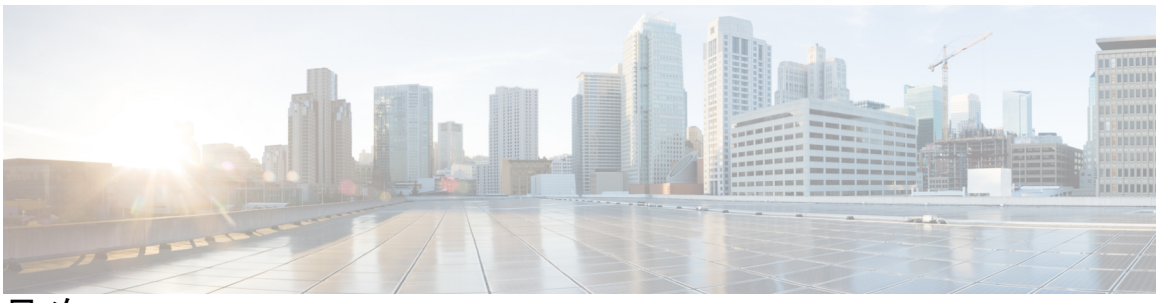
Cisco Catalyst 8000V エッジ ソフトウェア ハイアベイラビリティ コンフィギュレーション ガイド

最終更新：2024 年 10 月 15 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/



目 次

Full Cisco Trademarks with Software License ?

第 1 章

はじめに 1

対象読者および適用範囲 1

機能の互換性 1

表記法 2

通信、サービス、およびその他の情報 3

マニュアルに関するフィードバック 4

トラブルシューティング 4

第 2 章

ハイアベイラビリティの概要 5

ここで章マップを参照します 8

サポートされるトポロジ 8

冗長ノード 9

イベント タイプ 9

第 3 章

ハイ アベイラビリティの設定 11

Cisco IOS XE での IOX とゲストシェルの設定 11

Cisco Catalyst 8000V ルータ間にトンネルを設定 13

Configuring EIGRP over Virtual Tunnel Interfaces 14

Verify the Tunnel Surface 15

BFD ピアルータの設定 15

ハイ アベイラビリティ パッケージのインストール 16

第 4 章 Azure で実行されている Cisco Catalyst 8000V のハイアベイラビリティの設定 17

BFD ピアへのバインディングの作成 18

クラウド固有の冗長性パラメータの設定 18

冗長ノードの作成 19

冗長ノードパラメータの設定 20

冗長ノードパラメータのクリア 20

Cisco Catalyst 8000V ルータの認証 21

システム割り当て管理対象 ID 21

Azure Active Directory サービスプリンシパルを使用した認証 22

アプリケーション ID およびテナント ID の取得 24

アプリケーションの認証キーの作成 25

ゲストシェルでの Azure Active Directory アプリケーションの管理 25

デフォルトアプリケーションのクリア 26

アプリケーションリストのクリア 27

すべてのアプリケーションの管理 27

ルートテーブルの IAM の設定 28

ルートテーブルのエントリタイプ 30

ネットワーク セキュリティ グループの設定 30

第 5 章 Amazon Web Services 上で実行される Cisco Catalyst 8000V でのハイアベイラビリティの設定 33

冗長ノードの作成 34

冗長ノードパラメータの設定 35

冗長ノードパラメータのクリア 35

Cisco Catalyst 8000V ルータの認証 36

送信元/宛先アドレスチェックの無効化 37

ルートテーブルのエントリタイプ 37

セキュリティグループの設定 37

第 6 章 Google Cloud Platform で実行されている Cisco Catalyst 8000V でのハイアベイラビリティの設定 39

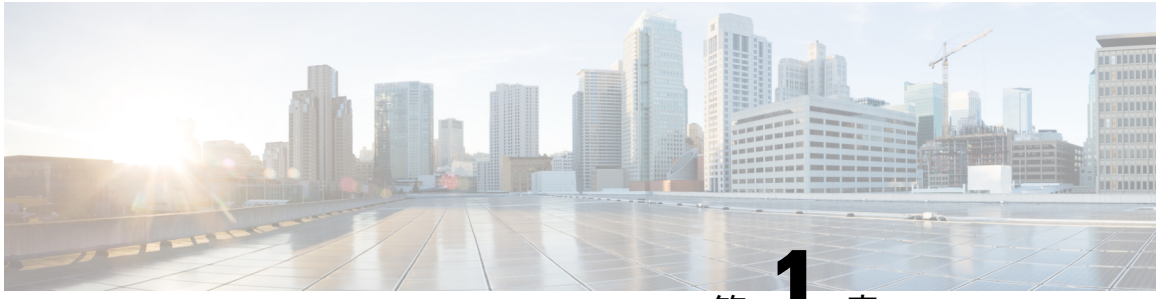
冗長性パラメータのクラウド固有の設定 41
冗長ノードの作成 43
冗長ノードパラメータの設定 43
Cisco Catalyst 8000V ルータの認証 44

第 7 章 設定例 45

第 8 章 ハイアベイラビリティの確認 47

第 9 章 ハイアベイラビリティに関する問題のトラブルシューティング 49

【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。



第 1 章

はじめに

ここでは、このマニュアルの対象読者、構成、および表記法について説明します。また、他のマニュアルの入手方法についても説明します。

この前書きは、次の項で構成されています。

- 対象読者および適用範囲 （1 ページ）
- 機能の互換性 （1 ページ）
- 表記法 （2 ページ）
- 通信、サービス、およびその他の情報 （3 ページ）
- マニュアルに関するフィードバック （4 ページ）
- トラブルシューティング （4 ページ）

対象読者および適用範囲

このドキュメントは、Cisco Enterprise ルータの設定担当者を対象としています。このドキュメントの対象者は、主に次のとおりです。

- ネットワーキングに関する技術的な背景知識と経験を持つお客様。
- ルータベースのインターネットワーキングに関する基本的な知識に精通しているが、Cisco IOS ソフトウェアについては経験の浅いシステム管理者。
- インターネットワーキング装置のインストールと設定を担当しているシステム管理者、および Cisco IOS ソフトウェアに精通しているシステム管理者。

機能の互換性

コンフィギュレーション ガイドで説明されているデバイスで使用可能な機能などの Cisco IOS XE ソフトウェアの詳細については、それぞれのルータのドキュメントセットを参照してください。

特定の機能のサポートを確認するには、Cisco Feature Navigator ツールを使用します。これは、特定のソフトウェアリリース、フィーチャセット、またはプラットフォームをサポートする Cisco IOS XE のソフトウェアイメージを判別できるツールです。

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
^ または **Ctrl**	^ および **Ctrl** シンボルは、Ctrl キーを表します。たとえば、**^D** または **Ctrl+D** というキーの組み合わせは、**Ctrl** キーを押しながら **D** キーを押すことを意味します。キーは大文字で表記されていますが、大文字と小文字の区別はありません。
string	ストリングは、イタリックで示される引用符を付けない一組の文字です。たとえば、SNMP コミュニティ ストリングとして public を設定する場合、ストリングの前後には引用符を使用しません。引用符を使用すると、その引用符も含めてストリングとみなされます。

コマンドシンタックスの説明には、次の表記法を使用しています。

表記法	説明
ボールド	ユーザが入力するコマンドおよびキーワードを示します。
イタリック体	イタリック体の文字は、ユーザが値を指定する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角かっこで囲んで示しています。
|	縦棒で区切られている場合、複数の任意または必須のキーワードまたは引数から、1 つを選択します。
[x | y]	角カッコで囲まれ、縦棒で区切られたキーワードまたは引数は、任意の選択肢です。
{x | y}	波カッコで囲まれ、縦棒で区切られたキーワードまたは引数は、必須の選択肢です。

省略可能または必須の要素内に、さらに省略可能または必須の選択肢を含める場合は、角カッコや波カッコを入れ子にして示しています。たとえば、次の表を参照してください。

表記法	説明
[x {y | z}]	角カッコ内の波カッコおよび縦棒は、任意の要素内の必須の選択肢です。

例では、次の表記法を使用しています。

表記法	説明
`screen`	画面に表示される情報の例は、Courier フォントで表します。
`bold screen`	ユーザの入力が必要なテキストの例は、太字の Courier フォントで表します。
< >	山カッコで囲まれたテキストは、パスワードなど、画面に出力されないテキストを表します。
!	行の先頭にある感嘆符（!）は、コメント行を表します。また、いくつかのプロセスでも、Cisco IOS XE ソフトウェアにより感嘆符が表示されることがあります。
[ ]	角カッコは、システム プロンプトに対するデフォルトの応答です。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

（注） 「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、Cisco Services [英語] にアクセスしてください。

- サービス リクエストを送信するには、Cisco Support [英語] にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco Marketplace にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。

シスコバグ検索ツール

Cisco バグ検索ツール（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理する Cisco バグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。

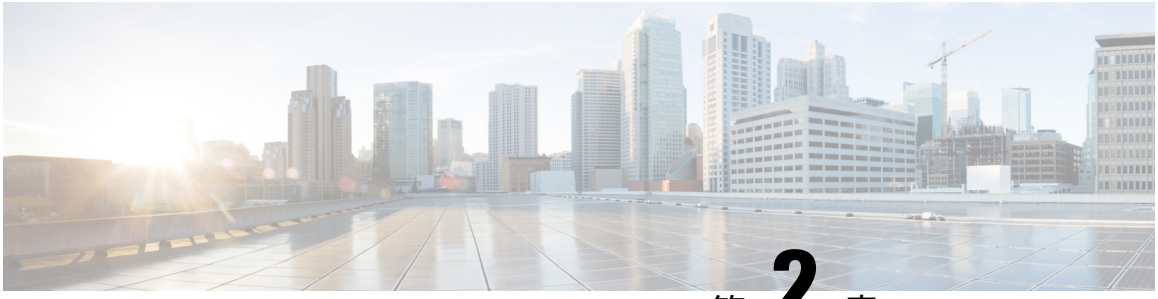
マニュアルに関するフィードバック

シスコのテクニカルドキュメントに関するフィードバックを提供するには、それぞれのオンラインドキュメントの右側のペインにあるフィードバックフォームを使用してください。

トラブルシューティング

トラブルシューティングの最新の詳細情報については、
https://www.cisco.com/c/ja_jp/support/index.html にある Cisco TAC Web サイトを参照してください。

製品カテゴリに移動し、リストから製品を選択するか、製品の名前を入力します。発生している問題に関する情報を見つけるには、**トラブルシュートおよびアラート**を参照してください。



第 2 章

ハイアベイラビリティの概要

ハイアベイラビリティは、2 つのピアルータ間のネットワーキング機能と設定データの冗長性を構築する機能を意味します。このガイドでは、ハイアベイラビリティと、さまざまなクラウド サービス プロバイダーで実行されている Cisco Catalyst 8000V エッジソフトウェア でハイアベイラビリティを設定する方法について説明します。

ハイアベイラビリティ機能は、Microsoft Azure、Google Cloud Platform（GCP）、および Amazon Web Services（AWS）で実行されている Cisco Catalyst 8000V ルータでサポートされています。Cisco Catalyst 8000V の一般的な使用例は、仮想ネットワーク内の 2 つのサブネットを相互接続することです。フロントエンド（パブリック）サブネットとバックエンド（プライベート）サブネットの間に Cisco Catalyst 8000V ルータを展開できます。Cisco Catalyst 8000V ルータは、バックエンドリソースへのアクセスのシングルポイント障害を表します。このシングルポイント障害を軽減するには、2 つのサブネット間に 2 つの Cisco Catalyst 8000V ルータを展開する必要があります。

バックエンドサブネットには、2 つの Cisco Catalyst 8000V インスタンスの 1 つであるネクストホップルータを指すエントリを含むルーティングテーブルが含まれています。ピア Cisco Catalyst 8000V ルータは、Bi-directional Forwarding Detection（BFD）プロトコルを使用してトンネルを介して相互に通信します。ルータとピア間の接続が失われると、BFD はイベントを生成します。このイベントにより、動作しているアクティブルータがルートテーブルのエントリを更新し、ルーティングテーブルがデフォルトルートを指すようにします。

ルーティングテーブルは Cisco Catalyst 8000V ルータのアップストリーム トラフィックを制御し、ルータに設定されているルーティングプロトコルはダウンストリーム トラフィックのパスを決定します。

クラウド環境では、仮想ネットワークは、一元化されたルートテーブルに基づく単純なルーティングメカニズムを実装するのが一般的です。ただし、各ルートテーブルにサブネットが割り当てられている複数のルートテーブルを作成することもできます。このサブネットはルート情報のソースとして機能し、ネットワークトポロジに応じて 1 つ以上の個別のルートを含むルートテーブルが自動的に入力されます。ルートテーブルでルートを設定することもできます。

