Cisco Nexus Dashboard Data Broker 構成ガイド、リリース 3.10.1

初版：2021 年 7 月 6 日

最終更新：2021 年 10 月 25 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: http://www.cisco.com/go/softwareterms.Cisco product warranty information is available at http://www.cisco.com/go/warranty. US Federal Communications Commission Notices are found here http://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.

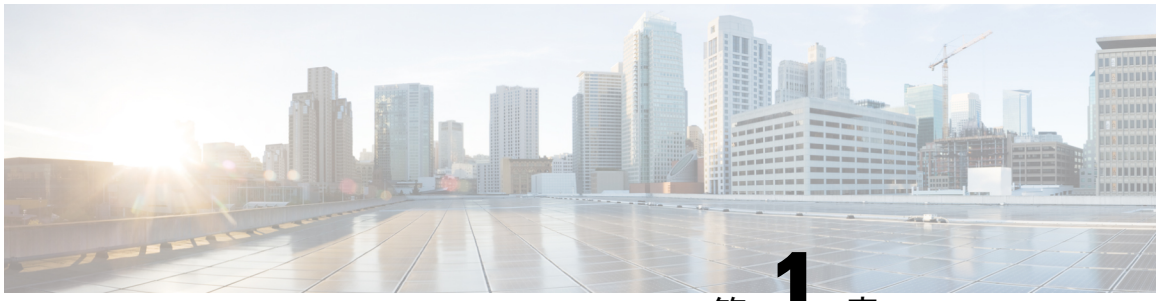
Any products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability 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: www.cisco.com go trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Trademarks



第 1 章

新機能と変更情報

新機能と変更情報

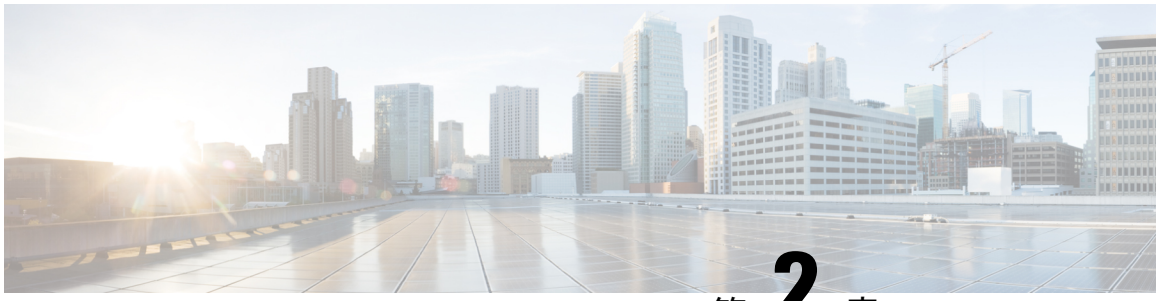
この章では、『Cisco Nexus Dashboard Data Broker 構成ガイド、リリース 3.10.1』に記載されている新機能および変更された機能に関するリリース固有の情報について説明します。

表 *1*：新機能および変更された機能

特長	説明	参照先
Cisco Nexus Dashboard および Cisco APIC 上のサービスとしての Cisco Nexus Dashboard Data Broker	Cisco Nexus Dashboard Data Broker は、Cisco Nexus Dashboard（ND）の一部となり、NetOps がプログラムによって完全なフローの集約を管理し、フィルタリングし、カスタム分析ツールに転送できるようになりました。 Cisco Nexus Dashboard Data Broker は、Cisco APIC でホストできます。ホスト APIC は、Cisco Nexus Dashboard Data Broker によって自動検出されます。	Cisco APIC および Cisco Nexus Dashboard でのサービスとしての Cisco Nexus Dashboard Data Broker
Cisco Nexus 3550-F Fusion L1 プラットフォームのサポート	Cisco Nexus Dashboard Data Broker の GUI から、Cisco Nexus 3550-F Fusion L1 プラットフォームを光タップ スイッチとして管理および設定できます。	タップ デバイス （102 ページ）および タップ構成 （181 ページ）

新機能と変更情報

特長	説明	参照先
実稼働スイッチとしてのCisco Catalystスイッチのサポート	Cisco Catalyst 9300 シリーズ スイッチを実稼働デバイスとして直接オンボードできます。これらは、ローカル スパンとして設定できます。	デバイスのスパン （96 ページ）
Cisco Digital Network Architecture Center(DNA-C)との統合	DNAC との Cisco Nexus Dashboard Data Broker コントローラの統合により、エンタープライズ スイッチのスパンを管理します。	Cisco Nexus Dashboard Data Broker と Cisco DNA Center の統一 （102 ページ）
Cisco Nexus Data Broker から Cisco Nexus Dashboard Data Broker へのブランド変更	リリース 3.10.1 以降、Cisco Nexus Data Broker (NDB) は Cisco Nexus Dashboard Data Broker に名前が変更されました。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。	このドキュメント全体。



第 2 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 以降、Cisco Nexus Data Broker (NDB) は Cisco Nexus Dashboard Data Broker に名前が変更されました。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 の基本的な顕著な機能:

- 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 と 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。
- ペイロードを破棄するための指定されたバイト数を超えるパケットの切り捨て。
- 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。
- タップ/スパン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。
- 複数の分断された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 *2:* サポートされる機能

機能名	**Cisco Nexus 9200** **C92304QC、** **C92160YC**	**Cisco Nexus 9300（第 1 世代）** **C93128TX、** **C9396TX**	**Cisco Nexus 9300（EX、FX、FX2）** **C93180LC-EX、** **C93180YC-EX、** **C93108TC-EX、** **C93108TC-FX、** **C93180YC-FX、** **C9336C-FX2、** **C93240YC-FX2、** **C93360YC-FX2**
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	Y	Y	Y
MPLS 除去- ラベル	N	Y	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	N	Y
Jumbo MTU	Y	Y	Y
NetFlow	N	N	Y
Q-in-Q タグ付け（タップおよびスパン入力ポート用)	N	Y	Y
スパン宛先	Y	Y	Y
タイムスタンプ機能	Y	N	Y
パケットの切り捨て	N	N	Y
タイムスタンプ ストリップ	Y	N	Y

機能名	Cisco Nexus 9200 C92304QC、 C92160YC	Cisco Nexus 9300（第 1 世代） C93128TX、 C9396TX	Cisco Nexus 9300（EX、FX、FX2） C93180LC-EX、 C93180YC-EX、 C93108TC-EX、 C93108TC-FX、 C93180YC-FX、 C9336C-FX2、 C93240YC-FX2、 C93360YC-FX2
入力ポート - タップ/スパン	Y	Y	Y
ローカル モニタリング ツール	Y	Y	Y
ERSPAN をサポートするリモート モニタリング ツール	Y	Y	Y
リモート送信元	Y	N	Y
UDF	Y	Y	Y
UDF v6	N	Y	Y
UDE	N	N	N
ICMPv6 をドロップ	Y	N	Y

表 *3:* サポートされている機能（続き）

機能名	Cisco Nexus 9300（EX、FX） C9504、 C9508、 C9516	Cisco Nexus 9364C、9332C	Cisco Nexus 9300-GX 93600CD-GX 9364C-GX 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

機能名	Cisco Nexus 9300（EX、FX） C9504、 C9508、 C9516	Cisco Nexus 9364C、9332C	Cisco Nexus 9300-GX 93600CD-GX 9364C-GX 9316D-GX
sFlow	Y	Y	Y
PTP/ タイムスタンプ	Y	Y	Y
Jumbo MTU	Y	Y	Y
NetFlow	Y	N	Y
Q-in-Q タグ付け（タップおよびスパン入力ポート用)	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 - タップ/スパン	Y	Y	Y
ローカル モニタリング ツール	Y	Y	Y
ERSPAN をサポートするリモート モニタリング ツール	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。ただし、次の Cisco Nexus シリーズ スイッチもサポートされています。

- Cisco Nexus 3000 シリーズ スイッチ：3048、3064
- Cisco Nexus 3100 シリーズ スイッチ：3172、3164、31108TC-V、31108PC-V、3132C-Z
- Cisco Nexus 3200 シリーズ スイッチ：3232
- Cisco Nexus 3500 シリーズ スイッチ

Cisco Nexus シリーズ スイッチの制限：

表 *4:* 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。 • MPLS ラベル ストリップの設定後に QinQ VLAN を追加できません。

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	プロンプトで次のいずれかのコマンドを入力します。 • **# hardware profile tcam region qos 0** • **# hardware profile tcam region racl 0** • **# hardware profile tcam region vacl 0** • **# hardware profile tcam region ifacl 1024 double-wide** • **# hardware access-list tcam region mac-ifacl 512** • **#feature nxapi** • **#feature lldp**

デバイス モデル	NX-API モード
Cisco Nexus 3164Q スイッチ	プロンプトで次のコマンドを入力します。 • **# hardware profile tcam region qos 0** • **# hardware profile tcam region racl 0** • **# hardware profile tcam region vacl 0** • **# hardware profile tcam region ifacl 1024 double-wide** • **# hardware access-list tcam region mac-ifacl 512** • **#feature nxapi** • **#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	プロンプトで次のいずれかのコマンドを入力します。 • **# hardware access-list tcam region e-racl 0** • **# hardware access-list tcam region span 0** • **# hardware access-list tcam region redirect 0** • **# hardware access-list tcam region vpc-convergence 0** • **# hardware access-list tcam region racl-lite 256** • **# hardware access-list tcam region l3qos-intra-lite 0** • **# hardware access-list tcam region ifacl 256 double-wide** • **# hardware access-list tcam region mac-ifacl 512** • **# hardware access-list tcam region ipv6-ifacl 256** • **#feature nxapi** • **#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	プロンプトで次のいずれかのコマンドを入力します。 • **# hardware access-list tcam region qos 0** • **# hardware access-list tcam region vacl 0** • **# hardware access-list tcam region racl 0** • **# hardware access-list tcam region redirect 0** • **# hardware access-list tcam region vpc-convergence 0** • **#hardware access-list tcam region ifacl 1024 double-wide** • **# hardware access-list tcam region mac-ifacl 512** • **# hardware access-list tcam region ipv6-ifacl 512** • **#feature nxapi** • **#feature lldp**
Cisco Nexus 9200、9300-EX、9336C-FX2、93240YC-FX2、およびN9K-C93360YC-FX2 スイッチ	プロンプトで次のいずれかのコマンドを入力します。 • **#hardware access-list tcam region ing-l2-span-filter 0**（Cisco Nexus 93108 シリーズ スイッチのみ） • **#hardware access-list tcam region ing-l3-span-filter 0**（Cisco Nexus 93108 シリーズ スイッチのみ） • **# hardware access-list tcam region ing-racl 0** • **hardware access-list tcam region ing-l3-vlan-qos 0** • **# hardware access-list tcam region egr-racl 0** • **# hardware access-list tcam region ing-ifacl 1024** • **#feature nxapi** • **#feature lldp**

デバイス モデル	NX-API モード
Cisco Nexus 9500-EX および 9500-FX シリーズ スイッチ（9504、9508、および 9516）	プロンプトで次のいずれかのコマンドを入力します。 • **# hardware access-list tcam region ing-racl 0** • **# hardware access-list tcam region ing-l3-vlan-qos 0** • **# hardware access-list tcam region egr-racl 0** • **# hardware access-list tcam region ing-ifacl 1024** • **#feature nxapi** • **#hardware acl tap-agg** • **#feature lldp**
Cisco Nexus 9300-GX シリーズ スイッチ	プロンプトで次のいずれかのコマンドを入力します。 • **# hardware access-list tcam region ing-racl 0** • **# hardware access-list tcam region ing-l3-vlan-qos 0** • **# hardware access-list tcam region egr-racl 0** • **# hardware access-list tcam region ing-ifacl 1024** • **#feature nxapi** • **#hardware acl tap-agg** • **#feature lldp**

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、Cisco Nexus Dashboard Data Broker の展開サイズごとのシステム要件を示します。

表 *5:* 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
ハードディスク	Cisco Nexus Dashboard Data Broker 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使用可能な最小 40 GB の空き領域。		
オペレーティングシステム	Java、できれば Ubuntu、Fedora、または Red Hat をサポートする最近の 64 ビット Linux の配布。		
その他	Java 仮想マシン 1.8		

ガイドラインと制約事項

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 サーバーで実行できます。最適な結果を得るためには、次の点を推奨します。

- Java 仮想マシン 1.8.0_45 以降。
- バックアップおよび復元スクリプトには、Python 2.7.3 以降のバージョンが必要です。Cisco Nexus Dashboard Data Broker がデバイス通信に TLS を使用する必要がある場合、これは TLS 構成を行うためにも必要です。
- JVM のパスにセットされているプロファイルの $JAVA_HOME 環境変数。
- 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（必須ではない）追加です。

- Cisco Nexus Dashboard Data Broker によるリンク ディスカバリでの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設定しないでください。
- 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、監視デバイス、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** および **feature lldp** CLI コマンドと 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 リストを通過し、レイヤ 2 パケット上で一致しません。

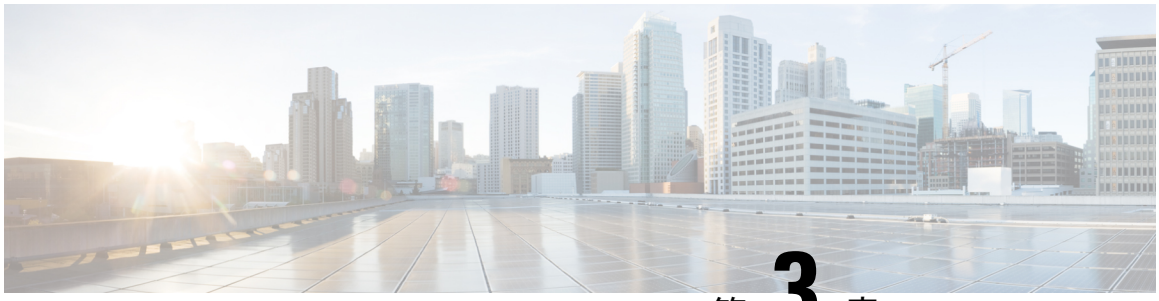
ファイル名マトリックス

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 3 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 以降、Cisco Nexus Data Broker (NDB) は Cisco Nexus Dashboard Data Broker に名前が変更されました。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 つ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 xnc/configuration/startup 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。

（注） IPv6 は、集中型 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。

（注） Cisco Nexus Dashboard Data Broker は、2 ノード構成または奇数ノード構成のみをサポートします。偶数のノードを構成すると、最後のノードがクラスター形成に含まれないため、セットアップ内のノードの数は奇数にしてください。

表 *6:* クラスタの動作ステータス

クラスタ インジケーター	クラスタのステータス	推奨
緑	使用可能	
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 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。 注: 2 ノード クラスタの場合、通常の操作を確実にするために、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 `xnc/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` ファイルに構成する必要があります。

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 `xnc/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。

ハイ アベイラビリティ クラスタのパスワード保護

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 `xnc/configuration` 設定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 `xncjgroups.xml` 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。

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

ステップ 5 AUTH 行からコメントを削除します。

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。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るという条件で、このパスワードをどんな値にでも変更できます。

ステップ 7 ファイルを保存し、エディタを終了します。

Cisco Nexus Dashboard Data Broker GUI へのログイン

HTTPS を使用して Cisco Nexus Data Broher GUI にログインできます。Cisco Nexus Dashboard Data Broker GUI のデフォルトの HTTPS Web リンクは、`https://IP_address:8443/monitor` です。

（注） Web ブラウザで *https://* プロトコルを手動で指定する必要があります。コントローラも HTTPS 用に構成する必要があります。

ステップ 1 Web ブラウザで、Cisco Nexus Dashboard Data Broker の Web リンクを入力します。

ステップ 2 起動ページで、次の手順を行います。

a) ユーザ名とパスワードを入力します。

デフォルトのユーザー名とパスワードは、admin/admin です。

b) **[ログイン]** をクリックします。

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。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**キーストア**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。

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。

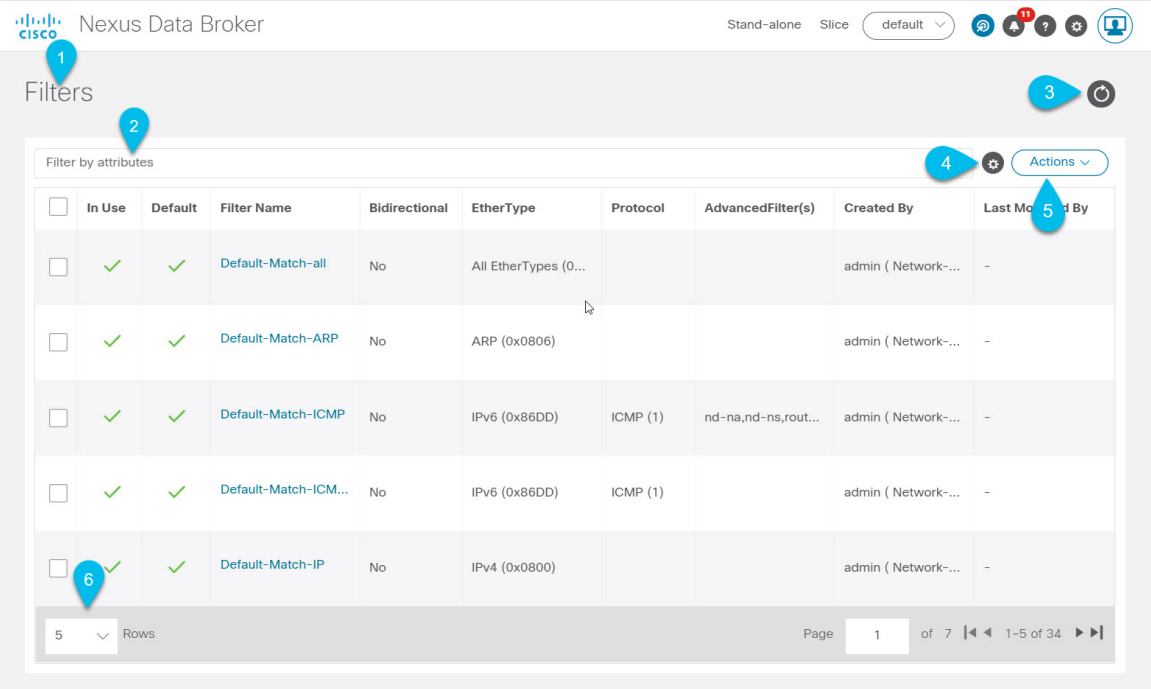
- ダッシュボード
- トポロジ
- デバイス
- 接続
- コンポーネント
- セッション
- 統計
- トラブルシューティング
- 管理

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]* 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。

  表の要素にカーソルを合わせると表示されるフィルタ 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]* 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]* 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]** 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]** 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 ヘッダー (右上隅) アイコンの概要について説明します。

表 *7 : Cisco Nexus Dashboard Data Broker* ヘッダー アイコン

アイコン	説明
クラスタ	現在の Nexus Dashboard Data Broker コントローラ インスタンスのロールを表示します - プライマリ (P) またはメンバー (M)。プライマリとメンバーの IP アドレスが表示されます。プライマリ クラスタの IP アドレスは (*) で示されます。 Nexus Dashboard Data Broker コントローラがクラスタにない場合、スタンドアロンが表示されます。
スライス（**Slice**）	ユーザーが現在ログインしているスライス名を表示します。 ドロップダウン リストから別のスライスを選択して、ネットワーク ビューを変更します。
図 *1 :* 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 *2 :* 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 アイコンをクリックします。詳細については、フローの管理 タブに移動します。
図 *3 :* ヘルプ メニュー バー 	次のオプションが表示されます。 • **新機能**—最新リリースの新機能を表示します。 • **ヘルプ**— オンライン ヘルプ コンテンツを表示します。

アイコン	説明
図 *4:* システム ツール メニュー バー 	次のオプションを提供します。 • **ログのダウンロード**—ログ ファイルをローカル マシンにダウンロードできます。 • **Northbound API** — Nexus Dashboard Data Broker REST API の詳細については、**Swagger** UI に移動します。 • **セッション タイムアウト** — セッション タイムアウト値を設定できます。 • **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。
図 *5:* ユーザー プロファイル メニュー バー 	次のオプションを提供します。 • **Welcome** *User* — GUI の現在のユーザーを表示します。 • **[パスワードの変更（Change Password）]**—パスワードを変更できます。 • **[ログアウト（Logout）]** — GUI からログアウトできます。

Syslog

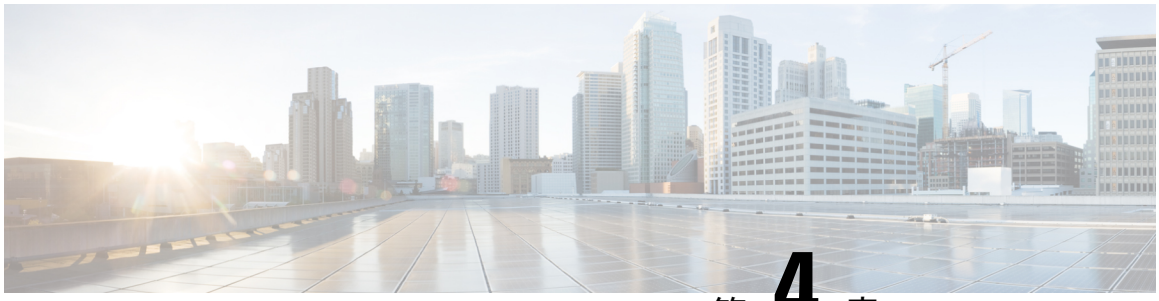
Nexus Dashboard Data Broker サーバー バックエンドでは、ログを Syslog サーバーに送信するように `logback.xml` ファイルを構成できます。必要に応じてログ形式をカスタマイズできます。ログバック ファイルは `/ndb/configuration/logback.xml` にあります。

（注） Nexus Dashboard Data Broker サーバーが実行されている場合は、`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>
```

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



第 4 章

TLS 証明書、KeyStore およびトラストストア ファイルの管理

この章では、TLS 証明書とトラストストア ファイルを生成するための情報と手順について説明します。

リリース 3.10.1 以降、Cisco Nexus Data Broker (NDB) は Cisco Nexus Dashboard Data Broker に名前が変更されました。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。

NXAPI に対して NDB サーバーと NDB スイッチの間での TLS 自己署名証明書の生成

このセクションでは、NDB サーバーと NDB スイッチの間で TLS 自己署名証明書を生成する方法について説明します。TLS を有効にするには、スイッチごとに証明書とキーを生成する必要があります。NDB サーバーと NDB スイッチの間で TLS 通信は、ポート 443 のみを使用します。

NDB サーバーと NXAPI の NDB スイッチの間で TLS 自己署名証明書を生成するには、次の手順を実行します。

- Nexus Dashboard Data Broker での TLS KeyStore と TrustStore パスワードの構成 （32 ページ）

（注） TLS を構成した後でポート 80 を使用して、通信するためのコントローラを構成できません。

自己署名証明書とキーの生成

このセクションでは、自己署名証明書とキーを生成する方法について説明します。

始める前に

スイッチの完全修飾ドメイン名（FQDN）として機能する各 NDB スイッチに対して **ip domain-name** コマンドを使用して、スイッチにドメイン名が設定されてい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 に対して構成されます。

ステップ 1 サーバにログインします。

ステップ 2 **openssl req** コマンドを使用して、秘密キーと自己署名証明書を生成します。

例：

```
docker@docker-virtual-machine:~/TLS$ openssl req -x509 -nodes -days 3650 -newkey rsa:2048 -out
sw1-ca.pem -outform PEM -keyout sw1-ca.key

Generating a 2048 bit RSA private key
...+++
.........................................+++
writing new private key to 'sw1-ca.key'
-----
You are about to be asked to enter information that will be incorporated into
 your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:CA
Locality Name (eg, city) []:SJ
Organization Name (eg, company) [Internet Widgits Pty Ltd]:cisco
```

```
Organizational Unit Name (eg, section) []:insbu
Common Name (e.g. server FQDN or YOUR name) []:N9K-117.cisco.com
Email Address []:myname@cisco.com
```

（注） 複数のスイッチがある場合、各スイッチに対して証明書ファイルとプライベート キーを生成します。

このコマンドは、証明書ファイル（sw1-ca.pem）およびプライベートキー（sw1-ca.key）を生成します。

ステップ 3 NDB スイッチにログインします。

ステップ 4 **copy** コマンドを使用して、証明書ファイル sw1-ca.pem とキー ファイル sw1-ca.key をスイッチにコピーします。

例：

```
N9K-117# copy scp://docker@10.16.206.250/home/docker/Mallik/TLS_CA_june_23/sw1-ca.pem bootflash:
Enter vrf (If no input, current vrf 'default' is considered): management
docker@10.16.206.250's password:
server.cer
                                                                    100% 4676
     4.6KB/s   00:00
Copy complete, now saving to disk (please wait)...

