Intercloud Fabric Router（CSR）のインストールと設定

This chapter contains the following sections:

Intercloud Fabric Router（CSR）について

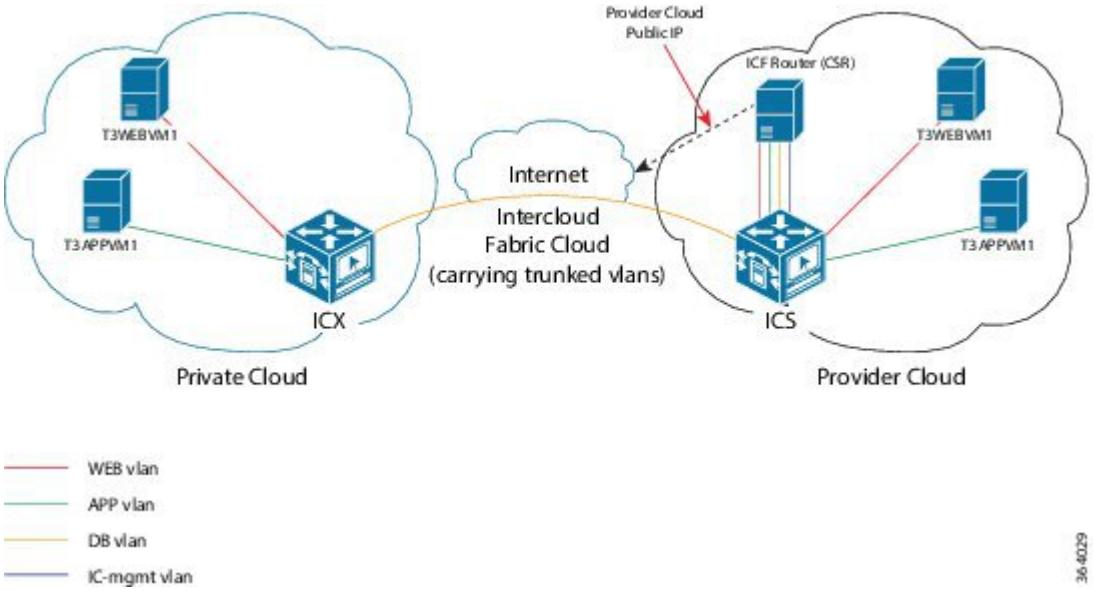
Intercloud Fabric Router（CSR）は、x86 サーバ ハードウェア上の仮想マシン（VM）インスタンスに配置されるクラウドベースの仮想ルータを提供します。 Intercloud Fabric Router（CSR）は、指定された Cisco IOS XE セキュリティ機能とスイッチング機能を仮想化プラットフォーム上で提供する仮想プラットフォームです。

Intercloud Fabric Router（CSR）は、Intercloud Fabric でエッジ デバイスとして動作し、次の機能を備えています。

- プロバイダー クラウドの仮想マシンに VLAN 間ルーティングを提供。
- プロバイダー クラウドの仮想マシンの NAT ゲートウェイとして機能。
- プロバイダー クラウドの仮想マシンに VPN 間ルーティングを提供。

- プライベート クラウドからプロバイダー クラウドへのデフォルト ゲートウェイの拡張を実現。

図 *1*：*Intercloud Fabric Router*（*CSR*）のトポロジ



Intercloud Fabric Router（CSR）は、プライベートおよびプロバイダー クラウド ソリューションのために Amazon Web Service（AWS）に展開することもできます。 Intercloud Fabric Router AMI の展開については、『Cisco CSR 1000V Series Cloud Services Router Deployment Guide for Amazon Web Services』を参照してください。

注意事項と制約事項

- Intercloud Fabric Router（CSR）は Microsoft Azure ではサポートされません。
- Intercloud Fabric Router には Intercloud Fabric（CSR）バージョン 3.14 が必要です。
- Intercloud Fabric Router（CSR）のネットワーク アドレス変換（NAT）機能は、Amazon Web Service（AWS）のアカウントにデフォルト VPC がある場合にのみ使用できます。
- Cisco Intercloud Services – V と連携している場合にダイナミック NAT を設定すると、リターン ネットワーク トラフィックが Intercloud Fabric Router（CSR）クラウド VM に到達できなくます。
- Intercloud Fabric Router（CSR）をプロバイダー クラウドに 展開する際に、プロバイダー クラウドに拡張されない VLAN のプライベート クラウド仮想マシンとプロバイダー クラウド仮想マシンとの間で、VLAN 間トラフィックが停止する可能性があります。デフォルト ゲートウェイとして設定されているデータ インターフェイスに、拡張されないプライベート クラウド VLAN のルーティングを追加する必要があります。 デフォルト ゲートウェイとして設定されているデータ インターフェイスがない場合は、拡張されないプライベート クラウ

ド VLAN のいずれかを使ってデータ インターフェイスを追加します。 次に、そのインターフェイスに残りの VLAN のルーティングを追加します。

- Intercloud Fabric Router（CSR）のインスタンスを削除し、すぐに同じ Intercloud Fabric Cloud で、その Intercloud Fabric Router（CSR）の同じまたは別のインスタンスを再作成しようとすると、「`can't create; object already exists`」というエラー メッセージが表示されることがあります。 10 分間待ってから、Intercloud Fabric Cloud で Intercloud Fabric Router（CSR）の新しいインスタンスを作成することをお勧めします。