サブネットには集中型ルートテーブルがあり、2 つの Cisco Catalyst 8000V ルータを冗長モードで動作させることができます。同じ仮想ネットワークに 2 つの Cisco Catalyst 8000V ルータを展開し、それらのインターフェイスを仮想ネットワーク内のサブネットに直接接続できます。

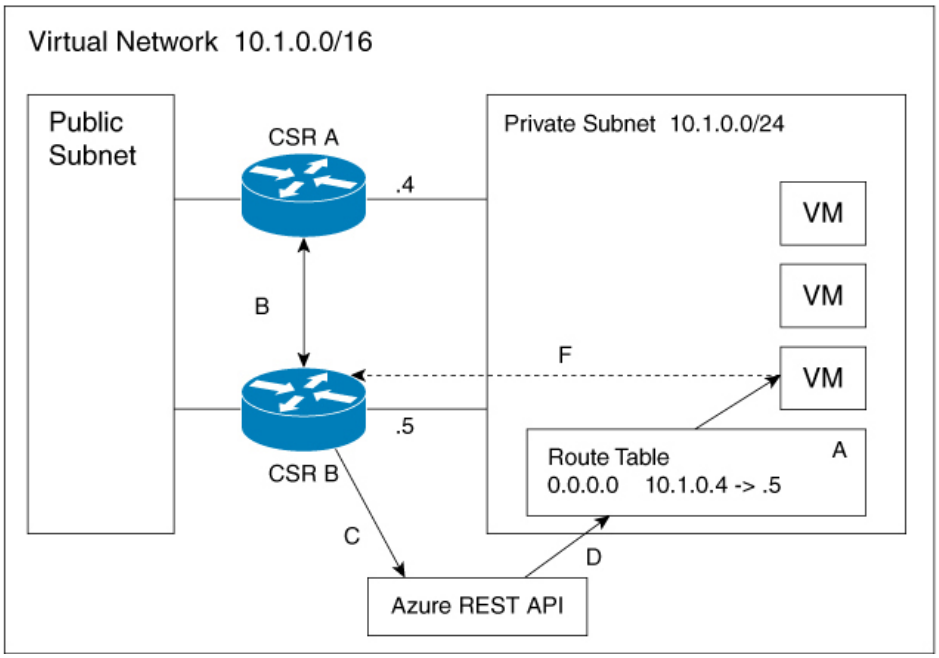
2 つの冗長 Cisco Catalyst 8000V ルータのいずれかを指すルートをルートテーブルに追加できます。常に、2 つの Cisco Catalyst 8000V ルータのいずれかがサブネットのネクストホップルータとして機能します。このルータは、サブネットのアクティブルータです。ピアルータはパッシブルータと呼ばれます。アクティブルータは、特定のルート宛先のネクストホップです。

Cisco Catalyst 8000V ルータは、Bi-directional Failure Detection（BFD）プロトコルを使用して、ピアルータが正常に動作しているかどうかを検出します。2つのピアルータ間にIPトンネルが作成され、各ルータは定期的にBFDプロトコルメッセージを他のルータに送信します。1台のルータがピアからの BFD メッセージの受信に一定期間失敗した場合、アクティブルータはピアルータに障害が発生したと判断します。

アクティブルータに障害が発生した場合、サブネットのルートテーブルを動的に更新して、パッシブルータを参照するように 1 つ以上のルートのネクストホップアドレスを変更できます。ピアルータがアクティブルータの障害を検出すると、ピアルータはプログラム API を使用してルートテーブルエントリを更新します。

ルートテーブルエントリでは、2 つの Cisco Catalyst 8000V ルータのどちらを「プライマリ」ルータにするかを設定します。もう一方のルータは、「セカンダリ」ルータとして設定されている場合はパッシブルータです。デフォルトでは、すべてのルートがセカンダリとして設定されます。

図 *1:* ハイアベイラビリティ - トポロジ



右側のサブネットのアドレスブロックは 12.1.0.0/24 です。このサブネットに接続されている 2 つの Cisco Catalyst 8000V ルータは、このリーフサブネットから出るトラフィックの冗長パスを提供します。サブネットは、サブネットに接続されている仮想マシンにルート情報を提供するルートテーブルに関連付けられます。

次のシナリオを考えてみます。最初に、ルートテーブル内のデフォルトルートに、ネクストホップルータの IP アドレス 12.1.0.4（Cisco Catalyst 8000V A）があります。サブネットから発

信されるすべてのトラフィックは、Cisco Catalyst 8000V A を通過します。Cisco Catalyst 8000V A は現在、デフォルトルートのアクティブルータです。Cisco Catalyst 8000V A で障害が発生すると、Cisco Catalyst 8000V B は Cisco Catalyst 8000V A からの BFD プロトコルメッセージの受信を停止するため、障害を検出します。Cisco Catalyst 8000V B は RESTAPI を介してルートテーブルに書き込み、12.1.0.0/24 サブネット（IP アドレス 12.1.0.5）での Cisco Catalyst 8000V B のインターフェイスへのデフォルトルートを変更します。Cisco Catalyst 8000V B は、15.0.0.0 ネットワークへのルートのアクティブルータになります。

ステップ	説明
A	アドレス 12.1.0.4 の Cisco Catalyst 8000V A は、15.0.0.0 ネットワークのアクティブルータです。
B	Cisco Catalyst 8000V A は失敗します。Cisco Catalyst 8000V B は、BFD プロトコルを使用して障害を検出します。
C	Cisco Catalyst 8000V B は、Azure REST API への HTTP 要求を使用します。
D	Azure は、ユーザー定義のルートテーブルの 15.0.0.0 ルートを Cisco Catalyst 8000V B の IP アドレスに更新します。
E	仮想マシンは、ルートテーブルの更新を確認します。
F	仮想マシンからのパケットは、Cisco Catalyst 8000V B に向けられています。

ハイ アベイラビリティ機能

ハイ アベイラビリティ バージョンは、いくつかの機能をサポートします。Cisco Catalyst 8000V でのハイアベイラビリティの概要を示します。

- **クラウド非依存**：このバージョンのハイアベイラビリティは、任意のクラウド サービス プロバイダーで実行されている Cisco Catalyst 8000V ルータで機能します。クラウドの用語とパラメータにはいくつかの違いがありますが、ハイアベイラビリティ機能を設定、制御、および表示するために使用される一連の関数とスクリプトは、さまざまなクラウド サービス プロバイダー間で共通です。ハイアベイラビリティは、AWS、Azure、および GCP で実行されている Cisco Catalyst 8000V ルータでサポートされています。個々のプロバイダーのクラウドでのハイアベイラビリティの現在のサポートについては、シスコにお問い合わせください。
- **アクティブ/アクティブ動作**：両方の Cisco Catalyst 8000V ルータを同時にアクティブに設定できます。これにより、負荷分散が可能になります。この動作モードでは、ルートテーブル内の各ルートには、2 台のルータのうち 1 台がプライマリルータとして機能し、もう

1 台がセカンダリルータとして機能します。負荷分散を有効にするには、すべてのルートを取得し、2 つの Cisco Catalyst 8000V ルータ間で分割します。

- **障害回復後のプライマリ Cisco Catalyst 8000V への復帰**：Cisco Catalyst 8000V を特定のルートのプライマリルータとして指定できます。この Cisco Catalyst 8000V が稼働している間は、これがルートのネクストホップになります。この Cisco Catalyst 8000V が失敗すると、ピア Cisco Catalyst 8000V がルートのネクストホップを引き継ぎ、ネットワーク接続を維持します。元のルータが障害から回復すると、ルートの所有権を再要求し、ネクストホップルータになります。

- **ユーザー指定のスクリプト**：ゲストシェルは、独自のスクリプトを展開できるコンテナです。HA は、ユーザーが提供するスクリプトにプログラミングインターフェイスを公開します。これは、フェールオーバーと復帰の両方のイベントをトリガーできるスクリプトを作成できるようになったことを意味します。また、独自のアルゴリズムとトリガーを開発して、特定のルートに転送サービスを提供する Cisco Catalyst 8000V を制御することもできます。

- **新しい設定および展開メカニズム**：HA の実装が Cisco IOS XE コードから移動されました。ハイアベイラビリティコードがゲストシェルコンテナで実行されるようになりました。ゲストシェルの詳細については、『Programmability Configuration Guide』の「Guest Shell」セクションを参照してください。冗長ノードの設定は、一連の Python スクリプトを使用してゲストシェルで実行されます。

- ここで章マップを参照します （8 ページ）
- サポートされるトポロジ （8 ページ）
- 冗長ノード （9 ページ）
- イベント タイプ （9 ページ）

ここで章マップを参照します

サポートされるトポロジ

1-for-1 冗長トポロジ：両方の Cisco Catalyst 8000V ルータが同じサブネットに直接接続されている場合、ルータは 1-for-1 冗長性を提供します。この 1-for-1 冗長性の例は前出の図に示されています。Cisco Catalyst 8000V 宛てのすべてのトラフィックは、いずれかのルータ（現在アクティブな Cisco Catalyst 8000V）にのみ送信されます。アクティブな Cisco Catalyst 8000V ルータは、サブネットのネクストホップルータです。もう一方の Cisco Catalyst 8000V ルータは、すべてのルートのパッシブルータです。

負荷分散トポロジ：このトポロジでは、両方の Cisco Catalyst 8000V ルータが同じ仮想ネットワーク内の異なるサブネットに直接接続されています。サブネット A からのトラフィックはルータ A に行き、サブネット B からのトラフィックはルータ B に行きます。これらの各サブネットは、異なるルートテーブルにバインドされています。ルータ A に障害が発生すると、サブネット A のルートテーブルが更新されます。ルータ A がネクストホップになる代わりに、ルートエントリがネクストホップとしてルータ B に変更されます。ルータ B に障害が発生す

ると、サブネット B のルートテーブルが更新されます。ルータ B がネクストホップになる代わりに、ルートエントリがネクストホップとしてルータ A に変更されます。

冗長ノード

冗長ノードは、ルートテーブル内のエントリを指定する一連の設定パラメータです。アクティブルータに障害が発生すると、ルートのネクストホップが更新されます。冗長ノードを設定するには、次の情報が必要です。

- ルートテーブル：クラウド内のルートテーブルの ID。ルートテーブルには、テーブルが作成されたリージョンまたはグループ、テーブルの作成者または所有者の識別子、および特定のテーブルの名前または識別子が含まれます。必要に応じて、テーブル内の個々のルートを指定できます。個々のルートを指定しない場合、冗長ノードはテーブル内のすべてのルートを表します。
- ログイン情報：Cisco Catalyst 8000V ルータの ID の認証。各クラウドプロバイダーは、ログイン情報の取得と指定のプロセスを異なる方法で処理します。
- ネクストホップ—トリガーイベントが発生したときにルートエントリに書き込まれるネクストホップアドレス。ネクストホップは、通常、保護されているサブネット上の Cisco Catalyst 8000V ルータのインターフェイスです。
- ピアルータ：このルータで障害が発生した後に、このルートのトラフィックを転送する冗長ルータを識別します。
- ルータロール—冗長ノードがプライマリロールまたはセカンダリロールのどちらで機能するかを識別します。これは省略可能なパラメータです。この値を指定しない場合、ルータロールはデフォルトでセカンダリロールになります。

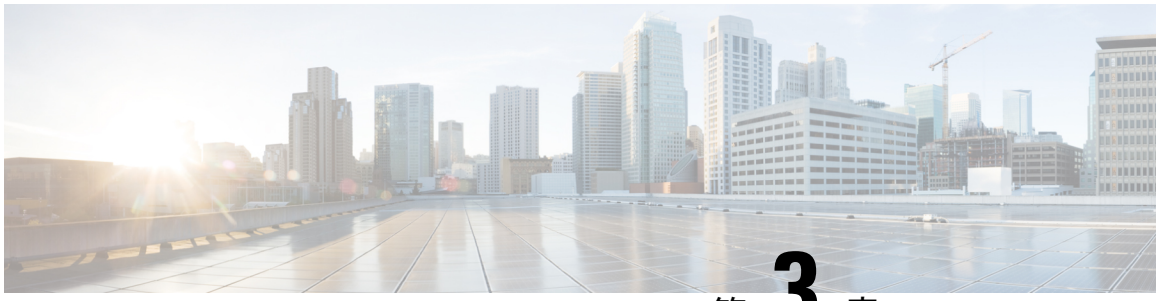
イベントタイプ

ハイアベイラビリティ機能は、次の 3 種類のイベントを認識して応答します。

- **ピアルータ障害**：ピアルートに障害が発生すると、ピアルータ障害イベントとして検出されます。このイベントに応答して、イベントハンドラは、冗長ノードで定義されているネクストホップアドレスを使用してルートエントリを書き込みます。このイベントを生成できるようにするには、ピアルータに BFD プロトコルを設定し、クラウドのハイアベイラビリティのために冗長性の下で BFD ピアを関連付けます。
- **プライマリルータに戻す**：ルータが障害から回復した後、プライマリルータに戻すイベントが発生します。このイベントの目的は、ルートのプライマリルータがアクティブルータとして再確立されるようにすることです。このイベントはタイマーによってトリガーされ、このイベントを設定する必要はありません。ルートテーブルエントリでは、イベントハンドラは、ルートに現在設定されているネクストホップアドレスと異なる場合にのみ、冗長ノードで定義されているネクストホップアドレスを変更します。

