# Cisco Intercloud Fabric スタートアップ ガイド リリース 2.2.1

**初版**：2015 年 04 月 19 日

**最終更新**：2015 年 05 月 14 日

**シスコシステムズ合同会社**
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。 このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。 このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。 添付されていない場合には、代理店にご連絡ください。

シスコが採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB（University of California, Berkeley）のパブリック ドメイン バージョンとして、UCB が開発したプログラムを採用したものです。 All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。 シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。 マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。 説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2014-2015 Cisco Systems, Inc. All rights reserved.

# 目 次


概要 1

Cisco Intercloud Fabric について 1

Cisco Intercloud Fabric 製品について 2

Cisco Intercloud Fabric のアーキテクチャ 3

Intercloud Fabric Director 4

Secure Cloud Extension 5

Cisco Intercloud Fabric の推奨ネットワーク トポロジ 7

**Cisco Intercloud Fabric のインストール 9**

Cisco Intercloud Fabric のインストールについて 9

システム要件 10

前提条件 12

注意事項と制約事項 15

Cisco Intercloud Fabric のライセンスについて 15

ライセンスの要件 16

製品アクセス キーの契約履行 16

VMware 環境への Intercloud Fabric のインストール ワークフロー 17

VMware 環境への Intercloud Fabric のインストール 18

Intercloud Fabric のライセンスのインストール 20

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 21

OpenStack 環境への Intercloud Fabric のインストール ワークフロー 24

OpenStack での Intercloud Fabric 環境の準備 25

テナントと仮想ネットワークの作成 25

OpenStack 環境への Intercloud Fabric のインストール 27

OpenStack 環境への Intercloud Fabric インフラストラクチャ コンポーネントのインストール 29

Microsoft 環境への Intercloud Fabric のインストール ワークフロー 32

インストールの準備 33

Intercloud Fabric zip ファイルの内容 33
Intercloud Fabric コンポーネント テンプレートの登録 35
Intercloud Fabric のインストールと設定 35
VM テンプレートによる Intercloud Fabric のインスタンス化 36
Intercloud Fabric 仮想マシンの設定 37
Intercloud Fabric VSM のインスタンス化と設定 39
VM テンプレートによるIntercloud Fabric VSM VM のインスタンス化 39
Intercloud Fabric VSM VM の設定 40
Intercloud Fabric Extender の展開と設定 43
VM テンプレートによるIntercloud Fabric Extender VM のインスタンス化 44
Intercloud Fabric Extender の設定 45
Microsoft 環境への Intercloud Fabric インフラストラクチャ コンポーネントのインストール 46
システム リソースの予約 48
**Intercloud Fabric Cloud の作成 49**
Intercloud Fabric Cloud の詳細 49
注意事項と制約事項 50
前提条件 50
Intercloud Fabric Cloud 作成のワークフロー 51
Intercloud Fabric のインフラストラクチャ ポリシーとプールの作成 52
MAC アドレス プールの追加 52
プライベート サブネットの追加 53
IP グループの追加 54
トンネル プロファイルの設定 55
ポート プロファイルの作成 58
ポート プロファイルおよびポート グループの設定 59
ネットワーク要素の追加 61
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 63
Intercloud Fabric Cloud の作成 63
サービスの管理 72
Intercloud Fabric Cloud の複製 75

**仮想マシンの展開 83**

仮想マシンの展開について 83

注意事項と制約事項 83

前提条件 85

仮想マシンの展開ワークフロー 86

仮想マシンの作成 87

ポリシーの作成 87

Intercloud Fabric ネットワーク ポリシーの作成 87

Intercloud Fabric システム ポリシーの作成 89

スタティック IP プール ポリシーの作成 90

ユーザ グループの作成 91

ユーザ グループへのユーザの追加 93

VMware ネットワーク ポリシーの作成 94

VMware コンピューティング ポリシーの作成 95

Intercloud Fabric 仮想データセンターの作成 96

プライベート仮想データセンターの作成 99

Intercloud Fabric へのイメージのアップロード 101

Intercloud Fabric Cloud でのテンプレートの作成 103

テンプレートへのカタログの追加 104

サービス要求の作成 106

アプリケーション カテゴリの管理 108

仮想マシンの移行 109

Intercloud Fabric Cloud への仮想マシンの移行 109

プライベート クラウドへの仮想マシンの移行 110

**クラウド仮想マシンのオンボード 111**

クラウド仮想マシンのオンボードについて 111

注意事項と制約事項 111

前提条件 112

Intercloud Fabric へのクラウド仮想マシンのオンボード 113

**Intercloud Fabric ファイアウォールのインストール 117**

Intercloud Fabric Firewall について 117

前提条件 118

注意事項と制約事項 118
基本的なトポロジ 119
Intercloud Fabric Firewall のインストール ワークフロー 119
Intercloud Fabric Cloud の作成 120
サービスの管理 129
Intercloud Fabric Firewallのインスタンス化 131
コンピュート セキュリティ プロファイルの設定 133
サービス パスの作成 135
ポート プロファイルへのサービス パスのバインド 137
Intercloud Fabric Firewall 用のポート プロファイルの編集 138
Intercloud Fabric Firewall のインストールの確認 139
**Intercloud Fabric Router（CSR）のインストールと設定 141**
Intercloud Fabric Router（CSR）について 141
注意事項と制約事項 142
前提条件 143
Intercloud Fabric Router（CSR）のインストールと設定に関するワークフロー 143
Intercloud Fabric Cloud の作成 144
サービスの管理 153
Intercloud Fabric Router（CSR）のインスタンス化 156
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 160
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 161
Intercloud Fabric Router のインストールの確認 165
**Intercloud Fabric Router（統合型）のインストールと設定 169**
Intercloud Fabric Router (Integrated)について 169
注意事項と制約事項 170
前提条件 171
Intercloud Fabric Router (Integrated) のインストールと設定に関するワークフロー 171
Intercloud Fabric Cloud の作成 171
Intercloud Fabric Router (Integrated) のサービスの有効化 180
Intercloud Fabric Router (Integrated) のルータ インターフェイスの設定 181
スタティック ルーティングの設定 186

Intercloud Fabric Router (Integrated) のネットワーク アドレス変換について 189
Intercloud Fabric Router (Integrated) の NAT ポリシーの設定 189
Intercloud Fabric Router (Integrated) のインストールの確認 194
**Cisco Intercloud Fabric のアップグレード 195**
Cisco Intercloud Fabric のアップグレードについて 195
前提条件 195
Intercloud Fabric のアップグレード ワークフロー 196
Intercloud Fabric アップグレード ソフトウェア バンドルのダウンロード 196
VM の展開とアップグレード 197
Upgrade VM のネットワークの設定 198
1 つの Intercloud Fabric VM イメージのダウンロード 199
setup_info ファイルの設定 200
Intercloud Fabric のアップグレード 202
Intercloud Fabric の アップグレードの出力例 203
Intercloud Fabric コンポーネントのアップグレード 204
サービス VM のアップグレード 205
Intercloud Fabric Router（CSR）のアップグレード 205
Intercloud Fabric Firewall（VSG）のアップグレード 206
**その他の情報 209**
Cisco Intercloud Fabric の関連資料 209
マニュアルの入手方法およびテクニカル サポート 210
マニュアルに関するフィードバック 211

第 1 章

# 概要

This chapter contains the following sections:


- Cisco Intercloud Fabric について，1 ページ
- Cisco Intercloud Fabric 製品について，2 ページ
- Cisco Intercloud Fabric のアーキテクチャ，3 ページ
- Cisco Intercloud Fabric の推奨ネットワーク トポロジ，7 ページ

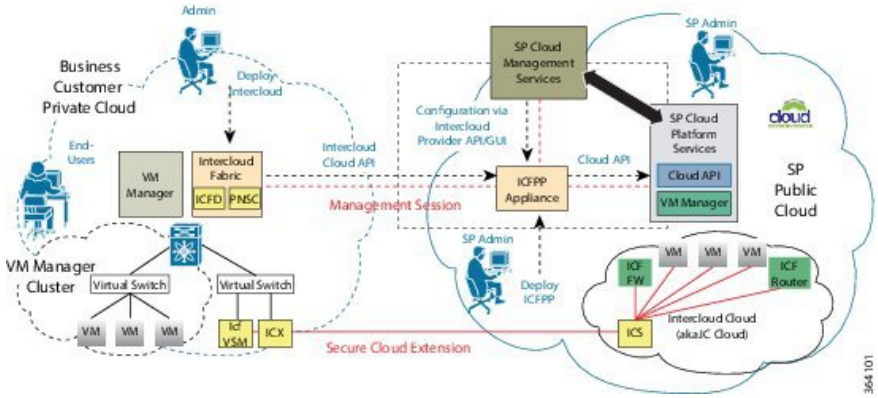

## Cisco Intercloud Fabric について

Cisco Intercloud Fabric はハイブリッド クラウドによって、ビジネス ニーズに迅速かつ柔軟に応え、潜在的な課題に対応します。 ハイブリッド クラウドはプライベートとプロバイダー クラウド間の相互作用です。ハイブリッドクラウドでは、安全かつスケーラブルな方法で、プライベート クラウドがプロバイダー クラウドへと拡張され、プライベート クラウドからプロバイダー クラウドのリソースを使用できます。 Cisco Intercloud Fabric を使用すると、複数のプロバイダー クラウドの異機種混在環境にワークロードを配置できます。 Cisco Intercloud Fabric は安全なハイブリッド クラウドのためのアーキテクチャ基盤を提供します。これによって企業は、必要に応じてオンデマンドで、プライベート クラウドをプロバイダー クラウドに簡単かつ安全に接続できます。ハイブリッド クラウドの導入によって、企業はパブリック クラウドとプロバイダー クラウドの両方のメリットを享受できます。 Cisco Intercloud Fabric には、次のような利点があります。

- 複数のプロバイダークラウドにわたる仮想ワークロードを、一元的に管理および制御できます。
- Amazon Web Service、Microsoft Azure、および Intercloud Fabric Provider ベースのクラウドなど、クラウド プロバイダーを選択できます。
- 安全性の高いスケーラブルな接続によって、プライベート クラウドをサービス プロバイダーのクラウドに拡張できます。
- ハイブリッドクラウドを通じて一貫性のあるネットワーク ポリシーとワークロード ポリシーを実現できます。

- 仮想ワークロードに対し、サービスプロバイダークラウドとの間でワークロードモビリティを実現できます。

**図 *1*：*Cisco Intercloud Fabric***




# Cisco Intercloud Fabric 製品について

企業またはサービス プロバイダーであるお客様に対応するために、Cisco Intercloud Fabric アーキテクチャには次の 2 種類の製品構成があります。

- Cisco Intercloud Fabric for Business
- Cisco Intercloud Fabric for Providers

Cisco Intercloud Fabric for Business は、環境全体で同一レベルのセキュリティとポリシーを維持しながら、プライベートクラウドをプロバイダークラウド環境に透過的に拡張することを希望している企業のお客様を対象としています。 Cisco Intercloud Fabric for Business は次のコンポーネントから構成されています。

- Intercloud Fabric 仮想マシン
- Secure Cloud Extension

『*Cisco Intercloud Fabric* スタートアップ ガイド』には、Cisco Intercloud Fabric for Business のコンポーネントのインストールに関する情報が記載されています。

Cisco Intercloud Fabric for Providers はプロバイダーによって管理されるクラウド環境を対象としており、企業のお客様が、クラウド環境全体で同一レベルのセキュリティとポリシーを維持しながら、プライベート クラウドをプロバイダーの クラウドに透過的に拡張できるようにします。

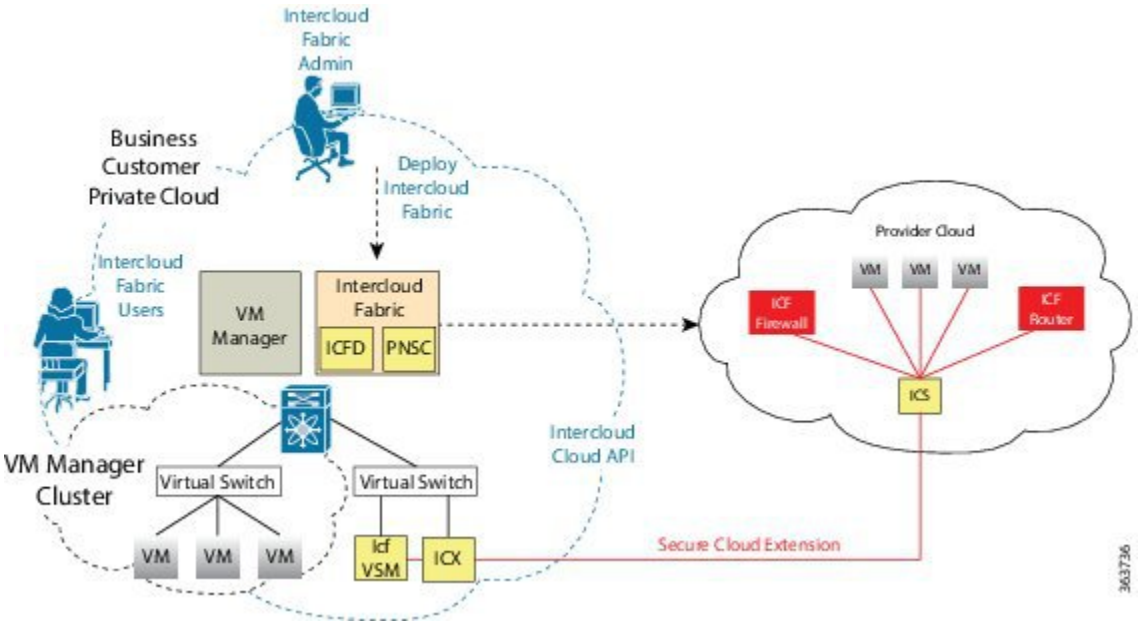
『*Cisco Intercloud Fabric Provider Platform Installation Guide*』には、Cisco Intercloud Fabric Providers のコンポーネントのインストールに関する情報が記載されています。

# Cisco Intercloud Fabric のアーキテクチャ

Cisco Intercloud Fabric は、プライベート クラウドおよびプロバイダー クラウドに仮想マシン（VM）として展開されるハイブリッド クラウド ソリューションです。 Cisco Intercloud Fabric for Business は次のコンポーネントから構成されています。

- Intercloud Fabric 仮想マシン：この VM には Intercloud Fabric Director と Prime Network Services Controller が含まれています。
- Secure Cloud Extension：このコンポーネントには Intercloud Fabric Extender（ICX）と Intercloud Fabric Switch（ICS）が含まれています。

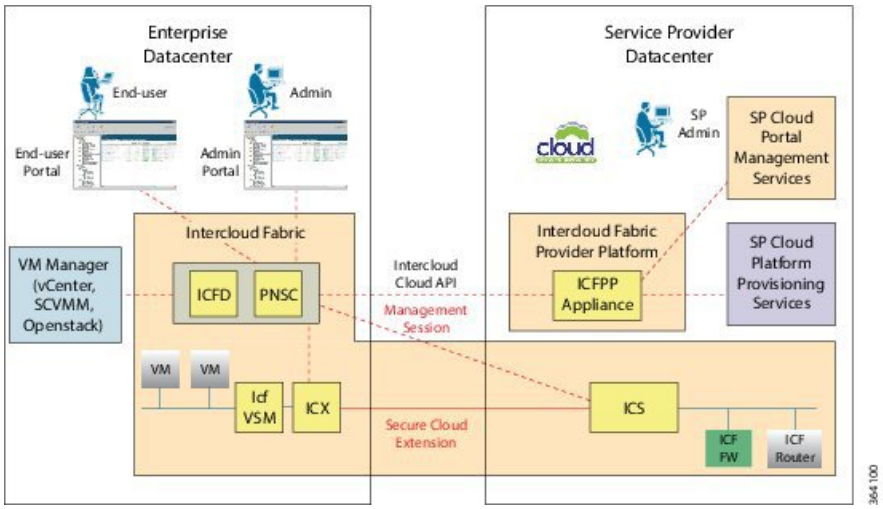
**図 *2*：*Intercloud Fabric for Business* のアーキテクチャ**