前提条件

- プロバイダー クラウドのアカウントを取得しておきます。
- Amazon Web Services の場合は、Intercloud Fabric Router（CSR）AMI を AWS に展開しておきます。 Intercloud Fabric Router AMI の展開については、『Cisco CSR 1000V Series Cloud Services Router Deployment Guide for Amazon Web Services』を参照してください。
- Amazon Web Services の場合、Intercloud Fabric Router から Intercloud Fabric（CSR）AMI を起動するには、事前に、次のいずれかの方法で契約条件に同意しておく必要があります。
  - Amazon Web Services マーケットプレイスで、Cisco CSR を検索し、Cisco CSR release 3.14.01.S Bring Your Own License（BYOL）の契約条件に同意します。
  - Amazon Web Services マーケットプレイスのアカウントから、Cisco CSR release 3.14.01.S Bring Your Own License（BYOL）付きの EC2 インスタンスを起動し、契約条件に同意します。
- Intercloud Fabric（CSR）の仮想データセンターをプロビジョニングする際は、仮想データセンターに関連付けられているネットワーク ポリシーに、Intercloud Fabric Router（CSR）のデータ インターフェイスの作成に必要な VLAN が含まれていることを確認します。

InterCloudFabricRouter（CSR）のインストールと設定に関するワークフロー

Intercloud Fabric 用の Intercloud Fabric Router（CSR）のインストールおよび設定は、以下の手順で行います。

手順

ステップ 1 Amazon Web Services の場合は、Intercloud Fabric を使用して、Amazon Web Services から Intercloud Fabric Router（CSR）を検出する。
Intercloud Fabric Cloud の作成を参照してください。

ステップ 2 他のプロバイダーの場合はすべて、Intercloud Fabric から Intercloud Fabric Router（CSR）サービスを作成するか、Intercloud Fabric Cloud の作成後に Intercloud Fabric Router（CSR）サービスを有効化する。

- Intercloud Fabric Cloud の作成を参照してください。
- Intercloud Fabric Cloud の作成時にサービスを有効化しなかった場合は、サービスの管理 を参照してください。

ステップ 3 Intercloud Fabric を使用して、Cisco Prime Network Services Controller から Intercloud Fabric Router（CSR）をインスタンス化する。
Intercloud Fabric Router（CSR）のインスタンス化, （16 ページ）を参照してください。

a) Cisco Prime Network Services Controller を使用して管理インターフェイスを作成する。Intercloud Fabric Router（CSR）をインスタンス化する際に、Prime Network Services Controller の [Add Edge Router] ウィザードで管理インターフェイスを作成できます。

b) Cisco Prime Network Services Controller を使用して、クラウド インターフェイスを作成する。Intercloud Fabric Router（CSR）をインスタンス化する際に、Prime Network Services Controller の [Add Edge Router] ウィザードでクラウド インターフェイスを作成できます。

c) Prime Network Services Controller を使用して、クラウドのパブリック インターフェイスを作成する。 パブリック クラウド インターフェイスは、NAT と VPN の設定に必要です。

ステップ 4 （任意） ネットワーク アドレス変換（NAT）およびポート アドレス変換（PAT）のポリシーを設定する。
ネットワーク アドレス変換およびポート アドレス変換のポリシーの設定, （21 ページ）を参照してください。

ステップ 5 Cisco Prime Network Services Controller を使用して、Intercloud Fabric Router（CSR）のインストールを確認する。
Intercloud Fabric Router のインストールの確認, （25 ページ）を参照してください。

Intercloud Fabric Cloud の作成

Intercloud Fabric Cloud を作成するには、次の手順を実行します。

はじめる前に

- プロバイダー アカウントを作成しておきます。
- クラウド プロバイダーの資格情報を確認します。
- icfTunnelNet という名前のトンネル ネットワークを作成しておきます。
- インフラストラクチャ コンポーネント（PNSC、Intercloud Fabric VSM など）をインストールしておきます。

- Cisco Nexus 1000V、VMware vSwitch、VMware VDS、Microsoft Hyper-V スイッチなど、分散仮想スイッチのポート プロファイルをプライベート クラウドに設定しておきます。
- デバイス プロファイル、MAC プール、トンネル プロファイル、スタティック IP グループなど、Intercloud Fabric インフラストラクチャのポリシーを作成しておきます。
- プライベート クラウドで Cisco Nexus 1000V を使用する場合は、Intercloud Fabric に Cisco Nexus 1000V スイッチを追加しておきます。 ネットワーク要素の追加を参照してください。
- 拡張を要するネットワークに必要な VLAN を Intercloud Fabric Extender トランク ポート プロファイルに設定します。
- サービスを管理するためのサービス バンドルをアップロードしておきます。 [Intercloud] > [Infrastructure] > [Upload Services Bundle] の順に選択し、サービス バンドルをアップロードします。

（注） Intercloud Fabric Router (Integrated)を管理するためのサービス バンドルをアップロードする必要はありません。

手順

ステップ 1 Intercloud Fabricにログインします。

ステップ 2 [Intercloud] > [IcfCloud] の順に選択します。

ステップ 3 [IcfCloud] ウィンドウで、[IcfCloud] タブを選択します。

ステップ 4 [IcfCloud] タブで、[Setup] ボタンをクリックします。
[Cloud Setup] ウィザードが表示されます。

ステップ 5 [Account Credentials] の次のフィールドに値を入力します。

（注） 次の表のフィールドの多くは、新しいプロバイダー アカウントの作成を選択した場合にのみ表示されます。また、表示されるフィールドはプロバイダーに固有のものです。