このプライマリルータに戻すイベントは、ゲストシェル環境で CRON ジョブを使用して定期的に生成されます。ジョブは5分ごとに実行されるようにスケジュールされ、プライマリモードで設定されている各冗長ノードに、このルータのネクストホップインターフェイスがルートテーブルに設定されているかどうかを確認します。ルートテーブルエントリがすでにこのルータのネクスト ホップ インターフェイスを指している場合、更新は必要ありません。モードパラメータの冗長ノード設定がセカンダリの場合、プライマリルータに戻すイベントは無視されます。

- **冗長ノードの検証**：イベントハンドラは、冗長ノードの検証イベントを検出し、冗長ノードによって指定されたルートエントリを読み取ります。イベントハンドラは、同じデータをルートエントリに書き戻します。このイベントは、自動的またはアルゴリズム的に生成されません。このイベントは、イベントハンドラが機能を実行できるかどうかを確認します。手動またはプログラムでスクリプトを実行して、冗長ノード検証イベントをトリガーします。検証イベントの詳細については、「Advanced Programming for High Availability on Microsoft Azure」セクションの「User-Defined Triggers」を参照してください。



第 3 章

ハイ アベイラビリティの設定

次のセクションでは、任意のクラウド サービス プロバイダーで実行されている Cisco Catalyst 8000V のハイアベイラビリティを設定するための一般的な設定手順を示します。

- Cisco IOS XE での IOX とゲストシェルの設定 （11 ページ）
- Cisco Catalyst 8000V ルータ間にトンネルを設定 （13 ページ）
- Configuring EIGRP over Virtual Tunnel Interfaces （14 ページ）
- Verify the Tunnel Surface （15 ページ）
- BFD ピアルータの設定 （15 ページ）
- ハイ アベイラビリティ パッケージのインストール （16 ページ）

Cisco IOS XE での IOX とゲストシェルの設定

次の Cisco IOS XE 設定は、ゲストシェルにアクセスするために必要なコマンドを示しています。これらの前提条件は startup-config ファイルに自動的に含まれるため、設定する必要はありません。

手順の概要

1. 次の設定を実行します：
2. ハイアベイラビリティを設定するには、IOX が設定され、実行されているかどうかを確認する必要があります。
3. 次のコマンドを入力して、ゲストアプリケーションが定義され、実行されていることを確認します。

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	次の設定を実行します： 例：	

	コマンドまたはアクション	目的
	iox ip nat inside source list GS_NAT_ACL interface GigabitEthernet1 vrf GS overload ip route vrf GS 0.0.0.0 0.0.0.0 GigabitEthernet1 192.168.35.1 global interface VirtualPortGroup0 vrf forwarding GS ip address 192.168.35.101 255.255.255.0 ip nat inside no mop enabled no mop sysid ip access-list standard GS_NAT_ACL permit 192.168.35.0 0.0.0.255 app-hosting appid guestshell app-vnic gateway1 virtualportgroup 0 guest-interface 0 guest-ipaddress 192.168.35.102 netmask 255.255.255.0 app-default-gateway 192.168.35.101 guest-interface 0 name-server0 8.8.8.8	
ステップ 2	ハイアベイラビリティを設定するには、IOX が設定され、実行されているかどうかを確認する必要があります。 **例**： show iox Virtual Service Global State and Virtualization Limits: Infrastructure version : 1.7 Total virtual services installed : 0 Total virtual services activated : 0 Machine types supported : LXC Machine types disabled : KVM Maximum VCPUs per virtual service : 1 Resource virtualization limits: Name Quota Committed Available --- system CPU (%) 75 0 75 memory (MB) 3072 0 3072 bootflash (MB) 20000 0 5745 IOx Infrastructure Summary: --- IOx service (CAF) : Running IOx service (HA) : Not Running IOx service (IOxman) : Running Libvirtd : Running	
ステップ 3	次のコマンドを入力して、ゲストアプリケーションが定義され、実行されていることを確認します。 **例**： show app-hosting list show app-hosting list App id State --- guestshell RUNNING	ゲストシェルの状態が前述のコマンドの出力で DEPLOYED と表示されている場合は、次のコマンドを使用してゲストシェルを有効にする必要があります。 guestshell enable Interface will be selected if configured in app-hosting Please wait for completion guestshell activated successfully Current state is: ACTIVATED guestshell started successfully Current state is: RUNNING Guestshell enabled successfully

Cisco Catalyst 8000V ルータ間にトンネルを設定

Cisco Catalyst 8000V ルータ間にトンネルを設定し、ピア障害検出のためにトンネルで双方向フォワーディング検出（BFD）およびルーティングプロトコル（EIGRP または BGP）を有効にする必要があります。ネットワークを通過する IP トラフィックを認証および暗号化するには、IPsec トンネルまたは VxLAN GPE トンネルを使用します。

手順

ステップ 1 IPsec トンネルを設定するには、コンフィギュレーション モード コマンドを入力して、次の設定を行います。crypto isakmp policy 1 コマンドは、プライオリティが高い（1）IKE ポリシーを定義し、config-isakmp コンフィギュレーション モードを開始します。

例：

```
Crypto isakmp policy 1
encr aes 256 authentication pre-share
crypto isakmp key cisco address 0.0.0.0
!
crypto ipsec transform-set uni-perf esp-aes 256 esp-sha-hmac mode tunnel
!
crypto ipsec profile vti-1
set security-association lifetime kilobytes disable set security-association lifetime seconds 86400
  set transform-set uni-perf
set pfs group2
!
interface Tunnel1
ip address 192.168.101.1 255.255.255.252
load-interval 30
tunnel source GigabitEthernet1 tunnel mode ipsec ipv4
tunnel destination 23.96.91.169 tunnel protection ipsec profile vti-1
bfd interval 100 min_rx 100 multiplier 3
```

ステップ 2 VxLAN GPE トンネルを作成するには、次の設定を入力します

```
interface Tunnel100
ip address 192.168.101.1 255.255.255.0
bfd interval 100 min_rx 100 multiplier 3 tunnel source GigabitEthernet1
tunnel mode vxlan-gpe ipv4 tunnel destination 40.114.93.164
tunnel vxlan vni 10000
```

VxLAN GPE トンネルの設定の詳細については、『Carrier Ethernet Configuration Guide』を参照してください。

トンネル宛先アドレスは、対応する Cisco Catalyst 8000V のパブリック IP アドレスである必要があります。トンネル IP アドレスには、任意の一意の IP アドレスを使用します。ただし、各冗長 Cisco Catalyst 8000V のトンネルエンドポイントは同じサブネット内にある必要があります。

（注） VxLANがトンネルを介してトラフィックを通過できるようにするには、クラウドのネットワーク セキュリティ グループでUDP ポート4789および4790が許可されていることを確認する必要があります。ネットワークセキュリティフィルタの設定については、クラウドプロバイダーのドキュメントを参照してください。

Configuring EIGRP over Virtual Tunnel Interfaces

次の手順を使用して、仮想トンネルインターフェイスを介して EIGRP を設定します。

（注） 次の手順で使用されるプロトコルである EIGRP を使用する以外に、BGP または OSPF を使用するオプションもあります。

始める前に

Cisco Catalyst 8000V ルータ間に VxLAN または IPsec トンネルを設定します。

手順

ステップ 1 **router eigrp** *as-number*

例：

```
Device(config)# router eigrp 1
```

EIGRP ルーティングプロセスを有効にし、ルータ コンフィギュレーション モードを開始します。

ステップ 2 **network** *ip-address subnet-mask*

EIGRP を使用してトンネルのネットワークを共有します。

例：

```
network 192.168.101.0 0.0.0.255
```

ステップ 3 **bfd all-interfaces**

EIGRP ルーティングプロセスに関連付けられたすべてのインターフェイスで、BFD をグローバルに有効にします。

例：

```
Device(config-router)# bfd all-interfaces
```

ステップ 4 **end**

ルータ コンフィギュレーション モードを終了し、ルータの特権 EXEC モードに戻ります。

例：

```
Device(config-router)# end
```

ステップ 5 show bfd neighbors

BFD ネイバーがアクティブになっていることを確認し、BFD が登録されているルーティング プロトコルを表示します。

例：

```
Device# show bfd neighbors

IPv4 Sessions
NeighAddr      LD/RD        RH/RS    State  Int
192.168.101.2  4097/4097    Up       Up     Tu100
```

Verify the Tunnel Surface

手順

トンネルインターフェイスが設定され、有効になっていることを確認するには、`show ip interface brief` コマンドを実行します。

例：

```
# show ip interface brief
 IP-Address OK? Method Status Protocol
GigabitEthernet1 192.168.35.20 YES DHCP up up
GigabitEthernet2 192.168.36.12 YES DHCP up up
Tunnel1                172.17.1.1         YES NVRAM      up up
VirtualPortGroup0 192.168.35.101     YES NVRAM      up up
```

BFD ピアルータの設定

手順

次のコマンドを実行します。

例：

```
redundancy
cloud-ha bfd peer <peer_router_ip_address>
```

このコンフィギュレーション コマンドは、ピアルータを識別します。IP アドレスは、2 つの Cisco Catalyst 8000V ルータ間で BFD プロトコルを伝送するトンネル内のピア Cisco Catalyst 8000V の IP アドレスです。

ハイ アベイラビリティ パッケージのインストール

手順

ステップ 1 `#Router> guestshell` コマンドを実行して、ゲストシェルを開始します。

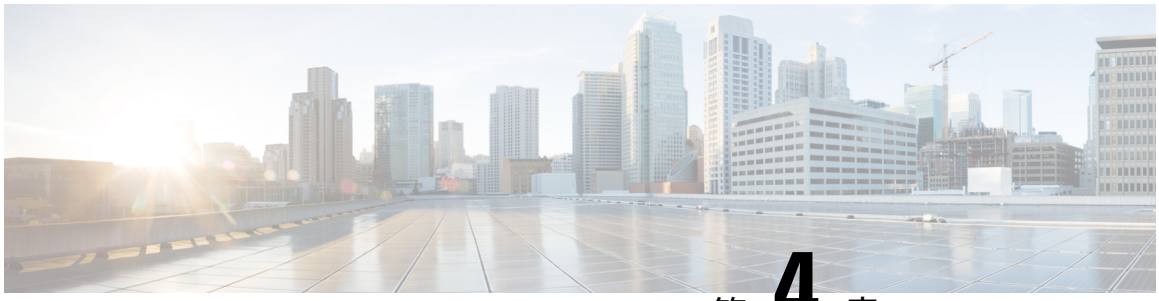
ステップ 2 Cisco Catalyst 8000V インスタンスが実行されているクラウドプロバイダーに基づいて、適切な Python パッケージをインストールします。

クラウドプロバイダー	パッケージ名
Microsoft Azure	csr_azure_ha
Amazon Web Services	csr_aws_ha
Google Cloud Platform	csr_gcp_ha

（注） Microsoft Azure のパッケージ名は、HAv2 と HAv3 の両方で同じです。`pip install csr_azure_ha --user` コマンドを実行してインストールを実行すると、最新の HA V3 がダウンロードされます。

ステップ 3 `[guestshell@guestshell]$ pip install <package_name> --user` コマンドを使用して、クラウドサービスプロバイダーに適したパッケージをインストールします。

ステップ 4 ホームディレクトリから、`cloud:[guestshell@guestshell]$ cd cloud` という名前のサブディレクトリに移動します。



第 4 章

Azure で実行されている Cisco Catalyst 8000V のハイアベイラビリティの設定

ハイアベイラビリティは、Cisco IOS XE 17.4 リリース以降の Cisco Catalyst 8000V でサポートされています。

- BFD ピアへのバインディングの作成 （18 ページ）
- クラウド固有の冗長性パラメータの設定 （18 ページ）
- 冗長ノードの作成 （19 ページ）
- 冗長ノードパラメータの設定 （20 ページ）
- 冗長ノードパラメータのクリア （20 ページ）
- Cisco Catalyst 8000V ルータの認証 （21 ページ）
- システム割り当て管理対象 ID （21 ページ）
- Azure Active Directory サービスプリンシパルを使用した認証 （22 ページ）
- アプリケーション ID およびテナント ID の取得 （24 ページ）
- アプリケーションの認証キーの作成 （25 ページ）
- ゲストシェルでの Azure Active Directory アプリケーションの管理 （25 ページ）
- デフォルトアプリケーションのクリア （26 ページ）
- アプリケーションリストのクリア （27 ページ）
- すべてのアプリケーションの管理 （27 ページ）
- ルートテーブルの IAM の設定 （28 ページ）
- ルートテーブルのエントリタイプ （30 ページ）
- ネットワーク セキュリティ グループの設定 （30 ページ）