Intercloud Fabric Provider Platform は拡張可能なアダプタ フレームワークを提供して、異なるプロバイダー クラウドのインフラストラクチャ管理プラットフォームとの統合や、他のクラウド API との統合を実現します。 これはプロバイダー クラウドに展開される仮想アプライアンスであり、サービス プロバイダーの顧客が Intercloud Fabric API を使用してクラウド リソースにアクセスできるようにします。 また、まざまなプロバイダー インフラストラクチャ プラットフォームに合

わせて API コールを変換するので、顧客は、サービス プロバイダーによって公開されるクラウド API に関係なく、ワークロードの移動を選択できます。

**図 *3*：*Intercloud Fabric for Providers* のアーキテクチャ**



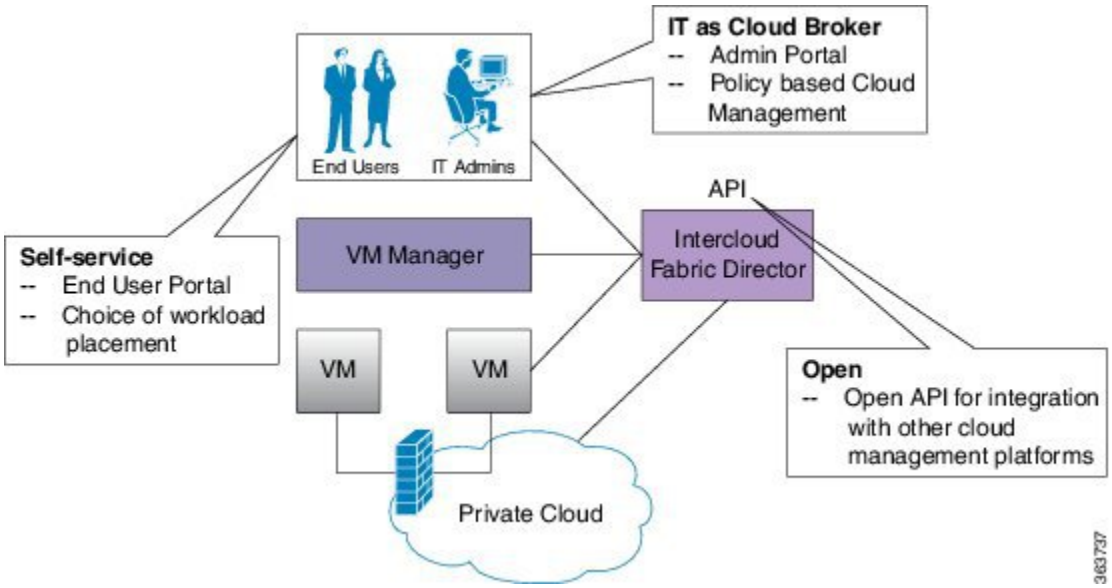

# Intercloud Fabric Director

Intercloud Fabric Director は、エンドユーザおよびIT管理者向けのハイブリッドクラウドソリューションにおいて管理と消費を一元化します。 エンドユーザおよびIT管理者がプライベートクラウドやプロバイダー クラウドに対してワークロードをプロビジョニングできるように、1つのコンソールを提供します。 Intercloud Fabric Director が公開するノースバウンド API によって、顧客はハイブリッド クラウド環境でのワークロード管理をプログラムしたり、他のクラウド管理プラットフォームと統合することができます。

Intercloud Fabric Director は、IT 管理者がハイブリッド クラウドのオファーを管理したり消費するためのセルフサービス ポータルと、エンドユーザがサービスを消費するためのセルフサービス ポータルも提供します。 エンドユーザ向けとして、Intercloud Fabric Director には、複数のクラウドからのオファーを組み合わせたサービスカタログと、複数のプロバイダークラウドに対応する1つの IT セルフサービス ポータルがあります。

IT 管理者向けとして、Intercloud Fabric Director には、ユーザの設定、カタログの作成、仮想マシン テンプレートの作成など、さまざまな管理タスクを実行できる IT 管理ポータルがあります。

**図 *4*：*Intercloud Fabric Director* の機能**




# Secure Cloud Extension

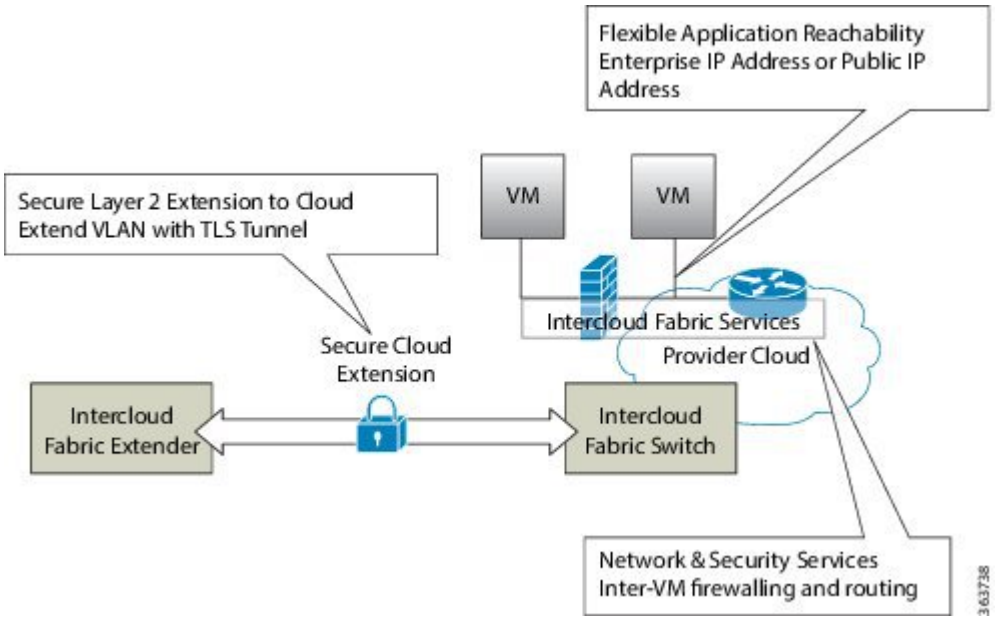
Secure Cloud Extension は、Cisco Intercloud Fabric ソリューションでのコア スイッチングとサービス インフラストラクチャの基礎を形成します。 Secure Cloud Extension は次の機能を提供します。

- プライベート クラウドからプロバイダー クラウドへのレイヤ 2 ネットワークの拡張
- プロバイダー クラウドで動作するアプリケーション向けの高度なスイッチング機能
- ゾーン ベースのファイアウォールやルーティングなど、プロバイダー クラウドでのサービスのサポート

Secure Cloud Extension は複数のコンポーネントから構成されており、これらは連携して上記の機能を提供します。 プライベート クラウドは、仮想アプライアンス ペア間で確立される非常にセキュアなトンネルを介して、プロバイダー クラウドに接続されます。 Intercloud Fabric Extender（ICX）はプライベート クラウドで実行され、Intercloud Fabric Switch（ICS）はプロバイダー クラウドで実行されます。 これらのアプライアンスをハイ アベイラビリティ ペアとして展開する

ことで、冗長性を実現できます。仮想サービスがこの環境内に展開され、プロバイダークラウドでファイアウォールとルーティングが有効になります。

**図 *5*：*Secure Cloud Extension***




### Intercloud Fabric Extender

Intercloud Fabric Extender は、プライベート クラウドで動作する仮想マシンです。 その役割は、プライベート クラウドの Intercloud Fabric コンポーネントとプロバイダー クラウドを相互接続する、セキュアなトンネルを確立することです。 Intercloud Fabric Extender の主な機能は次のとおりです。

- すべてのクラウド リソースを相互接続するセキュアなトンネルを確立します。
- プライベート クラウドの Cisco Nexus 1000V などの仮想スイッチとやり取りします。

### Intercloud Fabric Switch

Intercloud Fabric Switch は、プロバイダー クラウドで動作する仮想マシンです。 その役割は、プロバイダー クラウドの VM をプライベート クラウド VM やクラウド内の他の VM と接続する、セキュアなトンネルを確立することです。 Intercloud Fabric Switch の主な機能は次のとおりです。

- 仮想イーサネットモジュール（VEM）を実行して、Cisco Nexus 1000V 機能を提供します。
- VEM と Intercloud Fabric Extender を接続するセキュアなトンネルを確立します。
- クラウド すべての VM を接続するセキュアなトンネルを確立します。
- クラウド内の VM の統計情報をモニタしてレポートします。
- クラウド内のすべてのコンポーネント障害をモニタし、Cisco Prime Network Services Controller（PNSC）にレポートします。

VEM は Intercloud Fabric Switch に組み込まれており、次のような役割を担っています。

- プライベート クラウドで動作しているスーパーバイザ モジュール（VSM）機能と通信し、ポート プロファイルなどの VM 固有のネットワーク ポリシーを取得します。
- クラウド VM 間のネットワーク トラフィックを切り替えます。
- クラウド VM とプライベート クラウド間のネットワーク トラフィックを切り替えます。
- ネットワーク ポリシーをあらゆるスイッチング ネットワーク トラフィックに適用します。
- VEM 関連の統計情報を収集してレポートします。

### Cisco Intercloud Fabric エージェント

Cisco Intercloud Fabric エージェント（ICA）は、クラウドの VM にネットワーク オーバーレイをもたらします。 このエージェンは、クラウド内のゲスト VM を保護し、クラウドインフラストラクチャを抽象化します。 クラウド VM のオペレーティング システム内で動作するセキュア トンネル ドライバとしてプロバイダー クラウドで展開されます。 また、次のように、ネットワーク トラフィックを安全なオーバーレイ ネットワークにリダイレクトします。

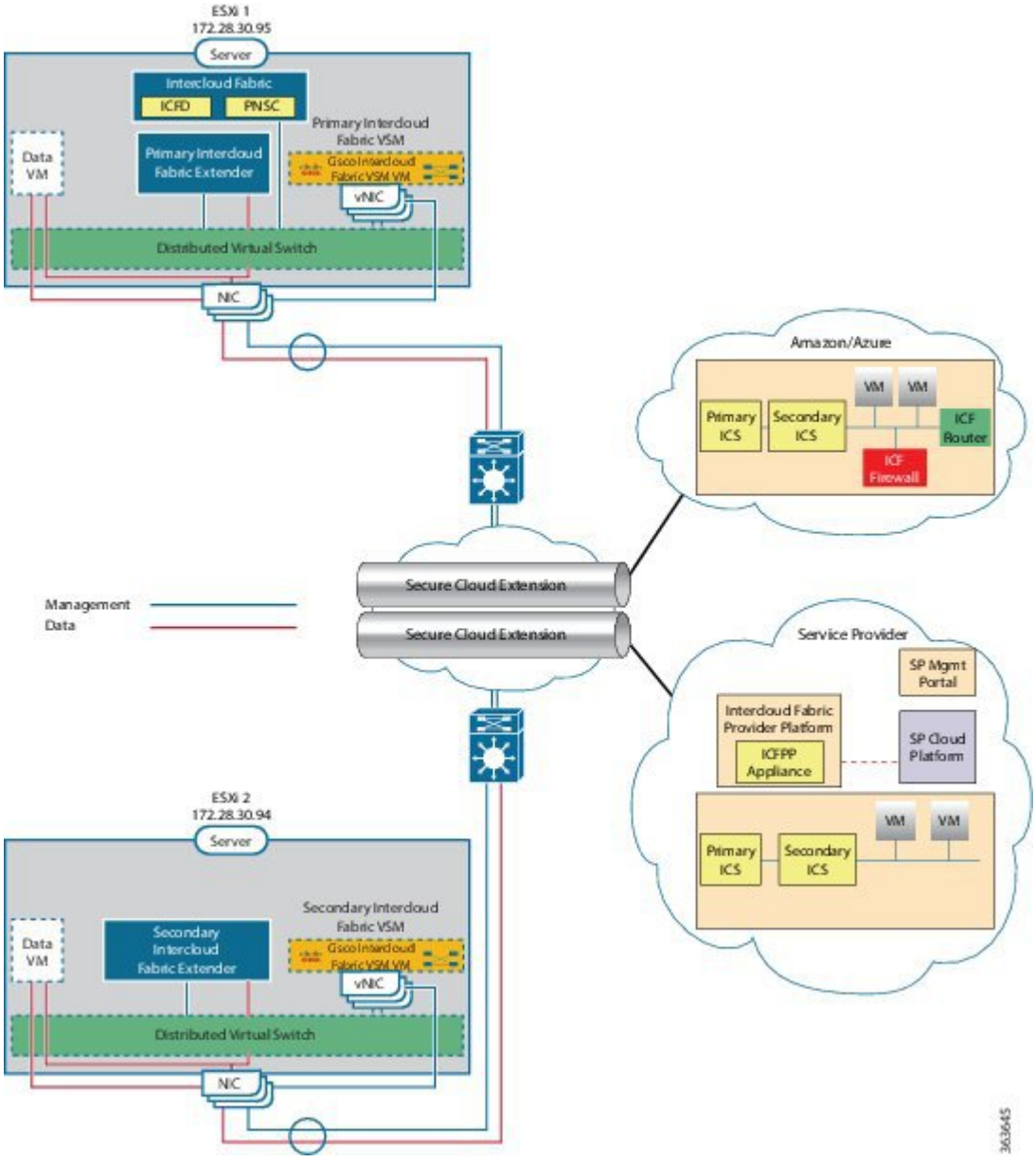
- Intercloud Fabric Switch に接続するセキュアなトンネルを確立し、クラウド内の VM がプライベート クラウドの VM やプロバイダー クラウドの VM と通信できるようにします。
- 安全なオーバーレイ関連の統計情報を収集します。

# Cisco Intercloud Fabric の推奨ネットワーク トポロジ

Intercloud Fabric の推奨ネットワーク トポロジは次のとおりです。

（注） VMware HA 対応クラスタに 2 台のサーバが配置されます。

図 *6*：***Intercloud Fabric*** の推奨ネットワーク トポロジ



第 2 章

# Cisco Intercloud Fabric のインストール

This chapter contains the following sections:


- Cisco Intercloud Fabric のインストールについて，9 ページ
- システム要件，10 ページ
- 前提条件，12 ページ
- 注意事項と制約事項，15 ページ
- Cisco Intercloud Fabric のライセンスについて，15 ページ
- VMware 環境への Intercloud Fabric のインストール ワークフロー，17 ページ
- OpenStack 環境への Intercloud Fabric のインストール ワークフロー，24 ページ
- Microsoft 環境への Intercloud Fabric のインストール ワークフロー，32 ページ
- システム リソースの予約，48 ページ