名前	説明
[Cloud Name] フィールド	Intercloud Fabric Director で作成した仮想アカウントの名前。この名前には、ハイフン、下線、ピリオド、コロンを含めて、1～16 文字の英数字を指定することができます。オブジェクトの作成後は、この名前は変更できません。
[Cloud Type] ドロップダウン リスト	プロバイダー クラウドのタイプを選択します。

名前	説明
[Provider Account] ドロップダウン リスト	既存のプロバイダーを選択するか、新しいプロバイダーアカウントを作成することを選択します。 選択したプロバイダーアカウントに基づいて、該当するフィールドが表示されます。
[Provider Account Name] フィールド	プロバイダー アカウントの名前。
[Access ID] フィールド	アカウントの所有者を識別する英数字のテキスト文字列。
[Access Key] フィールド	アカウントの一意のキー。
[URI] フィールド	アカウントの一意のリソース識別子。
[Username] フィールド	ユーザ名。
[Password] フィールド	パスワード。
[Validate Credentials] ボタン	資格情報を検証する場合にクリックします。残りのフィールドに入力するには、資格情報を検証する必要があります。
[Location] ドロップダウン リスト	プロバイダー クラウドの場所を選択します。
[Provider VPC] ドロップダウン リスト	プロバイダー クラウドのプロバイダー VPC を選択します。
[Provider Private Subnet] ドロップダウン リスト	プロバイダー クラウドのプロバイダー プライベート サブネットを選択します。

ステップ 6 [Next] をクリックします。

ステップ 7 [Configuration Details] の次のフィールドに値を入力します。

名前	説明
Network Configuration	[Advanced] チェックボックスをクリックして新しいポリシーを作成するか、[Next] をクリックしてデフォルト値で続行します。

名前	説明
[MAC Pool] ドロップダウン リスト	デフォルトまたは既存の MAC プールを選択するか、新しい MAC プールを作成することを選択します。 新しいMACプールの作成については、MACアドレス プールの追加 を参照してください。
[Tunnel Profile] ドロップダウン リスト	デフォルトまたは既存のトンネルプロファイルを選択するか、新しいトンネルプロファイルを作成することを選択します。 新しいトンネル プロファイルの作成については、トンネル プロファイルの設定 を参照してください。
[IP Group] ドロップダウン リスト	デフォルトまたは既存の IP グループを選択するか、新しい IP グループを作成することを選択します。 新しいIPグループの作成については、IPグループの追加 を参照してください。
[Private Subnet] ドロップダウン リスト	デフォルトまたは既存のプライベートサブネットを選択するか、プライベートサブネットを作成することを選択します。 新しいプライベートサブネットの作成については、プライベート サブネットの追加 を参照してください。
サービス	
[ICF Firewall (VSG)] チェックボックス	Intercloud Fabric Firewall（VSG）テンプレートを作成するには、[ICF Firewall] チェックボックスをオンにします。 サービスを選択すると、そのサービスのテンプレートをこのクラウドで利用できるようになります。 サービスを設定するには、PNSC を使用します。 Intercloud Fabric ファイアウォールのインストールを参照してください。

名前	説明
[ICF Router (Integrated)] チェックボックス	Azure クラウドでのみサポートされます。 関連する Intercloud Fabric Cloud インスタンスで [ICF Router (Integrated)] インスタンスを作成するには、[ICF Router (Integrated)] チェックボックスをオンにします。 [ICF Router (Integrated)] をインスタンス化した後、それを Prime Network Services Controller で設定できます（Intercloud Fabric Router (Integrated) のインストールと設定に関するワークフローを参照）。
[ICF Router (CSR)] チェックボックス	Intercloud Fabric Router（CSR）テンプレートを作成するには、[ICF Router (CSR)] チェックボックスをオンにします。 サービスを選択すると、そのサービスのテンプレートをこのクラウドで利用できるようになります。 サービスを設定するには、PNSC を使用します。 Intercloud Fabric Router（CSR）のインストールと設定, （1 ページ）を参照してください。
[Cloud Services Router (CSR) Management VLAN] フィールド	Intercloud Fabric Router（CSR）の管理 VLAN ID を入力します。 この VLAN は、Intercloud Fabric Router（CSR）を管理するために使用されます。 このプロパティを選択できるようにするには、[ICF Router (CSR)] チェックボックスをオンにする必要があります。

ステップ 8 [Next] をクリックします。

ステップ 9 [Secure Cloud Extension] の次のフィールドに値を入力します。

名前	説明
[Intercloud Extender Network]	Intercloud Fabric Extender の次のフィールドに値を入力します。
[VM Manager] ドロップダウン リスト	Intercloud Fabric Extender の VM マネージャを選択します。

