Cisco Nexus Data Broker 構成ガイド、リリース 2.2

初版：2015 年 09 月 30 日

最終更新：2016 年 04 月 12 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/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system.All rights reserved.Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

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: http://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.(1110R)

The Java logo is a trademark or registered trademark of Sun Microsystems, Inc. in the U.S. or other countries.

© 2016 Cisco Systems, Inc. All rights reserved.

目 次

Cisco Nexus Data Broker の概要 1

Cisco Nexus Data Broker について 1

サポートされる Web ブラウザ 4

注意事項と制約事項 4

Cisco Nexus シリーズ スイッチの前提条件 5

Cisco Nexus Data Broker の展開 7

Cisco Nexus Data Broker のインストール 7

Cisco Nexus Data Broker ソフトウェアのインストールまたはアップグレード 7

Cisco Nexus Data Broker ソフトウェアのインストール 8

アプリケーション ソフトウェアのアップグレード 9

アプリケーションの起動 11

アプリケーションの動作の確認 13

TLS 証明書、キーストア、およびトラストストア ファイルの管理 15

TLS 証明書、キーストア、およびトラストストア ファイルについて 15

TLS 資格情報の生成準備 16

Cisco Nexus Data Broker のログインと管理 23

Cisco Nexus Data Broker の設定 23

ハイ アベイラビリティ クラスタの設定 23

ハイ アベイラビリティ クラスタのパスワード保護 24

Cisco Nexus スイッチのコンフィギュレーション ファイルの編集 25

エッジ ポートのユーザ ロールの設定 27

Cisco Nexus Data Broker GUI へのログイン 27

HTTP へのコントローラのアクセス変更 28

Cisco Nexus Data Broker GUI の概要 29

コンフィギュレーションの変更の保存 30

Cisco Nexus 9000 シリーズ スイッチの設定 31

注意事項と制約事項 31

Cisco Nexus 9000 シリーズ スイッチでの TCAM ハードウェアのサイジングの設定 32
Cisco Nexus 9000 シリーズ スイッチ上での CLI を使用した Cisco NX-API の有効化 33
スイッチ間ポートとポート チャネルのスイッチ ポート モードのトランクの有効化 34
デバイスの管理 35
ノード名の追加 35
展開したノード情報の表示 37
ポート リストの表示 38
デバイスの追加 38
デバイスの編集 39
デバイスの削除 40
ノード グループの追加 40
ノード グループへのノードの追加 41
ノード グループからのノードの削除 42
ノード グループの削除 43
ゲートウェイ IP アドレスの追加 43
ゲートウェイ IP アドレスの削除 44
ポートの追加 45
ポートおよびデバイスの設定 47
Cisco Nexus Data Broker のポート タイプについて 47
VLAN タギング 48
ポート タイプの設定 49
複数のポートの設定 50
ポート タイプ設定の削除 50
モニタリング デバイスの設定 51
モニタリング デバイスの削除 52
ルート ノードの設定 53
Cisco onePK Agent 53
onePK エージェントへの接続 53
対称型ロード バランシング 54
対称型ロード バランシングの設定 54
MPLS タグ除去の有効化 55
MPLS タグ除去の設定 55

Q-in-Q の設定 56
パケット切り捨ての設定 56
タイムスタンプのタギングの設定 57
フローのフィルタリング 59
Cisco Nexus Data Broker ネットワークについて 59
転送パス オプションについて 60
フィルタおよび接続について 60
リダイレクションとサービス ノードについて 61
フィルタの追加 62
フィルタの編集 69
フィルタの削除 75
接続の追加 76
接続の変更 79
接続の複製 81
接続の削除 83
サービス ノードの追加 84
リダイレクションの追加 84
リダイレクションの変更 88
リダイレクションの削除 91
ロールおよびリソースの管理 93
Cisco Data Broker のユーザについて 93
ロールの作成 94
複数の分離されたネットワークにアクセスするためのロールの設定 94
ロールの削除 96
リソース グループの作成 96
リソース グループへのリソースの追加 96
ロールへのグループの割り当て 97
グループの割り当て解除 98
グループの削除 98
フローの管理 101
フロー プログラミングの概要 101
フロー エントリの追加 102

フローの詳細情報の表示 105
トラブルシューティング 107
トラブルシューティングの概要 107
フローおよびポートの詳細統計情報の表示 108
整合性がないコントローラ のフローまたは整合性がないノードのフロー 108
整合性がないフローの詳細のエクスポート 109
整合性がないフローの修正 109
SDN アナライザ 110
SDN アナライザの使用 110
SDN アナライザのデフォルト値の変更 111
スライスの管理 113
スライス マネージャの概要 113
スライスの追加 114
スライスへのノードとポートの追加 115
フロー スペックの追加 115
管理タスク 117
AAA サーバの概要 117
AAA サーバの追加 118
RADIUS サーバのユーザ認証の設定 118
AAA サーバの表示 119
ユーザとロール 119
ユーザ情報の表示 120
ユーザの追加 120
既存ユーザのパスワードの変更 122
ユーザの削除 122
クラスタ管理情報の表示 122
OSGi コンソールの表示 123
Northbound API コンテンツの表示 124
システム管理 124
システム ログ ファイルのダウンロード 125
システム設定ファイルのダウンロード 125
システム設定ファイルのアップロード 126

設定のバックアップと復元 126
管理者パスワードの回復 127
アプリケーション ソフトウェアのアンインストール 128

第 1 章

Cisco Nexus Data Broker の概要

この章の内容は、次のとおりです。

- Cisco Nexus Data Broker について，1 ページ
- サポートされる Web ブラウザ，4 ページ
- 注意事項と制約事項，4 ページ
- Cisco Nexus シリーズ スイッチの前提条件，5 ページ

Cisco Nexus Data Broker について

従来からアプリケーション トラフィックの可視性は、セキュリティ、トラブルシューティング、およびコンプライアンスを維持し、リソース計画を行うためのインフラ運用にとって重要なことでした。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不可欠となっています。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とっては困難です。

Cisco Nexus スイッチと Cisco Nexus Data Broker の連携によって実現する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では、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に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お客様に適しています。

さまざまなCisco Nexusスイッチを使用する柔軟性、および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、複製し、トラフィックを複数のモニタリング ツールに転送する能力が提供されます。このトラフィックは、異なるスイッチをまたいで接続できます。スイッチとの通信に OpenFlow 向けの

シスコのプラグインと Cisco NX-API エージェントを組み合わせて使用すると、Cisco Nexus 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 Data Broker は、複数の分離された Cisco Nexus Data Broker ネットワークの管理サポートを提供します。同一のアプリケーション インスタンスを使用して分離されている可能性のある、複数の Cisco Nexus 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 Cisco Nexus Data Broker ソリューションを各データセンターに導入する場合は、各モニタリングネットワークに対して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、1 つの アプリケーション インスタンスを使用して、5 つすべての独立した展開を管理できます。

Cisco Nexus Data Broker は、以下を提供します。

- OpenFlow モードまたは NX-API モードでの動作。

（注） OpenFlow モードおよび NX-API モードは、Cisco Nexus 3000 シリーズと Cisco Nexus 9000 シリーズの両方のスイッチでサポートされています。Cisco Nexus 9500 は、展開の NX-API モードのみをサポートします。Cisco Nexus 3500 は、展開のオープンフロー モードのみをサポートします。一度にイネーブルにできるモードは、OpenFlow または NX-API のいずれか 1 つのみです。

組み込みモードの Cisco Nexus Data Broker アプリケーションを起動または停止するには、ofa ファイルをアクティブまたは非アクティブにする必要があります。./runxnc.sh はこのアプリケーションの起動に適した方法ではないため使用しないでください。

一度にイネーブルにできるモードは、OpenFlow または NX-API のいずれか 1 つのみです。

（注） Cisco Nexus 3000 Release 7.x 以降、次の Cisco Nexus シリーズ スイッチで NX-API の設定がサポートされています。

- Cisco Nexus 3172 スイッチ
- Cisco Nexus 3132 スイッチ
- Cisco Nexus 3164 スイッチ
- Cisco Nexus 31128 スイッチ
- Cisco Nexus 3232 スイッチ
- Cisco Nexus 3264 スイッチ

- HTTP メソッドを使用した HTTP トラフィックのレイヤ 7 フィルタリング。
- VLAN および MPLS タグの除去。
- TAP および SPAN ポートの集約に対してスケーラブルなトポロジ。

- 入力ソースの TAP ポートおよび SPAN ポートにタグ付けする Q-in-Q。
- 対称型ロード バランシング。
- レイヤ 1 からレイヤ 4 の情報に基づいてトラフィックをモニタする一致ルール。
- トラフィックを複製して複数のモニタリング ツールに転送する機能。
- Precision Time Protocol（PTP）を使用したタイムスタンプ。
- 指定バイト数を超えるパケットの切り捨てによるペイロードの廃棄。
- TAP/SPAN アグリゲーション ネットワーク状態の変化への対応。
- 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 を使用した外部 Active Directory との統合。
- エンドツーエンドのパスの可視性。これには、トラブルシューティングに必要なポート レベルとフロー レベルの両方の統計情報が含まれます。
- 堅牢な Representational State Transfer（REST）API、およびすべての機能の実行を対象とした Web ベースの GUI。
- Open Flow 向けシスコのプラグイン（バージョン 1.0）のサポート
- Cisco Nexus Data Broker は、TAP/SPAN の集約として Cisco Nexus 9000 シリーズ スイッチをサポートするため、NX-API プラグインを追加します。NX-API は、JSON-RPC、XML、および JSON をサポートします。Cisco Nexus Data Broker は、JSON メッセージ形式の NX-API を使用して Cisco Nexus 9000 シリーズと対話します。

Cisco Nexus Data Broker を使用すると、次のことができます。

- Switched Port Analyzer（SPAN）と Test Access Point（TAP）ポートを分類する。
- Cisco APIC を介して Cisco ACI を統合し、SPAN 宛先および SPAN セッションを設定する。
- トラフィックをキャプチャするためのモニタリング デバイスを追加する。
- モニタリングの必要があるトラフィックをフィルタリングする。
- 単一または複数の SPAN および TAP ポートからのパケットを配信ポートを介して複数のモニタリング デバイスに

  リダイレクトする。
- モニタリング システムを表示および変更できるユーザを制限する。
- スイッチのタイプに応じて、次の追加機能を設定します。
  - MPLS タグ除去の有効化。
  - Cisco Nexus 3000 シリーズ スイッチの VLAN ID の設定。
  - Symmetric load balancing onCisco Nexus 3100 シリーズ スイッチ および Cisco Nexus 9000 シリーズ スイッチの対称的ロード バランシング。

- Cisco Nexus 3000 シリーズ スイッチ、3100 シリーズ スイッチ、および Cisco Nexus 9000 シリーズ スイッチでの Q-in-Q。
- Cisco Nexus 3500 シリーズ スイッチ のタイムスタンプのタギングおよびパケット切り捨て。

サポートされる Web ブラウザ

Cisco Nexus Data Broker では、次の Web ブラウザがサポートされています。

- Firefox 18.x 以降のバージョン
- Chrome 24.x 以降のバージョン

（注） Javascript 1.5 以降のバージョンをブラウザで有効にする必要があります。

注意事項と制約事項

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

- 2 GHz 以上の 1 個の 8 コア CPU。
- 最低 16 GB のメモリ。
- 最小 40 GB の空きハードディスク領域が、Cisco Nexus Data Broker アプリケーションをインストールするパーティションで使用できる必要があります。
- 次のような、Java を備えた 64 ビットの Linux ディストリビューション：
  - Ubuntu Linux
  - Red Hat Enterprise（RHEL）Linux
  - Fedora Linux
- 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用に Python 2.7.3 以降のバージョンが必要です。
- プロファイルの $JAVA_HOME 環境変数が JVM のパスにセットされている。
- JConsole および VisualVM は両方 JDK に含まれますが、トラブルシューティング用に追加するものとして推奨されます（ただし、必須ではありません）。

Cisco Nexus シリーズ スイッチの前提条件

Cisco Nexus Data Broker は Cisco Nexus 3000、3100、3200、3500、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、以下を行う必要があります。

- スイッチにログインする管理者権限があることを確認する。
- switch# show running-config interface mgmt0 コマンドを実行して、スイッチの管理インターフェイス（mgmt0）に IP アドレスが設定されていることを確認する。
- 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 リダイレクションが VLAN フィルタリングをサポートできるように、Cisco Nexus Data Broker で使用する VLAN 範囲をデータベースに追加する（たとえば、構文は **vlan <range of VLAN IDs>**、VLAN 範囲は <1-3967> など）。

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

デバイス モデル	OpenFlow モード	NX-API モード
Nexus 3000 シリーズ スイッチ	プロンプトで # hardware profile openflow コマンドを入力します。	Cisco Nexus 3000 シリーズ スイッチを使用すると、Openflow モードのみがサポートされます。
Nexus 3164Q スイッチ	OpenFlow モードは Nexus 3164Q スイッチでサポートされていません。	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**

デバイス モデル	OpenFlow モード	NX-API モード
Nexus 3200 シリーズ スイッチ	プロンプトで hardware access-list tcam region openflow 256 コマンドを入力します。	プロンプトで次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**
Nexus 9000 シリーズ スイッチ	プロンプトで hardware access-list tcam region openflow 512 コマンドを入力します。	プロンプトで次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**

第 2 章

Cisco Nexus Data Broker の展開

この章の内容は、次のとおりです。

- Cisco Nexus Data Broker のインストール，7 ページ

Cisco Nexus Data Broker のインストール

Cisco Nexus Data Broker ソフトウェアのインストールまたはアップグレード

重要

Cisco XNC Monitor Manager リリース 1.5 および 1.6 から Cisco Nexus Data Broker リリース 2.2 への直接のアップグレード パスはありません。Cisco XNC Monitor Manager リリース 1.5 および 1.6 がインストールされており、最新の Cisco Nexus Data Broker リリースに更新したい場合は、まず Cisco Nexus Data Broker 2.0 リリースにアップグレードする必要があります。手順については、『*Cisco Extensible Network Controller Deployment Guide*』を参照してください。

- Cisco Nexus Data Broker の新規インストールを完了するには、Cisco Nexus Data Broker ソフトウェアのインストール，（8 ページ）を参照してください。
- Cisco XNC Monitor Manager リリース 1.5 または リリース 1.6 を Cisco Nexus Data Broker 2.0 にアップグレードし、次に 2.2 リリースにアップグレードするには、『*Cisco Nexus Data Broker* 構成ガイド』のアップグレードのセクションを参照してください。

Cisco Nexus Data Broker ソフトウェアのインストール

手順

ステップ 1 Web ブラウザで、Cisco.com に移動します。

ステップ 2 [Support] で [All Downloads] をクリックします。

ステップ 3 中央のペインで、[Cloud and Systems Management] をクリックします。

ステップ 4 入力を求められたら、Cisco.com のユーザ名およびパスワードを入力して、ログインします。

ステップ 5 右側のペインで、[Network Controllers and Applications] をクリックし、[Cisco Nexus Data Broker] をクリックします。
リリース 2.2.0 のファイル情報が表示されます。Cisco Nexus Data Broker Software Application：ndb1000-sw-app-k9-2.2.0.zip

ステップ 6 Cisco Nexus Data Broker アプリケーション バンドルをダウンロードします。

ステップ 7 Linux マシンで、Cisco Nexus Data Broker をインストールする予定のディレクトリを作成します。たとえば、ホーム ディレクトリに、`CiscoNDB` を作成します。

ステップ 8 作成したディレクトリに Cisco Nexus Data Broker の zip ファイルをコピーします。

ステップ 9 Cisco Nexus Data Broker zip ファイルを解凍します。
Cisco Nexus Data Broker ソフトウェアが `xnc` というディレクトリにインストールされます。ディレクトリには、次の内容が含まれます。

- `runxnc.sh` ファイル：Cisco Nexus Data Broker を起動するために使用するファイル。
- `version.properties` ファイル：Cisco Nexus Data Broker のビルド バージョン。
- `captures` ディレクトリ：Cisco Nexus Data Broker で実行された分析の出力ダンプ ファイルが含まれるディレクトリ。

  （注） `captures` ディレクトリは Cisco Nexus Data Broker 分析ツールの実行後に作成されます。

- `configuration` ディレクトリ：Cisco Nexus Data Broker 初期化ファイルを含むディレクトリ。

  このディレクトリには、設定が保存されている `startup` サブ ディレクトリが含まれます。

- `bin` ディレクトリ：次のスクリプトを含むディレクトリです。
  - `xnc` ファイル：このスクリプトは、Cisco Nexus Data Broker の共通 CLI を含んでいます。
- `etc` ディレクトリ：プロファイル情報が含まれるディレクトリ。
- `lib` ディレクトリ：Cisco Nexus Data Broker Java ライブラリを含むディレクトリ。
- `logs` ディレクトリ：Cisco Nexus Data Broker ログを含むディレクトリ。

  （注） `logs` ディレクトリは、Cisco Nexus Data Broker アプリケーションが起動された後に作成されます。

- plugins ディレクトリ：OSGi プラグインが含まれるディレクトリ。
- work ディレクトリ：Web サーバの作業ディレクトリ。

（注） work ディレクトリは、Cisco Nexus Data Broker アプリケーションが起動された後に作成されます。

アプリケーション ソフトウェアのアップグレード

upgrade コマンドを使用して Cisco Nexus Data Broker リリース 2.0、リリース 2.0.1、または リリース 2.1 から Cisco Nexus Data Broker リリース 2.2 にアップグレードできます。このアップグレードはインプレース アップグレードです。つまり、製品ビットが置き換えられます。必要に応じて、元のインストールを復旧するため、バックアップ アーカイブが作成されます。

（注） アップグレード スクリプトを実行することで、Cisco Nexus Data Broker Release 2.0、Release 2.0.1、または Release 2.1 から Cisco Nexus Data Broker リリース 2.2 に直接アップグレードできます。Cisco XNC リリース 1.5 またはリリース 1.6 からアップグレードする場合、まずは Cisco Nexus Data Broker リリース 2.0 にアップグレードし、次に Cisco Nexus Data Broker リリース 2.2 にアップグレードする必要があります。

upgrade コマンドを実行する場合、インストールおよび設定がアップグレードされます。ただし、runxnc.sh や config.ini など、シェル スクリプトや設定ファイルに加えられた変更は上書きされます。アップグレード プロセスが完了したら、手動でこれらのファイルに変更を再適用します。

はじめる前に

- Cisco XNC Monitor Manager リリース 1.6 から Cisco Nexus Data Broker 2.0 にアップグレードした場合、パスワードをリセットし、コントローラを起動し、Cisco XNC Monitor Manager GUI の最上部のメニュー バーの [Save] ボタンを使用して設定を保存します。
- Nexus Data Broker 2.0 インストールを使用するすべてのコントローラ インスタンスを停止します。これにより、アップグレード中に更新されるファイル システムとの競合も回避されます。
- ハイ アベイラビリティ クラスタリングを使用している場合、クラスタ内のすべてのアプリケーション インスタンスを停止して、不整合がないことを確認します。
- config.ini および runxnc.sh ファイルをバックアップします。

重要　アップグレードする前に、`config.ini` および `runxnc.sh` ファイルを手動でバックアップする必要があります。バックアップ プロセスでは、それらのバックアップが実行されないためです。アップグレードする前にバックアップを行わない場合、加えた変更は失われます。

手順

ステップ 1　Web ブラウザで、Cisco.com に移動します。

ステップ 2　[Support] で [All Downloads] をクリックします。

ステップ 3　中央のペインで、[Cloud and Systems Management] をクリックします。

ステップ 4　右側のペインで、[Network Controllers and Applications] をクリックし、[Cisco Nexus Data Broker] をクリックします。

ステップ 5　Cisco Nexus Data Broker リリース 2.2 アプリケーション バンドル：Cisco Nexus Data Broker ソフトウェア アプリケーション：ndb1000-sw-app-k9-2.2.0.zip をダウンロードします。

ステップ 6　Linux マシンで、Cisco Nexus Data Broker をアップグレードする予定の一時ディレクトリを作成します。
たとえば、`Home` ディレクトリに、`CiscoNDB_Upgrade` を作成します。

ステップ 7　作成した一時ディレクトリに Cisco Nexus Data Broker リリース 2.2 の zip ファイルを解凍します。

ステップ 8　先ほど Cisco Nexus Data Broker 2.0 リリースをインストールしたときに作成した `xnc` ディレクトリに移動します。

ステップ 9　すべての Cisco Nexus Data Broker 2.0 リリース プロセスの実行を停止します。

ステップ 10　標準のバックアップ手順を使用して、Cisco Nexus Data Broker 2.0 リリースのインストールをバックアップします。

ステップ 11　Cisco Nexus Data Broker リリース 2.2 アップグレード ソフトウェア用に作成した一時ディレクトリの `xnc/bin` ディレクトリに移動します。

ステップ 12　**./xnc upgrade --perform --target-home** {*xnc_directory_to_be_upgraded*} **[--verbose] [--backupfile** {*xnc_backup_location_and_zip_filename*}**]** コマンドを入力して、アプリケーションをアップグレードします。
次のいずれかのオプションを選択できます。

オプション	説明
--perform--target-home {*xnc_directory_to_be_upgraded*}	Cisco XNC Monitor Manager インストールを Cisco Nexus Data Broker にアップグレードします。
--perform--target-home {*xnc_directory_to_be_upgraded*} **--backupfile** {*xnc_backup_location_and_zip_filename*}	Cisco XNC Monitor Manager インストールを Cisco Nexus Data Broker にアップグレードし、設定したディレクトリ パスにバックアップの .zip ファイルを作成します。 （注）　バックアップ ファイルの名前および .zip 拡張子を指定する必要があります。

オプション	説明
--rollback--target-home {*xnc_directory_to_be_upgraded*}	以前の Cisco XNC Monitor Manager インストールにロールバックします。
--rollback--target-home {*xnc_directory_to_be_upgraded*} **--backupfile** {*xnc_backup_location_and_zip_filename*}	設定した絶対パスのバックアップ ファイルを使用して、以前の Cisco XNC Monitor Manager インストールにロールバックします。
--verbose	コンソールに詳細情報を表示します。このオプションは、他のオプションとともに使用でき、デフォルトでは無効になっています。
--validate--target-home {*xnc_directory_to_be_upgraded*}	インストールを検証します。
./xnc ヘルプのアップグレード	**upgrade** コマンドのオプションを表示します。

