態に移行します。オーバーライドオプションは使用できません。必要に応じて、VM やネットワークリンクを修正します。

（注） IPv6 は、集中型 Cisco Nexus Dashboard Data Broker モードでのみサポートされ、組み込みモードではサポートされません。

表 *5:* クラスタの動作ステータス

| クラスタ インジケータ | クラスタのステータス | 推奨 |
|---|---|---|
| 緑 | 使用可能 | ステータスが動作中のため、推奨事項はありません。 |
| イエロー | 一部のクラスタ ノードが使用できません | 既存の Nexus Dashboard Data Broker の構成に変更を加えたり、追加したりしないでください。 |
| 赤 | ノードはクラスタから分離されています。 | 既存の Nexus ダッシュボード データ ブローカーの構成に変更を加えたり、追加したりしないでください。<br>注: 2 ノード クラスタの場合、正規の操作が行われるようにするために、いずれか 1 つのクラスタ ノードでのみオーバーライドする必要があります。 |

### 始める前に

- すべての IP アドレスは、到達可能で、相互に通信できる必要があります。
- クラスタ内のすべてのスイッチは、すべてのコントローラに接続する必要があります。
- すべてのコントローラは、同じ HA クラスタリング設定情報を `config.ini` ファイルに持つ必要があります。
- すべてのコントローラは、まったく同じ情報を `ndb/configuration/startup` ディレクトリに持つ必要があります。
- クラスタ パスワードを使用する場合、すべてのコントローラは同じパスワードを `ndbjgroups.xml` ファイルに設定する必要があります。
- ノードを優先プライマリとしてマークするには、 `config.ini` ファイルのスーパーノード リストの最初のノードとして必要なノード IP アドレスを追加します。常に最初のノードを優先プライマリとして使用する場合は、 `config.ini` ファイルで `enablePreferredPrimary=true` を設定します。

優先プライマリノードを変更するには、ndb コントローラを 停止 し、 config.ini ファイルに必要な変更を加えます。

スーパー ノードのリストで最初のノードを優先プライマリとしてマークしたくない場合は、config.ini ファイルでパラメータを *false* に変更します。

```
enablePreferredPrimary=false
```

これで、障害が発生し、プライマリノードがダウンした場合、別のメンバー ノードがプライマリ ノードの役割を引き継ぎます。以前のプライマリ ノードが 起動した場合でも、メンバー ノードが引き続きプライマリ ノードになります。

（注） データ ブローカ コントローラは、（config.ini ファイルで）設定されているスーパーノードの数を確認します。数が 3 未満の場合は、2 ノード クラスタがサポートされていないことを示すエラーを表示します。

**手順**

**ステップ 1** クラスタ内のインスタンスの 1 つでコマンド ウィンドウを開きます。

**ステップ 2** ソフトウェアをインストールしたときに作成された ndb/configuration ディレクトリに移動します。

**ステップ 3** 任意のテキスト エディタで config.ini ファイルを開きます。

**ステップ 4** 次のテキストを探してください。

```
# HA Clustering configuration (semi-colon-separated IP addresses of all controllers that are part
of the cluster.)
# supernodes=<ip1>;<ip2>;<ip3>;<ipn>
```

**ステップ 5** **例**：

IPv4 の例。

```
# HA Clustering configuration (semi-colon-separated IP addresses of all controllers that are part
of the cluster.)
supernodes=10.1.1.1;10.2.1.1;10.3.1.1;10.4.1.1;10.5.1.1
```

**例**：

IPv6 の例。

```
# HA Clustering configuration (semi-colon-separated IP addresses of all controllers that are part
of the cluster.)
supernodes=2001:22:11::1;2001:33::44::1;2001:55:66::1
```

**ステップ 6** ファイルを保存し、エディタを終了します。

**ステップ 7** クラスタ内の Cisco Nexus Dashboard Data Broker のインスタンスごとに、ステップ 3 からステップ 7 を繰り返します。

**ステップ 8** Cisco Nexus Dashboard Data Broker を再起動します。

Nexus Dashboard Data Broker クラスタ展開の場合、ノード間の予想される遅延は 3 秒で、再試行は 3 回です。遅延時間と最大再試行回数は設定できます。以下の手順を参照してください。

### 次のタスク

（オプション）この手順に従って、ノードの遅延時間と再試行回数を設定します。

1. クラスタ内のインスタンスの 1 つでコマンド ウィンドウを開きます。
2. ndb 設定ディレクトリに移動します。
3. 任意のテキスト エディタで ndbjgroups.xml ファイルを開きます。
4. 次のテキストを探します。

   ```
   FD timeout="3000" max_tries="3"/
   ```

5. *[*遅延時間（*Latency Time*）*]* の値と *[*最大再試行回数（*maximum_tries*）*]* の値を変更します。
6. ファイルを保存し、エディタを終了します。
7. クラスタのすべてのインスタンスに対して上記の手順を繰り返します。

# 高可用性クラスタのパスワード保護

### 手順

**ステップ 1** クラスタ内のインスタンスの 1 つでコマンド ウィンドウを開きます。

**ステップ 2** ndb/configuration ディレクトリに移動します。

**ステップ 3** 任意のテキスト エディタで ndbjgroups.xml ファイルを開きます。

**ステップ 4** 次のテキストを探します。

```
<!-- <AUTH auth_class="org.jgroups.auth.MD5Token" auth_value="ciscoXNC" token_hash="MD5"></AUTH>
-->
```

**ステップ 5** AUTH 行からコメントを解除します。

**例**：

```
<AUTH auth_class="org.jgroups.auth.MD5Token" auth_value="ciscoXNC" token_hash="MD5"></AUTH>
```

**ステップ 6** （任意） auth_value 属性のパスワードを変更します。

デフォルトでは、クラスタはパスワード「ciscoXNC」で保護されています。このパスワードは、どんな値にでも変更できます。ただし、クラスタ内のすべてのマシン上で同じ変更を行う必要があります。

**ステップ 7** ファイルを保存し、エディタを終了します。

# スタンバイ ノードの追加

リリース3.10.4以降では、クラスタをサポートするためにスタンバイノードを追加できます。`config.ini` ファイルでスーパーノードを構成する際には、スタンバイノードであることを示すために、スタンバイノードの IP アドレスに `-standby` を追加する必要があります。次に例を示します。

```
supernodes=<ip1>;<ip2>;<ip3>;<ip4>-standby
```

リリース 3.10.4 は、3 ノード クラスタのみをサポートします。3 つのノードすべてが正常に動作している場合、クラスタは完全に正常であるといい、（3 つのノードのうち）2 つが正常に動作している場合は部分的に正常であるといいます。1 つのノードのみが正常に動作している場合、つまり（クラスタの 3 つのノードのうち）2 つのノードが ダウンしている場合、クラスタは異常です。実行中のノードでクラスタを形成するスタンバイ ノードは、手動で起動する必要があります。

以下のような場合、スタンバイノードは自動的に終了します。

- 実行中のノードが突然終了した場合。
- リカバリ後、以前ダウンしていた 2 つのノードがアップ状態になった場合。

### スタンバイ ノードに対する注意事項と制限事項

- クラスタ内のすべてのノードがダウンしている場合は、スタンバイノードを起動できません。スタンバイ ノードでクラスタを形成するには、1 つのノードが実行されている必要があります。
- クラスタが正常な場合（つまり、3 ノード クラスタ内の 2 つのノードが正常に動作している場合）は、スタンバイ ノードを起動できません。
- スタンバイノードを起動する前には、クラスタが正常でなくなっていることを確認します。クラスタのノードがダウンしていること、そしてノード間の接続が中断されていないことを確認します。

  ノード 1 とノード 2 が一緒に配置され、ノード 3 とスタンバイ ノードが別の場所に一緒に配置されているシナリオを考えます。ノード 1 と 2 がノード 3 とスタンバイノードから一時的に切断された場合、ノード 1 と 2 がダウンしていると誤って解釈される可能性があります。この情報に基づいてスタンバイノードを起動すると、スタンバイノードとノード 3 がクラスタを形成します（ノード 1、2 が稼働している場合でも）。これにより、ノード 1 とノード 2 とノード 3 とスタンバイノード間の接続が復元されたとき、設定の不一致/損失が発生します。

# Cisco Nexus Dashboard Data Broker GUI へのログイン

Cisco Nexus Dashboard Data Broker、リリース 4.0 は、Nexus ダッシュボードのサービスとして利用できます。

ND GUI から Nexus Dashboard Data Broker にアクセスするには、次の手順を使用します。

### 始める前に

Nexus Dashboard リリース 3.0(1i)にログインします。

### 手順

**ステップ 1** ND GUI で、**[操作（Operate）]**>**[サービス（Services）]**>**[インストール済みサービス（Installed Services）]** に移動します。

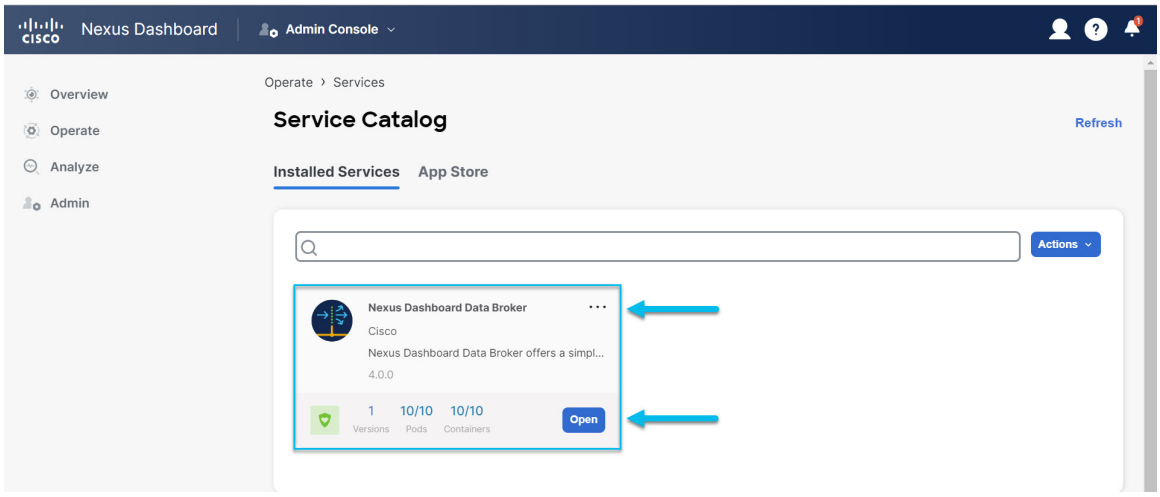
Nexus Dashboard Data Broker サービスが表示されます。

**ステップ 2** **[開く（Open）]** をクリックします。

標準の Nexus Dashboard Data Broker GUI 画面が表示されます。

Nexus Dashboard Data Broker GUI の個別のログインは必要ありません。

***図 1 : ND 上の Nexus Dashboard Data Broker***




3 つのドットをクリックして、Nexus Dashboard Data Broker を **[無効（Disable）]** または **[再起動（Restart）]** できます。

# コントローラ アクセスの変更

GUI への非暗号化（HTTP）アクセスおよびコントローラ アクセスへの API は、デフォルトで無効になっています。URL http://<host>:8080 ではコントローラにアクセスできません。

HTTP へのコントローラ アクセスを変更するには、次の手順を実行します。

### 始める前に

Cisco Nexus Dashboard Data Broker には、Cisco Nexus Dashboard Data Broker とブラウザ間の HTTPS 接続用の証明書が付属しています。これを別の証明書に変更できます。

スクリプト **generateWebUIcertificate.sh** は、**ndb/configuration** フォルダにあります。このスクリプトを実行すると、出荷された証明書が **old_keystore** に移動され、新しい証明書が **keystore** に生成されます。次回の Cisco Nexus Dashboard Data Broker の再起動時に、この新しい証明書が使用されます。

### 手順

**ステップ 1** 次の例に示すように、構成ディレクトリの `tomcat-server.xml` ファイルにあるポート 8080 のコネクタからコメント文字を削除します。

```
<Service name="Catalina">
<!--
<Connector port="8080" protocol="HTTP/1.1"
connectionTimeout="20000"
redirectPort="8443" server="Cisco NDB" enableLookups="false" />
-->
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS"
keystoreFile="configuration/keystore"
keystorePass="ciscondb" server="Cisco NDB"
connectionTimeout="60000" enableLookups="false" />
```

**ステップ 2** コントローラを再起動します。

# Cisco Nexus Dashboard Data Broker の GUI の概要

Cisco Nexus Dashboard Data Broker GUI には次のタブが含まれています。これらの各タブについては、このガイドの後続のページで（個別の章として）詳細に説明します。

- ダッシュボード
- トポロジ
- デバイス
- 接続
- コンポーネント
- [セッション（Sessions）]
- [統計（Statistics）]
- トラブルシュート

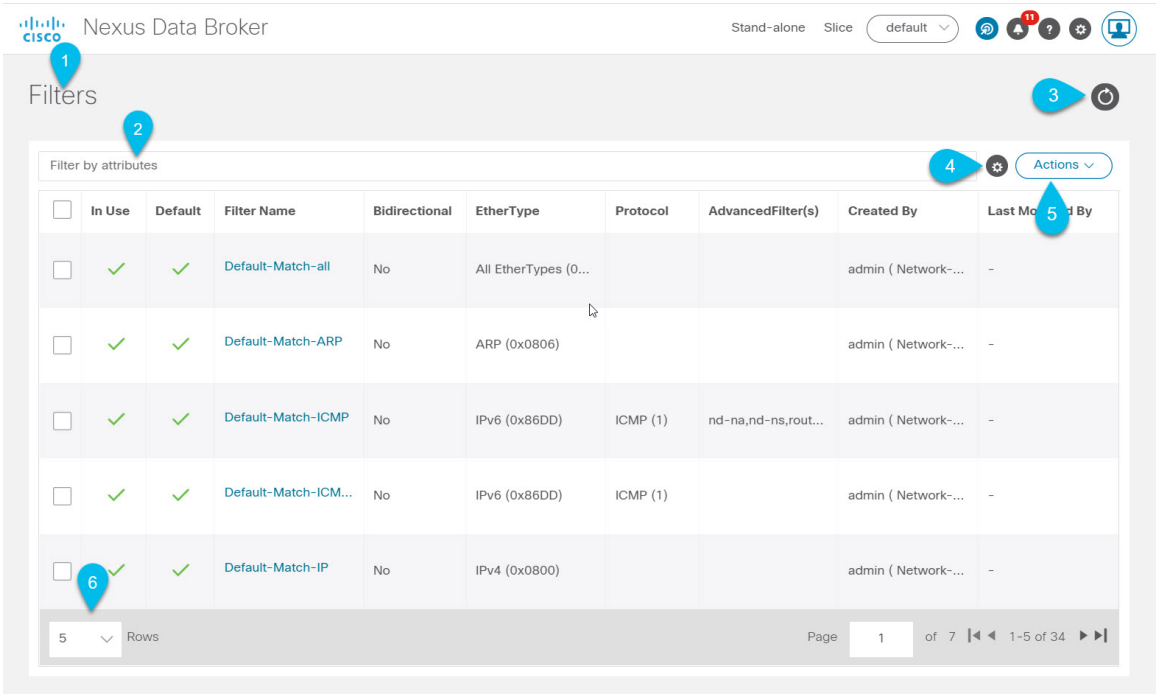
- [管理（Administration）]

ヘッダー アイコンの詳細については、ヘッダーを参照してください。

# Cisco Nexus Dashboard Data Broker の画面のコンポーネント

タブ/サブタブをクリックすると、そのタブの現在の情報が表で表示されます。

リリース 3.10.1 Cisco Nexus Dashboard Data Broker GUI のタブの 1 つを表す典型的な画面を次に示します。




- 1 - タブ/サブタブの名前。
- 2 - *[属性によるフィルタ（Filter by attributes）]* バーを使用して、選択したタブの詳細を含む表示された表でフィルタ処理を行います。属性、演算子、およびフィルタ値を選択します。

  テーブルの要素にカーソルを合わせると表示される *[フィルタ（Filter）]* アイコンに基づいて、表示されたテーブルをフィルタ処理することもできます。
- 3 - *[更新（Refresh）]* アイコンを使用して、表示されている詳細を更新し、タブ/サブタブに関する最新情報を取得します。
- 4—*[列のカスタマイズ（Column Customization）]* アイコンを使用して、表示されたテーブルに表示する列を選択します。
- 5—**[アクション（Actions）]** ボタンをクリックして、画面で使用可能なアクションを表示します。

- 6 — ポートレットに表示する行の数を、**[行（Rows）]** ドロップダウン リストから選択します。

# ヘッダー

このセクションでは、Cisco Nexus Dashboard Data Broker GUI のヘッダー（右上隅）アイコンの概要について説明します。

**表 *6 : Cisco Nexus Dashboard Data Broker* ヘッダー アイコン**

| アイコン | 説明 |
|---|---|
| スライス（Slice） | デフォルト スライスを表示します。 |
| 図 *2 :* 作成  | 頻繁に使用される構成および管理手順へのクイック ナビゲーションを提供します。 |
| 図 *3 :* アラーム  | 矛盾した NDB デバイスの数を表示します。[アラーム（Alarm）] のアイコンをクリックすると、詳細を表示している [フロー管理（Flow Management）] タブに移動します。 |
| 図 *4 : [*ヘルプ（***Help***）*]* メニュー バー  | 次のオプションが表示されます。<br>• **新機能**：最新リリースの新機能を表示します。<br>• **ヘルプ**：オンライン ヘルプ コンテンツを表示します。 |
| 図 *5 : [*システム ツール（***System Tools***）*]* メニュー バー  | 次のオプションを提供します。<br>• **アプリケーション プロパティ**：TLS 関連のパスワードを設定します。<br>• **[Northbound API]**：**[Swagger]** UI に移動します。Nexus Dashboard Data Broker の REST API の詳細が表示されます。<br>• **Nexus Dashboard Data Broker について**：ビルドやバージョンなど、Nexus Dashboard Data Broker の詳細を表示します。 |

| アイコン | 説明 |
| --- | --- |
| 図 *6 : [*ユーザー プロファイル（***User Profile***）*]* メニューバー<br>  | 次のオプションを提供します。<br>• **ようこそ** ユーザー：GUI の現在のユーザーを表示します。 |

# Syslog

Nexus Dashboard Data Broker サーバー バックエンドでは、ログを Syslog サーバーに送信するように `logback.xml` ファイルを構成できます。ログ形式は必要に応じてカスタマイズできます。logback 構成ファイルの場所は、`/ndb/configuration/logback.xml` です。

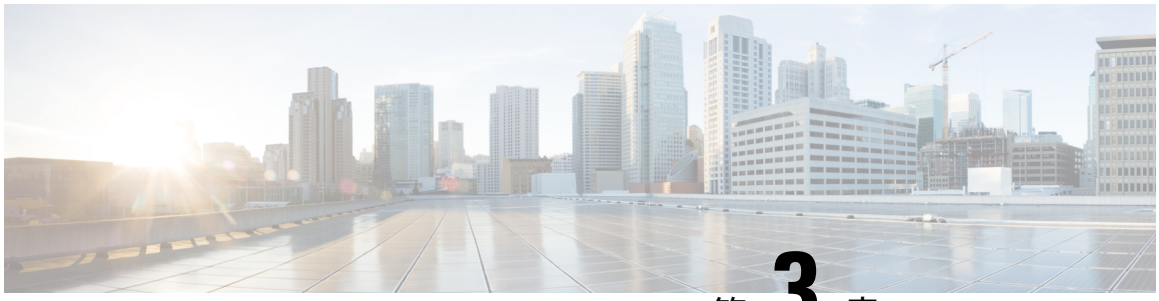
（注） Nexus Dashboard Data Broker サーバーを実行している場合は、`logback.xml` ファイルに変更を加えた後で、サーバーを再起動します。

```
Sample Syslog configuration:

Add below config with respective Syslog server IP address and port number in logback.xml
 file.
  <appender name="SYSLOG" class="ch.qos.logback.classic.net.SyslogAppender">
    <syslogHost>10.16.206.171</syslogHost>
    <facility>LOCAL7</facility>
    <port>514</port>
    <suffixPattern>[%thread] %logger %msg</suffixPattern>
  </appender>

Append "<appender-ref ref="SYSLOG" />" in root as shown below,
  <root level="error">
    <appender-ref ref="STDOUT" />
    <appender-ref ref="SYSLOG" />
    <appender-ref ref="ndb.log" />
  </root>
```

アップグレードを行うと、`logback.xml` ファイル内のこれらの構成変更は失われます。コントローラを新しい Nexus Dashboard Data Broker バージョンにアップグレードした場合には、-手動で構成を確認して復元してください。



第 3 章

# Cisco Nexus 9000 シリーズ スイッチの構成

リリース 3.10.1 から、Cisco Nexus Data Broker（NDB）の名前は、Cisco Nexus Dashboard Data Brokerに変更されました。ただし、GUIおよびインストール フォルダ構造と対応させるため、一部のNDBのインスタンスがこのドキュメントには残されています。NDB/ Nexus Data Broker/ Nexus Dashboard Data Brokerという記述は、相互に交換可能なものとして用いられています。

この章は、次の項で構成されています。



## Cisco Nexus 9000 シリーズ スイッチの注意事項と制限事項

Cisco Nexus Dashboard Data Broker を介した Cisco Nexus 9000 シリーズ スイッチの設定については、次の注意事項と制限事項を参照してください。

- Cisco Nexus Dashboard Data Broker は、Cisco Nexus 9000 シリーズ スイッチ ファミリの NX-API プロトコルをサポートします。
- Tap aggregation は、N9K-X9700-EX および N9K-X9700-FX ライン カードを搭載した Cisco Nexus 9500 プラットフォーム スイッチでサポートされます。
- N9K-X9700-EX およびN9K-X9700-FX ライン カードで tap aggregration を有効にするには、Cisco Nexus 9500 スイッチで hardware acl tap-agg をグローバルに構成します。
- Cisco Nexus Dashboard Data Broker によってプロビジョニングされるデバイスは、LLDP が有効になっていると想定されており、Cisco Nexus Dashboard Data Broker とのデバイスの関連付け中は、LLDP機能を無効にしないでください。LLDP機能が無効になっている場合、

デバイスを削除して再追加しないと修正できない不整合が Cisco Nexus Dashboard Data Broker で発生する可能性があります。

- Cisco Nexus Dashboard Data Broker は、ポート定義によって設定されたデバイス インターフェイスが L2 スイッチ ポートであり、これらのインターフェイスにデフォルトでスイッチポート トランクとしてのデバイス構成があると想定しています。
- Cisco Nexus 9000 シリーズ スイッチを NX-API モードの Cisco Nexus Dashboard Data Broker を介して Tap/SPAN 集約用に展開する前に、次の構成を完了する必要があります。
  - IPv4 ポート ACL または MAC ポート ACL 用の ACL TCAM のリージョン サイズを構成します。
  - **feature nxapi** コマンドを使用して、スイッチで NX-API 機能を有効にします。
  - すべてのスイッチ間ポートおよびポート チャネルで **switchport mode trunk** を構成します。

# Cisco Nexus 9000 シリーズ スイッチでの TCAM ハードウェア サイジングの設定

TCAM構成は、フィルタリング要件に基づいています。フィルタリング要件に基づいて、複数のTCAMエントリを構成する必要がある場合があります。SPANを構成するには、次の手順を実行します。

## 手順の概要

1. **hardware access-list tcam region <region> <tcam-size>** コマンドを使用して、次の TCAM リージョンを設定します。

## 手順の詳細

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **hardware access-list tcam region <region> <tcam-size>** コマンドを使用して、次のTCAMリージョンを設定します。 | NAT ACL[nat] size = 0<br>Ingress PACL [ing-ifacl] size = 1024<br>VACL [vacl] size = 0<br>Ingress RACL [ing-racl] size = 0<br>Ingress L2 QOS [ing-l2-qos] size = 256<br>Ingress L3/VLAN QOS [ing-l3-vlan-qos] size = 0<br>Ingress SUP [ing-sup] size = 512<br>Ingress L2 SPAN filter [ing-l2-span-filter] size = 256<br>Ingress L3 SPAN filter [ing-l3-span-filter] size = 0 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | Ingress FSTAT [ing-fstat] size = 0<br>span [span] size = 512<br>Egress RACL [egr-racl] size = 1792<br>Egress SUP [egr-sup] size = 256<br>Ingress Redirect [ing-redirect] size = 512<br>Egress L2 QOS [egr-l2-qos] size = 0<br>Egress L3/VLAN QOS [egr-l3-vlan-qos] size = 0<br>Ingress Netflow/Analytics [ing-netflow] size = 512<br>Ingress NBM [ing-nbm] size = 0<br>TCP NAT ACL[tcp-nat] size = 0<br>Egress sup control plane[egr-copp] size = 0<br>Ingress Flow Redirect [ing-flow-redirect] size = 0<br>Ingress PACL IPv4 Lite [ing-ifacl-ipv4-lite] size = 0<br>Ingress PACL IPv6 Lite [ing-ifacl-ipv6-lite] size = 0<br>MCAST NAT ACL[mcast-nat] size = 0<br>Ingress PACL Super Bridge [ing-pacl-sb] size = 1024<br>Ingress Storm Control [ing-storm-control] size = 0<br>Ingress VACL redirect [ing-vacl-nh] size = 0<br>Egress PACL [egr-ifacl] size = 0<br><br>Cisco Nexus 9000 シリーズ スイッチ TCAM ハードウェア サイジング構成の手順を追った説明については、*Cisco Nexus 9000 Series NX-OS Security Configuration Guide*を参照してください。<br><br>（注）<br>OpenFlow モードの Cisco Nexus ダッシュボード データ ブローカは、OpenFlow TCAM リージョンが倍幅で設定されている場合にのみ（たとえば、**hardware access-list tcam region openflow 512 double-wide**）、イーサネット MAC の送信元アドレスと接続先アドレスをマッチングする機能をサポートします。OpenFlow TCAM リージョンが非倍幅で設定されている場合、イーサ タイプのマッチングのみがマッチング機能としてサポートされます。 |

# CLI を使用した Cisco Nexus 9000 Series Switches での Cisco NX-API の有効化

トポロジで接続された複数の Cisco Nexus 9000 シリーズ スイッチを管理できるようになりました。Cisco Nexus Dashboard Data Broker プラグインは、LLDP を使用してスイッチの相互接続を検出し、Cisco Nexus Dashboard Data Broker 内のトポロジ サービスを更新できます。スイッチの相互接続には、物理リンクまたはポート チャネル インターフェイスを使用できます。トポ

ロジには、NDB デバイス リストに追加された Cisco Nexus 9000 シリーズ スイッチ間の相互接続のみが表示されます。トポロジの相互接続が GUI に表示されます。

Cisco Nexus 9000 シリーズ スイッチで Cisco NX-API を有効にするには、次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | 管理インターフェイスを有効にします。 | スイッチの管理インターフェイスを有効にします。 |
| ステップ 2 | switch# **conf t** | コンフィギュレーション モードを開始します。 |
| ステップ 3 | switch (config) # **feature nxapi** | NX-API 機能を有効にします。 |
| ステップ 4 | switch (config) # **nxapi http port** *80* | HTTP ポートを構成します。 |
| ステップ 5 | switch (config) # **nxapi https port** *443* | HTTPS ポートを構成します。<br>Cisco Nexus 9000 シリーズ スイッチで NX-API 機能を有効にするための段階的な設定情報については、*Cisco Nexus 9000 Series NX-OS Programmability Guide* を参照してください。 |

# スイッチ間ポートおよびポートチャネルでのトランクとしてのスイッチ ポート モードの有効化

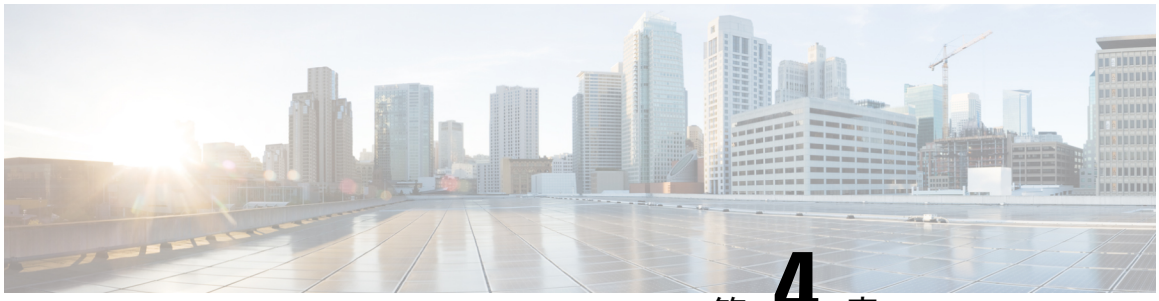
スイッチ間ポートおよびポート チャネルでスイッチ ポート モードを有効にするには、次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | switch(config)# **config t** | 構成モードを有効にします。 |
| ステップ 2 | switch(config)# interface {{**type** *slot*/*port*} \| {*port-channel number*}} | 設定するインターフェイスを選択します。 |
| ステップ 3 | switch(config-if)# **switchport mode** {*access* \| *trunk*} | スイッチ間ポートおよびポートチャネルでスイッチポートモードをアクセスまたはトランクとして設定します。 |
| ステップ 4 | switch(config)# **exit** | コンフィギュレーション モードを終了します。 |

# 第 部

# Cisco Nexus Dashboard Data Broker の構成



第 4 章

# ダッシュボード

この章では、Cisco Nexus Data Broker ダッシュボードについて詳しく説明します。ダッシュボードは、複数のコンポーネントとデバイスからの情報を統合された表示にまとめます。

リリース 3.10.1 から、Cisco Nexus Data Broker（NDB）の名前は、Cisco Nexus Dashboard Data Brokerに変更されました。ただし、GUI およびインストール フォルダ構造と対応させるため、一部の NDB のインスタンスがこのドキュメントには残されています。NDB/ Nexus Data Broker/ Nexus Dashboard Data Brokerという記述は、相互に交換可能なものとして用いられています。



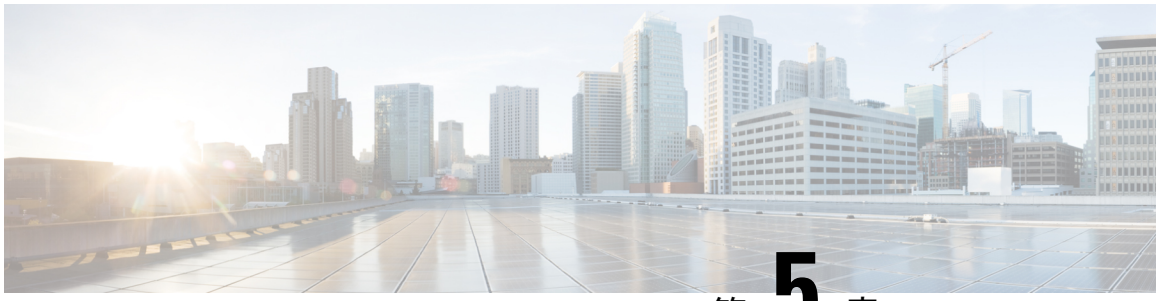
# ダッシュボード

**ダッシュボード**の目的は、ネットワーク管理者とストレージ管理者が Cisco Nexus Dashboard Data Broker の健全性とパフォーマンスに関する特定の領域に集中できるようにすることです。この情報は、24 時間のスナップショットとして提供されます。

メニュー バーから **[ダッシュボード（Dashboard）]** を選択します。**[ダッシュボード（Dashboard）]** ウィンドウには、次のダッシュレットが表示されます。

- **リソース別のステータス** — Nexus Dashboard Data Broker コントローラに接続されているリソースのステータスは、色分けされた丸で表示されます。リソースは次のとおりです。
  - NDB デバイス
  - 入力ポート
  - フィルタ
  - モニタリングツール
  - Connections
- **処理済みデータ/受信済みデータ（Data Handled / Received since）** 日付（*date*）：示された日付以降に Nexus Dashboard Data Broker コントローラによって受信および送信されたデータの総量。
- **NDB ランタイム**：現在のクラスタのランタイム。

- **NDB の最後の再起動**：クラスタが最後に再起動された日時。



第 5 章

# トポロジ

この章では、ネットワーク トポロジの詳細と、Cisco Nexus Dashboard Data Broker のデバイスと接続の詳細について説明します。

リリース 3.10.1 から、Cisco Nexus Data Broker（NDB）の名前は、Cisco Nexus Dashboard Data Brokerに変更されました。ただし、GUI およびインストール フォルダ構造と対応させるため、一部の NDB のインスタンスがこのドキュメントには残されています。NDB/ Nexus Data Broker/ Nexus Dashboard Data Brokerという記述は、相互に交換可能なものとして用いられています。



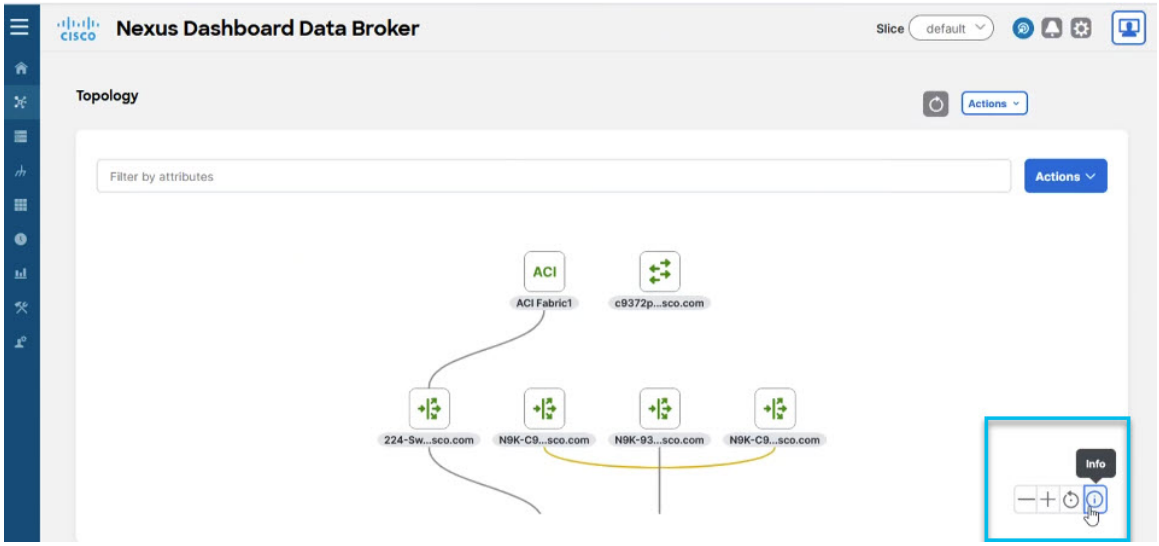
# トポロジ

**[トポロジ（Topology）]** タブには、Cisco Nexus Dashboard Data Broker ネットワークの統合ビューが表示されます。

Nexus Dashboard Data Broker リリース 4.0 以降、[トポロジ（Topology）] のさまざまなノードを示すために使用されるアイコンが変更され、外観が強化され、カスタマーエクスペリエンスが向上しました。

トポロジ図は階層形式で表示されます。SPAN デバイス（ACI ファブリックや実稼働スイッチなど）が最初の行に表示され、その後に NDB デバイスが続きます。最後の行はモニタリング ツールです。さまざまなノード間の接続も示されています。ページの下部にある **[情報（Info）]** アイコンをクリックして、**[トポロジの凡例（TopologyLegend）]** ウィンドウを表示します。**[トポロジの凡例（TopologyLegend）]** ウィンドウには、トポロジ図で使用されるアイコンへのキーが含まれています。

図 *7*: *[*情報（*Info*）*]* アイコン

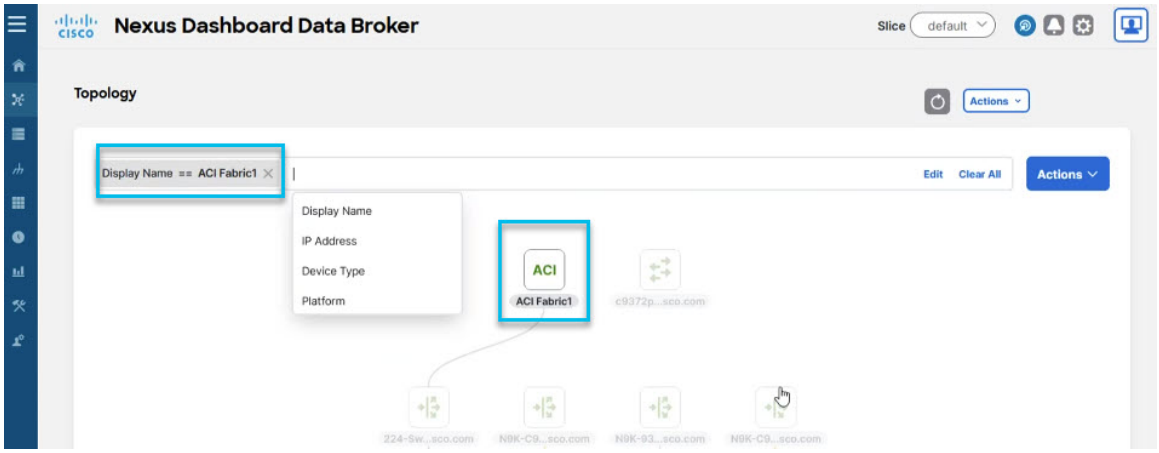



ノードに関する簡単な情報を取得するには、ノードをクリック（シングルクリック）します。ノードに関する詳細を表示するには、ノードをダブルクリックします。画面の右側に別のポップアップ ウィンドウが表示されます。

*[*属性でフィルタ処理（*Filter by attributes*）*]* 検索バーを使用して、トポロジの表示ノードをフィルタ処理します。フィルタ パラメータは、表示名、IP アドレス、デバイスタイプ、およびプラットフォームです。選択したパラメータに基づいて、関連するノードがトポロジ図で強調表示されます。検索条件を入力する形式を次の例に示します。

```
Display Name == ACI Fabric1
```

図 *8*: 属性によるフィルタ処理検索バー




トポロジ図は、デフォルトの垂直ビューで表示されます。トポロジ ビューを変更する詳細な手順については、トポロジ ビューの変更 （35 ページ） タスクを参照してください。

（注） 最新のトポロジを表示するには、**[更新（Refresh）]**（  ）をクリックします。

**[更新（Refresh）]** アイコンの横にある **[アクション（Actions）]** ボタンを使用すると、次のタスクを実行するためにすばやくアクセスできます。

- **NDB デバイスの追加（Add NDB Device）**：詳細については、NDB デバイスの追加を参照してください。
- **[スパン デバイスの追加（Add Span Device）]**：詳細については、スパン デバイスの追加（57 ページ）を参照してください。
- **[モニタリング ツールの追加（Add Monitoring Tool）]** — 詳細については、モニタリング ツールの追加を参照してください。

# トポロジ ビューの変更

トポロジ ビューには、デフォルトの垂直ビュー、水平ビュー、およびカスタム ビューの 3 つのレイアウトがあります。トポロジ表示を必要に応じてカスタマイズするには、次の手順を使用します。