## Cisco Intercloud Fabric のインストールについて

Cisco Intercloud Fabric for Business ソフトウェアは cisco.com から入手できます。 Cisco Intercloud Fabric for Business ソフトウェアには次の zip イメージが含まれています。

| 名前 | 説明 |
|---|---|
| icfb-k9-2.2.1-pkg.zip | VMware 環境に Intercloud Fabric をインストールするためのソフトウェア。<br><br>Intercloud Fabric Director および Cisco Prime Network Services Controller をインストールするには、このファイルを使用します。 VMware 環境への Intercloud Fabric のインストール，（18 ページ）を参照してください。 |

| 名前 | 説明 |
|---|---|
| icfb-k9-services-2.2.1-pkg.zip | Intercloud Fabric サービスを管理するためのソフトウェア。<br>クラウド セットアップ ウィザードを使用して Intercloud Fabric Firewall や Intercloud Fabric Router（CSR）などのサービスを管理するには、このファイルを使用します。Intercloud Fabric Cloud の作成, （63 ページ）を参照してください。 |
| icfb-k9-upgrade-2.2.1-pkg.zip | VMware 環境で Intercloud Fabric を 2.1.1a から 2.1.2 にアップグレードするためのソフトウェア。<br>Cisco Intercloud Fabric のアップグレードについて, （195 ページ）を参照してください。 |

OpenStack 環境や Microsoft 環境向けの Cisco Intercloud Fabric for Business も用意されています（機能に制限があります）。 詳細については、シスコのセールス担当者にお問い合わせください。

# システム要件

次の表は、Cisco Intercloud Fabric のインストールに対するシステム要件を示しています。

**表 *1*：システム要件**

| 要件 | 説明 |
|---|---|
| **Intercloud Fabric** | |
| CPU | 8 vCPU（64 ビット x86 CPU、VT 対応） |
| ネットワーク インターフェイス カード（vNIC） | 1 |
| RAM | 20 GB |
| ディスク | 350 GB |
| **Intercloud Fabric Extender** | |
| メモリ | 2 GB |
| CPU | 2 vCPU |
| ディスク | 3 GB |
| **Intercloud Fabric VSM** | |

| 要件 | 説明 |
|---|---|
| メモリ | 2 GB |
| CPU | 1 vCPU |
| ディスク | 3 GB |

（注） 仮想ディスクは、少なくとも 40 MB/s の帯域幅に対応できる必要があります。

表 *2*：ハイパーバイザ要件

| 要件 | 説明 |
|---|---|
| **VMware** | |
| Version | 5.1 または 5.5、ESXi |
| **OpenStack KVM** | |
| Version | Icehouse |
| Red Hat Enterprise Linux for OpenStack バージョン | 7.1 |
| **Microsoft System Center Virtual Machine Manager（SCVMM）** | |
| Version | SCVMM 2012 R2 |

表 *3*：クライアントのブラウザの要件

| 要件 | 説明 |
|---|---|
| ブラウザ | Google Chrome 32.0 以降<br>（注） Intercloud Fabric では Google Chrome を使用することをお勧めします。 |

表 *4*：プロバイダー クラウドのシステム要件

| プロバイダー/モデル | デバイス | vCPU | メモリ（GB） | ディスク（GB） |
|---|---|---|---|---|
| **AWS** | | | | |

| プロバイダー/モデル | デバイス | vCPU | メモリ（GB） | ディスク（GB） |
|---|---|---|---|---|
| c3.2xlarge | Intercloud Fabric Switch | 8 | 15 | 20 |
| c3.xlarge | Intercloud Fabric Router | 4 | 7.5 | 8 |
| m3.medium | Intercloud Fabric Firewall（VSG） | 1 | 3.75 | 2 |
| **Azure** | | | | |
| A3 | Intercloud Fabric Switch | 4 | 7 | 20 |
| A3 | Intercloud Fabric Firewall（VSG） | 2 | 3.5 | 2 |
| **その他のすべてのプロバイダー** | | | | |
| | Intercloud Fabric Switch | 4 | 4 | 20 |
| | Intercloud Fabric Firewall（VSG） | 1 | 3 | 3 |
| | Intercloud Fabric Router（CSR） | 4 | 4 | 8 |

（注） 最適なパフォーマンスを実現するために、上記の最小システム要件よりも余裕があるシステム リソースを、Intercloud Fabric Director 用に予約することをお勧めします。 詳細については、システム リソースの予約, （48 ページ） を参照してください。

# 前提条件

### クラウド プロバイダーの前提条件

- クラウド プロバイダーのプロバイダー アカウントを作成します。
- プロバイダー クラウドで作成された仮想マシンにクラウド プロバイダーが割り当てる、パブリック IP アドレスの範囲を調べます。

（注） 必要なリージョンのクラウド プロバイダーの IP アドレスを開く必要があります。

- Intercloud Fabric Extender がIntercloud Fabric Switch と通信できるように、ファイアウォールの特定のポートを開く必要があります。 ポート 443 は常に開いておく必要があります。 UDP トンネルでは、ポート 6644 も開く必要があります。 TCP のトンネルでは、ポート 6646 または 443 を使用できます。 トンネル プロファイルを設定する際は、選択したトンネル プロトコルとポートを指定します。
- Cisco Prime Network Services Controller の IP アドレスからクラウド プロバイダーへのアウトバウンドであるファイアウォールで、TCP ポート 22 と 443 を開く必要があります。

### Virtual Machine Manager の前提条件

- VMware 環境の場合：
  - VMware の指示に従い、ホスト管理用の vCenter Server をインストールして、準備します。
  - VMware vSphere Client をインストールします。
  - すべての Intercloud Fabric Cloud ホストで、サポート対象である ESX または ESXi のバージョン 5.1/5.5 が実行されていることを確認します。
  - VMware vCenter への管理者アクセスがあります。
  - 冗長性を確保するために、各ホストに 2 つの物理ネットワーク インターフェイス カード（NIC）を適用します。 NIC が 1 つでも導入は可能です。
  - Cisco Intercloud Fabric Director と Cisco Prime Network Services Controller は、すべての ESXi ホストにポート 443 で IP 接続できなければなりません。 Cisco Prime Network Services Controller はこのパスを使用して、ホストに Intercloud Fabric Extender イメージをアップロードします。
- OpenStack 環境の場合：
  - プライベート データセンター（企業側）で OpenStack が実行されている必要があります。
  - インフラストラクチャ コンポーネントと Intercloud Fabric Cloud を HA モードで展開するには、複数のコンピュート ノードが必要です。
- Microsoft 環境では、すべてのホストに Windows Server 2012 R2 がインストールされ、Hyper-V が有効になっていなければなりません。 これらのホストは、System Center Virtual Machine Manager（SCVMM）R2 UR5 以上で管理する必要があります。

### Cisco Intercloud Fabric の前提条件

- ICF、ICFD、および PNSC の IP、サブネット マスク、ゲートウェイに関する情報を確認します。
- DNS サーバおよびドメイン名情報を確認します。
- 適切な NTP サーバを使用していることを確認します。
- クラウド プロバイダーに接続するように日時が正しく設定されていることを確認します。
- 仮想マシン（VM）の管理ポート プロファイルまたは管理ネットワークの名前（Management）を確認します。

（注） 管理ポート プロファイルは、Cisco Nexus 1000V VSM で使用されるポート プロファイルと同じものでかまいません。 ポート プロファイルは VSM で設定され、Cisco Prime Network Services Controller 管理インターフェイスで使用されます。 この要件は、Cisco Nexus 1000V スイッチを使用する場合にのみ適用されます。VMware 仮想スイッチを使用する場合は適用されません。

- OpenStack 環境では、Cisco Nexus 1000V スイッチが必要です。
- 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。

### 仮想スイッチの前提条件

- **VMware**
  - VMware 仮想マシン上のトランク ポート グループのセキュリティ ポリシーに対して、VMware vSphere GUI で、[Promiscuous Mode]、[MAC Address Changes]、および [Forged Transmits] を [Accept] に設定します。 この要件は、VMware 仮想スイッチと分散スイッチを使用する場合にのみ適用されます。Cisco Nexus 1000V スイッチを使用する場合には適用されません。
  - Intercloud Fabric Extender が VMware vSwitch または分散スイッチ（VDS）でホストされており、vSwitch または分散スイッチが複数の物理 NIC に接続している場合は、Intercloud Fabric Extender がホストされている ESX ホストで [Net.ReversePathFwdCheckPromisc=1] の設定を有効にする必要があります。 この設定は、VMware vSphere UI の [Host] > [Configuration] > [Advanced Settings] > [Net] にあります。 この設定を有効にしないと、エンタープライズとクラウド VM トラフィックの間でトラフィックの損失やパケットの重複が発生したり、Intercloud Fabric VSM で Intercloud Fabric Switch モジュール フラップが発生する可能性があります。 この要件は、VMware 仮想スイッチまたは分散スイッチを使用して Intercloud Fabric Extender をホストする場合にのみ適用されます。Cisco Nexus 1000V スイッチを使用する場合には適用されません。
- Cisco Nexus 1000V スイッチ

プライベート クラウドで Cisco Nexus 1000V スイッチを使用する場合は、不明なユニキャスト フラッディングのブロック（UUFB）を無効化する必要があります。 UUFB を無効化するには、**no uufb enable** コマンドを入力します。 UUFB が無効化されたことを確認するには、**show run | include uufb** コマンドを入力します。

- **Microsoft Hyper-V**
  - Microsoft Hyper-V Hypervisor で使用される仮想スイッチは、ネイティブの Hyper-V スイッチでも、そのスイッチを Cisco Nexus 1000V ベースで拡張したものでもかまいません。
  - Intercloud Fabric Extender データ ポートはアクセス モードのみをサポートしています。
  - MAC スプーフィングを Intercloud Fabric Extender データ ポートで有効にする必要があります。
- **Openstack**

  OpenStack KVM には仮想スイッチのいずれの前提条件も適用されません。

# 注意事項と制約事項

- VMware 環境では、VMware vSphere または VMware vSwitch 向けの Cisco Nexus 1000V、または VDS がすでにプライベート クラウドにインストールされています。 詳細については、『Cisco Nexus 1000V for Hyper-V』を参照してください。
- OpenStack 環境では、KVM 向けの Cisco Nexus 1000V がすでにプライベート クラウドにインストールされています。 詳細については、『Cisco Nexus 1000V for KVM』を参照してください。
- Microsoft 環境では、Hyper-V 向けの Cisco Nexus 1000V はオプションです。 Hyper-V ホストではネイティブの Hyper-V スイッチを使用できます。
- OpenStack Icehouse リリースは、KVM 向けの Cisco Nexus 1000V でサポートされます。
- KVM 向け Cisco Nexus 1000V をインストールする際は、Red Hat Enterprise Linux OpenStack Platform Installer（RHEL-OSP Installer）を使用することをお勧めします。
- Intercloud Fabric Cloud は最大 100 台 の VM をサポートできます。
- Microsoft 環境では、SCVMM R2 UR5 以降を使用してください。

# Cisco Intercloud Fabric のライセンスについて

Cisco Intercloud Fabric では、ライセンス数は、プロバイダー クラウドでプロビジョニング可能な仮想マシンの数を基準にしています。ライセンス数はプロバイダークラウドのタイプに基づいています。

Amazon Web Services および Microsoft Azure では、仮想マシンごとに 2 つ以上のライセンスがチェックアウトされます。 たとえば、ライセンス数が 10 の場合は、プロバイダー クラウドで 5 台の VM をプロビジョニングできます。

Cisco Intercloud Services – V では、仮想マシンごとに 1 つ以上のライセンスがチェックアウトされます。 たとえば、ライセンス数が 10 の場合は、プロバイダー クラウドで 10 台の VM をプロビジョニングできます。

Cisco Intercloud Fabric には、評価ライセンスと永続ライセンスの 2 種類のライセンスがあります。

### 評価ライセンス

永続ライセンスを購入する前に、評価ライセンスを使用して Cisco Intercloud Fabric ソフトウェアを試すことができます。 Cisco Intercloud Fabric には評価ライセンスが組み込まれています。このライセンスは 60 日間有効で、20 のハイブリッド クラウド ユニット（HCU）に対応します。 評価期間は、ソフトウェアをインストールした時点から始まり、ライセンス ファイルが有効期限に達すると終了します。

### 永続ライセンス

プロバイダー クラウドでプロビジョニングする必要がある仮想マシンの数に基づいて、永続ライセンスを購入できます。 永続ライセンスには有効期限があり、購入したライセンスの数はライセンス ファイルによって示されます。

Cisco Intercloud Fabric の発注については、『*Cisco Intercloud Fabric for Business Data Sheet*』を参照してください。

# ライセンスの要件

Cisco Intercloud Fabric の永続ライセンスには次のライセンス要件があります。

Cisco Intercloud Fabric を使用するには、次の手順に従ってライセンスを取得する必要があります。

1. Cisco Intercloud Fabric をインストールする前に、Cisco Intercloud Fabric ライセンス キーを生成し、証明書（製品アクセス キー）を要求します。
2. シスコのソフトウェア ライセンス サイトに製品アクセス キー（PAK）を登録します（製品アクセス キーの契約履行, （16 ページ） を参照してください）。
3. Intercloud Fabric のインストール後、Intercloud Fabric のライセンスのインストール, （20 ページ） の説明に従って Intercloud Fabric のライセンスを更新します。
4. ライセンスの検証が完了すると、Intercloud Fabric の使用を開始できます。

# 製品アクセス キーの契約履行

### はじめる前に

PAK 番号が必要です。

### 手順

**ステップ 1** シスコ ソフトウェア ライセンスの Web サイトに移動します。

**ステップ 2** [Product License Registration] ページに転送されたら、トレーニングを受けるか、[Continue to Product License Registration] をクリックして続行してください。

**ステップ 3** [Product License Registration] ページで、[Get New Licenses from a PAK or Token] をクリックします。

**ステップ 4** [Enter a Single PAK or TOKEN to Fulfill] フィールドに PAK 番号を入力します。

**ステップ 5** [Fulfill Single PAK/TOKEN] をクリックします。

**ステップ 6** PAK を登録するために、[License Information] でその他のフィールドに情報を入力します。

| 名前 | 説明 |
|---|---|
| 組織名 | 組織名。 |
| Site Contact Name | サイトの連絡先の名前。 |
| Street Address | 組織の番地。 |
| City/Town | 市区町村名。 |
| 州/県 | 州/都道府県。 |
| Zip/Postal Code | 郵便番号。 |
| Country | 国名。 |

**ステップ 7** [Issue Key] をクリックします。
ライセンス契約した機能が表示され、デジタル ライセンス契約書と zip 圧縮のライセンス ファイルが電子メールに添付されて、ユーザ指定の電子メール アドレスに送信されます。

# VMware 環境への Intercloud Fabric のインストール ワークフロー

VMware 環境への Intercloud Fabric 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** OVA を使用して、VMware 環境に Intercloud Fabric をインストールする。

VMware 環境への Intercloud Fabric のインストール, （18 ページ）を参照してください。

**ステップ 2** （任意） Intercloud Fabric のライセンスをインストールする。
Intercloud Fabric のライセンスのインストール, （20 ページ）を参照してください。

**ステップ 3** Intercloud Fabric のインフラストラクチャ コンポーネントをインストールする。
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, （21 ページ）を参照してください。