名前	説明
[Datacenter] ドロップダウン リスト	Intercloud Fabric Extender を展開するデータセンターを選択します。 このフィールドは、Microsoft 環境で Intercloud Fabric Cloud を作成する場合には適用できません。
[Data Trunk Network] ドロップダウン リスト	データ トラフィックの Intercloud Fabric Extender 上のトランク インターフェイスを選択します。 このフィールドは、Microsoft 環境で Intercloud Fabric Cloud を作成する場合には適用できません。
[Management Interface Network] ドロップダウン リスト	データ トラフィックの Intercloud Fabric Extender 上の管理インターフェイスを選択します。 このフィールドは、Microsoft 環境で Intercloud Fabric Cloud を作成する場合には適用できません。
[Management VLAN] フィールド	管理インターフェイスの VLAN を選択します。この VLAN は、管理 IP プール ポリシーで指定された VLAN と一致させる必要があります。
[Management IP Pool Policy] ドロップダウン リスト	管理インターフェイスの IP プール ポリシーを選択するか、新しい IP プール ポリシーを作成します。 新しい IP プール ポリシーの作成については、スタティック IP プール ポリシーの作成 を参照してください。 このフィールドは、Microsoft 環境で Intercloud Fabric Cloud を作成する場合には適用できません。

名前	説明
[Separate Mgmt and Tunnel Interface] チェックボックス	管理インターフェイスとトンネルインターフェイスに対して異なる VLAN を使用する場合は、このチェックボックスをオンにします。 このチェックボックスをオンにしない場合は、デフォルトで、トンネルインターフェイスと管理インターフェイスに同じ VLAN が使用されます。 このプロパティを選択できるようにするには、[Advanced] チェックボックスをオンにする必要があります。 このフィールドは、Microsoft 環境で Intercloud Fabric Cloud を作成する場合には適用できません。
[Tunnel Interface Network] ドロップダウン リスト	データ トラフィックの Intercloud Fabric Extender 上のトンネルインターフェイスを選択します。 このドロップダウン リストは、[Separate Mgmt and Tunnel Interface] チェックボックスを選択した場合にのみ表示されます。 このフィールドは、Microsoft 環境で Intercloud Fabric Cloud を作成する場合には適用できません。
[Tunnel VLAN] フィールド	トンネル インターフェイスの VLAN を選択します。 このフィールドは、[Separate Mgmt and Tunnel Interface] チェックボックスを選択した場合にのみ表示されます。 このフィールドは、Microsoft 環境で Intercloud Fabric Cloud を作成する場合には適用できません。

名前	説明
[Tunnel IP Pool Policy] ドロップダウン リスト	トンネル インターフェイスの IP プール ポリシーを選択するか、新しい IP プール ポリシーを作成します。 新しい IP プール ポリシーの作成については、スタティック IP プール ポリシーの作成 を参照してください。 このドロップダウン リストは、[Separate Mgmt and Tunnel Interface] チェックボックスを選択した場合にのみ表示されます。 このフィールドは、Microsoft 環境で Intercloud Fabric Cloud を作成する場合には適用できません。
[Intercloud Extender Placement / Association]	
[ICX] ドロップダウン リスト	（Microsoft 環境のみ）Intercloud Fabric Extender のホストを選択します。 [Primary Intercloud Extender] と [Secondary Intercloud Extender] のデータストアを指定するには、[Advanced] チェックボックスをオンにして、次に [High Availability] チェックボックスをオンにします。
[Host] ドロップダウン リスト	Intercloud Fabric Extender のホストを選択します。 ハイ アベラビリティ構成の場合は、[Advanced] チェックボックスをオンにしてから、[High-Availability] チェックボックスをオンにして、[Primary Intercloud Extender] と [Secondary Intercloud Extender] のホストを指定します。 このフィールドは、Microsoft 環境で Intercloud Fabric Cloud を作成する場合には適用できません。

名前	説明
[Datastore] ドロップダウン リスト	Intercloud Fabric Extender のデータストアを選択します。 ハイ アベラビリティ構成の場合は、[Advanced] チェックボックスをオンにしてから、[High-Availability] チェックボックスをオンにして、[Primary Intercloud Extender] と [Secondary Intercloud Extender] のデータストアを指定します。 このプロパティを選択できるようにするには、[Advanced] チェックボックスをオンにする必要があります。 このフィールドは、Microsoft 環境で Intercloud Fabric Cloud を作成する場合には適用できません。
[Intercloud Switch Network]	クラウドの Intercloud Fabric スイッチに対して次のフィールドに値を入力します。 このプロパティを選択できるようにするには、[Advanced] チェックボックスをオンにする必要があります。
[Management VLAN] フィールド	管理インターフェイスの VLAN を選択します。
[Management IP Pool Policy] ドロップダウン リスト	管理インターフェイスの IP ポリシーを選択するか、新しい IP プール ポリシーを作成します。 新しい IP プール ポリシーの作成については、スタティック IP プール ポリシーの作成 を参照してください。
[VSG Service Interface]	このプロパティを選択できるようにするには、[ICF Firewall (VSG)] チェックボックスをオンにする必要があります。 このサービス インターフェイスは Intercloud Fabric Switch で作成され、Intercloud Fabric Firewall のデータ インターフェイスとの通信に使用されます。

名前	説明
[VLAN] フィールド	サービス インターフェイスの VLAN を選択します。 この VLAN は Intercloud Fabric Switch と Intercloud Fabric Firewall 間の通信に使用され、他の VLAN から完全に隔離されたプライベート VLAN の場合もあります。
[IP Pool Policy] ドロップダウン リスト	サービス インターフェイスの IP ポリシーを選択するか、新しい IP プール ポリシーを作成します。
[VSG Management]	このプロパティを選択できるようにするには、[ICF Firewall (VSG)] チェックボックスをオンにする必要があります。
[VSG Management VLAN] フィールド	管理インターフェイスの VLAN を選択します。この VLAN は Intercloud Fabric Firewall を管理するために使用されます。