**手順**

**ステップ 1** *[*属性でフィルタ（*Filter by attributes*）*]* フィールドの横にある **[アクション（Actions）]** ボタンをクリックします。

ポップアップに、使用可能なオプションが表示されます。

**ステップ 2** **[レイアウト（Layout）]** > **[水平（Horizontal）]** ビューをクリックして、レイアウトをデフォルトの垂直ビューから水平ビューに変更します。

水平ビューでは、ノードは階層形式で表示されません。

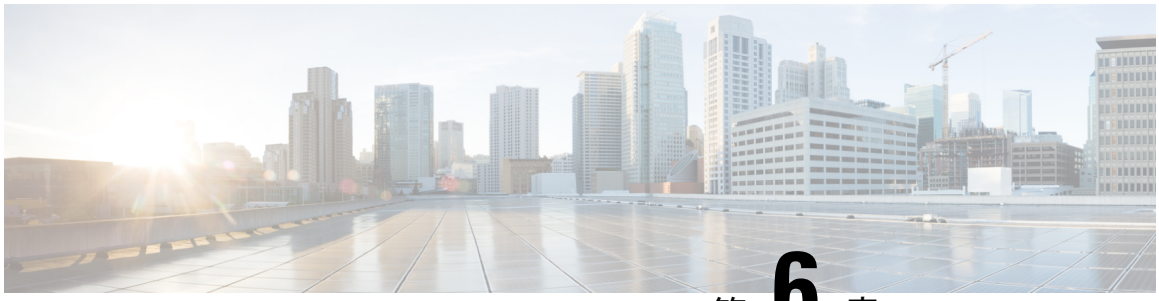
レイアウトを垂直表示から水平表示に変更することが目的の場合は、ここで停止できます。ビューをカスタマイズする必要がある場合は、次のステップに進みます。

**ステップ 3** **[レイアウト（Layout）]**をクリックし、 **[編集（Edit）]** オプションを有効にしてレイアウトを *[*カスタム（*Custom*）*]*に変更します。

これで、ノードの位置をドラッグして並べ替えることができます。

**ステップ 4** **[レイアウト（Layout）]** > **[保存（Save）]** をクリックします。

**[カスタム（Custom）]** レイアウト オプションが、すでに使用可能な垂直および水平レイアウト オプションに追加されました。



第 6 章

# デバイス

この章では、Cisco Nexus Dashboard Data Broker のデバイスについて詳しく説明します。

リリース 3.10.1 から、Cisco Nexus Data Broker（NDB）の名前は、Cisco Nexus Dashboard Data Brokerに変更されました。ただし、GUI およびインストール フォルダ構造と対応させるため、一部の NDB のインスタンスがこのドキュメントには残されています。NDB/ Nexus Data Broker/ Nexus Dashboard Data Brokerという記述は、相互に交換可能なものとして用いられています。



## デバイス

**[デバイス（Device）]** タブには、次のサブタブがあります。

- **NDB デバイス（NDB Devices）**：NDB コントローラによって管理される集約デバイス。詳細については、NDB デバイスを参照してください。
- **[スパン デバイス（Span Devices）]**：NDB に接続されたスイッチ（Nexus/Catalyst）およびコントローラ（Cisco APIC/Cisco DNAC）。詳細については、SPAN デバイス （54 ページ）を参照してください。
- **タップ デバイス（Tap Devices）**：NDB コントローラに接続されているタップ デバイス。詳細については、タップ デバイスを参照してください。
- **[デバイス グループ（Device Groups）]**：NDB デバイスが分離されるグループ。詳細については、デバイス グループを参照してください。

## NDB デバイス

**[NDB デバイス（NDB Devices）]** タブには、NDB コントローラに接続されているすべてのデバイスの詳細が表示されます。

表には次の詳細が表示されます。

表 *7: NDB* デバイス

| 列名 | 説明 |
|---|---|
| **[ステータス（Status）]**（表の最初の列） | NDB に接続されているデバイスの現在のステータス。色で示します。次のオプションがあります。<br>• 緑色：デバイスが動作可能であり、NDB コントローラに接続されていることを示します。<br>• 赤色：失敗を示します。デバイスは NDB コントローラに接続されていません。<br>• 黄色：デバイスは接続されていますが、まだ準備ができていないことを示します。デバイスを再起動し、ステータスが緑色になるまで数分間待ちます。更新して確認します。<br>• 灰色：デバイスがメンテナンス モードになっています。 |

| 列名 | 説明 |
| --- | --- |
| IP アドレス | |

| 列名 | 説明 |
| --- | --- |
| | デバイスの IP アドレス。<br><br>このフィールドはハイパーリンクです。IP アドレスをクリックすると、デバイスの詳細が表示されます。<br><br>**[IP アドレス（IP Address）]** をクリックします。デバイスに関する詳細情報を含む新しいペインが右側に表示されます。ここから実行できる追加アクションは次のとおりです。<br><br>• デバイスの編集<br>• デバイスをオフラインにする<br>• グローバル構成の編集<br><br>（注）<br>*[デバイスをオフラインにする（Take Device Offline）]* アクションは通常灰色で表示されています。メンテナンス モードのデバイスでのみ使用できます。<br><br>対応するタブをクリックして、デバイスの **[ポート（Ports）]**、**[ポート チャネル（Port Channels）]**、および **[ポート グループ（Port Groups）]** を表示することもできます。ポート チャネルとグループの詳細については、ポート チャネルとグループを参照してください。<br><br>**[詳細（Details）]** アイコン（  ）をクリックして、デバイスの詳細を取得します。新しいウィンドウは、選択されたデバイスに対する次の詳細を表示します。<br><br>• [全般（General）]<br>• ポート<br>• ポート チャネル<br>• Port Groups<br>• グローバル設定<br>• [セッションの監視]<br>• [フロー統計情報（Flow Statistics）]<br>• ポート統計情報<br>• [TCAM リソース使用率（TCAM Resource Utilization）]<br><br>**[詳細（Details）]** |

| 列名 | 説明 |
|---|---|
| | タブから実行できる追加のアクション：<br>• [グローバル ACL のトリガー（Trigger Global ACLs）]：このアクションは、デバイスの構成されていないインターフェイスを識別し、それらすべてのインターフェイスにグローバル ACL を付加します。グローバル ACL はデバイスのすべてのインターフェイスに設定する必要があります。<br>• ポートチャネルの追加 |
| デバイス名 | デバイスの構成時に管理者が指定したデバイス名（スイッチ名）。デバイス名は、デバイス ステータスが緑の場合にのみ表示されます。デバイスのステータスが赤または黄の場合、デバイス名は表示されません。 |
| プラットフォーム | デバイスのプラットフォーム。 |
| ノード ID（Node ID） | デバイスのノード ID。 |
| [プロファイル名（Profile Name）] | デバイスの追加時に構成されたデバイスのプロファイル。 |
| NX-OS | デバイス上で現在実行されているソフトウェアのバージョン。 |
| モード | スイッチが現在使用しているモード。次のオプションがあります。<br>• [NDB モード（NDB mode）]：スイッチ全体（すべてのインターフェイス）が NDB コントローラによって管理されることを示します。<br>• [ハイブリッド（Hybrid）]：デバイスの一部のインターフェイスのみが NDB コントローラーによって管理されることを示します。<br>（注）<br>デフォルトでは、この列は隠れています。デバイスの追加中にデバイスでハイブリッドモードが有効になっていた場合、この列が表示されます。 |
| ポート | NDB コントローラが NDB デバイスと通信するために使用するポート。 |

| 列名 | 説明 |
|---|---|
| ステータスの説明 | NDB デバイスと NDB コントローラ間の接続のステータス。次のオプションがあります。<br>• [接続成功（Connection succeeded）]：デバイスと NDB コントローラ間の接続が成功したことを示します。<br>• [接続失敗（Connection failed）]：デバイスと NDB コントローラ間の接続が失敗したことを示します。認証に失敗した、接続が拒否された（不正なポート）など、失敗の理由も表示されます。<br>• [接続の準備ができていません（Connection not ready）]：デバイスのリロードが失敗したことを示します。 |

**[NDB デバイス（NDB Devices）]** タブから次のアクションを実行できます。

- **[デバイスの追加（Add Device）]**：これを使用して、新しいデバイスを追加します。詳細については、デバイスの追加を参照してください。
- **[デバイスの再検出（Rediscover Device）]**：行の先頭にあるチェックボックスをオンにして、必要なデバイスを選択します。**[アクション（Actions）]** > **[デバイスの再検出（Rediscover Device(s)）]** をクリックします。ポップアップが表示されます。**[再検出（Rediscover）]** をクリックして、選択されたデバイスを再検出します。デバイスの再検出を行うと、グローバル ACL が再接続されます。

（注） デバイスが再検出されると、UDF、ポート、グローバル、および接続の再構成が行われ、これによりトラフィックが失われます。

構成エラーがある場合は、再検出を使用してデバイスを再構成します。

チェックボックスを選択せずに再検出アクションを選択すると、エラーが表示されます。デバイスを選択するように求められます。

- **[デバイスの再接続（Reconnect Device）]**：行の先頭にあるチェックボックスをオンにして、必要なデバイスを選択します。**[アクション（Actions）]**>**[デバイスの再接続（Reconnect Device）]** をクリックします。ポップアップが表示されます。**[再接続（Reconnect）]** をクリックして、選択したデバイスを再接続します。再接続アクションは、デバイスと NDB コントローラ間の接続が失敗した場合、再確立するために使用されます。

  チェックボックスを選択せずに再接続アクションを選択すると、エラーが表示されます。デバイスを選択するように求められます。

- **[プロファイルの更新（Update Profile）]**：このアクションを使用して、デバイスのプロファイルを追加または更新します。このタスクの詳細については、プロファイルの更新を参照してください。
- **[デバイスの削除（Delete Device）]**：行の先頭にあるチェックボックスをオンにして、必要なデバイスを選択します。**[アクション（Actions）]**>**[デバイスの削除（Delete Device）]** をクリックします。ポップアップ ウィンドウが表示されます。
  - **[削除（Delete）]**：このオプションを使用して、デバイス構成を保持したまま NDB コントローラからデバイスを削除します。

（注） リリース 3.10.5 以降、デバイスを削除すると、TLS 情報がコントローラに保持されます。同じ証明書を使用する場合は、デバイスを再度追加するときに、**[デバイスの追加 の確認（Confirm Add Device）]** ポップアップ ウィンドウで、**[いいえ（No）]** を選択して既存の証明書を使用し、TLS ポートを入力します。 **[はい（Yes）]** を選択すると、既存の証明書が削除され、新しい証明書が作成されます。

  - **[パージして削除（Purge and Delete）]**：このオプションを使用して、デバイスを削除し、NDB コントローラからデバイス構成も削除します。

チェックボックスを選択せずに削除アクションを選ぶと、エラーが表示されます。デバイスを選択するように求められます。

（注） デバイスに到達できず、NDB コントローラから切断された場合、NDB コントローラは 30 秒ごとにデバイスを見つけて接続しようとします。

グローバル拒否 ACL は、デバイス上の構成されていないすべてのインターフェイス（エッジ SPAN/TAP、パケット トランケーション、リモート送信元、およびローカルおよびリモート モニター）に自動的に追加されます。デフォルトでは、グローバル拒否 ACL 機能はすべてのデバイスで有効になっています。**config.ini** ファイルで configure.global.acls パラメータを false に設定することにより、グローバル拒否 ACL 機能を無効にすることができます。構成ファイルに変更を加えた後は、必ず NDB を再起動してください。

## デバイスの追加

NDB コントローラに 1 つのデバイスを追加するには、この手順を使用します。

Nexus Dashboard Data Broker リリース 3.10.5 以降では、GUI を使用して TLS 証明書を構成する必要があります。TLS 構成に必要な手順は、**[デバイスの追加（Add Device）]** 画面の一部です。TLS の CLI 方式はサポートされなくなりました。

### 始める前に

NDB コントローラにデバイスを追加する前に、次の手順を実行します。

- **feature nxapi** コマンドを使用して、デバイスで NXAPI を有効にします。
- デバイスを初めて NDB コントローラに追加する場合は、[デバイスの前提条件（Device Prerequisites）] オプションを使用します。

（注） サポートされている Cisco Nexus シリーズ スイッチとサポートされている NX-OS バージョンを確認するには、該当するリリースの *Cisco Nexus Data Broker* リリース ノートを確認してください。

### 手順

**ステップ 1** **[デバイス（Devices）]** > **[NDB デバイス（NDB Devices）]** に移動します。

**ステップ 2** **[アクション（Actions）]** ドロップダウン メニューから **[デバイスの追加（Add Device）]** を選択します。

**ステップ 3** **[デバイスの追加（Add Device）]** ダイアログ ボックスで、次の詳細を入力します。

表 *8:* デバイスの追加

| フィールド | 説明 |
|---|---|
| **[全般（General）]** | |
| **[IP アドレス/ホスト名（IP Address/ Hostname）]** | デバイス名または IP アドレスを入力します。複数のデバイスを追加するには、ホスト名または IP アドレスをコンマで区切って追加します。<br>TLS を有効にするには、ホスト名（ドメイン名を含む完全修飾ホスト名）を入力する必要があります。 |

| フィールド | 説明 |
|---|---|
| ユーザー名/ プロファイル（**Username/ Profile**） | **ユーザー名**または**プロファイル**のいずれかを選択します。<br>**[ユーザー名（Username）]** をクリックすると、次のフィールドが表示されます。<br>• **[ユーザー名（Username）]** : デバイスにログインするためのスイッチのユーザー名を入力します。<br>• **[パスワード（Password）]** : パスワードを入力します。<br>**[プロファイル（Profile）]**をクリックすると、次のフィールドが表示されます。<br>• **[プロファイル（Profile）]** : **[プロファイルの選択（Select Profile）]** ドロップダウン リストから、プロファイルを選択します。<br>（注）<br>複数のスイッチをプロファイルに関連付けることができます。プロファイル設定は、すべてのメンバースイッチに適用されます。 |
| 接続タイプ（**Connection Type**） | ドロップダウンリストから、接続タイプを選択します。現在、NX-API のみがサポートされています。 |
| **[ポート（Port）]** | デバイスの通信ポートを入力します。HTTP 経由の NX-API にはポート 80 を使用し、HTTPS には 443 を使用します。<br>TLS の構成の場合、ポートを TLS ポートとして構成するためのポート番号を指定します。 |

| フィールド | 説明 |
|---|---|
| デバイスの前提条件 | 灰色のボタンをクリックして、デバイスの前提条件を有効にします。バーが青色に変わり、ボタンが右に移動します。次のチェック ボックスが表示されます。<br>• インターフェイス コマンド：デフォルトでは、このチェックボックスはオンになっています。デバイスの前提条件により、一連のデフォルト インターフェイス コマンドが自動的に実行されます。<br>• リブート：このボタンをオンにして、NDB に追加する前にデバイスをリブートします。<br>• TCAM：このチェックボックスをオンにして、TCAM 値を設定します。**[デフォルト（Default）]** または **[スケール（Scale）]** を選択します。それぞれ 1024 または 2048 のメモリが割り当てられます。 |
| トランスポート層セキュリティ（TLS） | TLS を有効にして、TLS パラメータを設定します。情報アイコン（*i*）にカーソルを合わせると、ポップアップ ウィンドウが表示されます。 **[TLS パスワードの更新（Update TLS Passwords）]**へのリンクをクリックします。<br>（注）<br>TLS を使用して初めてデバイスを追加する場合は、この段階で TLS パスワードを入力する必要があります。以前にパスワードをすでに追加している場合は、ここでパスワードを再度追加する必要はありません。パスワードは、**[TLSパスワードの更新（Update TLS Passwords）]** 画面で追加できます。ヘッダーの歯車アイコンをクリックします。<br>表示されるフィールドについては、以降の手順Transport Layer Security の設定 （47 ページ） で説明します。 |

**ステップ 4** **[デバイスの追加（Add Device）]** をクリックします。

（注）
グローバル ACL は、デバイス上のすべてのインターフェイスに自動的に追加されます。デフォルトでは、デバイスに対してグローバル ACL が有効になっています。グローバル ACL を管理するには、config.ini ファイルに configure.global.acls パラメータを追加する必要があります。デバイスのグローバル ACL を無効にするには、configure.global.acls パラメータを *false* に設定し、デバイスを再起動します。

デバイスの追加プロセス中に、機能タップ集約が有効になります。

## Transport Layer Security の設定

この手順は、「デバイス」の章で説明されているデバイスの追加手順の一部です。

NDDB リリース 3.10.5 以降、Transport Layer Security（TLS）構成は [デバイスの追加（Add Device）] 画面の一部として実行できます。ここで説明する手順は、TLS を構成するためのものです。

### 始める前に

スイッチにドメイン名が構成されていることを確かめるため、**ip domain-name** コマンドを使用して、NDB スイッチごとに、完全修飾ドメイン名（FQDN）が機能することを確認します。次に例を示します。

```
conf t
ip domain-name cisco.com
hostname N9k-117
end
```

スイッチの FQDN は N9K-117.cisco.com に設定されています。

これらの TLS パスワードを構成します。

- トラストストアのパスワード
- キーストアのパスワード
- PEM パスフレーズ（自己署名 TLS の場合はオプション）
- チャレンジパスワード（自己署名TLSの場合はオプション）

### 手順

**ステップ 1** **[NDB デバイス（NDB Devices）] > [アクション（Actions）] > [デバイスの追加（Add Device）]** に移動します。

**ステップ 2** デバイスの詳細を入力したら、**[トランスポート レイヤ セキュリティ（Transport Layer Security）]** オプションを有効にします。

（注）
「始める前に」セクションに記載されている前提条件の TLS パスワードが構成されていない場合、TLS オプションを有効にすることはできません。ただし、この段階でこれらのパスワードを入力することもできます。 **[TLS パスワードの更新（Update TLS Passwords）]** ポップアップ画面でパスワードを入力し、 **[保存（Save）]** をクリックします。デバイスを初めてオンボーディングするときは、4 つのパスワードをすべてデフォルト値からカスタム値に変更することをお勧めします。

**ステップ 3** **[自己署名（Self-signed）]** または **[サードパーティ（Third-party）]** オプションのいずれかを選択します。

**ステップ 4** 次の詳細を入力します。これらは証明書の生成に使用されます。

a) **[国（Country）]** 名を入力します。
b) **[都道府県（State）]** 名を入力します。

c) **[市区町村名（Locality）]** を入力します。
d) **[組織（Organization）]** 名を入力します。
e) **[部署（Organization Unit）]** の名前を入力します。
f) 有効な **[電子メール ID（Email ID）]** を入力します。
g) **[有効期間（Validity Period）]** を日数単位で入力します。このフィールドは、**[自己署名（Self-signed）]** オプションにのみ適用されます。
h) 秘密キーを暗号化するには、**[セキュア証明書（Secure Certificate）]** を有効にします。このフィールドは、**[サードパーティ（Third-party）]** オプションにのみ適用されます。

**ステップ 5** **[CSR の生成とデバイスの追加（Generate CSR and Add Device）]**（サードパーティ証明書の場合）または **[デバイスの追加（Add Device）]**（自己署名証明書の場合）をクリックします。

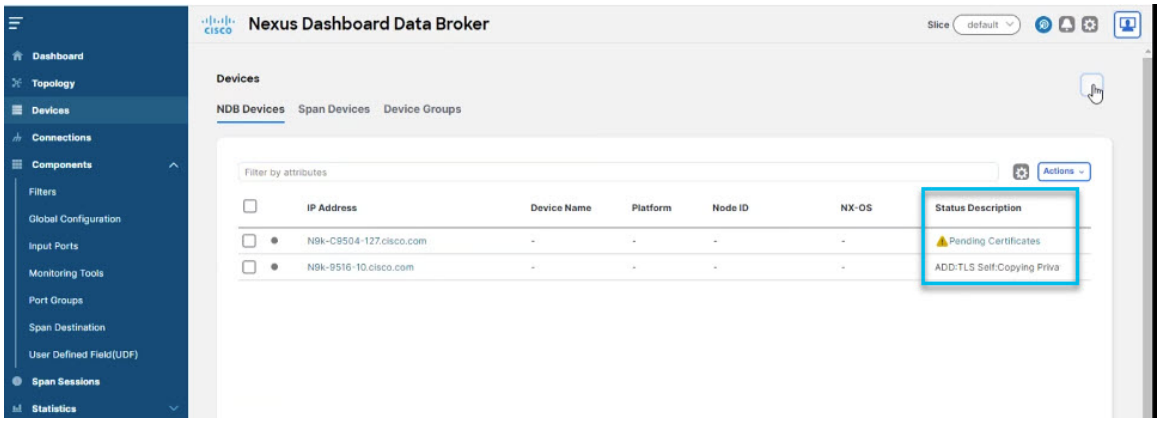
（自己署名証明書）使用可能なすべての NDB デバイスを示す [NDB デバイス（NDB devices）] 画面が表示されます。

（サードパーティ証明書）の後続の「次の作業」の項を参照してください。

## 次のタスク

サードパーティの TLS の場合は、**[保留中の証明書（Pending Certificates）]** をアップロードする必要があります。

**図 *9:* 保留中の証明書の追加**




[ステータスの説明（Status Description）] 列に表示されている **[保留中の証明書（Pending Certificates）]** リンクをクリックします。

選択する CA の階層に応じて、各 CSR に対して最大 3 通の証明書（証明書チェーン）を取得できます。このことは、NDB スイッチごとに、CA から 3 通の証明書（root、中間、ドメイン）を取得することを意味します。各タイプの証明書を識別するには、CA に確認する必要があります。証明書の命名規則は、認定機関ごとに異なる場合があります。たとえば、test-root-ca-2048.cer（ルート）、test-ssl-ca.cer（中間）、N9K-117.cisco.com.cer（ドメイン）のようになります。

要求をサードパーティの認証局に送信する場合は、関連する手順に従い、3つの（証明書）ファイルを取得します。

（注） 証明書でサポートされている形式は .PEM です。

## デバイスの編集

この手順を使用して、デバイスを編集します。

### 始める前に

1 つ以上のデバイスを作成します。

### 手順

**ステップ 1** **[デバイス]** > **[NDB デバイス]** に移動します。

**ステップ 2** 表示された表で、**IP アドレス**をクリックします。

新しいペインが右側に表示されます。

**ステップ 3** **[アクション（Actions）]** をクリックして、**[デバイスの編集（Edit Device）]** を選択します。

**ステップ 4** **[デバイスの編集（Edit Device）]** ダイアログ ボックスに、現在のデバイス情報が表示されます。これらのフィールドを必要に応じて変更します。

**表 *9*: デバイスの編集**

| フィールド | 説明 |
|---|---|
| **[全般（General）]** | |
| **[IP アドレス/ホスト名（IP Address/ Hostname）]** | デバイスの現在の IP アドレス。このフィールドは編集できません。 |

| フィールド | 説明 |
|---|---|
| ユーザー名/ プロファイル（**Username/ Profile**） | **[ユーザー名（Username）]**または**[プロファイル（Profile）]**のいずれかを選択します。<br>**[ユーザー名（Username）]** をクリックすると、次のフィールドが表示されます。<br>• **[ユーザー名（Username）]** : デバイスへのログインに使用されたユーザー名が表示されます。このフィールドは編集できます。<br>• **[パスワード（Password）]** : 入力したユーザー名のパスワードを入力します。<br>**[プロファイル（Profile）]**をクリックすると、次のフィールドが表示されます。<br>• **[プロファイル（Profile）]** : **[プロファイルの選択（Select Profile）]** ドロップダウン リストから、プロファイルを選択します。<br>（注）<br>複数のスイッチをプロファイルに関連付けることができます。プロファイル設定は、すべてのメンバー スイッチに適用されます。 |
| 接続タイプ（**Connection Type**） | ドロップダウンリストから、接続タイプを選択します。現在、NXAPI のみがサポートされています。 |
| **[ポート（Port）]** | デバイスの通信ポートを入力します。HTTP 経由の NX-API にはポート 80 を使用し、HTTPS には 443 を使用します。 |

| フィールド | 説明 |
|---|---|
| デバイスの前提条件 | 灰色のボタンをクリックして、デバイスの前提条件を有効にします。バーが青色に変わり、ボタンが右に移動します。次のチェック ボックスが表示されます。<br>• **インターフェイス コマンド**—デフォルトで、このチェックボックスはオンになっています。デバイスの前提条件により、一連のデフォルトインターフェイス コマンドが自動的に実行されます。<br>• **[リブート（Reboot）]**：このボタンをオンにして、NDB に追加する前にデバイスをリブートします。<br>• **[TCAM]**—このチェックボックスをオンにして、TCAM 値を設定します。**[デフォルト（Default）]** または **[スケール（Scale）]** を選択します。それぞれ 1024 または 2048 のメモリが割り当てられます。<br>デバイスの前提条件に関する詳細は、デバイスの前提条件 （52 ページ） を参照してください。 |

**ステップ 5** **[保存（Save）]** をクリックします。

## デバイス プロファイルの更新

この手順に従って、プロファイルをデバイスに割り当て（関連付け）、デバイスのプロファイルを更新します。

### 始める前に

1 つ以上のプロファイルを作成します。

### 手順

**ステップ 1** **[デバイス（Devices）]** > **[NDB デバイス（NDB Devices）]** に移動します。

**ステップ 2** **[アクション（Actions）]** ドロップダウンメニューの **[プロファイルの割り当て/更新（Assign/Update Profile）]** を選択します。

**ステップ 3** **[プロファイルの割り当て/更新（Assign/Update Profile）]** ダイアログ ボックスで、次の詳細を入力します。

表 *10 : [*プロファイルの割り当て/更新（***Assign/Update Profile***）*]*

| フィールド | 説明 |
|---|---|
| 全般 | |

| フィールド | 説明 |
|---|---|
| プロファル（**Profile**） | ドロップダウンメニューから**[プロファル（Profile）]**を選択します。 |
| 接続タイプ（**Connection Type**） | デフォルトの NXAPI 接続タイプが表示されます。 |

**ステップ 4** **[プロファイルの割り当て/更新（Assign/Update Profile）]** をクリックします。

## ポート チャネルの追加

この手順を使用すると、ポート チャネルを追加することができます。

ポート チャネルの詳細については、ポート チャネルとグループを参照してください。

### 手順

**ステップ 1** **[デバイス（Devices）]** > **[NDB デバイス（NDB Devices）]** に移動します。

**ステップ 2** **[IP アドレス（IP Address）]**をクリックし、詳細アイコンを選択します。

**ステップ 3** **[ポート チャネルの追加（Add Port Channel）]** ダイアログボックスで、次の詳細を入力します。

表 *11* : ポートチャネルの追加

| フィールド | 説明 |
|---|---|
| **[全般（General）]** | |
| **ID** | ポートチャネルの名前を入力します。 |
| 説明 | ポート チャネルの説明を入力します。 |
| **[ポート（Port）]** | **[ポートの選択（Select Port）]** をクリックします。必要なチェック ボックスをオンにして、**[選択（Select）]** をクリックします。 |

**ステップ 4** **[ポート チャネルの追加（Add Port Channel）]** をクリックします。

## デバイスの前提条件

Nexus Dashboard Data Broker は、新しく追加されたデバイスに基本構成をプッシュします。前提条件の構成を正常にプッシュするには、Nexus Dashboard Data Broker の新しいデバイスで NX-API が有効になっていることを確認します。NX-API デバイスを Nexus Dashboard Data Broker に対応させるために手動で設定する必要はありません。

デバイスの前提条件は、デバイスを追加または編集するとき、またはデバイスにプロファイルを追加または変更するときに構成できます。デバイスの追加 （43 ページ） または デバイスの編集 （49 ページ） を参照してください。

次の構成は、Nexus Dashboard Data Broker によって新しいスイッチにプッシュされます。

- STP の前提条件を満たさずに NDB デバイスをオンボードするとき（独立したリンクまたはポート チャネルが NDB デバイスに接続されている場合）、 **switchport mode trunk** コマンドと **spanning-tree bpdufilter enable** コマンドを手動で構成する必要があります。
- デバイス プラットフォームに基づく TCAM 構成
- スパニング ツリーで MST モードが有効になっている
- 基本 VLAN 構成
- 機能タップ集約が有効になっている。
- LLDP 機能が有効になっている（集中型モードの場合のみ）。

Nexus Dashboard Data Broker によってすべての構成が正常にプッシュされた後、デバイスが再起動されます。TCAM 設定のため、デバイスの再起動が必要です。NX-OS からのリブートがサポートされているのは 9.2(3) 以降です。

# ポート チャネルとポート グループ

### ポート チャネル

ポートチャネルは複数の物理インターフェイスの集合体で、論理インターフェイスを作成します。1 つのポートチャネルに最大 8 つの個別アクティブ リンクをバンドルして、帯域幅と冗長性を向上させることができます。ポート チャネル内のメンバー ポートに障害が発生すると、障害が発生したリンクで伝送されていたトラフィックはポートチャネル内のその他のメンバー ポートに切り替わります。これらの集約された各物理インターフェイス間でトラフィックのロード バランシングも行います。ポート チャネルの物理インターフェイスが少なくとも 1 つ動作していれば、そのポート チャネルは動作しています。

ポートチャネルは、互換性のあるインターフェイスをバンドルすることによって作成します。スタティック ポート チャネルのほか、Link Aggregation Control Protocol（LACP）を実行するポート チャネルを設定して稼働させることができます。変更した設定をポート チャネルに適用すると、そのポートチャネルのメンバインターフェイスにもそれぞれ変更が適用されます。たとえば、スパニングツリープロトコル（STP）パラメータをポートチャネルに設定すると、Cisco NX-OS はこれらのパラメータをポートチャネルのそれぞれのインターフェイスに適用します。

関連するプロトコルを使用せず、スタティック ポート チャネルを使用すれば、設定を簡略化できます。IEEE 802.3ad に規定されている Link Aggregation Control Protocol（LACP）を使用すると、ポートチャネルをより効率的に使用することができます。LACP を使用すると、リンクによってプロトコル パケットが渡されます。

### ポート グループ

デバイス（または複数の異なるデバイス）のポートをグループ化して、ポート グループを形成できます。ポート グループは、さまざまなスイッチのエッジ スパン ポートとエッジ タップ ポートの組み合わせにすることができます。ポート グループを使用している場合、ポート グループの個々のポートを選択することはできません。

## 対称型および非対称型ロード バランシング

Cisco Nexus Data Broker GUI および REST API インターフェイスから、NX-API 構成モードを使用して、対称型ロード バランシングを構成し、Cisco Nexus 9000 シリーズ スイッチで MPLS タグ ストリッピングを有効にすることができます。

次の表に、対称および非対称のロード バランシング オプションを示します。

| 設定タイプ | ハッシュ構成 | プラットフォーム | オプション（Options） |
|---|---|---|---|
| Symmetric | SOURCE_DESTINATION | Nexus 9000 シリーズ（すべて）、N3K-C3164xx、N3K-C32xx | IP、IP-GRE、IP-L4PORT、IP-L4PORT-VLAN、IP-VLAN、L4PORT、MAC |
| | | REST API | IP、IP-GRE、ポート、MAC、IP のみ、ポートのみ |
| 非対称型 | 送信元<br>送信先 | Nexus 9000 シリーズ（すべて）、N3K-C3164xx、N3K-C32xx | IP、IP-GRE、IP-L4PORT、IP-L4PORT-VLAN、IP-VLAN、L4PORT、MAC |
| | | REST API | IP、IP-GRE、ポート、MAC |

# SPAN デバイス

Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）は、効率的で高性能なトラフィック モニタリング システムです。ネットワーク トラフィックを複製し、パケットをモニタリングのためにアナライザに回送します。SPAN は、接続の問題のトラブルシューティング、ネットワーク使用率の計算、およびパフォーマンス モニタリングに使用されます。Nexus Dashboard Data Broker を使用して、デバイスを SPAN に追加、編集、削除、および再検出できます。

Cisco Nexus Dashboard Data Broker リリース 3.10.1 以降、Cisco Catalyst 9300 シリーズ スイッチは実稼働スイッチとしてサポートされています。Catalyst switch の詳細については、*Cisco.com* の関連するシスコのドキュメントを参照してください。

（注） Catalyst シリーズ スイッチ 9300-24UB は、リリース 3.10.1 に対応しています。サポートされている IOS XE バージョンは、16.09.05 以降です。

Catalyst スイッチは、Nexus Dashboard Data Broker GUI を使用して直接オンボードおよび管理できます。Catalyst スイッチは、Cisco DNA Center（Cisco DNAC）を使用してオンボードすることもできます。「Cisco Nexus Dashboard Data Broker と Cisco DNA Center の統合 （60 ページ）」を参照してください。

**[SPAN デバイス（Span Devices）]** タブには、SPAN に接続されているデバイスの詳細が表示されます。

詳細を表示するには、**[コントローラ（Controllers）]** または **[実稼働スイッチ（Production Switches）]** を選択します。

- **[コントローラ（Controllers）]**：Cisco APIC または Cisco DNAC を介して Nexus Dashboard Data Broker コントローラに接続されたネットワークまたはデバイス。
- **[実稼働スイッチ（Production Switches）]**：Nexus Dashboard Data Broker コントローラに接続されたスタンドアロンの Nexus または Catalyst スイッチ。

表 *12*：コントローラ

| 列 | 説明 |
|---|---|
| **[Active IP（アクティブ IP）]** | コントローラのアクティブな IP アドレス。IP アドレスをクリックすると、右側に新しいペインが表示されます。ここから実行できる追加アクションは次のとおりです。<br>• スパン デバイスの編集 （58 ページ）<br><br>Nexus Dashboard Data Broker コントローラと通信する Cisco APIC/Cisco DNAC コントローラの現在の IP アドレス。<br><br>IP アドレスをクリックすると、右側に新しいペインが表示され、詳細が表示されます。<br><br>Cisco DNAC コントローラの場合、Nexus Dashboard Data Broker が Cisco DNAC にインストールするテンプレート名が表示されます。テンプレートは次のとおりです。<br>• NDB モニター セッションの削除<br>• NDB モニター セッションの作成 |
| **[ユーザー名（Username）]** | コントローラに現在ログインしているユーザー名。 |

| 列 | 説明 |
|---|---|
| 名前（Name） | コントローラの名前。 |
| [プライマリ IP アドレス（Primary IP Address）] | コントローラのプライマリ IP アドレス。 |
| [セカンダリ IP アドレス（Secondary IP Address）] | （APIC のみ）コントローラのセカンダリ IP アドレス。 |
| [ターシャリ IP アドレス（Tertiary IP Address）] | （APIC のみ）コントローラの第 3 の IP アドレス。 |

表 *13 : [*実稼働スイッチ（*Production Switches*）*]*

| 列 | 説明 |
|---|---|
| [アクティブ IP（Active IP）] | デバイスのアクティブな IP アドレス。<br>IP アドレスをクリックすると、右側に新しいペインが表示されます。ここから実行できる追加アクションは次のとおりです。<br>• スパン デバイスの編集 （58 ページ） |
| [ユーザー名（Username）] | デバイスに現在ログインしているユーザー名。 |
| プラットフォーム | デバイスのプラットフォーム。 |

**[SPAN デバイス（Span Devices）]** タブから、次のアクションを実行できます。

- **[SPAN デバイスの追加（Add Span Device）]**：これを使用して、新しい SPAN デバイスを追加します。詳細については、スパン デバイスの追加 （57 ページ） を参照してください。
- **[SPAN デバイスの再検出（Rediscover Span Device）]**：行の先頭にあるチェックボックスをオンにして、必要なデバイスを選択します。**[アクション（Actions）]**>**[SPAN デバイスの再検出（Reciscover Span Device）]** をクリックします。ポップアップ ウィンドウが表示されます。**[再検出（Rediscover）]** をクリックして、選択したデバイスを再検出します。

  **[SPAN デバイスの再検出（Rediscover Span Device）]** オプションを使用して、Nexus Dashboard Data Broker コントローラと SPAN デバイス間の接続を再確立します。

  チェック ボックスを選択せずに再検出アクションを選択すると、エラーが表示されます。デバイスを選択するように求められます。
- **[SPAN デバイスの削除（Delete Span Device）]**：行の先頭にあるチェックボックスをオンにして、必要なデバイスを選択します。**[アクション（Actions）]**>**[SPAN デバイスの削除（Delete Span Device）]** をクリックします。

チェックボックスを選択せずに削除アクションを選ぶと、エラーが表示されます。デバイスを選択するように求められます。

## スパン デバイスの追加

SPAN に 1 つのデバイスを追加するには、この手順を使用します。

### 手順

**ステップ 1** **[デバイス（Devices）]** > **[スパン デバイス（Span Devices）]** に移動します。

**ステップ 2** **[アクション（Actions）]** ドロップダウン リストから、**[スパン デバイスの追加（Add Span Device）]** を選択します。

**ステップ 3** **[スパン デバイスの追加（Add Span Device）]** ダイアログ ボックスで、次の詳細を入力します。

表 *14 : [*スパン デバイスの追加（***Add Span Device***）*]*

| フィールド | 説明 |
|---|---|
| **[全般（General）]** | **[コントローラ（Controller）]** または **[実稼働スイッチ（Production Switch）]** を選択します。コントローラとしては、APIC または DNAC が可能です。実稼働スイッチ（PS）としては、Nexus または Catalyst スイッチが可能です。<br>それぞれで使用できるオプションについては、以下の行で説明します。 |
| **[コントローラ（Controller）]** に表示されるフィールド： | |
| **コントローラ タイプ（Controller Type）** | ドロップダウン リストからコントローラ タイプを選択します次のオプションがあります。<br>• Cisco APIC<br>• Cisco DNAC |
| **[IP アドレス/ホスト名（IP Address/Hostname）]** | コントローラの IP アドレスを入力します。 |
| **[IP アドレス（セカンダリ）（IP Address (Secondary)）]** | （オプション、APIC のみ）コントローラのセカンダリ IP アドレスを入力します。 |
| **[IP アドレス（ターシャリ）（IP Address (Tertiary)）]** | （オプション、APIC の場合のみ）コントローラの第 3 IP アドレスを入力します。 |
| **Username** | ユーザー名を入力します。 |
| **パスワード** | 認証のために必要なパスワードを入力します。 |

| フィールド | 説明 |
|---|---|
| **Cisco DNAC 名** | （Cisco DNAC のみ）Cisco DNAC 名を入力します。この名前は、Nexus Dashboard Data Broker コントローラによる識別に使用されます。 |
| **[実稼働スイッチ（Production Switch）]**に表示されるフィールド： | |
| **[アドレス（Address）]** | Nexus または Catalyst スイッチの IP アドレス。 |
| プラットフォームタイプ | ドロップダウンリストから選択します。次のオプションがあります。<br>• Nexus<br>• Catalyst |
| **[ポート（Port）]** | デバイス通信ポート。<br>Nexus スイッチのポート番号を入力します。<br>**[プラットフォーム タイプ（Platform Type）]**として Catalyst を選択した場合、デフォルトのポート値 22 が表示されます。Catalyst スイッチへの通信は SSH 経由です。 |
| **[ユーザー名（Username）]** | デバイスのユーザー名を入力します。 |
| パスワード（**Password**） | ユーザー名を認証するために必要なパスワードを入力します。 |
| パスワードを有効にする（**Enable Password**） | （Catalyst スイッチのみ）必要なパスワードを入力します。<br>（注）<br>スイッチがイネーブル モードでない場合は、パスワードを入力します。 |