N9K-117# copy scp://docker@10.16.206.250/home/docker/Mallik/TLS_CA_june_23/sw1-ca.key bootflash:
Enter vrf (If no input, current vrf 'default' is considered): management

docker@10.16.206.250's password:
cert.key
                                                                    100%
Copy complete, now saving to disk (please wait)...
```

（注） 複数のスイッチをお持ちの場合、すべてのスイッチに対してこの手順を繰り返します。

ステップ 5 証明書ファイル、sw1-ca.pem、およびキーファイル、sw1-ca.key を **nxapi** コマンドを使用してスイッチで構成します。

例：

```
N9K-117 (config)# nxapi certificate httpskey keyfile bootflash:sw1-ca.key
Upload done. Please enable. Note cert and key must match.
N9K-117 (config)#
N9K-117 (config)# nxapi certificate httpscrt certfile bootflash:sw1-ca.pem
Upload done. Please enable. Note cert and key must match.
 N9K-117 (config)#
```

（注） 複数のスイッチがある場合、各スイッチに対して対応する証明書ファイルとプライベート キーを構成します。

ステップ 6 **nxapi certificate** コマンドを使用して、スイッチの自己署名証明書を有効にします。.

例：

```
N9K-117 (config)# nxapi certificate enable
N9K-117 (config)#
```

（注） スイッチで自己署名証明書を有効化する間にエラーがないことを確認します。

ステップ 7 サーバにログインします。

ステップ 8 **copy** コマンドを使用して、sw1-ca.key および sw1-ca.pem ファイルをコピーし、.PEM 形式に変換します。

例：

```
cp sw1-ca.key sw1-ndb-privatekey.pem
cp sw1-ca.pem sw1-ndb-cert.pem
```

ステップ 9 **cat** コマンドを使用して、秘密キーと証明書ファイルを連結します。

例：

```
docker@docker-virtual-machine:~/TLS$ cat sw1-ndb-privatekey.pem sw1-ndb-cert.pem > sw1-ndb.pem
```

ステップ 10 **openssl** コマンドを使用して、.pem ファイルを .p12 ファイル形式に変換します。パスワードで保護された .p12 証明書ファイルを作成するように指示メッセージが表示されたら、エクスポート パスワードを入力してください。

例：

```
docker@docker-virtual-machine:~/TLS$openssl pkcs12 -export -out sw1-ndb.p12 -in sw1-ndb.pem
Enter Export Password: cisco123
Verifying - Enter Export Password: cisco123
Enter a password at the prompt. Use the same password that you entered in the previous Step
(cisco123)
```

ステップ 11 **keytool** コマンドを使用して、sw1-ndb.p12 をパスワード保護された Java キーストア（tlsKeyStore）ファイルに変換します。インストールされている java ディレクトリの jre/bin を使用します。

例：

```
docker@docker-virtual-machine:~/TLS$ ./(relativePath)/keytool -importkeystore -srckeystore
sw1-ndb.p12 -srcstoretype pkcs12 -destkeystore tlsKeyStore -deststoretype jks
Enter Destination Keystore password:cisco123
Re-enter new password:cisco123
Enter source keystore password:cisco123
Entry for alias 1 successfully imported.
Import command completed: 1 enteries successfully imported, 0 enteries failed or cancelled.
```

（注） デフォルトでは、「1」という名前のエイリアスが最初のスイッチに対して、tlsKeyStore に保存されます。NDB コントローラが複数のスイッチを管理している場合は、すべてのスイッチに対してこの手順を繰り返します。2 番目のスイッチを追加すると、ユーティリティを使用して最初のスイッチ エイリアスの名前を変更できます。以下に示された例を参照してください。

```
keytool -importkeystore -srckeystore sw2-ndb.p12 -srcstoretype pkcs12 -destkeystore
tlsKeyStore -deststoretype jks
keytool -importkeystore -srckeystore sw3-ndb.p12 -srcstoretype pkcs12 -destkeystore
tlsKeyStore -deststoretype jks
```

ステップ 12 **keytool** コマンドを使用して、java tlsKeyStore のコンテンツをリストして検証します。

例：

```
docker@docker-virtual-machine:~/TLS$ keytool -list -v -keystore tlsKeyStore | more
```

次のタスク

後続のタスク、*TLS TrustStore* ファイルの作成に進みます。

TLS トラストストア ファイルの作成

トラストストアは、1つ以上のスイッチに対して生成された自己署名証明書から作成されます。コントローラ内に1つ以上のスイッチの証明書を保持します。このセクションでは、「自己署名証明書とキーの生成」セクションで作成した自己署名証明書を使用してトラストストアを作成する方法について説明します。コントローラに複数のスイッチがある場合、各スイッチには個別の証明書ファイルがあります（たとえば、sw1-ndb-cert.pem、sw2-ndb-cert.pem）。

ステップ 1 サーバにログインします。

ステップ 2 **keytool** コマンドを使用して、証明書ファイル（たとえば、sw1-ndb-cert.pem）を Java トラストストア（tlsTrustStore）ファイルに変換します。パスワードで保護された Java トラストストア（tlsTrustStore）ファイルを作成するように求められたら、パスワードを入力します。パスワードは 6 文字以上にする必要があります。java ディレクトリにインストールされている jre/bin を使用します。

例：

```
docker@docker-virtual-machine:~/TLS$ ./(relativePath)/keytool -import -alias sw1 -file sw1-ndb-cert.pem
 -keystore tlsTrustStore -storetype jks
Enter Export Password: cisco123
Verifying - Enter Export Password: cisco123
Enter a password at the prompt. Use the same password that you entered in the previous Step (cisco123)
```

（注） NDB コントローラが複数のスイッチを管理している場合は、すべてのスイッチに対してこの手順を繰り返して、すべてのスイッチ キーを同じトラストストアに追加します。次に例を示します。

```
docker@docker-virtual-machine:~/TLS$ keytool -import -alias sw2 -file sw2-ndb-cert.pem
-keystore tlsTrustStore
docker@docker-virtual-machine:~/TLS$ keytool -import -alias sw3 -file sw3-ndb-cert.pem
-keystore tlsTrustStore
// Here sw2 and sw3 are alias for switch 2 and switch 3 for identification purpose.
```

ステップ 3 **keytool** コマンドを使用して、同じ tlsTrustStore 内の複数のスイッチのキーを一覧表示して確認します。

例：

```
docker@docker-virtual-machine:~/TLS$ keytool -list -v -keystore tlsTrustStore | more
```

TLS を使用した NDB の開始

TLS を使用して NDB を開始するには、次の手順を実行します。

ステップ 1 NDB サーバーにログインします。

ステップ 2 **runndb.sh** コマンドを使用して、NDB アプリケーションを停止します (実行中の場合)。

例：

```
 ./runndb.sh -stop
Controller with PID: 17426 -- Stopped!
```

ステップ 3 作成した tlsKeystore および tlsTruststore ファイルを NDB の構成フォルダ（ndb/configuration）にコピーします。

例：

```
cp tlskeystore /root/ndb/configuration
cp tlsTrustStore /root/ndb/configuration
```

ステップ 4 **runndb.sh** スクリプトを使用して、TLS で NDB アプリケーションを開始します。

例：

```
./runndb.sh -tls -tlskeystore ./configuration/tlsKeyStore -tlstruststore ./configuration/tlsTrustStore
```

例：

デフォルトのユーザー名（admin）とデフォルト以外のパスワード（たとえば、pwd123）で NDB を起動するには:

```
./runndb.sh -osgiPasswordSync -tls -tlskeystore ./configuration/tlsKeyStore -tlstruststore
./configuration/tlsTrustStore
If ndb password is changed, OSGi webconsole password needs to be changed.
To set non-default OSGi webconsole password, enter ndb Admin Password [default]:
 (Type the non-default password which was set)
```

（注） TLS を無効にするには、**./runndb.sh -notls** コマンドを実行します。TLS を無効にして NDB を開始するには、**./runndb.sh -notls -start** コマンドを実行します。TLS を無効にする前に、必ず NDB を停止してください。TLS を無効にした後、NDB サーバーに接続されているデバイスのポート番号を 80 に変更する必要があります。

Nexus Dashboard Data Broker での TLS KeyStore と TrustStore パスワードの構成

Nexus Dashboard Data Broker がパスワードで保護された TLS キーストアおよびトラストストアファイルを読み取れるようにするには、TLS キーストアおよびトラストストアのパスワードを構成する必要があります。Nexus Dashboard Data Broker で TLS キーストアとトラストストアのパスワードを構成するには、次の手順を実行します。

ステップ 1 Nexus Dashboard Data Broker サーバーにログインします。

ステップ 2 bin ディレクトリに移動します。

例：

```
cd ndb/bin
```

ステップ 3 **ndb config-keystore-passwords** コマンドを使用して、TLS キーストアとトラストストアのパスワードを構成します。

例：

```
./ndb config-keystore-passwords --user admin --password admin --url https://ip-address_localhost:8443
 --verbose --prompt --keystore-password keystore_password --truststore-password truststore_password
```

Nexus Dashboard Data Broker が AAA (Tacacs/LDAP/Radius) で構成されており、上記のコマンドで **ndb config-keystore-passwords** が失敗し、*401* 未承認エラーが表示された場合：

1. `ndb` または `xnc` ディレクトリに移動します。
2. `/runndb.sh -stop` を使用して、Nexus Dashboard Data Broker サーバーを停止します。
3. Nexus Dashboard Data Broker **config.ini** ファイルで値を *false* から *true* に変更して、フラグ `enable.LocalUser.Authentication` を有効にします。
4. `/runndb.sh -start` を使用して、Nexus Dashboard Data Broker サーバーを起動します。
5. **ndb config-keystore-passwords** コマンドを再度実行します。

（注） HA 環境では、クラスター内のすべての Nexus Dashboard Data Broker サーバーに対して上記の手順を実行する必要があります。

Nexus Dashboard Data Broker で TLS を有効にすると、Nexus Dashboard Data Broker サーバーと Nexus Dashboard Data Broker スイッチ間のすべての接続がポート 443 を使用して確立されます。ポート 443 を使用するように Nexus Dashboard Data Broker のデバイス接続を変更してください。

これらの手順を正常に完了すると、ポート 443 を使用してコントローラにネクサス スイッチを追加できます。スイッチの FQDN を使用して、デバイスを exus Dashboard Data Broker コントローラに追加します。

スイッチの WebUI Sandbox を使用して証明書情報を確認できます。

NDB サーバーと NXAPI の NDB スイッチ間での TLS サードパーティ証明書の生成

このセクションでは、NDB サーバーと NDB スイッチの間で TLS サードパーティ証明書を生成する方法について説明します。ネットワーク内のスイッチごとに個別の証明書とキーを要求する必要があります。NDB サーバーと NDB スイッチの間で TLS 通信は、ポート 443 のみを使用します。

NDB サーバーと NXAPI の NDB スイッチの間で TLS サード パーティ証明書を生成するには、次の手順を実行します。

- 認証局から証明書の取得
- NDB コントローラの TLS キーストアと Truststore ファイルの作成

- TLS を使用した NDB の開始
- Nexus Dashboard Data Broker での TLS KeyStore と TrustStore パスワードの構成

（注） 両方のセクションのすべての手順を実行して、コントローラとスイッチ間の TLS での通信が正常に行われるようにします。

認証局から証明書の取得

2 つの方法で認証局（CA）から証明書を取得できます。秘密キーと証明書の両方に対して CA に直接アプローチすることができます。CA は、CA の署名を発行した公開キーを含む証明書とともに、あなたに代わって秘密キーを生成します。

もう 1 つのアプローチでは、openssl などのツールを使用して秘密キーを生成し、証明書発行機関への証明書署名要求（CSR）を生成できます。CA は CSR からのユーザー識別情報を使用して、公開キーで証明書を生成します。

始める前に

スイッチの完全修飾ドメイン名（FQDN）として機能する各 NDB スイッチに対して **ip domain-name** コマンドを使用して、スイッチにドメイン名が設定されてい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 に対して構成されます。

ステップ 1 サーバにログインします。

ステップ 2 openssl コマンドを使用して、秘密鍵（cert.key）と証明書署名要求（cert.req）を生成します。

例：

```
docker@docker-virtual-machine:~/Mallik/TLS_CA$ openssl req -newkey rsa:2048 -sha256 -keyout cert.key
 -keyform PEM -out cert.req -outform PEM

Generating a 2048 bit RSA private key
...............+++
.....................+++
writing new private key to 'cert.key'
Enter PEM pass phrase:                          □ cisco123
Verifying - Enter PEM pass phrase:     □ cisco123
-----
You are about to be asked to enter information that will be incorporated into your certificate
request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
```

```
-----
Country Name (2 letter code) [GB]:US
State or Province Name (full name) [Berkshire]:CA
Locality Name (eg, city) [Newbury]:SJ
Organization Name (eg, company) [My Company Ltd]:cisco
Organizational Unit Name (eg, section) []:insbu
Common Name (eg, your name or your server's hostname) []:N9K-117.cisco.com
Email Address []:myname@cisco.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []: □ cisco123
An optional company name []:□ cisco123


docker@docker-virtual-machine: # ls
cert.key  cert.req
```

ステップ 3 openssl コマンドを使用して CSR を確認します。

例：

```
docker@docker-virtual-machine:~/Mallik/TLS_CA$ openssl req -noout -text -in cert.req
```

ステップ 4 秘密キーはセキュリティ パスフレーズで生成されます。秘密キーを復号する必要があります。秘密鍵からパスフレーズを削除するには、openssl コマンドを使用します。

例：

```
docker@docker-virtual-machine:~/Mk/TLS_CA$ ls
cert.key  cert.req
docker@docker-virtual-machine:~/Mk/TLS_CA$cp cert.key  cert.keybkp
docker@docker-virtual-machine:~/Mk/TLS_CA$ rm cert.key
docker@docker-virtual-machine:~/Mk/TLS_CA$ openssl rsa -in cert.keybkp -out cert.key

Enter pass phrase for cert.keybkp: cisco123
```

（注） この手順を繰り返して、すべてのスイッチの秘密キーからパスフレーズを削除します。

（注） 選択する CA の階層により、各 CSR に対して最大 3 つの証明書（証明書チェーン）を取得できます。このことは、各 NDB スイッチに対する CA から 3 つの証明書（root、中間、ドメイン）の取得を意味します。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。例： test-root-ca-2048.cer (root)、test-ssl-ca.cer (intermediate)、N9K-117.cisco.com.cer (domain)

証明書はほとんどの場合、.PEM ファイル形式で共有されます。

cert.req ファイルデータは、サードパーティの証明機関に提出する必要があります。関連する手順に従って、3 つの（証明書）ファイルを取得してください。

ステップ 5 **cat** コマンドを使用して、3 つの証明書ファイルから 1 つの証明書ファイルを作成します。この連結は、ドメイン証明書、root 証明書、中間証明書の順番で行われます。**cat** コマンドのシンタックス： *cat* ドメイン証明書ルート証明書中間証明書 > *server.cer*

例：

```
$cat N9K-117.cisco.com.cer test-root-ca-2048.cer test-ssl-ca.cer > server.cer
```

ステップ 6 新しく作成した server.cer ファイルを編集して、連結された END 行と BEGIN 行を分割します。ファイルで何も削除しないでください。

例：

```
-----END CERTIFICATE----------BEGIN CERTIFICATE-----


////// Modify the above line like this by adding a line feed between the two.
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
```

（注） この手順をすべてのスイッチで繰り返します。

ステップ 7 NDB スイッチにログインします。

ステップ 8 秘密キー（cert.key）と CA からの証明書（server.cer）を copy コマンドを使用してスイッチにコピーします。

例：

```
N9K-117# copy scp://docker@10.16.206.250/home/docker/Mallik/TLS_CA_june_23/server.cer bootflash:
Enter vrf (If no input, current vrf 'default' is considered): management
docker@10.16.206.250's password:
server.cer
                                                  100% 4676     4.6KB/s   00:00
Copy complete, now saving to disk (please wait)...

N9K-117# copy scp://docker@10.16.206.250/home/docker/Mallik/TLS_CA_june_23/cert.key bootflash:
Enter vrf (If no input, current vrf 'default' is considered): management
docker@10.16.206.250's password:
cert.key
                                               100%
Copy complete, now saving to disk (please wait)...
```

（注） すべてのスイッチに対してこの手順を繰り返します。

ステップ 9 **nxapi** コマンドを使用して、スイッチに証明書ファイル sw1-ca.pem とキーファイル sw1-ca.key を設定します。

例：

```
N9K-117 (config)# nxapi certificate httpskey keyfile bootflash:cert.key
Upload done. Please enable. Note cert and key must match.
N9K-117 (config)#
N9K-117 (config)# nxapi certificate httpscrt certfile bootflash:server.cer
Upload done. Please enable. Note cert and key must match.
 N9K-117 (config)#
```

（注） 複数のスイッチがある場合は、対応する証明書と秘密キーを各スイッチに構成します。

ステップ 10 **nxapi certificate** コマンドを使用して、スイッチの自己署名証明書を有効にします。.

例：

```
N9K-117 (config)# nxapi certificate enable
N9K-117 (config)#
```

（注） スイッチで自己署名証明書を有効にするときにエラーがないことを確認します。

NDB コントローラの TLS キーストアと Truststore ファイルの作成

NDB は証明書とキーを使用して、スイッチ間の安全な通信を保護します。キーストアにキーと証明書を保存します。これらのファイルは、NDB に tlsTruststore および tlsKeystore ファイルとして保存されます。NDB コントローラの Java tlsKeyStore および tlsTrustStore ファイルを生成するには、次の手順を実行します。

ステップ 1 TLS ディレクトリを作成し、それに移動します。

例：

```
mkdir -p TLS
cd TLS
```

ステップ 2 *mypersonalca* の下に 3 つのディレクトリと 2 つの前提条件ファイルを作成します。

例：

```
mkdir -p mypersonalca/certs
mkdir -p mypersonalca/private
mkdir -p mypersonalca/crl
echo "01" > mypersonalca/serial
touch mypersonalca/index.txt
```

コマンドを使用して、NDB に接続されている各スイッチの TLS 秘密キーと認証局（CA）ファイルを生成します。

ステップ 3 **openssl req -x509 -nodes -days 3650 -newkey rsa:2048 -out mypersonalca/certs/sw1-ca.pem -outform PEM -keyout mypersonalca/private/sw1-ca.key** コマンドを使用して、NDB に接続された各スイッチの TLS 秘密鍵と認証局（CA）ファイルを生成します。

この手順により、2048 ビットのキー長の PEM 形式の TLS 秘密キーと CA ファイル（mypersonalca/certs/sw1-ca.pem、mypersonalca/private/sw1-ca.key）が生成されます。複数のスイッチがある場合は、これらのスイッチの CSR を生成するときに提供された正確な値を使用して、すべてのスイッチに対して sw1-ca.pem および sw1-ca.key ファイルを作成する必要があります。

（注） 「認証局からの証明書の取得」セクションで cert.key を生成するときに提供されたのと同じ入力を使用します。入力に不一致があると、新しいキーが生成されます。

例：

```
docker@docker-virtual-machine:~/TLS$ openssl req -x509 -nodes -days 3650 -newkey rsa:2048 -out
mypersonalca/certs/sw1-ca.pem -outform PEM -keyout mypersonalca/private/sw1-ca.key
Generating a 2048 bit RSA private key
...+++
.........................................+++
writing new private key to 'mypersonalca/private/sw1-ca.key'
-----
```

```
You are about to be asked to enter information that will be incorporated into your certificate
request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:CA
Locality Name (eg, city) []:SJ
Organization Name (eg, company) [Internet Widgits Pty Ltd]:cisco
Organizational Unit Name (eg, section) []:insbu
Common Name (e.g. server FQDN or YOUR name) []:N9K-117.cisco.com
Email Address []:myname@cisco.com
```

「認証局からの証明書の取得」セクションで作成した cert.key と server.cer を現在のディレクトリ（TLS）にコピーします。単一のスイッチの証明書とキーファイルを選択します。これらのファイルは、コントローラに接続しているスイッチに対して以前、生成されました。現在のスイッチの server.cer と cert.key を使用して、TLS キーストア ファイルを作成します。

ステップ 4 「認証局からの証明書の取得」セクションで作成した cert.key と server.cer を現在のディレクトリ（TLS）にコピーします。単一のスイッチの証明書とキーファイルを選択します。これらのファイルは、コントローラに接続しているスイッチに対して以前、生成されました。現在のスイッチの server.cer と cert.key を使用して、TLS キーストア ファイルを作成します。

複数のスイッチが接続されている場合、各スイッチに対して個別にこの手順を繰り返します。

ステップ 5 **copy** コマンドを使用して、server.cer および cert.key ファイルをコピーし、.PEM 形式に変換します。

例：

```
cp cert.key sw1-ndb-privatekey.pem
cp server.cer sw1-ndb-cert.pem
```

ステップ 6 **cat** コマンドを使用して、秘密キー（sw1-ndb-privatekey.pem）と証明書ファイル（sw1-ndb-cert.pem）を単一の .PEM ファイルに連結します。

例：

```
cat sw1-ndb-privatekey.pem sw1-ndb-cert.pem > sw1-ndb.pem
```

ステップ 7 **openssl** コマンドを使用して、.PEM ファイルを .P12 形式に変換します。指示メッセージが表示されたらエクスポートパスワードを入力します。パスワードには少なくとも 6 文字が含まれなければなりません。例：cisco123 sw1-ndb.pem ファイルはパスワード保護された sw1-ndb.p12 ファイルに変換されます。

例：

```
docker@docker-virtual-machine:~/TLS$openssl pkcs12 -export -out sw1-ndb.p12 -in sw1-ndb.pem
Enter Export Password: cisco123
Verifying - Enter Export Password: cisco123
Enter a password at the prompt. Use the same password that you entered in the previous Step
(cisco123)
```

ステップ 8 **keytool** コマンドを使用して、sw1-ndb.p12 をパスワード保護された Java キーストア（tlsKeyStore）ファイルに変換します。このコマンドは、sw1-ndb.p12 ファイルをパスワード保護された tlsKeyStore ファイルに変換します。

例：

```
docker@docker-virtual-machine:~/TLS$ keytool -importkeystore -srckeystore sw1-ndb.p12 -srcstoretype
 pkcs12 -destkeystore tlsKeyStore -deststoretype jks
Enter Destination Keystore password:cisco123
```

（注） デフォルトでは、「1」というエイリアスが最初のスイッチの tlsKeyStore に保存されます。NDB コントローラが複数のスイッチを管理している場合は、すべてのスイッチに対してこの手順を繰り返します。2 番目のスイッチを追加すると、ユーティリティにより、最初のスイッチ エイリアスの名前を変更し、新しいスイッチのエイリアスを名前変更するためにプロビジョニングします。たとえば、以下を参照してください。

```
keytool -importkeystore -srckeystore sw2-ndb.p12 -srcstoretype pkcs12 -destkeystore
tlsKeyStore -deststoretype jks
keytool -importkeystore -srckeystore sw3-ndb.p12 -srcstoretype pkcs12 -destkeystore
tlsKeyStore -deststoretype jks
```

ステップ 9 keytool コマンドを使用して、java tlsKeyStore のコンテンツをリストして検証します。

例：

```
docker@docker-virtual-machine:~/TLS$ keytool -list -v -keystore tlsKeyStore | more
```

ステップ 10 **keytool** コマンドを使用して、証明書ファイル（sw1-ndb-cert.pem）を Java TrustStore（tlsTrustStore）ファイルに変換します。指示メッセージが表示されたときにパスワードを入力して、パスワード保護された Java TrustStore（tlsTrustStore）ファイルを作成します。パスワードは少なくとも 6 文字でなければなりません。

例：

```
docker@docker-virtual-machine:~/TLS$ keytool -import -alias sw1 -file sw1-ndb-cert.pem -keystore
 tlsTrustStore -storetype jks
Enter keystore password: cisco123
Re-enter new password: cisco123
Owner: EMAILADDRESS=myname@cisco.com, CN=localhost, OU=insbu, O=cisco, L=SJ, ST=CA, C=US
Issuer: EMAILADDRESS=myname@cisco.com, CN=localhost, OU=insbu, O=cisco, L=SJ, ST=CA, C=US
Serial number: c557f668a0dd2ca5
Valid from: Thu Jun 15 05:43:48 IST 2017 until: Sun Jun 13 05:43:48 IST 2027
Certificate fingerprints:
MD5: C2:7B:9E:26:31:7A:74:25:55:DF:A7:91:C9:5D:20:A3
SHA1: 3C:DF:66:96:72:12:CE:81:DB:AB:58:30:60:E7:CC:04:4D:DF:6D:B2
SHA256:
DD:FB:3D:71:B4:B8:9E:CE:97:A3:E4:2D:D3:B6:90:CD:76:A8:5F:84:77:78:BE:49:6C:04:01:84:62:2C:2F:EB
Signature algorithm name: SHA256withRSA
Version: 3

Extensions:

#1: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 0D B3 CF 81 66 4A 33 4E EF 86 7E 26 C3 50 9B 73 ....fJ3N...&.P.s
0010: 38 EF DF 40 8..@
]
]

#2: ObjectId: 2.5.29.19 Criticality=false
BasicConstraints:[
CA:true
PathLen:2147483647
]
```

```
#3: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 0D B3 CF 81 66 4A 33 4E EF 86 7E 26 C3 50 9B 73 ....fJ3N...&.P.s
0010: 38 EF DF 40 8..@
]
]

Trust this certificate? [no]: yes
Certificate was added to keystore
```

（注） NDB コントローラが複数のスイッチを管理する場合、すべてのスイッチに対してこの手順を繰り返して、同じ TrustStore にすべてのスイッチを追加してください。次に例を示します。

```
keytool -import -alias sw2 -file sw2-ndb-cert.pem -keystore tlsTrustStore
keytool -import -alias sw3 -file sw3-ndb-cert.pem -keystore tlsTrustStore
```

ステップ 11 keytool コマンドを使用して同じ tlsTrustStore のキーをリストし、検証します。

例：

```
docker@docker-virtual-machine:~/TLS$ keytool -list -v -keystore tlsTrustStore | more
```

TLS を使用した NDB の開始

TLS を使用して NDB を開始するには、次の手順を実行します。

ステップ 1 NDB サーバーにログインします。

ステップ 2 **runndb.sh** コマンドを使用して、NDB アプリケーションを停止します (実行中の場合)。

例：

```
 ./runndb.sh -stop
Controller with PID: 17426 -- Stopped!
```

ステップ 3 作成した tlsKeystore および tlsTruststore ファイルを NDB の構成フォルダ（ndb/configuration）にコピーします。

例：

```
cp tlskeystore /root/ndb/configuration
cp tlsTrustStore /root/ndb/configuration
```

ステップ 4 **runndb.sh** スクリプトを使用して、TLS で NDB アプリケーションを開始します。

例：

```
./runndb.sh -tls -tlskeystore ./configuration/tlsKeyStore -tlstruststore ./configuration/tlsTrustStore
```

例：

デフォルトのユーザー名（admin）とデフォルト以外のパスワード（たとえば、pwd123）で NDB を起動するには:

```
./runndb.sh -osgiPasswordSync -tls -tlskeystore ./configuration/tlsKeyStore -tlstruststore
./configuration/tlsTrustStore
If ndb password is changed, OSGi webconsole password needs to be changed.
To set non-default OSGi webconsole password, enter ndb Admin Password [default]:
 (Type the non-default password which was set)
```

（注） TLS を無効にするには、**./runndb.sh -notls** コマンドを実行します。TLS を無効にして NDB を開始するには、**./runndb.sh -notls -start** コマンドを実行します。TLS を無効にする前に、必ず NDB を停止してください。TLS を無効にした後、NDB サーバーに接続されているデバイスのポート番号を 80 に変更する必要があります。

Nexus Dashboard Data Broker での TLS KeyStore と TrustStore パスワードの構成

Nexus Dashboard Data Broker がパスワードで保護された TLS キーストアおよびトラストストアファイルを読み取れるようにするには、TLS キーストアおよびトラストストアのパスワードを構成する必要があります。Nexus Dashboard Data Broker で TLS キーストアとトラストストアのパスワードを構成するには、次の手順を実行します。

ステップ 1 Nexus Dashboard Data Broker サーバーにログインします。

ステップ 2 bin ディレクトリに移動します。

例：

```
cd ndb/bin
```

ステップ 3 **ndb config-keystore-passwords** コマンドを使用して、TLS キーストアとトラストストアのパスワードを構成します。

例：

```
./ndb config-keystore-passwords --user admin --password admin --url https://ip-address_localhost:8443
 --verbose --prompt --keystore-password keystore_password --truststore-password truststore_password
```

Nexus Dashboard Data Broker が AAA (Tacacs/LDAP/Radius) で構成されており、上記のコマンドで **ndb config-keystore-passwords** が失敗し、*401* 未承認エラーが表示された場合：

1. `ndb` または `xnc` ディレクトリに移動します。
2. `/runndb.sh -stop` を使用して、Nexus Dashboard Data Broker サーバーを停止します。
3. Nexus Dashboard Data Broker **config.ini** ファイルで値を *false* から *true* に変更して、フラグ `enable.LocalUser.Authentication` を有効にします。
4. `/runndb.sh -start` を使用して、Nexus Dashboard Data Broker サーバーを起動します。
5. **ndb config-keystore-passwords** コマンドを再度実行します。

（注） HA 環境では、クラスター内のすべての Nexus Dashboard Data Broker サーバーに対して上記の手順を実行する必要があります。

Nexus Dashboard Data Broker で TLS を有効にすると、Nexus Dashboard Data Broker サーバーと Nexus Dashboard Data Broker スイッチ間のすべての接続がポート 443 を使用して確立されます。ポート 443 を使用するように Nexus Dashboard Data Broker のデバイス接続を変更してください。

これらの手順を正常に完了すると、ポート 443 を使用してコントローラにネクサス スイッチを追加できます。スイッチの FQDN を使用して、デバイスを exus Dashboard Data Broker コントローラに追加します。

スイッチの WebUI Sandbox を使用して証明書情報を確認できます。

WebUI ブラウザと NDB サーバー の間でTLS 自己署名証明書を生成する

自己署名証明書を使用して、集中モードで実行されている Web ブラウザと NDB サーバー間の通信を保護できます。このセクションでは、WebUI ブラウザと NDB アプリケーション間の通信を保護するための自己署名証明書を生成する方法について説明します。デフォルトでは、Cisco NDB は、Cisco NDB に発行され、デフォルトの有効性で Cisco NDB によって発行されるデフォルトの証明書とともに出荷されます。構成フォルダーの下にある **generateWebUIcertificate.sh** スクリプトを使用して、自己署名証明書を作成できます。Cisco NDB リリース 3.5 以前の場合、これらの証明書は 6 か月間有効です。Cisco NDB リリース 3.6 以降、証明書のデフォルトの有効期間は 6 か月ですが、証明書の有効期間を設定できます。

（注） NDB の自己署名 TLS 証明書は、集中化モードでのみ作成できます。

- WebUI ブラウザと集中モードで実行されている NDB サーバーの間で TLS 自己署名証明書を生成する

集中型環境で実行されている WebUI ブラウザと NDB サーバーの間で TLS 自己署名証明書を生成する

次の手順を実行して、WebUI ブラウザと集中モードで実行されている NDB サーバーの間で TLS 自己署名証明書を生成します。

ステップ 1 NDB サーバーにログインし、現在のディレクトリ `\ndb\configuration` を変更します。

例：

```
[root@RHEL-VM-NDB-ACI]# cd \ndb\configuration
```

ステップ 2 **generateWebUIcertificate.sh** スクリプトを使用して、TLS 自己署名証明書を生成します。

例：

```
[root@RHEL-VM-NDB-ACI configuration]# ./generateWebUIcertificate.sh

**********************************
Entor Fully qualified domain name :
**********************************
NDB-browser This can be FQDN of the NDB java application as well
**************************
Enter Organizational unit :
**************************
INSBU
********************
Enter Organization :
********************
cisco
****************
Enter Location :
****************
SJ
*************
Enter State :
*************
CA
***************
Enter Country :
***************
USA
***************
Enter keypass :
***************
cisco123
*****************
Enter storepass :
*****************
cisco123
************************************
Enter the validity in number of days :
************************************
365  in NDB 3.5 this script will let you to specify the certificate validity.
*************************************************************************************************************************
Below process will rename the existing key file to <old_keystore>, will generate
 a new key file. Do you want to continue (y/n) ?
*************************************************************************************************************************
y
******************************
Self-Signed Certificate Created
******************************
Alias name: cisco
Creation date: Jan 6, 2019
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
```

```
Owner: CN=NDB-browser, OU=INSBU, O=cisco, L=SJ, ST=CA, C=USA
Issuer: CN=NDB-browser, OU=INSBU, O=cisco, L=SJ, ST=CA, C=USA
Serial number: b404be5
Valid from: Sun Jan 06 20:22:05 PST 2019 until: Mon Jan 06 20:22:05 PST 2020
Certificate fingerprints:
         MD5:  71:07:F6:4E:57:6A:08:3A:AD:06:32:B3:6C:5F:8F:52
         SHA1: 04:08:B9:D5:B7:EB:ED:E0:F9:22:49:14:FA:C6:09:39:22:32:43:A2
         SHA256:
34:D9:EB:34:0A:52:D1:4A:DD:F1:8B:14:D0:84:E4:1C:57:8B:2B:99:9B:E5:A1:4C:C7:8C:CD:AE:24:31:49:75