**ステップ 4** Intercloud Fabric Cloud を作成し、サービスを有効化する。
Intercloud Fabric Cloud の作成, （49 ページ）を参照してください。

# VMware 環境への Intercloud Fabric のインストール

OVA を使用して VMware 環境に Intercloud Fabric をインストールするには、次の手順を実行します。

## はじめる前に

- VMware vSphere または vCenter に接続するには、管理者権限が必要です。
- Intercloud Fabric の OVA イメージに VMware vSphere クライアントからアクセスできることを確認します。
- ICF、ICFD、PNSC のホスト名および静的 IP アドレスについて情報を入手しておきます。
- VMware vSphere Client を使用して vCenter に接続していることを確認します。ESX ホスト上に直接 OVA を展開しないでください。 ESX ホスト上に直接 OVA を展開しようとすると、次のエラー メッセージが表示されます：「`This OVF package uses features that are not supported when deploying directly to an ESX host`」。
- VMware HA が有効であることを確認します。 VMware vSphere のドキュメントを参照してください。
- ホストの仮想マシンのネットワークに対して無差別モードが有効になっていることを確認します。

## 手順

**ステップ 1** VMware vSphere（または vCenter）Client のログイン ダイアログボックスに、ログイン クレデンシャルを入力します。
**ステップ 2** [Login] をクリックします。
**ステップ 3** [Navigation] ペインで、Intercloud Fabric Director を導入する [Data Center] を選択します。
**ステップ 4** [File] > [Deploy OVF Template] を選択します。

[Deploy OVF Template] ウィンドウが表示されます。

**ステップ 5** [Source] ペインで、場所を参照してファイルを選択し、[Open] をクリックして OVF ソースの場所を選択します。

**ステップ 6** [OVF Template Details] ペインで、詳細情報を確認して [Next] をクリックします。

**ステップ 7** [End User License Agreement] ペインで、ライセンス契約を閲覧して [Accept] をクリックします。

**ステップ 8** [Name and Location] ペインで、次を実行します。

a) （任意） [Name] フィールドで VM 名を編集します。

b) Intercloud Fabric Director を導入する [Data Center] を選択して、[Next] をクリックします。

**ステップ 9** [Storage] ペインで、仮想マシン ファイルを保存する場所を選択します。

**ステップ 10** [Host/Cluster] ペインで必要なホスト、クラスタ、またはリソース プールを選択して、[Next] をクリックします。

**ステップ 11** [Disk Format] ペインで、データストアと使用可能領域を入力します。

**ステップ 12** [Disk Format] ペインで、次のいずれかのオプション ボタンをクリックして、[Next] をクリックします。

- [Thin Provisioned format]：データをディスクに書き込むときに、必要に応じてストレージを割り当てます。
- [Thick Provisioned (Lazy Zeroed)] 形式：シック形式で即座にストレージを割り当てます。 [Thick Provisioned (Lazy Zeroed)] 形式を使用することをお勧めします。
- [Thick Provisioned (Eager Zeroed)] 形式：シック形式でストレージを割り当てます。 このオプションを使用してディスクを作成する場合、時間がかかることがあります。

**ステップ 13** [Network Mapping] ペインで、該当するネットワークを選択して [Next] をクリックします。

**ステップ 14** [Properties] ペインで、次の情報を入力し、[Next] をクリックします。

- ICF ホスト名
- ICFD ホスト名
- ICF、ICFD PNSC の管理者/ルート パスワード
- ICF ホストの静的 IP アドレス
- ICFD ホストの静的 IP アドレス
- PNSC ホストの静的 IP アドレス
- ICF、ICFD、PNSC の IP サブネット マスク
- ICF、ICFD、PNSC の IP ゲートウェイ
- ICF、ICFD、PNSC のドメイン名
- ICF、ICFD、PNSC の DNS サーバの IP アドレス
- Syslog サーバの IP アドレス（オプション）

- ICF、ICFD、PNSC の NTP サーバの IP
- Time Zone

（注） NTP サーバの IP および Syslog サーバの IP に対して指定した値は、デフォルトのデバイス プロファイルに使用されます。

**ステップ 15** [Ready to Complete] ペインで、選択したオプションを確認して、[Finish] をクリックします。

**ステップ 16** VM で性能を発揮できるだけの十分な vCPU とメモリがあることを確認します。

**ステップ 17** VM の電源を入れます。

**ステップ 18** アプライアンスが起動したら、表示された Intercloud Fabric Director の IP アドレスをコピーして、サポートされている Web ブラウザに貼り付け、[Login] ページにアクセスします。
Intercloud Fabric の UI に接続できるまでに、最大 30 分かかる場合があります。

**ステップ 19** [Login] ページで、ステップ 14 で入力した ICF、ICFD、PNSC の管理者/ルート/shelladmin パスワードを入力して、ログインします。

# Intercloud Fabric のライセンスのインストール

Cisco Intercloud Fabric には評価ライセンスが組み込まれています。このライセンスは 60 日間有効で、20 のハイブリッド クラウド ユニット（HCU）に対応します。 評価期間の終了後は、永続ライセンスをインストールできます。 Intercloud Fabric の永続ライセンスをインストールするには、Intercloud Fabric の基本ライセンス ファイルをアップロードする必要があります。 ライセンスのカウントはクラウド プロバイダーによって異なり、仮想マシンのプロビジョニング時や移行時に適用されます。

## はじめる前に

- ライセンス ファイルを圧縮ファイルで受け取った場合は、展開して .lic ファイルをローカル マシンに保存します。
- シスコのソフトウェア ライセンス サイトで製品アクセス キー（PAK）を登録します。

## 手順

**ステップ 1** Intercloud Fabric にログインします。

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

**ステップ 3** （任意） Intercloud Fabric の評価ライセンスの詳細を表示するには、[License Keys] タブをクリックします。
Intercloud Fabric 評価ライセンス ファイルが表示されます。

**ステップ 4** （任意） Intercloud Fabric 評価ライセンス ファイルをクリックすると、有効期限やライセンス数などの詳細が表示されます。

**ステップ 5** Intercloud Fabric の永続ライセンスをインストールするには、[Update License] をクリックします。

**ステップ 6** [Update License] ダイアログボックスで、次のいずれかの操作を実行します。

- Intercloud Fabric の基本ライセンス ファイルをアップロードするには、[Browse] をクリックします。 移動して、Intercloud Fabric の基本ライセンス（CUIC-BASE-XX）を選択し、[Upload] をクリックします。
- ライセンス キーの場合は、[Enter License Text] チェックボックスを選択し、ライセンス キーのみをコピーして [License Text] フィールドに貼り付けます。 ライセンス キーは通常、ファイルの先頭の `Key ->` の後にあります。

ライセンス ファイルのフル テキストをコピーして [License Text] フィールドに貼り付けることもできます。

**ステップ 7** [Submit] をクリックします。
ライセンス ファイルが処理されて、更新の成功を確認するメッセージが表示されます。

**ステップ 8** Intercloud Fabric の永続ライセンスの詳細を表示するには、[License Keys] タブをクリックします。
Intercloud Fabric 永続ライセンス ファイルが表示されます。

**ステップ 9** Intercloud Fabric 永続ライセンス ファイルをクリックすると、有効期限やライセンス数などの詳細が表示されます。

**ステップ 10** [License Utilization] レポートを表示するには、[License Utilization] タブをクリックします。
レポートには、ライセンスの制限、使用可能なライセンスと使用中のライセンス、ライセンスのステータスなど、Intercloud Fabric ライセンスに関する詳細が含まれています。

# 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

[Infrastructure Setup] ウィザードを使用して、Intercloud Fabric インフラストラクチャ コンポーネント（Intercloud Fabric VSM など）をインストールするには、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、[Setup] ボタンをクリックします。
[Infrastructure Setup] ウィザードが表示されます。

**ステップ 4** [Networking and Placement] の次のフィールドに値を入力します。

| 名前 | 説明 |
|---|---|
| **[Networking and Placement]** | |
| [VM Manager] ドロップダウン リスト | 既存の VM マネージャを選択するか、新しい VM マネージャを追加します。<br>新しい VM マネージャの追加を選択した場合は、[VM Manager Type] から [Server Access URL] までのフィールドが表示されます。 |
| [VM Manager Type] ドロップダウン リスト | 追加する VM マネージャの ハイパーバイザ タイプを選択します。 |
| [VM Manager Name] フィールド | 追加する VM マネージャの名前。 |
| [Server Address] フィールド | 追加する VM マネージャのサーバ アドレス。 |
| [サーバのユーザID] フィールド | 追加する VM マネージャのサーバ ユーザ名。 |
| [サーバのパスワード] フィールド | 追加する VM マネージャのサーバ パスワード。 |
| [サーバアクセスポート] フィールド | 追加する VM マネージャのサーバ アクセス ポート番号。<br>HTTPS にデフォルト ポート 443 を使用します。VM マネージャの HTTP ポートにポート 80 を使用します。 |
| [サーバアクセスURL] フィールド | サーバ アクセス用の VM マネージャの URL。 |
| [VLAN] フィールド | Intercloud Fabric VSM の管理ネットワークに使用する VLAN。 |
| [IP Pool] ドロップダウン リスト | 既存の IP プールのポリシーを選択するか、新しい IP プール ポリシーを作成することを選択します。<br>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, （90 ページ） を参照してください。 |

| 名前 | 説明 |
|---|---|
| [Auto Assign Domain ID] チェックボックス | デフォルトでは、Intercloud Fabric VSM はドメイン ID 501 に設定されます。 ドメイン ID にデフォルト値を設定するには、このチェックボックスをオンにします。 1 ～ 1023 の間のドメイン ID を設定するには、このチェックボックスをオフにします。<br>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。 |
| [IcfVSM Domain ID] フィールド | Intercloud Fabric VSM のドメイン ID を入力します。 ドメイン ID は 1 ～ 1023 の間でなければなりません。<br>（注） ドメイン ID がネットワーク内で一意であることを確認してください。<br>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。 |
| **[ICF VSM Placement Details]** | |
| [Data-center] ドロップダウン リスト | 仮想マシンのデータセンターを選択します。<br>Intercloud Fabric VSM をプライマリおよびセカンダリとして配置するには、[High Availability] チェックボックスをオンにします。<br>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 Network] ドロップダウン リスト | 仮想マシンの管理ネットワークを選択します。<br>VLAN は、上記の [VLAN] フィールドに入力した VLAN と同じにする必要があります。 |
| [Host] ドロップダウン リスト | 仮想マシンのホストを選択します。 プライマリ ホストは PNSC と Intercloud Fabric VSM をホストます。<br>[High Availability] チェックボックスをオンにした場合は、プライマリおよびセカンダリ Intercloud Fabric VSM のホストを選択します。 |

| 名前 | 説明 |
|---|---|
| [Datastore] ドロップダウン リスト | VM のデータストアを選択します。使用可能なデータストアは名前でソートされます。<br>ストレージは、ローカルか、NFS や SAN などの共有リモートにできます。<br>[High Availability] チェックボックスをオンにした場合は、プライマリおよびセカンダリ Intercloud Fabric VSM のデータストアを選択します。 |

**ステップ 5** [Next] をクリックします。
インストールされている仮想マシンのサマリーが [Summary] ウィンドウに一覧表示されます。

**ステップ 6** [Submit] をクリックします。

**ステップ 7** タスクの状態を表示するには、[Infrastructure] 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 8** [Organizations] > [Service Requests] の順に選択します。

**ステップ 9** [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 10** [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。

# OpenStack 環境への Intercloud Fabric のインストール ワークフロー

OpenStack 環境への Intercloud Fabric 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** VM イメージ用に OpenStack に環境を準備する。
OpenStack での Intercloud Fabric 環境の準備, （25 ページ）を参照してください。

**ステップ 2** OpenStack ダッシュボードと CLI を使用して、テナント（プロジェクト）と仮想ネットワークを作成する。
テナントと仮想ネットワークの作成, （25 ページ）を参照してください。

**ステップ 3** QCOW2 イメージを使用して、OpenStack 環境に Intercloud Fabric をインストールする。
OpenStack 環境への Intercloud Fabric のインストール, （27 ページ）を参照してください。

**ステップ 4** （任意） Intercloud Fabric のライセンスをインストールする。
Intercloud Fabric のライセンスのインストール, （20 ページ）を参照してください。

**ステップ 5** Intercloud Fabric のインフラストラクチャ コンポーネントをインストールする。
OpenStack 環境への Intercloud Fabric インフラストラクチャ コンポーネントのインストール, （29 ページ）を参照してください。

**ステップ 6** Intercloud Fabric Cloud を作成し、サービスを有効化する。
Intercloud Fabric Cloud の作成, （49 ページ）を参照してください。

# OpenStack での Intercloud Fabric 環境の準備

OpenStack 環境に Intercloud Fabric をインストールするには、事前に OpenStack に VM イメージを作成しておく必要があります。

### 手順

**ステップ 1** 次の手順で、Intercloud Fabric**create VM image** スクリプト（`icf-create-vmimage-2.2.1.tar.gz`）用の環境を準備します。

a) Cisco Intercloud Fabric for Business 用の `ICFB-kvm-dk9-2.2.1-pkg.zip` ファイルをダウンロードします。 詳細については、シスコのセールス担当者にお問い合わせください。
b) ダウンロードした zip ファイルの内容を抽出します。
c) 抽出した `icf-create-vmimage-2.2.1.tar.gz` ファイルを OpenStack コントローラ ノードにコピーします。
d) コントローラ ノードにログインします。
e) 適切な名前のディレクトリを作成します（例：`icf-create-vmimage-workspace`）。
f) 次のコマンドを入力して、コントローラ ノードの `icf-create-vmimage-2.2.1.tar.gz` ファイルを、作成したディレクトリに解凍します。

```
tar -xvzf icf-create-vmimage-2.2.1.tar.gz -C target-directory
```

*target-directory* は、作成したディレクトリの名前です。

**ステップ 2** ターゲット ディレクトリに配置されている README.txt ファイルを検索します。
**ステップ 3** README.txt ファイルの手順に従って、VM イメージを作成します。

# テナントと仮想ネットワークの作成

OpenStack CLI またはダッシュボードを使用してテナントや仮想ネットワークを作成するには、次の手順を実行します。

### 手順

**ステップ 1** 管理テナントを作成して、管理テナント メンバー リストに管理ユーザを追加します。
管理テナントとは、Intercloud Fabric 仮想マシン、Intercloud Fabric Extender、および Intercloud Fabric VSM を含んでいる一種のプロジェクトと見なすことができます。

（注） 既存の管理者テナントや管理者プロジェクトを管理テナントとして使用できます。

詳細については、『*Cisco Nexus 1000V for KVM Virtual Network Configuration Guide*』を参照してください。

**ステップ 2** OpenStack ダッシュボードを使用してネットワーク プロファイルを作成します。

a) trunk タイプを使用して、Intercloud Fabric Extender データ トランクのネットワーク プロファイルを作成します。
b) VLAN タイプを使用して、管理ネットワークとトンネル ネットワーク のネットワーク プロファイルを作成します。

詳細については、『*Cisco Nexus 1000V for KVM Virtual Network Configuration Guide*』を参照してください。

**ステップ 3** Cisco Nexus 1000V KVM VSM CLI を使用して、デフォルトのポリシー プロファイル *default-pp* を作成します。
詳細については、『*Cisco Nexus 1000V for KVM Port Profile Configuration Guide*』を参照してください。

（注） デフォルトのポリシー プロファイル *default-pp* の名前は、`/etc/neutron/plugins/cisco/cisco_plugins.ini` で設定されます。*cisco_plugin.ini* ファイル内の名前が変更された場合は、それと同じ名前でデフォルトのポリシー プロファイルを作成する必要があります。

**例**：

```
# configure terminal
port-profile type vethernet default-pp
no shutdown
state enabled
publish port-profile
```

**ステップ 4** penStack ダッシュボードを使用して、管理テナントに管理ネットワークを作成し、それをステップ 2 で作成したネットワーク プロファイルに関連付けます。 また、管理ネットワークが外部接続していることを確認します。
詳細については、『*Cisco Nexus 1000V for KVM Virtual Network Configuration Guide*』を参照してください。