ステップ 13 元々 Cisco XNC Monitor Manager をインストールした xnc ディレクトリに移動します。

ステップ 14 以前に停止したアプリケーション プロセスを起動します。

（注） アップグレード後に Web UI から Cisco Nexus Data Broker にアクセスする場合は、Ctrl+F5 を押すか、Cmd キー、Shift キー、および R キーを同時に押します。

ステップ 15 アップグレードに関する問題が発生した場合は、次のタスクを実行します。

a) すべてのアプリケーション プロセスを停止します。
b) ステップ 6 で作成した一時ディレクトリに移動します。
c) **./xnc upgrade --rollback --target-home** {*xnc_directory_to_be_downgraded*} **--backupfile** {*xnc_backup_location_and_zip_filename*}**[--verbose]** コマンドを入力します。
d) アプリケーション プロセスを再起動します。

（注） ロールバック後に Web UI から Cisco XNC Monitor Manager にアクセスする場合は、Ctrl+F5 を押すか、Cmd キー、Shift キー、および R キーを同時に押します。

アプリケーションの起動

手順

ステップ 1 （任意） **./xnc reset-admin-password [--wait-seconds** {*wait_time*} **--password** {*password*}**]** コマンドを入力して、Cisco Nexus Data Broker とともに提供されているデフォルト パスワードを変更します。

{*password*} 変数は、ユーザ マネージャを再起動することで、指定した値に管理者パスワードをリセットします。{*wait_time*} はユーザ マネージャが再起動する間に待機する秒数です。最小の {*wait_time*} の値は 5 秒、最大は 60 秒です。

（注）
- パスワードは 8 ～ 256 文字で、大文字と小文字が含まれ、1 つ以上の数字および英数字以外の文字が必要です。
- パスワードを空白のままにすると、工場出荷時のデフォルトである「admin」にリセットされます。
- 管理パスワードをリセットするたびに、新しいパスワードがこれらの要件を必ず満たすようにしてください。そうしないと、Cisco Nexus Data Broker にログインできなくなります。

ステップ 2 **./runxnc.sh** コマンドを入力して、xnc ディレクトリに移動し、Cisco Nexus Data Broker を起動します。
次のいずれかのオプションを選択できます。

オプション	説明
オプションなし	Cisco Nexus Data Broker を **-start** オプションを使用して起動します。
-jmx	Cisco Nexus Data Broker JVM での Java Management Extensions（JMX）のリモートアクセスを有効化します。これは、パフォーマンス問題のトラブルシューティングに使用できます。
-jmxport*port_number*	指定した JVM ポートで JMX リモートアクセスを有効にします。
-debug	Cisco Nexus Data Broker JVM でデバッグを有効にします。
-debugsuspend	デバッガが接続されるまで Cisco Nexus Data Broker の起動を一時停止します。
-debugport*port_number*	指定した JVM ポートでのデバッグを有効にします。
-start	Cisco Nexus Data Broker を起動し、ポート 2400 番でのセキュアシェル（SSH）によるアクセスを提供します。 （注） SSH サーバは、ネットワーク管理者ロールを持つ Cisco Nexus Data Broker ユーザがアクセスできます。
-start*port_number*	Cisco Nexus Data Broker を起動し、指定したポート番号上のコントローラに SSH アクセスします。 （注） SSH サーバは、ネットワーク管理者ロールを持つ Cisco Nexus Data Broker ユーザがアクセスできます。*port_num* 値の有効な範囲は、1024 ～ 65535 です。
-stop	StopsCisco Nexus Data Broker.

オプション	説明
-status	すべての Cisco Nexus Data Broker のステータスを表示します。
-console	OSGi コンソールを使用して Cisco Nexus Data Broker を起動します。
-help	**./runxnc.sh** コマンドのオプションを表示します。
-tls	Cisco Nexus Data Broker と OpenFlow または onePK スイッチ間の TLS セキュア接続を有効にします。 TLS を有効にするには、**./runxnc.sh -tls-tlskeystore***keystore_file_location***-tlstruststore***truststore_file_location* コマンドを入力してコントローラを起動します。
-osgiPasswordSync	XNC パスワードを変更した場合、XNC と同一の OSGi Web コンソールのパスワードを設定します。 （注） この手順は任意です。アプリケーションがこのオプションなしで起動された場合、OSGi コンソールはデフォルトの資格情報を使用してアクセスできます。

（注） runxnc.sh スクリプトを使用して Cisco Nexus Data Broker を起動します。JAVA_HOME という名前のパス変数を設定する必要があります。これにより、起動に使用されるパス変数を設定し、OSGi フレームワークを指定したオプションを使用して起動します。ユーザが 1.7 より前の Java バージョンを使用して Cisco Nexus Data Broker アプリケーションの起動を試みると、エラー メッセージが表示されてアプリケーションが中断します。この問題を解決するには、現在の Java バージョンをアップグレードし、Cisco Nexus Data Broker を再起動します。現在使用している Java バージョンが 1.8.0_45 よりも前の場合、起動前に 1.8.0_45 以降にアップグレードすることを推奨する警告メッセージが表示されます。

アプリケーションの動作の確認

手順

ステップ 1 Cisco Nexus Data Broker をインストールした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 ディレクトリに移動します。

ステップ 3 **./runxnc.sh -status** コマンドを入力して、アプリケーションが実行中であることを確認します。

コントローラは次を出力し、コントローラが PID 21680 の Java プロセスを実行していることを示します。

```
Controller with PID:21680 -- Running!
```

（注） Nexus Data Broker は、Web ブラウザを介して以下でアクセスできます。

```
https://Nexus_data_broker_ip:8443
```

次の作業

コントローラにスイッチを接続します。詳細については、スイッチの構成ガイドを参照してください。

第 3 章

TLS 証明書、キーストア、およびトラストストア ファイルの管理

この章の内容は、次のとおりです。

- TLS 証明書、キーストア、およびトラストストア ファイルについて，15 ページ
- TLS 資格情報の生成準備，16 ページ

TLS 証明書、キーストア、およびトラストストア ファイルについて

（注） onePK デバイスをサポートするには、onePK または OpenFlow エージェントを使用する Cisco Nexus Data Broker に対するすべての接続に、Transport Layer Security（TLS）が必要です。NX-API デバイスの場合、TLS はオプションです。

（注） Cisco Nexus Data Broker を通常の方法で起動すると、デバイスへの接続は HTTP です。TLS プロトコルを使用して Cisco Nexus Data Broker を起動すると、デバイスへの接続は HTTPS で行われます。

Cisco Nexus Data Broker と OpenFlow または onePK スイッチ間の TLS 接続を有効にするには、TLS キーストアおよびトラストストアが必要です。TLS キーストア ファイルと TLS トラストストア ファイルは、パスワードで保護されています。

OpenFlow を介して Cisco Nexus Data Broker に接続する Cisco Nexus シリーズ スイッチには、秘密キー、証明書、認証局（CA）などの追加の資格情報が必要です。

- TLS のキーストア ファイルには、Cisco Nexus Data Broker が使用する秘密キーと証明書情報が含まれます。

- TLS トラストストア ファイルには、接続先スイッチの証明書に署名するために使用される認証局（CA）の証明書が含まれます。

Cisco Nexus Data Broker の実装において TLS 接続が必要な場合は、ネットワーク内の接続はすべて暗号化する必要があり、TLS を有効にして Cisco Nexus Data Broker を実行する必要があります。Cisco Nexus Data Broker が TLS を使用して起動した後で、TLS キーストア パスワード設定コマンドを実行して Cisco Nexus Data Broker のパスワードを入力し、キーストア ファイルをロック解除する必要があります。

TLS 資格情報の生成準備

OpenFlow および Cisco OnePK スイッチには、TLS を有効にするための暗号化設定が必要です。

NX-API プロトコル プラグインは、デバイスに対するセキュアな通信を行うための TLS をサポートするようになりました。セキュア ポートの 443 番で、NX-API プロトコル プラグインに接続できます。すべての設定、検出、および統計収集は、セキュアな通信を使用して実行されます。Cisco Nexus Data Broker は必要な証明書を使用して設定され、セキュア モードで起動される必要がありますCisco Nexus Data Broker が TLS モードで起動すると、すべてのデバイスは TLS 接続をサポートします。スイッチへの通常の非暗号化接続は受け入れられません。

注意 自己署名証明書は、小規模な環境でのテストにのみ適しています。個々の証明書の使用と失効に関する追加のセキュリティおよびきめ細かな制御のために、組織の認証局によって生成された証明書を使用する必要があります。また、実稼働環境ではこの手順によって生成されたキーと証明書を決して使用しないでください。

はじめる前に

以下の手順を行う Linux ホストに OpenSSL がインストールされていることを確認します。

手順

ステップ 1 **mkdir -p TLS** コマンドを使用して TLS ディレクトリを作成し、**cd TLS** コマンドを使用してそこに移動します。

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

ステップ 2 CA システムが内部で動作するためのディレクトリを設定します。**mkdir -p mypersonalca/<directory name>** コマンドを使用して `mypersonalca` の下に 3 つのディレクトリを作成します。`serial` ファイルおよび `index.txt` ファイルを初期化するため、**echo "01" > mypersonalca/serial** コマンドおよび **touch mypersonalca/index.txt** コマンドをそれぞれ入力します。

```
mkdir -p mypersonalca/certs
mkdir -p mypersonalca/private
mkdir -p mypersonalca/crl
```

echo "01" > mypersonalca/serial

touch mypersonalca/index.txt

serial ファイルおよび index.txt ファイルは、CA によって証明書ファイルのデータベースを維持するために使用されます。

ステップ 3 CA 設定ファイル（ca.cnf）を作成します。ca.cnf ファイルを保存する前に、デバイスに固有のいくつかの変更を加える必要があります。1 つの重要な変更は、ca.cnf ファイル内の [alt_names] セクションをデバイス IP アドレスに関連付けて変更することです。これらの IP アドレスは、設定ファイル内で指定されるものだからです。より小数の/多数の IP/DNS 名が必要であれば、これらの線を追加または削除できます。

（注） このステップは、NX-API のみに当てはまります。

次は、ca.cnf ファイルの内容の例です。

```
[ ca ]
default_ca              = CA_default


[ CA_default ]
dir                     = .
serial                  = $dir/serial
database                = $dir/index.txt
new_certs_dir           = $dir/newcerts
certs                   = $dir/certs
certificate             = $certs/cacert.pem
private_key             = $dir/private/cakey.pem
default_days            = 365
default_md              = sha1
preserve                = no
email_in_dn             = no
nameopt                 = default_ca
certopt                 = default_ca
policy                  = policy_match
copy_extensions         = copy


[ policy_match ]
countryName             = match
stateOrProvinceName     = match
organizationName        = match
organizationalUnitName  = optional
commonName              = supplied
emailAddress            = optional



[ req ]
default_bits            = 2048                  # Size of keys
default_keyfile         = example.key           # name of generated keys
default_md              = sha1                  # message digest algorithm
string_mask             = nombstr               # permitted characters
distinguished_name      = req_distinguished_name
```

```
req_extensions          = v3_req
x509_extensions         = v3_req


[ req_distinguished_name ]
# Variable name           Prompt string
#----------------------   ----------------------------------
0.organizationName      = Organization Name (company)
organizationalUnitName  = Organizational Unit Name (department, division)
emailAddress            = Email Address
emailAddress_max        = 40
localityName            = Locality Name (city, district)
stateOrProvinceName     = State or Province Name (full name)
countryName             = Country Name (2 letter code)
countryName_min         = 2
countryName_max         = 2
commonName              = Common Name (hostname, IP, or your name)
commonName_max          = 64


# Default values for the above, for consistency and less typing.
# Variable name                   Value
#------------------------------   ------------------------------
commonName_default              = www.cisco.com
0.organizationName_default      = Cisco
localityName_default            = San Jose
stateOrProvinceName_default     = CA
countryName_default             = US
emailAddress_default            = webmaster@cisco.com


[ v3_ca ]
basicConstraints        = CA:TRUE
subjectKeyIdentifier    = hash
authorityKeyIdentifier  = keyid:always,issuer:always



[ v3_req ]
# Extensions to add to a certificate request
basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment


# Some CAs do not yet support subjectAltName in CSRs.
# Instead the additional names are form entries on web
# pages where one requests the certificate...
subjectAltName          = @alt_names


[alt_names]
IP.1   = 1.1.1.1
IP.2   = 2.2.2.2
IP.3   = 3.3.3.3
IP.4   = 4.4.4.4
```

```
[ server ]
# Make a cert with nsCertType set to "server"
basicConstraints=CA:FALSE
nsCertType                      = server
nsComment                       = "OpenSSL Generated Server Certificate"
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid,issuer:always


[ client ]
# Make a cert with nsCertType set to "client"
basicConstraints=CA:FALSE
nsCertType                      = client
nsComment                       = "OpenSSL Generated Client Certificate"
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid,issuer:always
```

ステップ 4 ディレクトリ構造を作成し、設定ファイル（ca.cnf）をディスクに保存したら、TLS証明書ファイルを作成します。

openssl req -x509 -nodes -days 3650 -newkey rsa:2048 -out mypersonalca/certs/ca.pem -outform PEM -keyout mypersonalca/private/ca.key コマンドを入力することで、TLS 秘密キーおよび証明機関（CA）ファイルを生成します。このステップでは、PEM 形式の 2048 ビット長 TLS 秘密キーと CA ファイルを生成します。

openssl req -new -x509 -days 365 -nodes -out server.crt -keyout server.key -config Example.conf を入力することで、証明書（**server.key** および **server.crt**）ファイルを生成します。

ステップ 5 **server.key** および **server.crt** をそれぞれのデバイスにコピーし、次のコマンドを使用してインストールします。

configure terminal を使用してグローバル コンフィギュレーション モードを開始します。

nxapi certificate httpskey keyfile bootflash:///server.key を入力します。ここで、bootflash:/// は **server.key** のファイルの場所です。

nxapi certificate httpscrt certfile bootflash:///server.crt を入力します。ここで、bootflash:/// は **server.crt** のファイルの場所です。

nxapi certificate enable

ステップ 6 TLS キーストア ファイルの作成

（注） TLS キーストア ファイルは、Cisco Nexus Data Broker の設定ディレクトリに配置してください。

server.key を **xnc-privatekey.pem** にコピーします。このコマンドにより、ステップ 5 で生成された **server.key** ファイルをコピーします。たとえば、コマンド **cp server.key xnc-privatekey.pem** を使用します。

server.crt を **xnc-cert.pem** にコピーします。このコマンドにより、ステップ 5 で生成された *server.crt* ファイルのコピーを作成します。たとえば、コマンド **cp server.crt xnc-cert.pem** を使用します。

cat xnc-privatekey.pem xnc-cert.pem > xnc.pem コマンドを入力し、**xnc.pem** ファイルを作成します。これには、秘密キーと証明書が含まれています。

openssl pkcs12 -export -out xnc.p12 -in xnc.pem コマンドを入力して、PEM ファイル **xnc.pem** ファイルをファイル **xnc.p12** ファイルに変換します。プロンプトでパスワードを入力します。これがエクスポート パスワードになります。cisco123 など、パスワードには 6 文字以上が必要です。このステップおよびステップ 7 で同じパスワードを使用する必要があります。xnc.pem ファイルはパスワード保護された .p12 ファイルに変換されます。

keytool -importkeystore -srckeystore xnc.p12 -srcstoretype pkcs12 -destkeystore tlsKeyStore -deststoretype jks コマンドを入力して xnc.p12 を Java キーストア（tlsKeyStore）ファイルに変換します。このコマンドにより、xnc.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。プロンプトでパスワードを入力します。前のステップで入力したものと同一のパスワードを使用します。

ステップ 7 TLS 信頼ストア ファイルの作成

TLS トラストストア ファイルは、アプリケーション設定ディレクトリに配置してください。

mypersonalca/certs/ca.pem ファイルを **sw-cacert.pem** にコピーします。

keytool -import -alias swca1 -file sw-cacert.pem -keystore tlsTrustStore コマンドを入力して、**sw-cacert.pem** ファイルを Java トラストストア（tlsTrustStore）ファイルに変換します。

プロンプトでパスワードを入力します。**sw-cacert.pem** ファイルがパスワード保護された Java トラストストア（tlsTrustStore）ファイルに変換されます。*cisco123* など、パスワードには 6 文字以上が必要です。

ステップ 8 TLS を使用したアプリケーションの起動

tlsKeystore および tlsTruststore ファイルを NDB の /configuration フォルダにコピーします。コンソールから、**./runxnc.sh -tls -tlskeystore ./configuration/tlsKeyStore -tlstruststore ./configuration/tlsTrustStore** コマンドを入力して、Cisco Nexus Data Broker を起動します。これで Cisco Nexus Data Broker は、TLS が有効な状態で起動します。

ステップ 9 TLS キーストアおよびトラストストア パスワードの提供

TLS キーストアおよびトラストストア パスワードは、パスワード保護された TLS キーストアおよびトラストストア ファイルを読み取ることができるように、Cisco Nexus Data Broker に送信されます。

Cisco Nexus Data Broker をインストールしたコマンド ウィンドウを開きます。

xnc/bin ディレクトリに移動します。

./xnc config-keystore-passwords [--user {user} --password {password} --url {url} --verbose --prompt --keystore-password {keystore_password} --truststore-password {truststore_password}] コマンドを入力して、TLS キーストアおよび TLS トラストストア パスワードを提供します。

次の情報を入力します。

- Cisco Nexus Data Broker ユーザ名 {user}：ユーザ名
- Cisco Nexus Data Broker password {password}：ユーザのパスワードたとえば、デフォルトの管理者パスワードは *admin* です。

- Cisco Nexus Data Broker web URL {url}：アプリケーションの Web URL。たとえば、デフォルト URL は、https://Nexus_Data_Broker_IP:8443 です。
- TLS KeyStore パスワード {keystore_password}：TLS キーストア パスワード.
- TLS トラストストア パスワード {keystore_password}：TLS トラストストア パスワード
- 例：**./xnc config-keystore-passwords --user admin --password admin --url https://localhost:8443 --verbose --prompt --keystore-password cisco123 --truststore-password cisco123**

第 4 章

Cisco Nexus Data Broker のログインと管理

この章の内容は、次のとおりです。

- Cisco Nexus Data Broker の設定，23 ページ
- Cisco Nexus Data Broker GUI へのログイン，27 ページ
- HTTP へのコントローラのアクセス変更，28 ページ
- Cisco Nexus Data Broker GUI の概要，29 ページ
- コンフィギュレーションの変更の保存，30 ページ

Cisco Nexus Data Broker の設定

ハイ アベイラビリティ クラスタの設定

Cisco Nexus Data Broker は、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 モードのハイ アベイラビリティ クラスタリングをサポートします。Cisco Nexus Data Broker でハイ アベイラビリティ クラスタリングを使用するには、Cisco Nexus Data Broker のインスタンスごとに `config.ini` ファイルを編集する必要があります。

はじめる前に

- 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、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 xncjgroups.xml ファイルに設定する必要があります。ハイ アベイラビリティ クラスタのパスワード保護, （24 ページ）を参照してください。

手順

ステップ 1 クラスタ内のインスタンス上で Cisco Nexus Data Broker が実行されていないことを確認します。

ステップ 2 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 3 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 4 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 5 次のテキストを探します。

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

ステップ 6 # supernodes 行のコメントを削除し、<ip1>:<ip2><ip3>:<ipn> をクラスタ内の各 Cisco Nexus Data Broker インスタンスの IP アドレスで置き換えます。2 ～ 5 の IP アドレスを入力できます。

例：

```
# HA Clustering configuration (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
```

ステップ 7 ファイルを保存し、エディタを終了します。

ステップ 8 クラスタ内の Cisco Nexus Data Broker の各インスタンスに対してステップ 3 ～ 7 を繰り返します。

ステップ 9 Cisco Nexus Data Broker を再起動します。

ハイ アベイラビリティ クラスタのパスワード保護

xncjgroups.xml ファイルを使用して HA クラスタをパスワードで保護できます。このファイルは、Cisco Nexus Data Broker の各インスタンスに対してまったく同じにする必要があります。

手順

ステップ 1 クラスタ内のインスタンス上で Cisco Nexus Data Broker が実行されていないことを確認します。

ステップ 2 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 3 xnc/configuration ディレクトリに移動します。

ステップ 4 任意のテキスト エディタで xncjgroups.xmli ファイルを開きます。

ステップ 5 次のテキストを探します。

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

ステップ 6 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 7 （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場合、このパスワードをどのような値にでも変更できます。

ステップ 8 ファイルを保存し、エディタを終了します。

ステップ 9 クラスタ内の Cisco Nexus Data Broker の各インスタンスに対してステップ 4 ～ 8 を繰り返します。

ステップ 10 Cisco Nexus Data Broker を再起動します。

Cisco Nexus スイッチのコンフィギュレーション ファイルの編集

トポロジとインベントリが同期するように、Cisco Nexus Data Broker には、定期的に Cisco Nexus スイッチ インベントリとトポロジを再検出する機能があります。Cisco Nexus Data Broker は定期的にスイッチ インベントリとトポロジの相互接続、およびステータスを検出します。この情報は、ステータス別にGUI で更新されます。再検出の間隔は設定でき、デフォルト値は60秒です。

手順

	コマンドまたはアクション	目的
ステップ 1	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 2	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 3	次のパラメータを更新します。	

名前	事前定義された値（秒）	最小値（秒）	推奨値（秒）
of.messageResponseTimer	10	2	60
of.switchLivenessTimeout	—	60.5	120.5
of.flowStatsPollInterval	120	10	240
of.portStatsPollInterval	300	5	240
of.descStatsPollInterval	—	60	240

	コマンドまたはアクション	目的

名前	事前定義された値（秒）	最小値（秒）	推奨値（秒）
of.barrierMessagePriorCount	50	100	50
of.discoveryInterval	—	30	300
of.discoveryTimeoutMultiple	—	2	2
NX-API 関連システム パラメータ			
nx.connectionDelayTimer	300	—	300
nx.flowStatsPollInterval	120	—	120
nx.tableStatsPollInterval	120	—	120
nx.portStatsPollInterval	120	—	120
nx.descStatsPollInterval	120	—	120
nx.lldpPollingTimer	10	—	10
nx.portPollingTimer	20	—	20