         Signature algorithm name: SHA256withRSA
         Version: 3

Extensions:

#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 63 8A 92 8F 6F 0F 45 BD   EE 55 C5 A8 99 3B F6 F7  c...o.E..U...;..
0010: AC FA 4A 21                                        ..J!
]
]

*********************************
Displayed the generated keystore
*********************************
*************************************************
Configured the keystore details on tomcat-server.xml
*************************************************
*****************************************************************************************
The newly generated key will used on next NDB restart. Do you want to restart
NDB now (y/n) ?
*****************************************************************************************
y
Doesn't seem any Controller daemon is currently running
Running controller in background with PID: 13573, to connect to it please SSH
to this host on port 2400
NDB GUI can be accessed using below URL:
[https://10.16.206.160:8443]
[https://[fe80::250:56ff:fe90:b764]:8443]
[https://10.16.206.159:8443]
[https://192.168.1.123:8443]
[https://[fe80::250:56ff:fe90:9c79]:8443]

*************
NDB Restarted
*************
```

（注） **generateWebUIcertificate.sh** スクリプトは、NDB アプリケーションを再ロードして、ブラウザから NDB Java アプリケーションにアクセスしたときにブラウザがこの証明書の使用を開始するようにします。

ステップ 3 **keytool -list -v -keystore keystore_Name** コマンドを使用して、生成された証明書を復号化します。プロンプトが表示されたら、ストア パスワードを入力します。

例：

```
[root@RHEL-VM-NDB-ACI configuration]# keytool -list -v -keystore keystore
Enter keystore password:

Keystore type: JKS
Keystore provider: SUN

Your keystore contains 1 entry

Alias name: cisco
Creation date: Jul 6, 2019
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=NDB-browser, OU=INSBU, O=cisco, L=SJ, ST=CA, C=USA
Issuer: CN=NDB-browser, OU=INSBU, O=cisco, L=SJ, ST=CA, C=USA
Serial number: b404be5
Valid from: Sun Jan 06 20:22:05 PST 2019 until: Mon Jan 06 20:22:05 PST 2020
Certificate fingerprints:
         MD5:  71:07:F6:4E:57:6A:08:3A:AD:06:32:B3:6C:5F:8F:52
         SHA1: 04:08:B9:D5:B7:EB:ED:E0:F9:22:49:14:FA:C6:09:39:22:32:43:A2
         SHA256:
34:D9:EB:34:0A:52:D1:4A:DD:F1:8B:14:D0:84:E4:1C:57:8B:2B:99:9B:E5:A1:4C:C7:8C:CD:AE:24:31:49:75
         Signature algorithm name: SHA256withRSA
         Version: 3

Extensions:

#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 63 8A 92 8F 6F 0F 45 BD   EE 55 C5 A8 99 3B F6 F7  c...o.E..U...;..
0010: AC FA 4A 21                                        ..J!
]
]

*******************************************
*******************************************
```

ステップ 4 自己署名証明書は、ブラウザと互換性のない JKS 形式で生成されます。したがって、ブラウザに証明書をインポートする前に、これらの証明書を PKCS12 形式に変換する必要があります。次の手順を関ry法して、JKS 形式の証明書を PKCS12 形式に変換します。**keytool** コマンドを使用して、JKS 形式の証明書を PKCS12 形式に変換します。

（注） 変換する前に必ず元の証明書のコピーをとっておいてください。

例：

```
keytool -importkeystore -srckeystore keystore -srcstorepass cisco123 -srckeypass cisco123
-destkeystore keystore.p12 -deststoretype PKCS12 -srcalias cisco -deststorepass cisco123 -destkeypass
cisco123
```

（注） **keytool** コマンドの入力は、UI 証明書の生成中に提供される入力と一致する必要があります。

（注） 結果として得られる証明書ファイル（keystore.p12）は PKSC12 形式です。

ステップ 5 この証明書をブラウザーの信頼されたルート証明書ストアに追加します。証明書を信頼ルート証明書ストア ストアに追加する方法については、それぞれの Web ブラウザのヘルプを参照してください。

ゲストシェル環境を使用して、組み込みモードで実行されている Web ブラウザと NDB サーバー間で TLS 自己署名証明書を生成する

ゲスト シェル環境を使用して、Web ブラウザと組み込みモードで実行されている NDB サーバーとの間で TLS 自己署名証明書を生成するには、次の手順を実行します。

ステップ 1 **guestshell** コマンドを使用してゲスト シェルに接続します。

例：

```
N9K-C93108TC-EX-108# guestshell
[admin@guestshell ~]$
[admin@guestshell ~]$
```

ステップ 2 現在のディレクトリを \ndb\configuration に変更します。

例：

```
[admin@guestshell ~]$ cd \ndb\configuration
```

ステップ 3 /home/admin/ndb/configuration/generateWebUIcertificate.sh スクリプトを使用して、TLS 自己署名証明書を生成します。

例：

```
[root@RHEL-VM-NDB-ACI configuration]# ./generateWebUIcertificate.sh

***********************************
Entor Fully qualified domain name :
***********************************
NDB-browser This can be FQDN of the NDB java application as well
***************************
Enter Organizational unit :
***************************
INSBU
********************
Enter Organization :
********************
cisco
****************
Enter Location :
****************
SJ
*************
Enter State :
*************
CA
```

```
***************
Enter Country :
***************
USA
***************
Enter keypass :
***************
cisco123
*****************
Enter storepass :
*****************
cisco123
************************************
Enter the validity in number of days :
************************************
365 □ in NDB 3.5 this script will let you to specify the certificate validity.
*************************************************************************************************************************
Below process will rename the existing key file to <old_keystore>, will generate
 a new key file. Do you want to continue (y/n) ?
*************************************************************************************************************************
y
******************************
Self-Signed Certificate Created
******************************
Alias name: cisco
Creation date: Jan 6, 2019
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=NDB-browser, OU=INSBU, O=cisco, L=SJ, ST=CA, C=USA
Issuer: CN=NDB-browser, OU=INSBU, O=cisco, L=SJ, ST=CA, C=USA
Serial number: b404be5
Valid from: Sun Jan 06 20:22:05 PST 2019 until: Mon Jan 06 20:22:05 PST 2020
Certificate fingerprints:
         MD5:  71:07:F6:4E:57:6A:08:3A:AD:06:32:B3:6C:5F:8F:52
         SHA1: 04:08:B9:D5:B7:EB:ED:E0:F9:22:49:14:FA:C6:09:39:22:32:43:A2
         SHA256:
34:D9:EB:34:0A:52:D1:4A:DD:F1:8B:14:D0:84:E4:1C:57:8B:2B:99:9B:E5:A1:4C:C7:8C:CD:AE:24:31:49:75

         Signature algorithm name: SHA256withRSA
         Version: 3

Extensions:

#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 63 8A 92 8F 6F 0F 45 BD   EE 55 C5 A8 99 3B F6 F7  c...o.E..U...;..
0010: AC FA 4A 21                                        ..J!
]
]
```

```
*******************************
Displayed the generated keystore
*******************************
************************************************
Configured the keystore details on jetty-ssl-context.xml
************************************************
*****************************************************************************************
The newly generated key will used on next NDB restart. Do you want to restart
NDB now (y/n) ?
*****************************************************************************************
n
*************
The newly generated key will be used on the next NDB restart.
*************
```

（注） ブラウザからNDB Javaアプリケーションにアクセスするときに、ブラウザがこの証明書の使用を開始するようにするには、**guestshell reboot** コマンドを使用して guestshell を手動でリブートします。

ステップ 4 **keytool -list -v -keystore keystore_Name** コマンドを使用して、生成された証明書をデコードします。プロンプトが表示されたら、ストア パスワードを入力します。

例：

```
[root@RHEL-VM-NDB-ACI configuration]#  keytool -list -v -keystore keystore
Enter keystore password:

Keystore type: JKS
Keystore provider: SUN

Your keystore contains 1 entry

Alias name: cisco
Creation date: Jul 6, 2019
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=NDB-browser, OU=INSBU, O=cisco, L=SJ, ST=CA, C=USA
Issuer: CN=NDB-browser, OU=INSBU, O=cisco, L=SJ, ST=CA, C=USA
Serial number: b404be5
Valid from: Sun Jan 06 20:22:05 PST 2019 until: Mon Jan 06 20:22:05 PST 2020
Certificate fingerprints:
         MD5:  71:07:F6:4E:57:6A:08:3A:AD:06:32:B3:6C:5F:8F:52
         SHA1: 04:08:B9:D5:B7:EB:ED:E0:F9:22:49:14:FA:C6:09:39:22:32:43:A2
         SHA256:
34:D9:EB:34:0A:52:D1:4A:DD:F1:8B:14:D0:84:E4:1C:57:8B:2B:99:9B:E5:A1:4C:C7:8C:CD:AE:24:31:49:75
         Signature algorithm name: SHA256withRSA
         Version: 3

Extensions:

#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 63 8A 92 8F 6F 0F 45 BD   EE 55 C5 A8 99 3B F6 F7  c...o.E..U...;..
0010: AC FA 4A 21                                        ..J!
]
]
```

```
*****************************************
*****************************************
```

ステップ 5 自己署名証明書は、ブラウザと互換性のない JKS 形式で生成されます。ブラウザに証明書をインポートする前に、これらの証明書を PKCS12 形式に変換する必要があります。JKS 形式の証明書を PKCS12 形式に変換するには、次の手順を実行します。**keytool** コマンドを使用して、JKS 形式の証明書を PKCS12 形式に変換します。

（注） 変換する前に必ず元の証明書のコピーをとっておいてください。

例：

```
keytool -importkeystore -srckeystore keystore -srcstorepass cisco123 -srckeypass cisco123
-destkeystore keystore.p12 -deststoretype PKCS12 -srcalias cisco -deststorepass cisco123 -destkeypass
cisco123
```

（注） **keytool** コマンドの入力は、UI 証明書の生成中に提供される入力と一致する必要があります。

（注） 結果として得られる証明書ファイル（keystore.p12）は PKSC12 形式です。

ステップ 6 CA 証明書を Web ブラウザの信頼ルート証明書ストアにアップロードします。証明書を信頼ルート証明書ストアストアに追加する方法については、それぞれの Web ブラウザのヘルプを参照してください。証明書を Web ブラウザにアップロードするときにプロンプトが表示されたら、証明書の作成中に作成したパスワードを使用します。

ステップ 7 ゲスト シェルを再起動して、NDB を再起動します。

WebUI ブラウザと NDB サーバー間の TLS サードパーティ証明書の生成

Web ブラウザと集中モードで実行されている NDB サーバー間の通信を保護できます。このセクションでは、CA 証明書を生成し、証明書を JKS 形式に変換し、証明書を Web ブラウザーにアップロードする方法について説明します。CA証明書を生成するには、証明書署名要求（CSR）を生成し、認証局（CA）に送信して検証を受ける必要があります。オープン ソース ツールを使用して CSR を生成できます。

- WebUI ブラウザと集中モードで実行されている NDB サーバーの間で TLS サード パーティ証明書を生成する

集中型モードで実行中の WebUI ブラウザと NDB サーバーの間での TLS サードパーティ証明書の生成

次の手順を実行して、WebUI ブラウザと集中モードで実行されている NDB サーバーとの間で TLS サードパーティ証明書を生成します。

ステップ 1 **openssl req** コマンドを使用して証明書署名要求（CSR）を生成します。

例：

```
[root@NDB-server ~]# openssl req -newkey rsa:2048 -sha256 -keyout ndb-server.key -keyform PEM -out
 ndb-server.req -outform PEM
Generating a 2048 bit RSA private key
...+++
.............................................+++
writing new private key to 'ndb-server.key'
Enter PEM pass phrase:  cisco123
Verifying - Enter PEM pass phrase:  cisco123
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:US
State or Province Name (full name) [Berkshire]:CA
Locality Name (eg, city) [Newbury]:SJ
Organization Name (eg, company) [My Company Ltd]:cisco
Organizational Unit Name (eg, section) []:insbu
Common Name (eg, your name or your server's hostname) []:ndb-server.cisco.com
Email Address []:chburra@cisco.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:cisco123
An optional company name []:cisco123


[root@NDB-server ~]# ls
ndb-server.req   ndb-server.key
```

（注） ndb-server.req（CSR）ファイルは、証明書発行機関（CA）に提出されます。

（注） CA が提供する証明書をブラウザにエクスポートする時と同じ情報を使用する必要があります。CSR ファイル、cert.req が CA に提出されます。

ステップ 2 CSR 要求を確認または表示するには、**openssl req** コマンドを使用します。

例：

```
[root@NDB-server ~]# openssl req -noout -text -in ndb-server.req
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=US, ST=CA, L=SJ, O=cisco, OU=insbu,
CN=ndb-server.cisco.com/emailAddress=chburra@cisco.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:b5:30:75:e8:c8:5f:05:3b:0e:4f:aa:00:d9:64:
                    8d:bf:b2:80:20:56:c3:be:b0:4c:e0:52:e5:be:d8:
                    d2:74:85:4e:8a:ba:d3:1e:30:76:bf:e5:de:7d:51:
                    11:79:8e:bc:96:38:7a:23:5a:26:31:50:50:fa:29:
                    44:ab:56:b6:0d:41:38:ba:d1:d5:b4:e3:ba:a3:6c:
                    4a:35:73:27:d9:fd:5c:4b:21:85:1a:f9:4d:b0:9e:
                    f3:ae:ce:49:98:ef:a2:f8:11:ab:bd:7e:64:ee:68:
                    68:19:6e:8f:3c:54:30:0f:28:01:13:b0:3d:34:b8:
                    f9:f5:cc:4a:84:d8:e5:d2:27:47:cc:83:76:92:ad:
                    92:62:f3:a3:35:be:14:ce:38:af:2a:c5:2e:fa:b8:
                    31:6b:71:cd:56:00:1f:0d:cc:b0:f8:fc:b0:52:91:
                    f8:9c:cf:45:13:c9:b5:86:fa:30:dd:88:78:01:15:
                    fb:5c:c9:6f:5b:b7:80:28:6c:86:54:c0:f2:5f:35:
                    70:82:49:5c:79:1c:f2:23:dd:50:d5:47:12:37:a3:
                    3f:f9:1d:90:8f:c0:e8:18:09:2e:66:8d:c3:72:17:
                    7f:7d:27:da:b1:cc:26:2d:8c:6b:ee:c5:e8:b5:78:
                    31:7c:bb:ba:6d:2c:e5:a3:29:7e:c1:4a:93:19:ed:
                    9a:e7
                Exponent: 65537 (0x10001)
        Attributes:
            unstructuredName         :cisco123
            challengePassword        :cisco123
    Signature Algorithm: sha256WithRSAEncryption
        9c:9a:51:e0:1d:e4:0b:8f:c1:c6:f5:e0:d2:f6:30:0e:18:af:
        a7:b2:a4:4a:57:d7:07:44:cd:9c:fa:2d:0e:8b:c9:31:5b:16:
        6b:84:42:0b:ed:06:5c:ed:30:d8:9b:ee:5d:79:f4:8a:e3:52:
        3c:b3:4a:eb:6c:22:a2:f4:35:80:28:3a:67:62:7f:5f:dc:80:
        e0:74:f0:3c:39:26:39:3a:76:6a:6a:98:e9:68:f9:b7:58:bf:
        e7:44:2e:e7:73:0a:9c:62:28:b2:c6:09:41:81:b2:53:46:14:
        e6:e4:dc:ca:90:81:5a:5e:dc:1b:dc:36:2c:86:5f:37:29:4c:
        b0:ee:85:2b:34:f2:82:8a:d4:fc:a0:ce:10:e4:44:4e:d0:7a:
        37:6d:3e:f9:ff:a1:19:8c:db:06:bf:be:87:57:a1:cb:05:15:
        0b:9f:6c:8b:c2:ad:22:25:10:f0:4d:0f:4d:b7:be:71:87:f7:
        85:24:e7:2d:f9:59:86:1a:b7:88:57:16:93:31:1f:d7:e5:07:
        42:77:00:f9:ac:44:3b:6c:35:0f:80:5d:00:6f:ea:be:fe:e7:
        28:53:0c:6b:5f:0c:76:bf:8c:a7:60:57:63:05:06:ff:ac:3d:
        f1:63:54:d0:d0:13:44:b1:e9:53:6b:32:11:e2:83:26:04:f5:
        23:67:6b:de
```

ステップ 3 秘密キー、ndb-server.key はパスフレーズでセキュアされます。証明書秘密キーを復号する必要があります。秘密キーは **openssl rsa** コマンドを使用して復号します。

例：

```
[root@NDB-server ~]# cp ndb-server.key  ndb-server.keybkp
[root@NDB-server ~]# rm ndb-server.key
 [root@NDB-server ~]# openssl rsa -in ndb-server.keybkp -out ndb-server.key
Enter pass phrase for ndb-server.keybkp: cisco123
writing RSA key
```

（注） ndb-server.req ファイルのデータは、サード パーティの証明機関に提出する必要があります。関連する手順に従って、証明書ファイルを取得します。

選択する CA の階層により、各 CSR に対して最大 3 つの証明書（証明書チェーン）を取得できます。このことは、各 NDB スイッチに対する CA から 3 つの証明書（root、中間、ドメイン）の取得を意味します。証明書のそれぞれのタイプを識別するためには、CA を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。例：qvrca2.cer（root）、hydsslg2.cer（中間）、ndb-server.cisco.com-39891.cer（ドメイン）。

証明書はほとんどの場合、.PEM ファイル形式で共有されます。

ステップ 4 cat コマンドを使用して 3 つの証明書ファイルから 1 つの証明書ファイルを作成します。この連結は、ドメイン証明書、root 証明書、中間証明書の順番で行われます。cat コマンドのシンタックス：**cat** *domain certificate root certificate intermediate certificate* > *ndb-server.cer*

例：

```
[root@NDB-server ~]# cat ndb-server.cisco.com-39891.cer qvrca.cer hydsslg2.cer > ndb-server.cer
```

ステップ 5 新しく作成した server.cer ファイルを編集して、連結された END 行と BEGIN 行を分割します。ファイルで何かを削除しないでください。

例：

```
-----END CERTIFICATE----------BEGIN CERTIFICATE-----


////// Modify the above line like this by adding a line feed between the two.
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
```

ステップ 6 ndb-server.cer および ndb-server.key ファイルを使用して TLS NDB サーバー キーストア ファイルを作成します。copy コマンドを使用して、スイッチにファイルをコピーします。

例：

```
cp ndb-server.key ndb-server-ndb-privatekey.pem
      cp ndb-server.cer ndb-server-ndb-cert.pem
```

ステップ 7 cat コマンドを使用して、秘密鍵と証明書ファイルを単一の .PEM ファイルに結合します。

例：

```
cat ndb-server-ndb-privatekey.pem  ndb-server-ndb-cert.pem > ndb-server-ndb.pem
```

ステップ 8 CA が PEM 形式で証明書を提供し、証明書の拡張子は .pem です。PEM 形式の証明書を PKCS12 形式に変換する必要があります。PEM ファイルである ndb-server-ndb.pem を **openssl pkcs12** コマンドを使用し

て、.P12 ファイル形式に変更します。指示メッセージが表示されたらエクスポート パスワードを入力します。パスワードには少なくとも 6 文字が含まれなければなりません。例：cisco123 ndb-server-ndb.pem ファイルはパスワード保護された ndb-server-ndb.p12 ファイルに変換されます。

例：

```
[root@NDB-server ~]# openssl pkcs12 -export -out ndb-server-ndb.p12 -in ndb-server-ndb.pem
Enter Export Password:□cisco123
Verifying - Enter Export Password:□cisco123
```

ステップ 9 **keytool** コマンド を使用して、ndb-server-ndb.p12 をパスワード保護された Java キーストア（ndb-server-keystore）ファイルに変換します。このコマンドは、sw1-ndb.p12 ファイルをパスワードで保護された ndb-server-keystore ファイルに変換します。宛先 JKS ストアの新しいパスワードを作成し、プロンプトが表示されたら送信元キーストアのパスワードを入力します。

例：

```
[root@NDB-server ~]# .(relativePath)/keytool -importkeystore -srckeystore ndb-server-ndb.p12
-srcstoretype pkcs12 -destkeystore ndb-server-keystore -deststoretype jks
Enter destination keystore password:□cisco123
Re-enter new password:□cisco123
Enter source keystore password:--cisco123
Entry for alias 1 successfully imported.
Import command completed:  1 entries successfully imported, 0 entries failed
or cancelled
[root@NDB-server ~]#
```

ステップ 10 **keytool** コマンドを使用して、java tlsKeyStore のコンテンツをリストして検証します。

例：

```
[root@NDB-server ~]#.(relativePath)/keytool -list -v -keystore ndb-server-keystore
```

ステップ 11 証明書の生成中に提供されたキー ストア パスワードを使用して、`jetty-ssl-context.xml`（ndb/configuration/etc に格納）を構成します。VI エディタを使用して、KeyStorePath、KeyStorePassword、TrustStorePath、TrustStorePassword で次の行を編集できます。

例：

```
<Set name="KeyStorePath"><Property name="jetty.base" default="." />/<Property
name="jetty.sslContext.keyStorePath" deprecated="jetty.keystore"
default="configuration/ndb-server-keystore"/></Set>
<Set name="KeyStorePassword"><Property name="jetty.sslContext.keyStorePassword"
deprecated="jetty.keystore.password" default="cisco123"/></Set>

<Set name="KeyManagerPassword"><Property name="jetty.sslContext.keyManagerPassword"
deprecated="jetty.keymanager.password" default="cisco123"/></Set>
<Set name="TrustStorePath"><Property name="jetty.base" default="." />/<Property
name="jetty.sslContext.trustStorePath" deprecated="jetty.truststore"
default="configuration/ndb-server-keystore"/></Set>

<Set name="TrustStorePassword"><Property name="jetty.sslContext.trustStorePassword"
deprecated="jetty.truststore.password" default="cisco123"/></Set>
```

ステップ 12 NDB を再起動します。

ステップ 13 CA 証明書を Web ブラウザの信頼ルート証明書ストアにアップロードします。証明書を信頼ルート証明書ストア ストアに追加する方法については、それぞれの Web ブラウザのヘルプを参照してください。証

明書を Web ブラウザにアップロードするときにプロンプトが表示されたら、証明書の作成中に作成したパスワードを使用します。

ゲストシェル環境を使用して、組み込みモードで実行されている Web ブラウザと NDB サーバー間で TLS サード パーティ証明書を生成する

ゲスト シェル環境を使用して、組み込みモードで実行されている Web ブラウザと NDB サーバーの間で TLS サード パーティ証明書を生成するには、次の手順を実行します。

ステップ 1 feature コマンドを使用して、スイッチで bash-shell 機能を有効にします。

例：

```
N9396TX-116(config)# feature bash-shell
```

ステップ 2 run コマンドを使用して、スイッチで bash-shell モードを開始します。

例：

```
N9396TX-116(config)# run bash
bash-4.2$
```

ステップ 3 **openssl req** コマンドを使用して証明書署名要求（CSR）を生成します。プロンプトが表示されたら、必要な情報を入力します。

例：

```
bash-4.2$ openssl req -newkey rsa:2048 -sha256 -keyout ndb-server.key -keyform PEM -out
ndb-server.req -outform PEM
Generating a 2048 bit RSA private key
...+++
.............................................+++
writing new private key to 'ndb-server.key'
Enter PEM pass phrase:  cisco123
Verifying - Enter PEM pass phrase:  cisco123
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:US
State or Province Name (full name) [Berkshire]:CA
Locality Name (eg, city) [Newbury]:SJ
Organization Name (eg, company) [My Company Ltd]:cisco
Organizational Unit Name (eg, section) []:insbu
Common Name (eg, your name or your server's hostname) []:ndb-server.cisco.com
Email Address []:chburra@cisco.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:cisco123
An optional company name []:cisco123
```

```
bash-4.2$ ls

ndb-server.req   ndb-server.key
```

（注） openssl コマンドは、秘密キー ndb-server.key と証明書署名要求ファイル ndb-server.req を作成します。ndb-server.req（CSR）ファイルが証明書発行機関（CA）に送信されます。

（注） CA が提供する証明書をブラウザにエクスポートするときは、同じ情報を使用する必要があります。CSR ファイル cert.req が CA に送信されます。

ステップ 4 コンテンツを表示したり、CSR 要求を確認したりするには、**openssl req** コマンドを使用します。

例：

```
bash-4.2$ openssl req -noout -text -in ndb-server.req
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=US, ST=CA, L=SJ, O=cisco, OU=insbu,
CN=ndb-server.cisco.com/emailAddress=chburra@cisco.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:b5:30:75:e8:c8:5f:05:3b:0e:4f:aa:00:d9:64:
                    8d:bf:b2:80:20:56:c3:be:b0:4c:e0:52:e5:be:d8:
                    d2:74:85:4e:8a:ba:d3:1e:30:76:bf:e5:de:7d:51:
                    11:79:8e:bc:96:38:7a:23:5a:26:31:50:50:fa:29:
                    44:ab:56:b6:0d:41:38:ba:d1:d5:b4:e3:ba:a3:6c:
                    4a:35:73:27:d9:fd:5c:4b:21:85:1a:f9:4d:b0:9e:
                    f3:ae:ce:49:98:ef:a2:f8:11:ab:bd:7e:64:ee:68:
                    68:19:6e:8f:3c:54:30:0f:28:01:13:b0:3d:34:b8:
                    f9:f5:cc:4a:84:d8:e5:d2:27:47:cc:83:76:92:ad:
                    92:62:f3:a3:35:be:14:ce:38:af:2a:c5:2e:fa:b8:
                    31:6b:71:cd:56:00:1f:0d:cc:b0:f8:fc:b0:52:91:
                    f8:9c:cf:45:13:c9:b5:86:fa:30:dd:88:78:01:15:
                    fb:5c:c9:6f:5b:b7:80:28:6c:86:54:c0:f2:5f:35:
                    70:82:49:5c:79:1c:f2:23:dd:50:d5:47:12:37:a3:
                    3f:f9:1d:90:8f:c0:e8:18:09:2e:66:8d:c3:72:17:
                    7f:7d:27:da:b1:cc:26:2d:8c:6b:ee:c5:e8:b5:78:
                    31:7c:bb:ba:6d:2c:e5:a3:29:7e:c1:4a:93:19:ed:
                    9a:e7
                Exponent: 65537 (0x10001)
        Attributes:
            unstructuredName         :cisco123
            challengePassword        :cisco123
    Signature Algorithm: sha256WithRSAEncryption
        9c:9a:51:e0:1d:e4:0b:8f:c1:c6:f5:e0:d2:f6:30:0e:18:af:
        a7:b2:a4:4a:57:d7:07:44:cd:9c:fa:2d:0e:8b:c9:31:5b:16:
        6b:84:42:0b:ed:06:5c:ed:30:d8:9b:ee:5d:79:f4:8a:e3:52:
        3c:b3:4a:eb:6c:22:a2:f4:35:80:28:3a:67:62:7f:5f:dc:80:
        e0:74:f0:3c:39:26:39:3a:76:6a:6a:98:e9:68:f9:b7:58:bf:
        e7:44:2e:e7:73:0a:9c:62:28:b2:c6:09:41:81:b2:53:46:14:
        e6:e4:dc:ca:90:81:5a:5e:dc:1b:dc:36:2c:86:5f:37:29:4c:
        b0:ee:85:2b:34:f2:82:8a:d4:fc:a0:ce:10:e4:44:4e:d0:7a:
        37:6d:3e:f9:ff:a1:19:8c:db:06:bf:be:87:57:a1:cb:05:15:
        0b:9f:6c:8b:c2:ad:22:25:10:f0:4d:0f:4d:b7:be:71:87:f7:
        85:24:e7:2d:f9:59:86:1a:b7:88:57:16:93:31:1f:d7:e5:07:
        42:77:00:f9:ac:44:3b:6c:35:0f:80:5d:00:6f:ea:be:fe:e7:
        28:53:0c:6b:5f:0c:76:bf:8c:a7:60:57:63:05:06:ff:ac:3d:
```

```
        f1:63:54:d0:d0:13:44:b1:e9:53:6b:32:11:e2:83:26:04:f5:
        23:67:6b:de
```

ステップ 5 秘密キー ndb-server.key は、パスフレーズで保護されています。証明書の秘密キーの暗号化を解除する必要があります。**openssl rsa** コマンドを使用して秘密キーの暗号化を解除します。

例：

