Intercloud Fabric Cloud の作成

This chapter contains the following sections:

- Intercloud Fabric Cloud の詳細，1 ページ
- 注意事項と制約事項，2 ページ
- 前提条件，2 ページ
- Intercloud Fabric Cloud 作成のワークフロー，3 ページ
- Intercloud Fabric のインフラストラクチャ ポリシーとプールの作成，4 ページ
- ポート プロファイルおよびポート グループの設定，11 ページ
- ネットワーク要素の追加，13 ページ
- Microsoft Azure における Intercloud Fabric のセキュリティ クレデンシャルへのアクセス，15 ページ
- Intercloud Fabric Cloud の作成，15 ページ
- サービスの管理，24 ページ
- Intercloud Fabric Cloud の複製，27 ページ

Intercloud Fabric Cloud の詳細

Intercloud Fabric Cloud は、プライベート クラウドとプロバイダー クラウド間のセキュアな接続です。 Intercloud Fabric Cloud には 2 つの仮想ゲートウェイがあります（プライベート クラウドに 1 つ、プロバイダー クラウドに 1 つ）。プライベート クラウド上のゲートウェイは Intercloud Fabric Extender と呼ばれ、プロバイダー クラウド上のゲートウェイは Intercloud Fabric Switch と呼ばれます。 安全なレイヤ 4 トンネルによってゲートウェイを接続して、レイヤ 2 プライベート クラウド ネットワークをプロバイダー クラウドに拡張します。

注意事項と制約事項

- クラウド プロバイダーが Microsoft Azure の場合は、Azure ポータルに資格情報を登録する必要があります。
- クラウド プロバイダーが Microsoft Azure の場合は、Intercloud Fabric Cloud の展開を計画しているリージョンの Azure ポータルを使用して、手動でストレージ アカウントを作成する必要があります。 ストレージ アカウント名は、「pnsc」から始めて、3 ～ 24 の小文字の英数字（a ～ z、0 ～ 9）を含める必要があります。 ストレージ アカウントは、Microsoft Azure クラウド プロバイダー用の Intercloud Fabric Cloud を作成するために必要です。
- 仮想マシンの展開に必要なすべてのポート プロファイルを、Intercloud Fabric を使用して作成する必要があります。
- Intercloud Fabric Cloud の作成に必要なすべてのポート プロファイルを、Intercloud Fabric を使用して作成する必要があります。
- Intercloud ネットワーク ポリシーの作成に必要なすべてのポート プロファイルを、Intercloud Fabric を使用して作成する必要があります。
- Intercloud Fabric Firewall データ インターフェイスと管理インターフェイスに必要なすべてのポート プロファイルを、Intercloud Fabric を使用して作成する必要があります。
- Intercloud Fabric 内のファイアウォール保護を必要とする仮想マシンに必要なすべてのポート プロファイルを PNSC により更新し、vPath 構成に追加する必要があります。
- Intercloud Fabric Cloud の複製時は、送信元仮想マシンおよび宛先仮想マシンを移行しないでください。そのような移行は複製処理に影響を及ぼし、移行後に宛先仮想マシンで実行される処理にも影響します。

前提条件

- プロバイダー クラウドのアカウントを作成しておきます。
- Amazon AWS のアクセスキーやアクセス ID、シスコ クラウド サービス プロバイダーの URI など、クラウド プロバイダーの資格情報を取得しておく必要があります。
  - Amazon Web Services GUI で、[Sign IN] > [Security Credentials] > [Access Keys (Access Key ID and Secret Access Key)] の順に移動すると、Intercloud Fabric のセキュリティ クレデンシャルにアクセスできます。 [Access Keys (Access Key ID and Secret Access Key)]（+）アイコンをクリックして、AWS アクセス キー ID を取得します。 新しいアクセス キーを作成するには、[Create New Access Key] をクリックします。 キー ファイルをダウンロードして、アクセス キー ID とシークレット アクセス キーを入手します。 必要に応じて、[Show Access Key] リンクをクリックすると、アクセス キー ID とシークレット アクセス キーを表示できます。

- Microsoft Azure については、Microsoft Azure における Intercloud Fabric のセキュリティ クレデンシャルへのアクセス，（15 ページ） を参照してください。
- シスコ クラウド サービス プロバイダーの場合は、セキュリティ クレデンシャルの情報を含むウェルカム電子メールがシスコから送られます。

