パブリック クラウドでのハイ アベイラビリティのためのフェールオーバー

この章では、Microsoft Azure などのパブリッククラウド環境で ASA 仮想 のハイアベイラビリティを実現できるようにアクティブ/バックアップ フェールオーバーを設定する方法について説明します。

パブリック クラウドでのフェールオーバーについて

冗長性を確保するために、ASA仮想をアクティブ/バックアップハイアベイラビリティ（HA）設定でパブリッククラウド環境に展開します。パブリッククラウドでのHAでは、アクティブな ASA 仮想 の障害時に、バックアップ ASA 仮想 へのシステムの自動フェールオーバーをトリガーできるステートレスなアクティブ/バックアップソリューションが実装されます。

次のリストは、HA パブリック クラウド ソリューションの主要コンポーネントを示しています。

- **アクティブ ASA 仮想**：HA ピアのファイアウォール トラフィックを処理するように設定された HA ペア内の ASA 仮想。
- **バックアップ ASA 仮想**：ファイアウォール トラフィックを処理せず、アクティブ ASA 仮想 に障害が発生した場合にアクティブ ASA 仮想 を引き継ぐ HA ペア内の ASA 仮想。これは、フェールオーバーの際にピアの識別情報を引き継がないため、スタンバイではなくバックアップと呼ばれます。

- **HA エージェント**：ASA 仮想 上で実行され、ASA 仮想 の HA ロール（アクティブ/バックアップ）を判断し、その HA ピアの障害を検出し、その HA ロールに基づいてアクションを実行する軽量プロセス。

物理 ASA および非パブリック クラウドの仮想 ASA では、Gratuitous ARP 要求を使用してフェールオーバー条件を処理しますが、バックアップ ASA は、アクティブな IP アドレスと MAC アドレスに関連付けられていることを示す Gratuitous ARPP を送信します。ほとんどのパブリック クラウド環境では、このようなブロードキャスト トラフィックは許可されていません。このため、パブリック クラウドの HA 設定では、フェールオーバーが発生したときに通信中の接続を再起動する必要があります。

アクティブ装置の状態がバックアップ装置によってモニタされ、所定のフェールオーバー条件に一致しているかどうかが判別されます。所定の条件に一致すると、フェールオーバーが行われます。フェールオーバー時間は、パブリック クラウド インフラストラクチャの応答性に応じて、数秒～ 1 分を超える場合があります。

アクティブ/バックアップ フェールオーバーについて

アクティブ/バックアップ フェールオーバーでは、1 台の装置がアクティブ装置です。この装置がトラフィックを渡します。バックアップ装置は積極的にトラフィックを渡したり、アクティブ装置と設定情報を交換したりしません。アクティブ/バックアップ フェールオーバーでは、障害が発生した装置の機能をバックアップ ASA 仮想デバイスに引き継ぐことができます。アクティブ装置が故障すると、バックアップ状態に変わり、そしてバックアップ装置がアクティブ状態に変わります。

プライマリ/セカンダリの役割とアクティブ/バックアップ ステータス

アクティブ/バックアップ フェールオーバーを設定する場合、1 つの装置をプライマリとして設定し、もう 1 つの装置をセカンダリとして設定します。この時点で、2 つの装置は、デバイスとポリシーの設定、およびイベント、ダッシュボード、レポート、ヘルス モニタリングで、2 つの個別のデバイスとして機能します。

フェールオーバー ペアの 2 つの装置の主な相違点は、どちらの装置がアクティブでどちらの装置がバックアップであるか、つまりどちらの装置がアクティブにトラフィックを渡すかということに関連します。両方の装置がトラフィックを渡すことができますが、プライマリ装置だけがロード バランサ プローブに応答し、構成済みのルートをプログラミングしてルートの接続先として使用します。バックアップ装置の主な機能は、プライマリ装置の正常性を監視することです。両方の装置が同時にスタートアップした場合（さらに動作ヘルスが等しい場合）、プライマリ装置が常にアクティブ装置になります。

フェールオーバー接続

バックアップ ASA 仮想 は、TCP を介して確立されたフェールオーバー接続を使用して、アクティブ ASA 仮想 の正常性を監視します。

- アクティブ ASA 仮想 は、リッスンポートを開くことで接続サーバーとして機能します。

- バックアップ ASA 仮想 は、接続ポートを使用してアクティブ ASA 仮想 に接続します。
- 通常、ASA 仮想 装置間で何らかのネットワークアドレス変換が必要な場合を除き、リッスンポートと接続ポートは同じです。