```
bash-4.2$ cp ndb-server.key  ndb-server.keybkp
bash-4.2$ rm ndb-server.key
bash-4.2$ openssl rsa -in ndb-server.keybkp -out ndb-server.key
Enter pass phrase for ndb-server.keybkp: cisco123
writing RSA key
```

（注） 選択する CA の階層により、各 CSR に対して最大 3 つの証明書（証明書チェーン）を取得できます。このことは、各 NDB スイッチに対する CA から 3 つの証明書（root、中間、ドメイン）の取得を意味します。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。例：qvrca2.cer（root）、hydsslg2.cer（中間）、ndb-server.cisco.com-39891.cer（ドメイン）。

証明書はほとんどの場合、.PEM ファイル形式で共有されます。

ステップ 6 cat コマンドを使用して 3 つの証明書ファイルから 1 つの証明書ファイルを作成します。この連結は、ドメイン証明書、root 証明書、中間証明書の順番で行われます。cat コマンドのシンタックス：**cat** *domain certificate root certificate intermediate certificate > ndb-server.cer*

例：

```
bash-4.2$ cat ndb-server.cisco.com-39891.cer qvrca.cer hydsslg2.cer > ndb-server.cer
```

ステップ 7 新しく作成した server.cer ファイルを編集して、連結された END 行と BEGIN 行を分割します。ファイルで何も削除しないでください。

例：

```
-----END CERTIFICATE----------BEGIN CERTIFICATE-----


////// Modify the above line like this by adding a line feed between the two.
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
```

ステップ 8 ndb-server.cer および ndb-server.key ファイルを使用して TLS NDB サーバー キーストア ファイルを作成します。**copy** コマンドを使用して、スイッチにファイルをコピーします。

例：

```
cp ndb-server.key ndb-server-ndb-privatekey.pem
      cp ndb-server.cer ndb-server-ndb-cert.pem
```

ステップ 9 **cat** コマンドを使用して、秘密キーと証明書ファイルを単一の .PEM ファイルに結合します。

例：

```
cat ndb-server-ndb-privatekey.pem  ndb-server-ndb-cert.pem > ndb-server-ndb.pem
```

ステップ 10 CA は PEM 形式の証明書を提供し、証明書の拡張子は .pem です。PEM 形式の証明書を PKCS12 形式に変換する必要があります。PEM ファイルである ndb-server-ndb.pem を **openssl pkcs12** コマンドを使用して、.P12 ファイル形式に変更します。指示メッセージが表示されたらエクスポート パスワードを入力し

ます。パスワードには少なくとも 6 文字が含まれなければなりません。例：cisco123 ndb-server-ndb.pem ファイルはパスワード保護された ndb-server-ndb.p12 ファイルに変換されます。

例：

```
bash-4.2$ openssl pkcs12 -export -out ndb-server-ndb.p12 -in ndb-server-ndb.pem
Enter Export Password:□cisco123
Verifying - Enter Export Password:□cisco123
```

ステップ 11 証明書ファイルを NDB 構成フォルダーにコピーします。

例：

```
bash-4.2$ sudo cp ndb-server-ndb.p12
/isan/vdc_1/virtual-instance/guestshell+/rootfs/usr/bin/ndb/configuration/
```

ステップ 12 **exit** コマンドを使用して、bash シェル モードを終了します。

例：

```
bash-4.2$ exit
exit
N9396TX-116#
```

ステップ 13 guestshell コマンドを使用してゲスト シェルに接続します。

例：

```
N9396TX-116# guestshell
[admin@guestshell ~]$
```

ステップ 14 現在のディレクトリを ndb/configuration に変更します。

例：

```
[admin@guestshell ~]$ cd ndb/configuration
```

ステップ 15 **keytool** コマンドを使用して、ndb-server-ndb.p12 をパスワードで保護された Java KeyStore（ndb-server-keystore）ファイルに変換します。このコマンドは、ndb-server-ndb.p12 ファイルをパスワードで保護された ndb-server-keystore ファイルに変換します。宛先 JKS ストアの新しいパスワードを作成し、プロンプトが表示されたら送信元キーストアのパスワードを入力します。

例：

```
[admin@guestshell configuration]$ keytool -importkeystore -srckeystore ndb-server-ndb.p12
-srcstoretype pkcs12 -destkeystore ndb-server-keystore -deststoretype jks
Enter destination keystore password: □cisco123
Re-enter new password: □cisco123
Enter source keystore password: □cisco123
Entry for alias 1 successfully imported.
Import command completed:  1 entries successfully imported, 0 entries failed or cancelled
```

ステップ 16 **keytool** コマンドを使用して、java tlsKeyStore のコンテンツをリストして検証します。

例：

```
[admin@guestshell configuration]$ keytool -list -v -keystore ndb-server-keystore
```

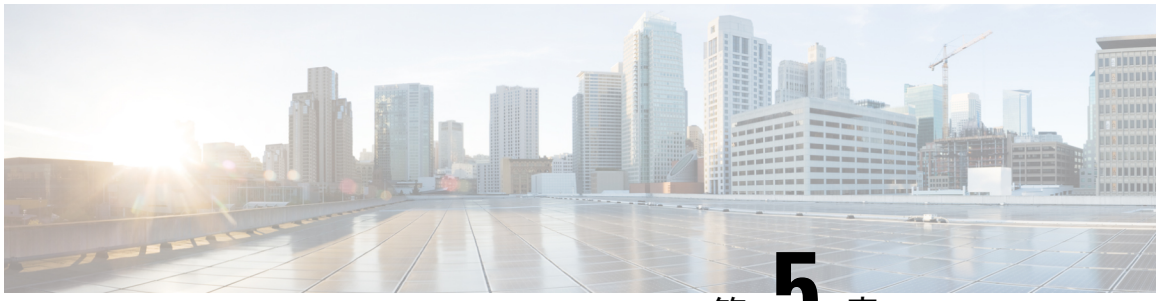
ステップ 17 証明書の生成中に提供されたキー ストア パスワードを使用して、jetty-ssl-context.xml（ndb/etc に格納）を構成します。VI エディタを使用して、keystore および keystorepass で次の行を編集できます。

例：

```
<Set name="KeyStorePath"><Property name="jetty.base" default="." />/<Property
name="jetty.sslContext.keyStorePath" deprecated="jetty.keystore"
default="configuration/ndb-server-keystore"/></Set>
<Set name="KeyStorePassword"><Property name="jetty.sslContext.keyStorePassword"
deprecated="jetty.keystore.password" default="cisco123"/></Set>

<Set name="KeyManagerPassword"><Property name="jetty.sslContext.keyManagerPassword"
deprecated="jetty.keymanager.password" default="cisco123"/></Set>

<Set name="TrustStorePath"><Property name="jetty.base" default="." />/<Property
name="jetty.sslContext.trustStorePath" deprecated="jetty.truststore"
default="configuration/ndb-server-keystore"/></Set>

<Set name="TrustStorePassword"><Property name="jetty.sslContext.trustStorePassword"
deprecated="jetty.truststore.password" default="cisco123"/></Set>
```

ステップ 18 CA 証明書を Web ブラウザの信頼ルート証明書ストアにアップロードします。証明書を信頼ルート証明書ストア ストアに追加する方法については、それぞれの Web ブラウザのヘルプを参照してください。証明書を Web ブラウザにアップロードするときにプロンプトが表示されたら、証明書の作成中に作成したパスワードを使用します。

ステップ 19 NDB を再起動します。



第 5 章

Nexus Dashboard でのアプリとしての Nexus Dashboard Data Broker の TLS の管理

この章には、次の詳細が含まれています。

アプリにおける NXAPI に対して NDB サーバーと NDB スイッチの間での TLS 自己署名証明書の生成

このセクションでは、アプリ展開で NDB サーバーと NDB スイッチの間で TLS 自己署名証明書を生成する方法について説明します。TLS を有効にするには、スイッチごとに証明書とキーを生成する必要があります。NDBswitch と NDB サーバー間の TLS 通信は、ポート 443 のみを使用します。

NDB サーバーと NXAPI の NDB スイッチの間で TLS 自己署名証明書を生成するには、次の手順を実行します。

（注） TLS を構成した後でポート 80 を使用して、通信するためのコントローラを構成できません。

自己署名証明書とキーの生成

この手順で、自己署名証明書を生成します。

始める前に

スイッチの完全修飾ドメイン名（FQDN）として機能する各 NDB スイッチに対して ip domain-name コマンドを使用して、スイッチにドメイン名が構成されていることを確認してください。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 に対して構成されます。

ステップ 1 ルート ユーザーとしてアプリ コンテナの 1 つにログインします。

ND/ APIC コンテナにログインするためには、Cisco Nexus Dashboard のコンテナへのログイン （71 ページ） または Cisco APIC のコンテナへのログイン （71 ページ） を参照してください。

ステップ 2 **openssl req** コマンドを使用して、秘密キーと自己署名証明書を生成します。

このコマンドは、証明書ファイル（sw1-ca.pem）と秘密キー（sw1-ca.key）を作成します。

```
docker@docker-virtual-machine:~/TLS$ openssl req -x509 -nodes -days 3650 -newkey rsa:2048 -out
sw1-ca.pem -outform PEM -keyout sw1-ca.key

Generating a 2048 bit RSA private key
...+++
.........................................+++
writing new private key to 'sw1-ca.key'

You are about to be asked to enter information that will be incorporated into your certificate
request.
What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few
 fields but you can leave some blank
For some fields there will be a default value, If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:CA Locality Name (eg, city) []:SJ
Organization Name (eg, company) [Internet Widgits Pty Ltd]:cisco Organizational Unit Name (eg,
section) []:insbu
Common Name (e.g. server FQDN or YOUR name) []:N9K-117.cisco.com Email Address []:myname@cisco.com
```

（注） 複数のスイッチがある場合は、スイッチごとに証明書ファイルと秘密キーを生成します。

ステップ 3 **scp** コマンドを使用して、証明書ファイル、sw1-ca.pem とキーファイル、sw1-ca.key をスイッチにコピーします。

例：

```
bash-4.2# scp sw1-ca.key admin@10.16.206.250:/
User Access Verification
Password:
sw1-ca.key
100% 1704   992.7KB/s   00:00
4.6KB/s 00:00

bash-4.2# scp sw1-ca.pem admin@10.16.206.250:/
```

```
User Access Verification
Password:
sw1-ca.key

100% 1704   992.7KB/s   00:00
4.6KB/s 00:00
```

（注） 複数のスイッチがある場合は、すべてのスイッチに対してこの手順を繰り返します。

ステップ 4 **cat** コマンドを使用して、sw1-ca.pem ファイルの内容を取得します。同じ内容をコピーします。

他のすべてのコンテナーに同じ名前のファイルを作成し、コピーした内容を vi エディタを使用してそのファイルに貼り付け、変更したファイルを保存します。同じ手順を実行して、`sw1-ca.key` ファイルの内容をすべてのコンテナにコピーします。

ステップ 5 証明書ファイル、sw1-ca.pem、およびキーファイル、sw1-ca.key を **nxapi** コマンドを使用してスイッチで構成します。

例：

```
N9K-117 (config)# nxapi certificate httpskey keyfile bootflash:sw1-ca.key
Upload done. Please enable. Note cert and key must match.
N9K-117 (config)# nxapi certificate httpscrt certfile bootflash:sw1-ca.pem
Upload done. Please enable. Note cert and key must match.
```

（注） 複数のスイッチがある場合、各スイッチに対して対応する証明書ファイルとプライベート キーを構成します。

ステップ 6 **nxapi certificate** コマンドを使用して、スイッチで自己署名証明書を有効にします。

例：

```
N9K-117 (config)# nxapi certificate enable
```

（注） スイッチで自己署名証明書を有効化する間にエラーがないことを確認します。

ステップ 7 アプリのコンテナーに root ユーザーとしてログインします。

ステップ 8 **copy** コマンドを使用して、sw1-ca.key および sw1-ca.pem ファイルをコピーし、.PEM 形式に変換します。

例：

```
cp sw1-ca.key sw1-ndb-privatekey.pem
cp sw1-ca.pem sw1-ndb-cert.pem
```

ステップ 9 **cat** コマンドを使用して、秘密キーと証明書ファイルを連結します。

例：

```
docker@docker-virtual-machine:~/TLS$ cat sw1-ndb-privatekey.pem sw1-ndb-cert.pem > sw1-ndb.pem
```

ステップ 10 **openssl** コマンドを使用して、.pem ファイルを .p12 ファイル形式に変換します。パスワードで保護された.p12 証明書ファイルを作成するように求められたら、エクスポート パスワードを入力します。

例：

```
docker@docker-virtual-machine:~/TLS$openssl pkcs12 -export -out sw1-ndb.p12 -in sw1-ndb.pem
Enter Export Password: cisco123
```

```
Verifying - Enter Export Password: cisco123
Enter a password at the prompt. Use the same password that you entered in the previous Step
(cisco123
```

ステップ 11 **keytool** コマンドを使用して、sw1-ndb.p12 をパスワードで保護された Java KeyStore (tlsKeyStore) ファイルに変換します。インストールされている java ディレクトリの `jre/bin` を使用します。

例：

```
docker@docker-virtual-machine:~/TLS$ ./(relativePath)/keytool -importkeystore -srckeystore
sw1-ndb.p12
-srcstoretype pkcs12 -destkeystore tlsKeyStore -deststoretype jks
Enter Destination Keystore password:cisco123 Re-enter new password:cisco123
Enter source keystore password:cisco123 Entry for alias 1 successfully imported.
Import command completed: 1 enteries successfully imported, 0 enteries failed or cancelled.
```

（注） デフォルトでは、「1」というエイリアスが最初のスイッチの tlsKeyStore に保存されます。NDB コントローラが複数のスイッチを管理している場合は、すべてのスイッチに対してこの手順を繰り返します。2番目のスイッチを追加すると、ユーティリティによって最初のスイッチのエイリアスの名前を変更でき、2番目のスイッチのエイリアスの名前を変更するプロビジョニングも提供されます。以下に示された例を参照してください。

```
keytool -importkeystore -srckeystore sw2-ndb.p12 -srcstoretype pkcs12 -destkeystore
tlsKeyStore -deststoretype jks
keytool -importkeystore -srckeystore sw3-ndb.p12 -srcstoretype pkcs12 -destkeystore
tlsKeyStore -deststoretype jks
```

ステップ 12 **keytool** コマンドを使用して、java tlsKeyStore のコンテンツを一覧表示して確認します。

例：

```
docker@docker-virtual-machine:~/TLS$ keytool -list -v -keystore tlsKeyStore | more
```

（注） すべてのコンテナーで手順 7 から 12 を繰り返します。

TLS トラストストア ファイルの作成

トラストストアは、1つ以上のスイッチに対して生成される自己署名証明書から作成されます。コントローラでは1つ以上のスイッチに対して証明書を保持します。このセクションでは、自己署名証明書とキーの生成セクションで作成した自己署名証明書を使用してトラストストアを作成する方法について説明します。コントローラーに複数のスイッチがある場合、各スイッチには個別の証明書ファイル（たとえば、sw1-ndb-cert.pem、sw2-ndb-cert.pem）があります。

TLS トラストストア ファイルを生成するには、次の手順を使用します。

（注） すべてのアプリ コンテナーでこの手順を実行します。

ステップ 1 ルートユーザーとしてアプリ コンテナにログインします。

ND/ APIC コンテナにログインするためには、Cisco Nexus Dashboard のコンテナへのログイン （71 ページ） または Cisco APIC のコンテナへのログイン （71 ページ） を参照してください。

ステップ 2 keytool コマンドを使用して、sw1-ndb-cert.pem などの証明書ファイルを Java トラストストア（tlsTrustStore）ファイルに変換します。指示メッセージが表示されたときにパスワードを入力して、パスワード保護された Java TrustStore（tlsTrustStore）ファイルを作成します。パスワードは少なくとも 6 文字でなければなりません。Java ディレクトリにインストールされている jre/bin を使用します。

例：

```
docker@docker-virtual-machine:~/TLS$ ./(relativePath)/keytool -import -alias sw1 -file sw1-ndb-cert.pem
-keystore tlsTrustStore
Enter Export Password: cisco123
Verifying - Enter Export Password: cisco123
Enter a password at the prompt. Use the same password that you entered in the previous Step (cisco123)
```

NDB コントローラが複数のスイッチを管理する場合、すべてのスイッチに対してこの手順を繰り返して、同じ TrustStore にすべてのスイッチを追加してください。次に例を示します。

```
docker@docker-virtual-machine:~/TLS$ keytool -import -alias sw2 -file sw2-ndb-cert.pem
-keystore tlsTrustStore
docker@docker-virtual-machine:~/TLS$ keytool -import -alias sw3 -file sw3-ndb-cert.pem
-keystore tlsTrustStore
// Here sw2 and sw3 are alias for switch 2 and switch 3 for identification purpose.
```

ステップ 3 keytool コマンドを使用して同じ tlsTrustStore の複数のスイッチに対するキーをリストし、検証します。

例：

```
docker@docker-virtual-machine:~/TLS$ keytool -list -v -keystore tlsTrustStore | more
```

TLS での Nexus Dashboard Data Broker の起動

TLS を使用して Nexus Dashboard Data Broker を起動するには、この手順を使用します。

ステップ 1 ルートユーザーとしてアプリ コンテナにログインします。

ND/ APIC コンテナにログインするためには、Cisco Nexus Dashboard のコンテナへのログイン （71 ページ） または Cisco APIC のコンテナへのログイン （71 ページ） を参照してください。

ステップ 2 作成した tlsKeystore および tlsTruststore ファイルをデータ ブローカーの構成フォルダーにコピーします。（/home/app/ndb/configuration - ND の場合および /home/app/local-data/configuration - APIC の場合）。

例：

```
for ND:
cp tlskeystore /home/app/ndb/configuration
cp tlsTrustStore /home/app/ndb/configuration
```

```
for APIC:
cp tlskeystore /home/app/local-data/configuration
cp tlsTrustStore /home/app/local-data/configuration
```

（注） すべてのアプリ コンテナで手順 1 と 2 を実行します。

ステップ 3 ホスト上のアプリ タイルからアプリを再起動します。

Nexus Dashboard Data Broker での TLS KeyStore と TrustStore パスワードの構成

Nexus Dashboard Data Broker がパスワードで保護された TLS KeyStore および TrustStore ファイルを読み取れるようにするには、TLS KeyStore および TrustStore パスワードを構成する必要があります。Nexus Dashboard Data Broker で TLS KeyStore と TrustStore のパスワードを構成するには、次の手順を実行します。

（注） すべてのコンテナでこの手順を実行します。

ステップ 1 ルート ユーザーとしてアプリ コンテナにログインします。

ND/ APIC コンテナにログインするためには、Cisco Nexus Dashboard のコンテナへのログイン （71 ページ） または Cisco APIC のコンテナへのログイン （71 ページ） を参照してください。

ステップ 2 `bin` ディレクトリに移動します。

例：`cd /home/app/ndb/bin`

ステップ 3 **ndb config-keystore-passwords** コマンドを使用して、TLS キーストアとトラストストアのパスワードを構成します。

例：

```
./ndb config-keystore-passwords --user admin --password admin --url https://localhost:8443
--verbose --prompt --keystore-password keystore_password --truststore-password truststore_password
```

このコマンドでパスワードの入力を求められたら、*admin* と入力します。

（注） KeyStore と TrustStore のパスワードのみがユーザー定義です。

TLS が Nexus Dashboard Data Broker で有効になった後で、Nexus Dashboard Data Broker サーバーと Nexus Dashboard Data Broker スイッチの間のすべての接続が ポート 443 を使用して確立されます。ポート 443 を使用するように Nexus Dashboard Data Broker のデバイス接続を変更してください。

これらの手順を正常に完了したら、ポート 443 を使用してコントローラにネクサス スイッチを追加できます。スイッチの FQDN を使用して、Nexus Dashboard Data Broker コントローラにデバイスを追加します。スイッチの WebUI サンドボックス分析を使用して、証明書情報を検証します。

アプリの NXAPI に対して NDB サーバーと NDB スイッチの間での TLS サード パーティ証明書の生成

このセクションでは、NDB サーバーと NDB スイッチの間で TLS サード パーティ証明書を生成する方法について説明します。ネットワーク内のスイッチごとに個別の証明書とキーを要求する必要があります。NDB サーバーと NDB スイッチの間で TLS 通信は、ポート 443 のみを使用します。

認証局から証明書の取得

2 つの方法で認証局（CA）から証明書を取得できます。秘密キーと証明書の両方に対して CA に直接アプローチすることができます。CA は、CA の署名を発行した公開キーを含む証明書とともに、あなたに代わって秘密キーを生成します。

もう 1 つのアプローチでは、openssl などのツールを使用して秘密キーを生成し、証明書発行機関への証明書署名要求（CSR）を生成できます。CA は CSR からのユーザー識別情報を使用して、公開キーで証明書を生成します。

始める前に

スイッチの完全修飾ドメイン名（FQDN）として機能する各 NDB スイッチに対して ip domain-name コマンドを使用して、スイッチにドメイン名が設定されてい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 に対して構成されます。

ステップ 1 ルート ユーザーとしてアプリ コンテナの 1 つにログインします。

ND/ APIC コンテナにログインするためには、Cisco Nexus Dashboard のコンテナへのログイン （71 ページ） または Cisco APIC のコンテナへのログイン （71 ページ） を参照してください。

ステップ 2 **openssl** コマンドを使用して、秘密キー（cert.key）と証明書署名要求（cert.req）を生成します。

例：

```
docker@docker-virtual-machine:~/Mallik/TLS_CA$ openssl req -newkey rsa:2048 -sha256 -keyout cert.key
```

```
-keyform PEM -out cert.req -outform PEM

Generating a 2048 bit RSA private key
.............+++
.....................+++
writing new private key to 'cert.key'
Enter PEM pass phrase:  cisco123 Verifying - Enter PEM pass phrase: cisco123

You are about to be asked to enter information that will be incorporated into your certificate
request.
What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few
 fields but you can leave some blank

For some fields there will be a default value, If you enter '.', the field will be left blank.

Country Name (2 letter code) [GB]:US
State or Province Name (full name) [Berkshire]:CA Locality Name (eg, city) [Newbury]:SJ
Organization Name (eg, company) [My Company Ltd]:cisco Organizational Unit Name (eg, section)
[]:insbu
Common Name (eg, your name or your server's hostname) []:N9K-117.cisco.com Email Address
[]:myname@cisco.com

Please enter the following 'extra' attributes to be sent with your certificate request
A challenge password []:   cisco123 An optional company name []: cisco123


docker@docker-virtual-machine: # ls
cert.key cert.req
```

ステップ 3 **openssl** コマンドを使用して CSR を確認します。

例：

```
docker@docker-virtual-machine:~/Mallik/TLS_CA$ openssl req -noout -text -in cert.req
```

ステップ 4 秘密キーは、セキュリティ パスフレーズを使用して生成されます。秘密キーの暗号化を解除する必要がある場合があります。秘密キーからパスフレーズを削除するには、**openssl** コマンドを使用します。

例：

```
docker@docker-virtual-machine:~/Mk/TLS_CA$ ls
cert.key cert.req
docker@docker-virtual-machine:~/Mk/TLS_CA$cp cert.key cert.keybkp
docker@docker-virtual-machine:~/Mk/TLS_CA$ rm cert.key
docker@docker-virtual-machine:~/Mk/TLS_CA$ openssl rsa -in cert.keybkp -out cert.key

Enter pass phrase for cert.keybkp: cisco123
```

（注） この手順を繰り返して、すべてのスイッチの秘密キーからパスフレーズを削除します。

選択する CA の階層により、各 CSR に対して最大 3 つの証明書（証明書チェーン）を取得できます。このことは、各 NDB スイッチに対する CA から 3 つの証明書（root、中間、ドメイン）の取得を意味します。証明書のそれぞれのタイプを識別するためには、CA を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。例: test-root-ca-2048.cer（ルート）、test-ssl-ca.cer（中間）、N9K-117.cisco.com.cer（ドメイン）。

証明書はほとんどの場合、.PEM ファイル形式で共有されます。cert.req ファイルのデータは、サードパーティの証明機関に提出する必要があります。関連する手順に従って、3 つの（証明書）ファイルを取得します。

ステップ 5 **cat** コマンドを使用して、3 つの証明書ファイルから 1 つの証明書ファイルを作成します。この連結は、ドメイン証明書、root 証明書、中間証明書の順番で行われます。**cat** コマンドのシンタックス: *cat domain certificateroot certificateintermediate certificate > server.cer*

例：

```
$cat N9K-117.cisco.com.cer test-root-ca-2048.cer test-ssl-ca.cer > server.cer
```

ステップ 6 新しく作成した server.cer ファイルを編集して、連結された END 行と BEGIN 行を分割します。ファイルで何かを削除しないでください。

例：

```
-----END CERTIFICATE----------BEGIN CERTIFICATE-----


////// Modify the above line like this by adding a line feed between the two.
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
```

（注） この手順をすべてのスイッチで繰り返します。

ステップ 7 copy コマンドを使用して、秘密キー（cert.key）と証明書を CA（server.cer）からスイッチにコピーします。

例：

```
bash-4.2# scp server.cer admin@10.16.206.250:/
User Access Verification
Password:
sw1-ca.key
                                                                    100% 1704   992.7KB/s   00:00
4.6KB/s 00:00

bash-4.2# scp cert.key admin@10.16.206.250:/
User Access Verification
Password:
sw1-ca.key

100% 1704   992.7KB/s   00:00
4.6KB/s 00:00
```

（注） この手順をすべてのスイッチで繰り返します。

ステップ 8 cat コマンドを使用して、server.cer ファイルの内容を取得します。同じ内容をコピーします。

他のすべてのコンテナに同じ名前のファイルを作成し、コピーした内容を vi エディターを使用してそのファイルに貼り付け、変更したファイルを保存します。

同じ手順を実行して、cert.key ファイルの内容をすべてのコンテナにコピーします。

ステップ 9 **nxapi** コマンドを使用して、スイッチに証明書ファイル sw1-ca.pem とキーファイル sw1-ca.key を設定します。

例：

```
N9K-117 (config)# nxapi certificate httpskey keyfile bootflash:cert.key Upload done. Please enable.
```

```
 Note cert and key must match. N9K-117 (config)#
N9K-117 (config)# nxapi certificate httpscrt certfile bootflash:server.cer
Upload done. Please enable. Note cert and key must match.
```

（注） 複数のスイッチがある場合は、対応する証明書と秘密キーを各スイッチに構成します。

ステップ 10 nxapi certificate コマンドを使用して、スイッチで自己署名証明書を有効にします。

例：

```
N9K-117 (config)# nxapi certificate enable N9K-117
```

（注） スイッチで自己署名証明書を有効にするときにエラーがないことを確認します。

Nexus Dashboard Data Broker Controller の TLS キーストアとトラストストア ファイル

Nexus Dashboard Data Broker は、証明書とキーを使用してスイッチ間の通信を保護します。キーと証明書をキーストアに保管します。これらのファイルは、Nexus Dashboard Data Broker に tlsTruststore および tlsKeystore ファイルとして保存されます。

Java tlsKeyStore および tlsTrustStor ファイルを生成するには、次の手順を使用します。

ステップ 1 TLS ディレクトリを作成し、そこに移動します。

例：

```
mkdir -p TLS cd TLS
```

ステップ 2 mypersonalca の下に 3 つのディレクトリと 2 つの前提条件ファイルを作成します。

例：

```
mkdir -p mypersonalca/certs
mkdir -p mypersonalca/private
mkdir -p mypersonalca/crl
echo "01" > mypersonalca/serial
touch mypersonalca/index.txt
```

コマンドを使用して、Nexus Dashboard Data Broker に接続されている各スイッチの TLS 秘密キーと認証局（CA）ファイルを生成します。

ステップ 3 「認証局からの証明書の取得」セクションで作成した cert.key と server.cer を現在のディレクトリ（TLS）にコピーします。単一のスイッチの証明書とキー ファイルを選択します。これらのファイルは、コントローラに接続するすべてのスイッチに対して以前に生成されました。現在のスイッチの server.cer と cert.key を使用して、TLS キーストア ファイルを作成します。

複数のスイッチが接続されている場合、各スイッチに対して個別にこの手順を繰り返します。

ステップ 4 **copy** コマンドを使用して、server.cer および cert.key ファイルをコピーし、.PEM 形式に変換します。

例：

```
cp cert.key sw1-ndb-privatekey.pem
cp server.cer sw1-ndb-cert.pem
```

ステップ 5 上記の手順で生成された .pem ファイルをすべてのコンテナにコピーします。

ステップ 6 **cat** コマンドを使用して、秘密キー（sw1-ndb-privatekey.pem）と証明書ファイル（sw1-ndb-cert.pem）を単一の .PEM ファイルに連結します。

例：

```
cat sw1-ndb-privatekey.pem sw1-ndb-cert.pem > sw1-ndb.pem
```

ステップ 7 **openssl** コマンドを使用して、.PEM ファイルを .P12 形式に変換します。指示メッセージが表示されたらエクスポートパスワードを入力します。パスワードには少なくとも6文字が含まれなければなりません。例：cisco123 sw1-ndb.pem ファイルは、パスワードで保護された sw1-ndb.p12 ファイルに変換されます。

例：

