# ACI サイトのインフラ コンフィギュレーションの展開



## インフラ設定の展開

ここでは、各 APIC サイトにインフラ設定を展開する方法について説明します。

### 手順

**ステップ 1** メイン ペインの右上の **[展開 (deploy)]** をクリックして、適切なオプションを選択して設定を展開します。

オンプレミスまたはクラウド サイトのみを設定した場合は、**[展開（Deploy）]** をクリックしてインフラ設定を展開します。

ただし、オンプレミスとクラウド サイトの両方がある場合は、次の 2 つの追加オプションを使用できます。

- **展開 & IPN デバイス設定ファイルをダウンロード（Deploy & Download IPN Device config files）:** オンプレミスの APIC サイトとクラウド IPN サイトの両方に設定をプッシュし、オンプレミスとクラウド サイト間のエンドツーエンド インターコネクトを有効にします。

  さらに、このオプションでは、クラウド サイトに導入された Cisco クラウド サービス ルータ（CSR）とオンプレミスの IPsec 終端デバイスとの間の接続を有効にするための設定情報を含む zip ファイルをダウンロードします。すべてまたは一部の設定ファイルのどちらをダウンロードするかを選択できるようにするための、フォローアップ画面が表示されます。

- **IPN デバイス設定ファイルのみダウンロード:** 設定を展開することなく Cisco クラウド サービス ルータ（CSR）間との接続を有効にするために使用する設定情報を含む zip ファイルをダウンロードします。

**ステップ 2** [確認（Confirmation）] ウィンドウで、**[はい（Yes）]** をクリックします。

[展開が開始されました。個々のサイトの展開ステータスについては左側のメニューを参照します。] メッセージが表示され、インフラ構成の展開が開始されたことが示されます。左側のペインのサイト名の横に表示されるアイコンで各サイトの進行状況を確認できます。

### 次のタスク

インフラ オーバーレイとアンダーレイの構成設定が、すべてのサイトのコントローラとクラウド CSR に展開されました。残りの手順では、サイト接続性情報の更新 の説明のように IPN デバイスをクラウド CSR のトンネルを使用して設定します。

# オンプレミスとクラウド サイト間の接続の有効化

オンプレミス サイトまたはクラウド サイトのみがある場合は、このセクションをスキップできます。

ここでは、オンプレミス APIC サイトとクラウド APIC サイト間の接続を有効にする方法について説明します。

デフォルトでは、Cisco Cloud APIC は冗長 Cisco Cloud サービス ルータ 1000V のペアを展開します。この項の手順では、2 つのトンネルを作成します。1 つはオンプレミスの IPsec デバイスからこれらの各 Cisco Cloud サービス ルータ 1000V 対する IPsec トンネルです。複数のオンプレミス IPsec デバイスがある場合は、各オンプレミス デバイスの CSR に同じトンネルを設定する必要があります。

次の情報は、オンプレミスの IPsec ターミネーション デバイスとして Cisco Cloud サービス ルータ 1000V のコマンドを提供します。別のデバイスまたはプラットフォームを使用している場合は、同様のコマンドを使用します。

### 手順

**ステップ 1** クラウド サイトに導入された CSR とオンプレミス IPsec ターミネーション デバイスとの間の接続を有効にするために必要な情報を収集します。

の手順の一部として、Nexus Dashboard Orchestrator の **[IPN デバイス設定ファイルの展開とダウンロード（Deploy & Download IPN Device config files）]** オプションまたは **[IPN デバイス設定ファイルのダウンロードのみ（Download IPN Device config files only）** オプションを使用して、必要な設定の詳細を取得できます。インフラ設定の展開 （1 ページ）

**ステップ 2** オンプレミスの IPsec デバイスにログインします。

**ステップ 3** 最初の CSR のトンネルを設定します。

最初の CSR の詳細は、Nexus Dashboard Orchestrator からダウンロードした ISN デバイスのコンフィギュレーション ファイルで確認できますが、次のフィールドには、特定の展開の重要な値が示されます。

- <*first-csr-tunnel-ID*> は、このトンネルに割り当てる一意のトンネル ID です。

- <*first-csr-ip-address*> は、最初の CSR の 3 番目のネットワーク インターフェイスのパブリック IP アドレスです。

  トンネルの宛先は、アンダーレイ接続のタイプによって異なります。

  - アンダーレイがパブリック インターネット経由の場合、トンネルの宛先はクラウド ルータ インターフェイスのパブリック IP です。
  - アンダーレイがプライベート接続（AWS の DX や Azure の ER など）を介している場合、トンネルの宛先はクラウド ルータ インターフェイスのプライベート IP です。

- <*first-csr-preshared-key*> は、最初の CSR の事前共有キーです。
- <*onprem-device-interface*> は、Amazon Web Services に展開された Cisco Cloud サービス ルータ 1000V への接続に使用されるインターフェイスです。
- <*onprem-device-ip-address*> は、Amazon Web Services に展開された Cisco Cloud サービス ルータ 1000V への接続に使用される <*interface*> インターフェイスです。
- <*peer-tunnel-for-onprem-IPsec-to-first-CSR*> は、最初のクラウド CSR に対してオンプレミスの IPsec デバイスのピア トンネル IP アドレスとして使用されます。
- <*process-id*> は OSPF プロセス ID です。
- <*area-id*> は、OSPF エリア ID です。