**ステップ 4** **[スパン デバイスの追加（Add Span Device）]** をクリックします。

Cisco DNAC コントローラがスパン デバイスとして正常に追加されると、Nexus Dashboard Data Broker は必要なプロジェクトとテンプレートを Cisco DNAC コントローラにインストールします。作成されたプロジェクトとテンプレートは、Cisco DNAC の *[Template Editor*（テンプレート エディタ）*]* で確認できます。

## スパン デバイスの編集

この手順に従って、スパン デバイスのパラメータを編集します。

### 始める前に

1 つ以上のスパン デバイスを作成します。

### 手順

**ステップ 1** **[デバイス]** > **[スパン デバイス]** に移動します。

**ステップ 2** 表示された表で、**IP アドレス**をクリックします。

新しいペインが右側に表示されます。

**ステップ 3** **[アクション（Actions）]** をクリックして、**[スパン デバイスの編集（Edit Span Devices）]** を選択します。

**ステップ 4** **[スパン デバイスの編集（Edit Span Device）]** ダイアログボックスに、現在のスパン デバイス情報が表示されます。これらのフィールドを必要に応じて変更します。

**表 *15*：スパン デバイスの編集**

| フィールド | 説明 |
|---|---|
| **[全般（General）]** | このフィールドは、編集できません。以前に**コントローラ**または**実稼働スイッチ**を選択した場合、その選択を変更することはできません。ただし、それらのパラメータは編集可能であり、以下の行で説明されています。 |
| **[コントローラ（Controller）]** に表示されるフィールド： | |
| **コントローラ タイプ（Controller Type）** | 以前に選択したコントローラ タイプ。このフィールドは、編集できません。 |
| **IP アドレス/ホスト名（IP Address/Hostname）** | コントローラのプライマリ IP アドレス。このフィールドは、編集できません。 |
| **IP アドレス（セカンダリ）（IP Address (Secondary)）** | （APIC の場合のみ）APIC デバイスのセカンダリ IP アドレスを入力します。 |
| **IP アドレス（ターシャリ）（IP Address (Tertiary)）** | （APIC の場合のみ）APIC デバイスの 3 次 IP アドレスを入力します。 |
| **Username** | コントローラのユーザー名。 |
| **パスワード** | 認証のために必要なパスワードを入力します。 |
| **Cisco DNAC 名** | （Cisco DNAC のみ）Cisco DNAC の名前。この名前は、Nexus Dashboard Data Broker コントローラによる識別に使用されます。 |
| **[実稼働スイッチ（Production Switch）]**に表示されるフィールド： | |
| **[アドレス（Address）]** | Nexus または Catalyst スイッチの IP アドレス。 |

| フィールド | 説明 |
|---|---|
| プラットフォームタイプ | 以前に選択したプラットフォーム タイプ。このフィールドは、編集できません。 |
| **[ポート（Port）]** | デバイス通信ポート。<br>ポート番号は、Nexus スイッチの場合は 80、Catalyst スイッチの場合は 22 です。 |
| ユーザー名 | デバイスのユーザー名。 |
| パスワード（**Password**） | ユーザー名を認証するために必要なパスワードを入力します。 |
| パスワードを有効にする（**Enable Password**） | （Catalyst switch のみ）スイッチを有効にするために必要なパスワードを入力します。 |

**ステップ 5** **[保存（Save）]** をクリックします。

## Cisco Nexus Dashboard Data Broker と Cisco DNA Center の統合

Cisco Digital Network Architecture Center（Cisco DNAC）は、ネットワークを管理できる強力なネットワーク コントローラおよび管理ダッシュボードです。

Cisco DNAC の詳細については、関連する *Cisco DNAC* のドキュメントを参照してください。

Cisco DNAC コントローラは、Nexus Dashboard Data Broker と統合できます。Catalyst スイッチの SPAN セッション構成は、Nexus Dashboard Data Broker UI から管理できます。Nexus Dashboard Data Broker は、オンボーディング中、Cisco DNAC 上に独立したプロジェクトとテンプレートを作成します。Nexus Dashboard Data Broker は、Catalyst スイッチのポートの詳細を Cisco DNAC と共有します。テンプレートに基づいて、Cisco DNAC は Catalyst スイッチで SPAN セッションを作成します。

Cisco DNAC コントローラの Nexus Dashboard Data Broker テンプレートの例：

```
monitor session $sessionNumber source $sourceType $sources $direction
monitor session $sessionNumber destination interface $destinationInterfaces
```

Nexus Dashboard Data Broker コントローラと Cisco DNAC 間の通信には REST API が使用されます。

# タップ デバイス

Cisco Nexus Dashboard Data Broker は、Cisco Nexus 3550-F L1 シリーズ スイッチをタップ デバイスとしてサポートします。タップ デバイスは、ネットワーク データのコピーを作成するものの、データを変更しないデバイスです。タップデバイスからのトラフィックは、Cisco Nexus Dashboard Data Broker に到達してさらに処理を受けます。

表 *16* : タップ デバイス

| 列 | 説明 |
|---|---|
| **[IP アドレス（IP Address）]** | タップ デバイスの IP アドレス。 |
| **デバイス名** | デバイスの名前。 |
| **[プラットフォーム（Platform）]** | タップデバイスのプラットフォーム。 |
| **[ノード ID（Node ID）]** | Cisco Nexus Dashboard Data Broker コントローラによる識別に使用されるタップ デバイスの一意の ID。 |
| **[プロファイル名（Profile Name）]** | 関連付けられたプロファイル名。<br>タップ デバイスの作成時に **[プロファイル（Profile）]** オプションが選択されていない場合、ここに情報は表示されません。 |
| **Version** | タップデバイスのソフトウェア バージョン。 |
| **[ステータスの説明（Status Description）]** | Cisco Nexus Dashboard Data Broker コントローラとタップ デバイス間の接続のステータス。次のオプションを使用できます。<br>• 接続成功（Successfully connected）：接続成功。<br>• 認証失敗（Authentication failure）：タップ デバイスの認証情報が正しくありません。<br>• 接続タイムアウト（Connection timed-out）：一定時間内にタップ デバイスに到達できませんでした。<br>• ホストへのルートがありません（No route to host）：タップ デバイスの IP アドレスが間違っています。<br>• デバイスからの無効な応答（Invalid response from device）：不正なデバイス（Cisco Nexus 3550-L1 以外のデバイス）。 |

**[タップ デバイス（Tap Device）]** タブから、次のアクションを実行できます。

- **[タップ デバイスの追加（Add Tap Device）]**：これを使用して、新しいタップ デバイスを追加します。詳細については、タップ デバイスの追加 （62 ページ） を参照してください。

- **プロファイルの割り当て/更新（Assign/ Update Profile）**：このアクションを使用して、タップデバイスのプロファイルを追加または更新します。このタスクの詳細については、プロファイルの更新を参照してください。
- **タップ デバイスの再接続（Reconnect Tap Device(s)）**：行の先頭にあるチェックボックスをオンにして、必要なデバイスを選択します。**[アクション（Actions）] > [デバイスを再接続（Reconnect Tap Devices(s)）]** をクリックします。ポップアップが表示されます。**[再接続（Reconnect）]** をクリックして、選択したタップ デバイスを再接続します。このオプションは、TAP デバイスと Nexus Dashboard Data Broker コントローラの間で*[*接続タイムアウト（*Connection Timed Out*）*]* エラーが発生した場合に使用します。
- **タップ デバイスの削除（Delete Tap Device）**：行の先頭にあるチェックボックスをオンにして、必要なタップ デバイスを選択します。**[アクション（Actions）] > [デバイスの削除（Delete Device）]** をクリックします。次の 2 つのオプションから選択できます。
  - **削除（Delete）**：タップ デバイスを Nexus Dashboard Data Broker から切断します。
  - **パージと削除（Purge and Delete）**：タップ デバイスを Nexus Dashboard Data Broker controller コントローラから切断し、関連付けられた構成を Nexus Dashboard Data Broker controller コントローラから削除します。

## タップ デバイスの追加

この手順を使用して、Cisco Nexus 3550-F L1 をタップ デバイスとして追加します。サポート対象の最小ソフトウェア バージョンは、1.15.0 です。

### 始める前に

- **configure http enable** を使用して、タップ デバイスで HTTP を有効にします。
- タップ デバイスに既存の構成がないことを確認します。

### 手順

**ステップ 1** **[デバイス] > [タップ デバイス]** に移動します。

**ステップ 2** **[アクション（Actions）]** ドロップダウン リストから、**[タップ デバイスの追加（Add Tap Devices）]** を選択します。

**ステップ 3** **[タップ デバイスの追加（Add Tap Device）]** ダイアログ ボックスで、次の詳細を入力します。

表 *17:* タップデバイスの追加

| フィールド | 説明 |
|---|---|
| **[IP アドレス/ホスト名（IP Address/Hostname）]** | デバイスの IP アドレスを入力します。 |

| フィールド | 説明 |
|---|---|
| デバイスのユーザー名を使用するか、関連付けられたプロファイルを使用して、タップ デバイスを追加することを選択できます。**[ユーザー名（Username）]** または **[プロファイル（Profile）]** を選択し、関連するフィールドに入力します。 | |
| **Username** | |
| **Username** | デバイスにログインするためのユーザー名を入力します。 |
| パスワード | ユーザ名のパスワードを入力します。 |
| **プロファイル（Profile）** | |
| プロファイル | ドロップダウンリストからプロファイルを選択します。 |
| **接続タイプ（Connection Type）** | このフィールドは読み取り専用です。デフォルト値（REST）が表示されます。 |

**ステップ 4** **[タップ デバイスの追加（Add Tap Device）]** をクリックします。

# デバイスグループ

**[デバイス グループ（Device Groups）]** タブには、デバイス グループの詳細が表示されます。表には次の詳細が表示されます。

**表 *18*：デバイスグループ**

| 列名 | 説明 |
|---|---|
| グループ | デバイスグループ名。<br>このフィールドはハイパーリンクです。グループ名をクリックすると、右側に新しいペインが表示され、グループに含まれるデバイスのリストが表示されます。ここから実行できる追加のアクションは次のとおりです。<br>• デバイス グループの編集 |
| デバイス | デバイス グループ内のデバイスの数。 |

次のアクションは、**[デバイス グループ（Device Groups）]** タブから実行できます。

- **[新しいデバイス グループ（Add Device Group）]**：新規デバイス グループを追加します。デバイス グループの追加を参照してください。

- **[デバイス グループの削除（Delete Device Group）]**：行の先頭にあるチェックボックスをオンにして、必要なデバイス グループを選択します。**[アクション（Actions）]** > **[デバイス グループの削除（Delete Device Group(s)）]** をクリックします。選択したデバイス グループが削除されます。チェックボックスを選択せずに削除アクションを選ぶと、エラーが表示されます。デバイス グループを選択するように求められます。

## デバイス グループの追加

新しいデバイス グループを追加するには、この手順を使用します。

### 手順

**ステップ 1** **[デバイス]** > **[デバイス グループ]** に移動します。

**ステップ 2** **[アクション（Actions）]** ドロップダウン メニューから **[デバイス グループの追加（Add Device Group）]** を選択します。

**ステップ 3** **[デバイス グループの追加（Add Device Group）]** ダイアログ ボックスから、次の詳細を入力します。

表 *19*：デバイスグループの追加

| フィールド | 説明 |
|---|---|
| **[全般（General）]** | |
| **Device Group Name** | デバイス グループの名前を入力します。 |
| デバイス | **[デバイスの選択（Select Devices）]** をクリックします。<br>**[デバイスの選択（Select Devices）]** ダイアログ ボックスが開きます。グループに追加するデバイスに対応するチェックボックスをオンにします。[選択（Select）] をクリックします。<br>（注）<br>デバイスがすでに別のグループに属しているかどうかを確認します。[はい（Yes）の場合]、デバイスは前のグループから削除され、新しいグループに追加されます。 |

**ステップ 4** **[デバイス グループの追加（Add Device Group）]** をクリックします。

## デバイス グループの編集

この手順に従って、デバイス グループを編集します。

### 始める前に

1 つ以上のデバイス グループを追加します。

### 手順

**ステップ 1** **[デバイス（Devices）]** > **[デバイス グループ（Device Groups）]** に移動します。

**ステップ 2** **デバイス グループ**の名前をクリックします。

新しいペインが右側に表示されます。

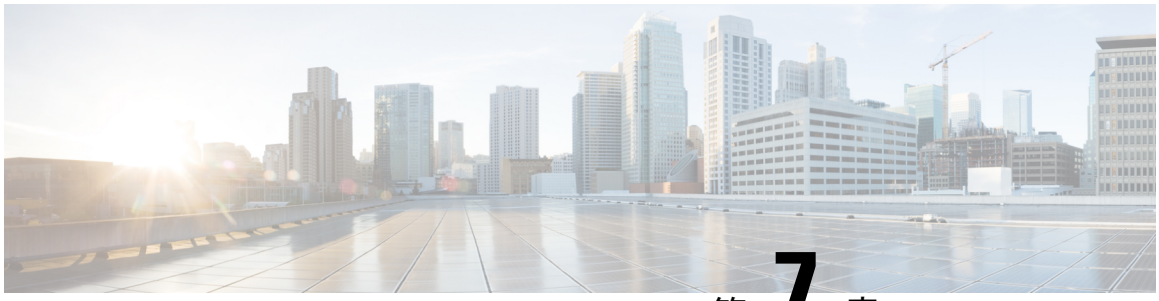
**ステップ 3** **[アクション（Action）]** > **[デバイス グループの編集（Edit Device Group）]** をクリックします。

表示されたウィンドウに、以下の詳細を入力します。

**表 *20* : デバイスグループを編集**

| フィールド | 説明 |
|---|---|
| **[全般（General）]** | |
| **Device Group Name** | デバイス グループ名。<br>このフィールドは編集できません。 |
| **デバイス** | 現在デバイス グループに属しているデバイスが表示されます。デバイスはグループから削除することができます。グループにデバイスを追加するには、**[デバイスの選択（Select Devices）]** をクリックします。<br>**[デバイスの選択（Select Devices）]** ダイアログ ボックスが開きます。グループに追加するデバイスに対応するチェックボックスをオンにします。[選択（Select）] をクリックします。<br>**（注）**<br>デバイスがすでに別のグループに属しているかどうかを確認します。[はい（Yes）の場合]、デバイスは前のグループから削除され、新しいグループに追加されます。 |

**ステップ 4** **[保存（Save）]** をクリックします。



第 7 章

# 接続

この章では、Cisco Nexus Dashboard Data Broker の接続について詳しく説明します。

リリース 3.10.1 から、Cisco Nexus Data Broker（NDB）の名前は、Cisco Nexus Dashboard Data Brokerに変更されました。ただし、GUI およびインストール フォルダ構造と対応させるため、一部の NDB のインスタンスがこのドキュメントには残されています。NDB/ Nexus Data Broker/ Nexus Dashboard Data Brokerという記述は、相互に交換可能なものとして用いられています。



## 接続

**[接続（Connections）]** タブには次のサブタブがあります。

- **[ユーザ接続（User Connections）]**：入力ポートとモニタリング ツール ポート間のトラフィックを管理するためのユーザ定義の接続。詳細については、ユーザ接続を参照してください。
- **[デフォルト接続（Default Connections）]**：デフォルトでは、ユーザ定義の接続が定義されるまで、入力ポートの着信トラフィックは拒否されます。詳細については、デフォルト接続を参照してください。

## ユーザー接続

**[ユーザー接続（User Connections）]** タブには、入力ポート（フィルタ付きまたはフィルタなし）とモニタリング ツール ポート間のすべてのユーザー定義接続の詳細が表示されます。

次の詳細を示す表が表示されます。

表 *21 :* ユーザー接続

| 列名 | 説明 |
|---|---|
| **接続名** | 接続の名前。<br>このフィールドはハイパーリンクです。接続の名前をクリックします。接続に関する詳細情報を含む新しいペインが右側に表示されます。接続のトポロジは、**[展開ビュー（Deployment View）]** または **[ネットワーク ビュー（Network View）]** で表示できます。<br>ここで実行できる追加のアクションは、次のとおりです。<br>• **[接続の編集（Edit Connection）]**：接続を編集するには、このアクションを選択します。詳細については、接続の編集を参照してください。<br>• **[接続のクローン（Clone Connection）]**：このアクションを選択して、接続を複製します。詳細については、接続の編集を参照してください。接続のクローン処理は、接続の編集に似ています。<br>**[詳細（Details）]** アイコン（  ）をクリックして、接続の詳細を取得します。新しいウィンドウは、選択された接続に対する次の詳細を表示します。<br>• 全般<br>• 展開ビュー<br>• ネットワーク ビュー<br>• [フロー統計情報（Flow Statistics）]<br>• ポート統計情報 |
| **[タイプ（Type）]** | 接続のタイプ。次のオプションがあります。<br>• [通常（Normal）]：ここでは、接続は入力ポートにフィルタを適用し、トラフィックをモニタリング ツールにリダイレクトします。<br>• [自動優先度（Auto Priority）]：ここでは、設定された自動優先度数に基づいて、接続がトラフィックをモニタリング ツールにリダイレクトします。詳細については、自動優先 （80 ページ）を参照してください。 |

| 列名 | 説明 |
|---|---|
| 適用フィルタ | 接続に適用される**許可**フィルタと**ドロップ**フィルタの数。選択に基づいて、マッチしたトラフィックがドロップまたは許可されます。<br>このフィールドはハイパーリンクです。表示された番号をクリックすると、右側に新しいペインが開きます。接続に適用されているすべてのフィルタのリストが表示されます。 |
| **[入力ポート/入力ポート グループ（Input Port/ Input Port Groups）]** | 接続の入力ポートと入力ポート グループの数。<br>このフィールドはハイパーリンクです。表示された番号をクリックすると、右側に新しいペインが開きます。送信元（そのトラフィックがNexus Dashboard Data Broker コントローラに到達する実稼働デバイス）および接続に適用可能なポートのリストが表示されます。 |
| **[モニタリング ツール/モニタリング ツール グループ（Monitoring Tools/ Monitoring Tools Group）]** | 接続のモニタリング ツールおよび/またはモニタリング ツール グループの数。<br>このフィールドはハイパーリンクです。表示された番号をクリックすると、右側に新しいペインが開きます。接続に適用可能なモニタリング ツールの一覧が表示されます。 |
| 説明 | 接続の説明。 |
| **[作成者（Created By）]** | 接続を作成したユーザー。 |
| **[最終更新者（Last Modified By）]** | 接続を最後に変更したユーザー。 |
| ステータスの説明 | 入力ポートとモニタリング ツール ポート間の接続の状態。ステータスの説明は、最新ステータスに基づく自動更新を行います。<br>また、  の *[更新（Refresh）]* をクリックして、最新ステータスを取得できます。 |

各行の先頭には、カラーコード（色分け）された丸と錠前が表示されます。接続のステータスに影響を与える要因としては、ソース ポートの運用状態と管理状態、モニタリング ツールの運用状態と管理状態、および接続に関連するセッションがあります。

- 緑色の丸は、最後の接続が成功したことを示します。
- 赤色の丸は、接続が失敗したことを示します。

- 黄色の丸は、接続が部分的に成功したことを示します。1つ以上の入力ポートとモニタリング ツールにエラーがあります。
- 灰色の丸は、接続が機能していないことを示します。すべての入力ポートとモニタリングツールの状態を確認してください。

錠前の記号は、接続パラメータの不正な変更を許可しないため、接続がロックされていることを示しています。接続を作成したユーザー（または管理者）または接続をロックしたユーザーのみが、必要な変更を行うことができます。接続は、追加中にロックできます。

**[ユーザー接続（User Connections）]** タブからは、次のアクションを実行できます。

- **[接続の追加（Add Connection）]**：接続を追加するには、このアクションを選択します。このタスクの詳細については、接続の追加を参照してください。
- **[接続の削除（Delete Connection）]**：行の先頭にあるチェックボックスをオンにして、必要な接続を選択します。**[アクション（Actions）]**ボタンをクリックし、**[接続の削除（Delete Connection）]** を選択します。選択した接続が削除されます。チェックボックスを選択せずに削除アクションを選ぶと、エラーが表示されます。接続を選択するように求められます。
- **インストールの切り替え（Toggle Install）**：行の先頭にあるチェックボックスをオンにして、必要な接続を選択します。**[アクション（Actions）]**ボタンをクリックし、**[インストールの切り替え（Toggle Install）]** を選択して接続をインストールします。**[インストールの切り替え（Toggle Install）]** は、NDB デバイスの接続のインストール/アンインストールを行いますが、接続設定が Nexus Dashboard Data Broker コントローラから削除されることはありません。

  チェック ボックスをオンにせずにインストールの切り替えアクションを選択すると、エラーが表示されます。接続を選択するように求められます。

**config.ini** ファイルで **configure.global.acls** パラメータを false に設定することにより、すべての ISL インターフェイスで拒否 ACL を無効にすることができます。構成ファイルに変更を加えた後は、Nexus Dashboard Data Broker を再起動してください。

CLI のアップグレード コマンドを使用し、**config.ini** ファイルで **configure.global.acls** パラメータを false に設定することにより、CLI アップグレードまたは構成アップロード中に、グローバル拒否 ACL または ISL 拒否 ACL を無効にすることができます。例：

```
configure.global.acls=false
```

# 接続の追加

接続を追加するために、この手順を使用します。接続は、デバイスの入力ポート（フィルタ付き）とデバイスのモニタリング ツール ポート間のリンクを確立します。

### 始める前に

次のタスクを完了します。

- 接続のフィルタを定義する
- モニタリング ツールを構成する（推奨）
- エッジ ポートを構成する（推奨）

接続を作成するには、次の制限事項と使用の注意事項に従ってください。

- QinQ VLAN を構成して、デバイス間で（複数のホップを使用して）自動優先順位を持つ新しい接続を追加します。
- 入力ポート/ポート グループごとに、自動優先順位の接続を 1 つだけ設定できます。

### 手順

**ステップ 1** **[接続（Connection）]** > **[ユーザー接続（User Connection）]** に移動します。

**ステップ 2** **[アクション（Actions）]** ドロップダウンリストで、**[接続の追加（Add Connection）]** を選択します。

**ステップ 3** **[接続の追加（Add Connection）]** ダイアログ ボックスで、次の詳細を入力します。

表 *22 :* 接続の追加

| フィールド | 説明 |
|---|---|
| **接続名** | 接続名を入力します。 |
| **説明** | 接続の説明を入力します。 |
| **優先度（Priority）** | 接続に設定する優先度を入力します。デフォルトの優先レベルは 100 です。範囲は 2 ～ 10000 です。数値が大きいほど優先度が高くなります。たとえば、200 は 100 よりも高い優先度を意味します。<br>ポートからの着信トラフィックは、優先度に基づいて照合されます。2 つの接続に同じ入力ポートと同じフィルタがある場合、トラフィックはより高い優先順位の接続を使用します。<br>（注）<br>デフォルトでは、編集は Cisco NDB 管理者ロールに対して有効になっています。 |
| **[接続のロック（Lock Connection）]** | 灰色のボタンをクリックして接続をロックします。灰色のボタンが青色に変わり、右に移動してロックが有効になったことを示します。<br>接続をロックすると、接続への不正な変更が防止されます。 |

| フィールド | 説明 |
|---|---|
| 自動優先（**AutoPriority**） | 灰色のボタンをクリックして、自動優先順位を有効にします。灰色のボタンが青色に変わり、右に移動して、自動優先が有効になったことを示します。<br><br>**[AutoPriority（自動優先）]**が有効な場合、**[Priority（優先度）]**フィールドは無効になります。NDB は、特定の基準（モニタリング ツールとフィルタ）に基づいて接続の優先度を自動的に割り当てます。<br><br>自動優先度は、接続内の複数のモニタリング ツールにフィルタをマッピングする柔軟性を提供します。詳細については、自動優先 （80 ページ）を参照してください。 |
| **[接続トポロジ（Connection Topology）]** | ここで、接続の**入力ポート、フィルタ、モニタリング ツール**を定義できます。 |

| フィールド | 説明 |
| --- | --- |
| 入力ポート | 接続の入力ポートを選択します。<br>**[入力ポート/グループの選択（Select Input Port(s)/ Group）]** をクリックします。**[入力ポート（Input Port）]** または **[入力ポート グループ（Input Port Group）]** を選択します。<br>**[入力ポート（Input Port）]** を選択すると、デバイスのリストが表示されます。<br>**1.** デバイスを選択するには、対応するチェックボックスをオンにします。選択したデバイスに応じて、デバイスの使用可能なポートが表示されます。<br>**2.** ポートを選択するには、対応するチェックボックスをオンにします。選択したポートの詳細が右側に表示されます。ポートの現在のステータスが色付きの丸で示されます。<br>（注）<br>**[入力ポートの追加（Add Input Port）]** をクリックして、選択したデバイスの入力ポートを追加します。詳細な手順については、**コンポーネント**の章の入力ポートの追加を参照してください。<br>**3.** **[選択（Select）]** をクリックして、選択した送信元ポートを接続の一部として含めます。<br>**[入力ポート グループ（Input Port Group）]** を選択すると、ポート グループのリストが表示されます。<br>**1.** ポート グループを選択するには、対応するチェック ボックスをオンにします。選択したポート グループの詳細が右側に表示されます。ポート グループの現在のステータスが色付きの丸で示されます。<br>（注）<br>**[入力ポート グループの追加（Add Input Port Group）]** をクリックして、入力ポート グループを追加します。詳細な手順については、**コンポーネント**の章の入力ポートの追加を参照してください。<br>.<br>**2.** **[選択（Select）]** をクリックして、選択した送信元ポート グループを接続の一部として含めます。 |

| フィールド | 説明 |
| --- | --- |
| **[フィルタ（Filter）]** | **[フィルタの選択（Select Filter）]** をクリックします。<br>1. フィルタを選択するには、対応するチェックボックスをオンにします。選択したフィルタの詳細が右側に表示されます。複数のフィルタを選択できます。フィルタが**許可**または**拒否**の動作を行うよう選択できます。許可は、入力ポートからのトラフィックが通過できるようにします。 拒否は、入力ポートからのトラフィックをドロップします。<br>（注）<br>**[フィルタの追加（Add Filter）]** をクリックして、フィルタを追加します。詳細な手順については、「フィルタの追加」を参照してください。<br>2. **[選択]** をクリックして、選択したフィルタを接続の一部として含めます。<br>（注）<br>**[自動優先（AutoPriority）]** が有効な場合、このフィールドは無効になります。 |

| フィールド | 説明 |
| --- | --- |
| モニタリング ツール | |

| フィールド | 説明 |
| --- | --- |
| | 自動優先が有効になっていない場合は、**[モニタリング ツール/グループの選択（Select Monitoring Tool(s)/Group）]** オプションが表示されます。<br><br>**[モニタリング ツール/グループの選択（Select Monitoring Tool(s)/Group）]** をクリックします。**[モニタリング ツール（Monitoring Tool）]** または **[ツール グループ（Tool Group）]** のいずれかを選択します。<br><br>**[モニタリング ツール（Monitoring Tool）]**を選択すると、モニタリング ツールの一覧が表示されます。<br><br>1. モニタリング ツールを選択するには、対応するチェックボックスをオンにします。モニタリング ツールの詳細が右側に表示され、モニタリング ツールの現在のステータスが表示されます。ステータスは、色分けされた円で示されます。<br><br>（注）<br>**[モニタリング ツールの追加（Add Monitoring Tool）]** をクリックして、モニタリング ツールを追加します。詳細な手順については、モニタリング ツールの追加を参照してください。<br><br>2. **[選択（Select）]** をクリックして、モニタリング ツールを接続の一部として含めます。<br><br>**[ツールグループ（Tool Group）]** を選択すると、モニタリング ツール グループのリストが表示されます。<br><br>1. ツール グループを選択するには、対応するチェック ボックスをオンにします。選択したツール グループの詳細が右側に表示されます。ツール グループの現在のステータスは、色分けされた円で示されます。<br><br>（注）<br>**[モニタリング ツール グループの追加（Add Monitoring Tool Group）]** をクリックして、モニタリング ツール グループを追加します。詳細な手順は、モニタリング ツールグループの追加を参照してください。<br><br>2. **[選択]**をクリックして、選択したツール グループを接続の一部として含めます。<br><br>自動優先が有効になっている場合は、**[モニタリング ツールとフィルタ ペアの選択（Select Monitoring Tool and Filter Pair）]** オプションが表示されます。 |

| フィールド | 説明 |
|---|---|
| | 1. 1 つ以上のモニタリング ツールとフィルタを選択します。<br>2. [選択（Select）] をクリックします。 |

**ステップ 4** **[接続の追加（Add Connection）]** をクリックして接続を追加するか、**[接続のインストール（Install Connection）]** をクリックして、NDB デバイスに接続を追加して展開します。

データ ブローカが、同じ Q-in-Q VLAN を持つ 2 つの接続を検出した場合（新しい接続を追加しているか、既存の接続を変更している場合）、接続をマージできます。 **[接続の追加（Add Connection）]** または **[接続のインストール（Install Connection）]**をクリックすると、ポップアップウィンドウが表示されます。 **[はい（Yes）]** をクリックして、2 つの接続をマージします。

# 接続の編集またはクローン処理

この手順に従って、接続を編集またはクローン処理します。

接続の編集は、既存の接続のパラメータを変更することを意味します。

接続のクローン処理とは、既存の接続と同じパラメータを使用して新しい接続を作成し、必要なパラメータを変更することを意味します。保存する前に、接続の名前を変更してください。

### 始める前に

1 つ以上の接続を作成します。

### 手順

**ステップ 1** **[接続（Connections）]** > **[ユーザー接続（User Connections）]** に移動します。

**ステップ 2** 表示された表で、**接続名**をクリックします。

新しいペインが右側に表示されます。

**ステップ 3** **[アクション（Actions）]** をクリックし、**[接続の編集（Edit Connection）]** を選択します。

接続を複製するには、**[接続のクローン処理（Clone Connection）]** を選択します。

**ステップ 4** **[接続の編集（Edit Connection）]** または **[接続のクローン処理（Clone Connection）]** ダイアログ ボックスに、現在の接続情報が表示されます。これらのフィールドを必要に応じて変更します。

**表 *23 :* 接続の編集/接続のクローン処理**

| フィールド | 説明 |
|---|---|
| 接続名 | 接続名です。 |

| フィールド | 説明 |
|---|---|
| 説明 | 接続の説明。 |
| 優先度（**Priority**） | 接続の現在の優先度。 |
| **[接続のロック（Lock Connection）]** | 灰色のボタンをクリックして接続をロックします。灰色のボタンが青色に変わり、右に移動してロックが有効になったことを示します。<br>接続をロックすると、接続への不正な変更が防止されます。 |
| **[自動優先（Auto Priority）]** | 接続の追加時に**[自動優先（Auto Priority）]**が有効になっていない場合、このフィールドは無効になります。 |
| **[接続トポロジ（Connection Topology）]** | ここで、接続の**入力ポート、フィルタ、モニタリング ツール**を定義できます。 |
| 入力ポート | 接続に含まれる現在の入力ポートが表示されます。接続からポートを削除するには、入力ポートの横にある十字マークをクリックします。入力ポートを編集するには、**[入力ポート/グループの選択（Select Input Port(s)/Group）]** をクリックします。**[入力ポート（Input Port）]** または **[入力ポート グループ（Input Port Group）]** を選択します。<br>**[入力ポート（Input Port）]** を選択すると、デバイスのリストが表示されます。<br>**1.** デバイスを選択するには、対応するチェックボックスをオンにします。選択したデバイスに応じて、デバイスの使用可能なポートが表示されます。<br>**2.** ポートを選択するには、対応するチェックボックスをオンにします。選択したポートの詳細が右側に表示されます。<br>**3.** **[選択（Select）]** をクリックして、選択した送信元ポートを接続の一部として含めます。<br>**[入力ポート グループ（Input Port Group）]** を選択すると、ポート グループのリストが表示されます。<br>**1.** ポート グループを選択するには、対応するチェック ボックスをオンにします。選択したポート グループの詳細が右側に表示されます。<br>**2.** **[選択（Select）]** をクリックして、選択した送信元ポート グループを接続の一部として含めます。 |

| フィールド | 説明 |
|---|---|
| **[フィルタ（Filter）]** | 接続に含まれている現在のフィルタが表示されます。接続からフィルタを削除するには、フィルタの横にある十字マークをクリックします。フィルタを編集するには、**[フィルタの選択（Select Filter(s)）]** をクリックします。<br>**1.** フィルタを選択するには、対応するチェック ボックスをオンにします。選択したフィルタの詳細が右側に表示されます。複数のフィルタを選択できます。<br>**2.** **[選択（Select）]** をクリックして、接続の一部として選択したフィルタを含めます。 |
| **[モニタリング ツール（Monitoring Tools）]** | 接続に含まれている現在のモニタリング ツールまたはツール グループが表示されます。モニタリング ツールまたはツール グループの横にある十字マークをクリックして、接続から削除します。これらのいずれかを編集するには、**[モニタリング ツール/グループの選択（Select Monitoring Tool(s)/ Group）]** をクリックします。**[モニタリング ツール（Monitoring Tool）]** または **[ツール グループ（Tool Group）]** のいずれかを選択します。<br>**[モニタリング ツール（Monitoring Tool）]**を選択すると、モニタリング ツールの一覧が表示されます。<br>**1.** モニタリングツールを選択するには、対応するチェックボックスをオンにします。モニタリング ツールの詳細が右側に表示され、モニタリング ツールの現在のステータスが表示されます。ステータスは、色分けされた円で示されます。<br>**2.** **[選択（Select）]** をクリックして、モニタリング ツールを接続の一部として含めます。<br>**[ツールグループ（Tool Group）]** を選択すると、モニタリング ツール グループのリストが表示されます。<br>**1.** ツール グループを選択するには、対応するチェック ボックスをオンにします。選択したツール グループの詳細が右側に表示されます。ツール グループの現在のステータスは、色分けされた円で示されます。<br>**2.** **[選択（Select）]** をクリックして、接続の一部として選択したツール グループを含めます。 |

**ステップ 5** **[保存（Save）]** をクリックします。

# 自動優先

自動優先度は、接続内の複数の接続先デバイスにフィルタを柔軟にマッピングできるようにします。自動優先度を使用する接続の優先度は、`config.ini` ファイルで構成された値に設定されます。config.ini ファイルの *connection.autopriority.priorityValue* 属性に、自動優先度を持つすべての新しい接続に使用される優先度の値を設定できます。接続情報には、許可されたフィルタと接続先デバイスが一覧表示されます。

# デフォルトの接続

**[デフォルトの接続（Default Connections）]** タブには、デフォルトの Nexus Dashboard Data Broker 接続の詳細が表示されます。デフォルトの拒否ルールはシステムによるもので、入力ポート、監視ツール、およびパケット切り捨てポートで構成されています。つまり、デフォルトでは、ユーザー定義の接続が構成されていない限り、入力ポートで受信したトラフィックは拒否されます。

デフォルトでは、拒否 ACL はすべてのスイッチ間リンク（ISL）インターフェイスで有効になっており、接続がインストールされていない場合、ISL インターフェイスのすべてのトラフィックがドロップされます。次の接続が ISL インターフェイスにインストールされています。

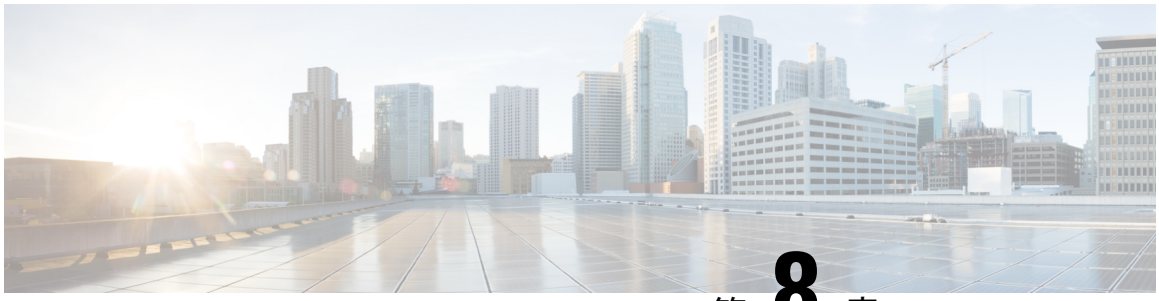
- Default-Deny-All、Default-Deny-MPLS、および Default-Deny-ARP フィルタを使用した Default-Deny-ISL-*device_name* 接続。この接続は、NXAPI モードのすべてのタイプのスイッチでサポートされています。
- Default-Deny-ICMP および Default-Deny-ICMP-All フィルタを使用した Default-Deny-ISL-ICMP-*device_name* 接続。この接続は、NXAPI モードの Nexus 9200、9300EX、9300FX、9500EX、および 9500FX スイッチでサポートされています。
- この機能は、config.ini ファイルの mm.addDefaultISLDenyRules 属性を使用して管理できます。デフォルトでは、mm.addDefaultISLDenyRules 属性は config.in ファイルに存在しません。この機能を無効にするには、mm.addDefaultISLDenyRules 属性を config.ini ファイルに追加し、それを false に設定してデバイスを再起動する必要があります。次に例を示します。

```
mm.addDefaultISLDenyRules = false
```

票には次の詳細が表示されます。

表 *24 :* デフォルトの接続

| 列名 | 説明 |
|---|---|
| 接続名（**Connection Name**） | デフォルトの接続名。<br>このフィールドはハイパーリンクです。接続の名前をクリックします。接続に関する詳細情報を含む新しいペインが右側に表示されます。<br>ここでは、次のアクションを実行できます。<br>• **[接続のクローン（Clone Connection）]**：このアクションを選択して、接続を複製します。詳細については、接続の編集を参照してください。接続のクローン処理は、接続の編集に似ています。<br>（注）<br>デフォルトの接続は編集できません。 |
| **[ドロップ フィルタ（Drop Filters）]** | 接続のドロップしたフィルタの数。<br>NDB のドロップ フィルタは、マッチしたトラフィックをドロップします。 |
| **[入力/モニタリング ポート（Input/Monitoring Port）]** | 入力ポートまたはモニタリング ポートの数。 |
| 説明 | 接続の説明。 |



第 8 章

# コンポーネント

この章では、Cisco Nexus Dashboard Data Broker のコンポーネントについて詳しく説明します。

リリース 3.10.1 から、Cisco Nexus Data Broker（NDB）の名前は、Cisco Nexus Dashboard Data Brokerに変更されました。ただし、GUI およびインストール フォルダ構造と対応させるため、一部の NDB のインスタンスがこのドキュメントには残されています。NDB/ Nexus Data Broker/ Nexus Dashboard Data Brokerという記述は、相互に交換可能なものとして用いられています。