**ステップ 5** OpenStack ダッシュボードを使用して、管理テナントに Intercloud Fabric Cloud エンタープライズ データ トランクのネットワークを作成し、それをステップ 2 で作成したネットワーク プロファイルに関連付けます。
エンタープライズ トランク ネットワークには、ポートの作成を調整するサブネットワーク範囲が必要です。

**ステップ 6** 次の手順で、トンネル インターフェイスのネットワークを設定します。

- OpenStack ダッシュボードを使用して、Intercloud Fabric Extender トンネル インターフェイス用のネットワークを作成し、そのネットワークに特定の名前 *icfTunnelNet* を付けます。 このネットワークは、管理ネットワークの代わりにトンネル ネットワークを備えた Intercloud Fabric Extender を展開する場合にのみ必要です。
- OpenStack ダッシュボードを使用して、Intercloud Fabric Extender トンネル インターフェイス用の個別のネットワークを作成します。 トンネル ネットワークが外部接続していることを確認します。 このネットワークは、Intercloud Fabric Extender 専用のトンネル インターフェイスが必要な場合にのみ必要です。

詳細については、『Cisco Nexus 1000V for KVM Virtual Network Configuration Guide』を参照してください。

# OpenStack 環境への Intercloud Fabric のインストール

OpenStack 環境に Intercloud Fabric をインストールするには、次の手順を実行します。

## はじめる前に

- Intercloud Fabric のイメージをダウンロード済みであることを確認します。 詳細については、シスコのセールス担当者にお問い合わせください。
- Intercloud Fabric は、管理ネットワーク上の管理テナントまたはプロジェクトにインストールする必要があります。
- Intercloud Fabric のインストールは、Red Hat Enterprise Linux OpenStack Platform および OpenStack Icehouse リリースでのみサポートされます。

## 手順

**ステップ 1** Cisco.com の次の場所から Intercloud Fabric のイメージをダウンロードします。
Cisco.com

**ステップ 2** ダウンロードしたイメージを OpenStack コントローラ ノードにコピーします。

**ステップ 3** OpenStack ダッシュボードにログインします。

**ステップ 4** OpenStack RC ファイルをダウンロードするためのプロジェクトを選択し、[Access & Security] > [Download OpenStack RC File] の順に選択します。

**ステップ 5** コントローラ ノードに OpenStack RC ファイルをコピーします。

```
source openrc.sh
```

**ステップ 6** OpenStack CLI を使用して Intercloud Fabric の VM イメージをアップロードします。

（注）　イタリック体のパラメータの値は必ず入力してください。

```
glance image-create --file image-name.qcow2
--name image-name --disk-format qcow2 --min-disk 340
--min-ram 20480 --container-format bare
```

**ステップ 7**　テキスト エディタを使用して、コントローラ モードでovf-env.xml ファイルを作成します。

（注）　イタリック体のパラメータの値は必ず入力してください。

**例**：

```
<?xml version="1.0" encoding="UTF-8"?>
<Environment
     xmlns="http://schemas.dmtf.org/ovf/environment/1"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xmlns:oe="http://schemas.dmtf.org/ovf/environment/1"
     xmlns:ve="http://www.vmware.com/schema/ovfenv"
     oe:id="">
  <PlatformSection>
      <Kind>KVM</Kind>
      <Version>6.1.0</Version>
      <Vendor>RedHat, Inc.</Vendor>
      <Locale>en</Locale>
   </PlatformSection>

   <PropertySection>
        <Property oe:key="DNSIp" oe:value="DNS-IPv4-address"/>
        <Property oe:key="DomainName" oe:value="domainname.com"/>
        <Property oe:key="GatewayIpV4" oe:value="Gateway-IPv4-address"/>
        <Property oe:key="HARole" oe:value="HA-role"/>
        <Property oe:key="HostName" oe:value="VM-name"/>
        <Property oe:key="ICFDHostname" oe:value="ICF-hostname"/>
        <Property oe:key="ICFDManagementIpV4" oe:value="ICFD-mgmt-IPv4-address"/>
        <Property oe:key="ManagementIpV4" oe:value="Mgmt-IPv4-address"/>
        <Property oe:key="ManagementIpV4Subnet" oe:value="subnet-mask-IPv4"/>
        <Property oe:key="NTPIpStr" oe:value="NTP-server-IPv4-address"/>
        <Property oe:key="OvfDeployment" oe:value="ovf"/>
        <Property oe:key="PNSCHostname" oe:value="PNSC-hostname"/>
        <Property oe:key="PNSCManagementIpV4" oe:value="PNSC-mgmt-IPv4-address"/>
        <Property oe:key="PNSCSharedSecret" oe:value="PNSC-shared-secret-password"/>
        <Property oe:key="PNSCSvcRegIpV4" oe:value="PNSC-service-reg-IPv4-address"/>
        <Property oe:key="Password" oe:value="PNSC-password"/>
        <Property oe:key="SyslogIpStr" oe:value="syslog-IPv4-address"/>
        <Property oe:key="TimeZoneStr" oe:value="timezone"/>
  </PropertySection>
</Environment>
```

**ステップ 8**　OpenStack CLI を使用して、VM のネットワーク ID を確認します。

```
neutron net-list
```

**ステップ 9**　OpenStack CLI を使用して、VM のサブネット ID を確認します。

```
neutron subnet-list
```

**ステップ 10**　OpenStack CLI を使用して、ポートを作成し、vNIC の 1 つの VM（PNSC-ICFD）に 3 つの IP アドレスを割り当てます。 サブネット ID はすべての IP アドレスに対して同一です。

（注）　イタリック体のパラメータの値は必ず入力してください。

```
neutron port-create --fixed-ip subnet_id=subnet ID,
ip_address= IP Address
--fixed-ip subnet_id= subnet ID,
ip_address= IP Address
--fixed-ip subnet_id= subnet ID,
```

```
ip_address= IP Address
Vlan network name
```

**ステップ 11** 次の属性を使って、1 つの VM のフレーバを作成します。

- vCPU：8
- RAM：20480 MB
- ルート ディスク：350 GB
- 一時的ディスク：0
- スワップ ディスク：0

```
nova flavor-create flavor-name flavor-id 20480 350 8
```

**ステップ 12** Intercloud Fabric VM を起動します。

（注） イタリック体のパラメータの値は必ず入力してください。

```
nova boot --flavor= flavor-ID
--image= image-ID
--config-drive=true
--file ovf-env.xml=ovf-env.xml
--nic port-id= port-ID
ICF-VM
```

**ステップ 13** 通常、インストール プロセスには 30 分かかります。
Horizon UI の 1 つの VM コンソールにアクセスすると、インストールを確認できます。

# OpenStack 環境への Intercloud Fabric インフラストラクチャ コンポーネントのインストール

[Infrastructure Setup] ウィザードを使用して、OpenStack 環境に Intercloud Fabric インフラストラクチャ コンポーネントをインストールするには、次の手順を実行します。

## はじめる前に

- Intercloud Fabric をインストールしておきます。
- Intercloud Fabric Cloud に必要なネットワークとサブネットをすべて作成しておきます。

### 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、[Setup] ボタンをクリックします。
[Infrastructure Setup] ウィザードが表示されます。

**ステップ 4** [Networking and Placement] の次のフィールドに値を入力します。

| 名前 | 説明 |
|---|---|
| **VM Manager 資格情報** | |
| [VM Manager] ドロップダウン リスト | 既存の VM マネージャを選択するか、新しい VM マネージャを作成することを選択します。<br>[Register New VM Manager] を選択した場合にのみ、このテーブルに [VM Manager Type] から [Secure] までのフィールドが表示されます。 |
| [VM Manager Type] ドロップダウン リスト | OpenStack を選択します。 |
| [VM Manager Name] フィールド | VM マネージャ名を入力します。 |
| [Server Address] フィールド | 基本サービスを実行しているコントローラの IP アドレス。 |
| [サーバのユーザID] フィールド | 作成する VM マネージャの管理ユーザ名。 |
| [サーバのパスワード] フィールド | 作成する VM マネージャの管理者パスワード。 |
| [サーバアクセスポート] フィールド | 作成する VM マネージャの基本サービス アクセス ポート番号。 |
| [Description] フィールド | VM マネージャの説明。 |
| [Contact] フィールド | VM マネージャの連絡先情報。 |
| [Location] フィールド | VM マネージャの場所。 |
| [Secure] チェックボックス | HTTPS または SSL 用に OpenStack を設定した場合は、このチェックボックスを選択してセキュア接続を確立します。<br>HTTPS または SSL 用に OpenStack を設定していない場合は、このチェックボックスをオフにします。 |

| 名前 | 説明 |
|---|---|
| **ネットワーキング** | |
| [IP Pool] ドロップダウン リスト | 既存の IP プールのポリシーを選択するか、新しい IP プール ポリシーを作成することを選択します。<br>（注） IP プール範囲が OpenStack のサブネット範囲と一致することを確認してください。<br>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，（90 ページ） を参照してください。 |
| [Auto Assign Domain ID] チェックボックス | デフォルトでは、Intercloud Fabric VSM はドメイン ID 501 に設定されます。 ドメイン ID にデフォルト値を設定するには、このチェックボックスをオンにします。 1 ～ 1023 の間のドメイン ID を設定するには、このチェックボックスをオフにします。<br>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。 |
| [Domain ID] フィールド | Intercloud Fabric VSM のドメイン ID を入力します。 ドメイン ID は 1 ～ 1023 の間でなければなりません。<br>（注） ドメイン ID がネットワーク内で一意であることを確認してください。<br>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。 |
| **[ICF VSM Placement Details]** | |

| 名前 | 説明 |
|---|---|
| [High Availability] ドロップダウン リスト | 仮想マシンのデータセンターを選択します。<br>Intercloud Fabric VSM をプライマリおよびセカンダリとして配置するには、[High Availability] チェックボックスをオンにします。<br>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。<br>少なくとも 2 つのノードをハイ アベイラビリティに設定する必要があります。 |
| [Project] ドロップダウン リスト | 仮想マシンのプロジェクトまたはテナントを選択します。 |
| [Management Network] ドロップダウン リスト | 仮想マシンの管理ネットワークを選択します。 |

**ステップ 5** [Next] をクリックします。
インストールされている仮想マシンのサマリーが [Summary] ウィンドウに一覧表示されます。

**ステップ 6** [Submit] をクリックします。

**ステップ 7** タスクの状態を表示するには、[Infrastructure] 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 8** [Organizations] > [Service Requests] の順に選択します。

**ステップ 9** [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 10** [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。

# Microsoft 環境への Intercloud Fabric のインストール ワークフロー

Microsoft 環境に Cisco Intercloud Fabric for Business をインストールするには、次のワークフローのタスクを実行します。

### 手順

**ステップ 1** インストールの準備をする。

インストールの準備, （33 ページ） を参照してください。

**ステップ 2** Intercloud Fabric 仮想アプライアンスをインスタンス化して設定する。
Intercloud Fabric のインストールと設定, （35 ページ） を参照してください。

**ステップ 3** Intercloud Fabric VSM 仮想マシンをインスタンス化して設定する。
Intercloud Fabric VSM のインスタンス化と設定, （39 ページ） を参照してください。

**ステップ 4** Intercloud Fabric Extender 仮想マシンをインスタンス化して設定する。
Intercloud Fabric Extender の展開と設定, （43 ページ） を参照してください。

**ステップ 5** Intercloud Fabric のライセンスをインストールする。
Intercloud Fabric のライセンスのインストール, （20 ページ） を参照してください。

**ステップ 6** Intercloud Fabric のインフラストラクチャ コンポーネントをインストールする。
Microsoft 環境への Intercloud Fabric インフラストラクチャ コンポーネントのインストール, （46 ページ） を参照してください。

**ステップ 7** Intercloud Fabric Cloud リンクを作成し、サービスを有効化する。
Intercloud Fabric Cloud の作成, （49 ページ） を参照してください。

# インストールの準備

環境に Cisco Intercloud Fabric をインストールする前に、次の項での説明に従って、要件を満たしていることを確認し、注意事項と制約事項を理解しておいてください。

- システム要件, （10 ページ）
- 前提条件, （12 ページ）
- 注意事項と制約事項, （15 ページ）

また、ポート プロファイルと仮想スイッチも Cisco Intercloud Fabric 用に設定する必要があります。詳細については、Microsoft のドキュメントを参照してください。

Cisco Intercloud Fabric イメージ ファイルの内容および SCVMM へのコンポーネント テンプレートの登録方法については、次の項目を参照してください。

- Intercloud Fabric zip ファイルの内容, （33 ページ）
- Intercloud Fabric コンポーネント テンプレートの登録, （35 ページ）

## Intercloud Fabric zip ファイルの内容

Microsoft 環境用の Cisco Intercloud Fabric for Business ソフトウェア パッケージは ZIP ファイルに圧縮されており、次の表に示す内容が含まれています。

| 項目 | ファイル | 説明 |
|---|---|---|
| **SCVMM Templates フォルダ** | | |
| *Cisco-ICF-ApplianceTemplate* フォルダ | | |
| Cisco-ICF-Appliance フォルダ | • Cisco-ICF-Appliance-Template.xml<br>• icf-2.2.1.vhd | • SCVMM OVF またはテンプレート ファイル<br>• VHD ファイル |
| Register-ICF-ApplianceTemplate.ps1 | | Intercloud Fabric アプライアンス テンプレートを SCVMM に登録するためのスクリプト |
| *Cisco-ICF-CloudVSMTemplate* フォルダ | | |
| Cisco-ICF-Cloud-VSM フォルダ | • Cisco-ICF-Cloud-VSM-Template.xml<br>• Cisco-ICF-Cloud-VSM.vhd<br>• n1000v-dk9.5.2.1.SK3.1.2.iso | • SCVMM OVF またはテンプレート ファイル<br>• ブランク VHD<br>• VSM ISO イメージ |
| Register-Cisco-ICF-Cloud-VSMTemplate.ps1 | | Intercloud Fabric Cloud VSM テンプレートを SCVMM に登録するためのスクリプト |
| *Cisco-ICF-ExtenderTemplate* フォルダ | | |
| Cisco-ICF-Extender フォルダ | • Cisco-ICF-Extender-Template.xml<br>• IChvm 2.2.1.vhd | • SCVMM OVF またはテンプレート ファイル<br>• VHD ファイル |
| Register-ICF-ExtenderTemplate.ps1 | | Cisco Intercloud Fabric Extender テンプレートを SCVMM に登録するためのスクリプト |
| 登録ファイル | | |
| Register-ICF-Templates.ps1 | | すべてのテンプレートを同時に SCVMM に登録するスクリプト |

| 項目 | ファイル | 説明 |
|---|---|---|
| **Services Bundle** | | |
| icfb-services-2.2.1.tar | | サービス バンドルには次のサービス用のファイルが含まれています。<br>• ICF Firewall（VSG）<br>• ICF Router（CSR） |

## Intercloud Fabric コンポーネント テンプレートの登録

SCVMM にコンポーネント テンプレートを登録するには、シスコが提供する PowerShell スクリプトを使用します。 次の手順で説明するように、テンプレートを個々に登録したり、すべてのテンプレートを同時に登録することができます。 テンプレートを登録すると、それらは SCVMM に表示されます。