BFD ピアへのバインディングの作成

手順

IOS XE リリース 17.4 以降でハイアベイラビリティを設定する場合は、次のコマンドを実行して BFD ピアへのバインディングを作成できます。

例：

```
redundancy
cloud-ha bfd peer <peerIpAddress>
```

クラウド固有の冗長性パラメータの設定

次の表に、Microsoft Azure に固有の冗長パラメータを示します。

パラメータスイッチ	スイッチ	説明
ノードインデックス	-i	このノードを一意に識別するために使用されるインデックス。有効な値は 1 ～ 255 です。
クラウドプロバイダー	-p	Azure クラウドのタイプ（azure、azusgov、または azchina）を指定します。
サブスクリプション ID	-s	Azure サブスクリプション ID。
リソース グループ名（Resource Group Name）	-g	更新するルートテーブルの名前。
ルートテーブル名	-t	更新するルートテーブルの名前。
Route	-r	更新されるルートの CIDR 形式での IP アドレス。IPv4 または IPv6 アドレスにできます。 ルートが指定されていない場合、冗長ノードは「仮想アプライアンス」タイプのルーティングテーブル内のすべて

パラメータスイッチ	スイッチ	説明
		のルートに適用されると見なされます。
ネクスト ホップ アドレス	-n	ネクストホップルータの IP アドレス。このルートテーブルを使用するサブネット上のこの Cisco Catalyst 8000V に割り当てられている IP アドレスを使用します。IPv4 または IPv6 アドレスにできます。
モード	-m	このルータが、このルートを処理するためのプライマリルータかセカンダリルータかを示します。デフォルト値は secondary です。

冗長ノードの作成

手順

次のスクリプトを実行して冗長ノードを作成し、データベースに追加します：`create_node { switch value } […[{ switch value }]`。

有効な冗長ノードには、次のパラメータを設定する必要があります。

- ノードインデックス
- クラウドプロバイダー
- サブスクリプション ID
- リソース グループ名（Resource Group Name）
- ルートテーブル名

```
create_node -i 10 -p azure -s b0b1a9e2-4444-4ca5-acd9-bebd1e6873eb -g ds-rg -t ds-sub2-RouteTable
-r 15.0.0.0/8 -n 192.168.7.4
```

設定が成功すると、スクリプトはゼロの値を返します。

冗長ノードパラメータの設定

手順

	コマンドまたはアクション	目的
ステップ 1	既存の冗長ノードのパラメータの値を変更するには、`set_params{ switch value } [...[{ switch value }]` スクリプトを実行します。 例： `set_params.py -i 10 -r 15.0.0.0/16 -n 192.168.7.5`	インデックスパラメータ（-i）は必須です。このコマンドは、指定されたパラメータの値を設定します。指定したパラメータが冗長ノードにすでに定義されている場合は、パラメータの値が更新されます。 `set_params -i 10 -n 192.168.7.5 -m primary` この例では、インデックス 10 の冗長ノードのネクストホップアドレスとモードが更新されます。 この設定が成功すると、スクリプトはゼロの値を返します。

冗長ノードパラメータのクリア

手順

既存の冗長ノードの指定されたパラメータの値をクリアする場合は、`clear_params -i value { switch } [...[{ switch }]` スクリプトを実行します。

例：

```
clear_params -i 10 -r -n
```

この例では、clear_params スクリプトはルートパラメータとネクスト ホップ アドレス パラメータの両方をクリアします。

関連する値をクリアする場合は、switch パラメータだけを指定します。パラメータの現在の値は含めないでください。

（注） index パラメータのみが必要です。指定された追加パラメータの値はクリアされます。

クリアに成功すると、スクリプトはゼロの値を返します。

Cisco Catalyst 8000V ルータの認証

Azure ネットワークのルーティングテーブルを更新するには、まず Cisco Catalyst 8000V ルータを認証する必要があります。これは、Azure Active Directory で Cisco Catalyst 8000V ルータを表すアプリケーションを作成することによって実現されます。権限が付与されたアプリケーションを使用して、Azure ネットワークリソースにアクセスできます。

次の 2 つのメカニズムを使用してアプリケーションを作成できます。

- システム割り当ての管理対象 ID：Azure は自動的にアプリケーションを作成し、それをルータにバインドします。このメカニズムは、以前は Azure による管理対象サービス ID と呼ばれていました。
- Azure Active Directory への手動アプリケーション登録：ここでは、ユーザーは Cisco Catalyst 8000V ルータを表すアプリケーションを Azure Active Directory に作成します。

ルータを表すアプリケーションを作成することで、Azure Active Directory で管理対象 ID を手動で作成できます。アプリケーションには、テナント ID、アプリケーション ID、およびアプリケーションキーの、一連の識別子が割り当てられます。これらのアプリケーション識別子は、デフォルトの AAD アプリケーションとして、または個々の冗長ノード内のいずれかで、ハイアベイラビリティ機能で設定する必要があります。

または、Cisco Catalyst 8000V を作成するときに、Cisco Catalyst 8000V インスタンスのシステム割り当て管理対象 ID を作成するように Azure を構成できます。この場合、ハイアベイラビリティ機能でアプリケーション識別子を設定する必要はありません。つまり、アプリケーションのテナント ID、アプリケーション ID、およびアプリケーションキーの設定がない場合、ハイアベイラビリティ機能は、Cisco Catalyst 8000V ルータがシステム割り当ての管理対象 ID を使用していると想定します。

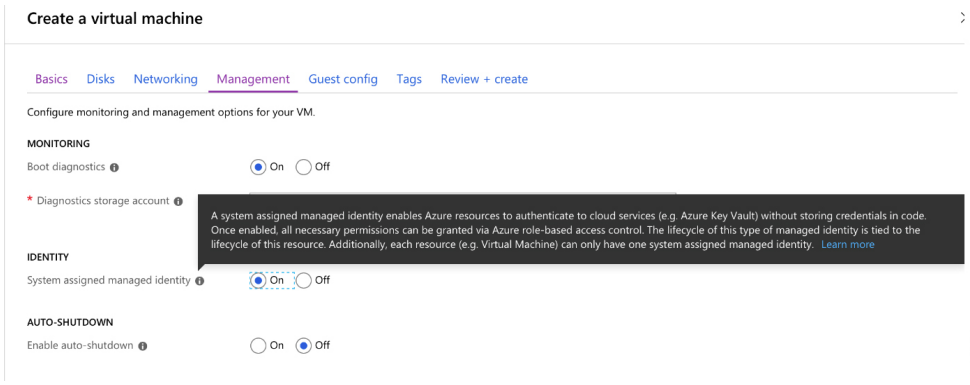
システム割り当て管理対象 ID

Cisco Catalyst 8000V ルータを作成するときに、Azure によってシステム管理対象 ID が割り当てられるように有効にすることができます。Azure Marketplace から Cisco Catalyst 8000V ルータを作成するには、次の 2 つの方法があります。

- ソリューションテンプレート：Cisco Catalyst 8000V ルータは他の Azure リソースとともに作成され、1 つのステップでネットワーキング ソリューションが作成されます。
- スタンドアロン：スタンドアロン Cisco Catalyst 8000V は、通常は既存の仮想ネットワーク内に、基本 Cisco Catalyst 8000V イメージを使用して作成されます。

Azure マーケットプレイスで提供されているソリューションテンプレートのいずれかを使用して Cisco Catalyst 8000V ルータを作成すると、Cisco Catalyst 8000V のシステム割り当ての管理対象 ID がデフォルトで有効になります。基本 Cisco Catalyst 8000V イメージを使用してスタンドアロン Cisco Catalyst 8000V を作成すると、次の図に示すように、システム管理対象 ID が有効になります。

図 *2:* システム管理対象 *ID* の有効化



Azure Active Directory サービスプリンシパルを使用した認証

このセクションでは、Microsoft Azure Resource Manager API にアクセスする権限を持つ Microsoft Azure Active Directory でアプリケーションを作成する方法について説明します。

手順の概要

1. Microsoft Azure のドキュメントで、Azure Active Directory へのアプリケーションの登録に関する最新の手順を参照してください。https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-v1-add-azure-ad-app も参照してください。
2. https://portal.azure.com にアクセスして、Microsoft Azure のポータルに移動します。
3. アカウント名を選択し、Microsoft Azure パスワードを使用してサインインします。
4. 左側のナビゲーションで、[Azure Active Directory] をクリックし、メインペインで [Active Directory] を選択します。ペインの上部にある [Switch Directory] をクリックして、[Active Directory] を選択します。
5. 新しいアプリケーションを作成する権限があるかどうかを確認します。Azure Active Directory でのアプリケーションの作成については、次の Microsoft Azure のドキュメントを参照してください。ポータルを使用してリソースにアクセスできる Azure Active Directory アプリケーションとサービスプリンシパルを作成します。
6. 使用する Active Directory に移動します。
7. 新しいアプリケーションを作成するには、[Create] > [New Application Registration] を選択します。
8. アプリケーションの名前を指定し、アプリケーションタイプとして [Web App/API] が選択されていることを確認します
9. サインオン URL を指定します。URI 形式のサインオン URL の名前を使用しますが、到達可能である必要はありません。次の形式の文字列を使用できます：`http://<your_directory_domain_name>/<app_name>` 。たとえば、アプリケー

ション名が myapp で、ディレクトリのドメイン名が \mydir.onmicrosoft.com の場合、サインオン URL は http://mydir.onmicrosoft.com/myapp です。

10. [Create] をクリックします。
11. [Azure Active Directory] ページに移動します。作成したアプリケーションを検索します。割り当てられたアプリケーション ID をメモします。

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	Microsoft Azure のドキュメントで、Azure Active Directory へのアプリケーションの登録に関する最新の手順を参照してください。https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-v1-add-azure-ad-app も参照してください。	
ステップ 2	https://portal.azure.com にアクセスして、Microsoft Azure のポータルに移動します。	
ステップ 3	アカウント名を選択し、Microsoft Azure パスワードを使用してサインインします。	
ステップ 4	左側のナビゲーションで、[Azure Active Directory] をクリックし、メインペインで [Active Directory] を選択します。ペインの上部にある [Switch Directory] をクリックして、[Active Directory] を選択します。	
ステップ 5	新しいアプリケーションを作成する権限があるかどうかを確認します。Azure Active Directory でのアプリケーションの作成については、次の Microsoft Azure のドキュメントを参照してください。ポータルを使用してリソースにアクセスできる Azure Active Directory アプリケーションとサービスプリンシパルを作成します。	
ステップ 6	使用する Active Directory に移動します。	
ステップ 7	新しいアプリケーションを作成するには、[Create] > [New Application Registration] を選択します。	
ステップ 8	アプリケーションの名前を指定し、アプリケーションタイプとして [Web App/API] が選択されていることを確認します	
ステップ 9	サインオン URL を指定します。URI 形式のサインオン URL の名前を使用しますが、到達可能である必要はありません。次の形式の文字列を使用でき	

	コマンドまたはアクション	目的
	ます： http://<your_directory_domain_name>/<app_name>。たとえば、アプリケーション名が myapp で、ディレクトリのドメイン名が \mydir.onmicrosoft.com の場合、サインオン URL は http://mydir.onmicrosoft.com/myapp です。	
ステップ 10	[Create] をクリックします。	
ステップ 11	[Azure Active Directory] ページに移動します。作成したアプリケーションを検索します。割り当てられたアプリケーション ID をメモします。	

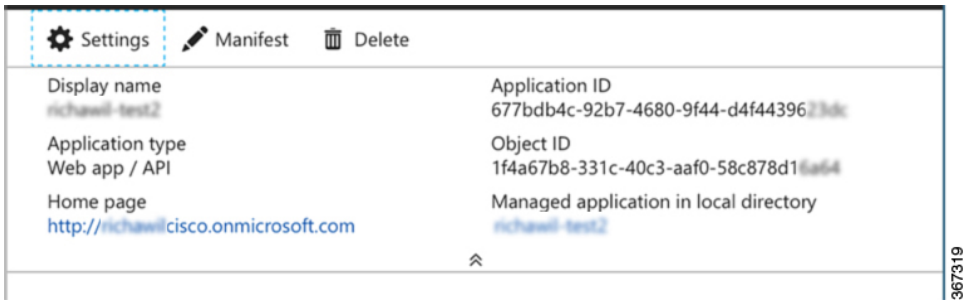
アプリケーション ID およびテナント ID の取得

始める前に

Microsoft Azure Active Directory でアプリケーションを作成します。

手順

ステップ 1 アプリケーションを作成すると、次の図に示すように、登録されたアプリケーションが画面に表示されます。



ステップ 2 ポータルを使用してリソースにアクセスできる Azure Active Directory アプリケーションとサービスプリンシパルを作成します。アプリケーション ID をメモします。Microsoft ドキュメントの「Get application ID and authentication key」セクションのステップ 2 を参照してください。