## フィルタ

**[フィルタ（Filters）]** タブには、Nexus Dashboard Data Broker コントローラで使用可能なすべてのフィルタの詳細が表示されます。このタブには、着信トラフィックのフィルタリング基準（接続で使用される）の情報が表示されます。

デフォルトのフィルタには、パケット フィルタリング用の次のプロトコルが含まれています。

- Default-match-all
- Default-match-IP
- Default-match-ARP
- Default-match-MPLS（ユニキャストおよびマルチキャスト）
- Default-match-ICMP
- Default-match-ICMP-All

次の詳細を含む表が表示されます。

表 *25:* フィルタ

| 列名 | 説明 |
|---|---|
| 使用中 | 緑色のチェック マークは、接続でフィルタが使用中であることを示します。 |
| **[フィルタ（Filter）]** | フィルタ名。<br>**[フィルタ（Filters）]** をクリックします。右側に新しいペインが表示され、フィルタに関する詳細情報が表示されます。ここから、次の追加のアクションを実行できます。<br>（注）<br>デフォルトのフィルタは編集できません。 |
| 双方向 | フィルタが双方向の場合、**[はい（Yes）]** が表示され、それ以外の場合は **[いいえ（No）]** が表示されます。<br>フィルタが双方向とマークされている場合、着信トラフィックと発信トラフィックは同じポートでフィルタリングされます。 |
| **Ethertype** | フィルタのレイヤ 2 イーサタイプ。 |
| プロトコル | フィルタが使用するレイヤ 3 プロトコル。 |
| **[高度なフィルタ（Advanced Filter(s)）]** | フィルタに関連付けられた高度なフィルタ。 |
| 作成者 | フィルタを作成したユーザー。 |
| **[最終更新者（Last Modified By）]** | フィルタを最後に変更したユーザー。 |
| ステータスの説明 | フィルタの現在のステータス。ステータスの説明は、最新のステータスに基づいて自動更新されます。<br>また、  の *[更新（Refresh）]* をクリックして、最新ステータスを取得できます。 |

**[フィルタ（Filters）]** タブでは、次のアクションを実行できます。

- **[フィルタの追加（Add Filter）]** — これを使用して、新しいフィルタを追加します。このタスクの詳細については、詳細を参照してください。
- **[フィルタの削除（Delete Filter）]**：行の先頭にあるチェックボックスをオンにして、削除するフィルタを選択し、**[アクション（Actions）]**>**[フィルタの削除（Delete Filter）]** をクリックします。選択したフィルタが削除されます。チェック ボックスを選択せずに削除ア

クションを選択すると、エラーが表示されます。フィルタを選択するように求められます。

# フィルタの追加

フィルタを追加するには、この手順に従います。着信トラフィックは、フィルタで定義されたパラメータに基づいて照合されます。

### 手順

**ステップ 1** **[コンポーネント（Components）]** > **[フィルタ（Filter）]** に移動します。

**ステップ 2** **[アクション]** ドロップダウン メニューから **[フィルタの追加（Add Filter）]** を選択します。

**ステップ 3** **[フィルタの追加（Add Filter）]** ダイアログボックスで、次の詳細を入力します。

表 *26 :* フィルタの追加

| フィールド | 説明 |
|---|---|
| フィルタ名（Filter Name） | フィルタの名前を入力します。 |
| **双方向** | 双方向トラフィック情報をフィルタ処理する場合は、このボックスをオンにします。送信元 IP、送信元ポートまたは送信元 MAC アドレスから接続先 IP、接続先ポート、または接続先 MAC アドレスを取得すること、および接続先 IP、接続先ポート、または接続先 MAC から送信元 IP、送信元ポート、または送信元 MAC アドレスを取得することができます。 |

| フィールド | 説明 |
| --- | --- |
| レイヤ 2 | |

| フィールド | 説明 |
| --- | --- |
| | レイヤ2フィルタリングの使用中に表示されるオプションは次のとおりです。<br>• [イーサネット タイプ（Ethernet Type）]：ドロップダウン リストからイーサネット タイプを選択します。次のオプションがあります。<br>  • IPv4<br>  • IPv6<br>  • LLDP<br>  • MPLS<br>  • ARP<br>  • [すべてのイーサネット タイプ（All Ethernet Types）]<br>  • [事前定義されたイーサネット タイプ（Predefined Ethernet Types）]：このオプションを選択する場合、`config.ini` ファイルに含まれているすべての事前定義されたイーサネット タイプがルールに関連付けられていること、さらにほかのパラメータは構成されていないことが必要です。<br>  • [イーサネット タイプの入力（Enter Ethernet Type）]：このオプションを選択した場合、イーサネット タイプを 16 進形式で入力します。<br>• [VLAN 識別番号（VLAN Identification Number）]：レイヤ 2 トラフィックの VLAN ID を入力します。単一の VLAN ID、VLAN ID の範囲、カンマ区切りの VLAN ID と VLAN ID 範囲を入力できます。<br>最大値は 4095 です。<br>• [VLAN 優先度（VLAN Priority）]：トラフィックの VLAN 優先度を入力します。VLAN 優先度は、レイヤ 2 トラフィックにのみマッチします。<br>• 送信元 MAC アドレス — 送信元デバイスの MAC アドレスを入力します。MAC アドレスは、レイヤ 2 トラフィックにのみマッチします。<br>• [接続先 MAC アドレス（Destination MAC Address）]：接続先デバイスの MAC アドレスを入力します。MAC アドレスは、レイヤ2トラフィックにのみマッチします。 |

| フィールド | 説明 |
| --- | --- |
| | • [MPLS ラベル値（MPLS Label Value）]：ラベル 1、ラベル 2、ラベル 3、ラベル 4 の MPLS 値を入力します。<br><br>**[PLS ラベル値（MPLS Label Value）]** フィールドは、**[イーサネット タイプ（Ethernet Type）]** が MPLS に設定されている場合にのみ表示されます。MPLS ラベル値がマッチします。 |

| フィールド | 説明 |
| --- | --- |
| **レイヤ 3**<br>レイヤ 3 のオプションを有効にするには、[レイヤ 2（Layer 2）] タブで **[IPv4]** または **[IPv6]** を **[イーサネット タイプ（Ethertype）]** として選択します。 | |

| フィールド | 説明 |
| --- | --- |
| | レイヤ3フィルタリングで表示されるオプションは次のとおりです。<br>• [送信元 IP アドレス（Source IP Address）]： レイヤ 3 トラフィックの送信元 IP アドレスを入力します。次のいずれかになります。<br>  • 標準の IPv4 または IPv6 形式のホスト IP アドレス<br>  • IPv4 または IPv6 のアドレス範囲<br>  • アドレス範囲と標準 IP アドレスの組み合わせ。例: 10.1.1.1、10.1.1.2-10.1.1.5<br>  • コンマで区切られた連続していないIPアドレス。例: 10.1.1.1、10.1.1.2、10.1.1.5<br>（注）<br>レイヤ 3 送信元 IP アドレスの範囲を設定する場合、レイヤ 4 の送信元または接続先ポートの範囲を設定することはできません。<br>レイヤ 3 送信元 IP アドレスの範囲を構成する場合、レイヤ 2 VLAN の識別子の範囲を構成することはできません。<br>• [接続先 IP アドレス（Destination IP Address）]：レイヤ3トラフィックの接続先IPアドレスを入力します。次のいずれかになります。<br>  • 標準の IPv4 または IPv6 形式のホスト IP アドレス<br>  • IPv4 または IPv6 のアドレス範囲<br>  • アドレス範囲と標準 IP アドレスの組み合わせ。例: 10.1.1.1、10.1.1.2-10.1.1.5<br>  • コンマで区切られた連続していないIPアドレス。例: 10.1.1.1、10.1.1.2、10.1.1.5<br>（注）<br>レイヤ 3 送信元 IP アドレスの範囲を設定する場合、レイヤ 4 の送信元または接続先ポートの範囲を設定することはできません。<br>レイヤ 3 送信元 IP アドレスの範囲を構成する場合、レイヤ 2 VLAN の識別子の範囲を構成することはで |

| フィールド | 説明 |
| --- | --- |
| | きません。<br>• L4 プロトコル — ドロップダウン リストからレイヤ 4 プロトコルを選択するか、**プロトコル番号（Protocol Number）**を入力します。<br>• [高度なフィルタ（Advanced Filter）]：このボタンをクリックすると、高度なフィルタ処理が有効になり、必要なオプションを選択するためのチェックボックスを使用できるようになります。高度なフィルタに関連するオプションの詳細については、高度なフィルタを参照してください。<br>• [カスタム フィルタ（Custom Filter）]：このボタンをクリックすると、ユーザー定義フィールド（UDF）を使用したカスタム フィルタ処理が有効になります。**[UDF の選択（Select UDFs）]** をクリックして、**[カスタム フィルタの選択（Select Custom Filters）]** ウィンドウでフィルタを選択します。[UDF の追加（Adding a UDF）]を使用して作成された UDF は、ここに表示されます。<br>選択した UDF がテーブルに表示されます。選択した UDF について、次の詳細を入力します。<br>• [値（Value）]：マッチさせる値（0 ～ 65535）を 10 進表記で入力します。たとえば、0x0806 と一致させたい場合は、0x0806 の 10 進表記である 2054 を入力します。<br>• [マスク（Mask）]：照合の際、値に適用されるマスクです。たとえば、2054（0x0806）に正確に一致させるには 65535（0xffff）と入力し、2048-2063（0x0800-0x080f）に一致させるには 65520（0xfff0）を使用します。<br>（注）<br>モニタリング ツール ポートが ISL デバイス上にある場合は、**[内部 VLAN にデフォルトの UDF を追加（Add Default UDF for inner vlan）]** チェックボックスを選択する必要があります。入力ポートに Q-in-Q が構成されていることを確認します。 |

| フィールド | 説明 |
| --- | --- |
| **Layer 4（レイヤ 4）**<br>レイヤ 4 のオプションを有効にするには、[レイヤ 2（Layer 2）] タブで **[IPv4]** または **[IPv6]** を **[Ethertype]** として選択し、[レイヤ 3（Layer 3）] タブで **[TCP]** または **[UDP]** を **[L4 プロトコル（L4 Protocol）]** として選択します。 | |

| フィールド | 説明 |
| --- | --- |
| | レイヤ4フィルタリングで表示されるオプションは次のとおりです。<br>• [送信元ポート（Source Port）]：ドロップダウンリストから送信元ポートを選択します。次のオプションがあります。<br>• FTP（データ）<br>• FTP（コントロール）<br>• SSH<br>• Telnet<br>• HTTP<br>• HTTPS<br>• [送信元ポートを入力（Enter Source Port）]：送信元ポートを入力します。単一のポート番号をコンマで区切って入力するか、接続先ポート番号の範囲を入力できます。<br>（注）<br>レイヤ 4 送信元ポートの範囲を入力すると、レイヤ 3 IP アドレスまたはレイヤ 2 VLAN 識別子の範囲を構成できません。<br>• [接続先ポート（Destination Port）]：ドロップダウンリストで、接続先ポートを選択します。次のオプションがあります。<br>• FTP（データ）<br>• FTP（コントロール）<br>• SSH<br>• Telnet<br>• HTTP<br>• HTTPS<br>• [接続先ポートを入力（Enter Destination Port）]：接続先ポートを入力します。単一のポート番号をコンマで区切って入力するか、接続先ポート番号の範囲を入力できます。<br>（注）<br>レイヤ 4 接続先ポートの範囲を入力すると、レ |

| フィールド | 説明 |
|---|---|
| | イヤ 2 VLAN 識別子またはレイヤ 3 IP アドレスの範囲を設定できません。 |
| レイヤ 7 | 未サポート |

（注）
カスタム フィルタリングの場合：1 つのフィルタに最大 4 つの UDF を追加できます。UDF オプションは、IPv4 および IPv6 のイーサタイプに対して有効になっています。

**ステップ 4** **[フィルタの追加（Add Filter）]** をクリックして、フィルタを追加します。

# フィルタの編集またはクローン

この手順に従い、フィルタを編集するか、またはフィルタのクローンを作成します。

フィルタの編集は、既存のフィルタのパラメータを変更することを意味します。

フィルタのクローンつまり複製とは、既存のフィルタと同じパラメータを使用して新しいフィルタを作成し、フィルタ パラメータに必要な変更を加えることを意味します。保存する前に、フィルタの名前を変更してください。

（注） デフォルトのフィルタは編集できません。

### 始める前に

1 つ以上のフィルタを追加します。

### 手順

**ステップ 1** **[コンポーネント（Components）]** > **[フィルタ（Filters）]** に移動します。

**ステップ 2** 表示された表で、いずれかの**フィルタ**をクリックします。

新しいペインが右側に表示されます。

**ステップ 3** **[アクション（Actions）]** をクリックし、**[フィルタのクローン（Clone Filter）]** を選択します。

**ステップ 4** **[フィルタのクローン（Clone Filter）]** または **[フィルタの編集（Edit Filter）]** ダイアログ ボックスに、現在のフィルタ情報が表示されます。これらのフィールドを必要に応じて変更します。

表 *27 :* フィルタの編集/クローン（***Edit/Clone Filter***）

| フィールド | 説明 |
|---|---|
| フィルタ名（Filter Name） | フィルタの名前。 |
| **双方向** | 双方向トラフィック情報をフィルタ処理する場合は、このボックスをオンにします。送信元 IP、送信元ポートまたは送信元MACアドレスから接続先IP、接続先ポート、または接続先MACアドレスを取得すること、および接続先IP、接続先ポート、または接続先MACから送信元IP、送信元ポート、または送信元MACアドレスを取得することができます。 |

| フィールド | 説明 |
| --- | --- |
| レイヤ 2 | |

| フィールド | 説明 |
| --- | --- |
| | レイヤ2の使用中に表示されるオプションは次のとおりです。<br>• [イーサネット タイプ（Ethernet Type）]：ドロップダウン リストからイーサネット タイプを選択します。次のオプションがあります。<br>• IPv4<br>• IPv6<br>• LLDP<br>• MPLS<br>• ARP<br>• [すべてのイーサネット タイプ（All Ethernet Types）]<br>• [事前定義されたイーサネット タイプ（Predefined Ethernet Types）]： このオプションを選択する場合、`config.ini` ファイルに含まれているすべての事前定義されたイーサネット タイプがルールに関連付けられていること、さらにほかのパラメータは構成されていないことが必要です。<br>• [イーサネット タイプの入力（Enter Ethernet Type）]：このオプションを選択した場合、イーサネット タイプを 16 進形式で入力します。<br>• [VLAN 識別番号（VLAN Identification Number）]：レイヤ 2 トラフィックの VLAN ID を入力します。単一の VLAN ID、VLAN ID の範囲、カンマ区切りの VLAN ID と VLAN ID 範囲を入力できます。<br>最大値は 4095 です。<br>• [VLAN 優先度（VLAN Priority）]：トラフィックの VLAN 優先度を入力します。<br>VLAN優先度は、レイヤ2トラフィックにのみマッチします。<br>• 送信元 MAC アドレス — 送信元デバイスの MAC アドレスを入力します。<br>MAC アドレスは、レイヤ 2 トラフィックにのみマッチします。<br>• [接続先 MAC アドレス（Destination MAC Address）]： |

| フィールド | 説明 |
| --- | --- |
| | 接続先デバイスの MAC アドレスを入力します。<br>MAC アドレスは、レイヤ 2 トラフィックにのみマッチします。<br>• [MPLS ラベル値（MPLS Label Value）]：ラベル 1、ラベル 2、ラベル 3、ラベル 4 の MPLS 値を入力します。<br>**[PLS ラベル値（MPLS Label Value）]** フィールドは、**[イーサネット タイプ（Ethernet Type）]** が MPLS に設定されている場合にのみ表示されます。MPLS ラベル値がマッチします。 |

| フィールド | 説明 |
| --- | --- |
| **レイヤ 3**<br>レイヤ 3 のオプションを有効にするには、[レイヤ 2（Layer 2）] タブで **[IPv4]** または **[IPv6]** を **[イーサネット タイプ（Ethertype）]** として選択します。 | |

| フィールド | 説明 |
| --- | --- |
| | レイヤ3の使用中に表示されるオプションは次のとおりです。<br>• [送信元 IP アドレス（Source IP Address）]： レイヤ 3 トラフィックの送信元 IP アドレスを入力します。次のいずれかになります。<br>• 標準の IPv4 または IPv6 形式のホスト IP アドレス<br>• IPv4 または IPv6 のアドレス範囲<br>• アドレス範囲と標準 IP アドレスの組み合わせ。例: 10.1.1.1、10.1.1.2-10.1.1.5<br>• コンマで区切られた連続していないIPアドレス。例: 10.1.1.1、10.1.1.2、10.1.1.5<br>（注）<br>レイヤ 3 送信元 IP アドレスの範囲を設定する場合、レイヤ 4 の送信元または接続先ポートの範囲を設定することはできません。<br>レイヤ 3 送信元 IP アドレスの範囲を構成する場合、レイヤ 2 VLAN の識別子の範囲を構成することはできません。<br>• [接続先 IP アドレス（Destination IP Address）]：レイヤ3トラフィックの接続先IPアドレスを入力します。次のいずれかになります。<br>• 標準の IPv4 または IPv6 形式のホスト IP アドレス<br>• IPv4 または IPv6 のアドレス範囲<br>• アドレス範囲と標準 IP アドレスの組み合わせ。例: 10.1.1.1、10.1.1.2-10.1.1.5<br>• コンマで区切られた連続していないIPアドレス。例: 10.1.1.1、10.1.1.2、10.1.1.5<br>（注）<br>レイヤ 3 送信元 IP アドレスの範囲を設定する場合、レイヤ 4 の送信元または接続先ポートの範囲を設定することはできません。<br>レイヤ 3 送信元 IP アドレスの範囲を構成する場合、レイヤ 2 VLAN の識別子の範囲を構成することはで |

| フィールド | 説明 |
| --- | --- |
| | きません。<br>• [L4 プロトコル（L4 Protocol）]：ドロップダウンリストからレイヤ 4 プロトコルを選択します。<br>• [高度なフィルタ（Advanced Filter）]：高度なフィルタ処理を有効にする場合には、このボタンをクリックして、必要なオプションを選択するためのチェックボックスをオンにしてください。高度なフィルタの詳細については、高度なフィルタを参照してください。<br>• [カスタム フィルタ（Custom Filter）]：このボタンをクリックすると、ユーザー定義フィールド（UDF）を使用したカスタム フィルタ処理が有効になります。**[UDF の選択（Select UDFs）]** をクリックして、**[カスタム フィルタの選択（Select Custom Filters）]** ウィンドウでフィルタを選択します。 |

| フィールド | 説明 |
| --- | --- |
| **Layer 4（レイヤ 4）**<br>レイヤ 4 のオプションを有効にするには、[レイヤ 2（Layer 2）] タブで **[IPv4]** または **[IPv6]** を **[Ethertype]** として選択し、[レイヤ 3（Layer 3）] タブで **[TCP]** または **[UDP]** を **[L4 プロトコル（L4 Protocol）]** として選択します。 | |

| フィールド | 説明 |
| --- | --- |
| | レイヤ4の使用中に表示されるオプションは次のとおりです。<br>• [送信元ポート（Source Port）]：ドロップダウン リストから送信元ポートを選択します。次のオプションがあります。<br>• FTP（データ）<br>• FTP（コントロール）<br>• SSH<br>• Telnet<br>• HTTP<br>• HTTPS<br>• [送信元ポートを入力（Enter Source Port）]：送信元ポートを入力します。単一のポート番号をコンマで区切って入力するか、接続先ポート番号の範囲を入力できます。<br>（注）<br>レイヤ 4 送信元ポートの範囲を入力すると、レイヤ 3 IP アドレスまたはレイヤ 2 VLAN 識別子の範囲を構成できません。<br>• [接続先ポート（Destination Port）]：ドロップダウン リストで、接続先ポートを選択します。次のオプションがあります。<br>• FTP（データ）<br>• FTP（コントロール）<br>• SSH<br>• Telnet<br>• HTTP<br>• HTTPS<br>• [接続先ポートを入力（Enter Destination Port）]：接続先ポートを入力します。単一のポート番号をコンマで区切って入力するか、接続先ポート番号の範囲を入力できます。<br>（注）<br>レイヤ 4 接続先ポートの範囲を入力すると、レ |

| フィールド | 説明 |
|---|---|
| | イヤ 2 VLAN 識別子またはレイヤ 3 IP アドレスの範囲を設定できません。 |
| レイヤ 7 | 未サポート |

**ステップ 5** **[保存（Save）]** をクリックします。

# 詳細フィルタ

高度なフィルタリングには、イーサネット タイプと、確認応答、FIN、フラグメント、PSH、RST、SYN、DSCP、優先順位、TTL、パケット長、NVE などの属性に基づいてトラフィックをフィルタリング（許可または拒否）するための複数のオプションが用意されています。高度なフィルタリングは、次のイーサネット タイプとオプションで利用できます。

**表 *28* : 高度なフィルタリングのサポート**

| データタイプ | サポートされるオプション |
|---|---|
| IPv4 | DSCP、フラグメント、優先順位、および TTL |
| IPv4 と TCP | 確認応答、DSCP、フラグメント、FIN、優先順位、PSH、RST、SYN、および TTL |
| IPv4 と UDP | DSCP、フラグメント、優先順位、および TTL |
| IPv6 | DSCP とフラグメント |
| IPv6 と TCP | 確認応答、DSCP、フラグメント、FIN、PSH、RST、および SYN |
| IPv6 と UDP | DSCP とフラグメント |

（注） 高度なフィルタリングは、Cisco Nexus 9000 プラットフォームの NX-API でのみ使用できます。

Time to Live（TTL）属性の範囲は 0 ～ 255 です。Nexus 9200 端末の場合、設定できる TTL の最大値は 3 です。残りの Nexus 9000 シリーズ デバイスの場合、NX-OS バージョン 7.0(3)I6(1) 以降では、TTL 値を最大 3 にすることができます。NXOS バージョン 7.0(3)I4(1) 以前では、範囲内の任意の値を設定できました。

### 高度なフィルタリングの使用に関する制限

高度なフィルタの構成中、次のことはできません。

- DSCP と優先順位を一緒に設定すること。
- フラグメントと ACK または SYN または FIN または PSH または RST を一緒に構成すること。
- UDP と IPv4 または IPv6 の組み合わせでフラグメントとポート番号を構成すること。
- IPv4 と TCP の組み合わせで優先順位と HTTP メソッドを構成すること。

# グローバル設定

**[グローバル構成（Global Configuration）]** タブには、Nexus Dashboard Data Broker コントローラに接続されているデバイスが表示されます。Nexus Dashboard Data Broker コントローラに追加された新しいデバイスは、デフォルトでここに表示されます。

（注） ここには、接続されているデバイス（接続状態が緑色で表示）のみが表示されます。デバイスが Nexus Dashboard Data Broker コントローラに追加されているが、接続されていない場合（接続ステータスは赤で示されます）、そのデバイスはここに表示されません。デバイスのステータスを確認するには、NDB デバイスを参照してください。

次の詳細の表が表示されます。

**表 *29*：グローバル設定**

| 列名 | 説明 |
|---|---|
| **Device** | デバイス名<br>これはハイパーリンクです。**デバイス**の名前をクリックして、デバイスのグローバル構成の詳細を取得できます。 |
| **Loadbalancing** | ロード バランシングのタイプを表示します。次のオプションがあります。<br>• Symmetric<br>• 非対称（Non-symmetric） |
| **PTP** | PTP が有効かどうかを表示します。次のオプションがあります。<br>• 有効<br>• 無効 |

| 列名 | 説明 |
|---|---|
| **Jumbo MTU** | デバイスのジャンボ MTU サイズ。<br>ジャンボMTUは、デバイスに構成できる最大の MTU です。 |
| **MPLS ストリップ** | デバイスでMPLSストリッピングが有効になっているかどうかを表示します。次のオプションがあります。<br>• 有効<br>• 無効 |
| **[MPLS フィルタ（MPLS Filter）]** | デバイスの MPLS フィルタリングが有効かどうかを表示します。次のオプションがあります。<br>• 有効<br>• 無効 |
| **Netflow** | デバイスの Netflow が有効かどうかを表示します。次のオプションがあります。<br>• 有効<br>• 無効 |

次のアクションは、**[グローバル構成（Global Configuration）]** タブから実行できます。

- **[グローバル構成の編集（Edit Global Configuration）]**：手順の詳細については、デバイスのグローバル構成の編集 （106 ページ）を参照してください。

# デバイスのグローバル構成の編集

この手順に従って、デバイスのグローバル構成を編集します。デバイスのパラメータはグローバルに変更できます。たとえば、ここで設定するジャンボ MTU 値は、デバイスの入力ポートの MTU 値を定義します。

デバイスの作成時にはいくつかの基本構成が作成され、いくつかのデフォルト値が設定されます。この手順を使用して、デバイスの 1 つ以上のパラメータを変更または追加します。

### 始める前に

1 つ以上のデバイスを作成します。デバイスのステータスを確認します。

手順

**ステップ 1** **[コンポーネント（Components）]** > **[グローバル構成（Global Configuration）]** に移動します。

**ステップ 2** 行の先頭にあるチェック ボックスをオンにしてデバイスを選択します。

**ステップ 3** **[アクション（Actions）]** ドロップダウン メニューから、**[グローバル構成の編集（Edit Global Configuration）]** を選択します。

**ステップ 4** **[グローバル構成の編集（Edit Global Configuration）]** ダイアログボックスで、次の詳細情報を入力します。

表 *30* : グローバル構成の編集

| フィールド | 説明 |
|---|---|
| **[全般（General）]** | |
| **[デバイス（Device）]** | デバイス名は、以前の選択に基づいて表示されます。 |
| **[ 負荷分散タイプの構成（Load Balancing Type Configuration）]** | ドロップダウン リストから **[対称（Symmetric）]** または **[非対称（Non-symmetric）]** を選択します。<br>負荷分散の詳細については、対称型および非対称型ロード バランシング （54 ページ） を参照してください。 |
| **[ハッシュ構成（Hashing Configuration）]** | ドロップダウン リストからハッシュ構成を選択します。表示されるドロップダウン リストは動的で、選択した負荷分散タイプによって異なります。 |
| **[ハッシュ タイプ（Hashing Type）]** | ドロップダウン リストからハッシュ タイプを選択します。 |
| **[MPLS の構成（MPLS Configuration）]** | |
| **[MPLS ストリップ タイプの設定（MPLS Strip Type Configuration ）]** | グレーのボタンをクリックして、MPLS ストリップ タイプの設定を有効にします。ボタンが青色に変わり、右に移動します。<br>入力ポートからのすべての MPLS パケットで、MPLS ヘッダーが取り除かれます。<br>（注）<br>Cisco Nexus 9300-GX シリーズ スイッチでは、MPLS ストリップ機能は、スイッチのリロード後にのみ機能します。 |

| フィールド | 説明 |
| --- | --- |
| **[ラベルのエージング（Label Age）]** | MPLS ラベルが期限切れになるまでの期間を設定します。このフィールドは、選択したデバイスでのみ使用できます。<br>サポートされているプラットフォームは、次の Cisco Nexus シリーズの 93128TX、3172、3164、3232、3132C-Z スイッチです。 |
| **[MPLS フィルタ構成を有効にする（Enable MPLS Filter Configuration）]** | グレーのボタンをクリックして、MPLS フィルタ構成を有効にします。ボタンが青色に変わり、右に移動します。<br>ここで有効になっている MPLS フィルタ構成は、デバイスの入力ポートに適用されます。 |
| **[sFlow 設定（sFlow Configuration）]** | |

| フィールド | 説明 |
|---|---|
| **[sFlow の有効化（Enable sFlow）]** | グレーのボタンをクリックして、サンプル フロー（sFlow）を有効にします。ボタンが青色に変わり、右に移動します。<br><br>sFlowの詳細については、サンプリングされたフロー （117 ページ） を参照してください。<br><br>次の詳細を入力します。<br><br>• **[エージェントの IP アドレス（Agent IP Address）]**：エージェントの IP アドレスを入力します。<br><br>• **[VRF の選択（Select VRF）]** — ドロップダウンリストから VRF を選択します。<br><br>• **[コレクタ IP アドレス（Collector IP Address）]**：コレクタ ポートの IP アドレスを入力します。<br><br>• **[コレクタ UDP ポート（Collector UDP Port）]**：sFlow コレクタの UDP ポートを入力します。<br><br>• **[カウンタ ポーリング間隔（Counter Poll Interval）]**：sFlow のポーリング間隔値を入力します。<br><br>• **[最大データグラム サイズ（Max Datagram Size）]**：最大データグラム サイズを入力します。<br><br>• **[最大サンプル サイズ（Max Sampled Size）]**：最大サンプル サイズを入力します。<br><br>• **[サンプリング レート（Sampling Rate）]**：データ サンプリング レートを入力します。<br><br>• **[データ ソース（Data Sources）]**：**[ポートの選択（Select Ports）]** をクリックし、必要なチェック ボックスをオンにしてポートを選択し、**[追加（Add）]** をクリックします。<br><br>（注）<br>デバイスの sFlow 設定を確認するには、 **show sflow** コマンドを使用します。 |
| **[PTP 構成（PTP Configuration）]** | |

| フィールド | 説明 |
|---|---|
| **[PTP の有効化（Enable PTP）]** | グレーのボタンをクリックしてPTPを有効にし、マスターから更新を受信します。ボタンが青色に変わり、右に移動します。<br><br>ここで有効になっている PTP は、入力ポートと監視ツールのタイムスタンプで使用されます。<br><br>PTP の詳細については、高精度時間プロトコル（116ページ） を参照してください。<br><br>次のフィールドが表示されます。<br><br>• **[送信元 IP アドレス（Source IP Address）]**：PTP アップデートを受信するための送信元 IP アドレスを入力します。<br><br>• **[ポート（Ports）]**：**[ポートの選択（Select Ports）]** をクリックし、チェックボックスをオンにして、PTP 送信元 IP を接続するために必要なポートを選択します。<br><br>（注）<br>PTP クロック タイムの同期を確保するには、ネットワーク内のすべてのデバイスでPTP を有効にする必要があります。 |
| **[ジャンボ MTU 構成（Jumbo MTU Configuration）]** | |
| **[MTU 値（MTU Value）]** | MTU 値を入力します。範囲は 1502 ～ 9216 です。ジャンボ MTU は、デバイスが受け入れることができる最大の MTU 値を設定します。<br><br>トラフィックの MTU サイズは通常 1500 です。MTU が 1500 を超えるトラフィックを受信するには、これを有効にします。ここで定義されたMTU値は、デバイスの入力ポートの着信トラフィックに適用されます。<br><br>**[デフォルトにリセット（Reset to Default）]** をクリックすると、MTU 値はデフォルト値の 1500 に設定されます。<br><br>（注）<br>MTU値は、指定された範囲内の偶数である必要があります。 |
| **[NetFlow の構成（NetFlow Configuration）]** | |

| フィールド | 説明 |
|---|---|
| **[Netflow の有効化（Enable NetFlow）]** | 灰色のボタンをクリックして、NetFlowを有効にします。ボタンが青色に変わり、右に移動します。<br>NetFlow の詳細については、NetFlow （116 ページ） を参照してください。<br>NetFlowパラメータを定義するには、次の構成を（指定された順序で） 完了してください。<br>• NetFlow のレコードの追加 （111 ページ）<br>• NetFlow のエクスポータの追加 （113 ページ）<br>• NetFlow のモニターの追加 （114 ページ）<br>NetFlow 設定を完了するには、NetFlow モニターを入力ポートに関連付けます。「入力ポートの追加 （119 ページ）」を参照してください。 |

**ステップ 5** [保存（Save）] をクリックします。

# NetFlow のレコードの追加

この手順を使用して、NetFlow レコードを作成します。

フロー レコードでは、パケットを識別するために NetFlow で使用するキーとともに、NetFlow がフローについて収集する関連フィールドを定義します。フロー レコードによってフロー用に収集するデータのサイズが決まります。キー フィールドは、*match* キーワードで指定されます。

## 手順

**ステップ 1** **[コンポーネント（Components）]** > **[グローバル構成（Global Configuration）]** に移動します。

**ステップ 2** 行の先頭にあるチェック ボックスをオンにしてデバイスを選択します。

**ステップ 3** **[アクション（Actions）]** ドロップダウン メニューから、**[グローバル構成の編集（Edit Global Configuration）]** を選択します。

**ステップ 4** **[グローバル構成の編集（Edit Global Configuration）]** ダイアログ ボックスで、灰色のボタンをクリックして **NetFlow を有効化**します。

**ステップ 5** **[レコードの追加（Add Record）]** をクリックして、次の詳細を入力します。

表 *31 :* レコードを追加

| フィールド | 説明 |
|---|---|
| **[名前（Name）]** | レコードの名前。 |
| **説明** | レコードの説明。 |
| **収集** | コレクション パラメータを定義します。<br>対応するチェックボックスをオンにして、次の 1 つ以上のパラメータに基づいたコレクションを有効にします。<br>• Counter Bytes<br>• Counter Packets<br>• IP バージョン（IP Version）<br>• Transport TCP Flags<br>• システム稼動開始時間<br>• システム稼動終了時間 |
| **アクションの** | 一致パラメータを定義します。<br>使用可能なオプションは、**レイヤ 2（Layer 2）**および**レイヤ 3/4（Layer 3/4）** です。いずれかをクリックして、一致パラメータを選択します。これらのパラメータについては、後の行で説明します。 |
| **レイヤ 2** | チェックボックスをオンにして、一致する 1 つ以上のレイヤ 2 パラメータを有効にします。<br>• 送信元 MAC アドレス<br>• 宛先 MAC アドレス<br>• Ethertype<br>• VLAN |

| フィールド | 説明 |
| --- | --- |
| **レイヤ 3/4** | チェックボックスをオンにして、一致する 1 つ以上のレイヤ 3 またはレイヤ 4 パラメータを有効にします。<br>• IPプロトコル<br>• IP TOS<br>• Transport Source Port<br>• Transport Destination Port<br>• IPv4 送信元アドレス<br>• IPv4 宛先アドレス<br>• 送信元 IPv6 アドレス<br>• 宛先 IPv6 アドレス<br>• IPv6 フロー ラベル<br>• IPv6 オプション |

**ステップ 6** **[レコードの追加（Add Record）]** をクリックします。

# NetFlow のエクスポータの追加

この手順に従って、NetFlowエクスポータを作成します。フローエクスポータの設定では、フローに対するエクスポートパラメータを定義し、リモートNetFlow Collectorへの到達可能性情報を指定します。

フローエクスポータでは、NetFlowエクスポートパケットに関して、ネットワーク層およびトランスポート層の詳細を指定します。

### 手順

**ステップ 1** **[コンポーネント（Components）]** > **[グローバル構成（Global Configuration）]** に移動します。

**ステップ 2** 行の先頭にあるチェック ボックスをオンにしてデバイスを選択します。

**ステップ 3** **[アクション（Actions）]** ドロップダウン メニューから、**[グローバル構成の編集（Edit Global Configuration）]** を選択します。

**ステップ 4** **[グローバル構成の編集（Edit Global Configuration）]** ダイアログ ボックスで、灰色のボタンをクリックして **NetFlow を有効化**します。

**ステップ 5** **[エクスポータを追加（Add Exporter）]** をクリックし、次の詳細を入力します。

表 *32 :* エクスポータの追加

| フィールド | 説明 |
|---|---|
| **[名前（Name）]** | エクスポータ名。 |
| **説明** | エクスポータの説明。 |
| **宛先（Destination）** | エクスポート先の IP アドレス。<br>対応するチェックボックスをオンにして、次のパラメータの 1 つ以上に基づいて収集を有効にします。 |
| **ソース（Source）** | 発信元の IP アドレス。<br>フローキャッシュが接続先に到達するために経由するデバイス上のインターフェイス。 |
| **UDP ポート** | NetFlow コレクタが NetFlow パケットをリスニングする UDP ポート。有効な範囲は 1 ～ 65535 です。 |
| **[DSCP]** | 差別化されたコード ポイント値。範囲は 0 ～ 63 です。 |
| **バージョン** | NetFlow のエクスポート バージョン。このフィールドは変更できません。<br>（注）<br>Cisco NX-OS は、バージョン 9 のエクスポート形式をサポートします。 |
| **[オプション エクスポータ（Option Exporter）]** | フローエクスポータ統計情報の再送信タイマー。値の範囲は 1 ～ 86400 秒です。 |
| **テンプレート データ タイムアウト** | テンプレートデータ再送信タイマーを設定します。値の範囲は 1 ～ 86400 秒です。 |

**ステップ 6** **[エクスポータを追加（Add Exporter）]** をクリックします。

# NetFlow のモニターの追加

この手順に従って、NetFlow モニターを作成します。

フロー モニタを作成して、フロー レコードおよびフロー エクスポータと関連付けることができます。1 つのモニタに属しているすべてのフローは、様々なフィールド上で照合するために関連するフロー レコードを使用します。データは指定されたフローエクスポータにエクスポートされます。

### 始める前に

次のように構成を行います。

- レコードの追加
- エクスポータの追加

### 手順

**ステップ 1** **[コンポーネント（Components）]** > **[グローバル構成（Global Configuration）]** に移動します。

**ステップ 2** 行の先頭にあるチェック ボックスをオンにしてデバイスを選択します。

**ステップ 3** **[アクション（Actions）]** ドロップダウン メニューから、**[グローバル構成の編集（Edit Global Configuration）]** を選択します。

**ステップ 4** **[グローバル構成の編集（Edit Global Configuration）]** ダイアログ ボックスで、灰色のボタンをクリックして **NetFlow を有効化**します。

**ステップ 5** **[モニターの追加（Add Monitor）]** をクリックし、次の詳細を入力します。

**表 *33* : モニタを追加**

| フィールド | 説明 |
|---|---|
| **[名前（Name）]** | モニターの名前。 |
| 説明 | モニターの説明。 |
| レコード | **[レコードの選択（Select Record）]** をクリックします。**[レコードの選択（Select Record）]** ウィンドウで、対応するラジオボタンをクリックしてレコードを選択します。選択したレコードの詳細が右側に表示されます。[選択（Select）] をクリックします。 |
| **[エクスポータ（Exporter）]** | **[エクスポータの選択（Select Exporter）]** をクリックします。**[エクスポータの選択（Select Exporter）]** ウィンドウで、対応するチェック ボックスをオンにしてエクスポータを選択します。選択したエクスポータの詳細が右側に表示されます。[選択（Select）] をクリックします。<br>（注）<br>モニターには最大 2 つのフロー エクスポータを選択できます |

**ステップ 6** **[モニターの追加（Add Monitor）]** をクリックします。

# 高精度時間プロトコル

PTP（Precision Time Protocol）デバイスには、通常のクロック、境界クロック、およびトランスペアレント クロックが含まれます。非 PTP デバイスには、通常のネットワーク スイッチやルータなどのインフラストラクチャ デバイスが含まれます。PTP システムは、PTP および非 PTP デバイスの組み合わせで構成できます。