フェールオーバー接続の状態によって、アクティブ ASA 仮想の障害を検出します。バックアップ ASA 仮想は、フェールオーバー接続が切断されたことを確認すると、アクティブ ASA 仮想で障害が発生したと判断します。同様に、バックアップ ASA 仮想 がアクティブ装置に送信されたキープアライブメッセージに対する応答を受信しない場合も、アクティブ ASA 仮想 で障害が発生したと判断します。

関連項目

ポーリングと Hello メッセージ

バックアップ ASA 仮想 はフェールオーバー接続を介してアクティブ ASA 仮想 に Hello メッセージを送信し、Hello 応答の返信を期待します。メッセージのタイミングには、ポーリング間隔、つまりバックアップ ASA 仮想 装置が Hello 応答を受信して次の Hello メッセージが送信されるまでの間の時間間隔が使用されます。応答の受信は、ホールド時間と呼ばれる受信タイムアウトによって強制されます。Hello 応答の受信がタイムアウトすると、アクティブ ASA 仮想 で障害が発生したとみなされます。

ポーリング間隔とホールド時間間隔は設定可能なパラメータです（アクティブ/バックアップ フェールオーバーの設定 （10 ページ） を参照）。

起動時のアクティブ装置の判別

アクティブ装置は、次の条件で判別されます。

- 装置がブートされ、ピアがすでにアクティブとして動作中であることを検出すると、その装置はバックアップ装置になります。
- 装置がブートされてピアを検出できないと、その装置はアクティブ装置になります。
- 両方の装置が同時に起動された場合は、プライマリ装置がアクティブ装置になり、セカンダリ装置がバックアップ装置になります。

フェールオーバー イベント

アクティブ/バックアップ フェールオーバーでは、フェールオーバーがユニットごとに行われます。次の表に、各障害イベントに対するフェールオーバーアクションを示します。この表には、各フェールオーバー イベントに対して、フェールオーバー ポリシー（フェールオーバーまたはフェールオーバーなし）、アクティブ装置が行うアクション、バックアップ装置が行うアクション、およびフェールオーバー条件とアクションに関する特別な注意事項を示します。

表 *1*: フェールオーバー イベント

障害イベント	ポリシー	アクティブアクション	バックアップアクション	注
バックアップ装置がフェールオーバー接続のクローズを確認	フェールオーバー	該当なし	アクティブになる アクティブを障害としてマークする	これは標準のフェールオーバーの使用例です。
アクティブ装置がフェールオーバー接続のクローズを確認	フェールオーバーなし	バックアップを障害としてマークする	n/a	非アクティブ装置へのフェールオーバーは発生しません。
アクティブ装置がフェールオーバーリンクで TCP タイムアウトを確認	フェールオーバーなし	バックアップを障害としてマークする	動作なし	アクティブ装置がバックアップ装置から応答を受信しない場合、フェールオーバーは発生しません。
バックアップ装置がフェールオーバー リンクで TCP タイムアウトを確認	フェールオーバー	該当なし	アクティブになる アクティブを障害としてマークする アクティブ装置にフェールオーバー コマンドの送信を試行する	バックアップ装置はアクティブ装置が動作を続行できないと見なし、引き継ぎます。 アクティブ装置がまだ起動しているが時間内に応答を送信できない場合、バックアップ装置はフェールオーバー コマンドをアクティブ装置に送信します。
アクティブ認証の失敗	フェールオーバーなし	なし	なし	バックアップ装置はルートテーブルを変更するため、バックアップ装置が Azure に認証する必要がある唯一の装置になります。 アクティブ装置が Azure に認証されているかどうかは関係ありません。
バックアップ認証の失敗	フェールオーバーなし	バックアップを未認証としてマークする	動作なし	バックアップ装置が Azure に認証されていない場合、フェールオーバーは発生しません。

障害イベント	ポリシー	アクティブアクション	バックアップアクション	注
アクティブ装置が意図的なフェールオーバーを開始	フェールオーバー	バックアップになる	アクティブになる	アクティブ装置は、フェールオーバー リンク接続を閉じることでフェールオーバーを開始します。 バックアップ装置は接続のクローズを確認し、アクティブ装置になります。
バックアップ装置が意図的なフェールオーバーを開始	フェールオーバー	バックアップになる	アクティブになる	バックアップ装置は、フェールオーバーメッセージをアクティブ装置に送信することによってフェールオーバーを開始します。 アクティブ装置はメッセージを確認すると、接続を閉じてバックアップ装置になります。 バックアップ装置は接続のクローズを確認し、アクティブ装置になります。
以前にアクティブだったユニットが復旧	フェールオーバーなし	バックアップになる	片方をバックアップとマークする	フェールオーバーは確実に必要でない限り発生しません。
アクティブ装置がバックアップ装置からのフェールオーバーメッセージを確認する	フェールオーバー	バックアップになる	アクティブになる	ユーザーが手動フェールオーバーを開始した場合に発生する可能性があります。または、バックアップ装置がTCPタイムアウトを確認したが、アクティブ装置がバックアップ装置からメッセージを受信できる場合に発生する可能性があります。