（注） 事前定義された値は、シスコにより Cisco Nexus Data Broker とともに出荷される `config.ini` ファイルに含められているものです。このテーブルの列のエムダッシュ（「—」）は、明示的に値を更新しない限り、最小値が使用されることを意味します。

ステップ 4	ファイルを保存し、エディタを終了します。	
ステップ 5	Cisco Nexus Data Broker を再起動します。	

エッジ ポートのユーザ ロールの設定

Cisco Nexus Data Broker アプリケーション ユーザ がエッジ ポートのルールを作成するために使用できるエッジ ポートを管理するため、`config.ini` ファイルの App-User ロール設定を変更してアプリケーションユーザ向けのロールベース アクセス コントロール（RBAC）を有効にする必要があります。変更を加えて Cisco Nexus Data Broker を再起動した後、次の制限事項に注意してください。

- Cisco Nexus Data Broker App-User ロールのユーザは、リソース グループの一部となっているか、またはそのロールに割り当てられているグループの送信元ポートのみにルールを作成することができます。
- Cisco Nexus Data Broker App-Admin ロールのユーザのみが、送信元なしでルールを作成できます。

App-User ロールの RBAC を有効にするには、次の手順を実行します。

手順

ステップ 1 編集用に `config.ini` ファイルを開きます。

ステップ 2 `# Enforce restriction on edge/tap ports user can capture (default false)` の行を見つけます。

ステップ 3 次の行からコメント文字を削除します。
`monitor.strictAuthorization=true`

ステップ 4 修正内容を保存し、ファイルを閉じます。

ステップ 5 Cisco Nexus Data Broker が動作している場合は、変更を有効にするためにアプリケーションを再起動します。

Cisco Nexus Data Broker GUI へのログイン

HTTPS を使用して Cisco Nexus Data Broker にログインできます。Cisco Nexus Data Broker のデフォルト HTTPS Web リンクは `https://Nexus_Data_Broker_IP: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 用に設定する必要があります。

手順

ステップ 1 Web ブラウザで、Cisco Nexus Data Broker 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名とパスワードは admin/admin です。

b) [Log In] をクリックします。

HTTP へのコントローラのアクセス変更

Cisco Nexus Data Broker リリース 2.1 以降では、GUI および API からコントローラへの非暗号化（HTTP）アクセスはデフォルトで無効になっています。コントローラには、URL http://<host>:8080 を使用してアクセスすることはできません。

HTTP にコントローラのアクセスを変更するには、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	次の例に示すように、設定ディレクトリの tomcat-server.xml ファイルの ポート 8080 のコネクタからコメント文字を削除します。
	
	例：
	`<Service name="Catalina">`
	`<!--`
	`<Connector port="8080" protocol="HTTP/1.1"`
	`connectionTimeout="20000"`
	`redirectPort="8443" server="Cisco XNC" enableLookups="false"`
	`/>`
	`-->`
	`<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"`
	`scheme="https" secure="true"`
	`clientAuth="false" sslProtocol="TLS"`
	`keystoreFile="configuration/keystore"`
	`keystorePass="ciscoxnc" server="Cisco XNC"`
	`connectionTimeout="60000" enableLookups="false" />`
	
	例：
	次の例に示すように、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 XNC" enableLookups="false"`
	`/>`
	
	`<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"`
	`scheme="https" secure="true"`	

	コマンドまたはアクション	目的
	clientAuth="false" sslProtocol="TLS" keystoreFile="configuration/keystore" keystorePass="ciscoxnc" server="Cisco XNC" connectionTimeout="60000" enableLookups="false" />	
ステップ 2	コントローラを再起動します。	

Cisco Nexus Data Broker GUI の概要

Cisco Nexus Data Broker GUI には、次のエリアおよびペインが含まれます。

- Cisco Nexus Data Broker の情報の主なカテゴリにアクセスできるウィンドウの上部全体にわたるメニュー バー。
- ネットワークを視覚的に表示する右側のトポロジ マップ。
- 選択したカテゴリの追加のビューと情報を表示する複数のペイン。

メニュー バーには、次のものが含まれています。

- オンライン ヘルプ ボタン：現在のページのオンライン ヘルプにアクセスできます。
- [Save] ボタン：Cisco Nexus Data Broker で行う追加および変更を保存できます。

（注） 設定の変更後は、[Save] ボタンを必ずクリックする必要があります。

- [Northbound API] ボタン：Northbound API コンテンツを新しいブラウザ タブで表示し、コンテンツと呼び出しを表示できます。
- 管理（[Admin]）ドロップダウンリスト：次の異なるタスクにアクセスできます。
  - [Management]：デバイス、フロー、ユーザ、スライス、Administration、Authorization、Authentication（AAA）設定を管理するため、OSGi コンソール、クラスタ情報を表示するため、およびネットワークのトラブルシューティングを行うためのアクセスを提供します。
  - [Settings]：ユーザ ロールとリソース グループを作成し、リソース グループにデバイスを割り当てることができます。
  - [Logout]：Cisco Nexus Data Broker からユーザをログアウトします。

トポロジ ツール

トポロジのペインの左側には、トポロジ図のサイズを拡大または縮小できるズーム スライダが含まれます。また、マウス ホイールを上または下にスクロールして、トポロジ図のサイズをそれぞれ拡大または縮小できます。

トポロジ図全体、単一のトポロジ要素、またはノード グループを移動できます。図、要素、またはノード グループを移動するには、それをクリックしてドラッグします。

ノードまたはエッジポートに関する情報を表示するには、ノードまたはエッジポートのアイコンにポインタを合わせます。表示される情報は、選択したデバイスによって異なります。

パスに関する情報を表示するには、トポロジ図のパスにポインタを合わせます。

フィルタに関する情報を表示するには、[Configure Filters] タブのフィルタの [Name] にポインタを合わせます。

ペインのサイズ変更

GUI 表示で、次のようにしてペイン サイズ変更グリッパをクリックすることで、ペインのサイズを変更できます。

- 左下のペインまたは右下のペインのいずれかの高さを増加または減少するには、ペイン上部のペイン サイズ変更グリッパをクリックし、マウスを使用して上または下にドラッグします。
- 左下のペインまたは右下のペインのいずれかを折りたたむには、両端矢印が表示されるまでペイン上部のペイン サイズ変更グリッパにポインタを合わせて、マウスを 1 回クリックします。
- 折りたたんだ左下のペインまたは右下のペインのいずれかを元に戻すには、両端矢印が表示されるまでペイン下部のペイン サイズ変更グリッパにポインタを合わせて、マウスを 1 回クリックします。
- 左の 2 つのペインの幅を同時に増加または減少させるには、ペイン上部のペイン サイズ変更グリッパをクリックし、マウスで左か右にドラッグします。

コンフィギュレーションの変更の保存

Cisco Nexus Data Broker で行った設定変更を定期的に保存する必要があります。アプリケーションを停止すると、Cisco Nexus Data Broker の保存されていない設定の変更は失われます。

手順

メニュー バーで、[Save] をクリックします。

第 5 章

Cisco Nexus 9000 シリーズ スイッチの設定

この章の内容は、次のとおりです。

- 注意事項と制約事項，31 ページ
- Cisco Nexus 9000 シリーズ スイッチでの TCAM ハードウェアのサイジングの設定，32 ページ
- Cisco Nexus 9000 シリーズ スイッチ上での CLI を使用した Cisco NX-API の有効化，33 ページ
- スイッチ間ポートとポート チャネルのスイッチ ポート モードのトランクの有効化，34 ページ

注意事項と制約事項

Cisco Nexus Data Broker を使用して Cisco Nexus 9000 シリーズ スイッチを設定するには、次の注意事項と制約事項を参照してください。

- Cisco Nexus Data Broker は、リリース 7.x 以降のデバイスの Cisco Nexus 9000 シリーズ ファミリでサポートされます。
- NX-API デバイスの Edit オプションは、現在のリリースではサポートされていません。
- Cisco Nexus Data Broker によってプロビジョニングされるデバイスでは、Cisco Nexus Data Broker との関連付けが行われているときに LLDP を有効化し、LLDP 機能の無効化は行わないでください。LLDP 機能を無効にした場合、デバイスの削除および再追加を行わないと修正できない不整合が Cisco Nexus Data Broker に発生する可能性があります。
- Cisco Nexus Data Broker では、ポート定義によって設定されるデバイス 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はデフォルトで switchport trunk のデバイス設定を備えていることが想定されています。
- Cisco Nexus 9000 シリーズ デバイスは、エッジ ポート用の VLAN ID、SPAN、エッジ ポート、および TAP インターフェイスをサポートしていません。

- Cisco Nexus Data Broker に追加したデバイスを削除する場合、ポート定義および接続と関連付けられたデバイスを先に削除する必要があります。
- 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。
- Cisco Nexus 9000 シリーズ スイッチを、NX-API プロトコルによって検出できる Cisco Nexus 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 Data Broker は、TAP アグリゲーション機能と JSON-RPC 用の NX-API のサポートを使用します。
- NX-API モードで Cisco Nexus Data Broker を使用して Tap/SPAN アグリゲーション用に Cisco Nexus 9000 シリーズ スイッチを展開する前に、次の設定を完了する必要があります。
  - スイッチの **hardware access-list tcam region {ifacl | mac-ifacl} 1024 double-wide** コマンドを使用した、IPV4 ポートの ACL または MAC ポート ACL 用 TCAM 領域サイズの設定。
  - スイッチの **feature manager** CLI コマンドを使用した NX-API の有効化。
  - すべてのスイッチ間ポートおよびポート チャネルでの **switchport mode trunk** の設定。
- OpenFlow モードで Cisco Nexus Data Broker を使用して Tap/SPAN アグリゲーション用に Cisco Nexus 9000 シリーズ スイッチを展開する前に、プロンプトでコマンド **hardware access-list tcam region openflow 512** を実行します。
- Cisco Nexus Data Broker は定期的にスイッチ インベントリ、トポロジの相互接続、およびステータスを検出します。この情報は、ステータス別に GUI で更新されます。再検出の間隔は設定できます。また、再検出のデフォルト値は 10 秒おきです。

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

手順

	コマンドまたはアクション	目的
ステップ 1	**hardware access-list tcam region <region> <tcam-size>** コマンドを使用して次の TCAM リージョンを設定できます。	• 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

	コマンドまたはアクション	目的
		• Egress 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 TCAM ハードウェア サイジング設定の手順については、『*Cisco Nexus 9000 Series NX-OS Security Configuration Guide*』を参照してください。

Cisco Nexus 9000 シリーズ スイッチ上での CLI を使用した Cisco NX-API の有効化

トポロジ内で接続されている複数の 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 Data Broker のプラグインは、LLDP を使用してスイッチの相互接続を検出でき、Cisco Nexus 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は、物理リンクにすることもポートチャネル インターフェイスにすることもできます。トポロジには、Cisco Nexus Data Broker デバイス リストに追加される 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は 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。	スイッチで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 ポートを設定します。
ステップ 5	switch (config) # **nxapi https port***443*	HTTPS ポートを設定します。 Cisco Nexus 9000 シリーズ スイッチで NX-API 機能を有効化するための手順の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。

スイッチ間ポートとポート チャネルのスイッチ ポート モードのトランクの有効化

スイッチ間ポートおよびポート チャネルのスイッチ ポート モードを有効にするには、次の手順を完了します。

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

第 6 章

デバイスの管理

この章の内容は、次のとおりです。

- ノード名の追加，35 ページ
- 展開したノード情報の表示，37 ページ
- ポート リストの表示，38 ページ
- デバイスの追加，38 ページ
- デバイスの編集，39 ページ
- デバイスの削除，40 ページ
- ノード グループの追加，40 ページ
- ノード グループへのノードの追加，41 ページ
- ノード グループからのノードの削除，42 ページ
- ノード グループの削除，43 ページ
- ゲートウェイ IP アドレスの追加，43 ページ
- ゲートウェイ IP アドレスの削除，44 ページ
- ポートの追加，45 ページ

ノード名の追加

わかりやすいノード名を追加すると、トポロジ図のノードを識別するのに便利です。

（注） この手順は、OpenFlow モードだけに適用できます。

手順

ステップ 1 [Admin] ドロップダウン リストから、[Management] を選択します。

ステップ 2 メニュー バーで [Devices] を選択してから、[Nodes Learned] タブをクリックします。

ステップ 3 [Node Name] 列の名前を変更するノードのリンクをクリックします。

ステップ 4 [Update Node Information] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Node ID] フィールド	OpenFlow スイッチなど、ネットワーク要素の固有識別子。
[Node Name] フィールド	ノードに割り当てる名前。 名前には 1 ～ 256 文字の英数字を含めることができます。使用できる特殊文字は、下線「_」、ハイフン「-」、プラス「+」、等号「=」、開き括弧「(」、閉じ括弧「)」、縦棒「|」、ピリオド「.」、およびアット マーク「@」です。
[Tier] ドロップダウン リスト	ネットワーク要素の階層プロパティを割り当てます。次のいずれかになります。 • Unknown • Access • Distribution • Core
[Operation Mode] ドロップダウン リスト	トラフィックがフローに基づいて処理される方法を選択します。次のいずれかになります。 • Allow reactive forwarding：デフォルト フローはプログラミングされません。フローに一致しないトラフィックが処理される方法はスイッチの実装によって異なります。 • Proactive forwarding only：次のデフォルト フローがスイッチでプログラミングされます。 ◦アドレス解決プロトコル（ARP）パケットをパントします。 ◦Link Layer Discovery Protocol（LLDP）パケットをパントします。 ◦他のすべてのトラフィックをドロップします。

（注） Proactive forwarding only モードは、NX-API デバイスには適用できません。

ステップ 5 [Save（保存）] をクリックします。

展開したノード情報の表示

手順

ステップ 1 [Admin] ドロップダウン リストから、[Management] を選択します。

ステップ 2 メニュー バーで [Devices] を選択してから、[Nodes Learned] タブをクリックします。

ステップ 3 右上隅のアイコンをクリックします。

ステップ 4 [Nodes Learned] ダイアログボックスに、次の設定できないフィールドが表示されます。

名前	説明
[Node Name] フィールド	ノードに割り当てられた名前。
[Node ID] フィールド	ノードの ID。
[Tier Name] フィールド	ノード用に選択された階層。
[MAC Address] フィールド	ノードの MAC アドレス。
[Ports] フィールド	ノード上のアクセス可能なポート。

ステップ 5 ブラウザ ウィンドウの右上隅にある [X] をクリックしてブラウザを閉じます。

ポート リストの表示

手順

ステップ 1 [Admin] ドロップダウン リストから、[Management] を選択します。
ステップ 2 メニュー バーで [Devices] を選択してから、[Nodes Learned] タブをクリックします。
ステップ 3 ノードの [Ports] リンクをクリックします。
ステップ 4 [Ports List] ダイアログボックスに、指定したノードのすべてのポートが表示されます。
ステップ 5 ブラウザ ウィンドウの右上隅にある [X] をクリックしてブラウザを閉じます。

デバイスの追加

管理がより容易になるよう、GUI を使用して NX-API デバイスを追加できるようになりました。

手順

ステップ 1 [Admin] ドロップダウン リストから、[Management] を選択します。
ステップ 2 メニュー バーで [Devices] を選択してから、[Device Connections] タブをクリックします。
ステップ 3 [Add Device] をクリックします。
ステップ 4 [Add Device] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Address] フィールド	デバイスに割り当てられている IP アドレス。NX-API デバイスの IP アドレスに加えて、デバイスの DNS 名を使用してデバイスを追加することもできます。
[Username] フィールド	デバイスに割り当てられたユーザの名前。
[Password] フィールド	デバイスに割り当てられたユーザのパスワード。 （注） 追加後に、デバイスのユーザ名またはパスワードを編集できます。
[Connection Type] フィールド	接続方式（たとえば、onePK/NX API）。

名前	説明
[Port Type] フィールド	NX-API 接続のためのポート番号。NX-API HTTPS 接続では、ポート番号はデフォルトで 443 です。コントローラが TLS モードで動作している場合、デバイスの HTTPS のポート番号を入力します。

ステップ 5 [Add Device] をクリックします。
ノードの設定が追加されます。入力したアドレスに物理デバイスが関連付けられると、成功のメッセージが表示されます。アドレスは、[Device Connections] タブの [Devices] の [Network Element Address] リストに青色で表示されます。
入力したアドレスに関連付けられた物理デバイスがない場合、接続は行われず、接続がタイム アウトしたことを示すエラー メッセージが表示されます。アドレスは、[Device Connections] タブの [Devices] の [Network Element Address] リストでグレー表示されます。

デバイスの編集

管理がより容易になるよう、GUI を使用して NX-API デバイスを編集できるようになりました。

手順

ステップ 1 [Admin] ドロップダウン リストから、[Management] を選択します。
ステップ 2 メニュー バーで [Devices] を選択してから、[Device Connections] タブをクリックします。
ステップ 3 [Edit Device] をクリックします。
ステップ 4 [Edit Device] ダイアログボックスで、次のフィールドを編集します。

名前	説明
[Username] フィールド	デバイスに割り当てられたユーザの名前。
[Password] フィールド	デバイスに割り当てられたユーザのパスワード。 （注） 追加後に、デバイスのユーザ名またはパスワードを編集できます。
[Connection Type] フィールド	接続方式（たとえば、onePK/NX API）。

名前	説明
[Port Type] フィールド	NX-API 接続のためのポート番号。NX-API HTTPS 接続では、ポート番号はデフォルトで 443 です。コントローラが TLS モードで動作している場合、デバイスの HTTPS のポート番号を入力します。

ステップ 5 [Edit Device] をクリックします。
ノードの設定が追加されます。入力したアドレスに物理デバイスが関連付けられると、成功のメッセージが表示されます。アドレスは、[Device Connections] タブの [Devices] の [Network Element Address] リストに青色で表示されます。
入力したアドレスに関連付けられた物理デバイスがない場合、接続は行われず、接続がタイム アウトしたことを示すエラー メッセージが表示されます。アドレスは、[Device Connections] タブの [Devices] の [Network Element Address] リストでグレー表示されます。

デバイスの削除

手順

ステップ 1 [Admin] ドロップダウン リストから、[Management] を選択します。
ステップ 2 メニュー バーで [Devices] を選択してから、[Device Connections] タブをクリックします。
ステップ 3 [Devices] リストで、削除する各デバイスの横のチェックボックスをオンにします。または、最上部のチェックボックスをオンにしてすべてのデバイスを削除します。
ステップ 4 [Remove Device] をクリックします。
ステップ 5 [Remove Device] 確認ダイアログ ボックスで、[Remove Devices] をクリックします。
（注） デバイスを削除する前に、そのデバイスにインストールされているポート定義と接続が削除されたことを確認する必要があります。ポート定義と接続が削除されていない場合は、デバイスとコントローラ間の整合性がない可能性があります。

ノード グループの追加

ノード グループを使用すると、Cisco Nexus Data Broker トポロジ図内でノードを視覚的にグループ化することができます。ノード グループは、ノード間リンクを作成しません。

手順

ステップ 1 [Admin] ドロップダウン リストから、[Management] を選択します。

ステップ 2 メニュー バーで [Devices] を選択してから、[Device Groups] タブをクリックします。

ステップ 3 [Add Group] をクリックします。

ステップ 4 [Add Node Group] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Name] フィールド	ノード グループに付与する名前。 名前には 1 ～ 256 文字の英数字を含めることができます。使用できる特殊文字は、下線「_」、ハイフン「-」、プラス「+」、等号「=」、開き括弧「(」、閉じ括弧「)」、縦棒「|」、ピリオド「.」、およびアット マーク「@」です。

ステップ 5 [Add Group] をクリックします。
ノード グループのリストに、グループの名前が表示されます。

次の作業

ノード グループにノードを追加します。

ノード グループへのノードの追加

ノードをノードグループに追加すると、トポロジ図内でノードをノードグループに視覚的に関連付けることができます。ノード グループは、図内で異なる色により強調表示されます。

（注） すでにノード グループに属するノードを新しいノード グループに追加すると、そのノードは最初のノード グループから自動的に削除され、新しいノード グループに追加されます。

はじめる前に

ノード グループを追加します。

手順

ステップ 1 [Admin] ドロップダウン リストから、[Management] を選択します。

ステップ 2 メニュー バーで [Devices] を選択してから、[Device Groups] タブをクリックします。

ステップ 3 [Node Groups] リストのノードの追加先となるノード グループの名前をクリックします。

ステップ 4 次のいずれかの方法でノードをグループに追加します。

- トポロジ図で 1 つ以上のノードをクリックしてから、トポロジ図の Add to group <group name> をクリックします。

- [Nodes in Group] タブをクリックして、次の操作を実行します。

a) [Add Nodes to Group - <group name>] ダイアログボックスで、ドロップダウンリストから 1 つ以上のノードを選択します。

b) [Add to Group] をクリックします。

[Nodes in Group] タブの [Nodes in Group - <group name>] リスト、およびトポロジ図内のノード グループ内にノードが表示されます。

ノード グループからのノードの削除

はじめる前に

ノード グループにノードを追加します。

手順

ステップ 1 [Admin] ドロップダウン リストから、[Management] を選択します。

ステップ 2 メニュー バーで [Devices] を選択してから、[Device Groups] タブをクリックします。

ステップ 3 [Node Groups] リストのノードの削除元となるノード グループの名前をクリックします。

ステップ 4 グループからノードを削除するには、次のいずれかを実行します。

- トポロジ図のノード グループをクリックして次のことを行います。

a) グループから削除するノードをクリックします。

b) トポロジ図の [Remove from group – <group-name>] をクリックします。

- [Nodes in Group] タブをクリックして、次の操作を実行します。

a) リスト内の削除する単一または複数のノードの横のチェックボックスをオンにします。または、リストの最上部のチェックボックスをオンにして、すべてのノードを削除するために選択します。

b) [Remove Nodes from <group-name>] をクリックします。

ステップ 5 [Remove Nodes] 確認ダイアログ ボックスで、[Remove] をクリックします。

ノード グループの削除

ノード グループを削除すると、そのグループに追加されているノードの関連付けが解除され、そのノード グループがトポロジ図に表示されることはなくなります。

手順

ステップ 1 [Admin] ドロップダウン リストから、[Management] を選択します。

ステップ 2 メニュー バーで [Devices] を選択してから、[Device Groups] タブをクリックします。

ステップ 3 [Node Groups] リストで、削除するノードグループの名前の横のチェックボックスをオンにするか、またはすべてのノード グループを削除するために最上部のチェックボックスをオンにします。