ステップ 10 [Next] をクリックします。
[Summary] ウィンドウに Intercloud Fabric Cloud のサマリーが一覧表示されます。

ステップ 11 [Submit] をクリックして、Intercloud Fabric Cloud を作成します。

ステップ 12 タスクの状態を表示するには、[IcfCloud] タブで、タスクのサービス リクエスト番号を検索します。

ステップ 13 [Organizations] > [Service Requests] の順に選択します。

ステップ 14 [Service Request] タブを選択します。 サービス リクエスト番号を検索するか、検索フィールドにサービス リクエスト番号を入力します。

ステップ 15 [View] をクリックして、ワークフロー ステータス、ログ、入力情報など、サービス リクエストの詳細情報を表示します。

サービスの管理

Intercloud Fabric Cloud の作成後にサービスを管理するには、次の手順を実行します。

はじめる前に

- Intercloud Fabric Cloud を作成しておきます。

- サービスを管理するためのサービス バンドルをアップロードしておきます。 [Intercloud] > [Infrastructure] > [Upload Services Bundle] の順に選択し、サービス バンドルをアップロードします。

（注） Intercloud Fabric Router (Integrated)を管理するためのサービス バンドルをアップロードする必要はありません。

手順

ステップ 1 Intercloud Fabricにログインします。

ステップ 2 [Intercloud] > [IcfCloud] の順に選択します。

ステップ 3 [IcfCloud] ウィンドウで、[IcfCloud] タブを選択します。

ステップ 4 IcfCloud を選択し、[Manage Services] をクリックします。
[Manage Services] ウィンドウが表示されます。

ステップ 5 [Manage Services] の次のフィールドに値を入力します。

名前	説明
[ICF Firewall] チェックボックス	Intercloud Fabric Firewall（VSG）テンプレートを作成するには、[ICF Firewall] チェックボックスをオンにします。
[Service Interface VLAN] フィールド	このサービス インターフェイスは Intercloud Fabric Switch で作成され、Intercloud Fabric Firewall のデータ インターフェイスとの通信に使用されます。 サービス インターフェイスの VLAN。 この VLAN は Intercloud Fabric Switch と Intercloud Fabric Firewall 間の通信に使用され、他の VLAN から完全に隔離されたプライベート VLAN の場合もあります。 このフィールドは、[ICF Firewall] チェックボックスを選択した場合にのみ表示されます。

名前	説明
[Service Interface IP Pool Policy] ドロップダウンリスト	サービス インターフェイスの IP ポリシーを選択するか、新しい IP プール ポリシーを作成します。 新しい IP プール ポリシーの作成については、スタティック IP プール ポリシーの作成 を参照してください。 このフィールドは、[ICF Firewall] チェックボックスを選択した場合にのみ表示されます。
[VSG Management VLAN] フィールド	管理インターフェイスの VLAN。 この VLAN は Intercloud Fabric Firewall を管理するために使用されます。 このフィールドは、[ICF Firewall] チェックボックスを選択した場合にのみ表示されます。 （注） ファイアウォール管理ポートプロファイルは、Intercloud Fabric Cloud の作成時に Intercloud Fabric Firewall サービスを選択すると自動的に作成されます。Intercloud Fabric Cloud の名前は、プレフィックスとしてポート プロファイルの名前に追加され、VLAN ID はサフィックスとしてポート プロファイルの名前に追加されます。例：icf-amz1_VSG_Management_72
[ICF Router (CSR)] チェックボックス	Intercloud Fabric Router（CSR）のテンプレートを作成するには、[ICF Router (CSR)] チェックボックスをオンにします。
[CSR Management VLAN]	Intercloud Fabric Router（CSR）の管理 VLAN ID を入力します。 このフィールドは、[ICF Router (CSR)] チェックボックスを選択した場合にのみ表示されます。
[ICF Router (Integrated)] チェックボックス	ICF ルータ（統合型）を作成するには、[ICF Router (Integrated)] チェックボックスをオンにします。

ステップ 6 [Submit] をクリックします。

Intercloud Fabric Router（CSR）のインスタンス化

[Add Edge Router] ウィザードを使用して Intercloud Fabric Router（CSR）をインスタンス化するには、次の手順を実行します。 このウィザードを使用すると、管理インターフェイスに加えてクラウド インターフェイスを作成できます。

（注） 1 つの管理インターフェイスと、少なくとも 2 つのクラウド インターフェイスを設定する必要があります。 デバイス間には 1 つのトランクしかないため、複数の VLAN 用のクラウド インターフェイスが必要です。

はじめる前に

- インフラストラクチャ コンポーネントをインストールしておきます。
- Intercloud Fabric Cloud を作成しておきます。
- CSR クラウド インターフェイス用の VLAN を含む VDC を作成しておきます。

手順

ステップ 1 Intercloud Fabric にログインします。

ステップ 2 [Intercloud] > [Infrastructure] の順に選択します。

ステップ 3 [Infrastructure] タブで、[Launch PNSC] ボタンをクリックします。
PNSC GUI が表示されます。

ステップ 4 PNSC GUI で、[Tenant Management] > [Root] > [Create tenant] の順に選択して、テナントを作成します。