### 手順

**ステップ 1** Cisco ポータルから SCVMM サーバに zip ファイルをダウンロードし、内容を抽出します。

**ステップ 2** SCVMM サーバで PowerShell ウィンドウを開きます。

**ステップ 3** すべてのテンプレートを同時に SCVMM に登録するには、スクリプト **.\SCVMM-Templates\Register-ICF-Templates.ps1** を実行します。

**ステップ 4** テンプレートを個々に SCVMM に登録するには、次の登録スクリプトを個別に実行します。

- Cisco-ICF-Appliance：**.\SCVMM-Templates\Cisco-ICF-ApplianceTemplate\ Register-ICF-ApplianceTemplate.ps1**
- Cisco-ICF-CloudVSM：**.\SCVMM-Templates\ Cisco-ICF-CloudVSMTemplate\ Register-Cisco-ICF-Cloud-VSMTemplate.ps1**
- Cisco-ICF-Extender：**.\SCVMM-Templates\Cisco-ICF-ExtenderTemplate\Register-ICF-ExtenderTemplate.ps1**

# Intercloud Fabric のインストールと設定

Intercloud Fabric は、Microsoft System Center Virtual Machine Manager（SCVMM）を使用して Intercloud Fabric をインストールして設定することにより、Microsoft Hyper-V Hypervisor 環境に展開されます。 詳細については、次のトピックを参照してください。

• VM テンプレートによる Intercloud Fabric のインスタンス化, （36 ページ）

• Intercloud Fabric 仮想マシンの設定, （37 ページ）

## VM テンプレートによる Intercloud Fabric のインスタンス化

VM テンプレートを使用して Intercloud Fabric VM をインスタンス化するには、次の手順を実行します。

### はじめる前に

- Microsoft System Center Virtual Machine Manager（SCVMM）に接続するには、管理者権限が必要です。
- Cisco Intercloud Fabric for Business（ICFB）Appliance イメージが SCVMM に登録されていることを確認します。

### 手順

**ステップ 1** SCVMM ユーザ インターフェイスにログインします。

**ステップ 2** 左側のナビゲーション ペインで [VMs and Services] をクリックし、メニュー バーで [Create Virtual Machine] を選択します。
[Create Virtual Machine Wizard] ウィンドウが表示されます。

**ステップ 3** [Select Source] パネルで、[Use an existing virtual machine, VM template, or virtual hard disk] を選択し、[Browse] オプションをクリックします。

**ステップ 4** [Type: VM Template] ヘッダーの下にあるリストから *Cisco-ICFB-Appliance-Template* ファイルを選択します。

**ステップ 5** [OK] をクリックし、次に [Next] をクリックします。

**ステップ 6** [Specify Virtual Machine Identity] パネルで、仮想マシンの名前を入力し、[Next] をクリックします。

**ステップ 7** [Configure Hardware] パネルで、仮想マシンのハードウェア設定を行います。
テンプレートを使用している場合は、大部分が設定済みです。 イメージのみ設定する必要があります。

**ステップ 8** [Select Destination] パネルで、[Place the virtual machine on a host; Destination: All Hosts] のデフォルト設定を保持し、[Next] をクリックします。

**ステップ 9** [Select Host] パネルで、ホストを選択し、[Next] をクリックします。

**ステップ 10** [Configure Settings] パネルで、設定を確認し、[Next] をクリックします。

**ステップ 11** [Select Networks] パネルで、仮想マシンの仮想スイッチを選択します。 各ネットワーク アダプタに対して、仮想スイッチのタイプ（[Standard Switch]、[Logical Switch] など）を選択し、[Next] をクリックします。

テンプレートには 1 つ NIC が表示されます。

**ステップ 12** MAC スプーフィングに対して NIC を有効化します（まだ有効化されていない場合）。

**ステップ 13** [Add Properties] パネルで、[Automatic Actions] のデフォルト設定を保持し、[Next] をクリックします。

**ステップ 14** [Summary] ウィンドウの [Confirm the Settings] パネルで、設定を確認します。

**ステップ 15** [Create] をクリックして、仮想マシンを作成します。
[Job Status] カラムには、現在のステータスを示す経過表示バーがあります。

**ステップ 16** 仮想マシンの作成が完了したら、SCVMM ユーザ インターフェイスの仮想マシンを右クリックし、[Power On] を選択します。

**ステップ 17** 仮想マシンを再び右クリックし、[Connect or View] > [Connect via Console] の順に選択します。

## Intercloud Fabric 仮想マシンの設定

Intercloud Fabric VM を設定するには、次の手順を実行します。

### はじめる前に

Intercloud Fabric VM がインスタンス化されており、コンソールからアクセスできること。

### 手順

**ステップ 1** コンソールを使用して SCVMM にログインし、Intercloud Fabric VM に接続します。

ログインすると、次の手順に示すとおりに設定情報を入力するよう SCVMM によって自動的に指示されます。

**ステップ 2** Intercloud Fabric のホスト名を入力します。

**ステップ 3** Intercloud Fabric Director のホスト名を入力します。

**ステップ 4** PNSC のホスト名を入力します。

**ステップ 5** Intercloud Fabric、Intercloud Fabric Director、および PNSC のパスワードを入力して確認します。

**ステップ 6** Intercloud Fabric のネットマスクを入力します。

**ステップ 7** Intercloud Fabric の IP アドレスを入力します。

**ステップ 8** Intercloud Fabric Director の IP アドレスを入力します。

**ステップ 9** PNSC の IP アドレスを入力します。

**ステップ 10** ゲートウェイの IP アドレスを入力します。

**ステップ 11** Intercloud Fabric、Intercloud Fabric Director、および PNSC のドメイン名を入力します。

**ステップ 12** DNS サーバの IP アドレスを入力します。

**ステップ 13** Intercloud Fabric、Intercloud Fabric Director、および PNSC の syslog サーバの IP アドレスを入力します。

**ステップ 14** Intercloud Fabric、Intercloud Fabric Director、および PNSC の NTP サーバの IP アドレスを入力します。

**ステップ 15** システムのタイム ゾーンを入力します。

**ステップ 16** （オプション）NFS サーバの IP アドレスを入力します。

**ステップ 17** （オプション）NFS サーバのマウント ポイントを入力します。
次のような出力が表示されます。

```
ICF IP             : 192.197.137.87
ICFD IP            : 192.197.137.89
PNSC IP            : 192.197.137.88
ICF hostname       : ICF-Appliance
ICFD hostname      : ICFD-Appliance
PNSC hostname      : PNSC
IPV4 netmask       : 255.255.255.224
IPV4 gateway       : 192.197.137.65
DNS IP             : 192.197.137208
Domain Name        : darknight.ourcompany.com
NTP server         : 192.104.222.16
Syslop IP          : 0.0.0.0
Timezone           : Asia/Calcutta
NFS Server         :
NFS mnt point      :

Is everything ok (y/n)
```

**ステップ 18** y を入力し、すべての設定を確定します。

# Intercloud Fabric VSM のインスタンス化と設定

Intercloud Fabric VSM は、SCVMM を使用して VM をインスタンス化し、その VM を設定することによって、Microsoft Hyper-V Hypervisor 環境に展開されます。 詳細については、次のトピックを参照してください。


- VM テンプレートによるIntercloud Fabric VSM VM のインスタンス化, （39 ページ）
- Intercloud Fabric VSM VM の設定, （40 ページ）


## VM テンプレートによるIntercloud Fabric VSM VM のインスタンス化

SCVMM を使用してIntercloud Fabric VSM VM をインスタンス化するには、次の手順を実行します。

### はじめる前に

Intercloud Fabric VSM イメージが SCVMM に登録されていることを確認します。

### 手順

**ステップ 1** SCVMM のユーザインターフェイスの左側のナビゲーション ペインで [VMs and Services] をクリックし、メニュー バーで [Create Virtual Machine] を選択します。

[Create Virtual Machine Wizard] が開きます。

**ステップ 2** [Select Source] パネルで、[Use an existing virtual machine, VM template, or virtual hard disk] を選択し、[Browse] をクリックします。

**ステップ 3** [Type: VM Template] で、*Cisco-ICF-Cloud-VSM-Template* ファイルを選択します。

**ステップ 4** [OK] をクリックし、次に [Next] をクリックします。

**ステップ 5** [Specify Virtual Machine Identity] パネルで、仮想マシンの名前を入力し、[Next] をクリックします。

**ステップ 6** [Configure Hardware] パネルで、仮想マシンのハードウェア設定を行います。 テンプレートを使用している場合は、大部分が設定済みです。 ISO イメージのみ設定する必要があります。

**ステップ 7** [Bus Configuration] ヘッダーの下にある中央ペインで、[Virtual DVD drive] をクリックします。

**ステップ 8** [Existing ISO image file] をクリックし、[Browse] をクリックします。

**ステップ 9** SCVMM ライブラリから ISO イメージを選択して [OK] をクリックし、次に [Next] をクリックします。

**ステップ 10** [Select Destination] パネルで、[Place the virtual machine on a host; Destination: All Hosts] のデフォルト設定を保持し、[Next] をクリックします。

**ステップ 11** [Select Host] パネルで、ホストが表示されたらそれを選択し、[Next] をクリックします。

**ステップ 12** [Configure Settings] パネルで、設定を確認し、[Next] をクリックします。

**ステップ 13** [Select Networks] パネルで、仮想マシンの仮想スイッチを選択します。 各ネットワーク アダプタに対して、仮想スイッチのタイプ（[Standard Switch]、[Logical Switch] など）を選択し、[Next] をクリックします。

**ステップ 14** [Add Properties] パネルで、[Automatic Actions] のデフォルト設定を保持し、[Next] をクリックします。

**ステップ 15** [Summary] ウィンドウの [Confirm the Settings] パネルで、設定が正確であることを確認します。

**ステップ 16** [Create] をクリックして、仮想マシンを作成します。
[Job Status] カラムの経過表示バーに状態が表示されます。

**ステップ 17** 仮想マシンが作成されたら、仮想マシンを右クリックし、[Power On] を選択します。

**ステップ 18** 仮想マシンを再び右クリックし、[Connect or View] > [Connect via Console] の順に選択します。

## Intercloud Fabric VSM VM の設定

この手順では、Intercloud Fabric VSM を Intercloud Fabric で使用するための設定方法について説明します。

この手順には次の情報が適用されます。

- この手順で表示されるプロンプトにただちに応答しない場合は、デフォルトのアクションが実行されます。
- 冗長 VSM VM をインストールする場合は、プライマリ VSM でソフトウェアを設定してから、セカンダリ VSM にソフトウェアをインストールします。

### はじめる前に

- Intercloud Fabric VSM 仮想マシン（VM）がインスタンス化され、電源がオンになっていること。
- VM のコンソールを開いておくこと。

### 手順

**ステップ 1** コンソールを使用して SCVMM にログインし、Intercloud Fabric VSM VM に接続します。

**ステップ 2** [Virtual Machine Viewer] ウィンドウで、ディスクをフォーマットするかどうかを尋ねるプロンプトが表示されたら、Y（はい）を入力します。

**ステップ 3** （長時間がかかる可能性がある）ターゲットディスクの読み取り/書き込みテストを実行するかどうか尋ねられたら、Y を入力します。
ソフトウェアがコピーされて CD-ROM ドライブがマウントされると、システム管理者アカウントのセットアップを開始するように指示されます。

**ステップ 4** プロンプトが表示されたら、管理者アカウントのパスワードを入力して確認します。
次のように、ハイ アベイラビリティ（HA）の設定を求めるメッセージが表示されます。

```
Enter HA role [standalone/primary/secondary]
```

**ステップ 5** Intercloud Fabric VSM HA ペアを作成することをお勧めします。 1 番目の VSM をプライマリ VSM として設定し、2 番目の VSM をセカンダリ VSM として設定します。
HA ロールをセカンダリとして設定すると、次のプロンプトが表示されます。

```
Setting HA role to secondary will cause a system reboot. Are you sure (yes/no)?
```

HA ロールをセカンダリに設定するには、Yes と入力します。

**ステップ 6** プロンプトが表示されたら、ドメイン ID を入力します。 ドメイン ID は、HA ペアの VSM VM が相互通信をするために必要です。 セカンダリ VSM をインストールする際は、プライマリ VSM 用に指定したドメイン ID と同じドメイン ID を入力します。

**ステップ 7** 基本設定ダイアログを開始するかどうか尋ねられたら、Yes と入力します。

**ステップ 8** 別のログイン アカウントを作成するかどうか尋ねられたら、No と入力します。

**ステップ 9** 読み取り専用の SNMP コミュニティ ストリングを設定するかどうか尋ねられたら、No と入力します。

**ステップ 10** 読み書き可能な SNMP コミュニティ ストリングを設定するかどうか尋ねられたら、No と入力します。

**ステップ 11** プロンプトが表示されたら、スイッチの名前を入力します。

**ステップ 12** アウトオブバンド管理を設定するかどうか尋ねられたら、次の例のように、Yes と入力して、mgmt0 IPv4 アドレスとサブネット マスクを入力します。

```
Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]: yes
Mgmt0 IPv4 address: 192.28.15.152
Mgmt0 IPv4 netmask: 255.255.255.0
```

**ステップ 13** プロンプトが表示されたら、次の例のように、Yesと入力してデフォルト ゲートウェイを設定し、ゲートウェイの IP アドレスを入力します。

```
Configure the default-gateway: (yes/no) [y]: yes
IPv4 address of the default gateway: 192.23.233.1
Configure Advanced IP options (yes/no) [n]:
```

**ステップ 14** 高度な IP オプションを設定するかどうかを尋ねられたら、No と入力します。

**ステップ 15** Telnet サービスを有効にするかどうか尋ねられたら、Yes と入力します。

**ステップ 16** プロンプトが表示されたら、次の例のように、Yes と入力して SSH サービスを有効化し、キー タイプとキー ビット数を入力します。

```
Enable the ssh service? (yes/no) [y]: yes
Type of ssh key you would like to generate (dsa/rsa) : rsa
Number of  key bits <768-2048> : 1024
Enable OpenStack support? (yes/no) [y]
```

**ステップ 17** VSM で OpenStack のサポートを有効化するかどうかに応じて、Yes または No と入力します。次のような情報が表示されます。

```
OpenStack support enables the following features(s):
   feature http-server
   feature segmentation
   feature network-segmentation-manager

Configure NTP server? (yes/no) [n]
```

**ステップ 18** 次の例のように、Yes と入力して NTP サーバを設定し、NTP サーバの IP アドレスを入力します。

```
NTP server IPv4 address: 192.68.1.1

Vem feature level will be set to 5.2(1)SK3(1.1)
Do you want to reconfigure? (yes/no) [n]
```

**ステップ 19** 再設定するかどうかを尋ねられたら、No と入力します。
次のように、設定が要約され、それを編集するかどうか尋ねられます。

```
The following configuration will be applied:
 Switchname n1000v
interface Mgmt0
ip address 192.28.15.152 255.255.255.0
no shutdown
vrf context management
ip route 0.0.0.0/0 192.28.15.1
no telnet server enable
  ssh key rsa 1024 force
  ssh server enable
  feature http-server
  feature segmentation
  feature network-segmentation-manager
  ntp server 1.1.1.1
  svs-domain
    no control vlan
    no packet vlan
```

```
    svs mode L3 interface mgmt0
    domain id 5

If you do not want to edit the configuration enter no and continue with the next step.

If you want to edit the configuration, enter yes and return to Step 6 to revisit each
command.

Would you like to edit the configuration? (yes/no) [n]:
```

**ステップ 20** 設定を編集するかどうか尋ねられたら、No と入力します。
設定の保存について尋ねる次のようなメッセージが表示されます。

```
Use this configuration and save it? (yes/no) [y]:
```