ステップ 4 [Remove Group] をクリックします。

ステップ 5 [Remove Group] 確認ダイアログ ボックスで、[Remove Group] をクリックします。
ノード グループは削除され、トポロジ図に表示されなくなります。

ゲートウェイ IP アドレスの追加

手順

ステップ 1 [Admin] ドロップダウン リストから、[Management] を選択します。

ステップ 2 メニューバーで [Devices] を選択してから、[Subnet Gateway Configuration] タブをクリックします。

ステップ 3 [Add Gateway IP Address] をクリックします。

ステップ 4 [Add Gateway IP Address] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Name] フィールド	ゲートウェイ IP アドレスに割り当てる名前。 名前には 1 ～ 256 文字の英数字を含めることができます。使用できる特殊文字は、下線「_」、ハイフン「-」、プラス「+」、等号「=」、開き括弧「(」、閉じ括弧「)」、縦棒「|」、ピリオド「.」、およびアット マーク「@」です。

名前	説明
[Gateway IP Address/Mask] フィールド	次の形式でのデフォルト ゲートウェイの IP アドレスとサブネット マスク： *IP_Address/Subnet_Mask* （注） • 展開が OpenFlow トラフィックのみの場合、ゲートウェイ IP アドレスは、そのサブネット上のホスト システムのデフォルト ゲートウェイとして使用される IP アドレスと同じアドレスに設定できます。 • 展開に OpenFlow および非 OpenFlow トラフィックが含まれている場合、ゲートウェイ IP アドレスは、そのサブネット上で使用されていない IP アドレスに設定する必要があります。

ステップ 5 [Save（保存）] をクリックします。

ゲートウェイ IP アドレスの削除

はじめる前に

1 つ以上のゲートウェイ IP アドレスを追加します。

手順

ステップ 1 [Admin] ドロップダウン リストから、[Management] を選択します。

ステップ 2 メニュー バーで [Devices] を選択してから、[Subnet Gateway Configuration] タブをクリックします。

ステップ 3 削除する各ゲートウェイ IP アドレスの名前の横にあるチェックボックスをオンにするか、または最上部のチェックボックスをオンにしてすべてのゲートウェイ IP アドレス エントリを削除します。

ステップ 4 [Remove Gateway IP Address] をクリックします。

ステップ 5 [Remove Gateway IP Address] 確認ダイアログ ボックスで、[Remove Gateway IP Address] をクリックします。

ポートの追加

手順

ステップ 1 [Admin] ドロップダウン リストから、[Management] を選択します。

ステップ 2 メニューバーで [Devices] を選択してから、[Subnet Gateway Configuration] タブをクリックします。

ステップ 3 [Add Ports] をクリックします。

ステップ 4 [Add Ports] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Gateway Name] ドロップダウン リスト	ポートをバインドするゲートウェイ アドレスの名前。
Node ID ドロップダウン リスト	ゲートウェイ アドレスにバインドするポートを含むノード。
[Select Port] ドロップダウン リスト	ゲートウェイ アドレスにバインドするポート。

ステップ 5 [Save（保存）] をクリックします。

第 7 章

ポートおよびデバイスの設定

この章の内容は、次のとおりです。

- Cisco Nexus Data Broker のポート タイプについて，47 ページ
- ポート タイプの設定，49 ページ
- 複数のポートの設定，50 ページ
- ポート タイプ設定の削除，50 ページ
- モニタリング デバイスの設定，51 ページ
- モニタリング デバイスの削除，52 ページ
- ルート ノードの設定，53 ページ
- Cisco onePK Agent，53 ページ
- 対称型ロード バランシング，54 ページ
- MPLS タグ除去の有効化，55 ページ
- Q-in-Q の設定，56 ページ
- パケット切り捨ての設定，56 ページ
- タイムスタンプのタギングの設定，57 ページ

Cisco Nexus Data Broker のポート タイプについて

Cisco Nexus Data Broker では、異なるポート タイプを設定できます。すべての設定済みポートは [Port Types] タブの [Configured Ports] テーブルに表示されます。

トラフィックの集約およびリダイレクトが容易になるように、ポートを入力 TAP/SPAN ポートまたはモニタリング ツール ポートに設定することができます。

（注） ソフトウェア バージョンが 7.x よりも前の場合、TAP の集約は NX-OS の現在のバージョンではサポートされていないことを示すエラー メッセージが表示されるため、指定のリリース以降にアップグレードする必要があります。7.0 ソフトウェア バージョンの詳細は NX-API だけに適用されます。

ポートを選択し、そのポートが入力の送信元ポートか、または出力のリダイレクト ポートかを定義できます。Cisco Nexus Data Broker の入力送信元ポートは、エッジ SPAN またはエッジ Tap ポートにマッピングされ、出力のリダイレクト ポートは、モニタリング ツール ポートにマッピングされます。この選択に対してスイッチ相互接続ポートは表示されません。

（注） ポート名のカラー コーディングは、ポート自体のステータスを示します。緑はポートがアップしていることを、オレンジはポートがダウンしていることを、赤は管理者によってダウンに設定されていることを意味します。

Edge Port

エッジ ポートは、トラフィックが監視ネットワークに入っていく入力ポートです。Cisco Nexus Data Broker は、次のエッジ ポートをサポートします。

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

エッジ ポートの設定はオプションです。

（注） Any-to-Multipoint（A2MP）転送パス オプションの場合、Cisco Nexus Data Broker は入力エッジ ポートまたは送信元ポートとして設定済みのエッジ ポートのみを使用します。

Delivery Port

配信ポートはトラフィックがモニタ ネットワークを出る出力ポートです。これらの発信ポートは外部モニタリング デバイスに接続されます。Cisco Nexus Data Broker でモニタリング デバイスを設定するとき、モニタリング デバイスに名前とアイコンを関連付けることができます。

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

VLAN タギング

Cisco Nexus Data Broker を使用すると、スイッチ ポートをエッジ ポートとして設定し、VLAN をそのポートに設定することができます。VLAN ID を設定し、Cisco onePK エージェントへの接続

がアップになっている場合、Cisco Nexus Data Broker は、Cisco Nexus 3000 シリーズ スイッチ、3100 シリーズ スイッチ、および Cisco Nexus 9000 シリーズ スイッチをプログラムし、そのポートで受信されるすべてのパケットに VLAN タギングを適用し、VLAN ID がエッジ ポートに設定されているものになるようにします。そのポートで受信されたパケットですでに VLAN タギングが適用されたフレームは、二重にタギングが適用され、一番外側の VLAN タグに、設定されたエッジ ポートと関連付けられている VLAN ID が含まれます。

（注） NX-API モードでの VLAN タギングがサポートされるようになり、これは、Cisco Nexus Data Broker UI から有効化できます。

ポート タイプの設定

手順

ステップ 1 トポロジ図で、ポートを設定するノードをクリックします。
サイド バーの [Ports] 領域には、ノード用の設定に利用できるポートのリストが表示されます。

ステップ 2 ノードのポートのリストで、設定するポートのポート ID の下の [Click to configure] をクリックします。

ステップ 3 [Select a port type] ドロップダウン リストから、次のいずれかを選択します。

- Add Monitoring Device
- Edge Port-SPAN
- Edge Port-TAP
- Production Port

[Monitoring Device]：トラフィックのキャプチャおよび対応する配信ポートの設定のためのモニタリング デバイスを作成します。

[Edge Port-SPAN]：宛先として設定されたアップストリームスイッチに接続された着信トラフィックのエッジ ポートを作成します。

[Edge Port-TAP]：物理タップのポートに接続された着信トラフィックのエッジ ポートを作成します。

[Production Port]：入力および出力トラフィックの実稼働ポートを作成します。

ステップ 4 （任意） [Port Description] フィールドに、ポートの説明を入力します。
ポートの説明には 1 ～ 256 文字の英数字を含めることができます。使用できる特殊文字は、下線「_」、ハイフン「-」、プラス「+」、等号「=」、開き括弧「(」、閉じ括弧「)」、縦棒「|」、ピリオド「.」、およびアット マーク「@」です。

ステップ 5 VLAN ID を入力します。

ポートはdot1qとして設定され、実稼働のVLAN情報を維持するように設定されています。VLAN ID は、トラフィックの送信元ポートを特定するために使用します。

ステップ 6 [Enable Packet Truncation] フィールドで、パケットの長さを入力します。

ステップ 7 [Submit] をクリックします。

複数のポートの設定

複数のポートまたはポートの範囲をポート定義用に設定できるようになりました。

手順

ステップ 1 GUI のサイド バーの [Configure Multiple Ports] をクリックします。

ステップ 2 [Select Ports] ドロップダウンリスト フィールドで、割り当てるポートを選択します。ctrl または shift を使用して、リダイレクション用に割り当てる複数のポートを選択できます。

ステップ 3 [Select Port Type] ドロップダウンリスト フィールドで、割り当てるポート タイプを選択します。

- Edge port-SPAN
- Edge port-TAP
- Production Port

ステップ 4 [Submit] をクリックします。

ポート タイプ設定の削除

はじめる前に

- 最低でも 1 つのポート タイプを設定する必要があります。
- 削除するポート タイプの設定はルールに使用しないでください。使用している場合、ルールの変更または削除のいずれかを行わないと、ポート タイプの設定を削除できません。

（注） 設定されたポートが SPAN またはエッジ ポートであり、これらのポートに基づく接続が作成されている場合、これらの接続を削除することはできません。接続の削除後にのみ、SPAN/エッジ ポートのポート定義を削除することができます。

手順

ステップ 1 [Port Types] タブから、次のいずれかを選択します。

- 削除するすべての [Configured Ports] を選択するには、最上部のチェックボックス。
- 単一または複数の設定済みポートのみを削除する場合は、その名前の横のチェックボックス。

ステップ 2 [Configured Ports] のリストの上で、[Remove Port Configuration] をクリックします。

ステップ 3 [Remove Port Configuration] 確認ダイアログ ボックスで、[Remove Port Configuration] をクリックします。
ポート設定が削除されます。

モニタリング デバイスの設定

手順

ステップ 1 トポロジ図で、モニタリング デバイスを設定するノードをクリックします。
[Port Types] タブには、ノード用の設定に利用できるポートのリストが表示されます。

ステップ 2 ノードのポートのリストで、設定するポートのポート ID の下の [Click to configure] をクリックします。

ステップ 3 [Select a port type] ドロップダウンリストから、[Add Monitoring Device] をクリックします。

ステップ 4 [Add Device] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Device Name] フィールド	モニタリング デバイスに使用する名前。 名前には 1 ～ 256 文字の英数字を含めることができます。使用できる特殊文字は、下線「_」、ハイフン「-」、プラス「+」、等号「=」、開き括弧「(」、閉じ括弧「)」、縦棒「|」、ピリオド「.」、およびアット マーク「@」です。 （注） モニタリング デバイスの追加後に、デバイス名は変更できます。

名前	説明
[Icons] の選択	アイコンの選択です。最初のものはデフォルトで選択されています。モニタリングデバイスに使用するアイコンを選択します。 （注） 追加後に、モニタリング デバイスのアイコンは変更できます。

ステップ 5 [Submit] をクリックします。

モニタリング デバイスの削除

（注） モニタ デバイスが接続の一部である場合、Cisco Nexus Data Broker は、ユーザがモニタ デバイスを削除することを許可しません。

はじめる前に

- ポートに対して少なくとも 1 つのモニタのデバイスを設定する必要があります。
- 削除するモニタリングデバイスはルールに使用しないでください。使用している場合、ルールの変更または削除のいずれかを行わないと、モニタリング デバイスを削除できません。

手順

ステップ 1 [Devices] タブをクリックします。

ステップ 2 [Device Name] リストで、次のいずれかを選択します。

- 削除するすべてのモニタリング デバイスを選択するには、最上部のチェックボックス。
- 単一または複数のモニタリングデバイスのみを削除するには、名前の横にあるチェックボックス。

ステップ 3 [Device Name] リストの上の [Remove Monitoring Devices] をクリックします。

ステップ 4 [Remove Monitoring Devices] 確認ダイアログ ボックスで、[Remove Devices] をクリックします。

ルート ノードの設定

ルート ノードは、Cisco Nexus Data Brokerによって自動的に選択されます。定義されたルート ノードが送信元スイッチと距離が離れすぎている場合は、手動で別のスイッチを設定できます。新しいルート ノードとしてエッジ ポートのあるスイッチを選択することを推奨します。

（注） ルート ノードの変更は、設定を保存するまで有効になりません。

手順

ステップ 1 [Root] タブから、[Configure Root Node] をクリックします。

ステップ 2 [Configure Root Node] ダイアログボックスで、ドロップダウン リストからノードを選択します。

ステップ 3 [Configure Root Node] をクリックします。
[Root] タブに [Configured Root Node] 表示され、[Current Root Node] が表示されます（存在する場合）。

ステップ 4 メニュー バーで [Save] をクリックします。
ルート ノードの追加や変更が保存されます。

Cisco onePK Agent

Cisco Nexus Data Broker 用の Cisco OnePK プラグインは、デバイス上の onePK エージェントを介して onePK デバイスと通信します。Cisco Nexus Data Broker で onePK デバイスの機能をサポートするには、アプリケーションが onePK エージェントに接続している必要があります。エージェントは、Cisco Nexus Data Broker と、Cisco Nexus Data Broker で設定され、onePK が有効化されたデバイスの間のメディエータとなります。

Cisco Nexus Data Broker の onePK が有効化されたデバイス間で通信をセキュリティ保護するには、Cisco Nexus Data Broker で Transport Layer Security（TLS）を設定する必要があります。詳細については、『*Cisco Nexus Data Broker* 構成ガイド』を参照してください。

onePK エージェントへの接続

対称型ロード バランシング、Q-in-Q、タギング、およびパケットの切り捨てなどの Cisco Nexus Data Broker の追加の機能をサポートするには、onePK エージェントに接続する必要があります。

手順

ステップ 1 [Admin] ドロップダウン リストから、[Management] を選択します。
ステップ 2 メニュー バーで [Devices] を選択してから、[Device Connections] タブをクリックします。
ステップ 3 [Add Device] をクリックします。
ステップ 4 [Add Device] ダイアログ ボックスで、[Connection Type] フィールドを onePK として選択します。
ステップ 5 [Add Device] をクリックします。

対称型ロード バランシング

Cisco Nexus Data Broker を使用すると、出力ポート チャネルに対称型ロード バランシングを設定できます。ロード バランシング設定はレイヤ 2 送信元 MAC アドレスと宛先 IP アドレス、またはレイヤ 2、レイヤ 3、またはレイヤ 4 送信元ポートおよび宛先ポートを使用します。スイッチのすべてのポート チャネル インターフェイスに対称型ロード バランシングを設定すると、特定の送信元および宛先の両方の方向のすべてのトラフィックが常に同一ポート チャネルのメンバー リンク上に流れます。

（注） Cisco Nexus Data Broker の対称型ロード バランシングは、Cisco Nexus 3100 シリーズ スイッチおよび Cisco 9000 シリーズ スイッチで利用可能です。

対称型ロード バランシングの設定

はじめる前に

- スイッチの TLS を設定およびプロビジョニングします。
- NX-API または onePK 接続を使用して Cisco Nexus Data Broker にデバイスを追加します。

手順

ステップ 1 トポロジ図で、対称型ロード バランシングを設定するノードをクリックします。
ステップ 2 サイド バーの [Symmetric Load Balancing] ドロップダウンリストから、次のいずれかを選択します。

- SOURCE_DESTINATION_IP：送信元と宛先の IP アドレス（レイヤ 2 を含む）
- [SOURCE_DESTINATION_IP_ONLY]：送信元と宛先の IP アドレスのみ

- [SOURCE_DESTINATION_PORT]：送信元と宛先の TCP/UDP ポート（レイヤ 2 およびレイヤ 3 を含む）
- [SOURCE_DESTINATION_PORT_ONLY]：送信元と宛先 TCP/UDP ポートのみ

ステップ 3 [Submit] をクリックします。

MPLS タグ除去の有効化

Cisco Nexus Data Broker GUI および REST API インターフェイスから、コンフィギュレーションモードとして NX-API を使用し、Cisco Nexus 3000 シリーズおよび Cisco Nexus 9000 シリーズ スイッチで MPLS タグの除去を有効化できるようになりました。

MPLS タグ除去の設定

はじめる前に

NX-API または onePK 接続を使用して Cisco Nexus Data Broker にデバイスを追加します。

手順

ステップ 1 トポロジ図で、MPLS タグ除去を設定するノードをクリックします。

ステップ 2 サイドバーの [MPLS Strip Configuration] ドロップダウンリストから、次のいずれかを選択します。

- Enable MPLS Strip。
- Disable MPLS Strip。

ステップ 3 サイドバーの [Label Age] フィールドから、MPLS 除去のラベル期間経過の値を入力します。MPLS 除去のラベル期間経過の設定は、61 ～ 31622400 です。

ステップ 4 [Submit] をクリックします。

Q-in-Q の設定

（注） Q-in-Q を設定する機能は、Cisco Nexus 3000 および 3100 シリーズ スイッチおよび NX-API モードの Nexus 9000 スイッチで利用できます。エッジ ポートに VLAN ID が設定されており、VLAN ID がそのエッジ ポートで維持されている場合、Q-in-Q は自動的に有効になります。

手順

ステップ 1 トポロジ図で、Q-in-Q を設定するノードをクリックします。

ステップ 2 サイド バーでエッジ ポートを設定し、エッジ ポートの VLAN ID を設定します。

ステップ 3 [Enable QinQ] をクリックします。

ステップ 4 [Connect to onePK Agent] ダイアログ ボックスで、次のフィールドに入力します。

名前	説明
[Address] フィールド	Cisco OnePK デバイスに割り当てられた IP アドレス。
[Username] フィールド	デバイスに割り当てるユーザのユーザ名。
[Password] フィールド	デバイスに割り当てるユーザのパスワード。

ステップ 5 [Submit] をクリックします。

パケット切り捨ての設定

（注） パケット切り捨ては、Cisco Nexus 3500 シリーズ スイッチ でのみ設定できます。

はじめる前に

- onePK デバイスを設定します。
- onePK エージェントに接続します。

手順

ステップ 1 トポロジ図で、パケット切り捨てを設定するノードをクリックします。

ステップ 2 サイド バーで、パケット切り捨てを設定するポートをクリックします。

ステップ 3 [Select a port type] ドロップダウン リストから、次のいずれかを選択します。

- Edge Port-SPAN
- Edge Port-TAP

ステップ 4 （任意） [Port Description] フィールドに、ポートの説明を入力します。
ポートの説明には 1 ～ 256 文字の英数字を含めることができます。使用できる特殊文字は、下線「_」、ハイフン「-」、プラス「+」、等号「=」、開き括弧「(」、閉じ括弧「)」、縦棒「|」、ピリオド「.」、およびアット マーク「@」です。

ステップ 5 （任意） VLAN ID を入力します。
ポートは dot1q として設定され、実稼働の VLAN 情報を維持するように設定されています。

ステップ 6 [Enable Packet Truncation] フィールドに、切り捨てられるパケット長をバイト単位で入力します。
（注） 64 バイト以上の 4 の倍数を入力することが推奨されています。

ステップ 7 [Submit] をクリックします。
ポート設定が保存されます。また、ポート名に加えて、ラベル TRUNC=<bytes> に切り捨てられたパケットのバイト数が表示されます。

タイムスタンプのタギングの設定

Cisco Nexus 3500 プラットフォーム スイッチを使用すると、次のことができます。

- 入力でユーザ定義のしきい値を超えた部分のパケットを切り捨てます。
- ナノ秒単位の正確さの Precision Time Protocol（PTP）を使用して、パケットにタイムスタンプを付与します。

PTP を使用すると、IEEE 1588 パケットに対して、ハードウェア内のパーサー レベルでイベント メッセージの到達時間を記録するために入力ポートでタイムスタンプが付与されます。タイムスタンプはパケットの最初のビットを指します（開始フレーム デリミタ [SFD] の後）。次に、パケットは、タイムスタンプと宛先ポート番号を付与されて CPU にコピーされます。次に、パケットは PTP スタックを通過します。Cisco Nexus 3548 シリーズ スイッチの高度な PTP クロック アルゴリズムは、あらゆるタイミングおよび周波数の情報を追跡し、正確な時間を保証できるように必要な調整を行います。

最後に、パケットは内部的に高プライオリティのパケットとしてマークされ、スイッチの優先出力が確実になり、出力ポートから送信されます。送信されたパケットに対応するタイムスタンプは先入れ先出し（FIFO）方式による伝送のタイムスタンプから利用できます。

タイムスタンプ タギング機能は、Cisco Nexus 3500 シリーズ スイッチにパケットが到達したときに正確な時間情報を提供し、デバイスをリモートで監視し、実際の時間を追跡できるようにします。タイムスタンプ タギング機能により、**ttag** コマンドが出力インターフェイスで設定されます。

ether-type <type> オプションにより、イーサネット フレームの Ethertype フィールドが設定されます。Ethertype は、どのプロトコルがペイロードでカプセル化されるのかを示すために使用されます。Ethertype 1（タイプ 0x88B5）は、この目的のために使用されます。

（注） タイムスタンプ タギングは、Cisco Nexus 3500 シリーズ スイッチ でのみ設定できます。

はじめる前に

- ノードの配信デバイスを設定します。
- onePK デバイスを設定します。

手順

ステップ 1 トポロジ図で、タイムスタンプ タギングを設定するノードをクリックします。

ステップ 2 サイド バーで、配信デバイスを設定します。

ステップ 3 サイド バーで、[Click to enable additional functionality] をクリックします。

ステップ 4 [Connect to onePK Agent] ダイアログ ボックスで、次のフィールドに入力します。

名前	説明
[Address] フィールド	Cisco OnePK デバイスに割り当てられた IP アドレス。
[Username] フィールド	デバイスに割り当てるユーザのユーザ名。
[Password] フィールド	デバイスに割り当てるユーザのパスワード。