PTPは、システムのリアルタイムPTPクロックが相互に同期する方法を指定する分散プロトコルです。これらのクロックは、グランドマスタークロック（階層の最上部にあるクロック）を持つマスター/メンバー同期階層に編成され、システム全体の時間基準を決定します。同期は、タイミング情報を使用して階層のマスターの時刻にクロックを調整するメンバーと、PTPタイミング メッセージを交換することによって実現されます。PTPは、PTP ドメインと呼ばれる論理範囲内で動作します。

PTPはネットワークに分散したノードの時刻同期プロトコルです。そのハードウェア タイムスタンプ機能は、優れた精度を提供します。

（注） PTP を設定すると、デフォルトの PTP 設定が、対応するデバイスのすべての ISL ポートと同期されます。

PTP の構成については、デバイスのグローバル構成の編集 （106 ページ） を参照してください。

# NetFlow

NetFlow は入力 IP パケットについてパケット フローを識別し、各パケット フローに基づいて統計情報を提供します。NetFlowのためにパケットやネットワーキング デバイスを変更する必要はありません。

Cisco Nexus 9300-FX プラットフォーム スイッチでは、フローをモニタするための十分な空き領域を確保するため、ing-netflow TCAM リージョンはデフォルトで 512 ずつに分割されます。さらに多くのスペースが必要な場合は、**hardware access-list tcam region ing-netflow size** コマンドを使用し、TCAM リージョンのサイズを 512 の倍数に変更します。

NetFlow は、次のプラットフォームでサポートされています。

- Cisco Nexus 9300 スイッチ — 9300-FX、FX2、EX
- Cisco Nexus 9500 スイッチ — 9500-FX、EX

NetFlow の構成については、デバイスのグローバル構成の編集 （106 ページ） を参照してください。

詳細については、『*Cisco Nexus 9000 Series NX-OS* システム管理構成ガイド』を参照してください。

# サンプリングされたフロー

NX-API の Nexus Dashboard Data Broker でサンプリングされた Flow（sFlow）を管理することができます。sFlow 使用すると、スイッチやルータを含むデータネットワーク内のリアルタイムトラフィックをモニターできます。sFlow では、トラフィックをモニタするためにスイッチとルータ上の sFlow エージェント ソフトウェアでサンプリング メカニズムを使用して、サンプル データを中央のデータ コレクタに転送します。

sFLow の構成については、デバイスのグローバル構成の編集（106 ページ） を参照してください。

# 入力ポート

**[入力ポート（Input Ports）]** タブには、NDB デバイスの入力ポートの詳細が表示されます。

Edge-SPAN、Edge-TAP、またはリモート ソース Edge-SPAN ポートが NX-API モードの構成で定義されている場合、**spanning-tree bpdufilter enable** コマンドはポートのインターフェイス モードで自動的に構成され、BPDU パケットをフィルタリングします。この構成は、すべての Cisco Nexus 3000 および 9000 シリーズ スイッチに適用されます。

Cisco Nexus シリーズ スイッチのすべてのスイッチ間ポートで **spanning-tree bpdufilter enable** コマンドを構成してください。

次の詳細を示す表が表示されます。

**表 *34 :* 入力ポート**

| 列名 | 説明 |
|---|---|
| **Device** | 入力ポートが構成されているデバイス。<br>このフィールドはハイパーリンクです。デバイス名をクリックすると、そのデバイスの詳細情報が表示されます。詳細と手順については、デバイス（37 ページ） の章を参照してください。 |
| **[ポート（Port）]** | 入力ポートとして構成されているデバイスのポート。<br>このフィールドはハイパーリンクです。**[ポート（Port）]**をクリックして、ポートの詳細を表示します。ここから実行できる追加のアクションは次のとおりです。<br>• *[入力ポートの編集（Editing an Input Port）]*<br>• 構成の削除：デバイスの入力ポートとしてのポートは削除されます。 |

| 列名 | 説明 |
|---|---|
| 使用中 | 緑色のチェック マークは、入力ポートが使用中であることを示します。 |
| 設定 | 入力ポートの構成情報（入力ポートの追加 （119 ページ） で設定されたパラメータに基づく）。 |
| タイプ | ポート タイプ。表示されるオプションは、次のとおりです。<br>• エッジ ポート：SPAN<br>• エッジポート：TAP<br>• リモート ソース エッジ：SPAN<br>• パケットの切り捨て |
| **[スパン接続先/タップ名（Span Destination/Tap Name）]** | 入力ポートに接続されているスパン先の詳細。<br>• ポートが実稼働スイッチに接続されている場合、*PS*、続いてデバイス ID、接続されたインターフェイスが表示されます。<br>• ポートが Cisco APIC/ または Cisco DNAC コントローラに接続されている場合、APIC については、DN 値がポッドとパスの詳細とともに表示されます。Cisco DNAC については、「*Cisco DNAC*」の後に Catalyst デバイス ID とインターフェイスが表示されます。<br>• ポートが Tap デバイスに接続されている場合、タップ構成名が表示されます。 |
| 作成者 | 入力ポートを作成したユーザー。 |
| 変更者 | 入力ポートを最後に変更したユーザー。 |

**[入力ポート（Input Ports）]** タブから、次のアクションを実行できます。

- **[入力ポートの追加（Add Input Port）]**：これを使用して、新しい入力ポートを追加します。このタスクの詳細については、入力ポートの追加 （119 ページ） を参照してください。
- **[入力ポートの削除（Delete Input Port）]**：行の先頭にあるチェック ボックスをオンにして、必要な入力ポートを選択します。**[アクション（Actions）]**>**[入力ポートの削除（Delete Input Port(s)）]** をクリックします。選択したポートが削除されます。

（注） 使用中の入力ポートは削除できません。

チェックボックスを選択せずに削除アクションを選ぶと、エラーが表示されます。デバイスを選択するように求められます。

# 入力ポートの追加

入力ポートを作成するには、この手順に従います。

デバイスの入力ポートは、トラフィックがパケット ブローカー ネットワークに入り、モニタリング ツールに送信されるポートです。

### 始める前に

1 つ以上のデバイスを追加します。

一部の入力ポート パラメータは、**[グローバル構成（Grobal Configuration）]** タブを使用してデバイス レベルで定義されます。これらのパラメータ（以下のリスト）を定義するには、グローバル構成の編集を参照してください。

- PTP
- Netflow
- MPLS フィルタリング
- Jumbo MTU

### 手順

**ステップ 1** **[コンポーネント（Components）]** > **[入力ポート構成（Input port Configuration）]** に移動します。

**ステップ 2** **[アクション（Actions）]** ドロップダウンリストで、**[入力ポートの追加（Add Input Port）]** を選択します。

**ステップ 3** **[入力ポートの追加（Add Input Port）]** ダイアログ ボックスで、次の詳細を入力します。

表 *35 :* 入力ポートの追加（***Add Input Port***）

| フィールド | 説明 |
|---|---|
| **[全般（General）]** | |

| フィールド | 説明 |
|---|---|
| デバイス | 入力ポートが構成されているデバイスを選択するには、次の手順に従います。<br>**[デバイスの選択（Select Device）]** をクリックします。**[デバイスの選択（Select Device）]** ウィンドウで、ラジオボタンを選択し、デバイスを選択します。[選択（Select）] をクリックします。 |
| **[ポート（Port(s)）]** | 入力ポートとして構成するポートを選択します。<br>**[ポートの選択（Select Port）]** をクリックします。**[ポートの選択（Select Port）]** ウィンドウで、必要なポートを選択します。[選択（Select）] をクリックします。 |
| **[ポート タイプ（Port Type）]** | ドロップダウンリストから選択して、入力ポートタイプを定義します。次のオプションがあります。<br>• **[エッジ ポート - SPAN（Edge Port - SPAN）]**：実稼働スイッチの構成済みセッションからの着信トラフィック用のエッジ ポートを作成します。<br>• **[エッジ ポート - TAP（Edge Port - TAP）]**：ISL 上の物理デバイスからの着信トラフィック用のエッジポートを作成します。<br>• **[リモート ソース エッジ ポート - SPAN（Remote Source Edge - SPAN）]**：実稼働スイッチの構成済みリモートセッションからの着信トラフィック用のエッジポートを作成します。 |
| ポートの説明 | ポートの説明を入力します。 |

| フィールド | 説明 |
| --- | --- |
| **VLAN（QinQ はサポートされていない）** | ポートは、実稼働 VLAN 情報を保持するために dot1q として設定されます。VLAN ID は、トラフィックの送信元のポートを識別するために使用されます。<br><br>Q-in-Q VLAN は、ISL 接続のすべての入力ポートで必須です。リリース 3.10.5 へのアップグレード後は、以前のリリースで作成された接続を使用できますが、以前に作成した接続のいずれかを変更/複製する必要がある場合は、Q-in-Q VLAN の追加が必須です。そうしないと、更新された接続に変更を保存できません。<br><br>（注）<br>インターフェイスに Q-in-Q を設定した後は、Q-in-Q 構成済みインターフェイスに VLAN フィルタを設定しないでください。<br><br>実稼働ポートは Q-in-Q で有効になっており、各実稼働ポートに一意の VLAN を割り当てる必要があります。この VLAN は、実稼働 VLAN 番号と重複しないようにする必要があります。 |
| **[ブロック送信（Block-Tx）]** | チェックボックスをオンにして、入力ポートから送信されているトラフィックをブロックします。<br><br>（注）<br>ユニキャストおよびマルチキャスト トラフィックのみがブロックされます。 |
| **ICMP v6 ネイバー請求をドロップ** | チェックボックスをオンにして、すべての ICMP トラフィックをドロップします。<br><br>デフォルトでは、Nexus 9300-EX および 9200 シリーズ スイッチの Edge-SPAN および Edge-TAP ポート タイプでは、すべての ICMP トラフィックがブロックされます。残りの Nexus 9000 シリーズ スイッチについては、ユーザーは ICMP トラフィックを拒否またはブロックする場合、この機能を手動で有効化しなければなりません。 |
| **IGMPv3 のブロック** | チェックボックスをオンにして、すべての IGMPv3 トラフィックをドロップします。<br><br>IGMPv3 トラフィックの拒否ルールが有効になっています。 |

| フィールド | 説明 |
|---|---|
| **[タイムスタンプ タギングの有効化（Enable Timestamp Tagging）]** | チェックボックスをオンにして、タイムスタンプ タグ付け機能を使用してパケットにタイムスタンプ タグを追加します。<br><br>Nexus 9300-EX および 9200 シリーズ スイッチの場合、この機能は Edge-SPAN および Edge-TAP ポートに適用されます。タイムスタンプ タギング機能を設定するには、デバイスで PTP 機能が有効になっていることを確認します。監視デバイスとエッジポートでタイムスタンプ タギングを有効にする必要があります。接続のいずれかの側、Edge-SPAN/Edge-TAP およびモニタリング デバイスでタイムスタンプ タギング機能が構成されていない場合、パケットはタイムスタンプでタギングされません。<br><br>（注）<br>グローバル設定を使用してデバイスで PTP が有効になっていない場合、このオプションはグレー表示されます。 |
| **[MPLS フィルタリングを有効にする（Enable MPLS Filtering）]** | チェックボックスをオンにし、MPLS フィルタ処理を有効にします。<br><br>（注）<br>グローバル設定を使用してデバイスに対して MPLS フィルタ処理が有効になっていない場合、このオプションはグレー表示されます。 |
| **[ジャンボ MTU を適用（Apply Jumbo MTU）]** | チェックボックスをオンにして、このポートで設定されたジャンボ MTU 値を有効にします。<br><br>（注）<br>グローバル構成を使用してデバイスにジャンボ MTU が構成されていない場合、このオプションはグレー表示されます。 |
| **[Netflow モニター（Netflow Monitor）]** | ドロップダウン リストからオプションを選択します。グローバル構成レベルで作成されたモニター名がここにリストされています。<br><br>（注）<br>グローバル設定を使用してデバイスに対して NetFlow が有効になっていない場合、このオプションはグレー表示されます。 |

各**[ポート タイプ（Port Type）]**に表示されるフィールドについては、以下で説明します。

a) （**ポート タイプ**：エッジ ポート-SPAN の場合のみ）次の詳細を入力します。

| フィールド | 説明 |
|---|---|
| 接続先デバイスのタイプ | これは、入力ポートの送信元（SPAN の接続先）です。<br>ドロップダウン リストから、必要なオプションを選択します。次のオプションがあります。<br>• コントローラ<br>• 実稼働スイッチ<br>上記のそれぞれのオプションについては、後続の行で説明します。 |
| コントローラ | **[コントローラの選択（Select Controller）]** をクリックします。**[(Cisco) ACI]** または **[(Cisco) DNAC]** を選択します。 |
| **[接続先デバイス タイプ（Destination Device Type）]**：**[コントローラ（Controller）] > [ACI]** のフィールド<br>インターフェイスの選択中に（以下で説明）、表示されるオプションに最新のポッド、ノード、およびそのインターフェイスが見つからない場合は、**[ファブリックの更新（Refresh Fabric）]** ボタンをクリックします。このアクションは、ACI ファブリックから最新のポッド、ノード、およびそのインターフェイスを取得します。<br>（注）<br>スパン先を設定する前に、APIC/ACI デバイスを追加する必要があります。 | |
| **[スパン先名（Span Destination Name）]** | スパン先の名前を入力します。 |
| ポッド | ポッドを選択します。 |
| ノード（Nodes） | ノードを選択します。 |
| **[ポート（Port）]** | ポートを選択します。 |
| **[MTU]** | APIC のスパン先の MTU 値を設定します。 |
| **[接続先デバイス タイプ（Destination Device Type）]** のフィールド：**[コントローラ（Controller）] > [(Cisco) DNAC]** | |
| **[スパン先名（Span Destination Name）]** | スパン先の名前を入力します。 |
| **[SPAN 接続先ポート（Span Destination Port）]** | **[SPAN 接続先ポート（Span Destination Port）]** をクリックし、Catalyst スイッチとポートを選択します。 |
| **[接続先デバイス タイプ]**：**[実稼働スイッチ]** のフィールド<br>（注）<br>SPAN 接続先を構成する前に、Nexus または Catalyst デバイスを追加する必要があります。 | |

| フィールド | 説明 |
|---|---|
| **[SPAN 先デバイス（Span Destination Device）]** | **[デバイスの選択（Select Device）]** をクリックし、デバイスを選択します。 |
| **[SPAN 先ポート（Span Destination Port）]** | **[ポートの選択（Select Port）]** をクリックして、ポートを選択します。 |

b) （**[ポート タイプ（Port Type）]** — エッジ ポート-TAP のみ）次の詳細を入力します。

| フィールド | 説明 |
|---|---|
| **[タップ構成名（Tap Configuration Name）]** | ドロップダウン リストからタップ構成を選択します。 |
| **[タップ構成タイプ（Tap Configuration Type）]** | タップデバイスからミラーリングされたトラフィックを受信する NDB デバイスのポートを選択します。<br>表示されるオプションは、選択した**[タップ構成名（Tap Configuration Name）]** の詳細に基づいています。Tap 構成中にミラー ポートのいずれかまたは両方をタップすることを選択した場合、対応する NDB エッジ ポート-タップ ポートが表示されます。 |

c) （**[ポート タイプ（Port Type）]**：リモート ソース エッジ-SPAN の場合のみ）次の詳細を入力します。

（注）
リモート送信元からのトラフィックを受信するために、最大 4 つのリモート送信元エッジ-SPAN ポートを構成できます。

| フィールド | 説明 |
|---|---|
| **[リモート入力終了セッション（Remote Input Termination Session）]** | |
| **[ERSPAN ID]** | ERSPAN ID を入力します。指定できる範囲は 1 ～ 1023 です。<br>ここで入力された ERSPAN ID は、リモート ソースのソース セッション ID と一致します。 |
| **[ループバック インターフェイスを使用（Use Loopback Interface）]** | チェックボックスをオンにして、ループバック インターフェイスを使用します。 |

| フィールド | 説明 |
|---|---|
| ループバック（Loopback） | **[ループバックの選択（Select Loopback）]** をクリックして、ループバック インターフェイスを選択します。構成されたループバック インターフェイスがない場合は、**[ループバックの追加（Add Loopback）]** をクリックします。ループバックの構成を参照してください。<br><br>ループバック インターフェイスを使用して、複数のリモート入力ポートを用意します。L3インターフェイスからのトラフィックは、ループバック インターフェイスに到達し、そこからセッションの接続先ポートに到達します。最初のリモート送信元エッジ スパン入力ポートをループバックで作成した場合、次のリモート送信元エッジ-SPAN ポートも同じループバック インターフェイスで構成する必要があります。最初のリモート送信元エッジ スパン入力ポートをループバックなしで作成した場合、次のリモート送信元エッジ SPAN ポートもループバック インターフェイスなしで構成する必要があります。 |
| **[セッション接続先（Session Destination）]** | **[接続先ポートの選択（Select Destination Port）]** をクリックして、接続先ポートを選択します（NDB デバイス上）。 |
| **[リモート入力セッション（Remote Input Session）]** | |
| **[リモート入力ポート（Remote Input Port）]** | **[リモート入力ポート（Remote Input Port）]** をクリックし、（NDB デバイス上の）リモート入力ポートを選択します。<br><br>（注）<br>リモート送信元エッジ-SPAN ポートに到達するトラフィック用に構成できるリモート入力ポートは 1 つだけです。ループバック インターフェイスを構成している場合、リモート入力ポートは、リモート送信元エッジ -SPAN ポートごとに異なる可能性があります。 |
| **IP アドレス** | IP アドレスを入力します。ここで入力する IP アドレスは、L3 ネットワーク経由でパケットが到達するリモート送信元ポートの IP アドレスです。<br><br>この値を入力する必要があるのは、最初のリモート送信元エッジ-SPAN ポートを構成する場合だけです。次の 3 つのポートを構成する際には、同じ IP アドレスがリモート送信元エッジ-SPAN ポートを持つ 4 つのセッションすべてに適用されるため、このフィールドはグレー表示されます。 |

| フィールド | 説明 |
|---|---|
| **[接続先デバイスのタイプ（Destination Device Type）]** | ドロップダウン リストから [デバイス タイプ（Device Type）] を選択します。<br>リモート送信元エッジ-SPAN ポートの場合、サポートされる接続先タイプは ACI です。 |
| **[スパン先 ACI ファブリック（Span Destination ACI Fabric）]** | [ACI ファブリックの選択] をクリックし、ACI ファブリックを選択します。 |
| スパン先名 | スパン先の名前を入力します。 |
| テナント | **[テナントの選択（Select Tenant）]** をクリックして、テナントを選択します。 |
| **[アプリケーション プロファイル（Application Profile）]** | **[アプリケーション プロファイルの選択（Select Application Profile ）]** をクリックして、アプリケーション プロファイルを選択します。 |
| **EPG** | **[EPG の選択]** をクリックして、EPG を選択します。 |
| 送信元 IP アドレス | 送信元 IP アドレスを入力します。この IP アドレスは、送信元パケットの IP サブネットのベース IP アドレスです。 |
| **[接続先 IP アドレス（Destination IP Address）]** | このフィールドには自動的に値が入力されます。<br>ここで入力される IP アドレスは、**[リモート入力ポート（Remote Input Port）]** の IP アドレスとして入力したものと同じアドレスです。<br>（注）<br>APIC/ACI デバイスの場合、これは接続先ポート（リモート入力ポート）であるため、接続先 IP と呼ばれます。 |
| **[フロー ID（ Flow ID）]** | このフィールドには自動的に値が入力されます。<br>フロー ID は、SPAN パケットのフロー ID です。これは、リモート ソース エッジ SPAN ポートに前に指定した ERSPAN ID と一致します。 |
| **TTL** | TTL 値を入力します。デフォルト値は 64 ホップです。 |
| **DSCP** | ドロップダウン リストから DSCP 値を選択します。 |
| **[MTU]** | スパン先ポートの MTU 値を入力します。範囲は 64 ～ 9216 です。 |

**ステップ 4** **[入力ポートの追加（Add Input Port）]** をクリックします。

## パケットの切り捨て

パケットの切り捨てでは、指定されたバイト位置から始まるパケットからバイトを破棄します。指定されたバイト位置以降のデータはすべて切り捨てられます。パケットの切り捨てが必要になるのは、目的の主な情報がパケットのヘッダーまたはパケットの最初の部分にある場合です。

（注） パケットの切り捨ては、ユニキャスト トラフィックでサポートされます（マルチキャスト トラフィックではサポートされません）。

表 *36* : パケット切り捨てのサポート

| EX シャーシ | FX シャーシ | Nexus 9364C、Nexus 9332C | Nexus 9336 C FX2 | -EX または -FX LC を備えた EOR スイッチ |
|---|---|---|---|---|
| MTU サイズの範囲は 320 ～ 1518 バイトです | MTU サイズの範囲は 64 ～ 1518 バイトです | MTU サイズの範囲は 64 ～ 1518 バイトです | MTU サイズの範囲は 64 ～ 1518 バイトです | LC に依存します |

# ループバックの構成

この手順を使用して、リモート ソース エッジ スパン入力ポートのループバックを設定します。

手順

**ステップ 1** **[入力ポート（Input Ports）]** > **[アクション（Actions）]** > **[入力ポートの追加（And Input Ports）]** に移動します。

**ステップ 2** **[ポート タイプ（Port Type）]** を [リモート ソース エッジ スパン ポート（Remote Source Edge Span Port）] として選択し、**[ループバック インターフェイスの使用（Use Loopback Interface）]** チェックボックスをオンにして、ループバック インターフェイスを選択します。

**ステップ 3** **[ループバックの構成（Configure Loopback）]** をクリックして、新しいループバック インターフェイスを作成します。

**[ループバックの構成（Configure Loopback）]** ダイアログ ボックスで、次の詳細を入力します。

表 *37* : ループバックの構成

| フィールド | 説明 |
|---|---|
| 全般 | |
| **ループバックID** | ループバック ID を入力します。 |
| **IP アドレス** | ループバック IP アドレスを入力します。 |

ステップ **4** **[ループバックの構成（Configure Loopback）]** をクリックします。

# モニタリングツール

**[モニタリング ツール]** タブには、NDB デバイスのモニタリング ツール ポートの詳細が表示されます。NDB デバイスのモニタリング ツール ポートからのトラフィックは、モニタリング ツールに送信されます。

次の詳細を示す表が表示されます。

表 *38* : モニタリングツール

| 列名 | 説明 |
|---|---|
| **Status** | ステータスは、2つの列を使用して定義されます。<br>最初の列は、モニタリングツールのトラフィックを示しています。<br>• 緑：モニタリング ツールが現在トラフィックを伝送していることを示します。<br>• 黄：モニタリング ツールが現在トラフィックを伝送していないことを示します。<br>2 番目の列は、モニタリング ツール ポートとモニタリング ツール間のリンクの状態を示します。モニタリング ツール ポートとモニタリング ツール間のリンクが稼働している場合、色は緑色です。<br>• 緑：リンクが起動して動作していることを示します。<br>• 赤：リンクがダウンしていることを示します。<br>• 黄：リンクが管理上ダウンしていることを示します。 |
| **[モニタリング ツール（Monitoring Tool）]** | モニタリング ツール名。<br>このフィールドはハイパーリンクです。**モニタリング ツール**の名前をクリックします。右側に新しいペインが表示され、モニタリングツールに関する詳細が表示されます。次の追加アクションがここで実行できます。<br>• モニタリング ツールの編集（135 ページ） |
| **ポート** | モニタリングツールのポート（デバイスに接続）。<br>ポートの詳細を表示するには、**[ポート（Port）]**の名前をクリックします。次の追加アクションがここで実行できます。<br>• モニタリング ツールの編集（135 ページ） |

| 列名 | 説明 |
|---|---|
| **[タイプ（Type）]** | モニタリング ツールのタイプ。次のオプションがあります。<br>• [ローカル モニタリング ツール（Local Monitoring Tool）]：ローカル ネットワークの NDB デバイス上にあるポート（L2 ポート）。<br>• [リモート モニタリング ツール（Remote Monitoring Tool）]：ローカル ネットワークの外部にあり、L3 ネットワーク経由で到達可能なポート。 |
| **使用中** | モニタリング ツール ポートが使用されている場合は、緑色のチェック マークが表示されます。それ以外の場合は空白のままです。 |
| **[パケットの切り捨て（Packet Truncation）]** | モニタリング ツール ポートでパケットの切り捨てが有効になっている場合は、緑色のチェック マークが表示されます。それ以外の場合は空白のままです。 |
| **ブロック受信** | モニタリング ツールからモニタリング ツール ポート（NDB デバイス上）への着信トラフィックがブロックされている場合、**[はい（Yes）]** と表示されます。 |
| **作成者** | モニタリング ツールを作成したユーザー。 |
| **最終更新者** | モニタリング ツールを最後に変更したユーザー。 |
| **ステータスの説明** | モニタリング ツールの現在のステータス。ステータスの説明は、最新ステータスに基づく自動更新を行います。<br>また、  の *[更新（Refresh）]* をクリックして、最新ステータスを取得できます。 |

**[モニタリング ツール（Monitoring Tools）]** タブから、次のアクションを実行できます。

- **[モニタリング ツールの追加（Add Monitoring Tool）]**：これを使用して、新しい監視デバイスを追加します。このタスクの詳細については、モニタリング ツールの追加を参照してください。

- **[モニタリング ツールの削除（Delete Monitoring Tool(s)）]**：行の先頭にあるチェックボックスをオンにして、必要なデバイスを選択します。選択したデバイスが削除されます。**[アクション（Actions）] > [モニタリング ツールの削除（Delete Monitoring Tool(s)）]** をクリックします。チェックボックスを選択せずに削除アクションを選ぶと、エラーが表示されます。デバイスを選択するように求められます。

（注） 使用中のモニタリング ツールは削除できません。

# モニタリング ツールの追加

この手順を使用して、モニタリング ツール ポートを追加します。次のものを作成できます。

- ローカル モニタリング ツール - ローカル ネットワークの NDB デバイス上にあるポート（L2 ポート）。
- リモート モニタリング ツール - ローカル ネットワークの外部にあり、L3 ネットワーク経由で到達可能なポート。

パケットの出力ポートであるモニタリング ツールに関連付けるパケット切り捨てポート（入力トラフィックをブロックするために使用）を作成できます。

### 始める前に

**制約事項**：

- 接続ごとに、スイッチごとに複数のリモート配信ポートを使用することはできません。
- インタースイッチド リンクを含むリモート モニタリング ツールは、ISL ごとに 1 つの接続のみに制限されます。
- モニタリングツールをパケット切り捨てインターフェイスで使用する場合は、パケット切り捨てポートのステータスが管理上アップ状態（緑色のアイコン）であり、リンクのもう一方の端がどの NDB デバイスにも接続されていないことを確認します。ポートのレイヤ 2 ステータスをアップに変更するには、別の非NDBデバイスに接続して、サードパーティのループバック光ファイバを使用してループバックを作成する必要があります。

（注） スイッチ上でパケットの切り捨てを使用して、最大 4 つのモニタリング ツールを設定できます。

### 手順

**ステップ 1** **[コンポーネント（Components）] > [モニタリング ツール（Monitoring Tools）]** に移動します。

**ステップ 2** **[アクション（Actions）]** ドロップダウンリストで、**[モニタリング ツールの追加（Add Monitoring Tool）]** を選択します。

**ステップ 3** **[モニタリング ツールの追加（Add Monitoring Tool）]** ダイアログ ボックスで、次の詳細を入力します。

表 *39* : モニタリング ツールの追加

| フィールド | 説明 |
|---|---|
| **[全般（General）]** | |
| モニタリング ツール名 | モニタリングツールの名前を入力します。 |
| デバイス名（**Device Name**） | **[デバイスの選択（Select Device）]** をクリックします。表示されたデバイス一覧から、ラジオボタンでデバイスを選択します。デバイスの詳細が右側に表示されます。<br>モニタリング ツールのポートはこのデバイスにあります。<br>**[デバイスの選択（Select Device）]** をクリックします。 |
| **[ポート（Port）]** | **[ポートの選択（Select Port）]** をクリックします。開いた **[インターフェイスの選択（Select Interface）]** ウィンドウで、ラジオボタンを使用してポートを選択します。表示されるインターフェースは、選択したデバイスによって異なります。<br>[選択（Select）] をクリックします。<br>選択したポートはモニタリング ツール ポートとしてマークされます。トラフィックはここからモニタリング ツールにリダイレクトされます。 |
| **[ポートの説明（Port Description）]** | ポートの説明を入力します。 |

| フィールド | 説明 |
|---|---|
| **[ローカル監視ツール（Local Monitor Tool）]** | ラジオ ボタンを選択して、ローカル モニター デバイスを選択します。このオプションを選択すると、モニタリング デバイスはローカル ネットワークからのものになります。<br>ローカル モニター デバイスには次のオプションが表示されます（以下の行で詳しく説明します）。<br>• [受信のブロック（Block Rx）]<br>• [ICMPv6 ネイバー勧誘をブロック（Block ICMPv6 Neighbour Solicitation）]<br>• [タイムスタンプ タギングの有効化（Enable Timestamp Tagging）]<br>• パケットの切り捨て<br>• [タイムスタンプ ストリップの有効化（Enable Timestamp Strip）]<br>• [ジャンボ MTU を適用（Apply Jumbo MTU）] |
| **[受信のブロック（Block Rx）]** | モニタリング ツールから（NDB デバイスのモニタリング ツール ポートへの）トラフィックをブロックします。このオプションは、デフォルトで選択されます。チェックボックスをオフにすると、このオプションをオフにできます。<br>（注）<br>Rx トラフィックは、N9K-X97160YC-EX ライン カード（NX-OS 9.3(3) 以降）を搭載した Cisco N9K-95xx スイッチの単方向イーサネットを使用してブロックされます。 |
| **[ICMPv6 ネイバー勧誘をブロック（Block ICMPv6 Neighbour Solicitation）]** | モニタリング ツールから（NDB デバイスのモニタリング ツール ポートへの）ICMP トラフィックをブロックします。このオプションは、デフォルトで選択されます。チェックボックスをオフにすると、このオプションをオフにできます。<br>Nexus 9300-EX および 9200 スイッチでサポートされます。残りの Nexus 9000 シリーズ スイッチについて、ユーザーは ICMP トラフィックを拒否またはブロックするために、この機能を手動で有効化しなければなりません。 |
| **IGMPv3 のブロック** | チェックボックスをオンにして、すべての IGMPv3 トラフィックをドロップします。<br>IGMPv3 トラフィックの拒否ルールが有効です。 |

| フィールド | 説明 |
|---|---|
| **[タイムスタンプ タギングの有効化（Enable Timestamp Tagging）]** | チェックボックスをオンにして、タイムスタンプのタグ付けを有効にします。モニタリング ツール ポートのすべての発信パケットにタイムスタンプ タグが付加されます。<br>単一のデバイスまたは複数のデバイスで、この機能を構成できます。<br>タイムスタンプ タギングを構成するために、デバイスで PTP が有効になっていることを確認します。モニタリング デバイスとエッジ ポートでタイムスタンプのタグ付けを有効にする必要があります。タイムスタンプのタグ付けが接続、つまり Edge-SPAN/Edge-TAP とモニタリング ツールのいずれかの側で構成されていない場合、パケットのタイムスタンプによるタグ付けは行われません。 |
| **[パケットの切り捨て（Packet Truncation）]** | チェックボックスをオンにしてパケットの切り捨てを有効にし、MTU サイズを入力します。<br>パケットの切り捨ては、MTU サイズに基づいて着信パケットからバイトを破棄します。これは、必要なトラフィックのみをモニタリング ツールのポートに送信するために行われます。これは、トラフィックを入力ポートからパケット切り捨てポートにリダイレクトすることによって実現されます。パケット チューニング ポートからの切り捨てられたパケットは、モニタリング ツールに到達します。<br>パケット切り捨てポートを設定するには、**[パケット切り捨てポートの選択（Select Packet Truncation Port）]** をクリックします。「切り捨てポートの追加」手順を参照してください。 |
| **[タイムスタンプ ストリップの有効化（Enable Timestamp Strip）]** | チェックボックスをオンにして、タイムスタンプ ストリップを有効にします。これにより、送信元のパケットからタイムスタンプ タグが削除されます。 |
| **[ジャンボ MTU を適用（Apply Jumbo MTU）]** | チェックボックスをオンにして、ジャンボ MTU を有効にします。<br>ジャンボ MTU は、デバイスにより大きなパケット サイズを設定します。**[ジャンボ MTU（Jumbo MTU）]** を **[グローバル構成（Global Configuration）]** で有効にして、デバイスのポートにジャンボ MTU のサイズを適用します。 |

| フィールド | 説明 |
|---|---|
| **[リモート モニタリング ツール（Remote Monitoring Tool）]** | ラジオ ボタンを選択して、リモート モニター デバイスを選択します。このオプションを選択すると、リモート ネットワークからのモニタリング デバイスが有効になります。<br>リモート モニター デバイスには、次のオプションが表示されます（以下の行で詳しく説明します）。<br>• 受信のブロック<br>• インターフェイスIP<br>• 宛先 IP（Destination IP）<br>• ERSPAN ID |
| **インターフェイスIP** | モニタリング ツール ポートに割り当てられる IP アドレス。 |
| Destination IP | ERSPAN が終端し、選択したポートから到達可能になる IP アドレス。 |
| **ERSPAN ID** | ERSPAN ID を入力します。範囲は 1 ～ 1023 です。<br>Cisco Nexus 9300 FX および EX シリーズ スイッチのカプセル化リモート スイッチ ポート アナライザ（ERSPAN）送信元セッション機能を使用して、ネットワーク外のデバイスをモニタリング デバイスとして使用できます。 |

**ステップ 4** **[モニタリング ツールの追加（Add Monitoring）]** をクリックします。

# モニタリング ツールの編集

この手順を使用して、モニタリング ツールのパラメータを編集します。

### 始める前に

1 つ以上のモニタリング ツールを追加します。

### 手順

**ステップ 1** **[コンポーネント（Components）]** > **[モニタリング ツール（Monitoring Tools）]** に移動します。

**ステップ 2** 表示された表で、**監視ツール**の名前をクリックします。

新しいペインは右側に表示されます。

**ステップ 3** **[アクション（Actions）]** をクリックし、**[編集（Edit）]** を選択します。

**ステップ 4** **[モニタリング ツールの編集（Edit Monitoring Tool）]** ダイアログボックスには、モニタリング ツールの最新の情報が表示されます。これらのフィールドを必要に応じて変更します。

**表 *40* : モニタリング ツールの編集**

| フィールド | 説明 |
|---|---|
| **[全般（General）]** | |
| **モニタリング ツール名** | モニタリング ツール名が表示されます。これは編集できません。 |
| **デバイス名（Device Name）** | モニタリング ツール ポートが存在するデバイス。 |
| **[ポート（Port）]** | モニタリング ツールのポート。 |
| **[ポートの説明（Port Description）]** | ポートの説明を入力します。 |
| **[ローカル監視ツール（Local Monitor Tool）]** | ラジオ ボタンを選択して、ローカル モニター デバイスを選択します。このオプションを選択すると、モニタリング デバイスはローカル ネットワークからのものになります。<br>ローカル モニター デバイスには次のオプションが表示されます（以下の行で詳しく説明します）。<br>• [受信のブロック（Block Rx）]<br>• [ICMPv6 ネイバー勧誘をブロック（Block ICMPv6 Neighbour Solicitation）]<br>• [タイムスタンプ タギングの有効化（Enable Timestamp Tagging）]<br>• パケットの切り捨て<br>• [タイムスタンプ ストリップの有効化（Enable Timestamp Strip）]<br>• [ジャンボ MTU を適用（Apply Jumbo MTU）] |
| **[受信のブロック（Block Rx）]** | モニタリング ツールから（NDB デバイスのモニタリング ツール ポートへの）トラフィックをブロックします。このオプションは、デフォルトで選択されます。チェックボックスをオフにすると、このオプションをオフにできます。<br>（注）<br>Rx トラフィックは、N9K-X97160YC-EX ライン カード（NX-OS 9.3(3) 以降）を搭載した Cisco N9K-95xx スイッチの単方向イーサネットを使用してブロックされます。 |

| フィールド | 説明 |
| --- | --- |
| **[ICMPv6 ネイバー勧誘をブロック（Block ICMPv6 Neighbour Solicitation）]** | モニタリング ツールから（NDB デバイスのモニタリング ツール ポートへの）ICMP トラフィックをブロックします。このオプションは、デフォルトで選択されます。チェックボックスをオフにすると、このオプションをオフにできます。<br><br>Nexus 9300-EX および 9200 スイッチでサポートされます。残りの Nexus 9000 シリーズ スイッチについて、ユーザーは ICMP トラフィックを拒否またはブロックするために、この機能を手動で有効化しなければなりません。 |
| **[タイムスタンプ タギングの有効化（Enable Timestamp Tagging）]** | チェックボックスをオンにして、タイムスタンプのタグ付けを有効にします。モニタリング ツール ポートのすべての発信パケットにタイムスタンプ タグが付加されます。<br><br>単一のデバイスまたは複数のデバイスで、この機能を構成できます。<br><br>タイムスタンプ タギングを構成するために、デバイスで PTP が有効になっていることを確認します。モニタリング デバイスとエッジポートでタイムスタンプのタグ付けを有効にする必要があります。タイムスタンプのタグ付けが接続、つまり Edge-SPAN/Edge-TAP とモニタリング ツールのいずれかの側で構成されていない場合、パケットのタイムスタンプによるタグ付けは行われません。 |
| **[パケットの切り捨て（Packet Truncation）]** | チェックボックスをオンにしてパケットの切り捨てを有効にし、MTU サイズを入力します。モニタリング ツールの追加時にパケット切り捨てポートが構成されていない場合、**[パケット切り捨てポートの選択（Select Packet Truncation Port）]** は無効になります。 |
| **[タイムスタンプ ストリップの有効化（Enable Timestamp Strip）]** | チェックボックスをオンにして、タイムスタンプ ストリップを有効にします。これにより、送信元のパケットからタイムスタンプ タグが削除されます。 |
| **[ジャンボ MTU を適用（Apply Jumbo MTU）]** | チェックボックスをオンにして、ジャンボ MTU を有効にします。<br><br>ジャンボ MTU は、デバイスにより大きなパケット サイズを設定します。**[ジャンボ MTU（Jumbo MTU）]** を **[グローバル構成（Global Configuration）]** で有効にして、デバイスのポートにジャンボ MTU のサイズを適用します。 |

| フィールド | 説明 |
|---|---|
| **[リモート モニタリング ツール（Remote Monitoring Tool）]** | ラジオ ボタンを選択して、リモート モニター デバイスを選択します。このオプションを選択すると、リモート ネットワークからのモニタリング デバイスが有効になります。<br>リモート モニター デバイスには、次のオプションが表示されます（以下の行で詳しく説明します）。<br>• 受信のブロック<br>• インターフェイスIP<br>• 宛先 IP（Destination IP）<br>• ERSPAN ID |
| **インターフェイスIP** | モニタリング ツール ポートに割り当てられる IP アドレス。 |
| Destination IP | ERSPAN が終端し、選択したポートから到達可能になる IP アドレス。 |
| **ERSPAN ID** | ERSPAN ID を入力します。範囲は 1 ～ 1023 です。<br>Cisco Nexus 9300 FX および EX シリーズ スイッチのカプセル化リモート スイッチ ポート アナライザ（ERSPAN）送信元セッション機能を使用して、ネットワーク外のデバイスをモニタリング デバイスとして使用できます。 |