ステップ 5 PNSC GUI で。[Resource Management] > [Managed Resources] > [tenant] の順に選択します。

ステップ 6 [Network Services Actions] ドロップダウン リストから [Add Edge Router] を選択します。
[Add Edge Router] ウィザードが表示されます。

ステップ 7 [Properties] の次のフィールドに値を入力します。

名前	説明
[Name] フィールド	エッジ ルータの名前。
[Description] フィールド	エッジ ルータの説明。
[Device Profile] ボタン	エッジ ルータ用の既存のデバイス プロファイルまたはデフォルトのデバイスプロファイルを選択します。

名前	説明
[Device Service Profile] ボタン	エッジ ルータ用の既存のデバイス サービス プロファイルまたはデフォルトのデバイス サービス プロファイルを選択します。
[Host Name] フィールド	ホスト名。
[VM Access]	
[User Name] フィールド	ユーザ名を入力します。
[Password] フィールド	パスワードを入力します。
[Confirm Password] フィールド	パスワードを確認します。

ステップ 8 [Next] をクリックします。

ステップ 9 [Service Device] の次のフィールドに値を入力します。

名前	説明
[Instantiate in Cloud] オプション ボタン	クラウド エッジ ルータをインスタンス化する場合に選択します。
[Select] オプション ボタン	クラウド エッジ ルータのインスタンス化に使用するクラウド イメージを選択します。
コンピューティング	
CPU コア	各インターフェイスに 4 つの CPU コアが割り当てられます。
メモリ	各インターフェイスに 4000 MB のメモリが割り当てられます。

ステップ 10 [Next] をクリックします。

ステップ 11 Intercloud Fabric Cloud を選択します。

ステップ 12 [Next] をクリックします。

ステップ 13 [Add Interfaces] をクリックして、管理インターフェイスを作成します。

ステップ 14 [Add Interfaces] の次のフィールドに値を入力します。

名前	説明
[Name] フィールド	管理インターフェイスの名前。

名前	説明
[Description] フィールド	管理インターフェイスの説明。
[Type] オプション ボタン	[Management] を選択します。
[Mode] オプション ボタン	モードを選択します。
[Port Profile] ドロップダウン リスト	*icf-link-name** 形式の名前が付いているポート プロファイルを選択します（ICS_Trunk_Tunnel など）。
[Category] オプション ボタン	[Tagged Interface] を選択します。
[VLAN] ドロップダウン リスト	インターフェイスの VLAN を選択します。VLAN ID は、前のステップで選択したポート プロファイルに含める必要があります。
[Sub Management Information]	
[Sub Management IP] フィールド	PNSC と Intercloud Fabric Router（CSR）間の通信に使用する IP アドレス。
[Port] フィールド	インターフェイスのサブ管理ポート。
[IP Address] フィールド	インターフェイスの IP アドレス。
[IP Subnet Mask] フィールド	IP アドレスのサブネット マスク。
[Gateway] フィールド	ゲートウェイ IP アドレス。

ステップ 15 [Next] をクリックします。

ステップ 16 [Add Interfaces] をクリックして、クラウド インターフェイスを作成します。 少なくとも 2 つのクラウド インターフェイスを作成します。

ステップ 17 [Add Interfaces] の次のフィールドに値を入力します。

名前	説明
[Name] フィールド	クラウド インターフェイスの名前。
[Description] フィールド	クラウド インターフェイスの説明。
[Type] オプション ボタン	[Ethernet] を選択します。

名前	説明
[Admin State] オプション ボタン	サブインターフェイスの管理状態を選択します。
[Interface Service Profile] ボタン	[Select] をクリックしてインターフェイス サービスプロファイルを選択するか、デフォルトのインターフェイス サービス プロファイルを追加します。
[Mode] オプション ボタン	デフォルトでは、[Trunk] が選択されます。
[Port Profile] ドロップダウン リスト	インターフェイスが属するトランク ポート プロファイルを選択します。
[Category] オプション ボタン	[Tagged Interface] を選択します。
[VLAN] ドロップダウン リスト	インターフェイスの VLAN を入力します。VLAN ID は、前のステップで選択したポートプロファイルに含める必要があります。
[Use As Default Gateway] チェックボックス	Extend Default Gateway（別名：アドレス解決プロトコル（ARP）フィルタリング）を設定するには、[Use As Default Gateway] チェックボックスをオンにします。
[DHCP] チェックボックス	アドレス解決プロトコル（ARP）フィルタリングを設定しない場合は、[Enable] チェックボックスをオンにします。 [Default Gateway] チェックボックスがオフの場合にのみ使用できます。
[IP Address] フィールド	HA が有効な場合は、プライマリ IP アドレス、および任意でセカンダリ IP アドレス。
[Subnet Mask] フィールド	IP アドレスのサブネット マスク。
[Extend Default Gateway] チェックボックス	アドレス解決プロトコル（ARP）フィルタリングを設定するには、このチェックボックスをオンします。
[Enterprise Gateway] フィールド	エンタープライズ ゲートウェイの IP アドレス。