ステップ 5 [Enable Timestamp Tagging] の横のチェック ボックスをオンにします。

ステップ 6 [Submit] をクリックします。
ポートは、[TS-Tag] ラベルが付いた状態で、[Port] リストに表示されます。

第 8 章

フローのフィルタリング

この章の内容は、次のとおりです。

- Cisco Nexus Data Broker ネットワークについて，59 ページ
- 転送パス オプションについて，60 ページ
- フィルタおよび接続について，60 ページ
- リダイレクションとサービス ノードについて，61 ページ
- フィルタの追加，62 ページ
- フィルタの編集，69 ページ
- フィルタの削除，75 ページ
- 接続の追加，76 ページ
- 接続の変更，79 ページ
- 接続の複製，81 ページ
- 接続の削除，83 ページ
- サービス ノードの追加，84 ページ
- リダイレクションの追加，84 ページ
- リダイレクションの変更，88 ページ
- リダイレクションの削除，91 ページ

Cisco Nexus Data Broker ネットワークについて

Cisco Nexus Data Broker ネットワークは、1 つ以上の Cisco Nexus 3000、3100、または 3500 シリーズ スイッチと、OpenFlow 用 Cisco プラグイン および実稼働ネットワーク インフラストラクチャの複数の SPAN が適用されたポートおよびネットワーク タップを接続するための専用の NX-API を備えた Cisco Nexus 9000 シリーズ スイッチで構成されます。Cisco Nexus Data Broker は、OpenFlow

プロトコルを使用してスイッチをプログラムします。Cisco Nexus Data Broker は、ネットワークを移動するパケットをフィルタリングし、接続されたモニタリング デバイスのプールにそれらを配信します。

転送パス オプションについて

Cisco Nexus Data Broker は、次の転送パス オプションをサポートしています。

- Multipoint-to-Multipoint：With the Multipoint-to-Multipoint（MP2MP）転送パス オプションを使用すると、入力エッジ ポート（SPAN または TAP トラフィックがモニター ネットワークに入ってくる）および出力配信ポートが定義されます。Cisco Nexus Data Broker はその配信ポートを使用して、これらの入力ポートから 1 つ以上のデバイスにトラフィックを送信しています。
- Any-to-Multipoint：Any-to-Multipoint（A2MP）転送パス オプションを使用すると、モニター ネットワークの入力エッジ ポートは認識されませんが、出力配信ポートは定義されます。Cisco Nexus Data Broker は、Single Source Shortest Path（SSSP）アルゴリズムを使用して、ルート ノードからその他すべてのノードへのループのない転送パスを自動的に計算します。

フィルタおよび接続について

Filters

Cisco Nexus Data Broker では、トラフィックをフィルタリングするために使用される HTTP トラフィックの条件のレイヤ 2（L2）、レイヤ 3（L3）、レイヤ 4（L4）、およびレイヤ 7（L7）フィルタリングを定義するためにフィルタを使用できます。フィルタで基準に一致するトラフィックは配信ポートに、さらにそこから接続されたモニタ デバイスへとルーティングされます。

Connections

接続を使用して、設定されたモニタ デバイスにフィルタを関連付けることができます。ソースの有無にかかわらず接続を設定できます。送信元ノードとポートのある接続ではMultipoint-to-Multipoint 転送パス オプションを使用します。ノードに送信元ポートがない接続はループフリーの Any-to-Multipoint 転送パス オプションを使用します。

Deny オプションを使用してルールが設定されている場合、入力エッジポートは定義されている場合もされていない場合もあります。Cisco Nexus Data Broker は、指定された入力エッジ ポートで、または入力エッジ ポートが定義されていない場合はすべてのノードでトラフィックを破棄します。

ルールごとに設定できるプライオリティがあります。高いプライオリティの接続は低いプライオリティの接続よりも優先されます。

接続は、インストールしなくても作成および保存できます。接続の保存後、インストールはCisco Nexus Data Broker GUI でオン/オフを切り替えることができます。

（注） Cisco Nexus Data Broker の切り替え機能を使用した接続のインストールまたはアンインストール後、120 秒間はデバイスを再起動しないでください。そうしないと、Cisco Nexus Data Broker によって設定されたパラメータが保存されず、Cisco Nexus Data Broker とデバイス間に不一致が生じる可能性があります。

デフォルト フィルタ

Cisco Nexus Data Broker には、デフォルト フィルタがすべてのトラフィックに一致する状態でプリインストールされています。デフォルト フィルタは All Ethertype を使用して一致の選択内容として作成されます。デフォルト フィルタの名前は、default-match-all です。Cisco Nexus Data Broker を最初から使用開始するとき、このフィルタはすぐに使用できます。

リダイレクションとサービス ノードについて

Cisco Nexus Data Broker を有効化した Cisco Nexus 3000 または Cisco Nexus 9300 スイッチのインライン リダイレクションを介して、ファイアウォールまたはスイッチから一部のトラフィックをサービス ノード（SourceFire IPS など）にリダイレクトできるようになりました。トラフィックは、実稼働の入力ポートからタップアグリゲーションスイッチを介して、サービスの入力および出力ポート経由でサービス ノードへとリダイレクトされます。最後に、トラフィックはサービス ノードから実稼働の出力ポートにリダイレクトされます。

サービス ノードを使用したリダイレクションの設定

Cisco Nexus 3000 および Cisco Nexus 9000 シリーズ スイッチの 2 つのポート間のトラフィックを複製できるようになりました。一方のポートは送信元ポートであり、もう一方のポートは宛先ポートです。この設定により、インターフェイス間のトラフィックをすばやくコピーすることができます。

また、サービス ノード（QRadar など）へのトラフィックをコピーし、スイッチにリダイレクトされたトラフィックとそのトラフィックを比較することもできます。トラフィックは、リダイレクトされるため、外部のモニタリング ツールへのトラフィックをコピーすることができます。リダイレクションのルールの一部として、リダイレクトされるトラフィックのコピー先となる宛先ポートを指定できます。トラフィックのコピーはすべてのサービス ノードの出力ポート（スイッチに入っていくトラフィック）から送信されます。トラフィックのコピー先となるポートは、物理ポートにすることも、論理的なポート チャネルにすることもできます。OpenFlow を使用しており、Ethertype 値のために * をサポートする機能を実装できます。

入力および出力の実稼働ポート間には、常に 1:1 のマッピングが存在します。スイッチは、リンク間の直接接続ではなく、実稼働ポートとサービス ポートの間に存在するため、入力ポートまたは出力ポートのいずれかが運用上ダウンした場合は、ポートをシャットダウンすることが重要です。入力ポートがダウンした場合、出力ポートは自動的にシャットダウンされます。出力ポートがダウンした場合、入力ポートは自動的にシャットダウンします。

サービス ノードに接続する入力ポートまたは出力ポートがダウンすると、そのサービス ノードは自動的にバイパスされます。そのサービス ノードに関連付けられたすべてのリダイレクションは、サービス ノードをバイパスするように更新されます。

トラフィックがサービス ノードによって処理されない場合、バックアップ フローがあり、実稼働の入力ポートに再度送信されます。

また、入力ポートを選択することで、およびノードの詳細を更新することで、サービス ノードの詳細を編集できます。[Edit] をクリックして詳細を編集します。サービス ノードを削除するには、サイド バーの [Service Nodes] 表示領域で [Remove Service Node] をクリックします。

（注） リダイレクションごとに最大 4 つのサービス ノードがサポートされます。

フィルタの追加

手順

ステップ 1 [Filters] タブで、[Add Filter] をクリックします。

ステップ 2 [Add Filter] ダイアログボックスの [Filter Description] セクションで、次のフィールドを入力します。

名前	説明
[Name] フィールド	フィルタの名前。名前には 1 ～ 256 文字の英数字を含めることができます。使用できる特殊文字は、下線「_」、ハイフン「-」、プラス「+」、等号「=」、開き括弧「(」、閉じ括弧「)」、縦棒「|」、ピリオド「.」、およびアット マーク「@」です。 （注） 名前を保存すると、それを変更することはできません。
[Bidirectional] チェックボックス	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 アドレスから送信元 IP、送信元ポート、または送信元 MAC アドレスへのトラフィック情報を取得する場合は、このボックスをオンにします。

ステップ 3 [Add Filter] ダイアログボックスの [Layer 2] セクションで、次のフィールドを入力します。

[Ethernet Type] フィールド	必須です。レイヤ2トラフィックのイーサネット タイプ。表示されるデフォルト値は IPv4 です。または、次のいずれかを選択可能できます。 • IPv6 • ARP • LLDP • Predefined EtherTypes • All EtherTypes • Enter Ethernet Type：[Enter Ethernet Type] をタイプとして選択した場合、イーサネットのタイプを 16 進数形式で入力します。[Predefined EtherTypes] を選択した場合は、config.in ファイルに含まれている、事前定義されたすべてのイーサネット タイプがルールと関連付けられるため、その他のパラメータは設定しないでください。 （注） フィルタごとに、複数のユーザ定義のイーサネット タイプを設定できるようになりました。これにより、異なるトラフィック タイプに単一のフィルタを設定できるように、「,」で区切られた任意の数のイーサネット タイプを適用できます。
[VLAN Identification Number] フィールド	レイヤ 2 トラフィックの VLAN ID。単一の VLAN ID、VLAN ID の範囲の値、またはコンマ区切りの VLAN ID 値、および VLAN ID の範囲（たとえば、1-4,6,8,9-12）を入力できます。 （注） NX-API の場合、レイヤ 3 アドレスを持つ VLAN ID はサポートされません。レイヤ 3 アドレスを持つ VLAN IDを設定すると、整合性のないフローが発生します。フローのトラブルシューティングおよび修正を行う必要があります。
[VLAN Priority] フィールド	レイヤ 2 トラフィックの VLAN のプライオリティ。

[Source MAC Address] フィールド	レイヤ2トラフィックの送信元MACアドレス。
[Destination MAC Address] フィールド	レイヤ 2 トラフィックの宛先 MAC アドレス。

ステップ 4 [Add Filter] ダイアログボックスの [Layer 3] セクションで、次のフィールドを入力します。

名前	説明
[Source IP Address] フィールド	レイヤ 3 トラフィックの送信元 IP アドレス。次のいずれかになります。 • ホスト IP アドレス（たとえば、10.10.10.10） • 不連続の送信元 IP アドレス（たとえば、10.10.10.10、10.10.10.11、10.10.10.12） • IPv4 アドレス範囲（たとえば、10.10.10.10-10.10.10.15） • IPv4 サブネット（たとえば、10.1.1.0/24） • IPv6形式のホストIPアドレス（たとえば、2001::0） （注） • [Source IP Address] フィールドにIPv6 アドレスの範囲を入力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と、レイヤ 4 送信元または宛先ポートの範囲を設定できません。 • レイヤ 3 送信元 IP アドレスの範囲を設定すると、レイヤ2VLAN ID の範囲は設定できません。

名前	説明
[Destination IP Address] フィールド	レイヤ 3 トラフィックの宛先 IP アドレス。次のいずれかになります。 • ホスト IP アドレス（たとえば、10.10.10.11） • IPv4 アドレス範囲（たとえば、10.10.10.11-10.10.10.18） • IPv4 サブネット（たとえば、10.1.1.0/24） • IPv6 形式のホスト IP アドレス（たとえば、2001::4） • サブネット（たとえば、10.0.0.0/25） （注） • [Destination IP Address] フィールドに IPv6 アドレスの範囲を入力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と、レイヤ 4 送信元または宛先ポートの範囲を設定できません。 • レイヤ 3 送信元 IP アドレスの範囲を設定すると、レイヤ 2 VLAN ID の範囲は設定できません。
[Protocol] ドロップダウン リスト	レイヤ 3 トラフィックのインターネットプロトコルを選択します。次のいずれかになります。 • ICMP • TCP • UDP • Enter Protocol タイプとして [Enter Protocol] を選択した場合は、10 進数、16 進数、または 8 進数形式の IP プロトコル番号を入力します。
[ToS Bits] フィールド	レイヤ 3 IP ヘッダー内の Type of Service（ToS）ビット。Differentiated Services Code Point（DSCP）値だけが使用されます。

ステップ 5 [Add Filter] ダイアログボックスの [Layer 4] セクションで、次のフィールドを入力します。

名前	説明
[Source Port] ドロップダウン リスト	レイヤ 4 トラフィックの送信元ポートを選択します。次のいずれかになります。 • FTP (Data) • FTP (Control) • SSH • TELNET • HTTP • HTTPS • Enter Source Port [Enter Source Port] を選択した場合は、単一のポート番号か、または送信元ポート番号の範囲のいずれかを入力します。 （注） • レイヤ 4 送信元ポートの範囲を設定すると、レイヤ 3 IP 送信元または宛先ポートの範囲を設定できません。 • レイヤ 4 送信元ポートの範囲を設定すると、レイヤ 2 VLAN ID の範囲は設定できません。

名前	説明
[Destination Port] ドロップダウン リスト	レイヤ 4 トラフィックの宛先ポートを選択します。次のいずれかになります。 • FTP (Data) • FTP (Control) • SSH • TELNET • HTTP • HTTPS • Enter Destination Port [Enter Destination Port] を選択した場合は、単一のポート番号か、または宛先ポート番号の範囲のいずれかを入力します。 （注） • レイヤ 4 宛先ポートの範囲を設定すると、レイヤ 3 IP 送信元または宛先ポートの範囲を設定できません。 • レイヤ 4 宛先ポートの範囲を設定すると、レイヤ 2 VLAN ID の範囲は設定できません。

ステップ 6 [Add Filter] ダイアログボックスの [Layer 7] セクションで、次のフィールドを入力します。

名前	説明
[HTTP Method] フィールド	HTTP メソッドの一致を設定し、そのメソッドに基づいてトラフィックをリダイレクトできます。単一フィルタ内での一致のための 1 つ以上のメソッドを選択します。このオプションは、宛先ポートが HTTP または HTTPS のときにのみ使用できます。 • Connect • Delete • get • Head • Post • Put • Trace （注） レイヤ 7 の一致は、NX-API モードを使用している場合のみでサポートされており、OpenFlow ではサポートされていません。 （注） TCP のオプションの長さはレイヤ 7 トラフィックのメソッドのいずれかを選択すると有効になります。
[TCP Option Length] フィールド	フィルタ設定を拡張して、テキストボックスに TCP オプションの長さを指定することができます。テキストボックスのデフォルト値は 0 です。フィルタ内のすべてのメソッドが同一のオプションの長さを備えています。 10 進形式で TCP オプションの長さを入力します。 （注） テキストボックスの値は、4 の倍数になっている必要があり、0 ～ 40 の範囲にすることができます。

ステップ 7 [Add Filter] をクリックします。

フィルタの編集

手順

ステップ 1 [Configure Filters] タブで、編集するフィルタの [Name] の横にある [Edit] をクリックします。

ステップ 2 [Edit Filter] ダイアログボックスで、次のフィールドを編集します。

名前	説明
[Name] フィールド	フィルタの名前。名前には 1 ～ 256 文字の英数字を含めることができます。使用できる特殊文字は、下線「_」、ハイフン「-」、プラス「+」、等号「=」、開き括弧「(」、閉じ括弧「)」、縦棒「|」、ピリオド「.」、およびアットマーク「@」です。 （注） 名前を保存すると、それを変更することはできません。
[Bidirectional] チェックボックス	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 アドレスから送信元 IP、送信元ポート、または送信元 MAC アドレスへのトラフィック情報を取得する場合は、このボックスをオンにします。

ステップ 3 [Edit Filter] ダイアログボックスの [Layer 2] セクションで、次のフィールドを入力します。

[Ethernet Type] フィールド	必須です。レイヤ 2 トラフィックのイーサネット タイプ。表示されるデフォルト値は IPv4 です。または、次のいずれかを選択できます。 • IPv6 • ARP • LLDP • Predefined EtherTypes • All EtherTypes • Enter Ethernet Type：[Enter Ethernet Type] をタイプとして選択した場合、イーサネットのタイプを 16 進数形式で入力します。[Predefined EtherTypes] を選択した場合は、config.in ファイルに含まれている、事前定義されたすべてのイーサネット タイプがルールと関連付けられるため、その他のパラメータは設定しないでください。 （注） フィルタごとに、複数のユーザ定義のイーサネット タイプを設定できるようになりました。これにより、異なるトラフィック タイプに単一のフィルタを設定できるように、「,」で区切られた任意の数のイーサネット タイプを適用できます。
[VLAN Identification Number] フィールド	レイヤ 2 トラフィックの VLAN ID。単一の VLAN ID、VLAN ID の範囲の値、またはコンマ区切りの VLAN ID 値、および VLAN ID の範囲（たとえば、1-4,6,8,9-12）を入力できます。 （注） NX-API の場合、レイヤ 3 アドレスを持つ VLAN ID はサポートされません。レイヤ 3 アドレスを持つ VLAN IDを設定すると、整合性のないフローが発生します。フローのトラブルシューティングおよび修正を行う必要があります。
[VLAN Priority] フィールド	レイヤ 2 トラフィックの VLAN のプライオリティ。
[Source MAC Address] フィールド	レイヤ2トラフィックの送信元MACアドレス。

[Destination MAC Address] フィールド	レイヤ 2 トラフィックの宛先 MAC アドレス。

ステップ 4 [Edit Filter] ダイアログボックスの [Layer 3] セクションで、次のフィールドを入力します。

名前	説明
[Source IP Address] フィールド	レイヤ 3 トラフィックの送信元 IP アドレス。次のいずれかになります。 • ホスト IP アドレス（たとえば、10.10.10.10） • 不連続の送信元 IP アドレス（たとえば、10.10.10.10、10.10.10.11、10.10.10.12） • IPv4 アドレス範囲（たとえば、10.10.10.10-10.10.10.15） • IPv4 サブネット（たとえば、10.1.1.0/24） • IPv6 形式のホスト IP アドレス（たとえば、2001::0） （注） • [Source IP Address] フィールドに IPv6 アドレスの範囲を入力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と、レイヤ 4 送信元または宛先ポートの範囲を設定できません。 • レイヤ 3 送信元 IP アドレスの範囲を設定すると、レイヤ 2 VLAN ID の範囲は設定できません。

名前	説明
[Destination IP Address] フィールド	レイヤ 3 トラフィックの宛先 IP アドレス。次のいずれかになります。 • ホスト IP アドレス（たとえば、10.10.10.11） • IPv4 アドレス範囲（たとえば、10.10.10.11-10.10.10.18） • IPv4 サブネット（たとえば、10.1.1.0/24） • IPv6形式のホストIPアドレス（たとえば、2001::4） • サブネット（たとえば、10.0.0.0/25） （注） • [Destination IP Address] フィールドに IPv6 アドレスの範囲を入力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と、レイヤ 4 送信元または宛先ポートの範囲を設定できません。 • レイヤ 3 送信元 IP アドレスの範囲を設定すると、レイヤ2 VLAN ID の範囲は設定できません。
[Protocol] ドロップダウン リスト	レイヤ3トラフィックのインターネットプロトコルを選択します。次のいずれかになります。 • ICMP • TCP • UDP • Enter Protocol タイプとして [Enter Protocol] を選択した場合は、10 進数、16 進数、または 8 進数形式の IP プロトコル番号を入力します。
[ToS Bits] フィールド	レイヤ 3 IP ヘッダー内の Type of Service（ToS）ビット。Differentiated Services Code Point（DSCP）値だけが使用されます。

ステップ 5 [Edit Filter] ダイアログボックスの [Layer 4] セクションで、次のフィールドを入力します。

名前	説明
[Source Port] ドロップダウン リスト	レイヤ 4 トラフィックの送信元ポートを選択します。次のいずれかになります。 • FTP (Data) • FTP (Control) • SSH • TELNET • HTTP • HTTPS • Enter Source Port [Enter Source Port] を選択した場合は、単一のポート番号か、または送信元ポート番号の範囲のいずれかを入力します。 （注） • レイヤ 4 送信元ポートの範囲を設定すると、レイヤ 3 IP 送信元または宛先ポートの範囲を設定できません。 • レイヤ 4 送信元ポートの範囲を設定すると、レイヤ 2 VLAN ID の範囲は設定できません。

名前	説明
[Destination Port] ドロップダウン リスト	レイヤ 4 トラフィックの宛先ポートを選択します。次のいずれかになります。 • FTP (Data) • FTP (Control) • SSH • TELNET • HTTP • HTTPS • Enter Destination Port [Enter Destination Port] を選択した場合は、単一のポート番号か、または宛先ポート番号の範囲のいずれかを入力します。 （注） • レイヤ 4 宛先ポートの範囲を設定すると、レイヤ 3 IP 送信元または宛先ポートの範囲を設定できません。 • レイヤ 4 宛先ポートの範囲を設定すると、レイヤ 2 VLAN ID の範囲は設定できません。

ステップ 6　[Edit Filter] ダイアログボックスの [Layer 7] セクションで、次のフィールドを入力します。

名前	説明
[HTTP Method] フィールド	HTTP メソッドの一致を設定し、そのメソッドに基づいてトラフィックをリダイレクトできます。単一フィルタ内での一致のための 1 つ以上のメソッドを選択します。このオプションは、宛先ポートが HTTP または HTTPS のときにのみ使用できます。 • Connect • Delete • get • Head • Post • Put • Trace （注） TCP のオプションの長さはレイヤ 7 トラフィックのメソッドのいずれかを選択すると有効になります。
[TCP Option Length] フィールド	フィルタ設定を拡張して、テキストボックスに TCP オプションの長さを指定することができます。テキストボックスのデフォルト値は 0 です。フィルタ内のすべてのメソッドが同一のオプションの長さを備えています。 10 進形式で TCP オプションの長さを入力します。 （注） テキストボックスの値は、4 の倍数になっている必要があり、0 ～ 40 の範囲にすることができます。

ステップ 7 [Edit Filter] をクリックします。

フィルタの削除

関連付けられたルールを持つフィルタを削除できます。これにより、すべてのルールを同時に削除します。

手順

ステップ 1 [Configure Filters] タブで、削除する 1 つまたは複数のフィルタの横のチェック ボックスをオンにして、[Remove Filters] をクリックします。
フィルタに関連付けられているルールがあれば、この情報が [Remove Filters] ダイアログ ボックスに表示されます。