注意事項と制約事項

この項では、この機能のガイドラインと制限事項について説明します。

パブリッククラウドでハイアベイラビリティを実現するための ASA 仮想 のフェールオーバー

冗長性を確保するために、ASA仮想をアクティブ/バックアップ ハイ アベイラビリティ（HA）設定でパブリッククラウド環境に展開します。

- Microsoft Azure パブリッククラウドでのみサポートされています。ASA 仮想 VM を設定する場合、サポートされる vCPU の最大数は 8、サポートされる最大メモリ容量は 64GB RAM

です。サポートされるインスタンスの包括的なリストについては、『ASA 仮想 Getting Started Guide』を参照してください。

- アクティブ ASA 仮想 で障害が発生したときにバックアップ ASA 仮想 へのシステムの自動フェールオーバーをトリガーできる、ステートレスなアクティブ/バックアップ ソリューションを実装します。

制限事項

- フェールオーバーはミリ秒ではなく、秒単位で行われます。
- HA の役割の決定と HA 装置として参加できるかどうかは、HA ピア間、および HA 装置と Azure インフラストラクチャとの間の TCP 接続に依存します。ASA 仮想 が HA 装置として参加できない状況がいくつかあります。
  - HA ピアへのフェールオーバー接続を確立できない。
  - Azure から認証トークンを取得できない。
  - Azure で認証できない。
- アクティブ装置からバックアップ装置に設定が同期されることはありません。フェールオーバー トラフィックの処理に関して、各装置で同様の設定を個々に構成する必要があります。
- フェールオーバー ルートテーブルの制限

  パブリッククラウドの HA のルートテーブルには次の制限があります。
  - 設定できるルートテーブルの数は最大 16 個です。
  - ルートテーブルで設定できるルートの数は最大 64 個です。

  いずれの場合も、制限に達すると、ルートテーブルまたはルートを削除して再試行することを推奨するアラートが表示されます。
- ASDM サポートはありません。
- IPSec リモート アクセス VPN はサポートされていません。

（注） パブリック クラウドでサポートされる VPN トポロジについては、『Cisco Adaptive Security Virtual Appliance (ASAv) Quick Start Guide』を参照してください。

- ASA 仮想 の VM インスタンスは、同じ可用性セットにある必要があります。Azure の現在の ASA 仮想 ユーザーである場合、既存の展開から HA にアップグレードすることはできません。インスタンスを削除し、Azure マーケットプレイスから ASA 仮想 4 NIC HA オファリングを展開する必要があります。

パブリック クラウドでのフェールオーバーのライセンス

ASA 仮想 はシスコ スマート ソフトウェア ライセンシングを使用しています。スマート ライセンスは、通常の操作に必要です。各 ASA 仮想 は、ASA 仮想 プラットフォームライセンスを使用して個別にライセンスを取得する必要があります。ライセンスをインストールするまで、スループットは 100 Kbps に制限されるため、予備接続テストを実行できます。ASA 仮想 の正確なライセンス要件については、『Cisco ASA シリーズの機能ライセンス』ページを参照してください。

パブリック クラウドでのフェールオーバーのデフォルト

デフォルトでは、フェールオーバー ポリシーは次の事項が含まれます。

- ステートレスなフェールオーバーのみ。
- フェールオーバートラフィックの処理に関して、各装置で同様の設定を個々に構成する必要があります。
- フェールオーバーの TCP 制御ポート番号は 44442 です。
- Azure ロード バランサの健全性プローブ ポート番号は 44441 です。
- 装置のポーリング時間は 5 秒です。
- 装置のホールド時間は 15 秒です。
- ASA 仮想 はプライマリインターフェイス（管理 0/0）のヘルスプローブに応答します。
- Azure サービスプリンシパルによる ASA 仮想 の認証は、プライマリインターフェイス（管理 0/0）で実行されます。

