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

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。

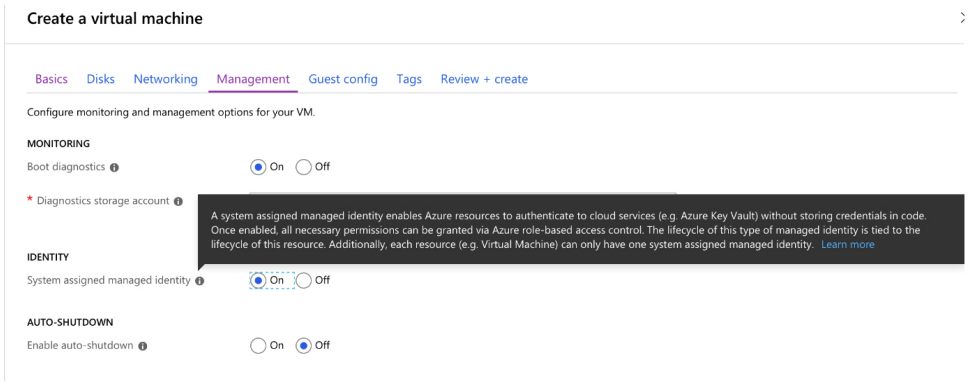
システム割り当て管理対象 ID

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 *1:* 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。	

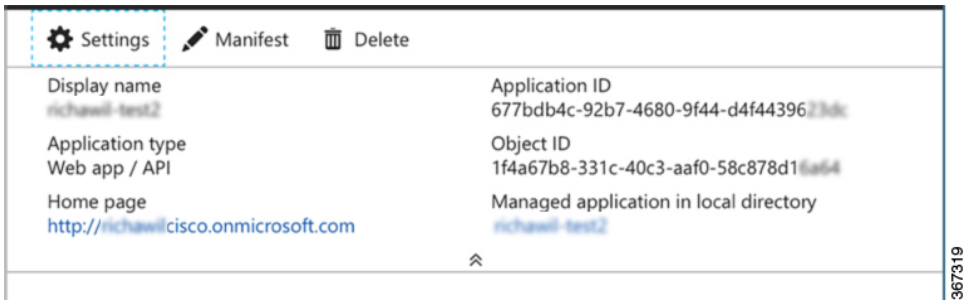
アプリケーション ID およびテナント ID の取得

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。

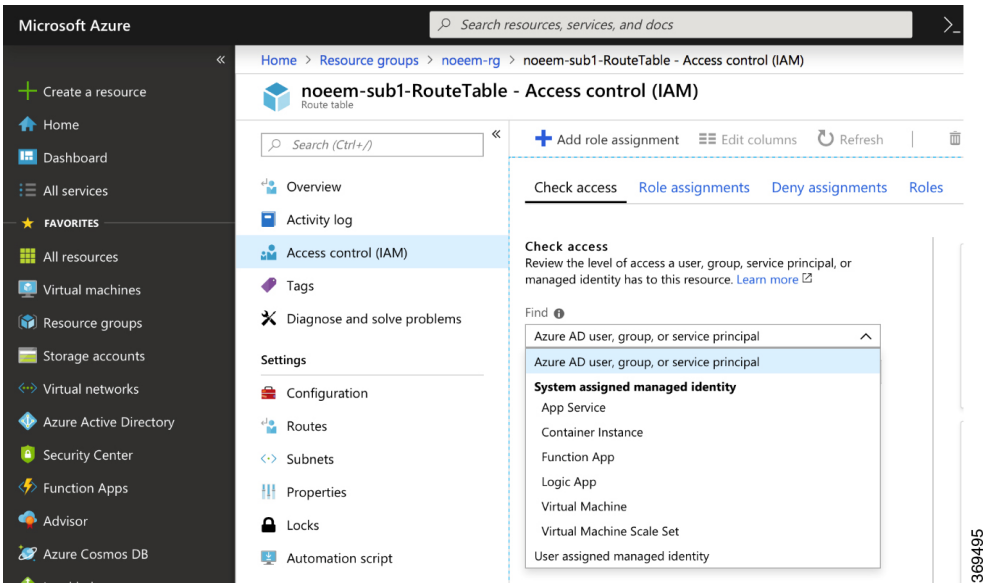
次の表に、冗長ノードの処理時に Cisco Catalyst 8000V ルータで使用されるアプリケーションをまとめます。

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

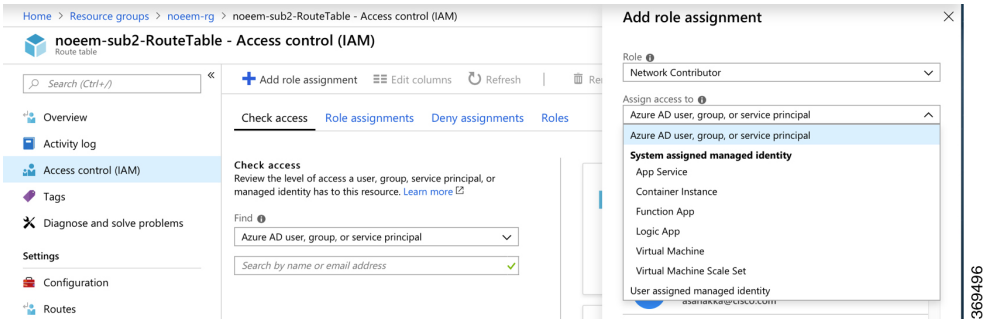
ルートテーブルの IAM の設定

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。

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。