ステップ 2 [Remove Filters] ダイアログ ボックスで、[Remove Filters] をクリックします。

接続の追加

はじめる前に

- 接続に割り当てるフィルタを追加します。
- モニタリング デバイスを設定します（オプション）。
- 1 つのエッジ ポートまたは複数のエッジ ポートを設定します（オプション）。

手順

ステップ 1 [Connections] タブで、[Add Connection] をクリックします。

ステップ 2 [Add Connection] ダイアログボックスで、[Connection Details] 領域の接続の [Connection Name] および [Priority] を追加できます。

フィールド	説明
Connection Name	接続名。 名前には 1 ～ 256 文字の英数字を含めることができます。使用できる特殊文字は、下線「_」、ハイフン「-」、プラス「+」、等号「=」、開き括弧「(」、閉じ括弧「)」、縦棒「|」、ピリオド「.」、およびアット マーク「@」です。
Description	新しい接続の作成時に説明を入力します。
Priority	接続のために設定するプライオリティ。 デフォルトは 100 で、有効な範囲は 0 ～ 10000 です。

ステップ 3 [Allow Matching Traffic] 領域で、次のフィールドを変更します。

フィールド	説明
[Allow Filters] ドロップダウンリスト	一致するトラフィックを許可するために使用するフィルタを選択します。 （注） [Traffic Drop Filters] に選択したものと同一のフィルタを [Allow Filters] に選択することはできません。
[Set VLAN] フィールド	接続のために設定する VLAN ID。
[Strip VLAN at delivery port] チェック ボックス	配信ポートに到達するまでにパケットから VLAN タグを削除するには、このチェックボックスをオンにします。 （注） [Strip VLAN at delivery port] の動作は、単一のエッジ ポートと、単一の分離したノードの 1 つ以上の配信デバイスの接続にのみ有効です。
[Destination Devices] リスト	フィルタに関連付けるモニタリング デバイス。名前の横のボックスをオンにして、1 つ以上のデバイスを選択できます。
[Traffic Drop Filters] ドロップダウンリスト	（注）

ステップ 4 [Drop Matching Traffic] 領域で次のフィールドに入力します。

フィールド	説明
Traffic Drop Filters	デフォルト フィルタの [Default-Match-all] を選択するか、またはその他のフィルタを使用して一致するトラフィックを破棄します。 （注） [Allow Filters] に選択したものと同一のフィルタを [Traffic Drop Filters] に選択することはできません。

ステップ 5 [Source Ports (Optional)] 領域で次のフィールドに入力します。

フィールド	説明
[Select Source Node] ドロップダウン リスト	割り当てる送信元ノードを選択します。 （注） 送信元ノードを選択しないと、Any-to-Multipoint のループフリーの転送パス オプションが使用され、すべての未配信のポートからのトラフィックがフィルタに対して評価されます。 （注） 新しいリダイレクションを設定すると、各入力ポートの一部となるフローの数を確認できます。ポート番号をクリックすると、フローの詳細が表示されます。
[Select Source Port] ドロップダウンリスト	割り当てる送信元ノードのポートを選択します。 （注） エッジ ポートのみを送信元ポートとして使用できます。 （注） 新しい接続の追加時に送信元ポートを選択しなかった場合は、次の警告メッセージが表示されます。「No source port is selected.Connection will be setup from all configured Edge-SPAN and Edge-TAP ports.」[OK] をクリックして、接続のインストール/作成を続行します。これにより、Any-to-Multipoint 接続をインストールしておらず、既存のトラフィックを妨げていないことが確実になります。[Cancel] をクリックして、接続設定のページに移動します。

（注） Edge-Tap または SPAN ポートと同様に、ポートはトポロジ内の各スイッチの上部に表示され、マウスでスイッチにポインタを合わせたときに特定のモニタリング ツールが一部となっている転送ルールの数を表示します。ポップアップ テーブル（モニタリング ツールが内部で使用されている）にルール（接続）名が表示されます。

ステップ 6 次のいずれかを実行します。

- [Save Connection] をクリックすると、接続が保存されますが、これは後からインストールするためのものではありません。
- [Install Connection] をクリックすると、接続が保存され、インストールが同時に行われます。
- 保存せずに接続を終了するには、[Close] をクリックします。

[Connection Setup] 画面に、次のフィールドが表示されます。

- Name
- Allow Filters
- Deny Filters
- Source Ports
- Devices
- Priority
- Last Modified By
- Description

接続の変更

はじめる前に

接続を変更する前に、接続を追加する必要があります。

手順

ステップ 1 [Connection Setup] タブで、変更する接続の [Name] の横にある [Edit] をクリックします。

ステップ 2 [Modify Connection] ダイアログボックスで、[Connection Details] 領域の接続の [Connection Name] および [Priority] を変更できます。

フィールド	説明
Connection Name	接続名。 名前には 1 ～ 256 文字の英数字を含めることができます。使用できる特殊文字は、下線「_」、ハイフン「-」、プラス「+」、等号「=」、開き括弧「(」、閉じ括弧「)」、縦棒「|」、ピリオド「.」、およびアット マーク「@」です。
Description	新しい接続の作成時に説明を入力します。
Priority	接続のために設定するプライオリティ。 デフォルトは 100 で、有効な範囲は 0 ～ 10000 です。

ステップ 3 [Allow Matching Traffic] 領域で、次のフィールドを変更します。

フィールド	説明
[Allow Filters] ドロップダウンリスト	一致するトラフィックを許可するために使用するフィルタを選択します。 （注） [Traffic Drop Filters] に選択したものと同一のフィルタを [Allow Filters] に選択することはできません。
[Set VLAN] フィールド	接続のために設定する VLAN ID。
[Strip VLAN at delivery port] チェック ボックス	配信ポートに到達するまでにパケットから VLAN タグを削除するには、このチェックボックスをオンにします。 （注） [Strip VLAN at delivery port] の動作は、単一のエッジ ポートと、単一の分離したノードの 1 つ以上の配信デバイスの接続にのみ有効です。
[Destination Devices] リスト	フィルタに関連付けるモニタリング デバイス。名前の横のボックスをオンにして、1 つ以上のデバイスを選択できます。
[Traffic Drop Filters] ドロップダウンリスト	（注）

ステップ 4 [Drop Matching Traffic] 領域で次のフィールドに入力します。

フィールド	説明
Traffic Drop Filters	デフォルト フィルタの [Default-Match-all] を選択するか、またはその他のフィルタを使用して一致するトラフィックを破棄します。 （注） [Allow Filters] に選択したものと同一のフィルタを [Traffic Drop Filters] に選択することはできません。

ステップ 5 [Source Ports (Optional)] 領域で次のフィールドに入力します。

フィールド	説明
[Select Source Node] ドロップダウン リスト	割り当てる送信元ノードを選択します。 （注） 送信元ノードを選択しないと、Any-to-Multipoint のループフリーの転送パス オプションが使用され、すべての未配信のポートからのトラフィックがフィルタに対して評価されます。
[Select Source Port] ドロップダウンリスト	割り当てる送信元ノードのポートを選択します。 （注） エッジ ポートのみを送信元ポートとして使用できます。

ステップ 6 [Submit] または [Close] をクリックします。

接続の複製

はじめる前に

接続を変更する前に、接続を追加する必要があります。

手順

ステップ 1 [Connection Setup] タブで、複製する接続の [Name] の横にある [Clone] をクリックします。

ステップ 2 [Clone Connection] ダイアログボックスで、[Connection Details] 領域の接続の [Connection Name] および [Priority] を変更できます。

フィールド	説明
Connection Name	接続名。 名前には 1 ～ 256 文字の英数字を含めることができます。使用できる特殊文字は、下線「_」、ハイフン「-」、プラス「+」、等号「=」、開き括弧「(」、閉じ括弧「)」、縦棒「|」、ピリオド「.」、およびアット マーク「@」です。
Description	新しい接続の作成時に説明を入力します。

フィールド	説明
Priority	接続のために設定するプライオリティ。 デフォルトは 100 で、有効な範囲は 0 ～ 10000 です。

ステップ 3 [Allow Matching Traffic] 領域で、次のフィールドを変更します。

フィールド	説明
[Allow Filters] ドロップダウンリスト	一致するトラフィックを許可するために使用するフィルタを選択します。 （注） [Traffic Drop Filters] に選択したものと同一のフィルタを [Allow Filters] に選択することはできません。
[Set VLAN] フィールド	接続のために設定する VLAN ID。
[Strip VLAN at delivery port] チェック ボックス	配信ポートに到達するまでにパケットから VLAN タグを削除するには、このチェックボックスをオンにします。 （注） [Strip VLAN at delivery port] の動作は、単一のエッジ ポートと、単一の分離したノードの 1 つ以上の配信デバイスの接続にのみ有効です。
[Destination Devices] リスト	フィルタに関連付けるモニタリングデバイス。名前の横のボックスをオンにして、1 つ以上のデバイスを選択できます。
[Traffic Drop Filters] ドロップダウンリスト	（注）

ステップ 4 [Drop Matching Traffic] 領域で次のフィールドに入力します。

フィールド	説明
Traffic Drop Filters	デフォルト フィルタの [Default-Match-all] を選択するか、またはその他のフィルタを使用して一致するトラフィックを破棄します。 （注） [Allow Filters] に選択したものと同一のフィルタを [Traffic Drop Filters] に選択することはできません。

ステップ 5 [Source Ports (Optional)] 領域で次のフィールドに入力します。

フィールド	説明
[Select Source Node] ドロップダウン リスト	割り当てる送信元ノードを選択します。 （注） 送信元ノードを選択しないと、Any-to-Multipoint のループフリーの転送パス オプションが使用され、すべての未配信のポートからのトラフィックがフィルタに対して評価されます。
[Select Source Port] ドロップダウンリスト	割り当てる送信元ノードのポートを選択します。 （注） エッジ ポートのみを送信元ポートとして使用できます。

ステップ 6 次のいずれかを実行します。

- [Save Cloned Connection] をクリックすると、接続が保存されますが、これは後からインストールするためのものではありません。
- [Install Cloned Connection] をクリックすると、接続が保存され、インストールが同時に行われます。
- 保存せずに接続を終了するには、[Close] をクリックします。

接続の削除

手順

ステップ 1 [Connection Setup] タブに移動します。
ステップ 2 削除する単一または複数の接続のチェックボックスをオンにします。
ステップ 3 [Remove Connections] をクリックします。

サービス ノードの追加

手順

ステップ 1 トポロジ図で、ノードをクリックします。

ステップ 2 サイド バーで、[Add Service Node] をクリックします。[Add Service Node] ウィンドウが表示されます。

ステップ 3 [Service Node Name] ウィンドウにサービス ノードの名前を入力します。

ステップ 4 [Service Node Ingress Port] ウィンドウのサービス ノードの入力ポートを選択します。

ステップ 5 [Service Node Egress Port] ウィンドウのサービス ノードの出力ポートを選択します。

ステップ 6 サービス ノード アイコンを選択します。

ステップ 7 [Submit] をクリックします。

リダイレクションの追加

（注） リダイレクションの設定機能は、リリース 6.0(2) U 5(2) 以降を実行している Cisco Nexus 3000 シリーズ スイッチでサポートされます。この機能は、Cisco Nexus 9300 スイッチの Release 7.x 以降および OpenFlow でサポートされています。

はじめる前に

- リダイレクションに割り当てるフィルタを追加します。
- モニタリング デバイスを設定します（オプション）。
- 1 つのエッジ ポートまたは複数のエッジ ポートを設定します（オプション）。
- 実稼働の入力ポート、実稼働の出力ポート、およびサービス ノードは、同じリダイレクション スイッチ上に配置してください。

手順

ステップ 1 [Redirections] タブで、[Add Redirection] をクリックします。

ステップ 2 [Add Redirection] ダイアログボックスで、[Redirection Details] エリアにリダイレクションの [Redirection Name] および [Priority] を追加できます。

フィールド	説明
Redirection Name	リダイレクションの名前。 名前には 1 ～ 256 文字の英数字を含めることができます。使用できる特殊文字は、下線「_」、ハイフン「-」、プラス「+」、等号「=」、開き括弧「(」、閉じ括弧「)」、縦棒「|」、ピリオド「.」、およびアット マーク「@」です。 （注） リダイレクションの名前を保存すると、それを変更することはできません。
Description	新しいリダイレクションの作成時に説明を入力します。
[Set auto priority] チェックボックス	リダイレクションの自動プライオリティを有効にするには、このオプションをオンにします。リダイレクションのプライオリティは、選択した入力ポートにインストールされた既存のリダイレクションに基づいて設定されます。
Priority	リダイレクションのために設定するプライオリティ。有効な値の範囲は 0 ～ 10000 です。デフォルトは 100 です。
[Automatic Fail-safe] チェックボックス	リダイレクションのフェールセーフ機能を有効にするには、このオプションをオンにします。この機能を有効にすると、実稼働の入力ポートおよび出力ポートから直接のフローが作成され、これはすべての低プライオリティの EtherType トラフィックに一致します。

ステップ 3 [Matching Traffic] エリアで、次のフィールドを変更します。

フィールド	説明
[Filters] ドロップダウンリスト	一致するトラフィックを許可するために使用するフィルタを選択します。 （注） フィルタに対する同じリダイレクションは選択できません。

ステップ 4 [Redirection Switch] エリアで、次のフィールドを変更します。

フィールド	説明
[Select Redirection Switch] ドロップダウンリスト	割り当てるリダイレクション スイッチを選択します。

（注） 1 つのリダイレクション スイッチあたり 1 つの入力ポートと 1 つの出力ポートのみを持つことができます。

ステップ 5 [Service Nodes (OPTIONAL)] エリアで、次のフィールドに入力します。

フィールド	説明
[Select Service Node] ドロップダウンリスト	割り当てるリダイレクション サービス ノードを選択し、[Add Service Node] をクリックします。

（注） 複数のサービス ノードを追加する場合は、パケットを転送する順番に追加する必要があります。

ステップ 6 [Production Ports] エリアで、次のフィールドに入力します。

フィールド	説明
[Select Production Ingress Port] ドロップダウンリスト	割り当てる実稼働の入力ポートを選択します。 （注） 入力ポートを1つだけ選択できます。複数の入力ポートは許可されません。入力ポートと出力ポートに同じポートを使用することはできません。 （注） 新しいリダイレクションを設定すると、各入力ポートの一部となるフローの数を確認できます。ポート番号をクリックすると、フローの詳細が表示されます。
[Select Production Egress Port] ドロップダウンリスト	割り当てる実稼働の出力ポートを選択します。 （注） 入力ポートを1つだけ選択できます。複数の入力ポートは許可されません。入力ポートと出力ポートに同じポートを使用することはできません。

ステップ 7 [Delievery Devices to copy traffic (OPTIONAL)] エリアで、次のフィールドに入力します。

フィールド	説明
[Select Device] ドロップダウン リスト	割り当てるデバイス（たとえば、ドロップダウンリストからスイッチ）を選択し、[Add Device] をクリックします。 （注） リダイレクションには、複数の配信デバイスを選択できます。

ステップ 8 次のいずれかを実行します。

- [Save Redirection] をクリックしてリダイレクションを保存しますが、これは後からインストールするためのものではありません。
- [Install Redirection] をクリックしてリダイレクションを保存し、同時にそれをインストールします。
- 保存せずにリダイレクションを終了するには、[Close] をクリックします。

ステップ 9 [Install Redirection] をクリックしてリダイレクションを保存し、同時にそれをインストールする場合、リダイレクション スイッチのリダイレクション パスは実稼働の入力ポート、サービス ノード、および実稼働の出力ポートに表示されます。

ステップ 10 [Flow Statistics] をクリックしてリダイレクション スイッチのフロー統計を表示します。
次のフィールドは、フロー統計情報に関する情報を提供します。

- [In Port] フィールド：トラフィックが一致した入力ポート。アスタリスク（「*」）は入力ポートを示します。
- [DL DRC] フィールド：着信トラフィックに一致する送信元 MAC アドレス。アスタリスク（「*」）は送信元 MAC アドレスを示します。
- [DL Dst] フィールド：着信トラフィックに一致する宛先 MAC アドレス。アスタリスク（「*」）は宛先 MAC アドレスを示します。
- [DL Type] フィールド：着信トラフィックに一致する EtherType。たとえば、「IPv4」または「IPv6」はすべての IP トラフィックのタイプに使用されます。
- [DL VLAN] フィールド：着信トラフィックに一致する VLAN ID。アスタリスク（「*」）は VLAN ID を示します。
- [VLAN PCP] フィールド：着信トラフィックに一致する VLAN のプライオリティ。このフィールドにはアスタリスク（「*」）がほとんど常に表示されます。
- [NW Src] フィールド：着信トラフィックの IPv4 または IPv6 送信元アドレス。アスタリスク（「*」）は IPv4 または IPv6 EtherType に基づく発信元アドレスを示します。
- [NW Dst] フィールド：着信トラフィックの IPv4 または IPv6 宛先アドレス。アスタリスク（「*」）は IPv4 または IPv6 EtherType に基づく宛先アドレスを示します。
- [NW Proto] フィールド：着信トラフィックに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 Src] フィールド：着信トラフィックに一致するようにネットワーク プロトコルに関連付けられた送信元ポート。アスタリスク（「*」）はポート値を示します。
- [TP Dst] フィールド：着信トラフィックに一致するようにネットワーク プロトコルに関連付けられた宛先ポート。アスタリスク（「*」）はポート値を示します。
- [Action] フィールド：「OUTPUT = OF|2」など、指定した条件に一致するトラフィックに対して実行される出力アクション。
- [Byte Count] フィールド：指定したフロー接続と一致する集約トラフィックのボリューム（バイト単位）。

- [Packet Count] フィールド：指定したフロー接続と一致する集約トラフィックのボリューム（パケット単位）。
- [Duration Seconds] フィールド：特定のフロー接続がスイッチにインストールされた時間（ミリ秒単位）
- [Idle Timeout] フィールド：フローテーブルから削除される前にフローをアイドル状態にできる時間（ミリ秒）。
- [Priority] フィールド：フローに割り当てられたプライオリティ。より高いプライオリティ値を持つフローが優先されます。

ステップ 11 [Close] をクリックして、フロー統計の表示ウィンドウを閉じます。

リダイレクションの変更

はじめる前に

リダイレクションを変更する前に、リダイレクションを追加する必要があります。

手順

ステップ 1 [Redirection Setup] タブで、変更する接続の [Name] の横にある [Edit] をクリックします。

ステップ 2 [Modify Redirection] ダイアログボックスで、[Redirection Details] 領域のリダイレクションの [Redirection Name] および [Priority] を変更できます。

フィールド	説明
Redirection Name	リダイレクションの名前。 名前には 1 ～ 256 文字の英数字を含めることができます。使用できる特殊文字は、下線「_」、ハイフン「-」、プラス「+」、等号「=」、開き括弧「(」、閉じ括弧「)」、縦棒「|」、ピリオド「.」、およびアット マーク「@」です。 （注） リダイレクションの名前を保存すると、それを変更することはできません。
Description	新しいリダイレクションの作成時に説明を入力します。
[Set auto priority] チェックボックス	リダイレクションの自動プライオリティを有効にするには、このオプションをオンにします。リダイレクションのプライオリティは、選択した入力ポートにインストールされた既存のリダイレクションに基づいて設定されます。

フィールド	説明
Priority	リダイレクションのために設定するプライオリティ。有効な値の範囲は 0 ～ 10000 です。デフォルトは 100 です。
[Automatic Fail-safe] チェックボックス	リダイレクションのフェールセーフ機能を有効にするには、このオプションをオンにします。この機能を有効にすると、実稼働の入力ポートおよび出力ポートから直接のフローが作成され、これはすべての低プライオリティの EtherType トラフィックに一致します。

ステップ 3 [Matching Traffic] エリアで、次のフィールドを変更します。

フィールド	説明
[Filters] ドロップダウンリスト	一致するトラフィックを許可するために使用するフィルタを選択します。 （注） フィルタに対する同じリダイレクションは選択できません。

ステップ 4 [Redirection Switch] エリアで、次のフィールドを変更します。

フィールド	説明
[Select Redirection Switch] ドロップダウンリスト	割り当てるリダイレクション スイッチを選択します。 （注） フィルタに対する同じリダイレクション スイッチは選択できません。

ステップ 5 [Service Nodes (OPTIONAL)] エリアで、次のフィールドに入力します。

フィールド	説明
[Select Service Node] ドロップダウンリスト	割り当てるリダイレクション サービス ノードを選択し、[Add Service Node] をクリックします。

ステップ 6 [Production Ports] エリアで、次のフィールドに入力します。

フィールド	説明
[Select Production Ingress Port] ドロップダウンリスト	割り当てる実稼働の入力ポートを選択します。 （注） 入力ポートを1つだけ選択できます。複数の入力ポートは許可されません。入力ポートと出力ポートに同じポートを使用することはできません。
[Select Production Egress Port] ドロップダウンリスト	割り当てる実稼働の出力ポートを選択します。 （注） 入力ポートを1つだけ選択できます。複数の入力ポートは許可されません。入力ポートと出力ポートに同じポートを使用することはできません。

ステップ 7 [Delievery Devices to copy traffic (OPTIONAL)] エリアで、次のフィールドに入力します。

フィールド	説明
[Select Device] ドロップダウン リスト	割り当てるデバイス（たとえば、ドロップダウンリストからスイッチ）を選択し、[Add Device] をクリックします。 （注） リダイレクションには、複数の配信デバイスを選択できます。

ステップ 8 次のいずれかを実行します。

- [Save Redirection] をクリックしてリダイレクションを保存しますが、これは後からインストールするためのものではありません。
- [Install Redirection] をクリックしてリダイレクションを保存し、同時にそれをインストールします。
- 保存せずにリダイレクションを終了するには、[Close] をクリックします。

リダイレクションの削除

手順

ステップ 1 [Redirection Setup] タブに移動します。

ステップ 2 削除する単一または複数のリダイレクションのチェックボックスをオンにします。

ステップ 3 [Remove Redirections] をクリックします。

第 9 章

ロールおよびリソースの管理

この章の内容は、次のとおりです。

- Cisco Data Broker のユーザについて，93 ページ
- ロールの作成，94 ページ
- 複数の分離されたネットワークにアクセスするためのロールの設定，94 ページ
- ロールの削除，96 ページ
- リソース グループの作成，96 ページ
- リソース グループへのリソースの追加，96 ページ
- ロールへのグループの割り当て，97 ページ
- グループの割り当て解除，98 ページ
- グループの削除，98 ページ