（注） フェールオーバーポート番号、ヘルスプローブポート番号、ポーリング時間、およびプライマリインターフェイスを変更するオプションについては、オプションのフェールオーバー パラメータの設定 （13 ページ）を参照してください。

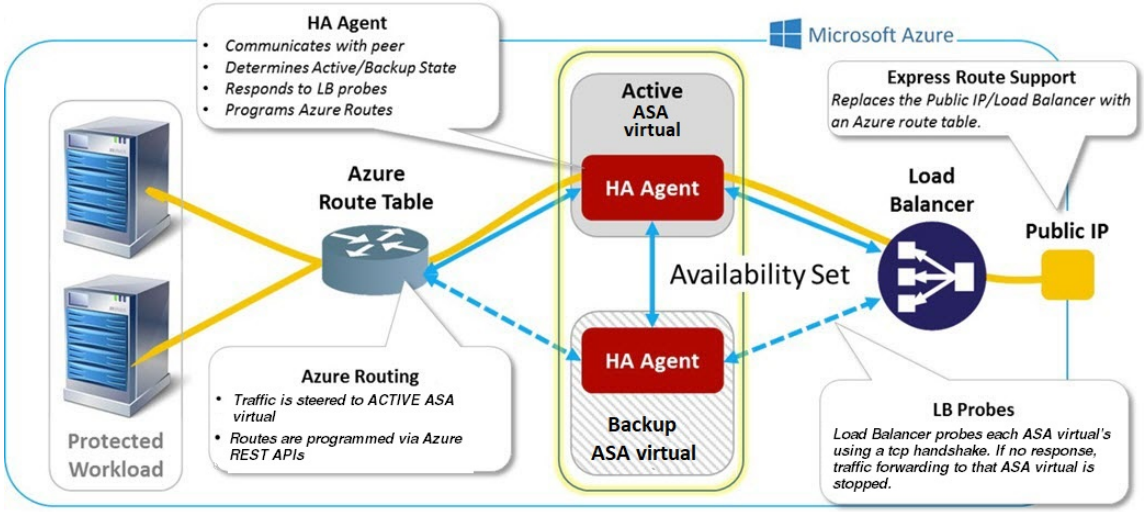
Microsoft Azure での ASA 仮想 ハイアベイラビリティについて

次の図に、Azure での ASA 仮想 HA 展開の概要を示します。アクティブ/バックアップ フェールオーバー設定の 2 つの ASA 仮想 インスタンスの背後でワークロードが保護されます。Azure ロードバランサは、3 ウェイ TCP ハンドシェイクを使用して両方の ASA 仮想 ユニットをプローブします。アクティブ ASA 仮想 は、3 ウェイハンドシェイクを完了して正常であること

を示しますが、バックアップ ASA 仮想 は意図的に応答しません。ロードバランサに応答しないことで、バックアップASA仮想はロードバランサには正常ではないように見え、トラフィックが送信されません。

フェールオーバーでは、アクティブ ASA 仮想 がロードバランサプローブへの応答を停止し、バックアップASA仮想が応答を開始することで、すべての新しい接続がバックアップASA仮想に送信されます。バックアップASA仮想は、ルートテーブルを変更してトラフィックがアクティブユニットからバックアップユニットにリダイレクトされるように API 要求を Azure ファブリックに送信します。この時点で、バックアップ ASA 仮想 がアクティブユニットになり、アクティブユニットは、フェールオーバーの理由に応じてバックアップユニットになるかオフラインになります。

図 *1 : Azure* での *ASA* 仮想 *HA* 展開



自動的に API 呼び出しによって Azure ルートテーブルが変更されるようにするには、ASA 仮想 HA ユニットに Azure Active Directory のログイン情報が必要です。Azure は、簡単に言えばサービス アカウントであるサービス プリンシパルの概念を採用しています。サービス プリンシパルを使用すると、あらかじめ定義されたAzureリソースセット内でタスクを実行するのに十分な権限と範囲のみを持つアカウントをプロビジョニングできます。

ASA 仮想 HA 展開でサービスプリンシパルを使用して Azure サブスクリプションを管理できるようにするには、次の 2 つの手順を実行します。

1. 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（Azure サービス プリンシパルについて （9 ページ） を参照）。
2. サービスプリンシパルを使用して Azure で認証するように ASA 仮想 インスタンスを設定します（「アクティブ/バックアップ フェールオーバーの設定 （10 ページ）」を参照）。