- Intercloud Fabric 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。 Intercloud Fabric のインフラストラクチャ コンポーネントのインストールを参照してください。
- 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,（13 ページ）を参照してください。
- Smart License ポータルから Intercloud Fabric Router（CSR 1000V）のライセンス トークンを生成しておきます。

Intercloud Fabric Cloud 作成のワークフロー

Intercloud Fabric Cloud のインストールは、以下の手順で行います。

手順

ステップ 1 Intercloud Fabric のインフラストラクチャ ポリシー、プロファイル、プール（Intercloud Fabric Extender の管理 IP プール、Intercloud Fabric Extender のトンネル IP プール、Intercloud Fabric スイッチの管理 IP プール、サービスのインターフェイス IP プール、クラウド内の VM の IP プールなど）を作成する。
Intercloud Fabric インフラストラクチャ ポリシーの作成を参照してください。

（注） ウィザードを使用して Intercloud Fabric Cloud を作成するときに、Intercloud Fabric のインフラストラクチャ ポリシーも作成できます。

ステップ 2 プライベート クラウドの分散仮想スイッチ（DVS）のポート プロファイルを作成する。
ポート プロファイルおよびポート グループの設定,（11 ページ） を参照してください。

ステップ 3 Intercloud Fabric Virtual Security Gateway の管理プロファイルとデータ ポート プロファイルを作成する。
Intercloud Fabric Firewall 用のポート プロファイルの作成を参照してください。

ステップ 4 ウィザードを使用して Intercloud Fabric Cloud を作成する。
Intercloud Fabric Cloud の作成,（15 ページ） を参照してください。

Intercloud Fabric のインフラストラクチャ ポリシーとプールの作成

Intercloud Fabric Cloud の 実装が成功するかどうかは、次の項目を適切に設定することによって決まります。

手順

ステップ 1 MAC アドレス プール。
MAC アドレス プールの追加, （4 ページ）を参照してください。

ステップ 2 プライベート サブネット。
プライベート サブネットの追加, （5 ページ）を参照してください。

ステップ 3 IP グループ。
IP グループの追加, （6 ページ）を参照してください。

ステップ 4 トンネル プロファイル。
トンネル プロファイルの設定, （7 ページ）を参照してください。

ステップ 5 ポート プロファイル。
ポート プロファイルの作成 , （10 ページ）を参照してください。

MAC アドレス プールの追加

MAC アドレス プールを追加し、仮想プライベート クラウドに MAC アドレスのグループを割り当てます。

手順

ステップ 1 Intercloud Fabricにログインします。

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

ステップ 3 [Intercloud Fabric Infrastructure Policies] ウインドウで、[MAC Pool] タブを選択します。

ステップ 4 [Add] をクリックして、MAC プールを作成します。
[Add MAC Pool] ウィンドウが表示されます。

ステップ 5 次の詳細を入力します。

名前	説明
[MAC Pool Name] フィールド	MAC プールの名前。

名前	説明
[Start MAC Address] フィールド	プールの開始 MAC アドレス（12 桁の 16 進数形式）。
[Count] フィールド	プール内のアドレスの数。 最小値は 1000 個の MAC アドレス、デフォルト値は 10000 個の MAC アドレスです。

ステップ 6 [Submit] をクリックして、MAC アドレス プールを作成します。

プライベート サブネットの追加

クラウド内の仮想マシンのプライベートサブネットを定義します。プライベートサブネットは、プロバイダー環境内のプライベート IP スペースを定義するために使用されます。

（注） プライベート サブネットは Microsoft Azure にのみ適用されます。

手順

ステップ 1 Intercloud Fabricにログインします。

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

ステップ 3 [Intercloud Fabric Infrastructure Policies] ウインドウで、[Private Subnet] タブを選択します。

ステップ 4 [Add] をクリックして、プライベート サブネットを作成します。
[Add Subnet] ウィンドウが表示されます。

ステップ 5 次の詳細を入力します。

名前	説明
[Subnet Name] フィールド	プライベート サブネットの名前。
[Subnet Address] フィールド	サブネットの IP アドレス。

ステップ 6 [Submit] をクリックして、プライベート サブネットを作成します。

IP グループの追加

IP グループは、Intercloud Fabric に必要なポートだけを Intercloud Fabric Cloud のクラウド VM のパブリック インターフェイスに対して開き、IP グループ内の IP アドレスからのアクセスのみを許可することによって、クラウド リソースを保護します。 許可される IP アドレスは、通常、エンタープライズ パブリック IP スペースです。