Cisco Data Broker のユーザについて

Cisco Nexus Data Broker は、ユーザ アクセスの管理にロールとレベルを使用します。次のレベルの 1 つを作成する各ロールに割り当てることができます。

- [App-Administrator]：すべての Cisco Nexus Data Broker リソースへのフル アクセスがあります。
- App-User：自身のリソース グループに割り当てられたリソース、および同様のアクセス許可を持つ別のユーザによって作成されたリソースへのフル アクセスがあります。

各ロールは、リソースの集まりである 1 つ以上のグループに割り当てられます。グループ リソースは非スイッチ間リンク（ISL）ポートであり、そのグループに固有のものとして割り当てられています。グループを作成した後は、そのグループをロールに割り当てることができます。

ロールの作成

手順

ステップ 1 メニュー バーで、[Admin] ドロップダウン リストをクリックし、[Settings] を選択します。

ステップ 2 [Roles] タブで [Add Role] をクリックします。

ステップ 3 [Add Role] ダイアログボックスで、次のフィールドに値を入力します。

フィールド	説明
[Name] フィールド	ロールの名前。 名前には 1 ～ 256 文字の英数字を含めることができます。使用できる特殊文字は、下線「_」、ハイフン「-」、プラス「+」、等号「=」、開き括弧「(」、閉じ括弧「)」、縦棒「|」、ピリオド「.」、およびアット マーク「@」です。
[Level] ドロップダウン リスト	ロールに割り当てるレベルを選択します。次のいずれかになります。 • [App-Administrator]：すべての Cisco Nexus Data Broker リソースへのフル アクセスがあります。 • App-User：自身のリソース グループに割り当てられたリソース、および同様のアクセス許可を持つ別のユーザによって作成されたリソースへのフル アクセスがあります。

ステップ 4 [Submit] をクリックします。

複数の分離されたネットワークにアクセスするためのロールの設定

複数の分離されたネットワークは、Cisco Nexus Data Broker アプリケーションでネットワーク スライスを作成するときに作成する仮想ネットワークです。ロールは、複数の Cisco Nexus Data Broker の分離されたネットワークへのロールベースのアクセスを許可するように設定できます。

たとえば、2つのネットワークがあるとして、最初のものを **dev** という名前にし、2番目のものを **prod** という名前にした場合、ネットワーク管理者は、それぞれのネットワークに対して異なる権限を持ち、両方のネットワークにアクセス権を持つユーザを作成できます。ネットワーク **dev** のアクセス レベルは App-Admin として割り当て、ネットワーク **prod** のアクセス レベルは App-User として割り当てることができます。

App-Admin 権限は、割り当てられたネットワーク（この場合は dev）上のそのユーザやその他のロールのルールおよびフィルタを作成、編集、および削除する機能を提供します。App-Use 権限は、割り当てられたネットワーク（この場合は prod）上のこのロールのみに所有されているルールおよびフィルタを作成、編集、および削除する機能を提供します。アプリケーション ユーザ ロールは、分離されたネットワークまたはロールが割り当てられたネットワーク用にのみ、ルールおよびフィルタを作成、編集、および削除できます。また、アプリケーション ユーザ ロールは、アプリケーション管理者によって作成されたフィルタを表示および適用できますが、編集または削除はできません。

手順

ステップ 1 Cisco Nexus Data Broker ネットワークに、Network-Admin ロールのユーザ名とパスワードを使用してログインします。

ステップ 2 **dev** ネットワークにいることを確認します。

ステップ 3 メニュー バーで、[Admin] ドロップダウンリストから [Settings] を選択します。

ステップ 4 [Add Role] をクリックします。

ステップ 5 [Add Role] ダイアログボックスの [Name] フィールドで、ロールの名前（たとえば、NDB-role-dev）を入力します。
名前には 1 ～ 256 文字の英数字を含めることができます。使用できる特殊文字は、下線「_」、ハイフン「-」、プラス「+」、等号「=」、開き括弧「(」、閉じ括弧「)」、縦棒「|」、ピリオド「.」、およびアット マーク「@」です。

ステップ 6 [Level] ドロップダウンリストから、[App-Administrator] を選択します。

ステップ 7 [Submit] をクリックします。

ステップ 8 メニュー バーで、ネットワークのドロップダウンリストから [prod] ネットワークを選択します。

ステップ 9 **prod** ネットワークについて、手順 3 と 4 を繰り返します。

ステップ 10 [Add Role] ダイアログ ボックスの [Name] フィールドに、NDB-role-prod を入力します。

ステップ 11 [Level] ドロップダウンリストから、[App-User] を選択します。

ステップ 12 [Submit] をクリックします。

ステップ 13 [Assign] タブの下のロール MM-role-prod に [allPorts] を割り当てます。
これでロール NDB-role-dev は、ネットワーク **dev** に対して App-Administrator アクセス許可を持つようになり、ロール NDB-role-prod は、ネットワーク **prod** に対して App-User アクセス許可を持つようになりました。

これで、これら両方のアプリケーション ロールを持つユーザを作成できるようになりました。

（注） 異なるアクセス レベルを持つネットワークを切り替えるには、Ctrl+F5 または Cmd+Shift+R を同時に押します。

ロールの削除

手順

ステップ 1 [Admin] ドロップダウン リストから、[Settings] を選択します。

ステップ 2 [Roles] タブの [Roles] テーブルで、削除するロールをクリックします。

ステップ 3 [Remove Roles] 確認ダイアログ ボックスで、[Remove] をクリックします。

リソース グループの作成

手順

ステップ 1 [Admin] ドロップダウン リストから、[Settings] を選択します。

ステップ 2 [Groups] タブで、[Add Group] をクリックします。

ステップ 3 [Add Resource Group] ダイアログボックスに、リソース グループに使用する名前を入力します。名前には 1 ～ 256 文字の英数字を含めることができます。使用できる特殊文字は、下線「_」、ハイフン「-」、プラス「+」、等号「=」、開き括弧「(」、閉じ括弧「)」、縦棒「|」、ピリオド「.」、およびアット マーク「@」です。

ステップ 4 [Submit] をクリックします。

次の作業

グループにリソースを追加します。

リソース グループへのリソースの追加

はじめる前に

リソース グループを作成します。

手順

ステップ 1 [Admin] ドロップダウン リストから、[Settings] を選択します。
ステップ 2 [Groups] タブで、リソースを追加するグループを選択します。
ステップ 3 トポロジ図でノードを選択します。
ステップ 4 [Add Ports to Group] ダイアログボックスで、グループに追加するポートを選択します。
ステップ 5 [Submit] をクリックします。
ステップ 6 追加するポートすべてに対してステップ 3 からステップ 5 を繰り返します。
ステップ 7 1 つ以上のポートを [Group Detail] テーブルで選択してから、[Remove Ports] をクリックすることで、1 つのリソースまたは複数のリソースを削除します。
ステップ 8 [Remove Ports] ダイアログ ボックスで、[Remove] をクリックします。

次の作業

ロールにリソース グループを割り当てます。

ロールへのグループの割り当て

はじめる前に

- ロールを作成します。
- リソース グループを作成します。

手順

ステップ 1 [Admin] ドロップダウン リストから、[Settings] を選択します。
ステップ 2 [Assign] タブをクリックします。
ステップ 3 グループを割り当てるロールの横の [Assign] をクリックします。
ステップ 4 [Create Role] ダイアログボックスで、次のフィールドに入力します。

フィールド	説明
[Assign Group] フィールド	ロールに割り当てるグループ。割り当てる 1 つ以上のグループを選択できます。 （注） アプリケーション管理者レベルのあるロールにグループを割り当てることはできません。

フィールド	説明
[Unassign Group] フィールド	ロールの割り当てを解除するグループ。割り当てを解除する 1 つ以上のグループを選択できます。 （注） アプリケーション管理者レベルのあるロールの allPorts グループについては割り当てを解除できません。

ステップ 5 [Apply] をクリックします。

グループの割り当て解除

手順

ステップ 1 [Admin] ドロップダウン リストから、[Settings] を選択します。

ステップ 2 [Assign] タブをクリックします。

ステップ 3 グループの割り当てを解除するロールの横の [Assign] をクリックします。

ステップ 4 [Configure Role] ダイアログボックスで、[Unassign Group] ドロップダウン リストにあるポートを選択します。

ステップ 5 [Apply] をクリックします。

グループの削除

次のグループは削除できません。

- デフォルトの allPorts グループ
- グループに割り当てられているロール

手順

ステップ 1 [Admin] ドロップダウン リストから、[Settings] を選択します。

ステップ 2 [Groups] タブで、削除するグループを選択します。

ステップ 3 [Remove Groups] をクリックします。

ステップ 4 [Remove Resource Groups] 確認ダイアログ ボックスで、[Remove] をクリックします。

第 10 章

フローの管理

この章の内容は、次のとおりです。

- フロー プログラミングの概要，101 ページ
- フロー エントリの追加，102 ページ
- フローの詳細情報の表示，105 ページ

フロー プログラミングの概要

Cisco Nexus Data Broker では、各ネットワーク デバイスの個々のフローを設定できます。フローは、レイヤ 1 からレイヤ 4 の基準に基づいて識別されます。フローが識別されると、フロー スペックに一致するパケットで実行されるアクションを指定できます。これは、OpenFlow スイッチだけに適用できます。

マッチングとアクションの基準はスイッチによって異なります。指定可能なアクションは次のとおりです。

- 1 つ以上のインターフェイスへのパケットのドロップまたはフォワーディング。
- パケットの VLAN ID と優先順位の設定。
- パケットの送信元および宛先 MAC アドレスの変更。
- パケットの送信元および宛先 IP アドレスの変更。

作成したすべてのフローは [Flows] タブの [Flow Entries] テーブルに表示されます。フローをデバイスにインストールすると、フローはアクティブになります。

フロー エントリの追加

手順

ステップ 1 [Admin] ドロップダウン リストから、[Management] を選択します。

ステップ 2 メニュー バーで [Flows] を選択してから、[Flow Entries] タブをクリックします。

ステップ 3 [Add Flow Entry] をクリックします。

ステップ 4 [Add Flow Entry] ダイアログボックスの [Flow Description] 領域で、次のフィールドに値を入力します。

名前	説明
[Name] フィールド	フローに割り当てる名前。 名前には 1 ～ 256 文字の英数字を含めることができます。使用できる特殊文字は、下線「_」、ハイフン「-」、プラス「+」、等号「=」、開き括弧「(」、閉じ括弧「)」、縦棒「|」、ピリオド「.」、およびアット マーク「@」です。 （注） 保存後にフロー エントリの名前を変更することはできません。
[Node] ドロップダウン リスト	デバイスの ID またはノード名を選択します。 （注） 選択したノードは、フロー エントリを保存するもので変更することはできません。
[Input Port] ドロップダウン リスト	トラフィックがフローを入力するノード上でポートを選択します。
[Priority] フィールド	フローに適用するプライオリティ。デフォルトのプライオリティは500です。高いプライオリティのフローは低いプライオリティのフローよりも優先されます。 （注） レイヤ 2、レイヤ 3、およびレイヤ 4 の一致フィールドすべてが等しい場合のみプライオリティが考慮されます。
[Hard Timeout] フィールド	フローテーブルから削除される前にフローがインストールされる時間（ミリ秒）。
[Idle Timeout] フィールド	フローテーブルから削除される前にフローをアイドル状態にできる時間（ミリ秒）。
[Cookie] フィールド	フローに追加される識別子。クッキーは、フローがインストールされ、各フロー ステータスとフローの期限切れメッセージの一部として返されるときにコントローラによって指定されます。

ステップ 5 [Layer 2] 領域で、次のフィールドに値を入力します。

名前	説明
[Ethernet Type] フィールド	レイヤ 2 トラフィックのイーサネット タイプ。IPv4 のイーサネットタイプは、16進数形式で、デフォルトで表示されます。デフォルト値を受け入れるか、または 16 進数形式で次のいずれかを入力します。 • IPv6 • ARP • LLDP
[VLAN Identification Number] フィールド	レイヤ 2 トラフィックの VLAN ID。
[VLAN Priority] フィールド	レイヤ 2 トラフィックの VLAN のプライオリティ。
[Source MAC Address] フィールド	レイヤ 2 トラフィックの送信元 MAC アドレス。
[Destination MAC Address] フィールド	レイヤ 2 トラフィックの宛先 MAC アドレス。

ステップ 6 [Layer 3] 領域で、次のフィールドに値を入力します。

名前	説明
[Source IP Address] フィールド	レイヤ 3 トラフィックの送信元 IP アドレス。 （注） 送信元 IP アドレスの形式は、レイヤ 2 の [Ethernet Type] フィールドに入力されたイーサネット タイプと一致している必要があります。
[Destination IP Address] フィールド	レイヤ 3 トラフィックの宛先 IP アドレス。 （注） 宛先 IP アドレスの形式は、レイヤ 2 の [Ethernet Type] フィールドに入力されたイーサネット タイプと一致している必要があります。
[ToS Bits] フィールド	レイヤ 3 IP ヘッダー内の Type of Service（ToS）ビット。 （注） DSCP ビットのみ Cisco Nexus 3000 シリーズ スイッチでサポートされます。

ステップ 7 [Layer 4] 領域で、次のフィールドに値を入力します。

名前	説明
[Source Port] フィールド	レイヤ 4 トラフィックの送信元ポート。
[Destination Port] フィールド	レイヤ 4 トラフィックの宛先ポート。
[Protocol] フィールド	レイヤ4トラフィックのインターネットプロトコル番号。10進数、16 進数、または 8 進数形式の IP プロトコル番号を入力します。

ステップ 8 [Actions] 領域で、1 つ以上のアクションを選択します。

- ドロップ
- ループバック
- フラッド
- ソフトウェア パス
- ハードウェア パス
- コントローラ
- 出力ポートの追加
- VLAN ID の設定
- VLAN プライオリティの設定
- VLAN ヘッダーのストリッピング
- Datalayer の送信元アドレスの変更
- Datalayer の宛先アドレスの変更
- ネットワークの送信元アドレスの変更
- ネットワークの宛先アドレスの変更
- ToS ビットの変更
- トランスポートの送信元ポートの変更
- トランスポートの宛先ポートの変更
- Flood All
- Enqueue
- Set VLAN CFI
- Push VLAN
- Set EtherType

ステップ 9 次のいずれかを実行します。

- [Install Flow] をクリックして、デバイスにフローをインストールします。
- [Save Flow] をクリックしてフローを [Flow Entries] テーブルに保存します。ただし、デバイスのフロー テーブルにフローはインストールしません。

フローの詳細情報の表示

手順

ステップ 1 [Admin] ドロップダウン リストから、[Management] を選択します。

ステップ 2 メニュー バーで [Flows] を選択してから、[Flow Entries] タブをクリックします。

ステップ 3 表示するフローを特定します。
[Search] コンボ ボックスに値を入力して、検索アイコンをクリックして表示されるエントリ数を制限します。

ステップ 4 [Flow Detail] タブの [Flow Overview] 領域で、次のいずれかのタスクを実行します。

- [Flow Entries] テーブルからフローを削除するには、[Remove Flow] をクリックします。
- デバイスのフロー テーブル内のフローを編集するには、[Edit Flow] をクリックします。
- デバイスのフロー テーブルにフローを削除するには、[Uninstall Flow] をクリックします。

第 11 章

トラブルシューティング

この章の内容は、次のとおりです。

- トラブルシューティングの概要，107 ページ
- フローおよびポートの詳細統計情報の表示，108 ページ
- 整合性がないコントローラ のフローまたは整合性がないノードのフロー，108 ページ
- 整合性がないフローの詳細のエクスポート，109 ページ
- 整合性がないフローの修正，109 ページ
- SDN アナライザ，110 ページ
- SDN アナライザの使用，110 ページ
- SDN アナライザのデフォルト値の変更，111 ページ

トラブルシューティングの概要

Cisco Nexus Data Broker には、ネットワーク接続のトラブルシューティングに使用できるさまざまなツールが含まれています。[Troubleshoot] タブで、次の作業を実行できます。

- ネットワークのすべてのノードを表示します。
- ネットワークの各ノードのポートに関する詳細情報を表示します。
- ネットワークの各ノードのフローに関する詳細情報を表示します。
- [Uptime] タブで、ノードが検出されたときに表示します。
- [Policy Analyzer] タブで、TIF ポリシーに関する詳細情報を表示します。
- 選択したフローと TIF ポリシーで分析を実行します。

フローおよびポートの詳細統計情報の表示

手順

ステップ 1 [Admin] ドロップダウン リストから、[Management] を選択します。

ステップ 2 メニュー バーで、[Troubleshoot] を選択してから、[Flow Check] タブをクリックします。

ステップ 3 [Existing Nodes] タブで、統計情報を表示するノードを探します。
[Search] コンボ ボックスに値を入力して、検索アイコンをクリックして表示されるエントリ数を制限します。

ステップ 4 次のいずれかの作業を実行します。

- ノードにプログラミングされたすべてのフローの詳細情報を表示するには、[Flows] をクリックします。
- ノードのすべてのポートの詳細情報を表示するには、[Ports] をクリックします。

（注） 統計情報は 120 秒ごとに更新されます。

整合性がないコントローラのフローまたは整合性がないノードのフロー

手順

ステップ 1 [Admin] ドロップダウン リストから、[Management] を選択します。

ステップ 2 メニュー バーで、[Troubleshoot] を選択してから、[Flow Check] タブをクリックします。

ステップ 3 [Select a node] ドロップダウン リストからノードを選択します。
ノードが表示され、[Inconsistent Controller Flows] および [Inconsistent Node Flows] の数が各タイプの横に示されます（存在する場合）。

ステップ 4 [Inconsistent Controller Flows] または [Inconsistent Node Flows] のいずれかをクリックして整合性のないフローの詳細を表示します。
詳細は、[Statistics] タブに表示されます。

次の作業

整合性のないコントローラ フローまたは整合性のないノード フローを修正します。

整合性がないフローの詳細のエクスポート

参照用に整合性がないコントローラまたは整合性がないノード フローの詳細を表示および保存するため、コンマ区切りファイルにそれらをエクスポートできます。

手順

ステップ 1 [Admin] ドロップダウン リストから、[Management] を選択します。

ステップ 2 メニュー バーで、[Troubleshoot] を選択してから、[Flow Check] タブをクリックします。

ステップ 3 [Select a node] ドロップダウン リストからノードを選択します。
ノードが表示され、[Inconsistent Controller Flows] および [Inconsistent Node Flows] の数が各タイプの横に示されます。

ステップ 4 [Inconsistent Controller Flows] または [Inconsistent Node Flows] のいずれかを選択します。
[Inconsistent Controller Flows] または [Inconsistent Node Flows] のリストが [Statistics] タブに表示されます。

ステップ 5 1 つ以上の整合性のないフローの横のチェックボックスをオンにするか、またはリストの最上部のチェックボックスをオンにして、リスト内のすべてのフローを選択します。

ステップ 6 [Export All] をクリックし、[Export Flow Details] をクリックします。

ステップ 7 `.csv` ファイルとして整合性のないフローの詳細を保存し、分析のために後で開けるようにします。

整合性がないフローの修正

（注） 整合性がないコントローラのフローを修正すると、フローはスイッチにインストールされています。整合性がないノード フローを修正すると、フローはスイッチから削除されます。コントローラはフロー情報の権威のある送信元であるためです。

手順

ステップ 1 [Admin] ドロップダウン リストから、[Management] を選択します。

ステップ 2 メニュー バーで、[Troubleshoot] を選択してから、[Flow Check] タブをクリックします。

ステップ 3 [Select a node] ドロップダウン リストからノードを選択します。
ノードが表示され、[Inconsistent Controller Flows] および [Inconsistent Node Flows] の数が各タイプの横に示されます。

ステップ 4 [Inconsistent Controller Flows] または [Inconsistent Node Flows] のいずれかをクリックします。
[Inconsistent Controller Flows] または [Inconsistent Node Flows] のリストが [Statistics] タブに表示されます。

ステップ 5 1 つ以上の整合性のないフローの横のチェックボックスをオンにするか、またはリストの最上部のチェックボックスをオンにして、リスト内のすべてのフローを選択します。

ステップ 6 [Fix Inconsistent Flows] をクリックします。

ステップ 7 [Fix Flows] 確認ダイアログボックスで、[Fix Inconsistent Flows] をクリックします。
[Flow Check] タブに、[Inconsistent Controller Flows] および [Inconsistent Node Flows] が各タイプについて更新済みの数とともに再表示されます。

（注） 手順 4 ですべての整合性のないフローを選択した場合、表示される数は 0 です。

SDN アナライザ

（注） SDN アナライザは NX-API によって定義されるインターフェイスには適用されません。

SDN アナライザは、選択するインターフェイスのパケット キャプチャ（pcap）ファイルをダウンロードします。個々の pcap ファイルは 1 つの zip ファイルに統合されます。

デフォルトで、SDN アナライザはネットワーク データ 100 MB ごとに 5 つの pcap ファイルをキャプチャします。データが設定した量を超えてキャプチャされると、古いデータが上書きされます。`config.ini` ファイルで、収集するデータの量を変更できます。

SDN アナライザの使用

SDN アナライザは Cisco Nexus Data Broker に到達するパケットをキャプチャし、結果を zip ファイルに出力します。zip ファイルの場所は、ブラウザの設定によって異なります。

はじめる前に

SDN アナライザを実行するには、Cisco Nexus Data Broker を実行するサーバ上でルート権限が必要です。

手順

ステップ 1 [Admin] ドロップダウン リストから、[Management] を選択します。
ステップ 2 メニュー バーで、[Troubleshoot] をクリックしてから、[SDN Analyzer] タブをクリックします。
ステップ 3 表示するインターフェイスをクリックしてから、[Start Analyzer] をクリックします。
ステップ 4 データの収集が完了したら、[Stop Analyzer] をクリックします。

SDN アナライザのデフォルト値の変更

手順

ステップ 1 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 2 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 3 次のパラメータの検索します。