関連項目

ロード バランサの詳細については、Azure のマニュアルを参照してください。

Azure サービス プリンシパルについて

Azure リソース（ルート テーブルなど）へのアクセスまたはリソースの変更が必要となるアプリケーションがある場合は、Azure Active Directory（AD）アプリケーションを設定し、必要な権限を割り当てる必要があります。この方法は、以下の理由から、自分のクレデンシャルでアプリケーションを実行するよりも推奨されます。

- 自分の権限とは異なる権限をアプリケーション ID に割り当てることができる。通常、割り当てる権限は、アプリケーションが実行する必要があるものだけに制限します。
- 職責が変わった場合でも、アプリケーションのクレデンシャルを変更する必要がない。
- 無人スクリプトの実行時に、証明書を使用して認証を自動化できる。

Azure ポータルに Azure AD アプリケーションを登録すると、アプリケーション オブジェクトとサービス プリンシパル オブジェクトの 2 つのオブジェクトが Azure AD テナントに作成されます。

- **アプリケーション オブジェクト**：Azure AD アプリケーションは、そのアプリケーションが登録されている Azure AD テナント（アプリケーションの「ホーム」テナント）にある唯一のアプリケーション オブジェクトによって定義されます。
- **サービス プリンシパル オブジェクト**：サービス プリンシパル オブジェクトは、特定のテナントでのアプリケーションの使用に関するポリシーと権限を定義し、アプリケーション実行時のセキュリティ プリンシパルの基礎を提供します。

Azure は、『*Azure Resource Manager Documentation*』で Azure AD アプリケーションとサービス プリンシパルを作成する方法について説明しています。詳しい手順については、次のトピックを参照してください。

- リソースにアクセスできる Azure AD アプリケーションとサービス プリンシパルをポータルで作成する
- Azure PowerShell を使用して資格情報でのサービス プリンシパルを作成する

（注） サービス プリンシパルを設定したら、**ディレクトリ ID**、**アプリケーション ID**、および**秘密鍵**を取得します。これらは、Azure 認証クレデンシャルを設定するために必要です（アクティブ/バックアップ フェールオーバーの設定 （10 ページ） を参照）。

Azure での ASA 仮想 ハイアベイラビリティの設定要件

#unique_480 unique_480_Connect_42_fig_cgx_dlh_h1b で説明しているのと同じ設定を導入するには、以下が必要です。

- 次の Azure 認証情報（Azure サービス プリンシパルについて （9 ページ） を参照）
  - ディレクトリ ID

- Application ID
- 秘密鍵

- 次の Azure ルート情報（Azure ルート テーブルの設定 （13 ページ） を参照）。
  - Azure サブスクリプション ID
  - ルート テーブル リソース グループ
  - テーブル名
  - アドレス プレフィックス
  - ネクスト ホップ アドレス。

- 次の ASA 設定（アクティブ/バックアップ フェールオーバーの設定 （10 ページ）、パブリック クラウドでのフェールオーバーのデフォルト （7 ページ） を参照）
  - アクティブ/バックアップ IP アドレス
  - HA エージェント通信ポート
  - ロード バランサのプローブ ポート
  - ポーリング間隔

（注） プライマリ装置とセカンダリ装置の両方で基本のフェールオーバー設定を構成します。プライマリ装置からセカンダリ装置に設定が同期されることはありません。フェールオーバー トラフィックの処理に関して、各装置で同様の設定を個々に構成する必要があります。

アクティブ/バックアップ フェールオーバーの設定

アクティブ/バックアップ フェールオーバーを設定するには、プライマリ装置とセカンデリ装置の両方で基本的なフェールオーバー設定を構成します。プライマリ装置からセカンダリ装置に設定が同期されることはありません。フェールオーバー トラフィックの処理に関して、各装置で同様の設定を個々に構成する必要があります。

始める前に

- Azure 可用性セットで ASA 仮想 HA ペアを展開します。
- Azure サブスクリプション ID とサービス プリンシパルの Azure 認証クレデンシャルを含む、Azure 環境情報を入手します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[Failover]** の順に選択します。