**ステップ 21** Yes と入力して設定を保存します。

**注意** 設定を保存しないと、入力した内容が次回の VSM の起動時に設定に反映されません。Yesと入力して設定を保存し、キックスタートとシステムイメージも自動的に設定されていることを確認します。

次のような情報が表示されます。

```
[########################################] 100%
The new configuration is saved into nonvolatile storage.
```

**ステップ 22** VSM CLI にログインして次のコマンドを入力し、Intercloud Fabric のインストールと設定, （35 ページ） でインストールして設定した PNSC 仮想マシンに VSM を登録します。

```
SWITCH# conf t
SWITCH(config)# nsc-policy-agent
SWITCH(config-nsc-policy-agent)# registration-ip 192.197.137.88
SWITCH(config-nsc-policy-agent)# shared-secret PNSC-shared-secret-password
SWITCH(config-nsc-policy-agent)# policy-agent-image bootflash:vsmcpa.3.0.2.1.bin
SWITCH(config-nsc-policy-agent)# exit
SWITCH(config)# show nsc-pa status
NSC Policy-Agent status is - Installed Successfully. Version 3.2(2b)-vsm
```

**ステップ 23**

**ステップ 24**

**ステップ 25**

# Intercloud Fabric Extender の展開と設定

Intercloud Fabric Extender は、SCVMM を使用して Intercloud Fabric Extender をインストールして設定することにより、Microsoft Hyper-V ハイパーバイザ環境に展開されます。 詳細については、次のトピックを参照してください。

- VM テンプレートによるIntercloud Fabric Extender VM のインスタンス化, （44 ページ）
- Intercloud Fabric Extender の設定, （45 ページ）

# VM テンプレートによるIntercloud Fabric Extender VM のインスタンス化

SCVMM を使用して Microsoft Hyper-V ハイパーバイザ環境内の Intercloud Fabric Extender VM をインスタンス化するには、次の手順を実行します。

## はじめる前に

Intercloud Fabric Extender イメージが SCVMM に登録されていることを確認します。

## 手順

**ステップ 1** SCVMM のユーザ インターフェイスの左側のナビゲーション ペインで [VMs and Services] をクリックし、メニュー バーで [Create Virtual Machine] を選択します。
[Create Virtual Machine Wizard] が開きます。

**ステップ 2** [Select Source] パネルで、[Use an existing virtual machine, VM template, or virtual hard disk] を選択し、[Browse] をクリックします。

**ステップ 3** [Type: VM Template] で、*Cisco-ICF-Extender-Template* ファイルを選択します。

**ステップ 4** [OK] をクリックし、次に [Next] をクリックします。

**ステップ 5** [Specify Virtual Machine Identity] パネルで、仮想マシンの名前を入力し、[Next] をクリックします。

**ステップ 6** [Configure Hardware] パネルで、仮想マシンのハードウェア設定を行います。 テンプレートを使用している場合は、大部分が設定済みです。

**ステップ 7** [Select Destination] パネルで、[Place the virtual machine on a host; Destination: All Hosts] のデフォルト設定を保持し、[Next] をクリックします。

**ステップ 8** [Select Host] パネルで、ホストが表示されたらそれを選択し、[Next] をクリックします。

**ステップ 9** [Configure Settings] パネルで、設定を確認し、[Next] をクリックします。

**ステップ 10** [Select Networks] パネルで、仮想マシンの仮想スイッチを選択します。 各ネットワーク アダプタに対して、仮想スイッチのタイプ（[Standard Switch]、[Logical Switch] など）を選択し、[Next] をクリックします。
テンプレートに 3 つの NIC が表示されます。

**ステップ 11** テンプレートの 3 番目の NIC が MAC スプーフィングに対して有効になっていることを確認します。

**ステップ 12** [Add Properties] パネルで、[Automatic Actions] のデフォルト設定を保持し、[Next] をクリックします。

**ステップ 13** [Summary] ウィンドウの [Confirm the Settings] パネルで、設定が正確であることを確認します。

**ステップ 14** [Create] をクリックして、仮想マシンを作成します。
[Job Status] カラムの経過表示バーに状態が表示されます。

**ステップ 15** 仮想マシンが作成されたら、仮想マシンを右クリックし、[Power On] を選択します。

**ステップ 16** 仮想マシンを再び右クリックし、[Connect or View] > [Connect via Console] の順に選択します。

## Intercloud Fabric Extender の設定

Intercloud Fabric Extender 仮想マシンを展開した後、その仮想マシンを使用環境に合わせて設定できます。

### はじめる前に

Intercloud Fabric Extender が SCVMM を使用して展開され、その電源がオンになっていること。

### 手順

**ステップ 1** SCVMM から Intercloud Fabric Extender 仮想マシンのコンソールに接続します。

**ステップ 2** 次の資格情報を使用して、Intercloud Fabric Extender 仮想マシンにログインします。

- ユーザ名：admin
- パスワード：Sfish123

（注） このパスワードはユーザ CLI を使用して変更できます。

**ステップ 3** 次のようにして、Intercloud Fabric Extender のホスト名を変更します。

```
switch# config t
switch(config)# hostname name
name(config-if)# ip address 192.36.90.100 255.255.0.0
```

*name* は、Intercloud Fabric Extender 仮想マシンに割り当てられたホスト名です。 この手順の以降の例では、ホスト名として *ICX* が使用されています。

**ステップ 4** 次のように、Intercloud Fabric Extender の管理 IP アドレスを設定します。

```
ICX# conf t
ICX(config)# interface mgmt 0
ICX(config-if)# ip address 192.36.90.100 255.255.0.0
ICX(config-if) # exit
ICX# show interface mgmt. 0
```

**ステップ 5** 次のように、Intercloud Fabric Extender のデフォルト ゲートウェイの IP アドレスを設定します。

```
ICX# conf t
ICX(config)# ip route 0.0.0.0 0.0.0.0 192.36.0.1
ICX(config)# exit
```

**ステップ 6** 次のように、Intercloud Fabric Extender を Intercloud Fabric のインストールと設定, （35 ページ）で展開して設定された PNSC に関連付けます。

```
ICX# conf t
ICX(conf t)# nsc-policy-agent
ICX(config-nsc-policy-agent)# registration-ip 192.36.90.37
ICX(config-nsc-policy-agent)# shared-secret PNSC-shared-secret-password
```

```
ICX(config-nsc-policy-agent)# policy-agent-image install
ICX(config-nsc-policy-agent)# exit
ICX# exit
ICX# show nsc-pa status
NSC Policy-Agent status is - Installed Successfully. Version VNMPAVERSION
```

**ステップ 7** 設定を確認します。

```
ICX# show running-config

!Generating configuration........
!version 1.0.1h.4.4
hostname ICX
interface mgmt 0
  ip address 192.36.90.100 255.255.0.0
ntp server 0.ubuntu.pool.ntp.org
ntp server 1.ubuntu.pool.ntp.org
ntp server 2.ubuntu.pool.ntp.org
ntp server 3.ubuntu.pool.ntp.org
ntp server ntp.ubuntu.com

nsc-policy-agent
  registration-ip 192.36.90.37
  shared-secret **********
  policy-agent-image install
  log-level info
```

**ステップ 8** 設定が正しい場合は、次のように設定を保存します。

```
ICX# copy running-config startup-config
```

# Microsoft 環境への Intercloud Fabric インフラストラクチャ コンポーネントのインストール

[Infrastructure Setup] ウィザードを使用して、Intercloud Fabric VSM などの Intercloud Fabric インフラストラクチャ コンポーネントをインストールするには、次の手順を実行します。

### 手順

**ステップ 1** Cisco Intercloud Fabric for Business アプライアンスにログインします。

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

**ステップ 3** [Infrastructure] タブで、[Setup] ボタンをクリックします。
[Infrastructure Setup] ウィザードが表示されます。

**ステップ 4** [Networking and Placement] の次のフィールドに値を入力します。

| 名前 | 説明 |
|---|---|
| **[Networking and Placement]** | |
| [VM Manager] ドロップダウン リスト | 既存の Hyper-V VM マネージャを選択するか、新しいVMマネージャを作成することを選択します。<br>[Register New VM Manager] を選択した場合、このテーブルには [VM Manager Type] から [Location] までのフィールドが表示されます。 |
| [VM Manager Type] ドロップダウン リスト | 作成する Virtual Machine Manager 資格情報のハイパーバイザ タイプを選択します。 |
| [VM Manager Name] フィールド | 作成する Virtual Machine Manager 資格情報の名前。 |
| [Server Address] フィールド | 作成する資格情報のサーバ アドレス。 |
| [サーバのユーザID] フィールド | 作成する資格情報のサーバ ユーザ名。 |
| [サーバのパスワード] フィールド | 作成する資格情報のサーバ パスワード。 |
| [Domain] フィールド | ドメイン名（Cisco.com など）。 |
| [Description] フィールド | 仮想マシンの説明。 |
| [Contact] フィールド | 管理者の連絡電子メール。 |
| [Location] フィールド | 仮想マシンの場所。 |
| [Icf VSM] ドロップダウン リスト | Intercloud Fabric クラウド用の Intercloud Fabric VSM を選択します。 |

**ステップ 5** [Next] をクリックします。
インストールされている仮想マシンのサマリーが [Summary] ウィンドウに一覧表示されます。

**ステップ 6** [Submit] をクリックします。

**ステップ 7** タスクの状態を表示するには、[Infrastructure] 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 8** [Organizations] > [Service Requests] の順に選択します。

**ステップ 9** [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 10** [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。

# システム リソースの予約

最適なパフォーマンスを実現するために、システム要件, （10 ページ）に記載されている最小システム要件よりも余裕があるシステム リソースを、Intercloud Fabric 用に予約することをお勧めします。

（注） システム リソースの予約方法については、VMware のドキュメントを参照してください。

## 手順

**ステップ 1** VMware vCenter にログインします。

**ステップ 2** Intercloud Fabric の VM を選択します。

**ステップ 3** VM をシャットダウンします。

**ステップ 4** VMware vCenter で [リソース割り当て] タブをクリックして現在のリソース割り当てを表示し、[編集] をクリックします。

**ステップ 5** [仮想マシン プロパティ] ペインで、リソースを選択して次の新しい値を入力することで、リソース割り当てを編集します。

- CPU：8vCPU、8000 Mhz
- メモリ：20 GB RAM
- ディスク領域：500 GB HDD

**ステップ 6** 新しいリソース割り当てが設定されたことを確認します。

第 3 章

# Intercloud Fabric Cloud の作成

This chapter contains the following sections:


- Intercloud Fabric Cloud の詳細，49 ページ
- 注意事項と制約事項，50 ページ
- 前提条件，50 ページ
- Intercloud Fabric Cloud 作成のワークフロー，51 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，52 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，59 ページ
- ネットワーク要素の追加，61 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，63 ページ
- Intercloud Fabric Cloud の作成，63 ページ
- サービスの管理，72 ページ
- Intercloud Fabric Cloud の複製，75 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 , （63 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, （21 ページ）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, （61 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, （59 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, （63 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, （52 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, （53 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, （54 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, （55 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 , （58 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。<br>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。<br>[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。<br>• AES-128-CBC（デフォルト）<br>• AES-128-GCM（TCP プロトコルを使用する場合は使用不可）<br>• AES-256-CBC<br>• AES-256-GCM（TCP プロトコルを使用する場合は使用不可）<br>• None（TCP プロトコルを使用する場合は使用不可）<br>[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。<br>• SHA-1（デフォルト）<br>• SHA-256<br>• SHA-384<br>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。<br>[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。<br>• AES-128-CBC（デフォルト）<br>• AES-128-GCM<br>• AES-256-CBC<br>• AES-256-GCM<br>• 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。<br>• SHA-1（デフォルト）<br>• SHA-256<br>• SHA-384<br>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。<br>（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。<br>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。<br>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。<br>• Telnet<br>• ssh<br>• http<br>• 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, （61 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。<br>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。<br>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, （52 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。<br>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, （55 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。<br>新しい IP グループの作成については、IP グループの追加, （54 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。<br>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, （53 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。<br>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。<br>Intercloud Fabric ファイアウォールのインストール, （117 ページ） 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。<br>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。<br>[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, （171 ページ）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。<br>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。<br>Intercloud Fabric Router（CSR）のインストールと設定, （141 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。<br>この VLAN は、Intercloud Fabric Router（CSR）を管理するために使用されます。<br>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。<br>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。<br>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。<br>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。<br>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, （90 ページ） を参照してください。<br>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。<br>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。<br>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。<br>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。<br>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。<br>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。<br>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。<br>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, （90 ページ） を参照してください。<br>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。<br>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。<br>[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。<br>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。<br>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。<br>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。<br>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。<br>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。<br>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。<br>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, （90 ページ） 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。<br>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。<br>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。<br>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。<br>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, （90 ページ） を参照してください。<br>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。<br>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。<br>（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。<br>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。<br>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。<br>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, （52 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。<br>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, （55 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。<br>新しい IP グループの作成については、IP グループの追加, （54 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。<br>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, （53 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。<br>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。<br>Intercloud Fabric ファイアウォールのインストール, （117 ページ）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。<br>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。<br>Intercloud Fabric Router（CSR）のインストールと設定, （141 ページ）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。<br>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。<br>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。<br>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。<br>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。<br>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, （90 ページ） を参照してください。<br>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。<br>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。<br>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。<br>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。<br>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。<br>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。<br>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。<br>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, （90 ページ） を参照してください。<br>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。<br>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。<br>[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。<br>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。<br>[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。<br>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。<br>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。<br>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, （90 ページ） 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。<br>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。

第 4 章

# 仮想マシンの展開

This chapter contains the following sections:


- 仮想マシンの展開について，83 ページ
- 注意事項と制約事項，83 ページ
- 前提条件，85 ページ
- 仮想マシンの展開ワークフロー，86 ページ
- 仮想マシンの作成，87 ページ
- 仮想マシンの移行，109 ページ


## 仮想マシンの展開について

Intercloud Fabric では、仮想マシン（VM）を作成して、その VM に仮想データセンター（VDC）を関連付けることができます。 また、VM を Intercloud Fabric Cloud に移行することもできます。

## 注意事項と制約事項

- アウトオブバンド操作は、Intercloud Fabric ではサポートされません。 クラウドプロバイダーのポータルから仮想マシンを終了させると、Intercloud Fabric GUI にステータスが反映されません。
- 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 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。
- トランク ポートは、クラウドの仮想マシンではサポートされません。
- トランク ポートは、クラウドに移行される仮想マシンではサポートされません。

- Microsoft Azure では、クラウド内の仮想マシンを終了させると、その仮想マシンは終了しますが、ストレージからイメージが削除されないため、プロバイダーによる仮想マシンへの課金は継続されます。 ストレージとイメージを削除するには、仮想マシンの作成に使用されたテンプレートを Intercloud Fabric GUI を使って削除します。
- Intercloud Fabric とクラウドプロバイダー間のネットワーク接続が遅いと、仮想マシンの移行など、イメージのアップロード操作が失敗することがあります。 イメージが 12 時間以内にアップロードされない場合、その操作は失敗したことになり、Intercloud Fabric によってイメージのアップロードが再試行されます。
- 特定のシスコ クラウド サービス プロバイダーでは、仮想マシンの移行後、仮想マシン イメージに対して sysprep を実行する必要があります。 sysprep を実行すると、Windows 管理者パスワードのリセットや参加先ドメインからの仮想マシンの削除など、仮想マシン内の一部の設定が変更されます。 sysprep の実行によるこれらの影響に対処するために、クラウド プロバイダーに仮想マシンを移行した後は、次の点に注意してください。