- troubleshoot.fileSize = 100
- troubleshoot.number = 5

ステップ 4 必要に応じてファイルを変更します。100 MG を超えないファイル サイズを使用し、pcap ファイルの数を増やすことをお勧めします。
ステップ 5 ファイルを保存し、エディタを終了します。
ステップ 6 Cisco Nexus Data Broker を再起動します。

第 12 章

スライスの管理

この章の内容は、次のとおりです。

- スライス マネージャの概要，113 ページ
- スライスの追加，114 ページ
- スライスへのノードとポートの追加，115 ページ
- フロー スペックの追加，115 ページ

スライス マネージャの概要

スライス マネージャは、ネットワークを多くの論理ネットワークにパーティション分割する方法をネットワーク管理者に提供します。この機能を使用すると、複数の分離されたネットワークを作成し、異なるロールおよびアクセス レベルをそれぞれに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。複数の分離されたネットワークは、Cisco Nexus 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 マネージャは、次の基準に基づいてスライスを作成します。

- 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。

- フロー スペック：送信元および宛先 IP、プロトコル、およびスライスに属するトラフィックの識別に使用される送信元ポートおよび宛先トランスポート ポートの組み合わせ。

  関連するネットワーク デバイスとインターフェイスが分離されている場合、フロー スペックはさまざまなスライスに割り当てることができます。

（注） VLAN ID を使用して、スライス トラフィックを分離することもできます。

スライスは、Network Administrator ロールを持つ Cisco Nexus Data Broker ユーザ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が管理できます。

各スライスに少なくとも 1 つの独自の属性が用意されている場合、スライスはオーバーラップできます。たとえば、スライスは同じ物理スイッチとポートを共有できますが、受信するトラフィックのタイプによって区別されます。

スライスの追加

手順

ステップ 1 [Admin] ドロップダウン リストから、[Management] を選択します。

ステップ 2 [Management] の [Admin] ドロップダウン リストから、[Slices] を選択します。

ステップ 3 [Admin] ドロップダウン リストから、[Slices] を選択します。

ステップ 4 [Slices] タブで、[Add Slice] をクリックします。

ステップ 5 [Add Slice] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Slice Name] フィールド	スライスに割り当てる名前。 名前には 1 ～ 256 文字の英数字を含めることができます。使用できる特殊文字は、下線（_）、ハイフン（-）、プラス（+）、等号（=）、縦棒（|）、ピリオド（.）、およびアット マーク（@）です。 （注） 保存後は、スライス名は変更できません。
[Static VLAN] フィールド	スライスに割り当てる静的 VLAN。

ステップ 6 [Add Slice] をクリックします。

スライスへのノードとポートの追加

はじめる前に

ノードとポートを追加するには、スライスをすでに作成してある必要があります。

手順

ステップ 1 [Admin] ドロップダウン リストから、[Management] を選択します。

ステップ 2 [Management] の [Admin] ドロップダウン リストから、[Slices] を選択します。

ステップ 3 [Admin] ドロップダウン リストから、[Slices] を選択します。

ステップ 4 [Slices] タブで、エントリを追加するスライスを選択します。
[Search] コンボ ボックスに値を入力して、検索アイコンをクリックして表示されるエントリ数を制限します。

ステップ 5 トポロジ図で、スライスに追加するノードをクリックします。

ステップ 6 [Add Slice Entr] ダイアログボックスで、スライスに追加するポート（複数可）を選択します。

ステップ 7 [Add Entry] をクリックします。

ステップ 8 スライスに追加するノードおよびポートごとにステップ 3 ～ 5 を繰り返します。

フロー スペックの追加

はじめる前に

フロー スペックを追加する前にスライスを作成します。

（注） デフォルトでは、フロー スペックは双方向です。

手順

ステップ 1 [Admin] ドロップダウン リストから、[Management] を選択します。

ステップ 2 [Management] の [Admin] ドロップダウン リストから、[Slices] を選択します。

ステップ 3 [Admin] ドロップダウン リストから、[Slices] を選択します。

ステップ 4 [Flow Spec] タブで、フロー スペックを追加するスライスを選択します。
[Search] コンボ ボックスに値を入力して、検索アイコンをクリックして表示されるエントリ数を制限します。

ステップ 5 [Detail] タブで、[Add Flow Spec] をクリックします。

ステップ 6 [Add Flow Spec] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Name] フィールド	フロー スペックに使用する名前。 名前には 1 ～ 256 文字の英数字を含めることができます。使用できる特殊文字は、下線「_」、ハイフン「-」、プラス「+」、等号「=」、開き括弧「(」、閉じ括弧「)」、縦棒「|」、ピリオド「.」、およびアット マーク「@」です。
[VLAN] フィールド	フロー スペックに使用する VLAN ID または VLAN ID の範囲。
[Source IP] フィールド	フロー スペックに使用する送信元 IP アドレス。
[Destination IP] フィールド	フロー スペックに使用する宛先 IP アドレス。
[Protocol] フィールド	ユーザがフロー スペックに使用する 10 進数形式の IP プロトコル番号。
[Source Port] フィールド	フロー スペックに使用する送信元ポート。
[Destination Port] フィールド	フロー スペックに使用する宛先ポート。

ステップ 7 [Add Flow Spec] をクリックします。

第 13 章

管理タスク

この章の内容は、次のとおりです。

- AAA サーバの概要，117 ページ
- ユーザとロール，119 ページ
- クラスタ管理情報の表示，122 ページ
- OSGi コンソールの表示，123 ページ
- Northbound API コンテンツの表示，124 ページ
- システム管理，124 ページ
- 設定のバックアップと復元，126 ページ
- 管理者パスワードの回復，127 ページ
- アプリケーション ソフトウェアのアンインストール，128 ページ

AAA サーバの概要

AAA を使用すると、ユーザは誰であるか（認証）、ユーザは何をできるか（権限付与）、およびユーザは何を行ったか（アカウンティング）をセキュリティ アプライアンスで判別できるようになります。Cisco Nexus 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 サーバと通信します。

AAA サーバを使用して、リモート認証と承認がサポートされます。各ユーザを認証するため、Cisco Nexus Data Broker は、ログイン資格情報と属性値（AV）の両方のペアを使用し、ユーザ管理の一部としてユーザに承認済みのロールを割り当てます。認証が正常に行われると、Cisco AV ペアはリソース アクセスの承認のために Cisco Nexus Data Broker に返されます。

AAA サーバの追加

（注） 設定された AAA サーバが到達可能であれば、ユーザの要求はローカルで認証されます。AAA サーバが到達可能であり、ユーザ認証が失敗する場合、ユーザの要求はローカルで認証されていません。

手順

ステップ 1 [Admin] ドロップダウン リストから、[Management] を選択します。

ステップ 2 [Management] の [Admin] ドロップダウン リストから、[AAA] を選択します。

ステップ 3 [Admin] ドロップダウン リストから、[AAA] を選択します。

ステップ 4 [AAA Configuration] ダイアログボックスで、[Add Server] をクリックします。

ステップ 5 [Add AAA Server] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Server Address] フィールド	AAA サーバの IP アドレス。
[Server Secret] フィールド	AAA サーバで設定された共有秘密。
[Protocol] ドロップダウン リスト	AAA サーバのプロトコルを選択します。次のいずれかになります。 • Radius+ • TACACS+

ステップ 6 [Save（保存）] をクリックします。

次の作業

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

RADIUS サーバのユーザ認証の設定

RADIUS サーバのユーザ認証は、Cisco Attribute-Value（av-pair）形式に準拠している必要があります。

手順

RADIUS サーバで、ユーザ用に Cisco av-pair 属性を次のように設定します。
`shell:roles="Network-Admin Slice-Admin"`

AAA サーバの表示

手順

ステップ 1 [Admin] ドロップダウン リストから、[Management] を選択します。
ステップ 2 [Management] の [Admin] ドロップダウン リストから、[AAA] を選択します。
ステップ 3 [Admin] ドロップダウン リストから、[AAA] を選択します。
ステップ 4 [AAA Configuration] ダイアログボックスで、サーバのアドレスをクリックします。
ステップ 5 [Remove AAA Configuration] ダイアログボックスでサーバ情報を確認したら、[Close] をクリックします。
ステップ 6 [AAA Configuration] ダイアログボックスで、[Close] をクリックします。

ユーザとロール

Cisco Nexus Data Broker は、ユーザおよびロールを使用してユーザ アクセスを管理します。特定のユーザに複数のロールを割り当てることができます。次のいずれかになります。

- Network Administrator：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。
- Network Operator：すべてのアプリケーションに対する読み取り専用の権限を提供します。
- Application User：指定されたアプリケーションに定義されている権限を提供します。
- Slice User：指定したスライスにアクセスできます。

各ユーザに 1 つのロールが割り当てられ、それによってユーザの権限が決まります。Slice User はロールとスライスの両方に割り当てられます。デフォルトで、Network Administrator ロールを持つ Admin ユーザは Cisco Nexus Data Broker のインストール時に作成されます。

ユーザ情報の表示

手順

ステップ 1 [Admin] ドロップダウン リストから、[Management] を選択します。

ステップ 2 [Management] の [Admin] ドロップダウン リストから、[Users] を選択します。

ステップ 3 [Admin] ドロップダウン リストから、[Users] を選択します。

ステップ 4 [User Management] ダイアログボックスでは、次の作業を実行できます。

- ユーザ名のリストと各ユーザに割り当てられたロールを表示します。
- ユーザを削除するか、ユーザのパスワードを変更するには、既存のユーザをクリックします。
- 新しいユーザを作成するには、[Add User] をクリックします。

ステップ 5 終了したら、[Close] をクリックします。

ユーザの追加

ユーザを作成した後で、パスワードは変更できますが、ユーザに割り当てられたロールは変更できません。

手順

ステップ 1 [Admin] ドロップダウン リストから、[Management] を選択します。

ステップ 2 [Management] の [Admin] ドロップダウン リストから、[Users] を選択します。

ステップ 3 [Admin] ドロップダウン リストから、[Users] を選択します。

ステップ 4 [User Management] ダイアログボックスで、[Add User] をクリックします。

ステップ 5 [ユーザの追加] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Username] フィールド	ユーザに割り当てる名前。 ユーザ名には、1 ～ 32 文字の英数字を含めることができ、ピリオド（「.」）、スラッシュ、（「/」）、ポンド記号（「#」）、パーセント記号（「%」）、セミコロン（「;」）、疑問符（「?」）、またはバックスラッシュ（「\」）を除く特殊文字を含めることができます。

名前	説明
[Password] フィールド	ユーザのパスワード。 パスワードは 8 ～ 256 文字の長さで、大文字と小文字を含み、少なくとも 1 つの数字と少なくとも 1 つの英数字以外の文字が必要です。
[Choose Role(s)] ドロップダウン リスト	ユーザに割り当てるロールを選択します。複数のロールを割り当てることができます。次のいずれかになります。 • Network Administrator：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。 • Network Operator：すべてのアプリケーションに対する読み取り専用の権限を提供します。 • Application User：指定されたアプリケーションに定義されている権限を提供します。 • Slice User：指定したスライスにアクセスできます。
[Role Name] フィールド	[Application User] を選択した場合、ロールに割り当てる名前を入力します。
[Slices] ドロップダウン リスト	[Slice User] を選択した場合、ユーザに割り当てるスライスを選択します。
[Slice Role] ドロップダウン リスト	[Slice User] を選択した場合、ユーザに割り当てるロールを選択します。次のいずれかになります。 • Administrator：指定したスライスに対する完全な管理者権限を提供します。 • Operator：指定したスライスに対する読み取り専用権限を提供します。
[Assign] ボタン	ユーザにロールを割り当てます。

ステップ 6 [Add User] をクリックします。

ステップ 7 [User Management] ダイアログボックスで、[Close] をクリックします。

既存ユーザのパスワードの変更

手順

ステップ 1 [Admin] ドロップダウン リストから、[Management] を選択します。
ステップ 2 [Management] の [Admin] ドロップダウン リストから、[AAA] を選択します。
ステップ 3 [Admin] ドロップダウン リストから、[Users] を選択します。
ステップ 4 [User Management] ダイアログボックスで、変更するユーザをクリックします。
ステップ 5 [Manage User] ダイアログボックスで、[Change Password] をクリックします。
ステップ 6 [Change Password] ダイアログボックスで、[New Password] および [Verify New Password] フィールドに新しいパスワードを入力します。
ステップ 7 [Submit] をクリックします。
ステップ 8 [Manage User] ダイアログボックスで、[Close] をクリックします。
ステップ 9 [User Management] ダイアログボックスで、[Close] をクリックします。

ユーザの削除

特定のユーザとしてサイン インした場合、そのユーザは削除できません。

手順

ステップ 1 [Admin] ドロップダウン リストから、[Management] を選択します。
ステップ 2 [Management] の [Admin] ドロップダウン リストから、[Users] を選択します。
ステップ 3 [Admin] ドロップダウン リストから、[Users] を選択します。
ステップ 4 [User Management] ダイアログボックスで、変更するユーザをクリックします。
ステップ 5 [Edit User] ダイアログボックスで、[Remove User] をクリックします。
ステップ 6 [User Management] ダイアログボックスで、[Close] をクリックします。

クラスタ管理情報の表示

（注） クラスタ管理ダイアログボックスは読み取り専用です。

（注） ユーザに関連する設定を保存するには、[Management] を選択して [Save] をクリックします。

はじめる前に

クラスタ管理情報を表示するには、高可用性クラスタリングを設定しておく必要があります。ハイ アベイラビリティ クラスタの設定，（23 ページ）を参照してください。

手順

ステップ 1 [Admin] ドロップダウン リストから、[Management] を選択します。

ステップ 2 [Management] の [Admin] ドロップダウン リストから、[AAA] を選択します。

ステップ 3 [Admin] ドロップダウン リストから、[Clusters] を選択します。
[Cluster Management] ダイアログボックスに、クラスタ内のすべての Cisco Nexus Data Broker インスタンスの IP アドレスが表示されます。クラスタは、次のアイコンのいずれかによって示すことができます。

- [*] アイコンは、現在表示されているクラスタ ノードを示します。
- [C] アイコンは、クラスタ ノードがコーディネータであることを示します。

ステップ 4 [Cluster Management] ダイアログボックスで、クラスタを選択します。
[Connected Nodes] ダイアログボックスに、選択したクラスタ内のすべてのノードが表示されます。

ステップ 5 [Connected Nodes] ダイアログボックスで、[Close] をクリックします。

ステップ 6 [Cluster Management] ダイアログボックスで、[Close] をクリックします。

OSGi コンソールの表示

アプリケーションを構成する Cisco Nexus Data Broker バンドルのすべてを、OSGi Web コンソールを表示することで確認できます。

（注） この手順は、[Cisco XNC Bundles] リストの OSGi Web コンソールで実行可能なあらゆる機能の実行手順の詳細を提供するものではありません。これは、OSGi Web コンソールを開き、バンドル情報を表示する手順を示します。

手順

ステップ 1 [Admin] ドロップダウン リストから、[Management] を選択します。

ステップ 2 [Admin] ドロップダウン リストから、[OSGi] を選択します。

ステップ 3 [Management] の [Admin] ドロップダウン リストから、[OSGi] を選択します。
新しいブラウザ タブが開きます。

ステップ 4 ユーザ名とパスワードを入力して、[Enter] キーを押します。
[Cisco – XNC Bundles] リストが表示されます。このページでは、アクティブなパッケージを表示し、バンドル名を指定するためのパッケージ名をフィルタし、その他のタスクを完了することができます。

ステップ 5 リストの表示が完了したら、[Cisco – XNC Bundles] ブラウザ タブを閉じます。

Northbound API コンテンツの表示

メニュー バーの [Northbound API] ツール（本のアイコン）を使用してブラウザのタブを開くことで、アプリケーションのすべての Cisco Nexus Data Broker Northbound API コンテンツを表示できます。

手順

ステップ 1 メニュー バーから、[Northbound API] ボタンをクリックします。
新しいブラウザのタブ（Swagger UI）が開き、Cisco Nexus Data Broker で使用される Northbound API コンテンツの完全なリストが開きます。

このタブから、次の作業を実行できます。

- API の動作の表示化または非表示化。
- API の動作のリスト化。
- API の動作の拡大。

ステップ 2 Northbound API コンテンツの表示が完了したら、ブラウザ タブを閉じます。

システム管理

Cisco Nexus Data Broker のシステム管理機能を使用すると、システムの設定ファイルをダウンロードおよび保存することができます。または、システムの設定ファイルをアップロードおよび復元することができます。また、ログ ファイルをダウンロードすることもできます。

システム ログ ファイルのダウンロード

分析に使用する Cisco Nexus Data Broker のログ ファイルをダウンロードできます。ログ ファイルは、.zip アーカイブ形式で保存されます。

手順

ステップ 1 [Admin] ドロップダウン リストから、[Management] を選択します。

ステップ 2 [Management] の [Admin] ドロップダウン リストから、[System] を選択します。
[System Administration] ダイアログボックスが表示されます。

ステップ 3 [Download Logs] をクリックします。
.zip ファイルを開くか保存するかを尋ねるダイアログボックスがブラウザで開きます。

ステップ 4 次のいずれかを実行します。

- `home/ndbconfig` など、選択した場所にアーカイブを保存します。
- 内容を表示するにはアーカイブを開き、次にそれを保存します。

システム設定ファイルのダウンロード

アップグレードまたは他の変更後にシステムを復元する必要が生じた場合に備えて、Cisco Nexus Data Broker のシステム構成ファイルをダウンロードして保存できます。システム構成ファイルは zip アーカイブに保存されます。

手順

ステップ 1 [Admin] ドロップダウン リストから、[Management] を選択します。

ステップ 2 [Management] の [Admin] ドロップダウン リストから、[System] を選択します。
[System Administration] ダイアログボックスが表示されます。

ステップ 3

ステップ 4 [Download Configuration] をクリックします。
ファイルを開くか保存するかを尋ねるダイアログボックスがブラウザで開きます。

ステップ 5 次のいずれかを実行します。

- `home/ndbconfig` など、選択した場所にアーカイブを保存します。
- 内容を表示するにはアーカイブを開き、次にそれを保存します。

システム設定ファイルのアップロード

障害やその他の事象の発生時には、Cisco Nexus Data Broker の保存済みのシステム設定ファイルをアップロードして、Cisco Nexus Data Broker アプリケーションを復元できます。設定の復元後、Cisco Nexus Data Broker を再起動する必要があります。

はじめる前に

システム設定ファイルをダウンロードし、zip アーカイブに保存します。

手順

ステップ 1 [Admin] ドロップダウン リストから、[Management] を選択します。

ステップ 2 [Management] の [Admin] ドロップダウン リストから、[System] を選択します。
[System Administration] ダイアログボックスが表示されます。

ステップ 3 [Upload Configuration] をクリックします。

ステップ 4 ファイル `configuration_startup.zip` の場所に移動します。

ステップ 5 アーカイブ ファイルをクリックします。
システム設定がアップロードされ、サーバを再起動するように伝えるメッセージがブラウザに表示されます。

ステップ 6 サーバを再起動し、Cisco Nexus Data Broker GUI に再度ログインします。

設定のバックアップと復元

バックアップおよび復元コマンドを使用すると、Cisco Nexus Data Broker の設定をバックアップし、復元することができます。

（注） XNC では、[Device Management] ページからたとえば、パスワード変更や新規ユーザなど、ODL に関連する設定を保存できます。

手順

ステップ 1 Cisco Nexus Data Broker をインストールしたコマンド 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/bin` ディレクトリに移動します。

ステップ 3 **./xnc config --backup** コマンドを入力して設定をバックアップします。

--backup オプションは、現在の xnc ディストリビューションのスタートアップ コンフィギュレーションのバックアップ アーカイブ（.zip 形式）を作成します。バックアップ アーカイブは {xncHome}/backup/ に格納されます。現在のタイムスタンプとファイル名を使用して、バックアップ コマンドが入力されるたびに新しいアーカイブが作成されます。

ステップ 4 **./xnc config --restore --backupfile** {*zip_filename*} コマンドを入力して、設定を復元します。
--restore オプションは、既存のバックアップ アーカイブから現在の xnc ディストリビューションのスタートアップ コンフィギュレーションを復元します。復元アクションには、バックアップ アーカイブの絶対パスが必要です。

ステップ 5 設定を復元する場合は、復元される設定を有効にするために Cisco Nexus Data Broker を停止し、再起動します。

管理者パスワードの回復

Cisco Nexus Data Broker のネットワーク管理者ユーザは、管理者パスワードを工場出荷時の設定に戻すことができます。

（注） このコマンドを使用したとき、ソフトウェアが実行される場合と実行されない場合があります。ソフトウェアが実行されない場合、パスワード リセットは、ソフトウェアが次回実行されたときに有効になります。

手順

ステップ 1 Cisco Nexus Data Broker をインストールした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/bin ディレクトリに移動します。

ステップ 3 **./xnc reset-admin-password** [**--wait-seconds** {*wait_time*} **--password** {*password*}] コマンドを入力して、管理者パスワードをリセットします。
管理者パスワードをデフォルトまたは指定したパスワードにリセットするか、ユーザ マネージャを再起動します。

- **wait-seconds** は、ユーザ マネージャが起動するのを待機する時間の長さ（秒）です。最小は 5 秒、最大は 60 秒です。
- **password** は、管理者パスワードです。

（注）
- パスワードは 8 ～ 256 文字で、大文字と小文字が含まれ、1 つ以上の数字および英数字以外の文字が必要です。
- パスワードを空白のままにすると、工場出荷時のデフォルトである「admin」にリセットされます。
- 管理パスワードをリセットするたびに、新しいパスワードがこれらの要件を必ず満たすようにしてください。そうしないと、Cisco Nexus Data Broker にログインできなくなります。

アプリケーション ソフトウェアのアンインストール

はじめる前に

続行する前に、Cisco Nexus Data Broker アプリケーションが停止していることを確認します。

手順

ステップ 1 Cisco Nexus Data Broker インストールを作成したディレクトリに移動します。
たとえば、ソフトウェアを `Home/CiscoNDB` にインストールした場合、`Home` ディレクトリに移動します。

ステップ 2 `CiscoNDB` ディレクトリを削除します。