Intercloud Fabric には次のポートが必要です。

- SSH ポート：TCP 22
- HTTPS ポート：TCP 443
- RDP ポート：TCP 3389
- Intercloud Fabric トンネル ポート：TCP 6644 および 6646
- Intercloud Fabric トンネル ポート：UDP 6644 および 6646

（注） IP グループの設定に失敗すると、クラウド VM、Intercloud Fabric スイッチ、エンタープライズ データセンターへの不正アクセスを許可してしまう可能性があります。

手順

ステップ 1 Intercloud Fabricにログインします。

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

ステップ 3 [Intercloud Fabric Infrastructure Policies] ウインドウで、[IP Group] タブを選択します。

ステップ 4 [Add] をクリックして、IP グループを作成します。
[Add IP Group] ウィンドウが表示されます。

ステップ 5 次の詳細を入力します。

名前	説明
[IP Group Name] フィールド	IP グループの名前。
[IPv4 Range] フィールド	IP グループに追加する IP アドレス範囲の IP アドレスとプレフィックス。

ステップ 6 [Submit] をクリックして、IP グループを作成します。

トンネル プロファイルの設定

トンネル プロファイルは接続パラメータ ポリシーをキー ポリシーと組み合わせ、特定のトンネル ポートのセキュアな通信を確実にします。 トンネル プロファイルを設定したら、次の要素間のトンネルに適用できます。

- Intercloud Fabric Extender と Intercloud Fabric Switch
- Intercloud Fabric Switch とクラウド VM

サイト間トンネル プロファイルは、Intercloud Fabric Extender と Intercloud Fabric Switch 間のトンネルで使用されます。 アクセス トンネル プロファイルは、Intercloud Fabric Switch とクラウド VM 間のトンネルで使用されます。

手順

ステップ 1 Intercloud Fabricにログインします。

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

ステップ 3 [Intercloud Fabric Infrastructure Policies] ウインドウで、[Tunnel Profile] タブを選択します。

ステップ 4 [Add] をクリックして、トンネル プロファイルを作成します。
[Add Tunnel Profile] ウィンドウが表示されます。

ステップ 5 次の詳細を入力します。

名前	説明
[Tunnel Profile Name] フィールド	トンネル プロファイルの名前。
[Site to Site Tunnel Profile]	サイト間トンネルのプロファイルを作成するには、次の詳細を入力します。
[Protocol] ドロップダウン リスト	トランク ポート プロファイルに使用するプロトコルを選択します（TCP または UDP）。 デフォルト プロトコルは UDP です。
[Use HTTPS] チェックボックス	TCP トンネルでポート 443 の使用を許可するには、このチェックボックスをオンにします。 このオプションは、[Protocol] ドロップダウン リストから TCP プロトコルを選択する場合にのみ使用できます。

名前	説明
[Rekey Period] フィールド	トランク ポート プロファイルのキー再生成間隔。これは、新しいキーを生成するまでの経過時間です（日、時間、分、秒）。最小値は5分です。 デフォルト値の 00:00:00:00 は再調整が発生しないことを示します。 [Protocol] ドロップダウン リストから TCP プロトコルを選択し、[Use HTTPS] チェックボックスをオンにした場合、このオプションは使用できません。
[Encryption Algorithm] ドロップダウン リスト	トランク ポート プロファイルの暗号化方式を選択します。 • AES-128-CBC（デフォルト） • AES-128-GCM（TCP プロトコルを使用する場合は使用不可） • AES-256-CBC • AES-256-GCM（TCP プロトコルを使用する場合は使用不可） • None（TCP プロトコルを使用する場合は使用不可） [Protocol] ドロップダウン リストから TCP プロトコルを選択し、[Use HTTPS] チェックボックスをオンにした場合、このオプションは使用できません。
[Hash Algorithm] ドロップダウン リスト	トランク ポート プロファイルのハッシュ アルゴリズムを選択します。 • SHA-1（デフォルト） • SHA-256 • SHA-384 このオプションは、[Encrypt Algorithm] フィールドで、[AES-128-CBC]、[AES-256-CBC]、または [None] を選択した場合に使用できます。 [Protocol] ドロップダウン リストから TCP プロトコルを選択し、[Use HTTPS] チェックボックスをオンにした場合、このオプションは使用できません。