**ステップ 5** **[保存（Save）]** をクリックします。

# ポート グループ

**[ポート グループ（Port Groups）]** タブには次のサブタブがあります。

- **[入力ポート グループ（Input Port Group）]**：デバイスの（または複数デバイスの）入力ポートがグループ化されて、入力ポート グループを形成します。詳細については、入力ポート グループを参照してください。
- **[モニタリング ツール グループ（Monitoring Tool Group）]**：デバイスの（または複数デバイスの）モニタリング ツール ポートがグループ化されて、モニタリング ツール グループが形成されます。詳細については、モニタリング ツール グループを参照してください。

# 入力ポート グループ

デバイス（または複数のさまざまなデバイス）の入力ポートがグループ化されて、ポート グループが形成されます。ポート グループは、さまざまなデバイスのエッジスパン ポートとエッジタップ ポートの組み合わせにすることができます。グループ化することで、接続の作成中、入力ポートを個別に選択する代わりに、複数の入力ポートを同時に選択できます。

次の詳細の表が表示されます。

**表 *41* : 入力ポート グループ**

| 列名 | 説明 |
|---|---|
| **[入力ポート グループ名（Input Port Group Name）]** | 入力ポートのグループ名。<br>このフィールドはハイパーリンクです。**[入力ポート グループ名（Input Port Group Name）]** をクリックします。入力ポート グループに関する詳細情報を提供する新しいペインが右側に表示されます。ここから実行できる追加のタスクは次のとおりです。<br>• [入力ポート グループの編集（Edit Input Port Group）] |
| **説明** | 入力ポート グループの説明。 |
| **[関連する接続（Associated Connections）]** | グループに関連付けられた接続。 |
| **[メンバー（Member(s)）]** | グループのメンバー入力ポートの数。 |
| **[作成者（Created By）]** | グループを作成したユーザー。 |
| **[最終修正者（Last Modified By）]** | グループを最後に変更したユーザ。 |

**[入力ポート グループ（Input Port Group）]** タブから、次のアクションを実行できます。

- **[入力ポート グループの追加（Add Input Port Group）]**：これを使用して、新しい入力ポート グループを追加します。このタスクの詳細については、入力ポート グループの追加を参照してください。
- **[入力ポート グループの削除（Delete Input Port Group(s)）]**：行の先頭にあるチェックボックスをオンにして、削除する入力ポート グループを選択し、**[アクション（Actions）]** > **[入力ポート グループの削除（Delete Input Port Group）]** をクリックします。選択した入力ポートグループが削除されます。チェックボックスを選択せずに削除アクションを選ぶと、エラーが表示されます。入力ポート グループを選択するよう求められます。

# 入力ポート グループの追加

この手順を使用して、入力ポート グループを作成します。

接続の作成中に、入力ポートを個別に選択する代わりに、グループ化することで複数の入力ポートを同時に選択できます。

### 始める前に

1 つ以上のデバイスを作成します。

### 手順

**ステップ 1** **[コンポーネント]** > **[ポート グループ]** > **[入力ポート グループ]** に移動します。

**ステップ 2** **[アクション（Actions）]** ドロップダウンリストで、**[入力ポートの追加（Add Input Port）]** を選択します。

**ステップ 3** **[入力ポート グループの追加（Add Input Port Group）]** ダイアログ ボックスで、次の詳細を入力します。

表 *42 : [*入力ポート グループの追加（***Add Input Port Group***）*]*

| フィールド | 説明 |
|---|---|
| **[全般（General）]** | |
| グループ名 | 入力ポート グループの名前を入力します。 |
| 説明 | グループの説明を入力します。 |
| ノードの選択（**Select Node**） | *[*すべてのノード（*All Nodes*）*]* ボックスで、ラジオ ボタンをクリックしてデバイスを選択します。 |
| **[ポートの選択（Choose Port(s)）]** | 入力ポートとして構成されているポートが表示されます。ポートをクリックして選択します。**[すべて追加（Add All）]** をクリックして、デバイスのすべての（入力）ポートを選択できます。 |
| **[選択したポート（Selected Port(s)）]** | 選択したポートがここに入力されます。これらは、グループの一部となるポートです。ポートを削除する場合は、ポートの横に表示されている×印をクリックします。**[すべて削除（Remove All）]** をクリックして、選択したすべてのポートを削除できます。 |

**ステップ 4** **[入力ポート グループの追加（Add Input Port Group）]** をクリックします。

# 入力ポート グループの編集

この手順に従って、入力ポート グループのパラメータを編集します。

### 始める前に

1 つ以上の入力ポート グループを作成します。

### 手順

**ステップ 1** **[コンポーネント（Components）]** > **[ポート グループ（Port Groups）]** > **[入力ポート グループ（Input Port Group）]** に移動します。

**ステップ 2** 表示された表で、**入力ポート グループ**名をクリックします。

新しいペインが右側に表示されます。

**ステップ 3** **[アクション（Actions）]** をクリックし、**[入力ポート グループの編集（Edit Input Port Group）]** を選択します。

**ステップ 4** [入力ポート グループの編集] ダイアログ ボックスに、グループの現在の情報が表示されます。これらのフィールドを必要に応じて変更します。

**表 *43 :* 入力ポート グループの編集**

| フィールド | 説明 |
|---|---|
| **[全般（General）]** | |
| グループ名 | 入力ポート グループ名。 |
| 説明 | グループの説明です。 |
| ノードの選択（Select Node） | *[*すべてのノード（*All Nodes*）*]* ボックスで、ラジオ ボタンをクリックしてデバイスを選択します。 |
| **[ポートの選択（Choose Port(s)）]** | 入力ポートとして構成されているポートが表示されます。ポートをクリックして選択します。**[すべて追加（Add All）]** をクリックして、デバイスのすべてのポートを選択できます。 |
| **[選択したポート（Selected Port(s)）]** | 選択したポートがここに入力されます。これらは、グループの一部となるポートです。ポートを削除する場合は、ポートの横に表示されている×印をクリックします。**[すべて削除（Remove All）]** をクリックして、選択したすべてのポートを削除できます。 |

**ステップ 5** **[保存（Save）]** をクリックします。

# モニタリング ツール グループ

デバイス間でグループ化されたモニタリング ツール ポートは、モニタリング ツール グループを形成します。

次の詳細の表が表示されます。

**表 *44 :*** モニタリング ツール グループ

| 列名 | 説明 |
|---|---|
| **[モニタリング ツール グループ名（Monitoring Tool Group Name）]** | モニタリング ツール グループの名前。<br>このフィールドはハイパーリンクです。**モニタリング ツール グループ**の名前をクリックします。右側に新しいペインが表示され、モニタリング ツール グループに関する詳細情報が提供されます。ここから実行できる追加のタスクは次のとおりです。<br>• モニタリング ツール グループの編集 |
| **説明** | モニタリング ツール グループの説明。 |
| **[関連する接続（Associated Connections）]** | モニタリング ツール グループを利用する接続。 |
| **[メンバー（Member(s)）]** | グループのメンバー モニタリング ツール ポートの数。 |
| **[作成者（Created By）]** | グループを作成したユーザー。 |
| **[最終修正者（Last Modified By）]** | グループを最後に変更したユーザ。 |

**[モニタリング ツール グループ（Monitoring Tool Group）]** タブから、次のアクションを実行できます。

- モニタリング ツール グループの追加 — これを使用して、新しいモニタリング ツール グループを追加します。このタスクの詳細については、モニタリング ツール グループの追加を参照してください。
- **[モニタリング ツール グループの削除（Delete Monitoring Tool Group(s)）]**：行の先頭にあるチェックボックスをオンにして、削除するツール グループを選択し、**[アクション（Action）]** > **[モニタリング ツール グループの削除（Delete Monitoring Tool Group(s)）]** をクリックします。選択したツール グループが削除されます。チェックボックスを選択せずに削除アクションを選ぶと、エラーが表示されます。ツール グループを選択するように求められます。

# モニタリング ツール グループの追加

この手順に従って、モニタリング ツール グループを作成します。

### 始める前に

1 つ以上のモニタリング ツールを作成します。

### 手順

**ステップ 1** **[コンポーネント（Components）]** > **[ポート グループ（Port Groups）]** > **[モニタリング ツール グループ（Monitoring Tool Group）]** に移動します。

**ステップ 2** **[アクション（Actions）]** ドロップダウンリストで、**[モニタリング ツール グループの追加（Add Monitoring Tool Group）]** を選択します。

**ステップ 3** **[モニタリング ツール グループの追加（Add Monitoring Tool Group）]** ダイアログ ボックスで、次の詳細を入力します。

**表 *45* : モニタリング ツール グループの追加**

| フィールド | 説明 |
|---|---|
| **[全般（General）]** | |
| グループ名 | モニタリング ツール グループの名前を入力します。 |
| 説明 | グループの説明を入力します。 |
| ノードの選択（**Select Node**） | *[*すべてのノード（*All Nodes*）*]* ボックスで、ラジオ ボタンをクリックしてデバイスを選択します。 |
| **[ポートの選択（Choose Port(s)）]** | モニタリング ツールのポートとして設定されているポートが表示されます。ポートをクリックして、選択します。**[すべて追加（Add All）]** をクリックして、デバイスのすべての（モニタリング）ポートを選択できます。 |
| **[選択したポート（Selected Port(s)）]** | 選択したポートがここに入力されます。これらは、グループの一部となるポートです。ポートを削除する場合は、ポートの横に表示されている×印をクリックします。**[すべて削除（Remove All）]** をクリックして、選択したすべてのポートを削除できます。 |

**ステップ 4** **[モニタリング ツール グループの追加（Add Monitoring Tool Group）]** をクリックします。

# モニタリング ツール グループの編集

この手順を使用して、モニタリング ツール グループのパラメータを編集します。

### 始める前に

1 つ以上のモニタリング ツール グループを作成します。

### 手順

**ステップ 1** **[コンポーネント]** > **[ポート グループ]** > **[モニタリング ツール グループ]** に移動します。

**ステップ 2** 表示された表で、**モニタリング ツール グループ**の名前をクリックします。

新しいペインが右側に表示されます。

**ステップ 3** **[アクション（Actions）]** をクリックし、**[モニタリング ツール グループの編集（Edit Monitoring Tool Group）]** を選択します。

**ステップ 4** **[モニタリング ツールグループの編集（Edit Monitoring Tool Group）]** ダイアログボックスに、現在のグループの情報が表示されます。これらのフィールドを必要に応じて変更します。

表 *46 : [*モニタリング ツールグループの編集（***Edit Monitoring Tool Group***）*]*

| フィールド | 説明 |
|---|---|
| **[全般（General）]** | |
| グループ名 | モニタリング ツール グループの名前。 |
| 説明 | グループの説明。 |
| ノードの選択（**Select Node**） | *[*すべてのノード（*All Nodes*）*]* ボックスで、ラジオ ボタンをクリックしてデバイスを選択します。 |
| **[ポートの選択（Choose Port(s)）]** | モニタリング ツールのポートとして設定されているポートが表示されます。ポートをクリックして、選択します。**[すべて追加（Add All）]** をクリックして、デバイスのすべての（モニタリング）ポートを選択できます。 |
| **[選択したポート（Selected Port(s)）]** | 選択したポートがここに入力されます。これらは、グループの一部となるポートです。ポートを削除する場合は、ポートの横に表示されている×印をクリックします。**[すべて削除（Remove All）]** をクリックして、選択したすべてのポートを削除できます。 |

**ステップ 5** [保存（Save）] をクリックします。

# スパン接続先

**[スパン接続先（Span Destination）]** タブには、NDB デバイスの入力ポートに接続されているスパン ポートの詳細が表示されます。スパン接続先は、入力ポートのトラフィック ソース（ACI または NX-OS デバイスから）です。L2 スパン接続先（ローカル）はエッジ スパン ポートに作成され、L3 スパン接続先（リモート）はリモート エッジ スパン ポートに作成されます。

次の詳細の表が表示されます。

**表 *47 : [スパン接続先（Span Destination）]***

| 列名 | 説明 |
|---|---|
| 名前 | スパン接続先ポートの名前。 |
| 接続先（Destinations） | スパン接続先が Cisco ACI/APIC 上にあるかどうかを示します。 |
| [入力ポート（Input Port）] | スパン接続先に接続されている NDB デバイスの入力ポート。 |
| 入力タイプ タイプ | 入力ポート タイプ。次のオプションがあります。<br>• エッジ SPAN ポート<br>• リモート送信元のエッジ-SPAN ポート |
| [スパン デバイス（Span Device）] | スパン デバイス（トラフィック送信元）。次のオプションがあります。<br>• Cisco ACI APIC<br>• Nexus スイッチ（実稼働スイッチ） |
| 作成者 | スパン接続先を作成したユーザー。 |
| [最終更新者（Last Modified By）] | スパン接続先を最後に変更したユーザー。 |
| ステータスの説明 | スパン接続先の現在のステータス。ステータスの説明は、最新ステータスに基づく自動更新を行います。<br>また、  の *[更新（Refresh）]* をクリックして、最新ステータスを取得できます。 |

**[スパン接続先（Span Destinations）]** タブから、次のアクションを実行できます。

- **[スパン接続先の削除（Delete Span Destinations）]**：行の先頭にあるチェックボックスをオンにして、削除するスパン先を選択し、**[アクション（Actions）]** > **[スパン接続先の削除（Delete Span Destinations）]** をクリックします。選択したスパン接続先が削除されます。チェックボックスを選択せずに削除アクションを選ぶと、エラーが表示されます。スパン接続先を選択するよう求められます。

（注） スパン接続先の追加については、入力ポートの追加 （119ページ）の手順を参照してください。スパン接続先（ACI/NX-OS デバイス上）は、NDB デバイスの入力ポートに接続されます。ACI/NX-OS デバイスがネットワークに正常に追加された後にのみ、SPAN 接続先を追加できます。

APIC SPAN 接続先の場合、入力ポートをエッジ-SPAN ポートとして構成し、そのポートが ACI 側に接続されている場合、ACI 側からポッド、ノード、およびポートを選択し、ポートを SPAN 接続先として設定できます。NX-OS（実稼働スイッチ）の SPAN 接続先で、入力ポートをエッジ-SPAN ポートとして設定し、ポートを NX-OS デバイスに接続した場合、NX-OS デバイスのノードとポートを選択し、ポートを SPAN 接続先として設定します。

# ユーザ定義フィールド

**[ユーザ定義フィールド（UDF）]** タブには、NDB デバイスの UDF の詳細が表示されます。

UDF を使用すると、オフセット値に基づいてパケットをフィルタリングできます。パケット内のオフセット値は、128 バイト以内で照合できます。

デフォルトでは、Nexus Dashboard Data Broker コントローラは、*udfInnerVlan* および *udfInnerVlanv6* という名前の 2 つの UDF を生成します。これらは、ISL ポートの内部 VLAN を照合するために使用されます。

**表 *48 : UDF* サポート マトリックス**

| UDF EtherType | プラットフォーム（Platform） |
|---|---|
| IPv4 | Cisco Nexus 9200 および 9300 シリーズのスイッチ |
| IPv6 | Cisco Nexus<br>93xx EX/FX、95xx EX/FX、92xx シリーズ スイッチ |

表 *49 : UDF* の対象リージョン

| プラットフォーム（Platform） | UDF の適格 TCAM リージョン |
|---|---|
| Cisco Nexus 9200、9300-EX/9300-FX、および 9500-EX/9500-FX シリーズ スイッチ | ing-ifacl |
| その他のプラットフォーム | ifacl |

次のような詳細を記した表が表示されます。

表 *50 :* ユーザ定義フィールド

| 列名 | 説明 |
|---|---|
| **UDF** | UDF 名。<br>このフィールドはハイパーリンクです。UDF の名前をクリックすると、右側に新しいペインが表示され、UDF の詳細が表示されます。ここから実行できる追加のタスクは次のとおりです。<br>• ユーザ定義フィールドの編集または複製。 |
| タイプ | **IPv4** または **IPv6** を表示します。 |
| キーワード | **Packet-Start** または **Header** を表示します。 |
| **[使用中（In Use）]** | 緑色のチェック マークは、UDF が現在使用中であることを示します。 |
| **[オフセット（Offset）]** | 設定されたオフセット値。 |
| 長さ（**Length**） | 一致したパケットの長さ（バイト数）。 |
| **[デバイス（Devices）]** | UDF が適用されているデバイスの数。 |
| **[作成者（Created By）]** | UDF を作成したユーザ。 |
| **[最終更新者（Last Modified By）]** | UDF を最後に変更したユーザ。 |

**[ユーザ定義フィールド（User Defined Field）]** タブから、次のアクションを実行できます。

- **UDF の追加（Add UDF）**：これを使用して、新しい UDF を追加します。このタスクの詳細については、UDF の追加を参照してください。
- **[UDF の削除（Delete UDF(s)）]**：行の先頭にあるチェック ボックスをオンにして、UDF を選択します。**[アクション（Actions）]** > **[UDF の削除（Delete UDF）]** をクリックします。

チェックボックスを選択せずに削除アクションを選ぶと、エラーが表示されます。UDF を選択するように求められます。

（注） UDF 定義の変更には、デバイスの再起動が必要です。

# ユーザー定義フィールドの追加

この手順を使用して、ユーザー定義フィールドを追加します。

一部のプロトコルは、一部の NX-OS デバイスではデフォルトでサポートされていません。これらのデバイスでのパケットのフィルタリングをサポートするには、UDF を使用します。

（注） UDF は、最大 2 つのオフセット バイトにマッチできます。パケット内の 3 つの連続するバイトをフィルタリングするには、UDF をスタックする必要があります。NDB GUI を使用して、2 つの UDF を順番に作成します。2 番目の UDF は、スタッキング UDF と呼ばれます。

手順

**ステップ 1** **[コンポーネント（Components）]** > **[ユーザー定義フィールド（User Defined Field）]** に移動します。

**ステップ 2** **[アクション（Actions）]** ドロップダウンリストで、**[UDF の追加（Add UDF）]** を選択します。

**ステップ 3** **[UDF の追加（Add UDF）]** ダイアログボックスで、次の詳細を入力します。

表 *51 : UDF* の追加

| フィールド | 説明 |
|---|---|
| **[UDF 名（UDF Name）]** | UDF の名前。 |
| タイプ | ドロップダウン リストから選択します。次のオプションがあります。<br>• IPv4<br>• IPv6 |

| フィールド | 説明 |
| --- | --- |
| **[キーワード（Keyword）]** | ドロップダウン リストから選択します。次のオプションがあります。<br>• ヘッダー<br>• Packet-Start<br>**ヘッダー** オプションが選択されている場合、内側（内側/外側ヘッダーからのオフセット ベース）および L3/L4（L3/L4 ヘッダーからのオフセット ベース）が有効になります。**[Packet-Start]** が選択されている場合、オフセット ベースはパケットから始まります。 |
| **ヘッダー** | ドロップダウン リストから選択します。次のオプションがあります。<br>• 内部<br>• 外部<br>このフィールドは、選択したキーワードが**[ヘッダー（Header）]**の場合にのみ有効です。内側または外側のヘッダーからベース オフセット値を選択できるようにします。 |
| **レイヤー** | ドロップダウン リストから選択します。次のオプションがあります。<br>• レイヤ 3<br>• レイヤ 4<br>このフィールドは、選択したキーワードが**[ヘッダー（Header）]**の場合にのみ有効です。オフセットの開始値がレイヤ 3 またはレイヤ 4 のどちらであるかを指定できます。 |
| **[オフセット（Offset）]** | バイト **オフセット**値を設定します。範囲は 0 ～ 127 です。<br>パケットのフィルタリングは、UDF で設定されたオフセット値に基づいて行われます。パケットは設定されたオフセット値から照合されます。 |

| フィールド | 説明 |
|---|---|
| **[長さ（Length）]** | 照合を行うパケットの長さ（バイト数）。範囲は 1 ～ 2 です。<br>位置はオフセット値に依存します。1 に設定されている場合、設定されたオフセットバイトの後の 1 バイトの照合を行います。 |
| **[デバイス（Devices）]** | UDF が作成されているデバイス。<br>**[デバイスの選択（Select Devices）]** をクリックします。<br>**[デバイスの選択（Select Devices）]** ウィンドウで、デバイスを選択して、**[デバイスの選択（Select Devices）]** をクリックします。 |

**ステップ 4** **[UDF の追加（Add UDF）]** をクリックします。

作成された UDF は、接続のフィルタを作成するときにカスタム フィルタとして使用されます。詳細については、フィルタの追加を参照してください。

（注）
UDF のアイコンは、作成直後は黄色です。デバイスを再起動したとき、UDF が正常にインストールされた場合には UDF アイコンの色は緑色に変わり、そうでない場合は赤色に変わります。

# ユーザー定義フィールドの編集またはクローン処理

この手順に従って、ユーザー定義フィールドを編集またはクローンします。

UDF の編集は、既存の UDF のパラメータを変更することを意味します。

UDF のクローンを作成すると、既存の UDF と同じパラメーターを使用する新しい UDF が作成されます。必要に応じて、デフォルト パラメータを変更できます。

### 始める前に

1 つ以上のユーザー定義フィールドを作成します。

### 手順

**ステップ 1** **[コンポーネント（Components）]** > **[ユーザー定義フィールド（User Definition Fields）]**に移動します。

**ステップ 2** 表示されたテーブルで、**[UDF]** をクリックします。

新しいペインは右側に表示されます。

**ステップ 3** **[アクション（Actions）]** をクリックし、**[UDF のクローン処理（Clone UDF）]** または **[UDF の編集（Edit UDF）]** を選択します。

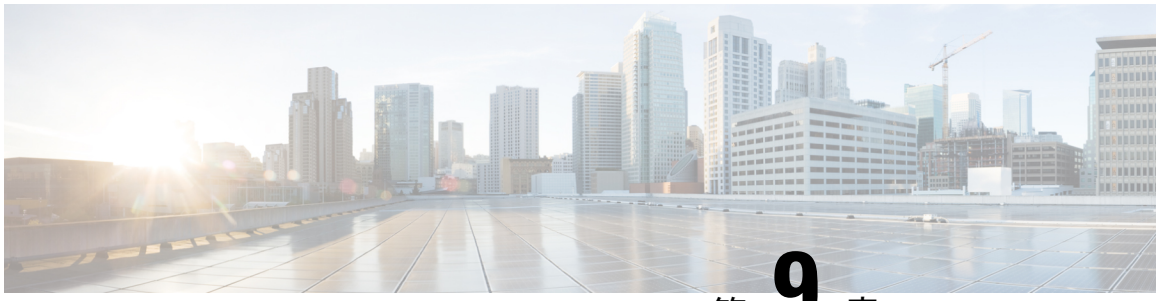
**ステップ 4** **[UDF のクローン処理（Clone UDF）]** または **[UDF の編集（Edit UDF）]** ダイアログ ボックスに、現在の UDF 情報が表示されます。これらのフィールドを必要に応じて変更します。

表 *52 : UDF*の編集

| フィールド | 説明 |
|---|---|
| **[UDF 名（UDF Name）]** | UDF の名前。<br>このフィールドは変更できません。 |
| **タイプ** | UDF の作成中に選択されたタイプ。<br>このフィールドは変更できません。 |
| **[キーワード（Keyword）]** | ドロップダウン リストから選択します。次のオプションがあります。<br>• ヘッダー<br>• Packet-Start |
| **ヘッダー** | UDF の作成中に選択されたヘッダー。<br>このフィールドは変更できません。 |
| **[レイヤー（Layer）]** | UDF の作成中に選択されたレイヤー。<br>このフィールドは変更できません。 |
| **[オフセット（Offset）]** | バイト **オフセット**値を設定します。範囲は 0 ～ 127 です。<br>パケットのフィルタリングは、UDF で設定されたオフセット値に基づいて行われます。パケットは設定されたオフセット値から照合されます。 |
| **[長さ（Length）]** | 照合を行うパケットの長さ（バイト数）。範囲は 1 ～ 2 です。<br>位置はオフセット値に依存します。1 に設定されている場合、設定されたオフセット バイトの後の 1 バイトの照合を行います。 |

| フィールド | 説明 |
| --- | --- |
| **[デバイス（Devices）]** | UDF が現在適用されているデバイス。現在のデバイスから UDF を削除すること、または他のデバイスに UDF を適用することができます。<br>**[デバイスの選択（Select Devices）]** をクリックします。<br>**[デバイスの選択（Select Devices）]** ウィンドウで、デバイスを選択して、**[デバイスの選択（Select Devices）]** をクリックします。<br>（注）<br>使用中の UDF をデバイスから削除することはできません。 |

**ステップ 5** [保存（Save）] をクリックします。



第 9 章

# セッション

この章では、Cisco Nexus Dashboard Data Brokerで作成されたセッションの詳細について説明します。

リリース 3.10.1 から、Cisco Nexus Data Broker（NDB）の名前は、Cisco Nexus Dashboard Data Brokerに変更されました。ただし、GUIおよびインストール フォルダ構造と対応させるため、一部のNDBのインスタンスがこのドキュメントには残されています。NDB/ Nexus Data Broker/ Nexus Dashboard Data Brokerという記述は、相互に交換可能なものとして用いられています。



# スパン セッション

**[スパン セッション（Span Session）]** タブには、Nexus Dashboard Data Broker コントローラのスパン セッションの詳細が表示されます。

スパン セッションは、スパン デバイスのスパン接続先とNDBデバイスの入力ポート間のリンクです。スパン セッションは部分的に Nexus Dashboard Data Broker ネットワークの外部にあり、スパンの接続先からモニタリング ツール ポートへのパケットのパスを定義します。

票には次の詳細が表示されます。

表 *53 :* スパン セッション

| 列名 | 説明 |
|---|---|
| **[Status]** | SPAN セッションのステータスは、デバイス/コントローラでのセッションの動作ステータスと、それに接続されている接続のステータスによって異なります。表示されたステータス アイコンをクリックすると、セッションと接続の詳細が表示されます。セッション ステータスに影響を与える要因は、スパンの接続先、送信元（実稼働スイッチ/コントローラ）、入力ポート、モニタリング ツール ポート、ISL リンク（該当する場合）です。<br>使用可能なステータスは次のとおりです。<br>• 緑：セッションは成功しています<br>• 黄：セッションは部分的に成功しました<br>• 赤：セッションが失敗しました<br>• 灰：セッションがインストールされていません |
| **[スパン セッション（Span Session）]** | スパン セッション名。<br>このフィールドはハイパーリンクです。**スパン セッション**の名前をクリックすると、右側に新しいペインが表示されます。ここでは、次の追加のアクションを実行できます。<br>• スパン セッションの編集またはクローン処理 （160 ページ） |
| **IP アドレス（IP Address）** | スパン セッションの送信元（スパン デバイス）の IP アドレス。 |
| **[スパン送信元（Span Sources）]** | スパン セッションの送信元ポートの数。<br>（注）<br>VLAN の場合、送信元ポートは ACI デバイスの EPG です。 |

| 列名 | 説明 |
|---|---|
| スパン接続先（Span Destination） | セッションのスパン接続先の数。<br>（注）<br>複数の SPAN 接続先を持つことができるのは ACI デバイスだけです 複数のスパン接続先がある場合、内部セッションが作成されます。これらの内部セッションは、ソース ポートの可用性に基づいて作成されます。<br>1 セッションにつき、1 つのスパン接続先だけがサポートされます。 |
| 接続（Cisco TMS Connection） | スパン セッションに関連付けられた接続の名前。 |
| 作成者 | スパン セッションを作成したユーザ。 |
| 最終更新者 | スパン セッションを最後に変更したユーザ。 |

**[スパン セッション（Span Sessions）]** タブから次のアクションを実行できます。

- **[スパン セッションの追加（Add Span Session）]**：このアクションを使用して、スパン セッションを追加します。スパン セッションの追加 （156 ページ） を参照してください。
- **[スパン セッション/接続先の同期（Synchronize Span Session/Destination）]**：このアクションを使用して、実稼働スイッチ（Nexus / Catalyst）またはコントローラ（Cisco APIC / Cisco DNAC）の情報を Nexus Dashboard Data Broker コントローラと同期します。スパン セッション情報がスイッチまたはコントローラで削除された場合、このアクションにより、スイッチまたはコントローラのスパン接続先設定とスパンセッション設定が、Nexus Dashboard Data Broker コントローラの設定と同期されます。
- **[インストールのトグル（Toggle Install）]**：このアクションを使用して、スパン セッションをインストール/アンインストールします。スイッチ（Nexus / Catalyst）/コントローラにスパン セッションをインストールできます。また、Nexus Dashboard Data Broker コントローラから削除せずにスパン セッションをアンインストールできます。スパン セッションはスイッチ/コントローラからアンインストールされますが、将来の使用のために Nexus Dashboard Data Broker コントローラに保存されたままになります。
- **[スパン セッションの削除（Delete Span Session）]**：行の先頭にあるチェックボックスをオンにして、削除するスパン セッションを選択し、**[アクション（Actions）]** > **[スパン セッションの削除（Delete Span Session(s)）]** をクリックします。選択されたスパン セッションが削除されます。チェックボックスを選択せずに削除アクションを選ぶと、エラーが表示されます。スパン セッションを選択するように求められます。

# スパン セッションの追加

この手順に従って、スパン セッションを追加します。

（注） Nexus スイッチには最大 4 つのアクティブなスパン セッションを追加できます。

Catalyst スイッチには、最大 8 つのアクティブなスパン セッションを追加できます。

### 始める前に

スパン セッションを設定する前に、コントローラ/プロダクション スイッチを追加します。

### 手順

**ステップ 1** **[セッション（Session）]** > **[スパン セッション（Span Sessions）]** に移動します。

**ステップ 2** **[アクション（Actions）]** ドロップダウン リストから、**[スパン スイッチの追加（Add Span Switches）]** を選択します。

**ステップ 3** **[スパン スイッチの追加（Add Span Switches）]** ダイアログ ボックスで、次の詳細を入力します。

表 *54 :* スパン セッションの追加

| フィールド | 説明 |
|---|---|
| **[スパン セッション名（Span Session Name）]** | スパン セッションの名前を入力します。 |
| **[スパン送信元（Span Sources）]** | スパン送信元を選択します。<br>**実稼働スイッチ**または**コントローラ**を選択します。<br>これらのそれぞれには、後の行で説明する一意のフィールド セットがあります。 |
| **[スパン送信元：コントローラ（Span Source: Controller）]** | |
| コントローラ | **[コントローラの選択（Select Controller）]** をクリックし、**[Cisco ACI]** または **[Cisco DNAC]** のいずれかを選択します。<br>ACI ネットワークの一部である Nexus デバイスのスパン ソースを作成するには、**[Cisco ACI]** を選択します。Catalyst スイッチのスパン ソースを作成するには、**[Cisco DNAC]** を選択します。 |

| フィールド | 説明 |
| --- | --- |
| **[リーフ ポート（Leaf Ports）]** | （ACI コントローラのみ）<br>ポッド、ノードおよびそのインターフェイスの選択中に、表示されるオプションで最新の詳細が見つからない場合は、**[ファブリックの更新（Refresh Fabric）]**ボタンをクリックします。このアクションは、ACI ファブリックから最新のポッド、ノード、およびそのインターフェイスを取得します。<br>複数のリーフポートからのトラフィックを取得するリーフポートを追加するには、**[リーフ ポート（Leaf Ports）]** を選択します。<br>**[リーフ ポートの選択（Select Leaf Ports）]** をクリックします。表示される **[リーフ ポートの選択（Select Leaf Port(s)）]** ウィンドウで、**ポッド**を選択します。選択したポッド内のデバイスが表示されます。**デバイス**とデバイスの**ポート**を選択します。 |
| **[EPG/AAEP]** | （ACI コントローラのみ）<br>EPG/AAEP の選択中に、表示されるオプションで最新の EPG/AAEP が見つからない場合は、**[ファブリックの更新（Refresh Fabric）]** ボタンをクリックします。このアクションにより、ACI ファブリックから最新の詳細が取得されます。<br>EPG/AAEP 送信元を追加するには、**[EPG/AAEP]** を選択します。<br>**[EPG/AAEP の選択（Select EPG/ AAEP）]** をクリックします。表示される **[EPG/ AAEP の選択（Select EPG/ AAEP）]** ウィンドウで、**テナント**、**プロファイル**、**EPG**、および **EPG メンバー** を選択します。表示される EPG メンバーは、動的、静的、AAEP です。[動的（Dynamic）] または [静的（Static）] を選択すると、メンバーの詳細が右側に表示されます。EPG メンバーとして **[AAEP]** を選択する場合には、**[AAEP の選択（Select AAEP）]** 列で AAEP を選択します。<br>（注）<br>EPG インターフェイスは、すべてのポートが同じリーフ スイッチ内にある場合にのみ機能します。<br>EPG が複数のスイッチに分散している場合は、すべてのリーフ スイッチで対応する SPAN 接続先を選択します。 |

| フィールド | 説明 |
|---|---|
| インターフェイス | （Cisco DNAC の場合のみ）<br>**[インターフェイスの選択（Select Interface）]** をクリックし、Catalyst スイッチとインターフェイスを選択します。 |
| **VLAN** | （Cisco DNAC の場合のみ）<br>VLAN ID を入力します。 |
| **[スパン送信元：実稼働スイッチ （Span Source: Production Switch）]** | |
| **[インターフェイス（Interface）]** | **[インターフェイスの選択（Select Interface(s)）]** をクリックし、**デバイス** と **ポート** を選択します。<br>選択したデバイスとポートがセッションで使用されます。 |
| **VLAN** | **[実稼働スイッチの選択（Select Production Switch）]** をクリックして、デバイスを選択します。VLAN ID を入力します。<br>VLAN ID と一致するデバイスがセッションで使用されます。 |
| **方向（Direction）** | デバイスのセッション送信元ポートのトラフィックを示します。<br>これらのオプションの 1 つを選択します。<br>• 着信<br>• 発信<br>• 両方 |

| フィールド | 説明 |
| --- | --- |
| **SPAN 宛先** | **[SPAN 接続先の選択（Select SPAN Destination）]** をクリックし、スパン接続先ポートを選択します。表示されるフィールドは以前の **[スパン送信元（Span Sources）]** の選択に基づいています。<br>（注）<br>スパン接続先ポートは、入力ポートの追加 （119 ページ）の手順を使用して以前に作成されました。<br><br>NDBデバイスに直接接続されている場合は、ローカル スパンの接続先を選択し、そうでない場合はリモート スパンの接続先を選択します。リモート スパンの接続先は、Nexus スイッチにのみ適用されます。<br>スパンセッションをインストールするために、Nexus Dashboard Data Broker コントローラは、ACI で作成されたスパン宛先をリストします。<br>Nexus SPANセッションをインストールするために、Nexus Dashboard Data Broker コントローラは、Nexus デバイス用に作成された SPAN 接続先をリストします。<br>Catalyst SPAN セッションをインストールするために、Nexus Dashboard Data Broker コントローラは、Catalyst スイッチ用に作成された SPAN 接続先をリストします。 |
| **[接続を適用（Apply Connection）]** | セッションの接続を選択します。<br>スパンセッションに既存の接続を関連付けるか、スパン セッションの新しい接続を作成できます。<br>（注）<br>セッションの一部であるすべてのスパン接続先も接続の一部であり、トラフィックをモニタリング ツールに転送する必要があります。<br><br>ボタンをクリックして、スパンセッションへの接続の追加を有効にします。**[接続の選択（Select Connection）]** をクリックして、**[接続の選択（Select Connection）]** ウィンドウから接続を選択します。 |

（注）
EPG の場合：

- EPG 選択の場合、EPG が選択されている場合、デフォルトでは、Nexus Dashboard Data Broker コントローラは、選択された EPG の静的または動的に設定されたインターフェイスの変更をリッスンします。変更がある場合は、SPAN セッションに適用されます。Web ソケット接続は、証明書で保護されていません。イベント リスニングを無効にするには、`ndb/configuration` フォルダの下の `config.ini` ファイルに `enableWebSocketHandle=false` を追加します。
- APIC に新しい EPG メンバーが追加されたときに、設定された SPAN セッションの一部として新しく追加された EPG メンバーに一致する SPAN 接続先がリーフ スイッチにない場合、Nexus Dashboard Data Broker はこのイベントを無視し、新しい EPG メンバーは Nexus Dashboard Data Broker に表示されません。

（注）
スパン接続先の場合：

SPAN 送信元の各リーフ スイッチに、対応する SPAN 接続先が少なくとも 1 つあることを確認します。

**ステップ 4** **[スパン セッションの追加（Add Span Session）]** をクリックして、実稼働スイッチまたはコントローラにインストールせずに、作成したスパンセッションを追加します。**[スパン セッションのインストール（Install Span Session）]** をクリックして、作成したスパン セッションを保存し、実稼働スイッチまたはコントローラにインストールします。

# スパン セッションの編集またはクローン処理

この手順に従って、スパン セッションを編集するか、そのクローンを作成します。

スパン セッションの編集は、既存のスパン セッションのパラメータの一部を変更することを意味します。

スパン セッションのクローンを作成するということは、既存のスパン セッションと同じパラメータを使用し、必要な変更を加えた新しいスパンセッションを作成することを意味します。スパン セッションの名前は、保存する前に変更してください。

### 始める前に

1 つ以上のスパン セッションを追加します。

### 手順

**ステップ 1** **[セッション]** > **[スパン セッション]** に移動します。

**ステップ 2** 表示されたテーブルで、**[セッション（Session）]**をクリックします。

新しいペインは右側に表示されます。

**ステップ 3** **[アクション（Actions）]** をクリックし、**[スパン セッションの編集（Edit Span Session）]** または **[スパン セッションのクローン作成（Clone Span Session）]** を選択します。