ステップ 3 [Azure Active Directory] を選択します。

ステップ 4 [プロパティ（Properties）] を選択します。[Directory ID] フィールドの値をメモします。これはテナント ID です。

アプリケーションの認証キーの作成

手順

ステップ 1 Microsoft Azure ポータルから、[Azure Active Directory] を選択します。

ステップ 2 [App Registration] を選択します。

ステップ 3 [Obtain the Application ID and Tenant ID] セクションで以前に作成したアプリケーションを選択します。

ステップ 4 [設定（Settings）] をクリックします。

ステップ 5 API アクセス用のキーを作成するには、[Keys] を選択し、[Duration] の値を指定します。[Duration] は、キーが無効になるまでの時間の長さです。

ステップ 6 [Value] フィールドの API キーをメモします。

注意 API キーは後で取得できないため、慎重に保管してください。

ステップ 7 API キーを URL のエンコードされていない形式に変換する必要があります。適切な変換ツールを見つけるには、URL エンコーダをインターネット検索エンジンに入力します。Microsoft Azure での Cisco Catalyst 8000V の障害検出の設定などの手順では、エンコードされていない API キーが必要になる場合があります。

例：

```
URL encoded API Key:   5yOhH593dtD%2FO8gzAlWgulrkWz5dH02d2STk3LdbI4c%3D
         URL unencoded API Key:  5yOhH593dtD/O8gzAlWgulrkWz5dH02d2STk3LdbI4c=
```

ゲストシェルでの Azure Active Directory アプリケーションの管理

ユーザー割り当ての ID として手動で作成されたか、またはシステム割り当ての ID かにかかわらず、Azure Active Directory 内のアプリケーションを管理するためにゲストシェル環境で実行できる一連のユーティリティスクリプトがあります。次の項では、これらのスクリプトの使用方法と、Cisco Catalyst 8000V ルータの認証に使用される冗長ノードとアプリケーション間のバインディングを設定する方法について説明します。

- ユーザー定義アプリケーションの管理：Cisco Catalyst 8000V ルータにユーザー割り当て ID を使用することを選択した場合は、Azure Active Directory で作成されたアプリケーションをハイアベイラビリティ機能で設定する必要があります。アプリケーションは、すべての冗長ノードまたは個々の冗長ノードに使用されるデフォルトのアプリケーションとして設定できます。
- デフォルトアプリケーションの設定：`set_default_aad_app` スクリプトを使用して、ユーザー割り当てのアプリケーションをデフォルトアプリケーションとして設定すると、冗長

ノードに個別のアプリケーションが設定されていない限り、すべての冗長ノードで指定されたアプリケーションが認証に使用されます。

デフォルトアプリケーションの設定

`set_default_aad_app.py{ switch value } […[{ switch value }]` スクリプトを実行して、デフォルトのアプリケーションを設定します。AAD 冗長ノードのパラメータについては、次の表を参照してください。

パラメータ名	スイッチ	説明
クラウドプロバイダー	-p	使用中の Azure クラウドを指定します {azure | azusgov | azchina}
テナント ID	-d	AAD インスタンスを識別します。
Application ID	-a	AAD 内のアプリケーションを識別します。
アプリケーションキー	-k	アプリケーション用に作成されたアクセスキー。キーは、エンコードされていない URL 形式で指定する必要があります。

```
[guestshell@guestshell]$ set_default_aad_app.py -p azure -d
c4426c0b-036f-4bfb-b2d4-5c910c5389d6 -a 3d6e2ef4-8160-4092-911d-53c8f68ba808 -k
hZFvMGfzJuwFiukez27e/duyztom1bj7QL0Yix+KY9c=
```

```
[guestshell@guestshell]$ set_default_aad_app.py -h
usage: set_default_aad_app.py [-h] -p {azure,azusgov,azchina} -a A -d D -k K
AAD Application
required arguments:
  -p {azure,azusgov,azchina} <cloud_provider> {azure | azusgov | azchina}
  -a A                    to add the applicationId
  -d D                    to add the tenantId
  -k K                    to add the applicationKey
```

デフォルトアプリケーションのクリア

デフォルトのユーザー割り当てアプリケーション設定をクリアするには、`clear_default_aad_app` スクリプトを使用します。

```
[guestshell@guestshell]$ clear_default_aad_app.py
```

アプリケーションリストのクリア

ユーザー割り当てアプリケーションを作成し、そのアプリケーションを個々の冗長ノードに関連付けると、これらのアプリケーションに関する情報がメモリにキャッシュされます。`show_auth_applications.py` スクリプトを使用して、既知のアプリケーションのリストを表示できます。clear_aad_application_list スクリプトを使用してキャッシュをクリアします。

```
[guestshell@guestshell]$ clear_aad_application_list.py
```

すべてのアプリケーションの管理

次のスクリプトを使用して、すべてのアプリケーション（ユーザー割り当てまたはシステム割り当て）を管理します。

認証アプリケーションの表示

Cisco Catalyst 8000V ルータは、設定されたアプリケーションのリストを保持します。このリストは、show_auth_applications スクリプトを使用して表示できます。

```
[guestshell@guestshell]$ show_auth_applications.py
```

認証トークンのクリア

冗長ノードでイベントがトリガーされると、Cisco Catalyst 8000V ルータは設定されたアプリケーションを使用して、Azure ネットワークから認証トークンを取得します。このトークンは、ルータに最大 5 分間キャッシュされます。`clear_token` スクリプトを使用して、キャッシュされたトークンをクリアできます。

このスクリプトは、デフォルトのユーザー割り当てアプリケーションまたはシステム割り当てアプリケーションのいずれかをクリアします。このスクリプトは、個々の冗長ノードで明示的に設定されているユーザー割り当てアプリケーションのトークンはクリアしません。

```
[guestshell@guestshell]$ clear_token.py
```

認証トークンの更新

Cisco Catalyst 8000V ルータは、`refresh_token` スクリプトを使用して、アクティブなアプリケーションの新しいトークンを強制的に取得できます。

このスクリプトは、デフォルトのユーザー割り当てアプリケーションまたはシステム割り当てアプリケーションのいずれかを更新します。このスクリプトは、個々の冗長ノードで明示的に設定されているユーザー割り当てアプリケーションのトークンは更新しません。

```
[guestshell@guestshell]$ refresh_token.py
```

アプリケーション認証の選択

認証用の Cisco Catalyst 8000V ルータを識別するために、システム割り当てまたはユーザー割り当てのアプリケーションを選択できます。単一の Cisco Catalyst 8000V ルータ内のすべてのアプリケーションに同じメカニズムを使用できます。また、複数の冗長ノードにまたがって複数のユーザー割り当てアプリケーションを使用することもできます。

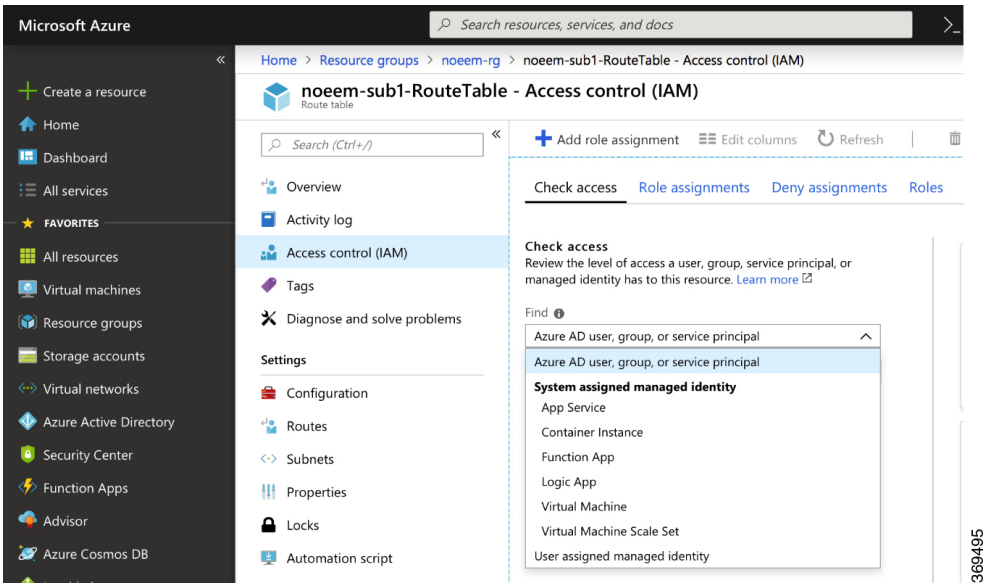
次の表に、冗長ノードの処理時に Cisco Catalyst 8000V ルータで使用されるアプリケーションをまとめます。

デフォルトのアプリケーションが設定されているか	ノードにユーザー割り当てアプリケーションが設定されているか	Cisco Catalyst 8000V はこのアプリケーションを使用するか
非対応	非対応	システム割り当てアプリケーション
非対応	対応	この冗長ノードで設定されたユーザー割り当てアプリケーション
対応	非対応	set_default_aad_app.py によってデフォルトとして設定されたユーザー割り当てアプリケーション
対応	非対応	この冗長ノードで設定されたユーザー割り当てアプリケーション

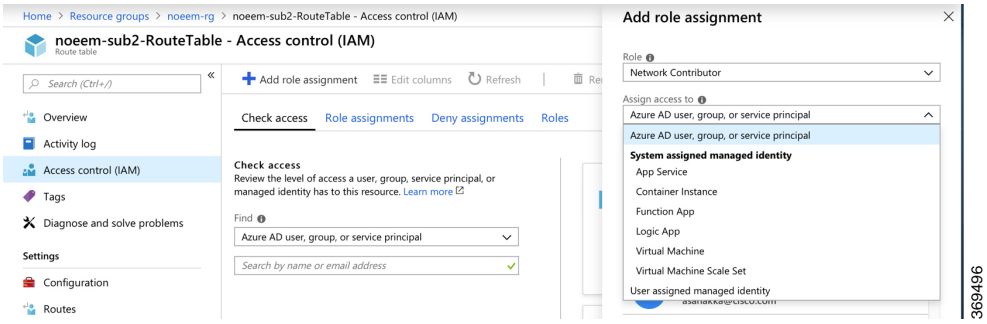
ルートテーブルの IAM の設定

手順

ステップ 1 既存のネットワークにアプリケーションを追加するには、[All Resources] ペインで、左側のペインからプライベート側サブネットを選択します。たとえば、noeem-sub1-RouteTable です。



ステップ 2 中央のペインで、[Access control (IAM)] を選択します。プラスアイコンを選択して、ロールの割り当てを追加します。



ステップ 3 [Add Role Assignment] 画面で、[Role to Network Contributor] を設定します。

ステップ 4 [Assign Access to Pulldown] メニューを選択します。システム割り当ての管理対象 ID を使用している場合は、[Virtual Machine] サブオプションを選択し、ステップ 6 に進みます。ユーザー割り当ての管理対象 ID を使用している場合は、オプションを選択し、ステップ 5 に進みます。

ステップ 5 [Select] フィールドに、[Azure Active Directory] で作成したユーザー割り当てアプリケーションの名前を入力します。[Save] をクリックします。

ステップ 6 [Select] フィールドに、Cisco Catalyst 8000V インスタンスに付けられた名前を入力します。Cisco Catalyst 8000V インスタンスがシステム割り当て ID に対して適切に設定されている場合は、Cisco Catalyst 8000V インスタンスが検索結果に表示されます。

ステップ 7 Cisco Catalyst 8000V インスタンスを名前で選択し、[Save] をクリックします。

ルートテーブルのエントリタイプ

Microsoft Azure のルートテーブルは、さまざまなエントリタイプをサポートしています。ルートのエントリタイプは、仮想ネットワークゲートウェイ、インターネット、または仮想アプライアンスのいずれかです。ネクストホップアドレスは、Azure ネットワーク内のリソースを識別します。

エントリタイプが [Virtual network gateway] または [Internet] のルートには、ネクストホップの明示的な IP アドレスがなく、ハイアベイラビリティ機能ではサポートされません。