ステップ 18 [Next] をクリックしてサマリーを確認し、[Finish] をクリックします。

ネットワーク アドレス変換ポリシーおよびポート アドレス変換ポリシーについて

Cisco Prime Network Services Controller は、展開されたネットワークでのアドレス変換を制御するために、ネットワーク アドレス変換（NAT）ポリシーおよびポート アドレス変換（PAT）ポリシーをサポートしています。 これらのポリシーは、IP アドレスおよびポートのスタティックおよびダイナミック両方の変換を行います。

Cisco Prime Network Services Controller では、次のポリシー項目を設定できます。

- NAT ポリシー：一致するものが見つかるまで順番に評価される、複数の規則を入れることができます。
- NAT ポリシー セット：エッジ セキュリティ プロファイルに関連付けることができる NAT ポリシーのグループ。 プロファイルが適用されると、NAT ポリシーは入力トラフィックにのみ適用されます。
- PAT ポリシー：エッジ ファイアウォールで、ソース ダイナミック インターフェイス PAT および宛先スタティック インターフェイス PAT をサポートします。

クラウド プロバイダーに対して NAT および PAT のポリシーを設定する際は、次のガイドラインが適用されます。

（注） クラウドプロバイダーに対してNATとPATのポリシーを正しく設定しないと、着信トラフィックがそのプロバイダーに到達しません。

- Amazon クラウドで動作させる場合は、AWS コンソールを使用して次のタスクを実行します。
  - Intercloud Fabric Router（CSR）にセカンダリ AWS のプライベート IP アドレスを設定します。
  - Elastic IP アドレスを借用して Intercloud Fabric Router（CSR）のセカンダリ IP アドレスにバインドします。
- ダイナミック NAT を設定してルールを追加する場合：
  - プレフィックス送信元条件を使用します。
  - クラウドのプライベート IP アドレスを含む送信元 IP アドレス プールを選択します。送信元 IP アドレス プールには、着信トラフィックが到達できるクラウド VM の IP アドレスが含まれている必要があります。

- Cisco Intercloud Services – V と連携している場合にダイナミック NAT を設定すると、リターン ネットワーク トラフィックが Intercloud Fabric Router（CSR）クラウド VM に到達できなくます。

- ダイナミック PAT を設定してルールを追加する場合：
  - プレフィックス送信元条件を使用します。
  - クラウド プロバイダーのアクセス可能なポートを含む送信元 IP PAT プールを選択します。

ネットワーク アドレス変換およびポート アドレス変換のポリシーの設定

NAT/PAT ポリシーを設定するには、次の手順を実行します。

手順

ステップ 1 Intercloud Fabricにログインします。

ステップ 2 [Intercloud] > [Infrastructure] の順に選択します。

ステップ 3 [Infrastructure] タブで、[Launch PNSC] ボタンをクリックします。
PNSC GUI が表示されます。

ステップ 4 PNSC GUI で、[Policy Management] > [Service Policies] > [root] > [Policies] > [NAT] > [NAT Policies] の順に選択します。

ステップ 5 [General] タブで、[Add NAT Policy] をクリックします。

ステップ 6 [Add NAT Policy] の次のフィールドに値を入力します。

名前	説明
[Name] フィールド	ポリシーの名前。
[Description] フィールド	エッジ ルータ ポリシーの説明。
[Admin State] オプション ボタン	ポリシーの管理状態。
[Add Rule] アイコン	ポリシーにルールを追加するには、[Add Rule] をクリックします。

ステップ 7 [Add NAT Policy Rule] の次のフィールドに値を入力します。

フィールド	説明
Name	ルールの名前。
Description	ルールの説明。
Original Packet Match Conditions	
Source Match Conditions	現在のポリシーを適用するために一致する必要がある送信元属性。 新しい条件を追加するには、[Add Rule Condition] をクリックします。 使用可能な送信元属性は、IP アドレスとネットワーク ポートです。
Destination Match Conditions	現在のポリシーを適用するために一致する必要がある宛先属性。 新しい条件を追加するには、[Add Rule Condition] をクリックします。 使用可能な宛先属性は、IP アドレスとネットワーク ポートです。
Protocol	ルールが適用されるプロトコルを指定します。 • ルールをすべてのプロトコルに適用するには、[Any] チェックボックスをオンにします。 • ルールを特定のプロトコルに適用するには、次の手順を実行します。 1 [Any] チェックボックスをオフにします。 2 [Operator] ドロップダウン リストから、修飾子 [Equal]、[Not equal]、[Member]、[Not Member]、[In range]、または [Not in range] を選択します。 3 [Value] フィールドで、プロトコル、オブジェクト グループ、または範囲を指定します。
[NAT Action] テーブル	

フィールド	説明
NAT Action	このドロップダウン リストから、[Static] または [Dynamic] のうち、必要な方のトランスレーション オプションを選択します。
Translated Address	元のパケットの一致条件ごとに、変換されたアドレスのプールを次のオプションの中から選択します。 • Resolved Source IP Pool • Resolved Source Port Pool • Resolved Source IP PAT Pool • Resolved Destination IP Pool • Resolved Destination Port Pool たとえば、送信元 IP アドレスの一致条件を指定する場合は、[Source IP Pool] オブジェクト グループを選択する必要があります。 同様に、宛先ネットワーク ポートの場合は、[Destination Port Pool] オブジェクト グループを選択する必要があります。 [Source IP PAT Pool] オプションは、ダイナミック変換を選択した場合にのみ使用可能です。 変換アクション用のオブジェクト グループを追加するには、[Add Object Group] をクリックします。 ステップ 8 を参照してください。