```
docker@docker-virtual-machine:~/TLS$openssl pkcs12 -export -out sw1-ndb.p12 -in sw1-ndb.pem
Enter Export Password: cisco123
Verifying - Enter Export Password: cisco123
Enter a password at the prompt. Use the same password that you entered in the previous Step
(cisco123)
```

ステップ 8 **keytool** コマンドを使用して、sw1-ndb.p12 をパスワードで保護された Java KeyStore（tlsKeyStore）ファイルに変換します。このコマンドは、sw1-ndb.p12 ファイルをパスワードで保護された tlsKeyStore ファイルに変換します。

例：

```
docker@docker-virtual-machine:~/TLS$ keytool -importkeystore -srckeystore sw1-ndb.p12 -srcstoretype
 pkcs12 -destkeystore tlsKeyStore -deststoretype jks
Enter Destination Keystore password:cisco123
```

（注） デフォルトでは、「1」というエイリアスが最初のスイッチの tlsKeyStore に保存されます。Nexus Dashboard Data Broker コントローラが複数のスイッチを管理している場合は、すべてのスイッチに対してこの手順を繰り返します。2番目のスイッチを追加すると、ユーティリティにより、最初のスイッチ エイリアスの名前を変更し、新しいスイッチのエイリアスを名前変更するためにプロビジョニングします。たとえば、以下を参照してください。

```
keytool -importkeystore -srckeystore sw2-ndb.p12 -srcstoretype pkcs12 -destkeystore
tlsKeyStore -deststoretype jks
keytool -importkeystore -srckeystore sw3-ndb.p12 -srcstoretype pkcs12 -destkeystore
tlsKeyStore -deststoretype jks
```

ステップ 9 **keytool** コマンドを使用して、java tlsKeyStore のコンテンツを一覧表示して確認します。

例：

```
docker@docker-virtual-machine:~/TLS$ keytool -list -v -keystore tlsKeyStore | more
```

ステップ 10 **keytool** コマンドを使用して、証明書ファイル（sw1-ndb-cert.pem）を Java TrustStore（tlsTrustStore）ファイルに変換します。指示メッセージが表示されたときにパスワードを入力して、パスワード保護された

Java TrustStore（tlsTrustStore）ファイルを作成します。パスワードは少なくとも 6 文字でなければなりません。

例：

```
docker@docker-virtual-machine:~/TLS$ keytool -import -alias sw1 -file sw1-ndb-cert.pem -keystore
 tlsTrustStore
Enter keystore password: cisco123 Re-enter new password: cisco123
Owner: EMAILADDRESS=myname@cisco.com, CN=localhost, OU=insbu, O=cisco, L=SJ, ST=CA, C=US Issuer:
 EMAILADDRESS=myname@cisco.com, CN=localhost, OU=insbu, O=cisco, L=SJ, ST=CA, C=US Serial number:
 c557f668a0dd2ca5
Valid from: Thu Jun 15 05:43:48 IST 2017 until: Sun Jun 13 05:43:48 IST 2027 Certificate
fingerprints:
MD5: C2:7B:9E:26:31:7A:74:25:55:DF:A7:91:C9:5D:20:A3
SHA1: 3C:DF:66:96:72:12:CE:81:DB:AB:58:30:60:E7:CC:04:4D:DF:6D:B2 SHA256:
DD:FB:3D:71:B4:B8:9E:CE:97:A3:E4:2D:D3:B6:90:CD:76:A8:5F:84:77:78:BE:49:6C:04:01:84:62:2C:2F:EB
Signature algorithm name: SHA256withRSA Version: 3

Extensions:

#1: ObjectId: 2.5.29.35 Criticality=false AuthorityKeyIdentifier [
KeyIdentifier [
0000: 0D B3 CF 81 66 4A 33 4E EF 86 7E 26 C3 50 9B 73 ....fJ3N...&.P.s
0010: 38 EF DF 40 8..@
]
]

#2: ObjectId: 2.5.29.19 Criticality=false BasicConstraints:[
CA:true PathLen:2147483647
]

#3: ObjectId: 2.5.29.14 Criticality=false SubjectKeyIdentifier [
KeyIdentifier [
0000: 0D B3 CF 81 66 4A 33 4E EF 86 7E 26 C3 50 9B 73 ....fJ3N...&.P.s
0010: 38 EF DF 40 8..@
]
]

Trust this certificate? [no]: yes Certificate was added to keystore
```

Nexus Dashboard Data Broker コントローラが複数のスイッチを管理している場合は、すべてのスイッチに対してこの手順を繰り返して、すべてのスイッチ キーを同じ TrustStore に追加します。次に例を示します。

```
keytool -import -alias sw2 -file sw2-ndb-cert.pem -keystore tlsTrustStore
keytool -import -alias sw3 -file sw3-ndb-cert.pem -keystore tlsTrustStore
```

ステップ 11 **keytool** コマンドを使用して、同じ tlsTrustStore 内の複数のスイッチのキーを一覧表示して確認します。

例：

```
docker@docker-virtual-machine:~/TLS$ keytool -list -v -keystore tlsTrustStore | more
```

（注） すべてのコンテナで手順 6 ～ 11 を実行します。

次のタスク

TLS を使用して Nexus Dashboard Data Broker を起動します。詳細な手順については、TLS での Nexus Dashboard Data Broker の起動 （63 ページ） を参照してください。

その後、TLS キーストアとトラストストアのパスワードを設定します。詳細な手順については、Nexus Dashboard Data Broker での TLS KeyStore と TrustStore パスワードの構成 （64 ページ） を参照してください。

Cisco Nexus Dashboard のコンテナへのログイン

この手順を使用して、Cisco Nexus Dashboard（ND）のコンテナにログインします。

ステップ 1 ssh と生成された一時的なルート パスワードを使用して、ルート ユーザーとして任意の ND ノードにログインします。

```
ssh root@10.16.206.50
root@10.16.206.50's password: <enter temporary root password here>
[root@ND-1 ~]#
```

ステップ 2 NDDB に関連する利用可能なポッドが一覧表示されます。

例：

```
[root@ND-1 ~]# kubectl -n cisco-ndb get pods
NAME          READY   STATUS    RESTARTS   AGE
ndbserver-0   1/1     Running   0          12d
ndbserver-1   1/1     Running   0          12d
ndbserver-2   1/1     Running   0          12d
```

ステップ 3 **kubectl -n cisco-ndb exec -it <pod-name> -- bash** コマンドを使用して、いずれかのポッドで実行されているコンテナへの bash シェルを取得します。

例：

```
[root@ND-1 ~]# kubectl -n cisco-ndb exec -it ndbserver-0 -- bash
```

Cisco APIC のコンテナへのログイン

この手順を使用して、Cisco APIC のコンテナにログインします。

ステップ 1 ssh と生成された一時的な root パスワードを使用して、root ユーザーとして APIC ノードのいずれかにログインします。

```
ssh root@10.16.206.247
```

```
Application Policy Infrastructure Controller
root@10.16.206.247's password: <enter temporary root password here>
```

ステップ 2 そのノードで実行されている NDDB コンテナが一覧表示されます。

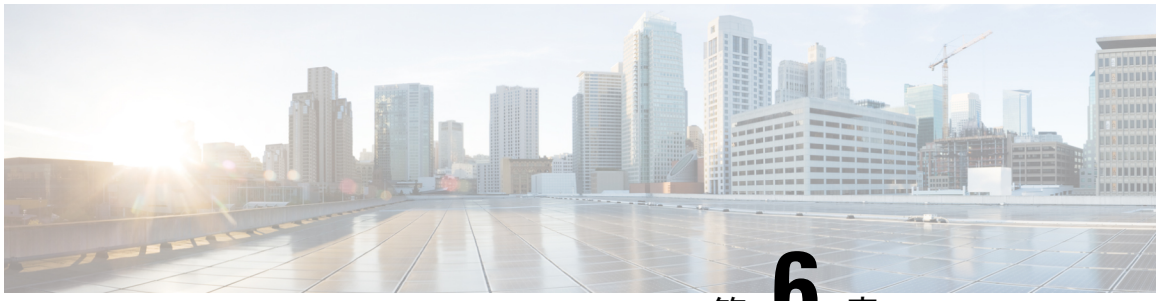
例：

```
[root@apic1 ~]# docker ps | grep ndb
2bb5309cbbae  31d3a284752b  "/opt/bin/conit.bi..."  5 days ago  Up 5 days
ndbserver-c1cf9a4d-ab31-06d3-b8c0-b01840fb6cc9
```

ステップ 3 **docker exec -it <container-id> /bin/bash** コマンドを使用して、そのコンテナに bash シェルを取得します。

例：

```
[root@apic1 ~]# docker exec -it ndbserver-c1cf9a4d-ab31-06d3-b8c0-b01840fb6cc9 /bin/bash
```



第 6 章

Cisco Nexus 9000 シリーズ スイッチの構成

リリース 3.10.1 以降、Cisco Nexus Data Broker (NDB) は Cisco Nexus Dashboard Data Broker に名前が変更されました。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約事項

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、次のガイドラインと制限事項を参照してください。

- Cisco NX-OS リリース 7.0(3)I7(2) 以降では、N9K-X9700-EXおよび N9K-X9700-FX ライン カードを備えた Cisco Nexus 9500 プラットフォーム スイッチの TAP 集約を有効にできます。
- N9K-X9700-EX および N9K-X9700-FX ライン カードで TAP AGG 機能を有効にするには、Cisco Nexus 9500 スイッチで hardware acl tap-agg をグローバルに設定する必要があります。
- Cisco Nexus Dashboard Data Broker は、リリース 7.x 以降の Cisco Nexus 9000 シリーズ デバイス ファミリの NX-API プロトコルをサポートします。
- 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 にあ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 トランクとしてデバイス設定があると想定しています。
- Cisco Nexus 9200 シリーズ スイッチは、Edge SPAN および Edge TAP ポートの Q-in-Q VLAN タギングをサポートしていません。
- Cisco Nexus 9000 シリーズ スイッチの場合、Cisco NX-OS ソフトウェアを Cisco NX-OS リリース 7.x 以降にアップグレードします。
- NX-API プロトコルを介して検出できる Cisco Nexus 9000 シリーズ スイッチを Cisco Nexus Dashboard Data Broker に追加できるようになりました。接続が成功すると、シャーシ モデル 9500 のすべてのラインカード情報が検出されます。
- 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、次の設定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 Dashboard Data Broker は、スイッチ インベントリ、トポロジの相互接続、およびステータスを定期的に再検出します。この情報は、ステータスに応じて GUI で更新されます。再検出間隔は構成でき、再検出間隔のデフォルト値は 10 秒ごとです。

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

	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。	• IPV4 PACL [ifacl] size = 1024 • IPV6 PACL [ipv6-ifacl] size = 0 • MAC PACL [mac-ifacl] size = 512 • Egress IPV4 RACL [e-racl] size = 256 • Egress IPV6 RACL [e-ipv6-racl] size = 0 • Ingress System size = 256 • Ingress System size = 256 • SPAN [span] size = 256 • Ingress COPP [copp] size = 256 Cisco Nexus 9000 シリーズ スイッチでの段階的な TCAM ハードウェア サイジング設定については、『*Cisco Nexus 9000 Series NX-OS Security Configuration Guide*』を参照してください。 （注） OpenFlow モードの Cisco Nexus ダッシュボード データ ブローカは、OpenFlow TCAM リージョンが倍幅として設定されている場合にのみ、イーサネット MAC の送信元アドレスと宛先アドレスを一致機能としてサポートします（たとえば、**hardware access-list tcam region openflow 512 double-wide**）。OpenFlow TCAM リージョンが非倍幅として設定されている場合、イーサ タイプの一致のみが一致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。 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

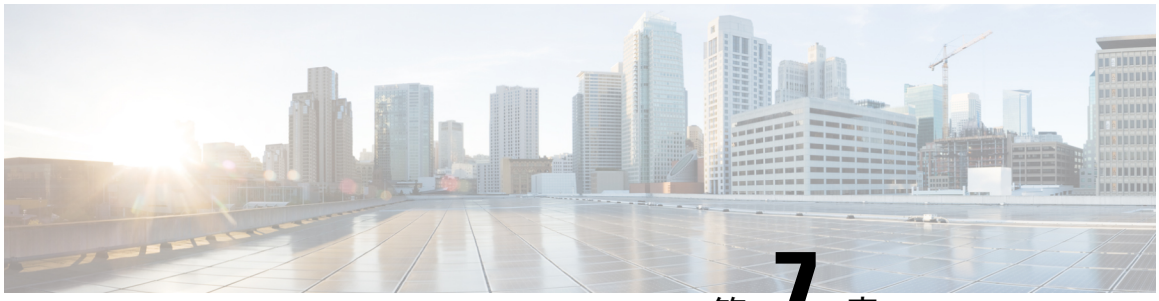
スイッチ間ポートおよびポート チャネルでスイッチ ポート モードを有効にするには、次の手順を実行します。

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構成します。
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 7 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 以降、Cisco Nexus Data Broker (NDB) は Cisco Nexus Dashboard Data Broker に名前が変更されました。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。

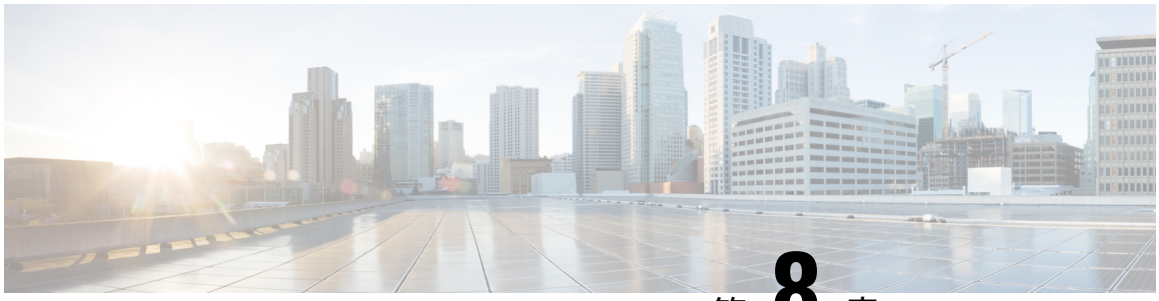
ダッシュボード

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
  - 接続（Connections）
- **Data Handled / Received since** *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。
- **クラスタ ランタイム** — 現在のクラスタのランタイム。

- **最後に再起動したクラスタ（Cluster Last Restart）** — クラスタが最後に再起動された日時。
- **パケット数別の上位接続（Top Connections by Packet Count）**（色分けされたバーで表示）- パケット数（接続のフローによって処理された合計パケット数）に基づく接続と、パケット数に基づく接続のおおよその帯域幅。リストは降順です。パケット数が最も多い接続が上部に表示されます。
- **受信パケット数別上位入力ポート（Top Input Ports by Received Packet Count）**（色分けされたバーで表示）ーポートで受信したパケット数に基づく入力ポート。リストは降順です。受信パケット数が最も多い送信元ポートが上部に表示されます。
- **送信パケット数別の上位モニタリング ツール（Top Monitoring Tools by Transmitted Packet Count）**（色分けされたバーで表示）ー 送信パケット数に基づくモニタリング ツール。リストは降順です。送信パケット数が最も多いモニタリング ツールが上部に表示されます。
- **フィルタリングされたパケット数による上位のフィルタ**（Top Filters by Filtered Packet Count）（色分けされたバーで表示）ー ACL でフィルタリングされたパケット数に基づいてフィルタリングします。リストは降順です。パケット数が最も多いフィルタが上部に表示されます。
- **TCAM リソース使用率別の上位デバイス（Top Device by TCAM Resource Utilization）**（色分けされたバーで表示）：TCAM リソース使用率に基づくデバイス。リストは降順です。使用率が最も高いデバイスが上部に表示されます。



第 8 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 以降、Cisco Nexus Data Broker (NDB) は Cisco Nexus Dashboard Data Broker に名前が変更されました。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] 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。

トポロジ図には、ネットワークの要素が表示されます。要素にカーソルを合わせると、その詳細が表示されます。要素をクリックすると、その要素の詳細が表示されます。

表示されるネットワーク要素は次のとおりです。

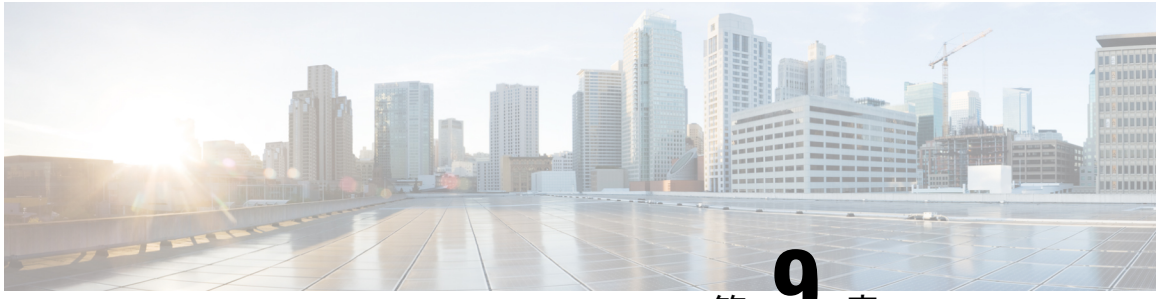
- 接続された NDB デバイス
- 入力ポート
- モニタリング ツール
- NX-OS デバイス
- ACI デバイス

（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。

[トポロジ] タブから、次のアクションを実行できます。

- **NDB デバイスの追加** — 詳細については、「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** — 詳細については、スパン デバイスの追加 （98 ページ） を参照してください。
- **モニタリング ツールの追加** — 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。



第 9 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 以降、Cisco Nexus Data Broker (NDB) は Cisco Nexus Dashboard Data Broker に名前が変更されました。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] タブには、次のサブタブがあります。

- **NDB デバイス** — 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** — NDB に接続されたスイッチ（Nexus/Catalyst）およびコントローラ（APIC/DNAC）。詳細については、「デバイスのスパン （96 ページ）」を参照してください。
- **タップ デバイス** — NDB コントローラに接続されているデバイスをタップします。詳細については、「タップ デバイス」を参照してください。
- **バイス グループ** — 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（Device Groups）」を参照してください。

NDB デバイス

[NDB デバイス] タブには、NDB コントローラー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 *8 : NDB* デバイス

列名	説明
ステータス（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。 • 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。 • 赤色 - 失敗を示し、デバイスが NDB コントローラに接続されていません。 • 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。リフレッシュして確認。 • 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。 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して、デバイスの詳細を表示します。 **[IP アドレス]** 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。 • デバイスの編集 • デバイスをオフラインにする • デバイスのグローバル構成の編集 （注） *[デバイスをオフラインにする]* アクションは通常灰色で表示されており、メンテナンスモードのデバイスでのみ使用できます。 対応するタブをクリックして、デバイスの**ポート**、**ポート チャネル**、および**ポート グループ**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 チャネルとポート グループ」を参照してください。 **詳細**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。 • [全般（General）] • ポート • ポート チャネル • Port Groups • グローバル設定 • [セッションの監視] • フロー統計 • ポート統計情報 • TCAM リソース使用率 **[詳細]** タブから実行できる追加のアクション： • グローバル ACL のトリガー — 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

列名	説明
	識別し、こ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。デバイスのすべてのインターフェイスにグローバル ACL を構成する必要があります。 • ポート チャネルの追加
デバイス名（Device Name）	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 ステータスが緑色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。
Platform	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。 • NDB モード — 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。 • ハイブリッド — デバイスの一部のインターフェイスのみが NDB コントローラによって管理されることを示します。 （注） 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る場合、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。 • 接続成功 — 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。 • 接続失敗 ー 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。 • 接続の準備ができていません ー 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 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**— 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**：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]** > **[デバイスの再検出]** 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。デバイスを再検出すると、グローバル ACL が再接続されます。

（注） デバイスを再検出すると、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** — 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]** > **[デバイスの再接続]** をクリックします。ポップアップが表示されます。**[再接続]** 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 コントローラ間の失敗した接続を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** — 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、「デバイス 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 —** 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** — 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。
  - **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 ソース、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。

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] 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、『*Cisco Nexus Data Broker* リリース ノート リリース *3.10*』を確認してください。

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 **[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]** ダイアログ ボックスで、次の詳細を入力します。

表 *9:* デバイスの追加

フィールド	説明
全般	
IP アドレス/ホスト名	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。
ユーザー名/ プロファイル	**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。 **[ユーザー名]** をクリックすると、次のフィールドが表示されます。 • **ユーザー名**：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。 • **パスワード**：パスワードを入力します。 **[プロファイル]** をクリックすると、次のフィールドが表示されます。 • **[プロファイル]** : **[プロファイルの選択]** ドロップダウン リストから、プロファイルを選択します。 （注） 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。プロファイル構成は、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）]	デバイス通信ポートを入力します。NX-API over HTTP にはポート 80 を、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。 • **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は自動的にデフォルトのインターフェイス コマンドのセットを実行します。 • **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。 • **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]** または **[スケール]** を選択します。1024 または 2048 のメモリがそれぞれ割り当てられます。 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 （94 ページ） を参照してください。
ハイブリッド モード	ハイブリッドモードを有効にするには、バーを右にスライドします。ハイブリッドモードでは、デバイスの一部のインターフェイスのみがNDBによって管理されます。 このオプションを表示するには、**nx.hybrid.support=true** を使用して **config.ini** ファイルを有効にする必要があります。NDB に接続されているすべてのデバイスでこの機能を使用するには、NDB を再起動します。

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

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。configure.global.acls パラメータを *false* に設定し、デバイスを再起動して、デバイスのグローバル ACL を無効にします。

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。

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。

新しいペインは右側に表示されます。

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

ステップ 4 **[デバイスの編集]** 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 *10* : デバイスの編集

フィールド	説明
全般	
IP アドレス/ホスト名	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。
ユーザー名/ プロファイル	**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。 **[ユーザー名]** をクリックすると、次のフィールドが表示されます。 • **[ユーザー名]** — 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。 • **[パスワード]** - 入力したユーザー名のパスワードを入力します。 **[プロファイル]** をクリックすると、次のフィールドが表示されます。 • **[プロファイル]—[プロファイルの選択]** ドロップダウン リストから、プロファイルを選択します。 （注） 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。プロファイル構成は、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。 • **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は自動的にデフォルトのインターフェイス コマンドのセットを実行します。 • **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。 • **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]** または **[スケール]** を選択します。1024 または 2048 のメモリがそれぞれ割り当てられます。 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 （94 ページ） を参照してください。

ステップ 5 **[デバイスの編集（Edit Device）]** をクリックします。

デバイス プロファイルの更新

この手順を使用して、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。

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 **[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]** ダイアログ ボックスで、次の詳細を入力します。

表 *11* : プロファイルの割り当て/更新

フィールド	説明
全般	
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。

フィールド	説明
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]** 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 チャネルとポート グループ」を参照してください。

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 **IP アドレス**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 *12 :* ポートチャネルの追加

フィールド	説明
全般	
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	**[ポートの選択]** 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]** 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設定をプッシュします。前提条件の設定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 （89 ページ） および/または デバイスの編集 （91 ページ） を参照してください。

次の設定は、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 の前提条件に従わずに 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
- LLDP 機能が有効になっています（Nexus Dashboard Data Broker の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 構成のため、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

デバイスのポート（またはさまざまなデバイス）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 バランシングを設定し、Cisco Nexus 3000 シリーズおよび 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、対称型および非対称型のロード 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
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 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

デバイスのスパン

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、パケットを監視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* で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 switch 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 switch は、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 の統一 （102 ページ）を参照してください。

[スパン 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]** または **[実稼働スイッチ]** を選択します。

- **コントローラ**：APIC または 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**：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 *13*：コントローラ

列	説明
Active IP	コントローラの Active IP アドレス。IP アドレスをクリックすると、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。 • スパン デバイスの編集 （100 ページ） Nexus Dashboard Data Broker コントローラと通信する APIC/DNAC コントローラの現在の 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、詳細が表示されます。 DNAC コントローラの場合、Nexus Dashboard Data Broker が 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。 • NDB モニタリング セッションの削除 • NDB モニタリング セッションの作成
ユーザー名	コントローラに現在ログインしているユーザー名。
名前	コントローラの名前。
プライマリ IP アドレス	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。

列	説明
ターシャリ IP アドレス	（APIC のみ）コントローラの第 3 の IP アドレス。

表 *14* : 実稼働スイッチ

列	説明
Active IP	デバイスのアクティブな IP アドレス。 IP アドレスをクリックすると、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。 • スパン デバイスの編集 （100 ページ）
ユーザー名	デバイスに現在ログインしているユーザー名。
Platform	デバイスのプラットフォーム。

[スパン デバイス] タブから、次のアクションを実行できます。

- **スパン デバイスの追加**：これを使用して、新しいスパン 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 （98 ページ）を参照してください。
- **スパン デバイスの再検出**：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]** > **[スパン デバイスの再検出]** 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、選択されたデバイスを再検出します。

  [スパン 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 コントローラとスパン デバイス間の接続を再確立します。

  チェックボックスをオンにせずに、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、指示メッセージが表示されます。
- **スパン デバイスの削除**：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）]** > **[スパン 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、指示メッセージが表示されます。

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。

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 **[アクション]** ドロップダウン リストから、**[スパン デバイスの追加]** を選択します。

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

表 *15 :* スパン デバイスの追加

フィールド	説明
全般	**コントローラ**または**実稼働スイッチ**を選択します。コントローラは、APIC または DNAC にすることができます。プロダクション スイッチ（PS）は、Nexus または Catalyst スイッチです。 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 に対して表示されるフィールド：	
コントローラ タイプ	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。 • APIC • DNAC
IP アドレス/ホスト名	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）	（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）	（オプション。APIC の場合のみ）コントローラのターシャリ IP アドレスを入力します。
ユーザ名（Username）	ユーザー名を入力します。
パスワード	認証のための必要なパスワードを入力します。
DNAC名	（DNAC のみ）DNAC の名前を入力します。この名前は、Nexus Dashboard Data Broker コントローラによる識別のために使用されます。
実稼働スイッチ のために表示されるフィールド：	
アドレス	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。 • Nexus • Catalyst

フィールド	説明
ポート	デバイス通信ポート。 Nexus スイッチのポート番号を入力します。 **プラットフォーム タイプ**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 switch への通信は SSH 経由です。
ユーザー名	デバイスのユーザー名を入力します。
パスワード	ユーザー名の認証のための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 に対してのみ）必要なパスワードを入力します。 （注） 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]** をクリックします。

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 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、DNAC の *Template Editor* で確認できます。

スパン デバイスの編集

この手順を使用して、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。

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。

新しいペインは右側に表示されます。

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

ステップ 4 **[スパン デバイスの編集]** 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 *16* : スパン デバイスの編集

フィールド	説明
全般	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、こ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。
コントローラに表示されるフィールド：	
コントローラ タイプ	以前に選択されたコントローラ 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	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）	（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）	（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。
ユーザ名（**Username**）	コントローラのユーザー名。
パスワード	認証のための必要なパスワードを入力します。
DNAC名	（DNAC のみ）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。
実稼働スイッチに表示されるフィールド：	
アドレス	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	以前に選択され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	デバイス通信ポート。 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	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 **[スパン デバイスの編集（Edit Span Device）]** をクリックします。

Cisco Nexus Dashboard Data Broker と Cisco DNA Center の統一

Cisco Digital Network Architecture Center（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。

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 から管理されます。Nexus Dashboard Data Broker は、オンボーディング中に DNAC 上に別の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 DNAC に共有します。テンプレートに基づいて、DNAC は Catalyst スイッチで SPAN セッションを作成します。

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
```

REST API は、Nexus Dashboard Data Broker コントローラと DNAC 間の通信に使用されます。

タップ デバイス

Cisco Nexus Dashboard Data Broker リリース 3.10.1 は、タップ デバイスとして Cisco Nexus 3550-F L1 シリーズ スイッチをサポートします。タップ デバイスは、ネットワーク データのコピーを作成しますが、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、さらに処理するために Cisco Nexus Dashboard Data Broker に到達します。Cisco Nexus 3550-F L1 が Cisco Nexus Dashboard Data Broker を使用してタップ デバイスとして実装される方法の詳細については、タップ構成について （185 ページ） を参照してください。

表 *17:* タップ デバイス

列	説明
IP アドレス	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	タップ デバイスのプラットフォーム。
ノード 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。

列	説明
プロファイル名	関連付けられたプロファイル名。 タップ デバイスの作成時に **[プロファイル]** 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	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。 • 接続成功（Successfully connected） - 接続成功 • 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 • 接続タイムアウト（Connection timed-out）：一定時間内にデバイスをタップできませんでした。 • ホストへのルートがありません（No route to host）：タップ デバイスの間違った IP アドレス • 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] 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 （104 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]**>**[デバイスを再接続]** をクリックします。ポップアップが表示されます。**[再接続]** 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 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 ダッシュボード データ ブローカ コントローラから切断します。
  - **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、関連付けられた設定を 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。

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]** ドロップダウン リストから、**[タップ デバイスの追加]** を選択します。

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

表 *18* : タップ デバイスを追加

フィールド	説明
IP アドレス/ホスト名	デバイスの IP アドレスを入力します。
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]** または **[プロファイル]** を選択し、関連するフィールドに入力します。	
ユーザ名（Username）	
ユーザ名（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	
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。