Cisco Catalyst 8000V インスタンスでハイアベイラビリティを設定すると、障害発生時に更新される個々のルートを指定できます。個々のルートが仮想アプライアンスのエントリタイプを持つように設定されていることを確認します。ルートテーブル内のすべてのエントリを表す冗長ノードを設定する場合は、すべてのルートのエントリタイプが仮想アプライアンスであることを確認します。

ネットワーク セキュリティ グループの設定

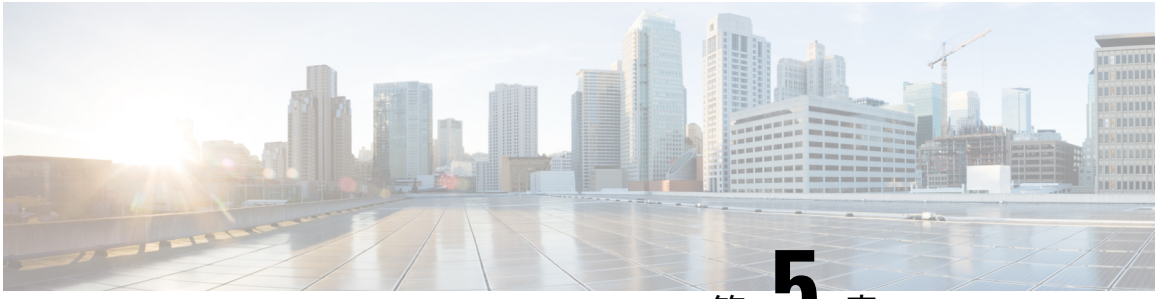
ルータの NIC0 にネットワーク セキュリティ グループが接続されている場合は、BFD プロトコルがインターフェイスを通過できるようにする必要があります。ポート 4789 および 4790 の通過を許可するインバウンドおよびアウトバウンド セキュリティ ルールを設定します。

コンソールタイムアウトの設定

Cisco Catalyst 8000V ルータへの SSH セッションを開始するときは、端末の VTY タイムアウトを無限に設定しないでください。つまり、exec-timeout 0 0 のように設定しないでください。タイムアウトにはゼロ以外の値を使用します。たとえば、exec-timeout 4 0 などです。このコマンドは、4 分 0 秒のタイムアウトを指定します。exec-timeout 0 0 コマンドを使用すると、Azure が 4 ～ 30 分のコンソールアイドル期間のタイムアウトを強制するため、問題が発生します。アイドルタイマーが期限切れになると、Azure は SSH セッションを切断します。しかし、exec-timeout 0 0 コンフィギュレーション コマンドによってタイムアウトが無限に設定されていると、セッションは Cisco Catalyst 8000V からはクリアされません。切断により、端末セッションが孤立します。Cisco Catalyst 8000V のセッションは無期限に開いたままになります。新しい SSH セッションを確立しようとすると、新しい仮想端末セッションが使用されます。このパターンが続くと、許可されている同時端末セッションの最大数に達し、新しいセッションを確立できなくなります。exec-timeout コマンドを正しく設定することに加えて、次の例に示すコマンドを使用して、アイドル状態の仮想端末セッションを削除することもお勧めします。

```
RouterA# show users
Line User Host(s) Idle Location
2 vty 0 cisco idle 00:07:40 128.107.241.177
* 3 vty 1 cisco idle 00:00:00 128.107.241.177
RouterA# clear line 2
```

（注） 上記のシナリオの回避策が効果がない場合は、最後の手段として、Azure ポータルで Cisco Catalyst 8000V ルータを再起動できます。



第 5 章

Amazon Web Services 上で実行される Cisco Catalyst 8000V でのハイアベイラビリティの設定

表 *1*: 冗長性パラメータのクラウド固有の設定

パラメータ	スイッチ	説明
ノードインデックス	-i	このノードを一意に識別するために使用されるインデックス。有効な値は 1 ～ 1023 です。
リージョン名	-rg	ルートテーブルを含むリージョンの名前。 たとえば、us-west-2 です。
ルートテーブル名	-t	更新するルートテーブルの名前。ルートテーブルの名前は、サブストリング rtb- で始まる必要があります。 例：rtb-001333c29ef2aec5f
Route	-r	ルートが指定されていない場合、冗長ノードはルーティングテーブル内のすべてのルートに適用されると見なされます。Cisco Catalyst 8000V インスタンスは、タイプがローカルまたはゲートウェイのルートを変更できません。

パラメータ	スイッチ	説明
ネクストホップインターフェイス	-n	宛先ルートに到達するためにパケットを転送するインターフェイスの名前。インターフェイスの名前は、サブストリング eni- で始まる必要があります。 たとえば、eni-07160c7e740ac8ef4 です。
モード	-m	このルータが、このルートを処理するためのプライマリルータかセカンダリルータかを示します。有効な値は、primary または secondary です。これは省略可能なパラメータです。デフォルト値は secondary です。

- 冗長ノードの作成 （34 ページ）
- 冗長ノードパラメータの設定 （35 ページ）
- 冗長ノードパラメータのクリア （35 ページ）
- Cisco Catalyst 8000V ルータの認証 （36 ページ）
- 送信元/宛先アドレスチェックの無効化 （37 ページ）
- ルートテーブルのエントリタイプ （37 ページ）
- セキュリティグループの設定 （37 ページ）

冗長ノードの作成

手順の概要

1. 次のスクリプトを実行して冗長ノードを作成し、データベースに追加します。

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	次のスクリプトを実行して冗長ノードを作成し、データベースに追加します。 例：	有効な冗長ノードには、次のパラメータが設定されている必要があります。 • ノードインデックス

	コマンドまたはアクション	目的
	`create_node { switch value } […[{ switch value }]`	• リージョン名 • ルートテーブル名 • ネクスト ホップ インターフェイス名 次の例を参考にしてください。 `create_node.py -i 2 -t rtb-001333c29ef2aec5e -rg us-west-2 -n eni-07160c7e740ac8ef3 -r 2600:1f14:49b:9b03::/64` 成功した場合、スクリプトはゼロの値を返します。

冗長ノードパラメータの設定

手順

既存の冗長ノードのパラメータの値を変更するには、`set_params -i node_index { switch value } […[{ switch value }]` スクリプトを実行します。

例：

```
set_params.py -i 10 -r 15.0.0.0/16 -m primary
```

インデックスパラメータ（-i）は必須です。このコマンドは、指定されたパラメータの値を設定します。指定したパラメータが冗長ノードにすでに定義されている場合は、パラメータの値が更新されます。

この設定が成功すると、スクリプトはゼロの値を返します。

冗長ノードパラメータのクリア

手順

既存の冗長ノードの指定されたパラメータの値をクリアする場合は、`clear_params -i node_index {switch … switch]` スクリプトを実行します。

例：

```
clear_params -i 10 -r -n
```

この例では、clear_params スクリプトはルートパラメータとネクスト ホップ アドレス パラメータの両方をクリアします。

関連する値をクリアする場合は、switch パラメータだけを指定します。クリアするパラメータに既存の値を指定しないでください。

クリアに成功すると、スクリプトはゼロの値を返します。

Cisco Catalyst 8000V ルータの認証

Cisco Catalyst 8000V ルータで AWS ネットワーク内のルーティングテーブルを更新する場合は、最初にルータを認証する必要があります。AWS では、Cisco Catalyst 8000V ルータがルートテーブルにアクセスすることを許可するポリシーを作成する必要があります。次に例を示します。

```
{
"Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "cloudwatch:",
                "s3:",
                "ec2:AssociateRouteTable",
                "ec2:CreateRoute",
                "ec2:CreateRouteTable",
                "ec2:DeleteRoute",
                "ec2:DeleteRouteTable",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:DescribeRegions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DisassociateRouteTable",
                "ec2:ReplaceRouteTableAssociation",
                "logs:CreateLogGroup",
                "logs:PutLogEvents"
            ],
            "Resource": "*"
        }
    ]
}
```

その後、このポリシーを使用して IAM ロールが作成され、EC2 リソースに適用されます。

Cisco Catalyst 8000V EC2 インスタンスが作成されたら、上記で作成した IAM ロールを各ルータにアタッチする必要があります。

（注） ポリシー、IAM ロールの作成方法、およびロールを EC2 インスタンスに関連付ける方法については、AWS のドキュメントを参照してください。

送信元/宛先アドレスチェックの無効化

AWS で作成されたネットワーク インターフェイスでは、デフォルトで、送信元アドレスと宛先アドレスのチェックが有効になっています。インターフェイスでは、通過するすべてのトラフィックがインターフェイスの送信元アドレスまたは宛先アドレスと一致することが確認され、一致しない場合はドロップされます。Cisco Catalyst 8000V でルーティングを実行するには、各 Cisco Catalyst 8000V インターフェイスでこの設定を無効にする必要があります。

（注） ネットワーク インターフェイスで送信元/宛先アドレスのチェックを無効にする方法については、AWS のドキュメントを参照してください

ルートテーブルのエントリタイプ

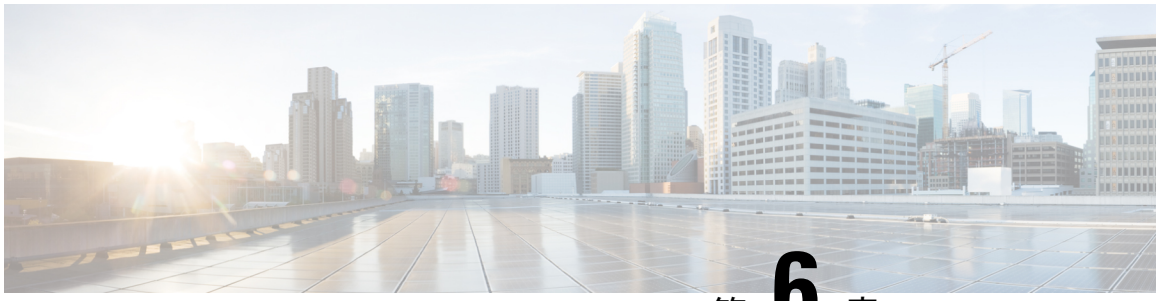
AWS クラウドのルートテーブルは、さまざまなターゲットタイプをサポートしています。これらのルートターゲットには、複数のタイプのゲートウェイと接続が含まれます。Cisco Catalyst 8000V ルータは、ネットワーク インターフェイス ターゲットを持つルートのみを更新できます。他のターゲットタイプのルートは、高可用性のために無視されます。

特定のルート宛先なしで冗長ノードを設定すると、Cisco Catalyst 8000V は、ターゲットタイプのネットワーク インターフェイスを使用して、ルートテーブル内のすべてのルートを更新しようとします。他のすべてのルートは無視されます。

セキュリティグループの設定

Cisco Catalyst 8000V の EC2 インスタンスの eth0 インターフェイスで使用されているセキュリティグループがある場合は、BFD プロトコルがインターフェイスを通過できるようにする必要があります。 ポート 4789 および 4790 の通過を許可するインバウンドおよびアウトバウンド セキュリティ ルールを設定します。

（注） セキュリティグループを設定し、それらをサブネットとネットワーク インターフェイスにアタッチする手順については、AWS のドキュメントを参照してください。



第 6 章

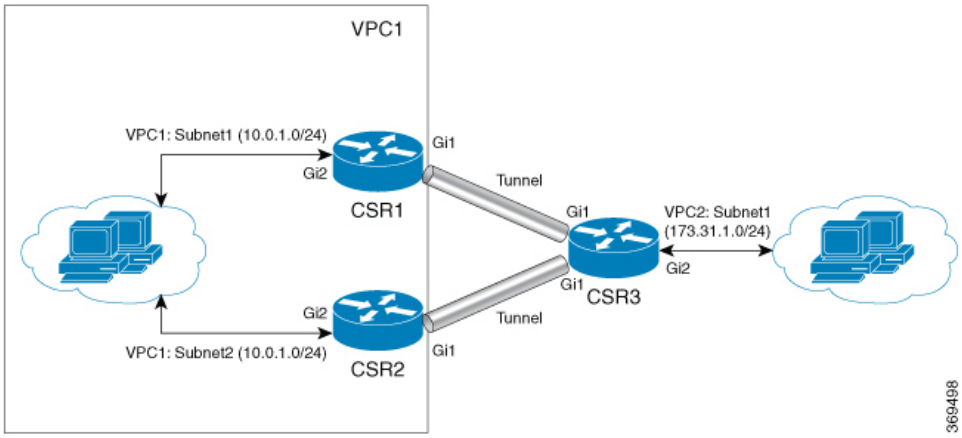
Google Cloud Platform で実行されている Cisco Catalyst 8000V でのハイアベイラビリティの設定