テーブルに表示されているパラメータを編集します。

**表 *55 :* スパン セッションの編集**

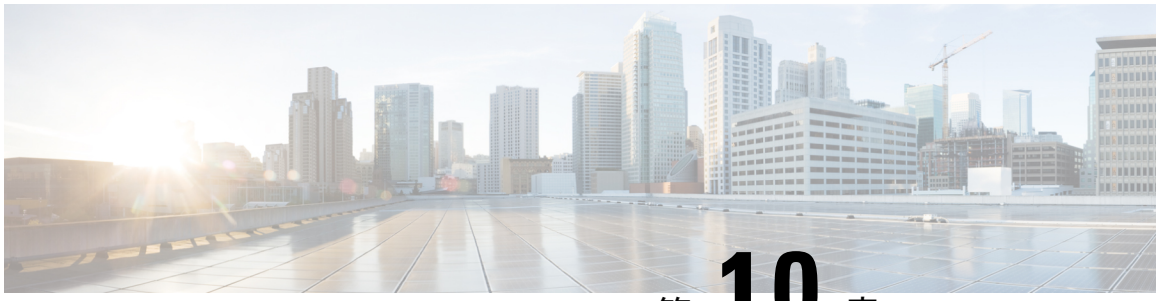
| フィールド | 説明 |
|---|---|
| **[スパン セッション名（Span Session Name）]** | スパン セッション名が表示されます。<br>このフィールドは編集できません。 |
| スパン ソース | 以前に選択したスパン ソースが表示されます。スパン ソースは変更できません。 |
| **[スパン送信元：コントローラ（Span Source: Controller）]** | |
| コントローラ | **[コントローラの選択（Select Controller）]** をクリックし、**[（Cisco）ACI]** または **[（Cisco）DNAC]** のいずれかを選択します。<br>ACI ネットワークの一部である Nexus デバイスのスパン ソースを作成するには、**[（Cisco）ACI]** を選択します。Catalyst スイッチのスパン ソースを作成するには、**[（Cisco）DNAC]** を選択します。 |
| **[リーフ ポート（Leaf Ports）]** | （ACI コントローラのみ）<br>複数のリーフ ポートからのトラフィックを取得するリーフ ポートを追加するには、**[リーフ ポート（Leaf Ports）]** を選択します。<br>**[リーフ ポートの選択（Select Leaf Ports）]** をクリックします。表示される **[リーフ ポートの選択（Select Leaf Port(s)）]** ウィンドウで、**ポッド**を選択します。選択したポッド内のデバイスが表示されます。**デバイス**とデバイスの**ポート**を選択します。 |

| フィールド | 説明 |
|---|---|
| **[EPG/AAEP]** | （ACI コントローラのみ）<br>EPG/AAEP 送信元を追加するには、**[EPG/AAEP]** を選択します。<br>**[EPG/AAEP の選択（Select EPG/ AAEP）]** をクリックします。表示される **[EPG/ AAEP の選択（Select EPG/ AAEP）]** ウィンドウで、**テナント**、**プロファイル**、**EPG**、および **EPG メンバー** を選択します。表示される EPG メンバーは、動的、静的、AAEP です。[動的（Dynamic）] または [静的（Static）] を選択すると、メンバーの詳細が右側に表示されます。EPG メンバーとして **[AAEP]** を選択する場合には、**[AAEP の選択（Select AAEP）]** 列で AAEP を選択します。<br>（注）<br>EPG インターフェイスは、すべてのポートが同じリーフ スイッチ内にある場合にのみ機能します。<br>EPG が複数のスイッチに分散している場合は、すべてのリーフ スイッチで対応する SPAN 接続先を選択します。 |
| **インターフェイス** | （Cisco DNAC の場合のみ）<br>**[インターフェイスの選択（Select Interface）]** をクリックし、Catalyst スイッチとインターフェイスを選択します。 |
| **VLAN** | （Cisco DNAC の場合のみ）<br>VLAN ID を入力します。 |
| **[スパン送信元：実稼働スイッチ （Span Source: Production Switch）]** | |
| **[インターフェイス（Interface）]** | スパン セッションの追加中に以前に選択したインターフェイスが表示されます。これらのインターフェイスは追加または削除できます。<br>**[インターフェイスの選択（Select Interface(s)）]** をクリックし、**デバイス** と **ポート** を選択します。<br>選択したデバイスとポートがセッションで使用されます。 |

| フィールド | 説明 |
| --- | --- |
| **VLAN** | **[実稼働スイッチの選択（Select Production Switch）]** をクリックして、デバイスを選択します。VLAN ID を入力します。<br><br>VLAN ID と一致するデバイスがセッションで使用されます。 |
| **方向（Direction）** | デバイスのセッション送信元ポートのトラフィックを示します。<br><br>これらのオプションの 1 つを選択します。<br><br>• 着信<br>• 発信<br>• 両方 |
| **SPAN 宛先** | **[SPAN 接続先の選択（Select SPAN Destination）]** をクリックし、スパン接続先ポートを選択します。表示されるフィールドは以前の **[スパン送信元（Span Sources）]** の選択に基づいています。<br><br>（注）<br>スパン接続先ポートは、入力ポートの追加 （119 ページ）の手順を使用して以前に作成されました。<br><br>NDB デバイスに直接接続されている場合は、ローカル スパンの接続先を選択し、そうでない場合はリモート スパンの接続先を選択します。リモート スパンの接続先は、Nexus スイッチにのみ適用されます。<br><br>スパンセッションをインストールするために、Nexus Dashboard Data Broker コントローラは、ACI で作成されたスパン宛先をリストします。<br><br>Nexus SPAN セッションをインストールするために、Nexus Dashboard Data Broker コントローラは、NX-OS デバイス用に作成された SPAN 接続先をリストします。<br><br>Catalyst SPAN セッションをインストールするために、Nexus Dashboard Data Broker コントローラは、Catalyst スイッチ用に作成された SPAN 接続先をリストします。 |

| フィールド | 説明 |
| --- | --- |
| **[接続を適用（Apply Connection）]** | セッションの接続を選択します。<br>スパンセッションに既存の接続を関連付けるか、スパン セッションの新しい接続を作成できます。<br>（注）<br>セッションの一部であるすべてのスパン接続先も接続の一部であり、トラフィックをモニタリングツールに転送する必要があります。<br>ボタンをクリックして、スパンセッションへの接続の追加を有効にします。**[接続の選択（Select Connection）]** をクリックして、**[接続の選択（Select Connection）]** ウィンドウから接続を選択します。 |

**ステップ 4** **[保存（Save）]** をクリックします。



第 10 章

# 統計

この章では、Cisco Nexus Dashboard Data Broker の接続とコンポーネントの統計について詳しく説明します。

リリース 3.10.1 から、Cisco Nexus Data Broker（NDB）の名前は、Cisco Nexus Dashboard Data Brokerに変更されました。ただし、GUI およびインストール フォルダ構造と対応させるため、一部の NDB のインスタンスがこのドキュメントには残されています。NDB/ Nexus Data Broker/ Nexus Dashboard Data Brokerという記述は、相互に交換可能なものとして用いられています。



## 接続

**[接続（Connections）]** タブには、Nexus Dashboard Data Broker コントローラで構成された接続のリストが表示されます。

次の詳細を示す表が表示されます。

| 列名 | 説明 |
|---|---|
| **接続（Connection）** | 接続名 。<br>このフィールドはハイパーリンクです。**接続**の名前をクリックして、接続に関する詳細情報を取得します。関連するアクションについては、接続のセクションを参照してください。 |
| **パケット数（Packet Count）** | 接続の集約トラフィックのボリュームをパケット数で表した値。 |

# フィルタ

**[フィルタ（Filter）]** タブには、接続で使用されるフィルタが表示されます。

次の詳細を示す表が表示されます。

| 列名 | 説明 |
|---|---|
| **[フィルタ（Filter）]** | フィルタ名。<br>これはハイパーリンクになっています。フィルタの詳細については、**フィルタ**の名前をクリックしてください。関連するアクションについては、フィルタセクションを参照してください。 |
| **[パケット数（Packet Count）]** | フィルタのパケットで表示される集約トラフィック ボリューム。 |

# [フロー（Flows）]

**[フロー（Flows）]** タブには、NDB デバイスのデバイス フローが表示されます。

**[デバイスの選択（Select Device）]** をクリックして、フロー統計を取得する NDB デバイスを選択します。別のデバイスのフロー統計を取得する場合は、**[デバイスの変更（Change Device）]** をクリックします。

次の詳細を示す表が表示されます。

| 列名 | 説明 |
|---|---|
| **[入力ポート（In Port）]** | トラフィックの照合が行われる入力ポート。 |
| **[DL 送信元（DL Src）]** | 着信トラフィックと照合される送信元MACアドレス。 |
| **[DL 接続先（DL Dst）]** | 着信トラフィックと照合される接続先MACアドレス。 |
| **[DL タイプ（DL Type）]** | 着信トラフィックと照合されるイーサタイプ。たとえば、**[IPv4]** または **[IPv6]** は、すべての IP トラフィック タイプに使用されます。 |
| **[DL VLAN]** | 着信トラフィックと照合される VLAN ID。 |
| **[VLAN PCP]** | 着信トラフィックと照合される VLAN 優先順位。 |

| 列名 | 説明 |
|---|---|
| **[NW 送信元（NW Src）]** | 着信トラフィックの IPv4 または IPv6 送信元アドレス。 |
| **[NW 接続先（NW Dst）]** | 着信トラフィックの IPv4 または IPv6 接続先アドレス。 |
| **[NW プロトコル（NW Proto）]** | 着信トラフィックと照合されるネットワークプロトコル。たとえば、「6」は TCP プロトコルを示します。 |
| **[TP 送信元（TP Src）]** | 着信トラフィックと照合されるネットワークプロトコルに関連付けられた送信元ポート。 |
| **[TP 接続先（TP Dst）]** | 着信トラフィックと照合されるネットワークプロトコルに関連付けられた接続先ポート。 |
| **[パケット数（Packet Count）]** | 指定されたフロー接続にマッチするパケット数で表された集約トラフィック ボリューム。 |

# 入力ポート

**[入力ポート（Input Ports）]** タブには、NDB デバイスの入力ポートのパケット数の詳細が表示されます。

次の詳細を示す表が表示されます。

| 列名 | 説明 |
|---|---|
| **[入力ポート（Input Ports）]** | デバイス名の入力ポート。<br>**入力ポート**をクリックして、入力ポートの詳細を取得します。関連するアクションについては、入力ポート （117 ページ）セクションを参照してください。 |
| **[パケット数（Packet Count）]** | 入力ポートでの集約トラフィック ボリュームをパケット単位で表示したもの。 |

# TCAM リソース使用率

**[TCAM リソース使用率（TCAM Resource Utilization）]** タブには、NDB デバイスの TCAM リソース使用率の詳細が表示されます。

次の詳細の表が表示されます。

表 *56 : TCAM* リソース使用率

| 列名 | 説明 |
|---|---|
| **Device** | デバイス名<br>このフィールドはハイパーリンクです。デバイスの詳細については、**デバイス**の名前をクリックしてください。関連するアクションについては、デバイスセクションを参照してください。 |
| **[使用率（Utilization）]** | 使用パターン。色によって示されます。<br>• 緑：TCAM 使用率が最適であることを示します。<br>• オレンジ：TCAM 使用率が範囲内にあることを示します。<br>• 赤：TCAM 使用率が上限に近づいていることを示します。 |

# モニタリングツール

**[モニタリング ツール（Monitoring Tools）]** タブには、NDB コントローラに接続されているモニタリング ツールのポートが表示されます。

次の詳細を示す表が表示されます。

| 列名 | 説明 |
|---|---|
| **[モニタリング ツール （Monitoring Tools）]** | モニタリング ツール名。<br>このフィールドはハイパーリンクです。詳細については、モニタリング ツールの名前をクリックしてください。関連するアクションについては、モニタリング ツールのセクションを参照してください。 |
| **Tx パケット** | モニタリング ツール ポートによって送信されたパケットの数。 |

# ポート

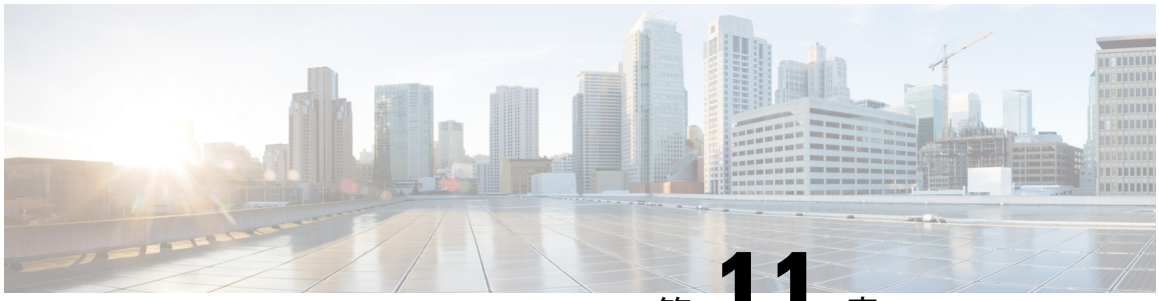
**[ポート（Ports）]** タブには、NDB デバイスのポートの統計が表示されます。

**[デバイスの選択（Select Device）]** をクリックして、選択したデバイスのポートの詳細を取得します。**[デバイスの変更（Change Device）]** をクリックして、別のデバイスを選択します。

次の詳細を示す表が表示されます。

| 列名 | 説明 |
|---|---|
| **Port** | 統計が表示されるデバイスのインターフェイス。<br>これはハイパーリンクです。詳細については、ポートをクリックしてください。 |
| **[Rx パケット数（Rx Pkts）]** | ポートで受信したパケットの数。 |
| **[Tx パケット数（Tx Pkts）]** | ポートで送信したパケットの数。 |
| **[Rx バイト数（Rx Bytes）]** | ポートで受信したバイト数。 |
| **[Tx バイト数（Tx Bytes）]** | ポートで送信したバイト数。 |
| **[Rx レート（kbps）（Rx Rate）]** | パケットの受信レート。 |
| **[Tx レート（kbps）（Tx Rate）]** | パケットの送信レート。 |
| **[Rx ドロップ（Rx Drops）]** | ポート（Rx）でパケットがドロップされる割合。 |
| **[Tx ドロップ（Tx Drops）]** | ポート（Tx）でパケットがドロップされる割合。 |
| **[Rx エラー（Rx Errs）]** | パケット受信中のポートでのエラー。 |
| **[Tx エラー（Tx Errs）]** | パケット送信中のポートでのエラー。 |
| **[Rx フレーム エラー（Rx Frame Errs）]** | パケット受信中のポートでのフレームエラー。 |
| **[Rx オーバーラン（Rx OverRun）]** | パケットの受信中にポートでオーバーラン エラーが発生しました。 |

**[アクション（Actions）]** > **[ポートのクリア（Clear Ports）]** をクリックして、選択したデバイスの統計データをクリアします。



第 11 章

# トラブルシューティング

この章では、Cisco Nexus Dashboard Data Broker のトラブルシューティングの詳細について説明します。

リリース 3.10.1 から、Cisco Nexus Data Broker（NDB）の名前は、Cisco Nexus Dashboard Data Brokerに変更されました。ただし、GUI およびインストール フォルダ構造と対応させるため、一部の NDB のインスタンスがこのドキュメントには残されています。NDB/ Nexus Data Broker/ Nexus Dashboard Data Brokerという記述は、相互に交換可能なものとして用いられています。



## 監査ログ

**[監査ログ（Audit Log）]** タブには、Nexus Dashboard Data Broker コントローラで実行されたアクティビティまたはアクションの記録が表示されます。

（注） 読み取り専用アクションは記録されません。

表には次の詳細が表示されます。

**表 *57* : 監査ログ**

| 列名 | 説明 |
|---|---|
| 日時 | アクティビティの日時 |

| 列名 | 説明 |
|---|---|
| **Module Name** | イベントが発生したモジュール。<br>これは、モジュールの内部マッピングに基づいています。たとえば、ログインとログアウトはセキュリティ モジュールの一部です。 |
| スライス（**Slice**） | アクション/イベントに関連するスライス。<br>一部のアクションはスライスに関連していないため、空白のままになっています。<br>スライス依存のアクションの例：コンポーネント、接続、セッション、統計。 |
| ユーザー（**User**） | イベント アクティビティに責任をもつユーザー。 |
| アクション（**Action**） | ユーザーが実行したアクションの簡単な説明。 |
| リソース（**Resource**） | アクションが実行されたオブジェクト。 |
| 説明 | 実行されたアクションの結果。次のオプションを使用できます。<br>• 障害の説明<br>• Success |
| **Origin** | アクションが実行された Nexus Dashboard Data Broker コントローラ。<br>（注）<br>スタンドアロン Nexus Dashboard Data Broker コントローラの場合、127.0.0.1 を表示します。 |
| モード（**Mode**） | アクションが実行されたモード。<br>（注）<br>リリース3.10では、集中モードのみがサポートされています。 |

**[監査ログ（Audit Log）]** タブから、次のアクションを実行できます。

- **[レコードの取得（Fetch Records）]**：これを使用して、表示される監査ログの数を設定します。

**[アクション（Actions）]** > **[レコードの取得（Fetch Records）]** をクリックし、**[レコード数（Record Count）]** フィールドに値を入力します。**[取得（Fetch）]** をクリックします。これに応じて、監査ログ テーブルがロードされます。

# フローの管理

**[フロー管理（Flow Management）]** タブでは、矛盾した接続とデバイス フローを表示し、矛盾したフローを管理できます。詳細を閲覧してダウンロードできるので、デバッグに活用できます。

**[フロー管理（Flow Management）]** タブには、次のサブタブがあります。

- **[整合性チェック（Consistency Check）]**：NX-API ベースのデバイスの不整合を表示します。NDB データベースとの ACL/ACE の不一致がある場合、不整合が自動的にトリガーされます。詳細については、整合性チェックを参照してください。
- **[接続フロー（Connection Flows）]**：接続用に生成された ACL および ACE の詳細を表示します。詳細については、接続フローを参照してください。
- **[デバイス フロー（Device Flows）]**：デバイス用に生成された ACL および ACE の詳細を表示します。詳細については、デバイス フローを参照してください。

## 整合性検査

**[整合性検査（Consistency Check）]** タブには、NX-API ベースのデバイスの不整合が表示されます。Nexus Dashboard Data Broker データベースとの間で ACL/ACE の不一致がある場合、不整合は自動的にトリガーされます。

ヘッダーの *[アラーム（Alarm）]* アイコン（  ）には、不整合のあるデバイスの数が表示されます。

表には次の詳細が表示されます。

**表 *58*：整合性検査**

| 列名 | 説明 |
|---|---|
| デバイス | デバイス名<br>このフィールドはハイパーリンクです。**デバイス**の名前をクリックすると、新しいペインが右側に表示されます。デバイスの詳細については、デバイスを参照してください。 |

| 列名 | 説明 |
| --- | --- |
| **[一貫性のないコントローラ フロー（Inconsistent Controller Flows）]** | 一貫性のないコントローラ フロー。<br>このフィールドはハイパーリンクです。示された番号をクリックすると、右側に新しいペインが表示され、ACL とその ACE のリストが表示されます。ここから次のアクションを実行できます。<br>• **[フローの修正（Fix Flows）]**：必要なチェックボックスを選択し、**[フローの修正（Fix Flows）]** をクリックします。選択したフロー（ACE）が修正され、それに応じて **[一貫性のないコントローラ フロー（Inconsistent Controller Flows）]** 列に表示される数が更新されます。<br>• **[すべてをエクスポート（Export All）]**：ACL および ACE としてリストされているフローのコピーを取得するには、このオプションを選択します。`.csv` ファイルがローカル マシンにダウンロードされます。これはデバッグに役立ちます。 |

| 列名 | 説明 |
| --- | --- |
| **[一貫性のないデバイス フロー（Inconsistent Device Flows）]** | デバイスの一貫性のないフローまたは古いフローです。コントローラ フローとの比較で、デバイスに欠落している ACL および ACE を示します。<br><br>このフィールドはハイパーリンクです。示された番号をクリックすると、右側に新しいペインが表示され、ACL とその ACE のリストが表示されます。ここから次のアクションを実行できます。<br><br>• **[フローの修正（Fix Flows）]**：必要なチェックボックスを選択し、**[フローの修正（Fix Flows）]** をクリックします。選択したフロー（ACE）が修正され、それに応じて **[一貫性のないコントローラ フロー（Inconsistent Controller Flows）]** 列に表示される数が更新されます。<br><br>• **[すべてのエクスポート（Export All）]**：ACE と共に ACL としてリストされたフローのコピーを取得するには、このオプションを選択します。`.csv` ファイルがローカル マシンにダウンロードされます。これはデバッグに役立ちます。 |

| 列名 | 説明 |
| --- | --- |
| **[NDB 以外のフロー（Non NDB Flows ）]** | デバイスに存在する ACL の数。ACL は、デフォルトのデバイス ACL にすることも、手動で追加することもできます。<br>このフィールドはハイパーリンクです。示された番号をクリックすると、右側に新しいペインが表示され、ACL とその ACE のリストが表示されます。ここから次のアクションを実行できます。<br>• **[フローの修正（Fix Flows）]**：必要なチェックボックスを選択し、**[フローの修正（Fix Flows）]** をクリックします。選択したフロー（ACE）が修正され、それに応じて **[一貫性のないコントローラ フロー（Inconsistent Controller Flows）]** 列に表示される数が更新されます。<br>• **[すべてのエクスポート（Export All）]**：ACE と共に ACL としてリストされたフローのコピーを取得するには、このオプションを選択します。`.csv` ファイルがローカル マシンにダウンロードされます。これはデバッグに役立ちます。 |

（注） Nexus Dashboard Data Broker によって生成された ACL は、*ndb_* プレフィックスで示されます。NDB 以外のフローは、それぞれのコンポーネントによって示されます。

次のアクションは、**[整合性チェック（Consistency Check）]** タブから実行できます。

- **[コントローラ フローの確認（Check Controller Flows）]** — デバイスを選択し、**[コントローラ フローの確認（Check Controller Flows）]** をクリックします。ACL と ACE を含む新しいペインが右側に表示されます。
- **デバイス フローの確認（Check Device Flows）**—デバイスを選択して、**[デバイス フローの確認（Check Device Flows）]** をクリックします。ACL と ACE を含む新しいペインが右側に表示されます。
- **[NDB 以外のフローを表示（View non-NDB Flow）]** — デバイスを選択し、**[NDB 以外のフローを表示（View non-NDB Flow）]** をクリックします。ACL と ACE を含む新しいペインが右側に表示されます。

# 接続フロー

**[接続フロー（Connections Flows）]** タブには、接続用に生成された ACL および ACE の詳細が表示されます。

票には次の詳細が表示されます。

**表 *59 :* 接続フロー**

| 列名 | 説明 |
|---|---|
| **接続（Connection）** | 接続名です。<br>このフィールドはハイパーリンクです。**接続**の名前をクリックすると、右側に新しいペインが表示され、接続の詳細が表示されます。ここで実行できるアクションについては、接続の章を参照してください。 |
| **フロー（Flows）** | 接続のフロー（ACE）の数（デバイス間でも可能）。<br>このフィールドはハイパーリンクです。表示された番号をクリックすると、右側に新しいペインが表示されます。接続名に続いて、ACL とそれに含まれる ACE が表示されます。ここから実行できるアクションは次のとおりです。<br>• **[すべてのエクスポート（Export All）]**：ACE と共に ACL としてリストされたフローのコピーを取得するには、このオプションを選択します。.csv ファイルがローカル マシンにダウンロードされます。 |

**[接続フロー（Connection Flows）]** タブから、次のアクションを実行できます。

- **[接続フローの確認（Check Connection Flows）]**：接続を選択し、**[接続フローの確認]** をクリックします。新しいペインは右側に表示されます。接続名に続いて、ACL とそれに含まれる ACE が表示されます。ここから実行できるアクションは次のとおりです。
  - **[すべてのエクスポート（Export All）]**：ACE と共に ACL としてリストされたフローのコピーを取得するには、このオプションを選択します。.csv ファイルがローカル マシンにダウンロードされます。

# デバイス フロー

**[デバイス フロー（Device Flows）]** タブには、デバイス用に生成された ACL および ACE の詳細が表示されます。

票には次の詳細が表示されます。

表 *60 :* デバイス フロー

| 列名 | 説明 |
|---|---|
| **Device** | デバイス名<br>このフィールドはハイパーリンクです。**[デバイス（Device）]** の名前をクリックすると、右側に新しいペインが表示され、デバイスの詳細が表示されます。ここで実行できるアクションについては、デバイスの章を参照してください。 |
| **フロー** | デバイスのフロー（ACE）の数（接続およびデバイスのすべてのポートにまたがる可能性があります）。<br>このフィールドはハイパーリンクです。表示された番号をクリックすると、右側に新しいペインが表示されます。接続名に続いて、ACL とそれに含まれる ACE が表示されます。ここから実行できるアクションは次のとおりです。<br>• **[すべてのエクスポート（Export All）]**：ACE と共に ACL としてリストされたフローのコピーを取得するには、このオプションを選択します。.csv ファイルがローカル マシンにダウンロードされます。 |

次のアクションは、**[デバイス フロー（Device Flows）]** タブから実行できます。

- **デバイス フローの確認（Check Device Flows）**：デバイスを選択して、**[デバイス フローの確認（Check Device Flows）]** をクリックします。新しいペインは右側に表示されます。デバイス名に続いて、ACL とそれに含まれる ACE が表示されます。ここから実行できるアクションは次のとおりです。
  - **[すべてのエクスポート（Export All）]**：ACE と共に ACL としてリストされたフローのコピーを取得するには、このオプションを選択します。.csv ファイルがローカル マシンにダウンロードされます。

# JSON エクスポート/インポート

**[JSON エクスポート/インポート（JSON Export/Import）]** タブでは、デバイス構成を JSON ファイル形式でエクスポートおよびインポートできます。構成ファイルには、すべての構成情

報（ポートチャネルを除く）とともに、接続されたデバイスと切断されたデバイスに関する情報が含まれています。

この **[JSON エクスポート/インポート（JSON Export/Import）]** タブには次のサブタブが含まれます。

- **[エクスポート（Export）]**：Nexus ダッシュボードデータブローカ コントローラから（ローカルマシンに）構成をエクスポートできるようにします。詳細については、エクスポートを参照してください。
- **[インポート（Import）]**：設定を Nexus Dashboard Data Broker コントローラにインポートできるようにします。詳細については、インポートを参照してください。

# エクスポート

**[エクスポート（Export）]** タブでは、Nexus Dashboard Data Broker コントローラから構成をエクスポートできます。

次の詳細の表が表示されます。

**表 *61* : エクスポート**

| 列名 | 説明 |
|---|---|
| **[ID]** | デバイスのシリアル番号 |
| 名前（Name） | デバイスの名前。 |
| **[IP アドレス（IP Address）]** | デバイスの IP アドレス。 |
| **[タイプ（Type）]** | デバイスのタイプです。次のオプションがあります。<br>• [NX]：NX-API デバイスに接続された NDB デバイス。<br>• [PS]：実稼働スイッチ（NX-OS）に接続された NDB デバイス。<br>• [AC]：ACI デバイスに接続された NDB デバイス。 |
| **[ステータス（Status）]** | デバイスのステータス。 |

次のアクションは、**[JSON のエクスポート/インポート（JSON Export/ Import）]** > **[エクスポート（Export）]** タブから実行できます。

- **構成のエクスポート**：**[アクション（Actions）]** > **[構成のエクスポート（Export Configuration）]** をクリックして、JSON 構成をローカル マシンにエクスポートします。

エクスポート中にデバイスの接続を含めるには、**[接続（Connections）]**チェックボックスをオンにします。**[エクスポート]** をクリックします。

# インポート

**[インポート（Import）]** タブは構成を Nexus Dashboard Data Broker コントローラにインポートできるようにします。

次の詳細の表が表示されます。

表 *62 :* インポート

| 列名 | 説明 |
|---|---|
| **[ID]** | デバイスのシリアル番号 |
| **[エクスポートされたデバイス名（Exported Device Name）]** | 構成のエクスポート元のデバイスの名前。 |
| **[IP アドレス（IP Address）]** | デバイスの IP アドレス。 |
| **[タイプ（Type）]** | デバイスのタイプです。次のオプションがあります。<br>• [NX]：NX-API デバイスに接続された NDB デバイス。<br>• [PS]：実稼働スイッチ（NX-OS）に接続された NDB デバイス。<br>• [AC]：ACI デバイスに接続された NDB デバイス。 |
| **[ステータス（Status）]** | インポートアクションのステータス。オプションは、成功、失敗、部分的、進行中、中止です。 |
| 説明 | 成功/失敗ステータスの説明。 |

次のアクションは、**[JSON エクスポート/インポート（JSON Export/Import）]** > **[インポート（Import）]** タブから実行できます。

- **[構成のインポート（Import Configuration）]** : **[アクション（Actions）]** > **[構成のインポート（Import Configuration）]** をクリックし、ローカルマシンから JSON ファイルを選択して **[アップロード（Upload）]** をクリックします。ドラッグアンドドロップして JSON ファイルをアップロードすることもできます。
- **[構成の適用（Apply Configuration）]** : **[アクション（Actions）]** > **[構成の適用（Apply Configuration）]** をクリックします。**[デバイスの編集（Edit Device）]** 画面が表示されま

す。構成を適用するデバイスの詳細を入力します。**[適用して互換性を確認（Apply and Check Compatibility）]** をクリックします。**[互換性マトリックス（Compatibility Matrix）]** 画面が表示されます。両方のデバイスに互換性がある場合、ステータスは緑色で示されます。**[適用（Apply）]** をクリックします。

このアクションのステータスは、**[インポート（Import）]** テーブルに示されます。

- **[インポートの削除（Delete Import）]**：**[アクション（Actions）]**>**[インポートの削除（Delete Import）]** をクリックして、インポートされた構成を削除します。

# デバイスのページ

**[デバイスのページ（Purge Device）]** タブには、削除された NDB デバイスの詳細が表示されます。デバイスを削除した場合には、Nexus Dashboard Data Broker コントローラからデバイスのみが削除され、デバイス構成は保持されます。一方、デバイスをパージした場合には、Nexus Dashboard Data Broker コントローラからデバイスが削除されるとともに、デバイス構成も削除されます。

表には次の詳細が表示されます。

**表 *63*：デバイスのページ**

| 列名 | 説明 |
|---|---|
| **[ノード ID（Node ID）]** | Nexus Dashboard Data Broker コントローラに接続されているデバイスのノード ID。 |
| **Device** | デバイス名 |
| **[IP アドレス（IP Address）]** | デバイスの IP アドレス。 |

*[属性によるフィルタ処理（Filter by attributes）]* バーを使用して、表示されているデバイス グループの詳細に基づいてテーブルをフィルタ処理します。属性、演算子、およびフィルタ値を選択します。

**[デバイスのページ（Purge Device）]** タブでは、次のアクションを実行できます。

- **[デバイスのページ（Purge Device）]**：行の先頭にあるチェックボックスをオンにして、必要なデバイスを選択します。**[デバイスのページ（Purge Device）]** をクリックします。

  これにより、古いデバイス構成がデータベースから削除されます。

# RMA

Return Material Authorization（**RMA**）タブには、削除され、交換待ちのデバイスのリストが表示されます。この機能は、RMA デバイスの設定を新しいデバイスにマッピングします。

表には次の詳細が表示されます。

**表 *64 : RMA***

| 列名 | 説明 |
|---|---|
| **[既存のノード ID（Existing Node ID）]** | （削除された）NDB デバイスのノード ID。 |
| **[ノード名（Node Name）]** | デバイス名 |
| **[シリアル番号（Serial Number）]** | デバイスのシリアル番号 |
| **[IP アドレス（IP Address）]** | デバイスの IP アドレス。 |

**[RMA]** タブから次のアクションを実行できます。

- **[ノード ID の置換（Replace Node ID）]** : チェックボックスをオンにしてノード ID を+選択します。**[アクション（Actions）]** > **[ノード ID の置換（Replace Node ID）]** をクリックします。表示されるポップアップ ウィンドウで、**[シリアル番号（Serial Number）]**を入力し、**[置換（Replace）]** をクリックします。選択したデバイスは、新しいシリアル番号のデバイスに置き換えられます。

（注） NX-API デバイスのシリアル番号を取得するには、非モジュラー シャーシの **show module** コマンドを使用するか（出力でシリアル番号を探します）、モジュラー シャーシ スイッチの **show hardware** コマンドを使用します（出力のスイッチ ハードウェア ID 情報でシリアル番号を探します）。

# [Tech Support]

**[テクニカル サポート（Tech Support）]** タブには、Nexus Dashboard Data Broker コントローラで作成されたテクニカル サポート ジョブの詳細が表示されます。

テクニカル サポートの詳細については、テクニカル サポートの概要 （185 ページ） をご覧ください。

表には次の詳細が表示されます。

表 *65 : [Tech Support]*

| 列名 | 説明 |
|---|---|
| **Job ID** | テクニカル サポート ジョブ用に作成されたジョブ ID。<br>このフィールドはハイパーリンクです。**ジョブ ID** をクリックして、ジョブの詳細を表示します。ローカルマシンにファイルをダウンロードするには、**[アクション（Actions）]** > **[ダウンロード（Download）]** をクリックします。<br>**[ダウンロードして削除（Download and Delete）]** オプションは、ジョブの詳細をローカル マシンにダウンロードし、Nexus Dashboard Data Broker コントローラから削除します。 |
| **ジョブ タイプ（Job Type）** | ジョブの操作タイプ。次のオプションがあります。<br>• 基本<br>• 拡張 |
| **Status** | テクニカル サポート ジョブのステータス。<br>使用可能なステータスは次のとおりです。<br>• 成功（Success）：ジョブは正常に完了しました。<br>• 一部（Partial）：ジョブの一部が成功しました。たとえば、複数のデバイスを選択した場合、選択したデバイスの 1 つで障害が発生した可能性があります。<br>• 失敗（Failure）：ジョブは成功しませんでした。<br>• 進行中（In progress）：ジョブは現在進行中です。<br>• 作成済み（Created）：ジョブは実行の準備ができていますが、現在キューに入っています。<br>• 停止（Stop）：ジョブは作成されましたが、完了が許可されていません。 |

次のアクションは、**[テクニカル サポート（Tech Support）]** タブから実行できます。

- **[ジョブのトリガー（Trigger Job）]**：これを使用して、テクニカルサポートジョブをトリガーします。詳細については、テクニカルサポートのトリガー（184 ページ）を参照してください。
- **[ジョブの再トリガー（Re-trigger Job）]**：次のチェックボックスを選択し、**[アクション（Actions）]** > **[ジョブの再トリガー（Re-trigger Job）]** をクリックしてジョブを再トリガーします。*[*進行中（*In Progress*）*]* および *[*作成済み（*Created*）*]* のジョブは再トリガーできません。再トリガーされたジョブが成功すると、テクニカル サポート ログ ファイルは最新のファイル セットに置き換えられます。
- **[ジョブの停止（Stop Job）]**：チェックボックスを選択し、**[アクション（Actions）]** > **[ジョブの停止（Stop Job）]** をクリックして、実行中のジョブを停止します。停止できるのは、*[*進行中（*In Progress*）*]* および *[*作成済み（*Created*）*]* のジョブのみです。
- **[ジョブの削除（Delete Job）]**：チェックボックスを選択し、**[アクション（Actions）]** > **[ジョブの削除（Delete Job）]** をクリックしてジョブを削除します。*[*進行中（*In Progress*）*]* のジョブは削除できません。

（注） 操作できる状態のジョブは、一度に削除/停止/再トリガーすることができます。

# テクニカル サポートのトリガー

この手順に従って、テクニカル サポート ジョブをトリガーします。

### 始める前に

1 つ以上のデバイスが Nexus Dashboard Data Broker に接続されており、AUX モードが無効になっていることを確認します。

デバイスに 64 MB 以上の空き容量があることを確認してください。不足していると操作は失敗し、*No Enough Space* エラーが表示されます。

### 手順

**ステップ 1** **[トラブルシューティング（Troubleshooting）]** > **[テクニカル サポート（Tech Support）]** に移動します。

**ステップ 2** **[アクション（Actions）]** > **[ジョブのトリガー（Trigger Job）]** をクリックします。

**ステップ 3** **[テクニカル サポートのトリガー（Trigger Tech Support）]** ダイアログボックスで、次の詳細を入力します。

表 *66 :* テクニカル サポートのトリガー

| フィールド | 説明 |
|---|---|
| **[トリガー設定（Trigger Settings）]** | |
| デバイス | データを収集する必要があるデバイス。<br>**[デバイスの選択（Select Device）]** をクリックし、デバイスを選択します。 |
| 操作タイプ | **[基本（Basic）]** または **[高度（Advanced）]** を選択します。<br>これらの各オプションの `show` コマンドがリストされています。 |

**ステップ 4** **[追加（Add）]** をクリックして、`show` コマンドの出力を収集します。

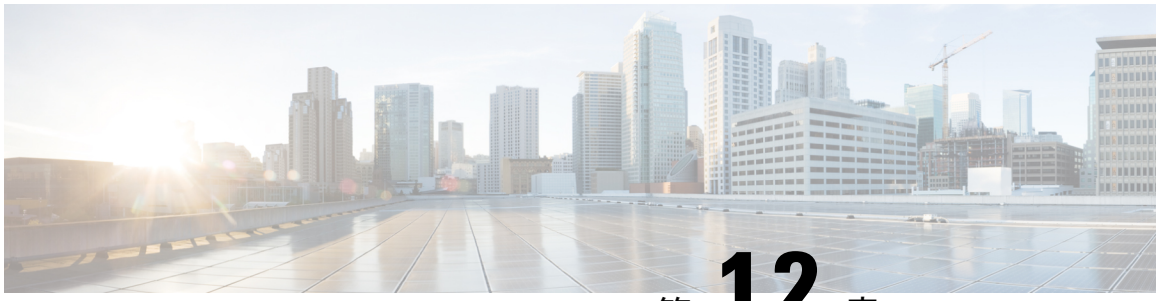
（注）
デフォルトでは、「Tech Support」フォルダの他に、「configuration」フォルダ、「configuration start up」フォルダ、および一般ログのフォルダがダウンロードされます。これにより、テクニカル サポート チームはすべての情報を収集し、より迅速な分析を行うことができます。

# テクニカル サポートの概要

NX-API デバイス機能のテクニカル サポートは、各スイッチから個別にデータを収集するのではなく、1 つまたは複数のスイッチから情報を一度に収集できます。関連するすべてのログがすぐに利用でき、ダウンロードできるため、デバッグ時に役立ちます。

スイッチからテクニカル サポート データを収集する際には、次の 2 つのモードで実行できます。

- 基本モード（Basic mode）：限定された一連の show コマンドが含まれています。
- 拡張モード（Advanced mode）：より幅広い一連の show コマンドが含まれています。:



第 12 章

# 管理

この章では、Cisco Nexus Dashboard Data Broker のプロファイルとユーザーについて詳しく説明します。

リリース 3.10.1 から、Cisco Nexus Data Broker（NDB）の名前は、Cisco Nexus Dashboard Data Brokerに変更されました。ただし、GUI およびインストール フォルダ構造と対応させるため、一部の NDB のインスタンスがこのドキュメントには残されています。NDB/ Nexus Data Broker/ Nexus Dashboard Data Brokerという記述は、相互に交換可能なものとして用いられています。



## AAA

**[AAA]** タブには、Nexus Dashboard Data Broker で使用可能な AAA サーバーの詳細が表示されます。AAA サーバーの詳細については、AAA サーバーの概要 （191 ページ） を参照してください。

次の詳細を示す表が表示されます。

| 列名 | 説明 |
|---|---|
| **Server Address** | AAA サーバの IP アドレス。 |

| 列名 | 説明 |
|---|---|
| **[プロトコル（Protocol）]** | サーバーで実行されているプロトコル。次のオプションがあります。<br>• TACACS<br>• RADIUS+<br>• LDAP |