フィールド	説明
接続タイプ	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（Device Groups）

[デバイス グループ] 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 *19* : 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。 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。 • 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]** 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** ー 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。

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 *20* : デバイスグループの追加

フィールド	説明
全般	
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。 **[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。 （注） すでにデバイスが別のグループの一部であるかどうかを確認します。一部である場合、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

この手順を使用して、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。

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 **デバイス グループ**名をクリックします。

新しいペインは右側に表示されます。

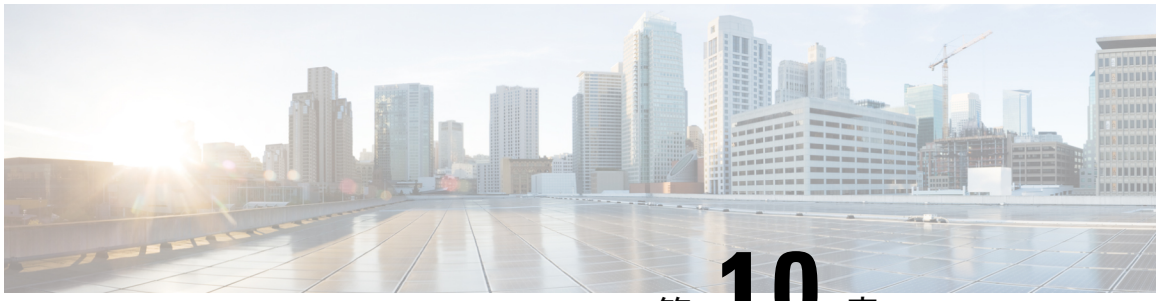
ステップ 3 **[アクション]** > **[デバイス グループの編集]** をクリックします。

表示されたウィンドウに、以下の詳細を入力します。

表 *21* : デバイスグループを編集

フィールド	説明
全般	
Device Group Name	デバイス グループ名。 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。グループからのデバイスを削除できます。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。 **[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。 （注） すでにデバイスが別のグループの一部であるかどうかを確認します。一部である場合、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 グループの編集]** をクリックします。



第 10 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 以降、Cisco Nexus Data Broker (NDB) は Cisco Nexus Dashboard Data Broker に名前が変更されました。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。

- **[ユーザー接続]** — 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ー定義の接続。詳細については、「ユーザー接続」を参照してください。
- **[デフォルト接続]**—デフォルトでは、ユーザー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、「デフォルトの接続」を参照してください。

ユーザー接続

[ユーザー接続] タブには、入力ポート (フィルター付きまたはフィルターなし) と監視ツール 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。

次の詳細の表が表示されます。

表 *22 :* ユーザー接続

列名	説明
接続名	接続の名前。 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。新しいペインは右側に表示され、接続の詳細な情報が示されます。接続のトポロジは、**展開ビュー**または**ネットワーク ビュー**で表示できます。 ここで実行できる追加のアクション: • **接続の編集** — 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、「接続の編集またはクローン処理」を参照してください。 • **接続のクローン処理**—接続のクローン処理をするには、このアクションを選択してください。詳細については、「接続の編集またはクローン処理」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。 **詳細**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。 • 全般 • 展開ビュー • ネットワーク ビュー • フロー統計 • 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。 • 通常—ここでは、接続は入力ポートにフィルターを適用し、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。 • 自動優先度—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 （119 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**フィルターと**ドロップ**フィルタの数。選択に基づいて、一致するトラフィックがドロップまたは許可されます。 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	接続の入力ポートおよび/または入力ポート グループの数。 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。ソース（トラフィックが Nexus Dashboard Data Broker コントローラに到達する本番デバイス）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	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。 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	接続を作成したユーザー。
[最終更新者（Last Modified By）]	接続を最後に更新したユーザー。

各行の先頭には、色分けされた円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は、送信元ポートの運用状態と管理状態、監視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です。

- 緑色の丸は、最後の接続が成功したことを示します。
- 赤い丸は、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ます。

ロック記号は、接続がロックされており、接続パラメータの不正な変更が許可されていないことを示します。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。接続の追加中に接続をロックできます。

[ユーザー接続] タブから、次のアクションを実行できます。

- **接続の追加** — 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**—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]** ボタンをクリックし、**[接続の削除]** 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]** ボタンをクリックし、**[インストールの切り替え]** を選択して接続をインストールします。 Toggle Install は NDB デバイスの接続をインストール/アンインストールしますが、接続設定は Nexus Dashboard Data Broker コントローラーから削除されません。

  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 upgrade 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設定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（フィルター付き）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）
- リハーサルを使用する（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。

ステップ 1 **[接続]** > **[ユーザー接続]** 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 *23 :* 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。数値が高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示します。 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。 （注） 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	接続をロックするためには、灰色のボタンをクリックします。灰色のボタンは青に変わり、右側に移動して、ロックが有効になっていることを示します。 接続をロックすると、接続への未承認の変更を防止します。
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、AutoPriority が有効になったことを示します。 **AutoPriority** が有効な場合、**Priority** 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。 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 （119 ページ）を参照してください。
接続トポロジ	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。 **[入力ポート/グループの選択]**をクリックします。**入力ポート**または**入力ポート グループ**を選択します。 **入力ポート**を選択する場合、デバイスのリストが表示されます。 **1.** デバイスを選択するためには、対応するチェックボックスをオンにします。選択されたデバイスに基づいて、デバイスの使用可能なポートが表示されます。 **2.** ポートを選択するためには、対応するチェックボックスをオンにします。選択されたポート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が色付きの丸で示されます。 （注） **[入力ポートの追加]**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、「入力ポートの追加」を参照してください。 **3.** **[選択]** 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。 **[入力ポート グループ]** を選択すると、ポート グループの一覧が表示されます。 **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。選択されたポート 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。 （注） **[入力ポート グループの追加]** 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、「入力ポート グループの追加」を参照してください。 **2.** **[選択]**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。 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。フィルタに**許可**または**拒否**の動作を使用することを選択できます。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。 （注） **[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。 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。 （注） **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	AutoPriority 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。 **[モニタリング ツール/グループの選択]** をクリックします。**[モニタリング ツール]** または **[ツール グループ]** のいずれかを選択します。 **モニタリング ツール**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。 **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、色分けされた丸で示されます。 （注） **[モニタリング ツールの追加]** 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。 **2.** **[選択]** 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。 **ツール グループ**を選択すると、モニタリング ツールグループの一覧が表示されます。 **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、色分けされた丸で示されます。 （注） **[モニタリング ツール グループの追加]** 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。 **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。 AutoPriority 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。 **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。 **2.** [選択（Select）] をクリックします。

ステップ 4 **[接続の追加]** をクリックして接続を追加するか、**[接続のインストール]** 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。

接続の編集またはクローン処理

この手順を使用して、接続を編集または複製します。

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。

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**」を選択します。

ステップ 4 **[接続の編集]** または **[接続のクローン処理]** 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 *24 :* 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。
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	接続をロックするためには、灰色のボタンをクリックします。灰色のボタンは青に変わり、右側に移動して、ロックが有効になっていることを示します。 接続をロックすると、接続への未承認の変更を防止します。
自動優先	接続の追加時に**自動優先**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	ここでは、接続に対して**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**または**入力ポート グループ**のいずれかを選択します。 **入力ポート**を選択する場合、デバイスのリストが表示されます。 **1.** デバイスを選択するためには、対応するチェックボックスをオンにします。選択されたデバイスに基づいて、デバイスの使用可能なポートが表示されます。 **2.** ポートを選択するためには、対応するチェックボックスをオンにします。選択されたポートの詳細が右側に表示されます。 **3.** **[選択]** をクリックして、接続の一部として選択した送信元ポートを含めます。 **入力ポート グループ**を選択する場合、ポート グループのリストが表示されます。 **1.** ポート グループを選択するためには、対応するチェックボックスをオンにします。選択されたポート グループの詳細が右側に表示されます。 **2.** **[選択]** をクリックして、接続の一部として選択した送信元ポート グループを含めます。
[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]** をクリックします。 **1.** フィルタを選択するためには、対応するチェックボックスをオンにします。選択され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。 **2.** **[選択]** 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。

フィールド	説明
モニタリング ツール	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]**をクリックします。**モニタリング ツール**または**ツール グループ**のいずれかを選択します。 **モニタリング ツール**を選択する場合、モニタリング ツールのリストが表示されます。 1. モニタリング ツールを選択するためには、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も表示されます。ステータスは、色付きの丸で示されます。 2. **[選択]**をクリックして、接続の一部としてモニタリング ツールを含めます。 **ツール グループ** を選択する場合、モニタリング ツール グループのリストが表示されます。 1. ツール グループを選択するためには、対応するチェックボックスをオンにします。選択されたツール 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が色付きの丸で示されます。 2. **[選択]** 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 **[接続の編集]** または **[接続のクローン処理]** をクリックします。

自動優先

自動優先度は、接続内の複数の宛先デバイスにフィルタをマッピングする柔軟性を提供します。自動優先度を使用した接続の優先度は、`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。

リハーサル

リハーサル機能を使用して、新しい接続に対して生成されるトラフィックの量を見積もることができます。この機能は、新しい接続のトラフィックを 30 秒間サンプリングし、その接続で

生成されるおおよそのトラフィックを推定します。新しい接続を追加する前に、リハーサル機能を使用できます。config.ini ファイルの mm.dryrun.timer パラメータを使用して、リハーサル機能を管理できます。リハーサル機能を有効にするには、mm.dryrun.timerパラメータをゼロより大きい値に設定します。mm.dryrun.timerパラメータがゼロに設定されている場合、リハーサル機能は無効になります。

リハーサル機能は、新しい接続のトポロジを推定トラフィックに関する情報とともに表示します。この機能は、新しい接続の数秒（config.ini ファイルの mm.dryrun.timer 値）のトラフィックをサンプリングし、その接続で生成されるおおよそのトラフィックを推定します。新しい接続を追加する前に、リハーサル機能を使用します。

デフォルトの接続

[デフォルトの接続] 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、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システムによって構成されます。つまり、デフォルトでは、ユーザー定義の接続が構成されるまで、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いるため、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 *25* : デフォルトの接続

列名	説明
接続名	デフォルトの接続名。 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。 ここでは、次のアクションを実行できます。 • **接続のクローン処理** — 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、「接続の編集またはクローン処理」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。 （注） デフォルトの接続は編集できません。
フィルタのドロップ	接続のドロップしたフィルタの数。 NDB のドロップ フィルタは、一致する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	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 11 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 以降、Cisco Nexus Data Broker (NDB) は Cisco Nexus Dashboard Data Broker に名前が変更されました。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] 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 *26 :* 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。 **[フィルタ]** 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。 • フィルタの編集またはクローン処理 （注） 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、**Yes** が表示されます。それ以外の場合は **No** が表示されます。 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	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	フィルタを最後に変更したユーザー。

[フィルタ] 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** — 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、「フィルタの追加」を参照してください。
- **フィルタの削除** — 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]** > **[フィルタの削除]** 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

この手順を使用して、フィルタを追加します。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。

ステップ 1 **[コンポーネント]** > **[フィルタ]** 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 *27 :* フィルタの追加

フィールド	説明
フィルタ名	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、すなわち、送信元 IP、送信元ポートまたは送信元MACアドレスから宛先IP、宛先ポート、または宛先MACアドレス、および宛先IP、宛先ポート、または宛先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ためにフィルタ処理する場合は、このボックスをオンにします。

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。 • イーサネット タイプ — 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。 • IPv4 • IPv6 • LLDP • MPLS • ARP • すべてのイーサネット タイプ • 事前定義されたイーサネット タイプ — 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イーサネット タイプは、このルールに関連付けられており、ほかのパラメータを構成してはなりません。 • イーサネット タイプの入力 — このオプションを選択する場合、16進形式でいーアsネットタイプを入力します。 • VLAN 識別番号 — 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。 最大値は 4095 です。 • VLAN 優先順位 — トラフィックの VLAN 優先順位を入力します。VLAN優先順位は、レイヤ2トラフィックのみに対して一致します。 • 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 トラフィックのみに対して一致します。 • 宛先 MAC アドレス — 宛先デバイスの MAC アドレスを入力します。MACアドレスは、レイヤ2トラフィックのみに対して一致します。 • MPLS ラベル値 — 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。

フィールド	説明
	[MPLS 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 に設定される場合のみ表示されます。MPLS ラベル値が一致します。

フィールド	説明
レイヤ 3 レイヤ 3 のオプションを有効にするには、**IPv4** または **IPv6** を **Ethertype** として [レイヤ 2] タブの下で選択します。	

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。 • 送信元 IP アドレス — 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。 • 標準的な IPv4 または IPv6 形式のホスト IP アドレス • IPv4 または IPv6 アドレス範囲 • 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 • コンマ区切りの不連続 IP アドレス。例：10.1.1.1, 10.1.1.2, 10.1.1.5 （注） 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 4 送信元または送信先ポートの範囲を構成することはできません。 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 2 VLAN 識別子の範囲は設定できません。 • 宛先 IP アドレス — レイヤ 3 トラフィックの宛先 IP アドレスを入力します。次のいずれかになります。 • 標準的な IPv4 または IPv6 形式のホスト IP アドレス • IPv4 または IPv6 アドレス範囲 • 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 • コンマ区切りの不連続 IP アドレス。例：10.1.1.1, 10.1.1.2, 10.1.1.5 （注） 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 4 送信元または送信先ポートの範囲を構成することはできません。 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 2 VLAN 識別子の範囲は設定できません。 • 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**を入力しま

フィールド	説明
	す。 • 高度なフィルタ — このボタンをクリックして、高度なフィルタ処理を有効にして、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。高度なフィルタに関連するオプションの詳細については、「詳細フィルタ」を参照してください。 • カスタム フィルタ — このボタンをクリックして、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を有効にします。**[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。ユーザー定義フィールドの追加 を使用して作成された UDF がここに表示されます。 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。 • 値 - 10 進表記（0 ～ 65535）で一致する値です。たとえば、0x0806 に一致させたい場合は、10 進表記で 0x0806 である 2054 を入力します。 • マスク - マッチングのために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。 （注） 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 UDF を追加]** チェックボックスをオンに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） レイヤ 4 のオプションを有効にするには、[レイヤ 2] タブで **[Ethertype]** として **[IPv4]** または **[IPv6]** を選択し、[レイヤ 3] タブで **[L4 プロトコル]** として **[TCP]** または **[UDP]** を選択します。	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。 • 送信元ポート — 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。 • FTP（データ） • FTP（コントロール） • SSH • Telnet • HTTP • HTTPS • 送信元ポートを入力 — 送信元ポートを入力します。カンマ区切りの単一のポート番号または送信元ポート番号の範囲を入力できます。 （注） 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。 • Destination Port — ドロップダウン リストで、宛先ポートを選択します。次のオプションがあります。 • FTP（データ） • FTP（コントロール） • SSH • Telnet • HTTP • HTTPS • 宛て先ポートの入力 — 宛て先ポートを入力します。カンマ区切りの単一のポート番号または送信元ポート番号の範囲を入力できます。 （注） レイヤ 4 宛先ポートの範囲を入力すると、レイヤ 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。

フィールド	説明
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処理

この手順を使用して、フィルタを編集またはクローン処理をします。

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行うことを意味します。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。

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、**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]** をクリックし、**[フィルタのクローン]** を選択します。

ステップ 4 **[フィルタのクローン]** または **[フィルタの編集]** 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 *28 :* 編集/フィルタのクローン

フィールド	説明
フィルタ名	フィルタの名前。

フィールド	説明
双方向	双方向トラフィック情報、すなわち、送信元 IP、送信元ポートまたは送信元 MAC アドレスから宛先 IP、宛先ポート、または宛先 MAC アドレス、および宛先 IP、宛先ポート、または宛先 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ためにフィルタ処理する場合は、このボックスをオンにします。

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。 • イーサネット タイプ — 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。 • IPv4 • IPv6 • LLDP • MPLS • ARP • すべてのイーサネット タイプ • 事前定義されたイーサネット タイプ — 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イーサネット タイプは、このルールに関連付けられており、ほかのパラメータを構成してはなりません。 • イーサネット タイプの入力 — このオプションを選択する場合、16進形式でいーアsネットタイプを入力します。 • VLAN 識別番号 — 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。 最大値は 4095 です。 • VLAN 優先順位 — トラフィックの VLAN 優先順位を入力します。 VLAN優先順位は、レイヤ2トラフィックのみに対して一致します。 • 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 トラフィックのみに対して一致します。 • 宛先 MAC アドレス — 宛先デバイスの MAC アドレスを入力します。 MAC アドレスは、レイヤ 2 トラフィックのみに対し

フィールド	説明
	て一致します。 • MPLS ラベル値 — 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。 **[MPLS 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 に設定される場合のみ表示されます。MPLS ラベル値が一致します。

フィールド	説明
レイヤ 3 レイヤ3のオプションを有効にするには、**IPv4** または **IPv6** を **Ethertype** として [レイヤ 2] タブの下で選択します。	

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。 • 送信元 IP アドレス — 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。 • ホスト IP アドレスは、標準的な IPv4 または IPv6 形式です • IPv4 または IPv6 アドレス範囲 • アドレスの範囲と標準的な IP アドレスの組み合わせ。例：10.1.1.1, 10.1.1.2-10.1.1.5 • コンマ区切りの不連続 IP アドレス。例：10.1.1.1, 10.1.1.2, 10.1.1.5 （注） 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 4 送信元または宛先ポートの範囲を構成することはできません。 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 2 VLAN 識別子の範囲は設定できません。 • 宛先 IP アドレス — レイヤ 3 トラフィックの宛先 IP アドレスを入力します。次のいずれかになります。 • ホスト IP アドレスは、標準的な IPv4 または IPv6 形式です • IPv4 または IPv6 アドレス範囲 • アドレスの範囲と標準的な IP アドレスの組み合わせ。例：10.1.1.1, 10.1.1.2-10.1.1.5 • コンマ区切りの不連続 IP アドレス。例：10.1.1.1, 10.1.1.2, 10.1.1.5 （注） 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 4 送信元または送信先ポートの範囲を構成することはできません。 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 2 VLAN 識別子の範囲は設定できません。 • L4 プロトコル — ドロップダウン リストからレイヤ 4 プロトコルを選択します。

フィールド	説明
	• 高度なフィルタ — このボタンをクリックして、高度なフィルタ処理を有効にして、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、「詳細フィルタ」を参照してください。 • カスタム フィルタ — このボタンをクリックして、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を有効にします。**[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） レイヤ 4 のオプションを有効にするには、[レイヤ 2] タブで **[Ethertype]** として **[IPv4]** または **[IPv6]** を選択し、[レイヤ 3] タブで **[L4 プロトコル]** として **[TCP]** または **[UDP]** を選択します。	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。 • 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。 • FTP（データ） • FTP（コントロール） • SSH • Telnet • HTTP • HTTPS • Enter Source Port — 送信元ポートを入力します。カンマ区切りの単一のポート番号または送信元ポート番号の範囲を入力できます。 （注） 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。 • Destination Port — ドロップダウン リストで、宛先ポートを選択します。次のオプションがあります。 • FTP (データ) • FTP（コントロール） • SSH • Telnet • HTTP • HTTPS • Enter Destination Port — 送信先ポートを入力します。カンマ区切りの単一のポート番号または送信元ポート番号の範囲を入力できます。 （注） レイヤ 4 宛先ポートの範囲を入力すると、レイヤ 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。

フィールド	説明
レイヤ 7	未サポート

ステップ 5 **[フィルタの編集（Edit Filter）]** または **[フィルタのクローン（Clone Filter）]** 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 *29* : 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
UDP を使用した IPv4	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
UDP を使用した IPv6	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 デバイスでは、NX-OS バージョン 7.0(3)I6(1) 以降の最大 TTL 値を 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す。

高度なフィルタリングの使用に関する制限

高度なフィルターの構成中、次のことはできません。

- DSCP と優先順位を一緒に構成します。

- フラグメントと ACK または SYN または FIN または PSH または RST を一緒に構成します。
- 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します。
- IPv4 と TCP の組み合わせで優先順位と HTTP メソッドを構成します。

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 *30*：グローバル設定

列名	説明
Device	デバイス名 これはハイパーリンクです。**デバイス**名をクリックして、デバイスのグローバル構成の詳細を取得します。
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。 • Symmetric • 非対称
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。 • 有効 • 無効

列名	説明
Jumbo MTU	デバイスのジャンボ MTU サイズ。 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。 • 有効 • 無効
MPLS フィルタ	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。 • 有効 • 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。 • 有効 • 無効

次のアクションは、**[グローバル構成]** タブから実行できます。

- **グローバル構成の編集**：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 （144 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

この手順を使用して、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を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。

デバイスが作成されると、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。

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

ステップ 2 業の先頭の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 *31* : グローバル構成の編集

フィールド	説明
全般	
デバイス	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	ドロップダウン リストから **[対称]** または **[非対称]** を選択します。 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 （96 ページ） を参照してください。
ハッシュ構成	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	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 ストリップ タイプの構成	グレーのボタンをクリックして、MPLS ストリップ タイプの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。 入力ポートからのすべての MPLS パケットは、MPLS ヘッダーが取り除かれます。 （注） 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。
ラベルのエージング	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。 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 スイッチです - 93128TX、3172、3164、3232、3132C-Z。

フィールド	説明
MPLS フィルタ構成を有効にする	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。 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 構成	
sFlow の有効化	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。 sFlowの詳細については、サンプリングされたフロー （153 ページ） を参照してください。 次の詳細を入力します。 • **エージェントの IP アドレス** — エージェントの IP アドレスを入力します。 • **VRF の選択** — ドロップダウンリストから [VRF] を選択します。 • **コレクタ IP アドレス** — コレクタ ポートの IP アドレスを入力します。 • **コレクタ UDP ポート** — sFlow コレクターの UDP ポートを入力します。 • **カウンタ ポーリング間隔** — sFlow のポーリング間隔値を入力します。 • **最大データグラム サイズ** — 最大データグラム サイズを入力します。 • **最大サンプル サイズ** — 最大サンプル サイズを入力します。 • **サンプリング レート** — データ サンプリング レートを入力します。 • **データ ソース** — **[ポートの選択]** 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]** をクリックします。 （注） 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 設定	

フィールド	説明
PTP の有効化	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。 ここで有効になっている PTP は、入力ポートとモニタリング ツールのタイムスタンプに使用されます。 PTPの詳細については、高精度時間プロトコル（152ページ） を参照してください。 次のフィールドが表示されます。 • **送信元 IP アドレス** — PTP アップデートを受信するためのソース IP アドレスを入力します。 • **ポート** ：**[ポートの選択]** をクリックし、チェックボックスをオンにして、PTP ソース IP が接続されている必要なポートを選択します。 （注） 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	
MTU 値	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MTU値を設定します。 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。 **[デフォルトにリセット]** をクリックして、MTU 値をデフォルト値の 1500 に設定します。 （注） 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	

フィールド	説明
Netflow の有効化	灰色のボタンをクリックして、ネットフローを有効にします。ボタンが青色に変わり、右に移動します。 Netflow の詳細については、NetFlow （153 ページ） を参照してください。 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）完了します。 • NetFlow のレコードの追加 （148 ページ） • NetFlow のエクスポータの追加 （150 ページ） • NetFlow のモニターの追加 （151 ページ） NetFlow設定を完了するには、NetFlowモニタリングを入力ポートに関連付けます。入力ポートの追加 （156 ページ）を参照してください。

ステップ 5 **[グローバル構成の編集]** 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。

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

ステップ 2 業の先頭の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、**ネットフローを有効にします**。

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

表 *32 :* レコードを追加

フィールド	説明
名前（Name）	レコードの名前。

フィールド	説明
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。 check box 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。 • Counter Bytes • Counter Packets • IP バージョン • Transport TCP Flags • システム稼動開始時間 • 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。 使用可能なオプションは、**レイヤ 2** および**レイヤ 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、後続の行で説明します。
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。 • 送信元 MAC アドレス • 宛先 MAC アドレス • イーサタイプ • 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 および/またはレイヤ 4 パラメータを有効にします。 • IPプロトコル • IP TOS • Transport Source Port • Transport Destination Port • IPv4 送信元アドレス • IPv4 宛先アドレス • 送信元 IPv6 アドレス • 宛先 IPv6 アドレス • IPv6 フロー ラベル • 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

この手順を使用して、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。

ステップ 1 **[コンポーネント]** > **[グローバル構成]** 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]** ドロップダウン メニューから、**[グローバル構成の編集]** を選択します。
ステップ 4 **[グローバル構成の編集]** 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**にします。
ステップ 5 **[エクスポータを追加]** をクリックし、次の詳細を入力します。

表 *33 :* 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。

フィールド	説明
説明	エクスポータの説明。
宛先（Destination）	エクスポート宛先 IP アドレス。 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。 フローキャッシュが宛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。値の範囲は 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 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。 （注） 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	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]** をクリックします。

NetFlow のモニターの追加

この手順を使用して、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
- エクスポーターの追加

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

ステップ 2 業の先頭の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、**ネットフローを有効にします**。

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

表 *34 :* 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]** をクリックします。**[レコードの選択]** 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	**[エクスポータを選択]** をクリックします。**[エクスポータの選択]** 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ーを選択します。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。 （注） 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（2Precision Time Protocol）デバイスには、オーディナリ 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。

PTPは、次のプラットフォームでのみサポートされています。

- Cisco Nexus 9200 スイッチ
- Cisco Nexus 9300 スイッチ — 9300-FX、FX2、EX
- Cisco Nexus 9500 スイッチ — 9500-FX、EX
- Cisco Nexus 3548 スイッチ

（注） PTPを構成すると、デフォルトのPTP構成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 （144 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 （144 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（144ページ）を参照してください。

入力ポート

[入力ポート] 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** コマンドを設定してください。

次の詳細の表が表示されます。

表 *35 :* 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。 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（83ページ）の章を参照してください。
ポート	入力ポートとして構成されているデバイスのポート。 このフィールドはハイパーリンクです。**ポート**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アクションは次のとおりです。 • 入力ポートの編集 • 構成の削除 — ポートはデバイスの入力ポートとして削除されます。
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。

列名	説明
設定	入力ポートの構成情報（入力ポートの追加（156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。 • エッジ ポート-SPAN • エッジポート-TAP • リモート ソース Edge-SPAN • パケットの切り捨て
スパン宛先/タップ名	入力ポートに接続されているスパン宛先の詳細。 • ポートが実稼働スイッチに接続されている場合は、*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。 • ポートが APIC/ACI コントローラまたは DNAC コントローラに接続されている場合、APIC の場合、DN 値がポッドとパスの詳細とともに表示されます。DNAC の場合、「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。 • 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] 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** — 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 （156 ページ） を参照してください。
- **入力ポートの削除** — 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、指示メッセージが表示されます。

入力ポートの追加

この手順を使用して、入力ポートを作成します。

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]** 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（以下にリスト）を定義するには、「デバイスのグローバル構成の編集」を参照してください。

- PTP
- NetFlow
- MPLS フィルタ処理
- Jumbo MTU

ステップ 1 **[コンポーネント]** > **[入力ポート構成]** 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]** ダイアログ ボックスで、次の詳細を入力します。

表 *36* : 入力ポートの追加

フィールド	説明
全般	
デバイス（Device）	入力ポートが構成されているデバイスを選択するには。 **[デバイスの選択（Select Device）]** をクリックします。**[デバイスの選択]** 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	入力ポートとして構成するポートを選択します。 **[ポートの選択]** をクリックします。**[ポートの選択]** 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。

フィールド	説明
ポート タイプ	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。 • **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。 • **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。 • **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。
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。 （注） 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。
ブロック送信	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。 （注） 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。 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、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。この機能は、現在 NX-OS バージョン I5 以降の NX-API ベースのスイッチに使用できます。

フィールド	説明
タイムスタンプ タギング	チェックボックスをオンにして、タイムスタンプ タギング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。 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 タグ付け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グ付けされません。 （注） 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	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。 （注） 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	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。 （注） 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	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。 （注） 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**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、入力ポートのソース（スパン宛先）です。 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。 • コントローラ • 生産スイッチ 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]** をクリックします。**ACI** または **DNAC** を選択します。
宛先デバイス タイプのフィールド：**コントローラ > ACI** （注） 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	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	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。
宛先デバイス タイプのフィールド: **コントローラ > DNAC**	
スパン先名	スパン先の名前を入力します。
SPAN 先ポート	**[SPAN 先ポート]** をクリックし、Catalyst スイッチとポートを選択します。
宛先デバイス タイプのフィールド: 生産スイッチ （注） スパン先を構成する前に、Nexus または Catalyst デバイスを追加する必要があります。	
スパン先デバイス	**[デバイスの選択]** をクリックし、デバイスを選択します。
スパン先ポート	**[ポートの選択]** をクリックして、ポートを選択します。

b) （**ポート タイプ** — 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	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	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。 表示されるオプションは、選択した**タップ構成名**の詳細に基づいています。タップ構成の追加 （182ページ）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** — リモート ソース Edge-SPAN の場合のみ）次の詳細を入力します。