フィールド	説明
NAT Options	必要に応じて、次のチェックボックスをオン/オフします。 • [Enable Bidirectional]：双方向接続（ホストからの接続とホストへの接続）を開始するには、このチェックボックスをオンにします。 スタティック アドレス変換の場合のみ使用可能です。 • [Enable DNS]：NAT に対して DNS を有効にするには、このチェックボックスをオンにします。 • [Enable Round Robin IP]：ラウンド ロビン方式で IP アドレスを割り当てるには、このチェックボックスをオンにします。 ダイナミック アドレス変換の場合のみ使用可能です。 • [Disable Proxy ARP]：プロキシ ARP を無効にするには、このチェックボックスをオンにします。 スタティック アドレス変換の場合のみ使用可能です。

ステップ 8 （任意） [Add Object Group] の次のフィールドに値を入力します。

フィールド	説明
Name	オブジェクト グループ名。 この名前には、識別子として 2 ～ 32 文字を使用できます。ハイフン、下線、ピリオド、コロンを含む英数字を使用できます。保存後は、この名前を変更できません。
Description	オブジェクト グループの簡単な説明。 この説明には、ID となる 1 ～ 256 文字を使用できます。ハイフン、下線、ピリオド、コロンを含む英数字を使用できます。
Attribute Type	使用可能な属性タイプ：Network、VM、User Defined、vZone、Time Range オブジェクト グループ式を追加するには、属性タイプと属性名を設定する必要があります。

フィールド	説明
Attribute Name	選択した属性タイプに対して使用できる属性名。
[Expression] テーブル	
Add Object Group Expression	クリックすると、オブジェクトグループ式が追加されます。
Operator	選択した式に使用する演算子。
Value	選択した式に使用する値。

ステップ 9 [OK] をクリックします。

Intercloud Fabric Router のインストールの確認

Intercloud Fabric Router のインストールを確認するには、次の手順を実行します。

手順

ステップ 1 Intercloud Fabric Router の CLI にログインします。

ステップ 2 **show running configuration** コマンドを入力して、インストールを確認します。

例：

```
# show running configuration
Building configuration...

Current configuration : 5052 bytes
!
! Last configuration change at 19:01:11 UTC Tue Mar 10 2015
!
version 15.5
service timestamps debug datetime msec
no service timestamps log uptime
no platform punt-keepalive disable-kernel-core
platform console auto
!
hostname CSR11
!
boot-start-marker
boot-end-marker
!
!
no logging buffered
no logging console
no logging monitor
!
```

```
no aaa new-model
!
ip domain name opsourcecloud.net
!
!
subscriber templating
!
multilink bundle-name authenticated
!
crypto pki trustpoint TP-self-signed-1700464965
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1700464965
 revocation-check none
 rsakeypair TP-self-signed-1700464965
!
!
license udi pid CSR1000V sn 916Z0U0VCZ5
license boot level lite
remote-management
  pnsc host 10.3.1.99 local-port 58443 shared-secret AL]\cFcCRZIiYZUaiRcRgbIfOEE\eWAAB
!
username admin privilege 15 secret 5 $1$CX8v$0Io63wbgoLfsjpVQJ7ltn.
!
redundancy
!
!
ip ssh rsa keypair-name ssh-key
ip ssh version 2
!

interface VirtualPortGroup0
 ip unnumbered GigabitEthernet1.301
 ip mtu 1352
!
interface GigabitEthernet1
 description configured by PolicyAgent
 no ip address
 negotiation auto
!
interface GigabitEthernet1.301
 encapsulation dot1Q 301
 ip address 10.3.1.39 255.255.0.0
 ip mtu 1352
!
interface GigabitEthernet1.311
 description configured by PolicyAgent
 encapsulation dot1Q 311
 ip address 192.168.11.39 255.255.255.0
 ip mtu 1352
 ip access-group default-ingress in
 ip access-group default-egress out
!
interface GigabitEthernet1.312
 description configured by PolicyAgent
 encapsulation dot1Q 312
 ip address 192.168.12.39 255.255.255.0
 ip mtu 1352
 ip access-group default-ingress in
 ip access-group default-egress out
!
!
interface GigabitEthernet8
 description configured by PolicyAgent
 ip address 10.229.179.12 255.255.255.0
 ip mtu 1352
 ip access-group default-ingress in
 ip access-group default-egress out
 negotiation auto
!
!
virtual-service csr_mgmt
 vnic gateway VirtualPortGroup0
```

```
  guest ip address 10.3.1.49
 activate
!
ip forward-protocol nd
!
no ip http server
ip http secure-server
ip route 10.3.1.49 255.255.255.255 VirtualPortGroup0
ip route 173.36.216.0 255.255.255.0 10.3.1.1
!
ip access-list extended default-egress
ip access-list extended default-ingress

no logging trap
!
!
!
control-plane
!
banner exec ^CWARNING: This device is managed by Prime Network Services Controller.
RESTful API is read only. Changing configuration using CLI is not recommended.^C
banner login ^CWARNING: This device is managed by Prime Network Services Controller.
RESTful API is read only. Changing configuration using CLI is not recommended.^C
!
line con 0
 stopbits 1
line vty 0 4
 login local
 transport input ssh
!
!
end
```