Google Cloud では、各スタティックルートは VPC に関連付けられたルートテーブルに属し、次のフィールドで構成されます。

- [Name] および [Description]：これらのフィールドはルートを識別します。名前は必須ですが、説明は任意です。プロジェクト内のすべてのルートには、一意の名前を付ける必要があります。
- ネットワーク：各ルートは、1 つの VPC ネットワークにのみ関連付ける必要があります。
- [Destination range]：宛先範囲は、着信パケットを受信するシステムの IP アドレスを含む単一の IPv4 CIDR ブロックです。GCP は IPv6 宛先範囲をサポートしていません。宛先は CIDR 表記で表す必要があり、可能な最も広範な宛先は 0.0.0.0/0 です。
- [Priority]：優先順位は、複数のルートの宛先が同じ場合に使用するルートを決定するために使用されます。数値が小さいほど優先順位が高くなります。たとえば、優先順位の値が 100 のルートは、優先順位の値が 200 のルートよりも優先順位が高くなります。
- [Next hop]：スタティックルートには、デフォルトのインターネットゲートウェイ、GCP インスタンス、またはクラウド VPN トンネルを指すネクストホップを含めることができます。詳細については、スタティックルートのネクストホップを参照してください。
- [Tags]：リストされたタグの少なくとも 1 つを持つインスタンスにのみルートが適用されるように、ネットワークタグのリストを指定できます。タグを指定しない場合、GCP はネットワーク内のすべてのインスタンスにルートを適用します。

詳細については、https://cloud.google.com/vpc/docs/routes を参照してください。Google ネットワーク内の 2 つの Cisco Catalyst 8000V ルータのアクティブ/アクティブ動作でハイアベイラビリティを設定するには、宛先範囲ごとにルートコレクションに2つのルートを作成する必要があります。各ルートは、2 つのルータのいずれかをネクストホップとして指します。

これをよりよく理解するために、次のトポロジを考えます。



上記のトポロジでは、HA モードで 2 つのルータが設定されています。両方のルータには、VPC1 に 1 つのインターフェイスがあり、VPC に別のインターフェイスがあります。これら 2 つの Cisco Catalyst 8000V ルータには、VPC2 にインターフェイスを持つ別の Cisco Catalyst 8000V インスタンスに設定されたトンネルがあります。このシナリオでは、VPC 2 の宛先範囲（172.31.0.0/16）の VPC1 のルートエントリは次のとおりです。

route-vcp2-c8000v1	172.31.0.0/16	100	なし	IP：10:1:0:3	test-vpc
route-vcp2-c8000v2	172.31.0.0/16	200	なし	IP：10.0.2.3	test-vpc

アクティブルートは、ルートの優先順位に基づいて決定されます。route-vpc2-c8000v1 の値が小さいため、このルートの優先順位が高くなり、Cisco Catalyst 8000V 1 がアクティブルートになります。

障害回復後のプライマリ Cisco Catalyst 8000V への復帰

Cisco Catalyst 8000V 1 が失敗すると、Cisco Catalyst 8000V 2 は BFD トンネルを介してピア障害イベントを検出し、ルート収集から route-vpc2-c8000v1 を削除して、route-vpc2-c8000v2 を宛先範囲 172.31.0.0/16 のアクティブルートとします。

Cisco Catalyst 8000V 1 が回復すると、route-vpc2-c8000v1 ルートがルートコレクションに追加され、VPC 2 へのすべてのトラフィックのプライマリルートに戻ります。両方のルートエントリに等しいルート優先順位を設定することが可能であることに注意してください。この場合、Google Cloud は両方のルートを使用してトラフィックを宛先範囲に送信します。

各 Cisco Catalyst 8000V インスタンスで、2 つの Cisco Catalyst 8000V インスタンスとしてネクストホップを使用して、ルートコレクションの各ルートエントリに対応するノードを作成する必要があります。

HA でモード（プライマリまたはセカンダリ）オプションを使用して新しいノードを作成する場合は、優先順位が高い（番号が小さい）ルートがプライマリとしてマークされ、優先順位が低いルートがセカンダリとしてマークされていることを確認します。

ユーザー指定のスクリプト

ゲストシェルは、独自のスクリプトを展開できるコンテナです。ハイアベイラビリティは、ユーザー指定のスクリプトにプログラミングインターフェイスを公開するため、フェールオーバーイベントと復帰イベントの両方をトリガーできるスクリプトを作成できます。独自のアルゴリズムとトリガーを開発して、特定のルートへの転送サービスを提供する Cisco Catalyst 8000V を制御できます。

- 冗長性パラメータのクラウド固有の設定 （41 ページ）
- 冗長ノードの作成 （43 ページ）
- 冗長ノードパラメータの設定 （43 ページ）
- Cisco Catalyst 8000V ルータの認証 （44 ページ）

冗長性パラメータのクラウド固有の設定

パラメータ	このパラメータは必須ですか。	スイッチ	説明
ノードインデックス	対応	-i	このノードを一意に識別するために使用されるインデックス。有効な値は 1 ～ 255 です。
クラウドプロバイダー	対応	-p	このパラメータには gcp を指定します。
プロジェクト	対応	-g	Google プロジェクト ID を指定します。
routeName	対応	-a	この Cisco Catalyst 8000V がネクストホップであるルート名。たとえば、図 2 の Cisco Catalyst 8000V 1 でノードを設定する場合、route-vpc2-c8000v1 になります。
peerRouteName	対応	-b	BFD ピア Cisco Catalyst 8000V がネクストホップであるルート名。たとえば、図 2 の Cisco Catalyst 8000V 1 でノードを設定する場合、route-vpc2-c8000v2 になります。

パラメータ	このパラメータは必須ですか。	スイッチ	説明
Route	あり	-r	更新されるルートの CIDR 形式での IP アドレス。IPv4 または IPv6 アドレスにできます。 ルートが指定されていない場合、冗長ノードは仮想アプライアンスタイプのルーティングテーブル内のすべてのルートに適用されると見なされます。 注：現在、Google Cloud は VPC で IPv6 をサポートしていません。
ネクスト ホップ アドレス。	対応	-n	ネクストホップルータの IP アドレス。このルートテーブルを使用するサブネット上のこの Cisco Catalyst 8000V に割り当てられている IP アドレスを使用します。値は IPv4 または IPv6 アドレスにできます。 注：現在、Google Cloud は VPC で IPv6 をサポートしていません。
hopPriority	対応	-o	現在の Cisco Catalyst 8000V がネクストホップであるルートのルート優先順位。
VPC	対応	-v	現在の Cisco Catalyst 8000V をネクストホップとするルートが存在する VPC ネットワーク名。

冗長ノードの作成

手順

次のスクリプトを実行して冗長ノードを作成し、データベースに追加します：`create_node { switch value } […[{ switch value }]`。

有効な冗長ノードには、次のパラメータを設定する必要があります。

- ノードインデックス
- クラウドプロバイダー
- プロジェクト ID
- ルート名
- ピアルート名
- Route
- ネクスト ホップ アドレス
- ホップ優先順位
- VPC 名

```
create_node -i 1 -g <project-id> -r dest_network -o 200 -n nexthop_ip_addr -a route-name1 -b
route-name2 -p gcp -v vpc_name
```

設定が成功すると、スクリプトはゼロの値を返します。

冗長ノードパラメータの設定

手順

既存の冗長ノードのパラメータの値を変更するには、`set_params{ switch value } […[{ switch value }]` スクリプトを実行します。

例：

```
set_params -i 10 -r 15.0.0.0/16 -n 172.168.7.5
```

インデックスパラメータ（-i）は必須です。このコマンドは、指定されたパラメータの値を設定します。指定したパラメータが冗長ノードにすでに定義されている場合は、パラメータの値が更新されます。

ゼロのノードインデックス値を指定すると、指定されたパラメータに対してコマンドによって指定された値が、これらのパラメータのデフォルト値として扱われます。

この設定が成功すると、スクリプトはゼロの値を返します。

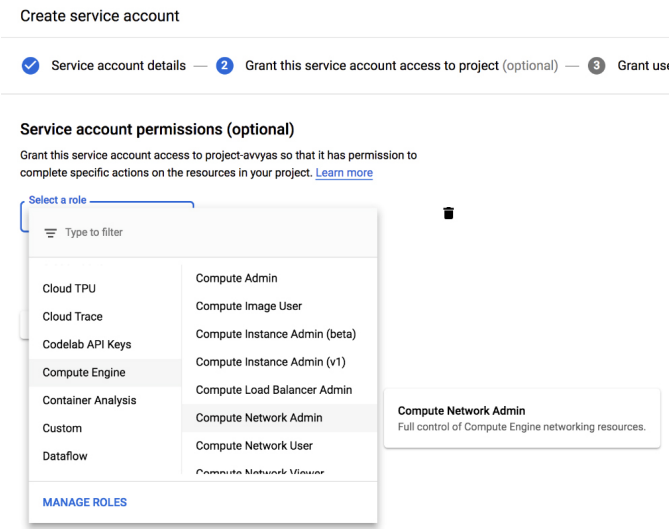
Cisco Catalyst 8000V ルータの認証

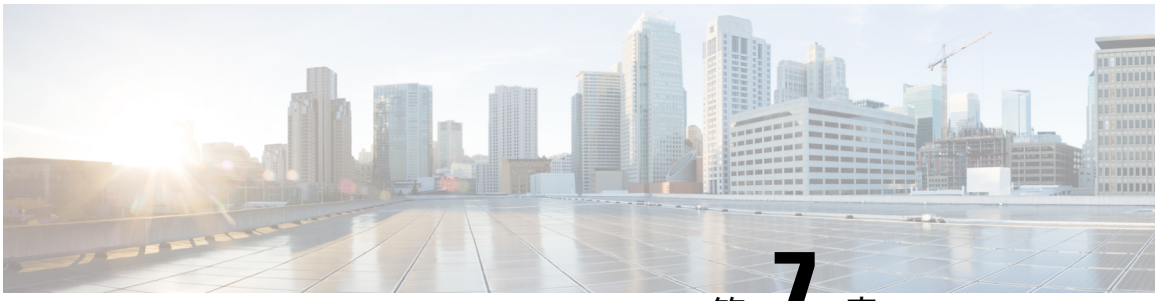
手順の概要

1. Cisco Catalyst 8000V ルータに関連付けられているサービスアカウントに、少なくともコンピューティング ネットワーク管理者権限があることを確認します。

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco Catalyst 8000V ルータに関連付けられているサービスアカウントに、少なくともコンピューティング ネットワーク管理者権限があることを確認します。	 また、「credentials.json」という名前のログイン情報ファイルに必要な権限を指定し、/home/guestshell ディレクトリの下に配置することもできます。ログイン情報ファイルは、Cisco Catalyst 8000V インスタンスに関連付けられたサービスアカウントを介して提供される権限をオーバーライドします。



第 7 章

設定例

例：アクティブ/アクティブ構成の冗長ノード

宛先ネットワーク 'dest_network' のネクストホップが Cisco Catalyst 8000V 1 のルートエントリに route-name1 が対応し、ネクストホップが Cisco Catalyst 8000V 2 のルートエントリに route-name2 が対応する HA 構成を考えます。ルータをアクティブ/アクティブモードで設定するには、route-name1 と route-name2 に等しいルートプライオリティを設定します。この場合、Google クラウドは、アフィニティの 5 タプルハッシュを使用してルート間でトラフィックを分散し、ECMP ルーティング設計を実装します。

VPC の Google ルート収集のルートエントリに対応する両方のルータのノード設定は次のようになります。

```
create_node -i 1 -g <project-id> -r dest_network -o 200 -n nexthop_ip_addr_c8000v1 -a
route-name1 -b route-name2 -p gcp -v vpc_name
```

```
create_node -i 2 -g <project-id> -r dest_network -o 200 -n nexthop_ip_addr_c8000v2 -a
route-name2 -b route-name1 -p gcp -v vpc_name
```

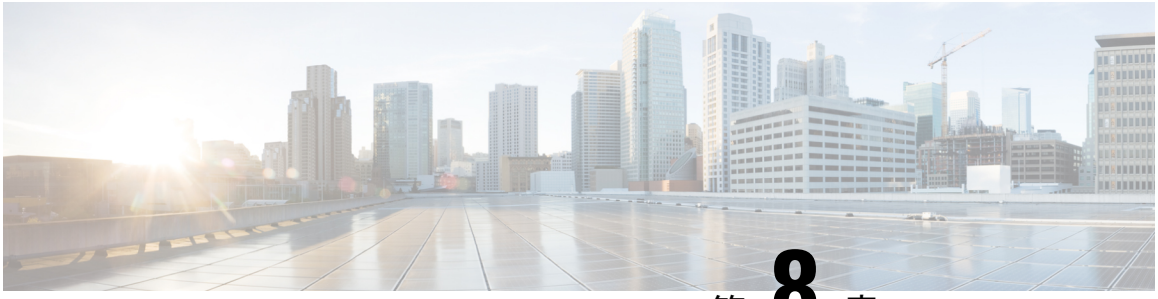
例：アクティブ/パッシブ構成の冗長性ノード

同様に、Cisco Catalyst 8000V インスタンスをアクティブ/パッシブモードで設定するには、一方のルートのプライオリティをもう一方のルートよりも高く設定します。この場合、Google クラウドは、VPC vpc_name から dest_network に優先順位の高いルート（この例では route-name1）を介してすべてのトラフィックをルーティングします。