ステップ 2 [Cloud] タブで、[Unit] チェックボックスをオンにして [Failover Unit] ドロップダウン オプションを展開します。

ステップ 3 [Failover Unit] ドロップダウン メニューから [primary] を選択します。

両方の HA 装置が同時に起動した場合は、プライマリ装置がアクティブな HA ロールを引き受けます。

ステップ 4 （オプション）[Port] チェックボックスをオンにして、[Control] および [Probe] フィールドを展開します。

a) [Control] フィールドに有効な TCP 制御ポートを入力します。または、デフォルトのポート 44442 のままにします。

制御ポートは、アクティブ ASA 仮想とバックアップ ASA 仮想間で TCP フェールオーバー接続を確立します。

b) [Probe] フィールドに有効な TCP プローブ ポートを入力します。または、デフォルトのポート 44441 のままにします。

プローブ ポートは、Azure ロード バランサ プローブの宛先ポートとして使用される TCP ポートです。

ステップ 5 （オプション）[Time] チェックボックスをオンにして、[Poll Time] および [Hold Time] フィールドを展開します。

a) [Poll Time] フィールドに有効な時間（秒）を入力します。または、デフォルトの 5 秒のままにします。

ポーリング時間の範囲は、1 ～ 15 秒です。ポーリング間隔を短くすると、ASA で障害を検出し、フェールオーバーをトリガーする速度が速くなります。ただし短時間での検出は、ネットワークが一時的に輻輳した場合に不要な切り替えが行われる原因となります。

b) [Hold Time] フィールドに有効な時間（秒）を入力します。または、デフォルトの 15 秒のままにします。

hello パケットを受信できなかったときから装置が失敗としてマークされるまでの時間が、保持時間によって決まります。ホールド時間の範囲は 3 ～ 60 秒です。装置のポーリング時間の 3 倍未満のホールド時間の値を入力することはできません。

ステップ 6 [Peer] チェックボックスをオンにして、[Peer IP-Address] および [Peer Port] フィールドを展開します。

a) [Peer IP-Address] フィールドに、HA ピアへの TCP フェールオーバー制御接続を確立するために使用する IP アドレスを入力します。

b) （オプション）[Peer Port] フィールドに有効な TCP 制御ポートを入力します。mataha,デフォルトのポート 44442 のままにします。

ピアポートは、アクティブ ASA 仮想 とバックアップ ASA 仮想 間で TCP フェールオーバー接続を確立します。

ステップ 7 [Authentication] チェックボックスをオンにして、[Application-id]、[Directory-id]、および [Key] フィールドを展開します。

Azure サービスプリンシパルの認証クレデンシャルを設定できます。この認証クレデンシャルにより、ASA 仮想 HA ピアがルートテーブルなどの Azure リソースにアクセスしたり、それらのリソースを変更したりできるようになります。サービスプリンシパルを使用すると、定義済みの Azure リソース セット内でタスクを実行するための最小限の権限を持つ Azure アカウントをプロビジョニングできます。ASA 仮想 HA の場合は、ユーザー定義のルートを変更するのに必要な権限に制限されます（「Azure サービス プリンシパルについて （9 ページ）」を参照）。

a) Azure サービス プリンシパルの Azure アプリケーション ID を [Application-id] フィールドに入力します。

Azure インフラストラクチャからアクセス キーを要求するときは、このアプリケーション ID が必要です。

b) Azure サービス プリンシパルの Azure ディレクトリ ID を [Directory-id] フィールドに入力します。

Azure インフラストラクチャからアクセス キーを要求するときは、このディレクトリ ID が必要です。

c) Azure サービス プリンシパルの Azure 秘密鍵を [Key] フィールドに入力します。

Azure インフラストラクチャからアクセス キーを要求するときは、この秘密鍵が必要です。[Encrypt] フィールドがオンの場合、この秘密鍵は実行コンフィギュレーションで暗号化されます。

ステップ 8 [Subscription] チェックボックスをオンにして、[Sub-id] フィールドを展開します。

これは、更新が必要なルート テーブルが属するアカウントのサブスクリプション ID です。

ステップ 9 [Enable Cloud Failover] チェックボックスをオンにします。

ステップ 10 [Apply] をクリックします。

デバイスに変更を適用するまで、フェールオーバーは実際にはイネーブルになりません。

ステップ 11 セカンダリ装置でまだフェールオーバーが有効になっていない場合は、[デバイスリスト（Device List）] からセカンダリ ASA 仮想 に接続するか、ASA 仮想 の IP アドレス **https**://*asa_ip_address*/**admin** を使用して新しい ASDM セッションを開始します。

ステップ 12 手順 1 ～ 10 を繰り返して、セカンダリ装置でアクティブ/バックアップ フェールオーバーを設定します。

プライマリ装置からセカンダリ装置に設定が同期されることはありません。フェールオーバートラフィックの処理に関して、各装置で同様の設定を個々に構成する必要があります。