名前	説明
[Access Tunnel Profile]	アクセス トンネル プロファイルを作成するには、次の詳細を入力します。
[Use Same as the Site to Site Tunnel Profile] チェックボックス	サイト間トンネルプロファイルと同じ設定を使用するには、このチェックボックスをオンにします。
[Protocol] ドロップダウン リスト	アクセス トランク ポート プロファイルに使用するプロトコルを選択します（TCP または UDP）。 デフォルト プロトコルは UDP です。
[Rekey Period] フィールド	アクセス トランク ポート プロファイルのキー再生成間隔。これは、新しいキーを生成するまでの経過時間です（日、時間、分、秒）。最小値は 5 分です。 デフォルト値の 00:00:00:00 は再調整が発生しないことを示します。
[Encryption Algorithm] ドロップダウン リスト	アクセス トランク ポート プロファイルの暗号化方式を選択します。 • AES-128-CBC（デフォルト） • AES-128-GCM • AES-256-CBC • AES-256-GCM • なし
[Hash Algorithm] ドロップダウン リスト	アクセス トランク ポート プロファイルのハッシュ アルゴリズムを選択します。 • SHA-1（デフォルト） • SHA-256 • SHA-384 このオプションは、[Encrypt Algorithm] フィールドで、[AES-128-CBC]、[AES-256-CBC]、または [None] を選択した場合に使用できます。
[Keep Alive Duration] フィールド	キープアライブ メッセージが送信される前に、アクティビティなしで接続を維持できる時間の長さ（分と秒単位）。 デフォルト値は 1 秒です。

名前	説明
[Timeout] フィールド	接続を閉じる前に、アイドル状態を維持できる時間の長さ（分と秒単位）。デフォルト値は 5 分です。

ステップ 6 [Submit] をクリックして、トンネル プロファイルを作成します。

ポート プロファイルの作成

Intercloud Fabric でポート プロファイルを作成するには、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] > [Network] の順に選択します。

ステップ 3 [All Clouds] ドロップダウン リストからクラウドを選択します。

ステップ 4 [IcfVSM] タブで、VSM を選択します。

ステップ 5 [Add Port Profile] ボタンをクリックします。
[Add Port Profile] が表示されます。

ステップ 6 ポート プロファイルの次のフィールドに値を入力します。

名前	説明
[Port Profile Name] フィールド	ポート プロファイルの名前。
[VLAN ID] フィールド	ポート プロファイルの VLAN ID。
[Enable for Services] チェックボックス	サービスに対してポート プロファイルを有効にします。 （注） 管理ポート プロファイルやデータ ポート プロファイルを作成する場合は、このオプションを選択しないでください。このオプションは、クラウド VM でファイアウォール サービスを有効にする場合にのみ適用できます。

名前	説明
（オプション）[Org] ドロップダウン リスト	既存の組織を選択するか、新しい組織を作成します。 組織とは、IP バインディング情報を保存するための構造です。 **org***org_name* コマンドを使用して、Intercloud Fabric Switch（VEM）での IP バインディングの学習を有効にできます。 VEM で IP バインディングが学習されると、その情報は PNSC および Intercloud Fabric ファイアウォールに同期されます。 このフィールドは、[Enable for Services] チェックボックスを選択した場合にのみ表示されます。
（オプション）[New Org Name] フィールド	組織の名前。 このフィールドは、[Enable for Services] チェックボックスを選択した場合にのみ表示されます。

ステップ 7 [Next] をクリックします。

ステップ 8 [Port Profile] タブでポート プロファイルを表示します。

ポート プロファイルおよびポート グループの設定

この項には、Intercloud Fabric の vNIC、Intercloud Fabric Extender、および Cisco Prime Network Services Controller（PNSC）仮想マシンに関連付ける必要がある、ポート プロファイルとポート グループに関する情報が記載されています。

仮想マシンの展開に Cisco Nexus 1000V を使用する場合は、Cisco Nexus 1000V VSM でポート プロファイルを作成する必要があります。 VMware vSwitch または VDS を使用する場合は、vCenter でポート グループを作成する必要があります。 ポート プロファイルの作成については、『*Cisco Nexus 1000V Port Profile Configuration Guide*』 を参照してください。 ポート グループの作成については、VMware vSphere のドキュメントを参照してください。

Intercloud Fabric ソリューション向けに、次の vNIC を設定する必要があります。

- Intercloud Fabric Director には 1 つの vNIC があります。この vNIC は、Intercloud Fabric Director への管理アクセス、および PNSC、Intercloud Fabric VSM、エンタープライズ サーバ（DNS、NTP など）への接続を実現する、アクセス ポート プロファイルまたはポート グループに関連付ける必要はあります。