次のアクションは、**[AAA]** タブから実行できます。

- **[サーバーの追加（Add Server）]**：これを使用して、新しいAAAサーバーを追加します。詳細な手順については、AAA サーバーの追加 （188 ページ） を参照してください。
- **[サーバーの削除（Delete Server）]**：行の先頭にあるチェックボックスをオンにして、削除するサーバーを選択し、**[アクション（Actions）]** > **[AAA サーバーの削除（Delete AAA Server）]** をクリックします。選択したサーバーが削除されます。チェックボックスを選択せずに削除アクションを選ぶと、エラーが表示されます。サーバーを選択するように求められます。

# AAA サーバーの追加

この手順に従って、AAA サーバーを追加します。

### 手順

**ステップ 1** **[管理（Administration）]** > **[AAA]** に移動します。

**ステップ 2** **[アクション]** ドロップダウン メニューから **[AAA サーバーの追加（Add AAA Server）]** を選択します。

**ステップ 3** **[AAA サーバーの追加（Add AAA Server）]** ダイアログボックスで、次の詳細を入力します。

表 *67 : AAA*サーバーの追加

| フィールド | 説明 |
|---|---|
| **[全般（General）]** | |
| プロトコル | AAA サーバーのプロトコルを選択します。<br>• RADIUS<br>• LDAP<br>• TACACS<br>各オプションに関連するフィールドについては、以下で説明します。 |

| フィールド | 説明 |
|---|---|
| プロトコル：**Radius** | |
| **[サーバー アドレス（Server Address）]** | サーバーの IP アドレスとドメイン名 |
| **[シークレット（Secret）]** | AAA サーバーで構成されたシークレット。 |
| プロトコル：**LDAP** | |
| **[サーバー アドレス（Server Address）]** | サーバーの IP アドレスとドメイン名 |
| **[ポート（Port）]** | AAA サーバーの通信ポート。 |
| **[ユーザー RDN（User RDN）]** | LDAP サーバーでの認証に使用される相対識別名（RDN） を入力します。<br>LDAP サーバーで定義されたユーザー階層です。例: AAA で LDAP を構成する場合、次の階層（LDAP で定義）を考慮してください。ユーザー「cn=admin,ou=People,dc=ndb,dc=local」の場合、ユーザー RDN は「ou=People,dc=ndb ,dc = ローカル」です。NDB が LDAP で構成された後、ログインするには、ユーザー名に *cn* 値のみを指定する必要があります。この場合、ユーザー名は「admin」になります。 |
| **[ロール属性（Role Attribute）]** | ユーザーの LDAP 認証属性であるロール属性を入力します。<br>ロール属性は、DN の LDAP 内の任意の属性にすることができます。<br>たとえば、*sn* をローカル LDAP サーバーで定義されたロール属性とします。したがって、NDB の管理者ユーザーの場合、*sn* 属性の値として「network-admin」を持つことができます。<br>NDB がロール属性とユーザー RDN および管理ユーザーを使用して LDAP サーバーに接続すると、LDAP は認証として *sn* 値（「network-admin」）を返します。 |

| フィールド | 説明 |
|---|---|
| **[ロール タイプ マッピング（Role Type Mapping）]** | デフォルト設定を有効にするために、ボタンをクリックします。**ロール マッピング**の値のリストが表示されます。**デフォルト**を有効にした場合、既存でマップされている値は次のとおりになります。<br>• ネットワーク管理者：*network-admin*<br>• ネットワークオペレータ：*network-operator*<br>• アプリケーションユーザー：*application-user*<br>• スライスユーザー：*slice-user*<br>**デフォルト**を無効にして、LDAP で定義された値を持つロールのカスタム マッピングを提供します。**[ロール マッピング（Role Mapping）]** 列のドロップダウン リストからロールを選択し、**[ロール タイプ マッピング（Role Type Mapping）]** 列に LDAP で定義された値を入力します。<br>ロール タイプ マッピングの行をさらに追加するには、**[行の追加（Add Row）]** をクリックします。 |
| **[タイムアウト（Timeout）]** | LDAP サーバーが応答するまでの最大待ち時間を入力します。 |
| プロトコル：**TACACS+** | |
| **[サーバ アドレス（Server Address）]** | TACACS+ サーバーの IP アドレス。 |
| **[シークレット（Secret）]** | TACACS+ サーバーで構成されたシークレット。 |
| **[ユーザー名（Username）]** | サーバーにログインするためのユーザー名。 |
| **パスワード（Password）** | サーバーにログインするためのパスワード。 |
| **[サーバーの確認（Check Server）]** | **[サーバーの確認（Check Server）]** をクリックして、サーバーにアクセスできるかどうか、および認証資格情報が有効かどうかを確認します。 |

（注）
ndb コントローラのユーザー管理が TACACS または AAA を介して実行されている場合、ndb コントローラの管理者パスワードを変更することはお勧めしません。

**ステップ 4** **[AAA サーバーの追加（Add AAA Servers）]** をクリックして、サーバーを追加します。

### 次のタスク

AAA サーバーのプロトコルとして RADIUS を選択した場合は、RADIUS のユーザー認証を設定する必要があります。

### ユーザー認証用の RADIUS サーバーの設定

RADIUS サーバーでのユーザー認証は、Cisco Attribute-Value（av-pair）形式に準拠している必要があります。RADIUS サーバーで、ユーザーの Cisco av-pair 属性を次のように設定します。

```
shell:roles="Network-Admin Slice-Admin"
```

# AAA サーバーの概要

AAA によって、セキュリティ アプライアンスが、ユーザーが誰か（認証）、ユーザーが何を実行できるか（認可）、およびユーザーが何を実行したか（アカウンティング）を判別することが可能になります。Cisco Nexus Dashboard Data Broker は Remote Authentication Dial-In User Service（RADIUS）または Terminal Access Controller Access Control System Plus（TACACS+）を使用して、AAA サーバーと通信します。

AAA サーバーは、リモート認証と認可をサポートします。各ユーザーを認証するために、Cisco Nexus Dashboard Data Broker はログイン クレデンシャルと属性値（AV）ペアの両方を使用します。AV ペアは、ユーザー管理の一環として、ユーザーに許可された役割を割り当てます。認証に成功すると、Cisco AV ペアは、リソース アクセス許可のために Cisco Nexus Dashboard Data Broker に返されます。

# バックアップ/復元

**[バックアップ/復元（Backup/Restore）]** タブから、次のアクションを実行できます。

- **ローカルにバックアップ（Backup Locally）**：設定はローカル マシンにバックアップされます。
- **[ローカルに復元（Restore Locally）]**：表示される **[ローカルに復元（Restore Locally）]** ウィンドウで、**[ファイルの選択（Choose a file）]** をクリックし、ローカル マシンからファイルを選択して構成を復元します。

  Nexus Dashboard Data Broker の再起動後にアップロードされたバックアップを基に、Nexus Dashboard Data Broker でデバイスの構成を再構成する場合は、**[復元（Restore）]** チェックボックスを選択します。次の構成が再構成されます。

  - グローバル設定
  - ポート設定
  - UDF
  - Connections

（注） バックアップ/復元は、Nexus Dashboard Data Broker リリース 3.10.4 および 4.0 でのみサポートされます。つまり、リリース 3.10.4 からリリース 4.0 またはリリース 4.0 から 4.0 への復元がサポートされることを意味します。

4.0 リリースのバックアップを復元すると、TLS トラストストアとキーストア ファイルが自動的にバックアップの一部になります。リリース 3.10.4 から 4.0 にアップグレードするには、プロンプトが表示されたらトラストストア ファイルとキーストア ファイルをアップロードし、**[復元（Restore）]**をクリックする必要があります。復元中の場合、「復元中です。更新しないでください。」というバナーが表示されます。

# バックアップのスケジュール

**[バックアップのスケジュール（Schedule of Backups）]** タブには、Nexus Dashboard Data Broker コントローラのスケジュールされたバックアップの詳細が表示されます。

詳細を記した次の表が表示されます。

**表 *68 :* バックアップ**

| 列名 | 説明 |
|---|---|
| **開始日（Start Date）** | バックアップの開始日。 |
| **開始時刻（Start Time）** | バックアップの開始時刻。 |
| **終了日（End Date）** | バックアップの終了日。 |
| **パターン（Pattern）** | バックアップ パターン。次のオプションがあります。<br>• 毎日<br>• 毎週<br>• 毎月 |
| **発生回数（Occurrences）** | 選択したパターンに基づく発生数。 |

**[バックアップ（Backup）]** タブから、次のアクションを実行できます。

- **バックアップのスケジュール（Schedule Backup）**：これを使用して、バックアップをスケジュールします。バックアップのスケジュール作成（193 ページ）を参照してください。
- **ローカルにバックアップ（Backup Locally）**：設定はローカル マシンにバックアップされます。
- **[ローカルに復元（Restore Locally）]** — 表示される **[ローカルに復元（Restore Locally）]** ウィンドウで、ローカル マシンからファイルを選択して構成を復元します。

Nexus Dashboard Data Broker の再起動後にアップロードされたバックアップを基に、Nexus Dashboard Data Broker でデバイスの構成を再構成する場合は、**[復元（Restore）]** チェックボックスを選択します。次の構成が再構成されます。

- グローバル設定
- ポート設定
- UDF
- Connections

**[復元（Restore）]** チェックボックスは、NDB リリース 3.8 以降からダウンロードした構成にのみ適用できます。

## バックアップのスケジュール作成

この手順に従って、バックアップをスケジュールします。

Nexus Dashboard Data Broker の次のバージョンにアップグレードする前に、必ずバックアップを作成することをお勧めします。

### 手順

**ステップ 1** **[管理（Administration）]** > **[バックアップ/復元（Administration）]** に移動します。

**ステップ 2** **[アクション（Actions）]** ドロップダウンリストから、**[バックアップのスケジュール作成（Schedule Backup）]** を選択します。

**ステップ 3** **[バックアップのスケジュール作成（Schedule Backup）]** ダイアログボックスで、次の詳細を入力します。

*表 69 : Schedule Backup*

| フィールド | 説明 |
|---|---|
| **[スケジュール（Schedule）]** | |
| 開始日 | バックアップの開始日。 |
| **[開始時刻（Start Time）]** | バックアップの開始時刻を入力します。 |

| フィールド | 説明 |
|---|---|
| 繰り返し | 次のいずれかのオプションを選択します。<br>• **[毎日（Daily）]**：バックアップ操作は毎日行われます。<br>• **[毎週（Weekly）]**：バックアップ操作は、毎週、選択した曜日に実行されます。<br>• **[毎月（Monthly）]**：バックアップ操作は、毎月、選択した日に開始されます。<br>（注）<br>選択した月の末日までにバックアップを実行するには、**[最終日（Last Day）]** チェックボックスをオンにします。 |
| **[終了（End）]** | バックアッププロセスの停止に関する次のいずれかのオプションを選択します。<br>• **[終了日なし（No End Date）]**：バックアップはずっと継続します。<br>• **[終了日（End Date）]**：バックアップは指定された終了日まで継続します。<br>• **[発生（Occurrences）]** — **[発生数（Number of Occurrences）]** フィールドで選択した数に基づいてバックアップを実行します。 |
| **[有効化（Enable）]** | **[有効化（Enable）]** チェックボックスはデフォルトでオンになっています。スケジュールに従ってバックアップを有効にするには、チェックボックスをオンのままにします。 |

**ステップ 4** **[スケジュール（Schedule）]** をクリックします。

# バックアップ

**[バックアップ（Backups）]** タブにはバックアップ情報が表示されます。

ここに表示される情報は、Scheduling Backup を使用して生成されたスケジュールに基づいています。次の詳細を示す表が表示されます。

| 列名 | 説明 |
|---|---|
| 品目 | バックアップの時間。 |
| **[クラスタ バックアップ ステータス（Cluster Backup Status）]** | Nexus Dashboard Data Broker コントローラのクラスタ バックアップ ステータス。次のオプションがあります。<br>• 成功<br>• 失敗 |
| 説明 | バックアップの説明。 |
| **[復元トリガー（Restore Triggers）]** | 復元バックアップがトリガーされたときのタイムスタンプ。 |

**[バックアップ（Backups）]** タブからは次のアクションを実行できます。

- **[NDB サーバーへのバックアップ（Backup to NDB Server）]**：NDB サーバーで指定された時刻にバックアップが作成されます。このオプションを選択すると、バックアップの詳細が **[バックアップ（Backups）]** タブに表示されます。
- **[バックアップの復元（Restore Backup）]**：選択したバックアップが、Nexus Dashboard Data Broker コントローラで復元されます。復元には常に最新のバックアップを選択することをお勧めします。古いバックアップを選択すると、最近のトポロジの変更のため接続エラーが発生する可能性があります。

（注） バックアップを復元した後には、Nexus Dashboard Data Broker コントローラを再起動してください。

- **[バックアップの削除（Delete Backup）]**：行の先頭にあるチェックボックスをオンにして、削除するバックアップを選択し、**[アクション（Actions）]** > **[バックアップの削除（Delete Backup(s)）]** をクリックします。

# Transport Layer Security

リリース 3.10.5 から、 GUI を使用して Transport Layer Security（TLS）を有効にできます。証明書を持つ KeyStore と TrustStore がすでにある場合は、TLS ファイルのアップロード （196 ページ） の手順を参照してください。

# TLS ファイルのアップロード

この手順を使用して、既存のKeyStoreおよびTrustStoreファイルをデータ ブローカ コントローラと同期します。

### 始める前に

キーストアとトラストストアのファイルを準備します。

### 手順

**ステップ 1** **[管理** （Administration）] > **[TLS]** > **[アクション（Actions）]** > **[TLS ファイルのアップロード（Upload TLS Files）]**の順に選択します。

**ステップ 2** 表示される **[トランスポート層セキュリティの有効化（Enable Transport Layer Security）]** 画面で、次のように入力します。

- 有効化メソッド：サーバまたはローカル パスからアップロードできます。
- KeyStore：KeyStore ファイルをドラッグ アンド ドロップします。
- Password：キーストア ファイルのパスワードを入力します。
- TrustStore：TrustStore ファイルをドラッグ アンドドロップします。
- パスワード：TrustStore ファイルのパスワードを入力します。

**ステップ 3** **[保存（Save）]** をクリックします。

# Cluster

**[クラスタ（Cluster）]** タブには、Nexus Dashboard Data Broker コントローラで使用可能なクラスタの詳細が表示されます。Nexus Dashboard Data Broker は、クラスタ内に最大 5 つのコントローラを使用したアクティブ/アクティブ モードでの高可用性クラスタリングをサポートします。

次の詳細を示す表が表示されます。

| 列名 | 説明 |
|---|---|
| コントローラ | コントローラの IP アドレス。 |
| タイプ | 表示されるオプションは、**[プライマリ（Primary）]** または **[メンバー（Member）]** です。 |

（注） バックアップおよびアップロード機能を正しく動作させるには、クラスタ内のすべてのサーバーを停止してから再起動する必要があります。この間、機能を構成しないでください。いったんアップロード構成が完了したら、データの不整合につながる可能性があるため、クラスタ内の他のノードからは何も構成しないでください。

（注） バックアップがアップロードされたら、クラスタのすべてのインスタンスをシャットダウンし、バックアップがアップロードされるサーバーを最初に起動する必要があります。

# プロファイル

**[プロファイル（Profiles）]** タブには、Nexus Dashboard Data Broker コントローラで使用可能なプロファイルの詳細が表示されます。プロファイルを使用すると、Nexus Dashboard Data Broker コントローラに関連付けられた複数のデバイスを管理できます。複数のデバイスをプロファイルに接続できます。

プロファイル構成は、すべてのメンバー スイッチに適用されます。

次の詳細を示す表が表示されます。

| 列名 | 説明 |
|---|---|
| **プロファイル名（Profile Name）** | プロファイルの名前。 |
| **ユーザ名** | プロファイルを作成したユーザー名。 |

*[*属性によるフィルタ処理（*Filter by attributes*）*]* バーを使用して、表示されているフィルタの詳細に基づいてテーブルをフィルタ処理します。属性、演算子、およびフィルタ値を選択します。

**[プロファイル（Profile）]** タブから、次のアクションを実行できます。

- **[プロファイルの追加（Add Profile）]**：これを使用して、新しいプロファイルを追加します。このタスクの詳細については、プロファイルの追加を参照してください。
- **[プロファイルの削除（Delete Profile）]**：行の先頭にあるチェックボックスをオンにして必要なプロファイルを選択し、**[プロファイルの削除（Delete Profile）]** をクリックします。選択したプロファイルが削除されます。チェックボックスを選択せずに削除アクションを選ぶと、エラーが表示されます。プロファイルを選択するように求められます。

（注） 使用中のプロファイルは削除できません。

# プロファイルの追加

この手順に従って、新しいプロファイルを追加します。

### 手順

**ステップ 1** **[管理（Administration）]** > **[プロファイル（Profile）]** に移動します。

**ステップ 2** **[アクション（Actions）]** ドロップダウン メニューから **[プロファイルの追加（Add Profile）]** を選択します。

**ステップ 3** **[プロファイルの追加（Add Profile）]** ダイアログ ボックスに次の詳細を入力します。

表 *70 :* プロファイルの追加

| フィールド | 説明 |
|---|---|
| プロファイル名（**Profile Name**） | プロファイル名を入力します。 |
| **Username** | デバイスにログインするためのユーザー名を入力します。 |
| パスワード | ユーザー名に対してパスワードを入力します。<br>パスワードは 8 ～ 256 文字の長さで、大文字と小文字を含み、少なくとも 1 個の数字と、少なくとも 1 個の英数字以外の文字を含む必要があります。 |

**ステップ 4** **[プロファイルの追加（Add Profile）]** をクリックして新しいプロファイルを作成します。

# プロファイルの編集

プロファイルを編集するには、次の手順に従います。

（注） プロファイルを編集すると、そのプロファイルを使用しているデバイスが再接続されます。

### 始める前に

1 つ以上のプロファイルを作成します。

### 手順

**ステップ 1** **[管理（Administration）]** > **[プロファイル（Profile）]** に移動します。

**ステップ 2** 表示された表で、**プロファイルの名前**をクリックします。

新しいペインが右側に表示されます。

**ステップ 3** **[アクション（Actions）]** をクリックし、**[プロファイルの編集（Edit Profile）]** を選択します。

**ステップ 4** **[プロファイルの編集（Edit Profile）]** ダイアログ ボックスに、現在のプロファイル情報が表示されます。これらのフィールドを必要に応じて変更します。

**表 *71* : プロファイルの編集**

| フィールド | 説明 |
|---|---|
| **プロファイル名（Profile Name）** | プロファイル名が表示されます。変更はできません。 |
| **Username** | デバイスにログインするためのユーザー名を入力します。 |
| **パスワード** | ユーザー名に対してパスワードを入力します。<br>パスワードは 8 ～ 256 文字の長さで、大文字と小文字を含み、少なくとも 1 個の数字と、少なくとも 1 個の英数字以外の文字を含む必要があります。 |

**ステップ 5** **[ 保存（Save）]** をクリックしてプロファイルを編集します。

# スライス

**[スライス（Slices）]** タブには、Nexus Dashboard Data Broker で使用できるスライスの詳細が表示されます。

スライスを使用すると、ネットワークを多数の論理ネットワークに分割できます。詳細については、スライスについて （202 ページ）を参照してください。

別のネットワーク パーティションを表示するには、ヘッダーの **[スライス（Slices）]** ボタンを使用してスライスを切り替えます。初期の Nexus Dashboard Data Broker ビルドの一部として、1 つのスライスが使用可能になっており、**デフォルト** スライスと呼ばれます。次の構成は、Nexus Dashboard Data Broker コントローラーのデフォルト スライスでのみ実行できます。

- 新しいデバイスの追加
- デバイスのグローバル構成の編集
- ユーザのプロファイルの変更
- ユーザおよび関連付けられたロールのパラメータの変更
- 矛盾のあるないデバイスと接続フローの修正

次の詳細を示す表が表示されます。

| 列名 | 説明 |
|---|---|
| スライス | スライスの名前。<br>このフィールドはハイパーリンクです。**スライス**の名前をクリックすると、右側に新しいペインが表示されます。ここから実行できる追加のアクション：<br>• スライスの編集 |
| ポートの構成 | 現在スライスの一部であるデバイス（または複数の異なるデバイス）のポート。 |
| **[利用可能なポート（Available Port(s)）]** | 現在スライスの一部ではないが、スライスに追加できるデバイス（または複数の異なるデバイス）のポート。 |

**[スライス（Slices）]** タブでは、次のアクションを実行できます。

- **[スライスの追加（Add Slice）]**：このアクションの詳細については、スライスの追加を参照してください。
- **[スライスの削除（Delete Slice）]**：削除するスライスを選択し、**[アクション（Actions）]** > **[スライスの削除（Delete Slice(s)）]** をクリックします。チェックボックスを選択せずに削除アクションを選択すると、エラーが表示され、スライスを選択するように求められます。

# スライスの追加

この手順に従って、スライスを追加します。

（注） デバイスは複数のスライスの一部にすることができます。ポートは、任意の時点で1つのスライスの一部にしかなれません。

### 始める前に

デバイスのポートを新しいスライスに追加する前に、すでにデフォルトスライスの一部であるデバイスのすべてのポート構成と接続をクリアします。

手順

**ステップ 1** **[管理（Administration）]** > **[スライス（Slices）]** に移動します。

**ステップ 2** **[アクション（Actions）]** ドロップダウン メニューから **[スライスの追加（Add Slice）]** を選択します。

**ステップ 3** **[スライスの追加（Add Slice）]** ダイアログボックスで、次の詳細を入力します。

表 *72:* スライスの追加

| フィールド | 説明 |
|---|---|
| **[全般（General）]** | |
| **[ スライス名（Slice Name）]** | スライスの名前を入力します。 |
| **[ポート（Port）]** | **[ポートの選択（Select Ports）]** をクリックし、**[ポートの選択（Select Ports）]** ウィンドウでデバイスと必要なポートを選択します。<br>（注）<br>デバイスのすべてのポートが同じスライス上にあることを確認してください。 |

**ステップ 4** **[スライスの追加（Add Slice）]** をクリックして、スライスを作成します。

（注）
新しいスライスが追加されると、デフォルトのスライスは読み取り専用モードになります。アクティブなポート構成や接続がデフォルトのスライスに存在する場合、それは使用不可になります。

スライスに追加されたデバイスがスライスに表示されます。たとえば、デバイス D1 がスライス S1 に追加され、デバイスが保守モード（または障害状態または未準備状態）になると、デバイスはS1に表示されなくなり、デフォルトのスライスに表示されます。

# スライスの編集

スライスを編集するには、この手順に従います。

### 始める前に

スライスからポートを削除する前に、ポートのポート構成を削除してください。

手順

**ステップ 1** **[管理（Administration）]** > **[スライス（Slices）]** に移動します。

**ステップ 2** スライスの名前をクリックします。右側に新しいウィンドウが開きます。

**ステップ 3** **[アクション（Actions）]** > **[スライスの編集（Edit Slice）]** をクリックします。

**[スライスの編集（Edit Slice）]** ウィンドウが表示されます。

**ステップ 4** **[スライスの編集（Edit Slice）]** ウィンドウで必要な変更を行います。次の詳細情報が表示されます。

表 *73 :* スライスの編集

| フィールド | 説明 |
|---|---|
| **[全般（General）]** | |
| **[ スライス名（Slice Name）]** | スライスの名前。このフィールドは変更できません。 |
| **[ポート（Port）]** | スライスの一部であるポートが一覧表示されます。必要に応じて削除/追加できます。 |

**ステップ 5** **[保存（Save）]** をクリックします。

# スライスについて

スライスを使用すると、ネットワークを多数の論理ネットワークに分割できます。この機能により、複数の切り離されたネットワークを作成し、それぞれに異なるロールとアクセス レベルを割り当てることができます。各論理ネットワークは、部門、個人のグループ、またはアプリケーションに割り当てることができます。切り離された複数のネットワークは、Cisco Nexus Dashboard Data Broker アプリケーションを使用して管理できます。

スライスは、次の基準に基づいて作成されます。

- ネットワーク デバイス：スライスに使用できるデバイス。ネットワーク デバイスはスライス間で共有できます。
- ネットワーク デバイス インターフェイス：スライスに使用できるデバイス インターフェイス。ネットワーク デバイス インターフェイスはスライス間で共有できます。

スライスは、ネットワーク管理者ロールを持つ Cisco Nexus Dashboard Data Broker ユーザーが作成する必要があります。作成後、スライスは Slice Administrator ロールを持つユーザーが管理できます。

# システム情報

**[システム情報（System Information）]** タブには、Nexus Dashboard Data Broker コントローラおよび Nexus Dashboard Data Broker コントローラ ホストに関するすべての情報が表示されます。この情報は、次の 2 つの見出しの下にあります。

- **[NDB 情報（NDB Information）]**：インストール タイプ、現在のビルド番号、以前のビルド番号などの情報が含まれます。
- **[システム情報（System Information）]**：Nexus Dashboard Data Broker コントローラ ホストの合計メモリ、物理メモリ、使用済みメモリ、空きメモリなどの情報が含まれます。

# ユーザ管理

**[ユーザー管理（User Management）]** タブには、次のサブタブがあります。

- **[ユーザー（Users）]**：Nexus Dashboard Data Broker コントローラーのユーザー。詳細については、ユーザーを参照してください。
- **[ロール（Roles）]**：ユーザーが割り当てられているロール。詳細については、ロールを参照してください。
- **[グループ（Groups）]**：ポートが割り当てられているデバイス グループ。詳細については、グループを参照してください。

## ユーザー

**[ユーザー（Users）]** タブには、Nexus Dashboard Data Broker コントローラのユーザーの詳細が表示されます。

次の詳細を示す表が表示されます。

| 列名 | 説明 |
|---|---|
| ユーザー | ユーザーのログイン名。<br>このフィールドはハイパーリンクです。**ユーザー**をクリックすると、新しいペインが右側に表示されます。次の追加アクションがここで実行できます。<br>• パスワードの変更<br>• 役割の変更<br>• **ユーザーの削除**<br>（注）<br>デフォルトの管理者ユーザーとしてログインしている場合、**[ユーザーの削除（Delete User）]**および**[ロールの変更（Change Role）]**オプションは使用できません。TACACS を使用してログインしている場合、**[パスワードの変更（Change Password）]**オプションは使用できません。 |
| ロール | ユーザーの作成中に割り当てられたユーザーのロール。 |

**[ユーザー（Users）]** タブから次のアクションを実行できます。

- **[ユーザーの追加（Add User）]**：これを使用して、新しいユーザーを追加します。このタスクの詳細については、ユーザーの追加を参照してください。
- **[ユーザーの削除（Delete User）]**：行の先頭にあるチェックボックスをオンにして、削除するユーザーを選択し、**[ユーザーの削除（Delete User）]** をクリックします。選択したユーザーが削除されます。チェックボックスを選択せずに削除アクションを選ぶと、エラーが表示されます。ユーザーを選択するように求められます。

## ユーザーの追加

この手順に従って、新しいユーザを追加します。

### 始める前に

新しいユーザに割り当てることができるロールを作成します。

### 手順

**ステップ 1** **[管理（Administration）]** > **[ユーザ管理（User Management）]** > **[ユーザ（User）]** に移動します。

**ステップ 2** **[アクション（Actions）]** ドロップダウン メニューから **[ユーザの追加（Add User）]** を選択します。

**ステップ 3** **[ユーザーの追加（Add User）]** ダイアログボックスで、次の詳細を入力します。

表 *74 :* ユーザの追加

| フィールド | 説明 |
|---|---|
| **[ユーザ名（Username）]** | ユーザ名を入力します。 |
| **パスワード** | ユーザのパスワードを入力します。<br>パスワードは 8 ～ 256 文字の長さで、大文字と小文字を含み、少なくとも 1 つの数字と、少なくとも 1 つの英数字以外の文字を含む必要があります。 |
| **パスワードの確認** | パスワードを再入力して確認します。 |
| **[ユーザ タイプの選択（Choose User Type）]** | 次のいずれかのオプションを選択します。<br>• **[通常ユーザ（Regular User）]** : スライスのない NDB コントローラにログインできます（デフォルトのスライス）。<br>• **[スライス ユーザ（Slice User）]** : 特定のスライスにのみアクセスできます。 |
| **[スライスを選択（Select Slice）]**<br>このフィールドは、ユーザ タイプが**スライス ユーザ**の場合にのみ適用されます。 | ドロップダウン リストからデバイスを選択します。作成されたユーザは、選択したスライスにのみアクセスできます。 |
| **[ロールの設定（Set Role）]**<br>このフィールドは、ユーザ タイプが**通常ユーザ**の場合にのみ適用されます。 | **[ロールの選択（Select Role）]** を選択します。表示される **[ロールの選択（Select Rols）]** ダイアログボックスで、ユーザに割り当てるロールのチェックボックスをオンにします。ロールの詳細が右側に表示されます。**[選択（Select）]** をクリックしてロールを割り当てます。特定のユーザーに複数のロールを割り当てることができます。<br>使用可能なロール オプションは次のとおりです。<br>• ネットワーク管理者（Network Admin）：すべてのアプリケーションに対する完全な管理者権限を提供します。<br>• ネットワーク オペレータ（Network Operator）：すべてのアプリケーションに読み取り専用権限を提供します。 |

**ステップ 4** **[ユーザの追加（Add User）]** をクリックして、新しいユーザを追加します。

（注）
ユーザを作成した後で、パスワードは変更できますが、ユーザに割り当てられたロールは変更できません。

## ユーザーのパスワードの変更

ユーザーのパスワードを変更するには、次の手順に従います。

### 始める前に

1 人以上のユーザーを作成します。

### 手順

**ステップ 1** **[管理（Administration）]** > **[ユーザー管理（User Management）]** > **[ユーザー（Users）]** に移動します。

**ステップ 2** **ユーザー**の名前をクリックします。右側に新しいウィンドウが開きます。

**ステップ 3** **[アクション（Action）]** > **[パスワードの変更（Change Password）]** をクリックします。

**[パスワードの変更（Change Password）]** ウィンドウが表示されます。

**ステップ 4** **[パスワードの変更（Change Password）]** ウィンドウで必要な変更を行います。次の詳細情報が表示されます。

表 *75 :* パスワードの変更

| フィールド | 説明 |
|---|---|
| **[全般（General）]** | |
| **[ユーザー名（ User Name）]** | ユーザ名。このフィールドは変更できません。 |
| **[現在のパスワード（Current Password）]** | ユーザーの現在のパスワードを入力します。<br>（注）<br>このフィールドは、管理者ユーザーにのみ表示されます。 |
| **パスワード（Password）** | 新しいパスワードを入力します。 |
| **[パスワードの確認（Verify）]** | 再度、新しいパスワードを入力します。 |

**ステップ 5** **[パスワードを変更（Change Password）]** をクリックします。

# ユーザーの役割の変更

ユーザーのロールを変更するためには、次の手順を使用します。

### 始める前に

1 人以上のユーザーを作成します。

### 手順

**ステップ 1** **[管理（Administration）]** > **[ユーザー管理（User Management）]** > **[ユーザー（Users）]** に移動します。

**ステップ 2** **ユーザー**の名前をクリックします。右側に新しいウィンドウが開きます。

**ステップ 3** **[アクション（Action）]** > **[ロールの変更（Change Role）]** をクリックします。

**[ロールの変更（Change Role）]** ウィンドウが表示されます。

**ステップ 4** **[ロールの変更（Change Role）]** ウィンドウで必要な変更を行います。次の詳細情報が表示されます。

表 *76 :* 役割の変更

| フィールド | 説明 |
|---|---|
| **[全般（General）]** | |
| **[ユーザー名（ User Name）]** | ユーザ名。このフィールドは変更できません。 |
| **ユーザー タイプの選択** | **[通常ユーザー（Regular User）]** または **[スライス ユーザー（Slice User）]**のいずれかを選択します。 |
| **[スライスを選択（Select Slice）]** | ドロップダウン リストからオプションを選択します。<br>このオプションは、ユーザー タイプの選択が **[スライス ユーザー（Slice User）]** の場合にのみ表示されます。 |
| **[ロールの選択（Select Role）]** | **[ロールの選択（Select Role）]** をクリックすると、**[ロールの選択（Select Role）]** ウィンドウが表示されます。ラジオボタンを使用してロールを選択し、**[選択（Select）]** をクリックします。<br>このオプションは、ユーザー タイプの選択が **[通常のユーザー（Regular User）]** である場合にのみ表示されます。 |

**ステップ 5** **[保存（Save）]** をクリックします。

# ロール（Roles）

**[ロール（Roles）]** タブには、Nexus Dashboard Data Broker コントローラで使用可能なロールの詳細が表示されます。デフォルトのロールは次のとおりです。

- Network-Admin
- network-operator

票には次の詳細が表示されます。

| 列名 | 説明 |
|---|---|
| ロール | ロールの名前。<br>表示名はハイパーリンクです。**ロール**の名前をクリックすると、右側に新しいペインが表示されます。ここから実行できる追加アクションは次のとおりです。<br>• グループの割り当て |

| 列名 | 説明 |
| --- | --- |
| レベルの設定 | 役割に割り当てられたレベルです。次のレベルが利用可能です。<br>• アプリ管理者（App-Administrator）：すべてのデータ ブローカー リソースへのフル アクセス権がありますが、App-Administrator には、NXAPI または実稼働デバイスを Nexus Dashboard Data Broker に追加することはできません。[管理（Administration）] タブが App-Administrator ロール用の Nexus Dashboard Data Broker で使用できないためです。<br>• アプリユーザー（App-User）：自分のリソース グループに割り当てられている接続とリダイレクト、および同様の権限を持つ別のユーザーによって作成されたリソースを作成、編集、複製、または削除するアクセス権があります。アプリユーザーは、Edge-SPAN、タップ、監視デバイス、および本番ポートのみを表示できます。<br>アプリ ユーザーは、Nexus ダッシュボード データ ブローカーのトポロジ ページで、同様の権限を持つ別のユーザーによって作成されたリソースを表示できます。ただし、Edge-SPAN または別のアプリユーザーによって作成された接続を構成することはできません。<br>• アプリオペレータ（App-Operator）：読み取り専用操作にアクセスできます。 |
| **[グループ（Group）]** | ロールに割り当てられたグループ。 |

**[ロール（Roles）]** タブから、次のアクションを実行できます。

- **[ロールの追加（Add Role）]**：これを使用して、新しいロールを追加します。このタスクの詳細については、ロールの追加を参照してください。
- **[ロールの削除（Delete Role）]**：行の先頭にあるチェックボックスをオンにして削除するロールを選択し、**[アクション（Actions）]** メニューから **[ロールの削除（Delete Role）]** をクリックします。チェックボックスを選択せずに削除アクションを選ぶと、エラーが表示されます。ロールを選択するように求められます。

（注） デフォルト ロールは削除できません。

## ロールの追加

以下の手順に従い、ロールを追加し、そのロールをグループに関連付けます。

### 始める前に

ロールに関連付ける 1 つ以上のグループを作成します。

### 手順

**ステップ 1** **[管理（Administration）] > [ユーザー管理（User Management）] > [ロール（Roles）]** に移動します。

**ステップ 2** **[アクション（Actions）]** ドロップダウン メニューから **[ロールの追加（Add Role）]** を選択します。

**ステップ 3** **[ロールの追加（Add Role）]** ダイアログボックスで、次の詳細を入力します。

表 *77:* ロールの追加

| フィールド | 説明 |
|---|---|
| **[ロール名（Role Name）]** | ロール名を入力します。 |
| **レベルの選択** | ドロップダウン リストからレベルを選択します。 |

**ステップ 4** **[追加（Add）]** をクリックしてロールを追加します。

## ロールへのグループの割り当て

この手順を使用して、グループをロールに割り当てます。これにより、ロールは割り当てられたグループのポートのみにアクセスできます。

### 始める前に

1 つ以上のグループを追加します。

### 手順

**ステップ 1** **[管理（Administration）] > [ユーザー管理（User Management）] > [ロール（Roles）]** に移動します。

**ステップ 2** 表示されたテーブルで**ロール**の名前をクリックします。

新しいペインが右側に表示されます。

**ステップ 3** **[アクション（Actions）]** > **[グループの割り当て（Assign Group）]** をクリックします。

次の詳細を入力します。

表 *78 :* グループの割り当て

| フィールド | 説明 |
|---|---|
| **ロール名（Role Name）** | ロール名。このフィールドは編集できません。 |
| **[レベルの選択（Select Level）]** | ロールのレベル。このフィールドは編集できません。 |
| **[グループの設定（Set Groups）]** | **[グループの選択（Select Group）]** をクリックし、表示される **[グループの選択（Select Group）]** ウィンドウでグループを選択します。 |

**ステップ 4** **[割り当て（Assign）]** をクリックします。

# グループ

**[グループ（Group）]** タブには、ポート グループの詳細が表示されます。デフォルトのグループは次のとおりです。

- allPorts

グループは、1 つのデバイスまたは多数のデバイスにまたがるポートのグループにすることができます。

次の詳細を示す表が表示されます。

| 列名 | 説明 |
|---|---|
| **[グループ（Group）]** | グループの名前。<br>表示名はハイパーリンクです。名前をクリックすると、グループの詳細が表示されます。 |
| **[ポート（Ports）]** | グループに割り当てられたポートの数。 |

**[グループ（Group）]** タブから、次のアクションを実行できます。

- **[グループの追加（Add Group）]**：これを使用して、新しいグループを追加します。詳細については、グループの追加を参照してください。
- **[グループの削除（Delete Group）]**：行の先頭にあるチェックボックスをオンにして削除するグループを選択し、**[アクション（Action）]** メニューから **[グループの削除（Delete Group）]** をクリックします。チェックボックスを選択せずに削除アクションを選ぶと、エラーが表示されます。グループを選択するように求められます。

（注） デフォルト グループは削除できません。

## グループの追加

新しいグループを作成するには、次の手順を実行します。

ユーザーのポートへのアクセスを定義するためのグループが作成されます。グループはロールに割り当てられます。ユーザーはロールに関連付けられます。

### 手順

**ステップ 1** **[管理（Administration）] > [ユーザー管理（User Management）] > [グループ（Groups）]** に移動します。

**ステップ 2** **[アクション（Actions）]** ドロップダウン メニューから **[グループの追加（Add Group）]** を選択します。

**ステップ 3** **[グループの追加（Add Group）]** ダイアログ ボックスから、次の詳細を入力します。

表 *79* : グループの追加

| フィールド | 説明 |
|---|---|
| **[グループ名（Group Name）]** | グループ名を入力します。 |
| 選択したポート | **[ポートの選択（Select Ports）]** をクリックします。表示された **[ポートの選択（Select Ports）]** ダイアログ ボックスで、チェック ボックスをオンにして、ポートをグループに割り当てます。ポートの詳細が右側に表示されます。**[選択（Select）]** をクリックしてポートを割り当てます。 |

**ステップ 4** **[グループの追加（Add Group）]** をクリックして、グループを追加します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。