次の例は、Nexus Dashboard Orchestrator リリース 3.3(1) および Cloud APIC リリース 5.2(1) 以降でサポートされている IKEv2 プロトコルを使用したサイト間接続設定を示しています。IKEv1 を使用している場合は、NDO からダウンロードした IPN 設定ファイルの外観が若干異なる場合がありますが、原則は同じです。

```
crypto ikev2 proposal ikev2-proposal-default
    encryption aes-cbc-256 aes-cbc-192 aes-cbc-128
    integrity sha512 sha384 sha256 sha1
    group 24 21 20 19 16 15 14 2
exit

crypto ikev2 policy ikev2-policy-default
    proposal ikev2-proposal-default
exit

crypto ikev2 keyring key-ikev2-infra:overlay-1-<first-csr-tunnel-id>
    peer peer-ikev2-keyring
        address <first-csr-ip-address>
        pre-shared-key <first-csr-preshared-key>
    exit
exit

crypto ikev2 profile ikev2-infra:overlay-1-<first-csr-tunnel-id>
    match address local interface <onprem-device-interface>
    match identity remote address <first-csr-ip-address> 255.255.255.255
    identity local address <onprem-device-ip-address>
    authentication remote pre-share
    authentication local pre-share
    keyring local key-ikev2-infra:overlay-1-<first-csr-tunnel-id>
    lifetime 3600
    dpd 10 5 on-demand
exit
```

```
crypto ipsec transform-set infra:overlay-1-<first-csr-tunnel-id> esp-gcm 256
    mode tunnel
exit

crypto ipsec profile infra:overlay-1-<first-csr-tunnel-id>
    set pfs group14
    set ikev2-profile ikev2-infra:overlay-1-<first-csr-tunnel-id>
    set transform-set infra:overlay-1-<first-csr-tunnel-id>
exit

interface tunnel 2001
    ip address <peer-tunnel-for-onprem-IPsec-to-first-CSR> 255.255.255.252
    ip virtual-reassembly
    tunnel source <onprem-device-interface>
    tunnel destination <first-csr-ip-address>
    tunnel mode ipsec ipv4
    tunnel protection ipsec profile infra:overlay-1-<first-csr-tunnel-id>
    ip mtu 1400
    ip tcp adjust-mss 1400
    ip ospf <process-id> area <area-id>
    no shut
exit
```

例：

```
crypto ikev2 proposal ikev2-proposal-default
    encryption aes-cbc-256 aes-cbc-192 aes-cbc-128
    integrity sha512 sha384 sha256 sha1
    group 24 21 20 19 16 15 14 2
exit

crypto ikev2 policy ikev2-policy-default
    proposal ikev2-proposal-default
exit

crypto ikev2 keyring key-ikev2-infra:overlay-1-2001
    peer peer-ikev2-keyring
        address 52.12.232.0
        pre-shared-key 144904725321902286651389219409672714611O
    exit
exit

crypto ikev2 profile ikev2-infra:overlay-1-2001
    ! Please change GigabitEthernet1 to the appropriate interface
    match address local interface GigabitEthernet1
    match identity remote address 52.12.232.0 255.255.255.255
    identity local address 128.107.72.62
    authentication remote pre-share
    authentication local pre-share
    keyring local key-ikev2-infra:overlay-1-2001
    lifetime 3600
    dpd 10 5 on-demand
exit

crypto ipsec transform-set infra:overlay-1-2001 esp-gcm 256
    mode tunnel
exit

crypto ipsec profile infra:overlay-1-2001
    set pfs group14
    set ikev2-profile ikev2-infra:overlay-1-2001
    set transform-set infra:overlay-1-2001
exit

! These tunnel interfaces establish point-to-point connectivity between the on-prem device and the
```

```
 cloud Routers
! The destination of the tunnel depends on the type of underlay connectivity:
! 1) The destination of the tunnel is the public IP of the cloud Router interface if the underlay
is via internet
! 2) The destination of the tunnel is the private IP of the cloud Router interface if the underlay
 is via private
     connectivity like DX on AWS or ER on Azure

interface tunnel 2001
    ip address 5.5.1.26 255.255.255.252
    ip virtual-reassembly
    ! Please change GigabitEthernet1 to the appropriate interface
    tunnel source GigabitEthernet1
    tunnel destination 52.12.232.0
    tunnel mode ipsec ipv4
    tunnel protection ipsec profile infra:overlay-1-2001
    ip mtu 1400
    ip tcp adjust-mss 1400
    ! Please update process ID according with your configuration
    ip ospf 1 area 0.0.0.1
    no shut
exit
```

**ステップ 4** 設定する必要があるその他の CSR について、前の手順を繰り返します。

**ステップ 5** オンプレミスの IPsec デバイスでトンネルがアップしていることを確認します。

ステータスを表示するには、次のコマンドを使用します。両方のトンネルがアップとして表示されていない場合は、この項の手順で入力した情報を確認して、問題が発生している可能性がある場所を確認します。両方のトンネルがアップとして表示されるまで、次のセクションに進まないでください。

```
ISN_CSR# show ip interface brief | include Tunnel
Interface              IP-Address      OK? Method Status                Protocol
Tunnel1000             30.29.1.2         YES manual up                    up
Tunnel1001             30.29.1.4         YES manual up                    up
```

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。