VPC の Google ルート収集のルートエントリに対応する両方のルータのノード設定は次のようになります。

```
create_node -i 1 -g <project-id> -r dest_network -o 200 -n nexthop_ip_addr_c8000v1 -a
route-name1 -b route-name2 -p gcp -v vpc_name
```

```
create_node -i 2 -g <project-id> -r dest_network -o 400 -n nexthop_ip_addr_c8000v2 -a
route-name2 -b route-name1 -p gcp -v vpc_name
```

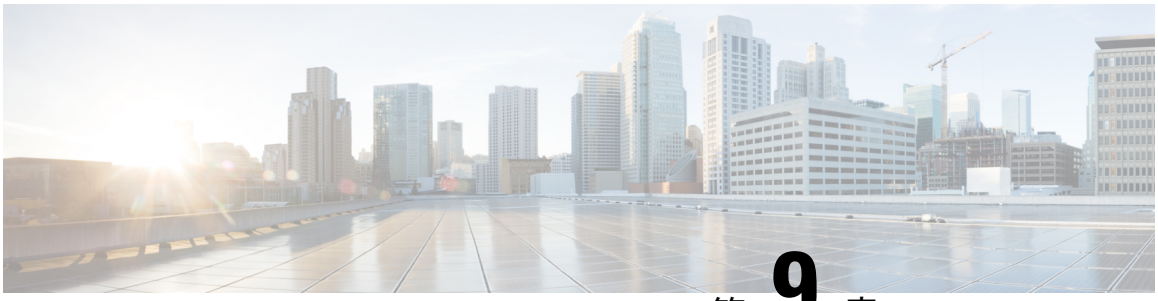


第 8 章

ハイアベイラビリティの確認

ログファイルを確認して、次の検証手順を実行します。詳細ログファイルをディレクトリ ~/cloud/HA/events に書き込むことができます。このログファイルを調べて、操作が成功したかどうかを確認します。

```
[guestshell@guestshell events]$ node_event.py -i node_index -e verify
[guestshell@guestshell events]$ cd /home/guestshell/cloud/HA/events
[guestshell@guestshell events]$ ls event.2018-06-13 20:10:21.093942
```



第 9 章

ハイアベイラビリティに関する問題のトラブルシューティング

生成されたイベントファイルを開きます。このファイルは、冗長ノードによって記述されたルートの読み取りと更新の試行のデバッグログです。HA セットアップが期待どおりに機能している場合、設定出力にステータス「Event Handling completed」が表示されます。システムにこのステータスが表示されない場合は、ログファイルを詳しく調べて、検証のどの手順が失敗したかを判断します。

失敗の一般的な原因は次のとおりです。

- 認証情報を取得できません。
- ゲストシェルにはネットワークアクセスがありません。
- 認証サービスがゲストシェルで実行されていません。
- Cisco Catalyst 8000V のログイン情報がないか、正しくありません。
- ルータはルートテーブルエントリにアクセスできません。
- 冗長ノードでルートテーブルが正しく識別されませんでした
- ルータにルートテーブルへのアクセス権限が付与されていませんでした
- 冗長ノードで指定された特定のルートが存在しません

（注） 検証イベントで `node_event` スクリプトを使用して、冗長ノードの設定と動作をテストすることを推奨します。

例：ハイアベイラビリティのトラブルシューティングの問題

`router#show iox` コマンドを実行します。考えられる問題と、それらの問題を確認して解決する方法を示す次の例を参照してください。

```
Router#show iox
```

```
IOx Infrastructure Summary:
---------------------------
IOx service (CAF)    : Running
IOx service (HA)     : Not Supported
IOx service (IOxman) : Running
Libvirtd             : Running

Router#guestshell enable

Router#show app-hosting list
App id                           State
------------------------------------------------------
guestshell                       RUNNING

Router#guestshell
[guestshell@guestshell ~]$

[guestshell@guestshell ~]$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=38 time=25.7 ms

Possible Cause:
The configuration of IOX and the creation of the VirtualPortGroup interface to provide
the guestshell network access is part of the "day zero" configuration of the C8000V.
If any of the above steps did not work, check that the startup configuration of the
C8000V has been altered.

How to Fix:
A reload of the C8000V will re-apply the day zero configuration.

---------

Problem:
HA package installation failure

How to Check:
Router#guestshell
Router#guestshell
[guestshell@guestshell ~]$ ls
cloud
[guestshell@guestshell ~]$ cd cloud
[guestshell@guestshell cloud]$ ls
HA

You should see the directory ~/cloud/HA.
On an Azure provided cloud, you should also see a ~/cloud/authMgr directory.

Possible Cause:
The HA package was not installed, or was not installed using the --user option.

How to Fix:
Install the package and set up the environment:
 pip install c8000v_<provider>_ha --user
 source ~/.bashrc

---------

Problem:
HA server not running.

How to Check:
[guestshell@guestshell ~]$ systemctl status c8000v_ha
● c8000v_ha.service - C8000V High Availability service
   Loaded: loaded (/etc/systemd/user/c8000v_ha.service; enabled; vendor preset: disabled)
```

```
   Active: active (running) since Mon 2019-04-08 15:01:51 UTC; 2h 1min ago
 Main PID: 286 (python)
   CGroup: /system.slice/libvirtd.service/system.slice/c8000v_ha.service
           ├─286 python /home/guestshell/.local/lib/python2.7/site-packages/c...
           └─295 python /home/guestshell/.local/lib/python2.7/site-packages/c...

On an Azure provided network, the auth-token service should also be running.
[guestshell@guestshell ~]$ systemctl status c8000v_ha
● c8000v_ha.service - C8000V High Availability service
   Loaded: loaded (/etc/systemd/user/c8000v_ha.service; enabled; vendor preset: disabled)

   Active: active (running) since Mon 2019-04-08 15:01:51 UTC; 2h 1min ago
 Main PID: 286 (python)
   CGroup: /system.slice/libvirtd.service/system.slice/c8000v_ha.service
           ├─286 python /home/guestshell/.local/lib/python2.7/site-packages/c...
           └─295 python /home/guestshell/.local/lib/python2.7/site-packages/c...
[guestshell@guestshell ~]$ systemctl status auth-token
● auth-token.service - Authentication Token service
   Loaded: loaded (/etc/systemd/user/auth-token.service; enabled; vendor preset: disabled)

   Active: active (running) since Mon 2019-04-08 16:08:15 UTC; 57min ago
 Main PID: 542 (python)
   CGroup: /system.slice/libvirtd.service/system.slice/auth-token.service
           └─542 /usr/bin/python /home/guestshell/.local/lib/python2.7/site-p...

Possible Cause:
If the HA server has an error and crashes, it is automatically restarted.

How to Fix:
A service can be restarted manually
[guestshell@guestshell ~]$ sudo systemctl start c8000v_ha


---------

Problem:
C8000V authentication not working on Azure.
This is an Azure specific error.

How to check:
If you perform a node_event on a redundancy node, and it fails while trying to read the
 route table, it will generate a file ~/cloud/HA/events/routeTableGetRsp.
[guestshell@guestshell ~]$ cat routeTableGetRsp
{"error":{"code":"AuthenticationFailedMissingToken","message":"Authentication failed.
The 'Authorization' header is missing the access token."}}

Possible Cause:
There are multiple possible causes.  And it depends upon the authentication mechanism
you are using:
 - System assigned managed identity
 - Registered application in Azure Active Directory (AAD)

Likely cause of a failure using system assigned managed identity is that it is not enabled
 on C8000V.

How to Fix:
Verify the C8000V is enabled for system assigned managed identity.
In the Azure portal, navigate to the virtual machine running the C8000V.
Under the Settings menu, select the Identity item.
Under the system assigned tab, verify the status is set to On.

When using AAD for authentication, the likely cause of the error is a mis-configuration
 of the application or a mis-match in the identifiers for the application configured in
```

```
 the guestshell.

How to Fix:
The application in AAD must be given the proper permissions to read and write a route
table.
In the Azure portal, navigate to the registered application you have created.
Under the API Access menu, select the Required permissions item.
Select the Windows Azure Active Directory API.  In the Enable Access pane, verify the
following permissions are set:
 - Application permission to read and write directory data
 - Delegated permission to sign in and read user profile
Select the Windows Azure Service Management API.  In the Enable Access pane, verify the
 following permissions are set:
 - Delegated permission to access Azure service management as organization users

How to Fix:
In the Azure portal, navigate to the registered application you have created.
Select the Setting button for the application.
Verify the application_id, tenant_id, and application key in the portal match the values
 configured in guestshell.  Verify the application key configured in guestshell is in
URL unencoded format.

-------------

Problem:
Route table entry not updated by a peer failure event.

How to Check:
For every node event a log file is generated in the directory ~/cloud/HA/events.
This file will indicate the event that was processed and its result.  Examine this file
 for possible errors.  It is likely in the case of an error that a file
~/cloud/HA/events/routeTableGetRsp is also written.  Also examine this file for additional
 insights.

Possible Causes:
A route was not correctly identified in a redundancy node.  Depending upon what parameter
 in the redundancy node is in error, you may see different results.

Some examples:
[guestshell@guestshell events]$ cat routeTableGetRsp
{"error":{"code":"SubscriptionNotFound","message":"The subscription
'b0b1a9e2-444c-4ca5-acd9-bebd1e6874ef' could not be found."}}
This implies the Azure subscription ID was not entered correctly.

[guestshell@guestshell events]$ cat node*
Route GET request failed with code 403
Route table get response:
 {"error":{"code":"AuthorizationFailed","message":"The client
'b3ce41c0-bcef-41d7-9741-26bea31221c1' with object id
'b3ce41c0-bcef-41d7-9741-26bea31221c1' does not have authorization to perform action
'Microsoft.Network/routeTables/read' over scope
'/subscriptions/b0b1a9e2-444c-4ca5-acd9-bebd1e6873eb/resourceGroups/gsday0-rg/providers/Microsoft.Network/routeTables/gsday0-sub4-RouteTable'."}}
Route table not found.
This implies the name of the route table was incorrect or does not exist.

[guestshell@guestshell events]$ cat node*
Did not find route 17.0.0.0/8 event type peerFail
This implies that the route does not exist.

How to Fix:
Make sure the identifiers in the redundancy node match the values in the cloud provider's
 portal.

------------
```

```
Problem:
Route table entry not updated by a peer failure event.

How to Check:
For every node event a log file is generated in the directory ~/cloud/HA/events.
This file will indicate the event that was processed and its result.  Examine this file
 for possible errors.  It is likely in the case of an error that a file
~/cloud/HA/events/routeTableGetRsp is also written.  Also examine this file for additional
 insights.

Possible Causes:
The C8000V has not been given permission to access the route table.
Fetching the route table
Route table get response:
 {"error":{"code":"AuthorizationFailed","message":"The client
'b3ce41c0-bcef-41d7-9741-26bea31221c1' with object id
'b3ce41c0-bcef-41d7-9741-26bea31221c1' does not have authorization to perform action
'Microsoft.Network/routeTables/read' over scope
'/subscriptions/b0b1a9e2-444c-4ca5-acd9-bebd1e6873eb/resourceGroups/gsday0-rg/providers/Microsoft.Network/routeTables/gsday0-sub2-RouteTable'."}}
Route GET request failed with code 403
Route table get response:
 {"error":{"code":"AuthorizationFailed","message":"The client
'b3ce41c0-bcef-41d7-9741-26bea31221c1' with object id
'b3ce41c0-bcef-41d7-9741-26bea31221c1' does not have authorization to perform action
'Microsoft.Network/routeTables/read' over scope
'/subscriptions/b0b1a9e2-444c-4ca5-acd9-bebd1e6873eb/resourceGroups/gsday0-rg/providers/Microsoft.Network/routeTables/gsday0-sub2-RouteTable'."}}
Route table not found.
C8000V HA: Set route table for verify
Route Table not found


If none of these troubleshooting tips have resolved your problem, run this command:
[guestshell@guestshell ~]$ cd ~/cloud/HA
[guestshell@guestshell ~]$ bash debug_ha.sh
[guestshell@guestshell ~]$ ls /bootflash
You should see a file name ha_debug.tar.  Copy this file off the C8000V and provide it
to Cisco Technical Support for analysis.
```

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。