デバイスに変更を適用するまで、フェールオーバーは実際にはイネーブルになりません。

次のタスク

必要に応じて、追加のパラメータを設定します。

- Azure ルート情報の設定（Azure ルート テーブルの設定 （13 ページ） を参照）。

オプションのフェールオーバー パラメータの設定

必要に応じてフェールオーバー設定をカスタマイズできます。

Azure ルート テーブルの設定

ルートテーブル設定は、ASA 仮想 がアクティブなロールを引き継ぐときに更新する必要のある Azure ユーザー定義ルートに関する情報で構成されています。フェールオーバーでは、内部ルートをアクティブ装置に向ける必要があります。アクティブ装置は、設定されたルートテーブル情報を使用して自動的にルートを自身に向けます。

（注） アクティブ装置とバックアップ装置の両方でAzureルートテーブル情報を設定する必要があります。

始める前に

- プライマリ装置とセカンダリ装置の両方でこれらの設定を構成します。プライマリ装置からセカンダリ装置への設定の同期はありません。
- Azure サブスクリプション ID とサービス プリンシパルの Azure 認証クレデンシャルを含む、Azure 環境情報を入手します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[Failover]** の順に選択します。

ステップ 2 [Route-Table] タブをクリックして、[Add] をクリックします。

a) [Route Table Name] フィールドに、ルート テーブルの名前を入力します。

最大 16 個のルート テーブルを設定できます。または、ルート テーブル リストのエントリを編集または削除できます。

b) （オプション）[Sub-id] フィールドに、Azure サブスクリプション ID を入力します。

ここで対応する Azure サブスクリプション ID を指定することで、2 つ以上の Azure サブスクリプションのユーザー定義ルートを更新できます。Azure サブスクリプション ID を指定せずに [Route Table Name] を入力すると、グローバル パラメータが使用されます。

（注）
[Configuration] > **[Device Management]** > **[High Availability and Scalability]** > **[Failover]** からアクティブ/バックアップ フェールオーバーを設定するときに、Azure サブスクリプション ID を入力します（アクティブ/バックアップ フェールオーバーの設定 （10 ページ）を参照）。

ステップ 3 [Route-Table-Mode] をクリックします。ルート テーブルへのエントリを追加、編集、または削除できます。

ステップ 4 [Add] をクリックします。

Azure ユーザー定義ルートに対して次の値を入力します。

a) [Route Table] ドロップダウン リストからルート テーブルを選択します。
b) [Azure Resource Group] フィールドに、Azure ルート テーブルを含む Azure リソース グループの名前を入力します。
c) [Route Name] フィールドに、ルートの一意の名前を入力します。
d) [Prefix Address/Mask] フィールドに、CIDR 表記で IP アドレス プレフィックスを入力します。
e) [Next Hop Address] フィールドに、ネクストホップ アドレスを入力します。これは、ASA 仮想 のインターフェイスの IP アドレスです

（注）
最大 64 個のルートを設定できます。

ステップ 5 [Apply] をクリックして変更内容を保存します。

パブリック クラウドでのフェールオーバーの管理

この項では、フェールオーバーを有効にした後でクラウド内の フェールオーバー 装置を管理する方法について説明します。ある装置から別の装置にフェールオーバーを強制的に変更する方法についても説明します。

フェールオーバーの強制実行

スタンバイ装置を強制的にアクティブにするには、次のコマンドを実行します。

始める前に

シングル コンテキスト モードのシステム実行スペースで次のコマンドを使用します。

手順

ステップ 1 **[Monitoring]** > **[Properties]** > **[Failover]** > **[Status]** の順に選択します。

ステップ 2 装置レベルでフェールオーバーを強制するには、次のいずれかのボタンをクリックします。

- 装置をアクティブ装置にするには、[Make Active] をクリックします。
- 装置をスタンバイ装置にするには、[Make Standby] をクリックします。

ルートの更新

Azure のルートの状態がアクティブロールの ASA 仮想 と矛盾している場合は、次のように ASA 仮想 でルート更新を強制できます。

始める前に

シングル コンテキスト モードのシステム実行スペースで次のコマンドを使用します。

手順

ステップ 1 **[Monitoring]** > **[Properties]** > **[Failover]** > **[Status]** の順に選択します。

ステップ 2 [Update Route] をクリックします。

このコマンドは、アクティブロールの ASA 仮想 でのみ有効です。認証に失敗すると、出力は `Route changes failed` となります。

Azure 認証の検証

Azure で ASA 仮想 HA の展開を成功させるには、サービスプリンシパルの設定が完全かつ正確である必要があります。適切な Azure 認証がないと、ASA 仮想 ユニットはリソースにアクセスして、フェールオーバーを処理したりルート更新を実行したりできません。フェールオーバー設定をテストして、Azure サービス プリンシパルの次の要素に関連するエラーを検出できます。