- PNSC には 1 つの vNIC があります。この vNIC は、PNSC への管理アクセス、Intercloud Fabric Director、Intercloud Fabric VSM、Intercloud Fabric Extender、エンタープライズ サーバ（DNS、NTP など）への接続、およびサービス プロバイダー ネットワークに接続するためのインターネット接続を実現する、ポート プロファイルまたはポート グループに関連付ける必要があります。
- Intercloud Fabric Extender には次の 3 つの vNIC があります。
  - **トンネル vNIC**：トンネル vNIC は、Intercloud Fabric Extender と Intercloud Fabric Switch 間にセキュアなトンネルを確立するために使用されます。 この vNIC の使用は任意です。 使用する場合は、サービス プロバイダーへのインターネット アクセスを実現するアクセス ポート プロファイルまたはポート グループに関連付ける必要があります。 また、管理 vNIC を使用して、Intercloud Fabric Extender と Intercloud Fabric Switch 間にセキュアなトンネルを確立することもできます。 デフォルトでは、管理 vNIC を使用して、Intercloud Fabric Switch へのセキュアなトンネル接続が確立されます。 Intercloud Fabric Cloud を作成する際は、Intercloud Fabric Cloud セットアップ ウィザードで [Advanced] チェックボックスをオンにすると、セキュアなトンネルの作成にトンネル vNIC を使用することができます。
  - **管理 vNIC**：管理 vNIC は、Intercloud Fabric Extenderへの管理アクセス、および PNSC、Intercloud Fabric VSM、エンタープライズ サーバ（DNS、NTP など）への接続を実現するために使用されます。 この vNIC は、Intercloud Fabric Extender への管理アクセス、および PNSC、Intercloud Fabric VSM、エンタープライズ サーバ（DNS、NTP など）への接続を実現する、アクセス ポート プロファイルまたはポート グループに関連付ける必要があります。 また、管理 vNIC を使用して、サービス プロバイダー ネットワークの Intercloud Fabric Switch へのセキュアなトンネル接続を確立することもできます。 管理 vNIC を使用してIntercloud Fabric Switch へのセキュアなトンネルを確立する場合は、管理アクセスおよびサービスプロバイダーへのインターネットアクセスも実現する、ポート プロファイルまたはポート グループに管理 vNIC を関連付ける必要があります。
  - **エンタープライズ データ トランク vNIC**：エンタープライズ データ トランク vNIC は、セキュアなトンネルを介してトラフィックを送受信するアップリンクとして使用されます。 この vNIC は、トランク ポート プロファイルまたはポート グループに関連付ける必要があります。 トランク ポート プロファイルには、プロバイダー クラウドに拡張するために必要なすべての VLAN を含める必要があります。 プライベート クラウドで VMware vSwitch または VDS を使用する場合は、データ トランク vNIC に関連するポート グループに対して無差別モードを有効化しなければなりません。

PNSC、Intercloud Fabric Director、および Intercloud Fabric Extender 管理 vNIC に共通するアクセス ポートプロファイルまたはポートグループを作成できます。 管理vNICの代わりにトンネルvNICを使用して、Intercloud Fabric Switch へのセキュアなトンネル接続を確立する場合は、別のアクセス ポート プロファイルまたはポート グループを作成する必要があります。

（注） ネイティブ VLAN がサポートされません。 ポート プロファイルとポート グループで明示的に VLAN を指定する必要があります。

（注） Intercloud Fabric Extender トランク インターフェイスのトランク ポート プロファイルには、内部トンネル トランク インターフェイスのトランク ポート プロファイルで Intercloud Fabric Extender および Intercloud Fabric スイッチ用として指定された VLAN が含まれていなければなりません。

VMware vSwitch を使用する場合は、次のポート プロファイルを設定する必要があります。

- Intercloud Fabric Extender トンネル インターフェイスのポート グループ。 このポート グループは、トランキング モードのすべての VLAN を許可する必要があります。

手順

ステップ 1 Cisco Nexus 1000V がプライベート クラウドで使用されている場合に、Cisco Nexus 1000V に管理ポート プロファイルを作成するための設定例。

```
port-profile type vethernet VLAN-36
  vmware port-group
  switchport mode access
  switchport access vlan 36
  no shutdown
  state enabled
```