（注） リモート ソース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 ソース Edge-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	
ERSPAN ID	ERSPAN ID を入力します。指定できる範囲は 1 ～ 1023 です。 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 インターフェイスの使用	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。
ループバック（**Loopback**）	**[ループバックの選択]** 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]** 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。 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宛先ポートに到達します。最初のリモート ソース エッジ スパン入力ポートがループバックで作成された場合、次のリモート ソース 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設定する必要があります。最初のリモート ソース エッジ スパン入力ポートがループバックなしで作成された場合、次のリモート ソース 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設定する必要があります。

フィールド	説明
セッション宛先	**[宛先ポートの選択]** をクリックして、宛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	
[リモート入力ポート（Remote Input Port）]	**[リモート入力ポート]** 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。 （注） リモート ソース Edge-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設定している場合、リモート入力ポートは、リモート ソース 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。 この値を入力する必要があるのは、最初のリモート ソース Edge-SPAN ポートを構成する場合だけです。構成する次の 3 つのポートでは、同じ IP アドレスがリモート ソース 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。
宛先デバイスのタイプ	ドロップダウン リストから [デバイス タイプ] を選択します リモート ソース Edge-SPAN ポートの場合、サポートされる宛先タイプは ACI です。
スパン先 ACI ファブリック	**[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	**[アプリケーション プロファイルの選択]** 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、ソース パケットの IP サブネットのベース IP アドレスです。

フィールド	説明
宛先 IP アドレス	このフィールドには自動的に値が入力されます。 ここで入力される IP アドレスは、**リモート入力ポート**の IP アドレスとして入力したものと同じアドレスです。 （注） APIC/ACI デバイスの場合、これは宛先ポート（リモート入力ポート）であるため、宛先 IP と呼ばれます。
フロー ID	このフィールドには自動的に値が入力されます。 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 ポートに以前に指定された 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]	スパン宛先ポートの 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]** をクリックします。

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。

ステップ 1 **[入力ポート]** > **[アクション]** > **[入力ポートの追加]** 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。

フィールド	説明
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。

次の詳細の表が表示されます。

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。 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。 • 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。 • 黄色 - 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。 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。 • 緑色：リンクが起動して動作していることを示します。 • 赤色：リンクがダウンしていることを示します。 • 黄色 - リンクが管理上ダウンしていることを示します。

列名	説明
モニタリング ツール	モニタリング ツール名。 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**名をクリックします。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。 • モニタリング ツールの編集 （169ページ）
ポート	モニタリング ツール ポート（デバイス付き）。 ポートの詳細を表示するには、**ポート**名をクリックします。次の追加アクションがここで実行できます。 • モニタリング ツールの編集 （169ページ）
[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。 • 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。
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	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]** が表示されます。
作成者	モニタリング ツールを作成したユーザー。

列名	説明
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。

[モニタリング ツール] 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** — これを使用して、新しいモニタリング 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」の追加を参照してください。
- **モニタリング ツールの削除** — 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、指示メッセージが表示されます。

（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の切り捨てポート（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。
- 監視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(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 Up 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。

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	
モニタリング ツール名	モニタリング ツール名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。 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。 **[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]** 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。 [選択（Select）] をクリックします。 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	ポートの説明を入力します。

フィールド	説明
ローカル モニタリング ツール	ラジオ ボタンでローカル モニタリング ツールを選択します。このオプションを選択することで、モニタリングデバイスがローカル ネットワークから指定されます。 次のオプションは、ローカルモニタリングデバイスに対して表示されます（以下の行で詳細が説明されます）。 • Block Rx • ICMPv6 ネイバー勧誘をブロック • タイムスタンプ タギングの有効化 • パケットの切り捨て • タイムスタンプ ストリップの有効化 • ジャンボ MTU の適用
Rx のブロック	モニタリング ツールからのトラフィックをブロックします（NDB デバイスのモニタリング ツール ポートに指定）。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ことで、このオプションをオフにすることができます。 （注） 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	モニタリング ツールからの ICMP トラフィックをブロックします（NDB デバイスのモニタリング ツール ポートに指定）。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ことで、このオプションをオフにすることができます。 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。

フィールド	説明
タイムスタンプ タギングの有効化	チェックボックスをオンにして、タイムスタンプ タギングを有効にします。タイムスタンプ タグは、モニタリング ツール ポートのすべての送信パケットに追加されます。 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。 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のいずれかの側で構成されていない場合、Edge-SPAN/Edge-TAP とモニタリング ツール、次にパケットがタイムスタンプにタグ付けされていません。
パケットの切り捨て	Check the check box to enable packet truncation and enter the MTU siz 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の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、監視ツールに到達します。 パケットの切り捨てポートを設定するには、**[パケットの切り捨てポートの選択（Select Packet Truncation Port）]** をクリックします。詳細な手順については、パケット切り捨てポートの追加 （172 ページ） 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	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。これは送信元パケットからタイムスタンプ タグを削除します。
ジャンボ MTU を適用	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。 ジャンボ MTU にデバイスのより大きなパケット サイズを設定します。**ジャンボ MTU** を **グローバル構成**で有効にして、デバイスのポートにジャンボ MTU 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	ラジオ ボタンでリモート モニタリング ツールを選択します。このオプションを選択することで、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。 次のオプションは、リモートモニタリングデバイスに対して表示されます（以下の行で詳細が説明されます）。 • Block Rx • インターフェイスIP • 宛先 IP • 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。
宛先 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。 Cisco Nexus 9300 FX および EX シリーズ スイッチの Encapsulated Remote Switch Port Analyzer（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]** 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。

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、監視ツール名をクリックします。

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]** 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	
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	ポートの説明を入力します。
ローカル モニタリング ツール	ラジオ ボタンを選択して、ローカル モニタリング 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。 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)。 • Block Rx • ICMPv6 ネイバー勧誘をブロック • タイムスタンプ タギングの有効化 • パケットの切り捨て • タイムスタンプ ストリップの有効化 • ジャンボ MTU を適用
Rx のブロック	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ことで、このオプションをオフにすることができます。 （注） 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	モニタリング ツールから（NDB デバイスの監視ツール 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ことで、このオプションをオフにすることができます。 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	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。タイムスタンプ タグは、モニタリング ツール ポートのすべての送信パケットに追加されます。 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。 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のいずれかの側で構成されていない場合、Edge-SPAN/Edge-TAP とモニタリング ツール、次にパケットがタイムスタンプにタグ付けされていません。
パケットの切り捨て	Check the check box to enable packet truncation and enter the MTU siz 監視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]** は無効になります。
タイムスタンプ ストリップの有効化	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。これは送信元パケットからタイムスタンプ タグを削除します。
ジャンボ MTU の適用	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。 ジャンボ MTU にデバイスのより大きなパケット サイズを設定します。**ジャンボ MTU** を **グローバル構成**で有効にして、デバイスのポートにジャンボ MTU 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	ラジオ ボタンでリモート モニタリング ツールを選択します。このオプションを選択することで、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。 次のオプションは、リモートモニタリングデバイスに対して表示されます（以下の行で詳細が説明されます）。 • Block Rx • インターフェイスIP • 宛先 IP • 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。
宛先 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。 Cisco Nexus 9300 FX および EX シリーズ スイッチの Encapsulated Remote Switch Port Analyzer（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。

パケット切り捨てポートの追加

この手順を使用して、パケット切り捨てポートを作成します。パケット切り捨てポートは、モニタリング ツール ポートの入力ポートとして機能します。したがって、作成されたパケットモニタリングツールポートは入力ポートとしてリストされ、未使用のパケット切り捨てポートは 入力ポート （154 ページ） タブから削除できます。

始める前に

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。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、パケットの切り捨てが必要です。

表 *41 :* 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

ステップ 1 **[コンポーネント]** > **[モニタリング ツール]** 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 デバイスとポートを選択し、**[パケット切り捨て]** チェックボックスをオンにして、パケット切り捨てを有効にします。

ステップ 4 **[パケット切り捨てポートの選択]** をクリックします。

ステップ 5 表示される **[パケット切り捨てポートの選択]** ウィンドウで、**[パケット切り捨てポートの追加]** をクリックします。

ステップ 6 **[パケット切り捨ての追加（Add Packet Truncation）]** ダイアログ ボックスで、次の詳細を入力します。

表 *42 :* パケット切り捨ての追加

フィールド	説明
全般	
Device	デバイス名が下に表示されます。
ポート	**[ポートの選択]** をクリックします。**[ポートの選択]** ウィンドウで、ラジオボタンを選択してポートを選択します。 **[送信（Submit）]** をクリックします。
ポート タイプ	デフォルトでは、パケット切り捨てポートが選択されています。
ポートの説明	切り捨てポートのポートの説明。
ICMPv6 ネイバー請求をドロップ	パケット トランケーション ポートの入力 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。

ステップ 7 [追加（Add）] 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** — デバイスの（またはデバイス全体の）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** ：デバイスの（またはデバイス全体の）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、ツール グループのモニタリング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。接続を作成する間に、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グループ化して同時に選択することができます。

次の詳細の表が表示されます。

表 *43* : 入力ポート グループ

列名	説明
入力ポート グループ名	入力ポート グループ名。 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**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。 • 入力ポート グループの編集
説明	入力ポート グループの説明。
関連づけられた接続	グループに関連付けられた接続。
メンバー	グループのメンバー入力ポートの数。
作成者	グループを作成したユーザー。
最終修正者	グループを最後に修正したユーザー。

[入力ポート グループ] 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** — 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** — 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]** > **[入力ポート グループの削除]** 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。

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]** ダイアログ ボックスで、次の詳細を入力します。

表 *44* : 入力ポート グループの追加

フィールド	説明
全般	
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	*[*すべてのノード*]* 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	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]** 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	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]** 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

この手順を使用して、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。

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、**[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 *45 :* 入力ポート グループの編集

フィールド	説明
全般	
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*）*]* ボックスから、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	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]** 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	選択したポートがここに自動入力されます。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、ポートの隣のバツ印（x）をクリックします。**[すべてを削除（Remove All）]** をクリックして、すべての選択したポートを削除します。

ステップ 5 **[入力ポート グループの編集（Edit Input Port Grou）]** をクリックします。

ツール グループのモニタリング

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 *46 :* ツール グループのモニタリング

列名	説明
モニタリング ツール グループ名	モニタリング ツール グループ名 このフィールドはハイパーリンクです。**モニタリング ツールのグループ名**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。 • 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	モニタリング ツール グループを利用した接続。
メンバー	グループのメンバーモニタリングツールのポート数。
作成者	グループを作成したユーザー。
最終修正者	最後にグループを修正したユーザー。

[モニタリング ツール グループ] 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** — 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]** > **[モニタリング ツール グループの削除]** 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

この手順を使用して、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。

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 *47*: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	
グループ名	モニタリング ツール グループ名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	*[*すべてのノード*]* 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	モニタリング ツール ポートとして構成され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]** 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	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]** 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]** 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。

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**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]** をクリックし、**[モニタリング ツール グループの編集]** 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]** 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 *48* : モニタリング ツールグループの編集

フィールド	説明
全般	
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*）*]* ボックスから、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	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]** 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	選択したポートがここに自動入力されます。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、ポートの隣のバツ印（x）をクリックします。**[すべてを削除（Remove All）]** をクリックして、すべての選択したポートを削除します。

ステップ 5 **[モニタリング ツール グループの編集]** をクリックします。

スパン宛先

[スパン宛先（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。スパン宛先は、入力ポートのトラフィックの送信元（ACI または NX-OS デバイスから）です。L2 スパン宛先（ローカル）はエッジ スパン ポートに作成され、L3 スパン宛先 (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 *49 :* スパン宛先

列名	説明
名前	スパン宛先ポートの名前。
宛先（**Destinations**）	スパン宛先が ACI/APIC、DNAC、Nexus、またはCatalystデバイス上にあるかどうかを示します。
入力ポート	スパン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。 • エッジ スパン ポート • リモート ソース エッジ スパン ポート
スパン デバイス	スパンデバイス（トラフィック ソース）。次のオプションがあります。 • APIC/ACI または DNAC コントローラ • CatalystまたはNexusスイッチ（実稼働スイッチ）
作成者	スパン宛先を作成したユーザー。
最終更新者	スパン宛先を最後に更新したユーザー。

[スパン宛先] タブから、次のアクションを実行できます。

- **[スパン宛先の削除]**：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]** > **[スパン宛先の削除]** をクリックします。選択したスパン宛先が削除されます。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。スパン宛先を選択するよう求められます。

（注） スパン宛先の追加については、入力ポートの追加（156ページ） の手順を参照してください。スパン宛先（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ています。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 宛先を追加できます。

APIC SPAN 宛先の場合、入力ポートを Edge-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、ポートをスパン

宛先として構成できます。 NX-OS（実稼働スイッチ）の SPAN 宛先の場合、入力ポートを Edge-SPAN ポートとして設定し、ポートが NX-OS デバイスに接続されている場合、NX-OS デバイスのノードとポートを選択し、 SPAN 宛先としてのポート。

タップ構成

[タップ構成] タブには、Nexus Dashboard Data Broker コントローラーのタップ構成の詳細が表示されます。このタブには、タップ デバイスのネットワーク ポートとミラー ポート、およびタップ デバイスに接続されている NDB デバイス ポートのマッピングに関する情報が表示されます。

票には次の詳細が表示されます。

表 *50* : タップ構成

列名	説明
Tap Name	タップ構成名。 タッ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。次の追加手順を実行できます。 • タップ構成の編集 （184 ページ）
Device	タップ構成が作成されるタップ デバイス。
Port-1	実稼働ネットワークからトラフィックを受信するタップ デバイスのポート。
Port-2	本番ネットワークからトラフィックを受信するタップ デバイスのポート。
Port-1 Mirror	タップ デバイスの **Port-1** からミラーリングされたトラフィックを受信し、NDB Port-1 Edge Port-TAP に転送するタップ デバイスのポート。
Port-2 Mirror	タップ デバイスの **Port-2** からミラーリングされたトラフィックを受信し、NDB Port-2 Edge Port-TAP に転送するタップ デバイスのポート。
Port-1 Edge Port-TAP	タップ デバイスの **Port-1 Mirror** ポートからトラフィックを受信する NDB デバイスのポート。

列名	説明
Port-2 Edge Port-TAP	タップ デバイスの **Port-2 Mirror** ポートからトラフィックを受信する NDB デバイスのポート。
作成者	タップ構成を作成したユーザー。
変更者	タップ構成を変更したユーザー。

[タップ構成] タブから、次のアクションを実行できます。

- **[タップ構成の追加]**— これを使用して、タップ構成を追加します。詳細については、タップ構成の追加 （182 ページ）を参照してください。
- **[タップ構成の編集]** — これを使用して、既存のタップ構成を編集します。詳細については、タップ構成の編集 （184 ページ）を参照してください。
- **[タップ構成の削除]**—行の先頭にあるチェックボックスをオンにして、削除するタップ構成を選択し、**[アクション]** > **[タップ構成の削除]** をクリックします。
- **[タップ構成の同期（Sync Tap Configuration）]** — このオプションを使用して、タップ デバイスのタップ設定を Nexus Dashboard Data Broker コントローラのタップ設定と同期します。

タップ構成の追加

タップ構成を追加するために、この手順を使用します。

始める前に

1 つ以上のタップ デバイスを追加します。

ステップ 1 **[構成（Components）]** > **[タップ構成（Tap Configurations）]** 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、**[タップ構成の追加（Add Tap Configuration）]** を選択します。

ステップ 3 **[タップ構成の追加（Add Tap Configuration）]** ダイアログ ボックスで、次の詳細を入力します。

表 *51 :* タップ構成を追加

フィールド	説明
Tap Name	タップ構成の名前を入力します。

フィールド	説明
Tap Device	タップ構成が構成されているタップ デバイスを選択します。 **[デバイスの選択]** をクリックし、表示される **[タップ デバイスの選択]** ウィンドウからタップ デバイスを選択します。**[タップ デバイスの追加]** をクリックして、タップ デバイスの追加を選択することもできます。
タップ着信トラフィックのポート	次のオプションから選択してください。ポート-1、ポート-2、両方 いずれかのポートまたは両方のポートからタップ トラフィックを選択できます。
ネットワークポート	**[ポートの選択（Select Port）]** をクリックして、ポート-1 および ポート-2 を選択します。 これらは、実稼働ネットワークからトラフィックを受信するタップ デバイスのポートです。両方のネットワーク ポート間で双方向トラフィックが確立されます。
ミラー ポート	**[ポートの選択（Select Port）]** をクリックして、トラフィックをミラーするポートを選択します。ネットワーク ポート-1 からのトラフィックは、ミラー ポート-1 に送られ、ネットワーク ポート-2 からのトラフィックはミラー ポート-2 に送信されます。 ネットワーク ポートからのトラフィックは、ミラー ポートに送信（ミラーリング）され、次にNDBデバイスに送信されます （注） タップ受信トラフィックに **[両方（Both）]** としてオプションを選択した場合のみ、ポート-1 および ポート-2 の両方が使用可能になります。
NDB Edge ポート-TAP	**[ポートの選択（Select Port）]** をクリックして、NDB デバイスの Edge ポート-TAP ポートを選択します。ミラー ポートからのトラフィックをここで受信しました。 （注） ここで NDB Edgeポート-TAP ポートを選択しない場合は、入力ポートの追加 （156 ページ） の手順を使用してポートを関連付けることができます。

ステップ 4 **[タップ構成の追加（Add Tap Configuration）]** をクリックします。

タップ構成の編集

この手順を使用して、タップ構成のパラメータを編集します。

始める前に

1 つ以上のタップ構成を追加します。

ステップ 1 **[コンポーネント]** > **[タップ構成]** に移動します。

ステップ 2 表示された表で、**タップ名**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、**[タップ構成の編集（Edit Tap Configuration）]** を選択します。

ステップ 4 **[タップ構成の編集]** ダイアログボックスには、タップ構成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 *52 :* タップ構成の編集

フィールド	説明
タップ名	構成名をタップします。
タップ デバイス	タップ構成が作成されたタップ デバイス。
タップ受信トラフィックのためのポート	以前に選択したオプションが表示されます。変更したい場合： これらのオプション（ポート 1、ポート 2、両方）から選択します。 いずれかのポートまたは両方のポートからのトラフィックをタップするように選択できます。
ネットワークポート	以前に選択したオプションが表示されます。変更したい場合： **[ポートの選択]** をクリックして、Port-1 と Port-2 を選択します。

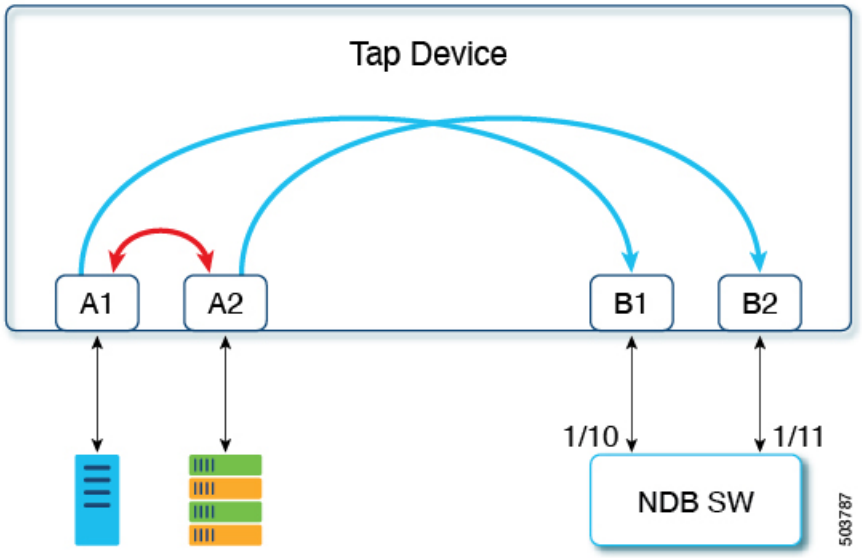
フィールド	説明
ポートのミラー（**Mirror Port(s)**）	以前に選択したオプションが表示されます。変更したい場合： **[ポートの選択]** をクリックして、トラフィックをミラーリングするポートを選択します。ネットワーク ポート 1 からのトラフィックはミラー ポート 1 に送信され、ネットワーク ポート 2 からのトラフィックはミラー ポート 2 に送信されます。 （注） ポート 1 とポート 2 の両方を使用できるのは、着信トラフィックをタップするためのオプションを**両方**として選択した場合のみです。
NDB エッジ ポート-タップ	以前に選択したオプションが表示されます。変更したい場合： **[ポートの選択]** をクリックして、NDB デバイスのエッジ ポート-TAP ポートを選択します。ミラー ポートからのトラフィックはここで受信されます。 （注） ここで NDB Edge Port-TAP ポートを選択しない場合は、入力ポートの追加 （156 ページ） の手順を使用してポートを関連付けることができます。

ステップ 5 **[タップ構成の編集（Edit Tap Configuration）]** をクリックします。

タップ構成について

タップ デバイスは、1 つ以上の本番スイッチ/ネットワークからのネットワーク トラフィックのコピー（ミラー）を作成します。Cisco Nexus 3550-F L1 シリーズ スイッチをタップ デバイスとして使用することをお勧めします。

以下のトポロジを参照すると、タップ デバイスのポート A1 および A2 は、実稼働スイッチ/ネットワークからトラフィックを受信します。これらはネットワーク ポートと呼ばれます。ネットワーク ポート間で双方向トラフィック フローが確立されます。ネットワーク ポート上のトラフィックは、ミラー ポートと呼ばれるポート B1 および B2 にミラーリングされます。ミラー ポートからのトラフィックは、NDB デバイスのエッジ ポート-TAP ポートに到達します。タップ デバイスのミラー ポートと NDB デバイスのエッジ ポート-TAP ポートは物理的に接続されています。



Cisco Nexus ダッシュボード データ ブローカーで Cisco Nexus 3550-F L1 スイッチをタップ デバイスとして使用する利点

- 使いやすさ。Cisco Nexus ダッシュボード データ ブローカー GUI を使用して、Cisco Nexus 3550-F L1 を設定および管理できます。
- コスト効率。Cisco Nexus 3550-F Fusion は、1 つの 1RU デバイスで 16 個のファイバタップ（48 ポート）を代替できます。

ユーザ定義フィールド

[ユーザー定義フィールド (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 バイト以内で一致できます。

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 *53 : UDF* サポート マトリックス

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

表 *54 : UDF* の対象地域

プラットフォーム	UDF 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

次の詳細の表が表示されます。

表 *55 :* ユーザ定義フィールド

列名	説明
UDF	UDF 名。 このフィールドはハイパーリンクです。UDF 名をクリックすると、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。 • ユーザー定義フィールドの編集またはクローン処理 。
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。
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。
Offset	設定されたオフセット値。
Length	一致したパケットの長さ
Devices	UDF が適用されているデバイスの数。
作成者	UDF を作成したユーザー。
最終修正者	UDF を最後に修正したユーザー。

[ユーザー定義フィールド] タブから、次のアクションを実行できます。

- **UDF の追加** — 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、「ユーザー定義フィールドの追加 」を参照してください。
- **UDF の削除** — 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、デバイスのリブートが必要です。

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 バイトに一致できます。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。

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 *56 : UDF* の追加

フィールド	説明
UDF 名	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。 • IPv4 • IPv6

フィールド	説明
キーワード	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。 • ヘッダー • Packet-Start **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。 • 内部 • 外部 このフィールドは、選択したキーワードが**ヘッダー**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。 • レイヤ 3 • レイヤ 4 このフィールドは、選択したキーワードが**ヘッダー**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	バイトの**オフセット**値を設定します。範囲は 0 ～ 127 です。 パケットのフィルタ処理は、UDF で設定されたオフセット値に基づいて行われ、パケットは設定されたオフセット値と等しくなります。

フィールド	説明
長さ	一致するパケットの長さ（バイト数）。範囲は 1 ～ 2 です。 オフセット値が 1 に設定されている場合、長さはオフセット値に依存します。その後、設定されたオフセット バイトで始まる 1 バイトが一致します。
デバイス	UDF が作成されているデバイス。 **[デバイスの選択（Select Devices）]** をクリックします。 **[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]** 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、作成直後は黄です。デバイスを再起動すると、UDF が正常にインストールされると、UDF アイコンの色が緑に変わり、そうでない場合は赤に変わります。

ユーザー定義フィールドの編集またはクローン処理

この手順を使用して、ユーザー定義フィールドを編集またはクローン処理します。

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ことは、既存の UDF と同じパラメーターを使用して新しい UDF が作成されることを意味します。必要に応じて、テストのデフォルト 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。

ステップ 1 **[コンポーネント]** > **[ユーザー定義フィールド]**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]** をクリックし、**[UDF のクローン処理]** または **[UDF の編集]** を選択します。

ステップ 4 **[UDF のクローン処理]** または **[UDF の編集]** 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 *57 : UDF*の編集

フィールド	説明
UDF 名	UDF の名前。 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。 このフィールドは変更できません。
キーワード	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。 • ヘッダー • パケット開始
ヘッダー	UDF の作成中に選択されたヘッダー。 このフィールドは変更できません。
レイヤー	UDF の作成中に選択されたレイヤ。 このフィールドは変更できません。
オフセット	バイト **オフセット**値を設定します。範囲は 0 ～ 127 です。 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実行され、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	一致するパケットの長さ (バイト数)。範囲は 1 ～ 2 です。 1 に設定されている場合、長さはオフセット値に依存します。次に、設定されたオフセットバイトで始まる 1 バイトが一致します。

フィールド	説明
デバイス	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 を削除するか、他のデバイスに UDF を適用できます。 **[デバイスの選択（Select Devices）]** をクリックします。 **[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。 （注） 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 **[UDF の編集]** または **[UDF のクローン処理]** をクリックします。

第 12 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 以降、Cisco Nexus Data Broker (NDB) は Cisco Nexus Dashboard Data Broker に名前が変更されました。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] タブには、Nexus Dashboard Data Broker コントローラーのスパン 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 デバイスのスパン宛先と 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、スパンの宛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 *58 :* 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、スパンの宛先、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。 使用可能なステータスは次のとおりです。 • 緑 - セッションは成功しています • 黄色 - セッションは部分的に成功しました • 赤 - セッションが失敗しました • 灰色 - 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	スパン セッション名 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**名をクリックすると、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。 • スパン セッションの編集またはクローン処理 （199 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 ソース	スパン セッションの送信元ポートの数。 （注） VLAN の場合、送信元ポートは ACI デバイスの EPG です。

列名	説明
スパン宛先	セッションのスパン宛先の数。 （注） 複数のスパン宛先を持つことができるのはACIデバイスだけで、複数のスパン宛先がある場合、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、送信元ポートの可用性に基づいて作成されます。 1 セッションにつき、1 つのスパン宛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ー。
最終更新者	スパンセッションを最後に変更したユーザー。

[スパン セッション] 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** — 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 （195 ページ） を参照してください。
- **スパン セッション/宛先の同期** — 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（APIC / 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/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宛先設定とスパン 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** — 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するか、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**：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]**>**[スパン セッションの削除]** 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

この手順を使用して、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。

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 **[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 *59* : 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	スパン セッションの名前を入力します。
スパン ソース	スパン ソースを選択します。 **実稼働スイッチ**または**コントローラ**を選択します。 これらのそれぞれには、後続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	
コントローラ	**[コントローラの選択]** をクリックし、**ACI** または **DNAC** のいずれかを選択します。 **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、ACI を選択します。catalyst switch のスパン ソースを作成するには、**DNAC** を選択します。
リーフ ポート	（ACI コントローラのみ） 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]** を選択します。 **[リーフ ポートの選択]** をクリックします。表示される **[リーフ ポートの選択]** 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） EPG/AAEP ソースを追加するには、**EPG/AAEP** を選択します。 **[EPG/ AAEP の選択]** をクリックします。表示される **[EPG/ AAEP の選択]** 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、ダイナミック、スタティック、AAEP です。ダイナミック、スタティックを選択すると、メンバーの詳細は右側に表示されます。EPG メンバーとして **AAEP** を選択するときに、**[AAEP の選択]** 列で AAEP を選択します。 （注） EPG インターフェイスは、すべてのポートが同じリーフ スイッチ内にあるときにのみ機能します。 EPG が複数のスイッチにわたる場合、すべてのリーフ スイッチで対応する SPAN 宛先を選択します。
インターフェイス	（DNAC に対してのみ） **[インターフェイスの選択]** をクリックし、Catalyst switch とインターフェイスを選択します。
VLAN	（DNAC に対してのみ） VLAN ID を入力します。
スパン ソース：実稼働スイッチ	
インターフェイス	**[インターフェイスの選択]** をクリックし、**[デバイス]** と **[ポート]** を選択します。 選択されたデバイスとポートは、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。 VLAN ID と一致するデバイスがセッションで使用されます。