- ディレクトリ ID
- Application ID

- Authentication Key

始める前に

シングル コンテキスト モードのシステム実行スペースで次のコマンドを使用します。

手順

ステップ 1 **[Monitoring]** > **[Properties]** > **[Failover]** > **[Status]** の順に選択します。

ステップ 2 [Test Authentication] をクリックします。

認証に失敗すると、コマンド出力は `Authentication Failed` となります。

ディレクトリ ID またはアプリケーション ID が正しく設定されていない場合、Azure は認証トークンを取得するための REST 要求で指定されたリソースを認識しません。この条件エントリのイベント履歴は次のようになります。

```
Error Connection - Unexpected status in response to access token request: Bad Request
```

ディレクトリ ID またはアプリケーション ID は正しいが、認証キーが正しく設定されていない場合、Azure は認証トークンを生成する権限を許可しません。この条件エントリのイベント履歴は次のようになります。

```
Error Connection - Unexpected status in response to access token request: Unauthorized
```

パブリック クラウドでのフェールオーバーのモニター

この項では、フェールオーバー ステータスをモニターする方法について説明します。

フェールオーバー ステータス

（注） フェールオーバー イベントが発生した後、デバイスのモニタリングを継続するには、ASDM を再起動するか、または [Devices] ペインに表示される別のデバイスに切り替えて、元の ASA に戻る手順を実行する必要があります。この操作が必要なのは、ASDM がデバイスから切断されて再接続された場合、接続のモニタリングが再確立されないためです。

- アクティブ/バックアップ フェールオーバー ステータスをモニターするには、**[Monitoring]** > **[Properties]** > **[Failover]** > **[Status]** を選択し、[Failover Status] をクリックします。
- タイムスタンプ、重大度レベル、イベント タイプ、およびイベント テキストを含むフェールオーバー イベント履歴を表示するには、**[Monitoring]** > **[Properties]** > **[Failover]** > **[History]** を選択します。

フェールオーバー メッセージ

フェールオーバーの syslog メッセージ

ASA は、深刻な状況を表すプライオリティ レベル 2 のフェールオーバーについて、複数の syslog メッセージを発行します。これらのメッセージを表示するには、syslog メッセージ ガイドを参照してください。Syslog メッセージの範囲は 1045xx と 1055xx です。

（注） フェールオーバーの最中に、ASA は論理的にシャットダウンした後、インターフェイスを起動し、syslog メッセージを生成します。これは通常のアクティビティです。

スイッチオーバー中に生成される syslog の例を次に示します。

```
%ASA-3-105509: (Primary) Error sending Hello message to peer unit 10.22.3.5, error:
Unknown error
%ASA-1-104500: (Primary) Switching to ACTIVE - switch reason: Unable to send message to
 Active unit
%ASA-5-105522: (Primary) Updating route-table wc-rt-inside
%ASA-5-105523: (Primary) Updated route-table wc-rt-inside
%ASA-5-105522: (Primary) Updating route-table wc-rt-outside
%ASA-5-105523: (Primary) Updated route-table wc-rt-outside
%ASA-5-105542: (Primary) Enabling load balancer probe responses
%ASA-5-105503: (Primary) Internal state changed from Backup to Active no peer
%ASA-5-105520: (Primary) Responding to Azure Load Balancer probes
```

パブリック クラウドの導入に関連する各 syslog には、装置の役割が最初に追加されます（(Primary) または (Secondary)）。

フェールオーバー デバッグ メッセージ

デバッグ メッセージを表示するには、**debug fover** コマンドを入力します。詳細については、コマンド リファレンスを参照してください。

（注） CPUプロセスではデバッグ出力に高プライオリティが割り当てられているため、デバッグ出力を行うとシステムパフォーマンスに大きく影響することがあります。このため、特定の問題のトラブルシューティングを行う場合や、Cisco TAC とのトラブルシューティング セッションの間に限り **debug fover** コマンドを使用してください。

SNMP のフェールオーバー トラップ

フェールオーバーに対する SNMP syslog トラップを受信するには、SNMP トラップを SNMP 管理ステーションに送信するように SNMP エージェントを設定し、syslog ホストを定義し、お使いの SNMP 管理ステーションに Cisco syslog MIB をコンパイルします。

パブリック クラウドでのフェールオーバーの履歴

機能名	リリース	機能情報
Microsoft Azure でのアクティブ/バックアップ フェールオーバー	7.9(1)	この機能が導入されました。

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。