ステップ 2 Cisco Nexus 1000V がプライベート クラウドで使用されている場合に、Cisco Nexus 1000V にトンネル ポート プロファイルを作成するための設定例。

```
port-profile type vethernet VLAN-37
  vmware port-group
  switchport mode access
  switchport access vlan 37
  no shutdown
  state enabled
```

ステップ 3 Cisco Nexus 1000V がプライベート クラウドで使用されている場合に、Cisco Nexus 1000V にトランク ポート プロファイルを作成するための設定例。

```
port-profile type vethernet Trunk
  vmware port-group
  switchport mode trunk
  switchport trunk allowed vlan 36-37,208,1300-1315
  no shutdown
  state enabled
```

ネットワーク要素の追加

Cisco Nexus 1000V スイッチを使用している場合は、Intercloud Fabric Cloud を作成する前に、Intercloud Fabric に Cisco Nexus 1000V スイッチを追加する必要があります。 Intercloud Fabric のネッ

トワーク要素として Cisco Nexus 1000V スイッチを追加すると、そのスイッチが [Managed Network Element] タブに表示されます。

手順

ステップ 1 Intercloud Fabricにログインします。

ステップ 2 [Administration] > [Managed elements] の順に選択します。

ステップ 3 [Managed Network Elements] タブで、[Add Network Element] をクリックします。

ステップ 4 [ネットワーク機器の追加] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[POD] ドロップダウン リスト	ネットワーク要素が属するポッドを選択します。
[デバイスカテゴリ] ドロップダウン リスト	デバイス カテゴリとして [Cisco Nexus 1000V] を選択します。
[デバイスIP] フィールド	Cisco Nexus 1000V スイッチの IP アドレス。
[Protocol] ドロップダウン リスト	使用されるプロトコルを選択します。 リストには次の内容が含まれます。 • Telnet • ssh • http • https
[Port] フィールド	使用するポート番号。
[ログイン] フィールド	ログイン名。
[Password] フィールド	ログイン名に関連付けられるパスワード。

ステップ 5 [Submit] をクリックします。

Microsoft Azure における Intercloud Fabric のセキュリティ クレデンシャルへのアクセス

Microsoft Azure で Intercloud Fabric のセキュリティ クレデンシャルにアクセスするには、次の手順を実行します。

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。

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、[Export Azure Certificate] をクリックします。

ステップ 4 Microsoft Azure 管理ポータルにログインします。

ステップ 5 [Settings] > [Management Certificate] の順に選択します。

ステップ 6 [Upload] をクリックし、証明書をアップロードします。

ステップ 7 [Items] ページで、一番上にある [Subscription] ドロップダウン リストからサブスクリプション ID を選択します。

次の作業

このサブスクリプション ID を使用して Intercloud Fabric で Intercloud Fabric Cloud を作成します。

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, （13 ページ）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。
[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。

名前	説明
[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。
[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, （4 ページ） を参照してください。

名前	説明
[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, （7 ページ） 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, （6 ページ） 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, （5 ページ） 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 Cloud の複製

Intercloud Fabric Cloud を複製するには、次の手順を実行します。 元の Intercloud Fabric Cloud とまったく同じ設定で Intercloud Fabric Cloud の複製を作成するには、[1-click Clone] をクリックします。

（注） [1-click Clone] は、Microsoft 環境で Intercloud Fabric Cloud を作成する場合はサポートされません。

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、Intercloud Fabric Cloud を選択し、[Clone] 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。

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、1 ～ 16 文字を含めることができます。 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。 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。
[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です。
[Access Key] フィールド	アカウントの一意のキーです。

名前	説明
[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。
[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, （4 ページ） 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, （7 ページ） を参照してください。

名前	説明
[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, （6 ページ） 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, （5 ページ） 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。
[ICF Router (Integrated)] チェックボックス	[ICF Router (Integrated)] テンプレートを作成するには、[ICF Router (Integrated)] チェックボックスをオンにします。
[ICF Router (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を参照してください。

名前	説明
[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。

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。
[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。

名前	説明
[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。
[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。

名前	説明
[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。
[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 Network Placement]	
[Host] ドロップダウン リスト	Intercloud Fabric Extender のホストを選択します。 [Primary Intercloud Extender] と [Secondary Intercloud Extender] のホストを指定するには、[High Availability] チェックボックスをオンにします。 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。

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。 [Primary Intercloud Extender] と [Secondary Intercloud Extender] のデータストアを指定するには、[High Availability] チェックボックスをオンにします。 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。
[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。
[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。

名前	説明
[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 を複製します。

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 [サービスリクエスト] 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。