フィールド	説明
方向（Direction）	デバイスのセッション ソース ポートのトラフィックを示します。 これらのオプションの 1 つを選択します。 • 着信 • 発信 • 両方
SPAN 宛先	**[スパン宛先の選択（Select SPAN Destination）]** をクリックして、スペイン宛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 ソース]** の選択に基づいています。 （注） スパン宛先ポートは、入力ポートの追加（156 ページ） の手順を使用して以前作成されました。 NDB デバイスに直接接続されている場合、ローカル スパン宛先を選択し、それ以外の場合はリモート スパンの宛先を選択します。リモート スパンの宛先は、Nexus スイッチにのみ適用できます。 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。 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ACI で作成された宛先をリストします。 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、Catalyst switch に対して作成されたスパン宛先をリストします。

フィールド	説明
接続を適用	セッションの接続を選択します。 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。 （注） セッションの一部であるすべてのスパン宛先もまた、モニタリング ツールへの直接トラフィックへの接続の一部となるセッションの一部でなければなりません。 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]** をクリックして、**[接続の選択]**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 の静的またはダイナミック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、スパン 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 宛先がリーフ 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） スパン宛先の場合：

スパン送信元の各リーフ スイッチに、対応するスパン宛先が少なくとも 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]** 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]** 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

この手順を使用して、スパン セッションを編集またはクローン処理をします。

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処理するということは、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 セッションを保存する前にその名前を変更してください。

始める前に

1 つ以上のスパン セッションを追加します。

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**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]** をクリックし、**[スパン セッションの編集]** または **[スパン セッションのクローン処理]** 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 *60* : スパン セッションの編集

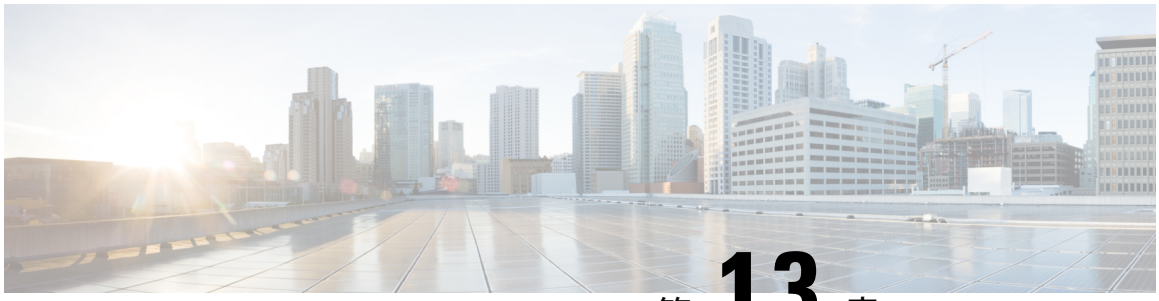
フィールド	説明
スパン セッション名	スパン セッション名が表示されます。 このフィールドは、編集できません。
スパン ソース	以前に選択したスパン ソースが表示されます。スパン ソースは変更できません。
スパン ソース：コントローラ	
コントローラ	**[コントローラの選択]** をクリックして、**ACI** または **DNAC** を選択します。 ACI ネットワークの一部である Nexus デバイスのスパン ソースの作成のために、 **ACI** を選択します。catalyst switch のスパン ソースの作成のために、**DNAC** を選択します。
リーフ ポート	（ACI コントローラに対してのみ） **[リーフ ポート]** を選択して、複数のリーフ ポートからトラフィックをキャプチャするために、リーフ ポートを追加します。 **[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]** ウィンドウで、**[ポッド（Pod）]** を選択します。選択されたポッド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 コントローラに対してのみ） **[EPG/ AAEP]** を選択して、EPG/ AAEP ソースを追加します。 **[EPG/ AAEP の選択]** をクリックします。表示される **[EPG/ AAEP の選択]** 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、ダイナミック、スタティック、AAEP です。ダイナミック、スタティックを選択すると、メンバーの詳細は右側に表示されます。EPG メンバーとして **AAEP** を選択するときに、**[AAEP の選択]** 列で AAEP を選択します。 （注） EPG インターフェイスは、すべてのポートが同じリーフ スイッチ内にあるときにのみ機能します。 EPG が複数のスイッチにわたる場合、すべてのリーフ スイッチで対応する SPAN 宛先を選択します。
インターフェイス	（DNAC に対してのみ） **[インターフェイスの選択]** をクリックし、Catalyst switch とインターフェイスを選択します。
VLAN	（DNAC に対してのみ） VLAN ID を入力します。
スパン ソース：実稼働スイッチ	
インターフェイス	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を追加または削除できます。 **[インターフェイスの選択]** をクリックし、**[デバイス]** と **[ポート]** を選択します。 選択されたデバイスとポートは、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。 VLAN ID と一致するデバイスがセッションで使用されます。

フィールド	説明
方向（Direction）	デバイスのセッション ソース ポートのトラフィックを示します。 これらのオプションの 1 つを選択します。 • 着信 • 発信 • 両方
SPAN 宛先	**[スパン宛先の選択（Select SPAN Destination）]** をクリックして、スペイン宛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 ソース]** の選択に基づいています。 （注） スパン宛先ポートは、入力ポートの追加（156 ページ） の手順を使用して以前作成されました。 NDB デバイスに直接接続されている場合、ローカル スパン宛先を選択し、それ以外の場合はリモート スパンの宛先を選択します。リモート スパンの宛先は、Nexus スイッチにのみ適用できます。 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。 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ACI で作成された宛先をリストします。 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、Catalyst switch に対して作成されたスパン宛先をリストします。

フィールド	説明
接続の適用	セッションの接続を選択します。 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。 （注） セッションの一部であるすべてのスパン宛先もまた、モニタリング ツールへの直接トラフィックへの接続の一部となるセッションの一部でなければなりません。 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]** をクリックして、**[接続の選択]**ウィンドウから接続を選択します。

ステップ **4** **[スパン セッションの編集]** または **[スパン セッションのクローン処理]** をクリックします。



第 13 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 以降、Cisco Nexus Data Broker (NDB) は Cisco Nexus Dashboard Data Broker に名前が変更されました。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] タブには、Nexus Dashboard Data Broker コントローラーで構成された接続のリストが表示されます。

次の詳細の表が表示されます。

列名	説明
接続（Connection）	接続名 このフィールドはハイパーリンクです。**接続**名をクリックして、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」セクションを参照してください。
パケット数（Packet Count）	接続のパケットに表示される集約トラフィックのボリューム。

フィルタ

[フィルタ] タブには、接続で使用されるフィルタが表示されます。

次の詳細の表が表示されます。

列名	説明
フィルタ	フィルタ名。 これはハイパーリンクです。フィルタの詳細については、**フィルタ**名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に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] 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] 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]** をクリックします。

次の詳細の表が表示されます。

列名	説明
ポートにおいて	トラフィックが一致する入力ポート。
DL 送信元	着信トラフィックと一致する送信元MACアドレス。
DL 送信先	着信トラフィックと一致する送信先MACアドレス。
DLタイプ	着信トラフィックに一致するイーサタイプ。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一致する VLAN ID。
VLAN PCP	着信トラフィックと一致するVLAN優先順位。
NW 送信元	着信トラフィックのIPv4またはIPv6送信元アドレス。

列名	説明
NW 送信先	着信トラフィックの IPv4 または IPv6 送信先アドレス。
NW プロトコル	着信トラフィックと一致するネットワーク 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	着信トラフィックと一致するネットワーク プロトコルに関連付けられた送信元ポート。
TP 送信先	着信トラフィックと一致するネットワーク プロトコルに関連付けられた送信先ポート。
パケット数	指定されたフロー接続と一致するパケットに表示される集約トラフィックのボリューム。

入力ポート

[入力ポート] 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。

次の詳細の表が表示されます。

列名	説明
Input Ports	デバイス名の入力ポート。 **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 （154 ページ）セクションを参照してください。
Packet Count	入力ポートのパケットに表示される集約トラフィック ボリューム。

TCAM リソース使用率

[TCAM リソース使用率] 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 *61 : TCAM* リソース使用率

列名	説明
Device	デバイス名 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**名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	色で示された使用率パターン。 • 緑：TCAM 使用率が最適であることを示します。 • オレンジ：TCAM 使用率が範囲内にあることを示します。 • 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] タブには、NDB コントローラー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。

次の詳細の表が表示されます。

列名	説明
モニタリング ツール	モニタリング ツール名。 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 ツール名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」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

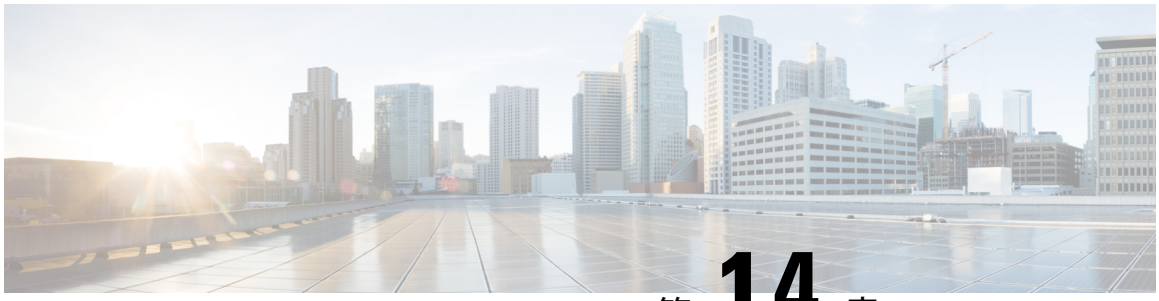
[ポート] タブには、NDB デバイスのポートの統計が表示されます。

[デバイスの選択]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]** をクリックして、別のデバイスを選択します。

次の詳細の表が表示されます。

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。 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	ポートで受信したパケットの数。
Tx パケット数	ポートで送信したパケットの数。
Rx バイト数	ポートで受信したバイトの数。
Tx バイト数	ポートで送信したバイトの数。
Rx レート（kbps）	パケットの受信速度。
Tx レート（kbps）	パケットの送信速度。
Rx ドロップ	ポート（Rx）でパケットがドロップされる速度。
Tx ドロップ	ポート(Tx)でパケットがドロップされる速度。
Rx エラー	パケット受信中のポートでのエラー。
送信エラー	パケット送信中のポートでのエラー。
Rx フレーム エラー	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	パケットの受信中にポートで発生したオーバーラン エラー。

[アクション] > **[ポートのクリア]** 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 14 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 以降、Cisco Nexus Data Broker (NDB) は Cisco Nexus Dashboard Data Broker に名前が変更されました。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] 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。

票には次の詳細が表示されます。

表 *62 :* 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。 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/イベントに関するスライス。 一部のアクションはスライスに関連せず、空白のままになっています。 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。 • 障害の説明 • 成功
Origin	アクションが実行された Nexus Dashboard Data Broker コントローラ。 （注） スタンドアロン Nexus Dashboard Data Broker コントローラの場合、127.0.0.1 が表示されます。
モード（**Mode**）	アクションが実行されたモード。 （注） 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] 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] > **[レコードの取得]** をクリックし、**[レコード数]** フィールドに値を入力します。**[取得]** 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] 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、デバギングに活用できます。

[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** — 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、不整合は自動的にトリガーされます。詳細については、整合性検査を参照してください。
- **接続フロー** — 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** ：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] 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 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 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 *63 :* 整合性検査

列名	説明
デバイス（Device）	デバイス名 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、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ー フロー	一貫性のないコントローラー フロー。 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。 • **Fix Flows**—必要なチェックボックスを選択し、**[Fix Flows]** をクリックします。選択したフロー (ACE) が固定され、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。 • **すべてをエクスポート**：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。
一貫性のないデバイス フロー	デバイスの一貫性のないフローまたは古いフロー。コントローラ フローと比較したときに、デバイスに欠落している ACL および ACE を示します。 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。 • **Fix Flows**—必要なチェックボックスを選択し、**[Fix Flows]** をクリックします。選択したフロー (ACE) が固定され、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。 • **すべてのエクスポート（Export All）**—このオプションを選択して、ACE と共に ACL としてリストされたフローのコピーを取得します。.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	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。 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。 • **Fix Flows**—必要なチェックボックスを選択し、**[Fix Flows]** をクリックします。選択したフロー (ACE) が固定され、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。 • **すべてのエクスポート（Export All）**—このオプションを選択して、ACE と共に ACL としてリストされたフローのコピーを取得します。`.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。非 NDB 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]** 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] 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 *64 :* 接続フロー

列名	説明
接続（**Connection**）	接続名です。 このフィールドはハイパーリンクです。**接続**名をクリックすると、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	接続のフロー (ACE) の数（デバイス間でも可能）。 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。 • **すべてのエクスポート**（**Export All**）—このオプションを選択して、ACE と共に ACL としてリストされたフローのコピーを取得します。`.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] 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** — 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**）—このオプションを選択して、ACE と共に ACL としてリストされたフローのコピーを取得します。`.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] 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。

次の詳細を含む表が表示されます。

表 *65*：デバイス フロー

列名	説明
Device	デバイス名 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、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）。 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。接続名が表示され、ACL とそれが含む ACE が続きます。ここで実行される可能性のあるアクションは、次のとおりです。 • **すべてのエクスポート（Export All）**—このオプションを選択して、ACE と共に ACL としてリストされたフローのコピーを取得します。.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]** 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。新しいペインが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。ここで実行される可能性のあるアクションは、次のとおりです。
  - **すべてのエクスポート（Export All）**—このオプションを選択して、ACE と共に ACL としてリストされたフローのコピーを取得します。.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] 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]** タブには次のサブタブが含まれます。

- **[エクスポート]** — 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]** — 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] 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 *66 :* 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	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。 • NX：NX-API デバイスに接続された NDB デバイス。 • PS：実稼働スイッチ（NX-OS）に接続された NDB デバイス。 • AC：ACI デバイスに接続された NDB デバイス。
ステータス	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]** > **[エクスポート]** タブから実行できます。

- **構成のエクスポート** — **[アクション]** > **[構成のエクスポート]** 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]** チェックボックスを選択します。**[エクスポート]** をクリックします。

インポート

[インポート] 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 *67*：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	構成のエクスポート元のデバイスの名前。
IP アドレス	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。 • NX—NX-API デバイスに接続された NDB デバイス。 • PS—実稼働スイッチ（NX-OS）に接続された NDB デバイス。 • AC—ACI デバイスに接続された NDB デバイス。
ステータス	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]** > **[インポート]** タブから実行できます。

- **構成のインポート** — **[アクション]** > **[構成のインポート]** 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]**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** — **[アクション]** > **[構成の適用]** をクリックします。**[デバイスの編集（Edit Fabric）]** 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** 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** テーブルに示されます。
- **インポートの削除** — **[アクション]** > **[インポートの削除]** 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。デバイスを削除すると、Nexus Dashboard Data Broker コントローラからのみ削除されますが、デバイス設定は保持されますが、デバイスを削除すると、デバイスが削除され、Nexus Dashboard Data Broker コントローラからもデバイス設定が削除されます。

票には次の詳細が表示されます。

表 *68 :* デバイスのページ

列名	説明
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	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]** をクリックします。

  これは、古いデバイス構成をデータベースから削除するのに役立ちます。

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 *69 : RMA*

列名	説明
既存のノード ID	（削除された）NDB デバイスのノード ID。
ノード名	デバイス名
シリアル番号	デバイスのシリアル番号

列名	説明
IP アドレス	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 を置き換える** — 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]**>**[ノード ID の置換]** 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**を入力し、**[置換]**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 Serial-Num 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）。

テクニカル サポート

[テクニカル サポート] タブには、Nexus ダッシュボード データ ブローカー 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 （223 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 *70* : テクニカル サポート

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。 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。 **[ダウンロードして削除]** 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。

列名	説明
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。 • 基本 • 拡張
Status	テクニカル サポート ジョブのステータス。 使用可能なステータスは次のとおりです。 • 成功 — ジョブは正常に完了しました。 • 一部 — 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。 • 失敗 — ジョブは成功しませんでした。 • 進行中： ジョブが現在、進行中です。 • 作成済み - ジョブは実行の準備ができていますが、キューに入っています。 • 停止 - ジョブは作成されましたが、完了できませんでした。

次のアクションは、**[テクニカル サポート]** タブから実行できます。

- **ジョブのトリガー**：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（223 ページ）」を参照してください。
- **ジョブの再トリガー**：次のチェックボックスを選択し、**[アクション]** > **[ジョブの再トリガー]** をクリックしてジョブを再トリガーします。進行中および作成済み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** ： チェックボックスを選択し、**[アクション]** > **[ジョブの停止]** 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、進行中および作成済みのジョブのみです。
- **ジョブの削除** — チェックボックスを選択し、**[アクション]** > **[ジョブの削除]** をクリックしてジョブを削除します。進行中のジョブは削除できません。

（注） 複数の適格なジョブを一度に削除/停止/再トリガーできます。

テクニカル サポートのトリガー

この手順を使用して、テクニカル サポート ジョブをトリガーします。

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。それ以外の場合、操作は失敗し、*No Enough Space* エラーが表示されます。

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

ステップ 2 **[アクション]** > **[ジョブのトリガー]** 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 *71* : 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	
デバイス（Device）	データを収集する必要があるデバイス。 **[デバイスの選択]** をクリックし、デバイスを選択します。
操作タイプ	**[基本]** または **[高度]** を選択します。 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]** 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。

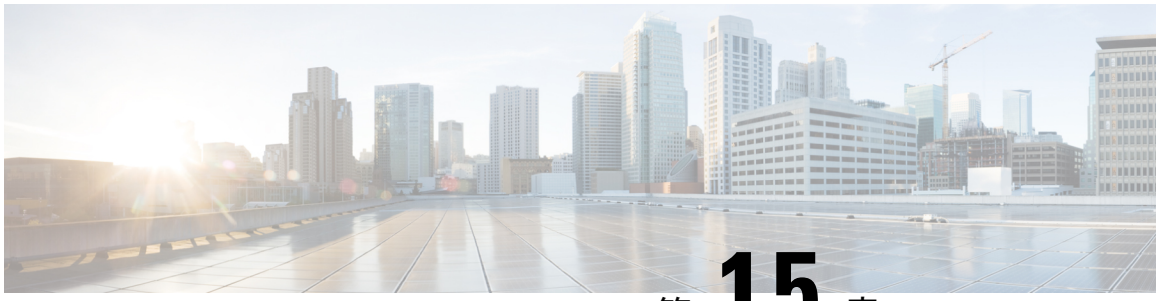
テクニカル サポートの概要

NX-API デバイス機能のテクニカル サポートにより、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、これはデバッグ中に役立ちます。

スイッチからのテクニカル サポート データの収集は、次の 2 つのモードで実行できます。

- 基本モード - 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 - より幅広い一連の show コマンドが含まれています。



第 15 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 以降、Cisco Nexus Data Broker (NDB) は Cisco Nexus Dashboard Data Broker に名前が変更されました。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 （228 ページ） を参照してください。

次の詳細の表が表示されます。

列名	説明
Server Address	AAA サーバの IP アドレス。
プロトコル	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。 • TACACS • RADIUS+ • 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 サーバを追加します。詳細な手順については、AAA サーバーの追加 （226 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

この手順を使用して、AAA サーバーを追加します。

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 *72 : AAA*サーバーの追加

フィールド	説明
全般	
プロトコル	AAA サーバーのプロトコルを選択します。 • RADIUS • LDAP • TACACS 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。
プロトコル：**Radius**	
サーバー アドレス	サーバーの IP アドレスとドメイン名
シークレット	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	サーバーの IP アドレスとドメイン名
ポート	AAA サーバーの通信ポート。

フィールド	説明
ユーザー 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。 LDAPサーバーで定義されたユーザー階層。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=local」。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」です。
ロール属性	ユーザーの LDAP 認証属性であるロール属性を入力します。 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。 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。 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	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**を有効にしている場合、既存のマップされた値は次のとおりになります。 • network-admin ー ネットワーク管理者 • network-operator — ネットワーク オペレータ • application-user—アプリケーションユーザー • slice-user — スライス ユーザー **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]**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]** 列に LDAP で定義された値を入力します。 **[行の追加]** をクリックして、ロール タイプ マッピングの行をさらに追加します。
タイムアウト	LDAP サーバーが応答するまでの待ち時間を入力します。
プロトコル：**TACACS+**	
サーバー アドレス	TACACS+ サーバーの IP アドレス。
シークレット	TACACS+ サーバーで構成されたシークレット。
ユーザー名	サーバーにログインするためのユーザー名。
パスワード	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	**[サーバーの確認]** 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。

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。

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] タブには 2 つのサブタブがあります。

- **スケジュールされたバックアップ** — Nexus Dashboard Data Broker コントローラでのバックアップのスケジュールの詳細については、バックアップのスケジュール （229 ページ）を参照してください。
- **バックアップ** — Nexus Dashboard Data Broker コントローラで完了したバックアップの詳細については、バックアップ （231 ページ）を参照してください。

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] 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。

次の詳細の表が表示されます。

表 *73*: 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。 • 毎日 • 毎週 • 毎月
発生回数（Occurences）	選択したパターンに基づく発生数。

[バックアップ] 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** — 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 （230 ページ） を参照してください。
- **ローカルにバックアップ** — 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** — 表示される **[ローカルに復元]** 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から、Nexus Dashboard Data Broker でデバイスの構成を再構成する場合は、**[復元]** 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
  - 接続（Connections）

  [復元] 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

この手順を使用して、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、常にバックアップを作成することをお勧めします。

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 74 : Schedule Backup

フィールド	説明
スケジュール	
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。 • **毎日** — バックアップ操作は毎日行われます。 • **毎週** — バックアップ操作は、毎週、選択した曜日に実行されます。 • **毎月** — 毎月、選択した日付にバックアップ操作が開始されます。 （注） 選択した月末まで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**）	次のいずれかのオプションを選択して、バックアップ プロセスを停止します。 • **終了日なし（No End Date）** — 引き続きバックアップを取得します。 • **終了日（End Date）** — 指定された終了日までバックアップを継続します。 • **発生（Occurences）** — **[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作成します。
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] タブに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、バックアップのスケジュール作成を使用して生成されたスケジュールに基づいています。次の詳細の表が表示されます。

列名	説明
品目	バックアップの時間。

列名	説明
クラスタのバックアップ ステータス	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。 • 成功 • 失敗
説明	バックアップの説明。
トリガーの復元	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] タブから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**—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]** タブに表示されます。
- **バックアップの復元** — 選択したバックアップは、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に基づいて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、Nexus Dashboard Data Broker コントローラを再起動します。

- **バックアップの削除** — 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]** > **[バックアップの削除]** をクリックします。

Cluster

[クラスタ] 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。

次の詳細の表が表示されます。

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**または**メンバー**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。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、クラスター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、クラスター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] 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。

次の詳細の表が表示されます。

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] 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** — 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** — 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]** 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

この手順を使用して、新しいプロファイルを追加します。

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てください。

表 *75 :* 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。
ユーザ名（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。
Password	ユーザー名に対してパスワードを入力します。 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、次の手順を使用します。

（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。

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、**プロファイル名**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、**[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]** 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 *76 :* 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、変更できません。
ユーザ名（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。
Password	ユーザー名に対してパスワードを入力します。 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 プロファイルを編集するには、**[プロファイルの編集]** をクリックします。

スライス

[スライス] 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 （238 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]** 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であり、**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
- ユーザーのプロファイルの変更
- ユーザーおよび関連するロールのパラメーターの変更
- 一貫性のないデバイスと接続フローの修正

次の詳細の表が表示されます。

列名	説明
スライス	スライスの名前。 このフィールドはハイパーリンクです。**スライス**名をクリックすると、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は次のとおりです。 • 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（または異なるデバイス）のポート。
利用可能なポート	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（または複数のデバイス）のポート。

[スライス] タブで次のアクションを実行できます。

- **スライスの追加** — 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** — 削除するスライスを選択し、**[アクション]** > **[スライスの削除]** 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

この手順を使用して、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。

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 *77 :* スライスの追加

フィールド	説明
全般	
スライス名	スライスの名前を入力します。
[ポート（Port）]	**[ポートの選択]** をクリックし、**[ポートの選択]** ウィンドウでデバイスと必要なポートを選択します。 （注） 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]** 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および/または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準備不可状態）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

この手順を使用して、スライスを編集します。

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。

ステップ 1 **[管理]** > **[スライス]** に移動します。

ステップ 2 **スライス**名をクリックします。新しいウィンドウが右側に開きます。

ステップ 3 **[アクション]** > **[スライスの編集]** 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 *78 :* スライスの編集

フィールド	説明
全般	

フィールド	説明
スライス名	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 **[スライスの編集]** 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。複数の切り離されたネットワークは、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] 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** — 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** — 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]** — 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」を参照してください。
- **[ロール]**—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（Roles）」を参照してください。
- **[グループ]**：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

[ユーザー] 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。

次の詳細の表が表示されます。

列名	説明
ユーザー	ユーザーのログイン名。 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。 • ユーザーのパスワードの変更 • ユーザーの役割の変更
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] 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** — 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** — 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]**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

この手順を使用して、新しいユーザーを追加します。

始める前に

新しいユーザーに割り当てることができるロールを作成します。

ステップ 1 **[管理]** > **[ユーザー管理]** > **[ユーザー]** 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 **[ユーザーの追加（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 *79 :* ユーザの追加

フィールド	説明
ユーザー名	ユーザ名を入力します。
Password	管理ユーザーのパスワードを入力します。 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。
パスワードの確認	パスワードを再入力して確認します。
ユーザー タイプの選択	次のいずれかのオプションを選択します。 • **通常ユーザー** — スライスなしで 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)。 • **スライス ユーザー** — 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 このフィールドは、ユーザータイプが**スライス ユーザー**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。作成されたユーザーは、選択したスライスにのみアクセスできます。

フィールド	説明
ロールの設定 このフィールドは、ユーザータイプが**通常ユーザー**の場合にのみ適用されます。	**[ロールの選択]** を選択します。表示される **[ロールの選択]** ダイアログ ボックスで、ユーザー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]**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。 使用可能なロール オプションは次のとおりです。 • 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。 • 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 **[ユーザーの追加]** をクリックして、新しいユーザーを追加します。

（注） ユーザーを作成した後で、パスワードは変更できますが、ユーザー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表示するためには、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。

ステップ 1 **[管理]** > **[ユーザー管理]** > **[ユーザー]** に移動します。

ステップ 2 **ユーザー**名をクリックします。新しいウィンドウが右側に開きます。

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 *80 :* パスワードの変更

フィールド	説明
全般	

フィールド	説明
ユーザー名	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	ユーザー名の現在のパスワードを入力します。 （注） このフィールドは、管理者ユーザーのみに表示されます。
パスワード	新しいパスワードを入力します。
パスワードの確認	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。

ステップ 1 **[管理]** > **[ユーザー管理]** > **[ユーザー]** に移動します。

ステップ 2 **ユーザー**名をクリックします。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 *81 :* 役割の変更

フィールド	説明
全般	
ユーザー名	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**または**スライス ユーザー**のいずれかを選択します。
スライスを選択	ドロップダウンリストからオプション選択します。 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]** の場合にのみ表示されます。

フィールド	説明
ロールの選択	**[ロールの選択]**をクリックすると、**[ロールの選択]** 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]** をクリックします。 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**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] 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。 表示名はハイパーリンクです。**ロール**名をクリックすると、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。 • ロールへのグループの割り当て

列名	説明
レベル	ロールに割り当てられるレベル。次のレベルが利用可能です。 • 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は、NXAPI または実稼働デバイスを Nexus Dashboard Data Broker に追加できません。管理者タブが App-Administrator ロール用の Nexus Dashboard Data Broker で使用できないためです。 • 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。App-Userは、Edge-SPAN、タップ、監視デバイス、および実稼働ポートのみを表示できます。 App-User は、Nexus Dashboard Data Broker 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 App-User によって作成された接続を構成することはできません。 • App-Operator - 読み取り専用操作にアクセスできます。
グループ	ロールに割り当てられるグループ。

[ロール] タブから、次のアクションを実行できます。

- **ロールの追加** — 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**—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]** メニューから **[ロールの削除]** 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

この手順を使用して、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。

ステップ 1 **[管理]** > **[ユーザー管理]** > **[ロール]** 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 *82 :* 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。

ステップ 1 **[管理]** > **[ユーザー管理]** > **[ロール]** に移動します。

ステップ 2 表示されたテーブルで**ロール**名をクリックします。

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]** > **[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 *83 :* 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。

フィールド	説明
[レベルの選択]	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]	**[グループの選択]** をクリックし、表示される **[グループの選択]** 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] 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。

次の詳細の表が表示されます。

列名	説明
グループ	グループの名前。 表示された名前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	グループに割り当てられたポートの数。

[グループ] 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**— 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** — 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]** メニューから **[グループの削除]** 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。グループは役割に割り当てられます。ユーザーは役割に関連付けられています。

ステップ 1 **[管理]** > **[ユーザー管理]** > **[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 **[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 *84* : グループの追加

フィールド	説明
グループ名	グループ名を入力します。
選択したポート	**[ポートの選択]** をクリックします。開いた **[ポートの選択]** 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]** 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。

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。

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。