  1. Windows パスワードは、**Assign VM** ダイアログボックスの [VM Name] フィールドに入力した仮想マシンの名前にリセットされます。 仮想データセンターへの仮想マシンの割り当てを参照してください。 仮想マシン名が 10 文字未満の場合は、仮想マシンの名前にリセットされたパスワードに、10 文字の制限を満たすために必要な文字数が付加されます。
  2. 仮想マシンがドメインに属していた場合は、移行が完了して、プライベート クラウドのネットワークへの接続が復旧した後に、その仮想マシンを手動でドメインに再参加させる必要があります。

- Intercloud Fabric Cloud からプライベートクラウドに仮想マシンを移行する前に、仮想マシンのプライベート クラウドに十分なストレージ容量があることを確認してください。
- Intercloud Fabric Cloud からプライベートクラウドに仮想マシンを移行する前に、デフォルトのコンピューティング ポリシーにリソース プールを追加する必要があります。 これにより、移行時に [Migrate VM Back on Premise] ウィンドウで、その追加したリソース プールを選択できるようになります。
- Intercloud Fabric Cloud からプライベートクラウドに仮想マシンを移行する前に、移行する仮想マシンのポート プロファイルが、移行先プライベート VDC のネットワーク ポリシーのポート プロファイルと完全に一致していることを確認してください。
- プライベート クラウドから Intercloud Fabric Cloud に仮想マシンを移行する前に、移行する仮想マシンのポート プロファイルが、移行先 Intercloud Fabric Cloud VDC のネットワーク ポリシーのポート プロファイルと完全に一致していることを確認してください。
- 
- Amazon Web Service（AWS）は、特定の EC2 インスタンス タイプに対して拡張ネットワーキング機能をサポートしています。 AWS に Windows 仮想マシンを移動するには、Windows 仮想マシンに Intel ドライバをロードする必要があります。
  - ◦ AWS の拡張ネットワーキング機能の詳細については、『Enhanced Networking』を参照してください。

- Windows で拡張ネットワーキング機能を有効化する方法については、『Enabling Enhanced Networking on Windows』を参照してください。
-

- Intercloud Fabric では、最大 8 台のディスクと共に、仮想マシンと仮想マシン テンプレートを移行できます。
- Linux ベースの仮想マシンでは、`fstab (/etc/fstab)` および grub コンフィギュレーション ファイル（`/boot/grub/menu.lst`）で、永続名を使用してディスクを参照する必要があります。 ディスクの永続的な名前として UUID またはラベルを使用できます。
- Linux ベースの仮想マシンでは、特定バージョンのデフォルトの DVD カーネルのみがサポートされます。
- **一時仮想マシンについて**
  - Amazon Web Services で Linux 仮想マシンを作成し、アップロードしたイメージをホストする場合は、Intercloud Fabric によって一時的な仮想マシンが作成されます。
  - Intercloud Fabric は、一時的な仮想マシンに対して *PNSC IP Address* **tmp** *UUID* 形式の命名規則を使用します。
  - Intercloud Fabric は、300 GB のディスク容量を備えた c3.large インスタンス タイプの一時仮想マシンを作成します。
  - Intercloud Fabric は、一時仮想マシンのディスク使用状況をモニタし、必要に応じて新しい一時仮想マシンを作成します。
  - 作成される一時仮想マシンはリージョン固有であり、Intercloud Fabric は同じリージョン内でその一時仮想マシンを再利用します。
  - Intercloud Fabric は、非アクティブな状態が 12 時間続くとその一時仮想マシンを終了させます。
- Cisco Intercloud Fabric は、VM 要件に最も合致するプロバイダー クラウドの VM インスタンスを選択します。

# 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。
- Intercloud Fabric 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。
- 必要なポリシーを設定しておきます。
- 次のポートでトラフィックを許可するように、ゲスト オペレーティング システムのファイアウォールを設定しておきます。

- TCP トラフィック（SSH）用のポート 22
- TCP 用のポート 6644
- UDP 用のポート 6644

- Cisco Intercloud Services – V および CloudStack の場合は、ゲスト VM に `vmware-tools` がインストールされている必要があります。
- Linux VM の場合は、SSH、SCP、sudo、mkinitrd バイナリをインストールしておきます。

# 仮想マシンの展開ワークフロー

仮想マシンの展開は、以下の手順で行います。

**手順**

**ステップ 1** 仮想マシンを作成する。

a) ポリシーを作成する。
ポリシーの作成, （87 ページ）を参照してください。

b) 仮想データセンター（VDC）を作成する。
Intercloud Fabric 仮想データセンターの作成, （96 ページ）を参照してください。

c) イメージを更新する。
Intercloud Fabric へのイメージのアップロード, （101 ページ）を参照してください。

d) テンプレートを作成する。
Intercloud Fabric Cloud でのテンプレートの作成, （103 ページ）を参照してください。

e) テンプレートにカタログを追加する。
テンプレートへのカタログの追加, （104 ページ）を参照してください。

f) サービス リクエストを作成する。
サービス要求の作成, （106 ページ）を参照してください。

**ステップ 2** 仮想マシンを Intercloud Fabric Cloud に移行する。

a) プライベート仮想データセンター（VDC）を作成する。
プライベート仮想データセンターの作成, （99 ページ）を参照してください。

b) 仮想マシンを Intercloud Fabric Cloud に移行する。
Intercloud Fabric Cloud への仮想マシンの移行, （109 ページ）を参照してください。

**ステップ 3** プライベート クラウドに仮想マシンを移行する。

a) Intercloud Fabric 仮想データセンター（VDC）を作成する。
Intercloud Fabric 仮想データセンターの作成, （96 ページ）を参照してください。

b) プライベート クラウドに仮想マシンを移行する。

プライベート クラウドへの仮想マシンの移行, （110 ページ）を参照してください。

# 仮想マシンの作成

## ポリシーの作成

仮想マシンの展開の成功は、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** ユーザ グループ
ユーザ グループの作成, （91 ページ）を参照してください。

**ステップ 2** ユーザの追加
ユーザ グループへのユーザの追加, （93 ページ）を参照してください。

**ステップ 3** スタティック IP プール ポリシー
スタティック IP プール ポリシーの作成, （90 ページ）を参照してください。

**ステップ 4** Intercloud Fabric ネットワーク ポリシー
Intercloud Fabric ネットワーク ポリシーの作成, （87 ページ）を参照してください。

**ステップ 5** Intercloud Fabric システム ポリシー
Intercloud Fabric システム ポリシーの作成, （89 ページ）を参照してください。

**ステップ 6** VMware ネットワーク ポリシー
VMware ネットワーク ポリシーの作成, （94 ページ）を参照してください。

**ステップ 7** VMware コンピューティング ポリシー
VMware コンピューティング ポリシーの作成, （95 ページ）を参照してください。

### Intercloud Fabric ネットワーク ポリシーの作成

Intercloud Fabric ネットワーク ポリシーを作成するには、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** [Policies] > [Virtual/Hypervisor Policies] > [Network] の順に選択します。

**ステップ 3** [Network] ウィンドウで、[Intercloud Network Policy] タブをクリックします。

**ステップ 4** [Intercloud Network Policy] タブで、[Add] ボタンをクリックします。
[Add Intercloud Network Policy Information] ウィンドウが表示されます。

**ステップ 5** [Add Intercloud Network Policy Information] の次のフィールドに値を入力します。

| 名前 | 説明 |
|---|---|
| [Policy Name] フィールド | ネットワーク ポリシーの名前。 |
| [ポリシーの説明] フィールド | ネットワーク ポリシーの説明。 |
| [Cloud Name] ドロップダウン リスト | Intercloud Fabric Cloud ネットワーク ポリシーの名前。 |
| [NICs] ドロップダウン リスト | 既存の NIC を選択するか、新しいポリシーを作成します。 |
| [NIC Name] フィールド | 仮想マシン ネットワークの NIC のエイリアス。 |
| [Mandatory] チェックボックス | このチェックボックスをオンにすると、NIC が編集不可になります。 |
| [Port Groups] ボタン | クリックして、ポート プロファイルまたはポート グループを選択します。 |
| [Port Profile Name] チェックボックス | リストからポート プロファイルまたはポート グループを選択します。 選択するポート グループが VMware vSwitch または Cisco Nexus 1000V スイッチのポート グループである場合、そのポート グループは Intercloud Fabric VSM で自動的に作成されます。<br>（注） Cisco Nexus 1000V スイッチを Intercloud Fabric に追加しておきます。ネットワーク要素の追加, （61 ページ）を参照してください。 |
| [Select IP Address Type] ドロップダウン リスト | ネットワーク ポリシーの IP アドレス タイプを選択します。 |

| 名前 | 説明 |
|---|---|
| [Static IP Pool] ボタン | リストからスタティック IP プール ポリシーを選択します。<br>このフィールドは、[Select IP Address Type] ドロップダウン リストから [Static] を選択すると表示されます。 |
| [Save NIC] ボタン | 保存する場合にクリックします。 |

**ステップ 6** [Submit] をクリックします。

## Intercloud Fabric システム ポリシーの作成

Intercloud Fabric システム ポリシーを作成するには、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** [Policies] > [Virtual/Hypervisor Policies] > [System Policy] の順に選択します。

**ステップ 3** [System Policy] ウインドウで、[Intercloud System Policy] タブを選択します。

**ステップ 4** [Intercloud System Policy] タブで、[Add] ボタンをクリックします。
[Add Intercloud System Policy Information] ウィンドウが表示されます。

**ステップ 5** [Add Intercloud System Policy Information] の次のフィールドに値を入力します。

| 名前 | 説明 |
|---|---|
| [Policy Name] フィールド | システム ポリシーの名前。 |
| [ポリシーの説明] フィールド | システム ポリシーの説明。 |
| [VM名のテンプレート] フィールド | VM テンプレートの名前。 |
| [End User VM Name or VM Prefix] チェックボックス | エンドユーザがVMの名前を定義できるようにするには、このチェックボックスをオンにします。 |
| [DNSドメイン] フィールド | DNS ドメインの名前。 |
| [DNSサーバリスト] フィールド | DNS サーバの IP アドレス。 |

**ステップ 6** [Submit] をクリックします。

## スタティック IP プール ポリシーの作成

スタティック IP プール ポリシーを作成するには、次の手順を実行します。

Intercloud Fabric では、IP プールは以下で使用されます。

- PNSC、プライベート クラウドの Intercloud Fabric VSM などのインフラストラクチャ コンポーネント
- プロバイダー クラウドの Intercloud Fabric Extender や Intercloud Fabric スイッチなどのインフラストラクチャ コンポーネント
- クラウド内の仮想マシンのアドレス

IP の作成時は以下のガイドラインに従ってください。

- 次の 3 種類の IP プールを作成することをお勧めします。
  - IP プール 1：PNSC、インフラストラクチャのセットアップ時にプライベート クラウドで作成された Intercloud Fabric VSM などのインフラストラクチャ コンポーネント用
  - IP プール 2：インフラストラクチャのセットアップ時にプロバイダー クラウドで作成された Intercloud Fabric Extender や Intercloud Fabric スイッチなどのインフラストラクチャ コンポーネント用
  - IP プール 3：クラウド内の仮想マシンのアドレス用
- 複数のアプリケーション層が必要な場合は、さらに多くの IP プールを作成する必要があります。 インフラストラクチャのセットアップ時に IP プールの詳細を表示したり編集したりできない場合は、Intercloud Fabric のセットアップ時に、プライベート クラウドのインフラストラクチャ コンポーネント用の IP プールを指定する必要があります。
- 1 つの IP プールを選択して、それを複数の Intercloud Fabric Cloud 間で使用する場合、その IP は通信可能である必要があります。 それ以外の場合は、Intercloud Fabric Extender と Intercloud Fabric スイッチおよび関連サービスに十分対応できる大きなサブネット プールを使用します。
- 3 番目のプール セットには既存の名前は不要ですが、クラウドの仮想マシンで使用されます。

手順

**ステップ 1** Intercloud Fabricにログインします。

**ステップ 2** [Policies] > [Virtual/Hypervisor Policies] > [Network] の順に選択します。

**ステップ 3** [Network] ウィンドウで、[Static IP Pool Policy] タブを選択します。

**ステップ 4** [Static IP Pool Policy] タブで、[Add] ボタンをクリックします。
[Static IP Pool Policy Information] ウィンドウが表示されます。

**ステップ 5** [Static IP Pool Policy Information] の次のフィールドに値を入力します。

| 名前 | 説明 |
|---|---|
| [Policy Name] フィールド | ポリシーの名前。 |
| [ポリシーの説明] フィールド | ポリシーの説明。 |
| [Static IP Pools] ペイン | エントリを追加するには、プラスアイコンをクリックします。 |

**ステップ 6** [Add Entry to Static IP Pools] の次のフィールドに値を入力します。

| 名前 | 説明 |
|---|---|
| [静的IPプール] フィールド | ポリシーの IP プール範囲。 |
| [Subnet Mask] フィールド | ポリシーのサブネット マスク。 |
| [ゲートウェイIPアドレス] フィールド | ポリシーのゲートウェイ アドレス。 このフィールドは Intercloud Fabric にとって必須です。 |
| [VLAN ID] フィールド | ポリシーの VLAN ID。 このフィールドは Intercloud Fabric にとって必須です。 |

**ステップ 7** [Submit] をクリックします。

## ユーザ グループの作成

ユーザ グループを作成するには、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** [Administration] > [Users and Groups] の順に選択します。

**ステップ 3** [Users and Group] ウィンドウで、[User Group] タブを選択します。

**ステップ 4** [User Group] タブで、[Add Group] ボタンをクリックします。

**ステップ 5** [Add Group] 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 | ユーザ グループの名前。 |
| [Description] フィールド | ユーザ グループの説明。 |
| [Code] フィールド | ユーザ グループのコード。 |
| [コストセンター] フィールド | ユーザ グループが属するコスト センターの名前。 |
| [連絡先の電子メール] フィールド | 管理者の電子メール アドレス。 |
| [First Name] フィールド | 管理者の名前。 |
| [Last Name] フィールド | 管理者の姓。 |
| [Phone] フィールド | 管理者の電話番号。 |
| [Address] フィールド | 管理者の住所。 |
| [グループ共有ポリシー] ドロップダウン リスト | グループ共有ポリシーを選択します。<br>このフィールドは Intercloud Fabric に適用できません。 |
| [Allow resource Assignment to Users] チェックボックス | リソース制限を有効にする場合はこのチェックボックスをオンにし、リソース制限を無効にする場合はオフにします。チェックボックスをオンにすると、グループに対するリソース制限を設定するためのオプションが示され、ゼロ以外のリソース制限がすべて適用されます。<br>このフィールドは Intercloud Fabric に適用できません。 |

**ステップ 6** [Add] をクリックして、ユーザ グループを作成します。

## ユーザ グループへのユーザの追加

### はじめる前に

グループにユーザを追加する前に、そのグループが作成されていることを確認してください。

### 手順

**ステップ 1** Intercloud Fabricにログインします。

**ステップ 2** [Administration] > [Users and Groups] の順に選択します。

**ステップ 3** [ログインユーザ] タブをクリックします。

**ステップ 4** [Login Users] タブで、[Add Group] ボタンをクリックします。

**ステップ 5** [ユーザの追加] 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。

| フィールド名 | 説明 |
|---|---|
| [User Role] ドロップダウン リスト | ユーザ ロールを選択します。<br>（注） [Group Admin] ユーザ タイプは、ユーザ グループに割り当てることができる唯一の管理者ユーザ ロールです。 |
| [User Group] ドロップダウン リスト | ユーザが属するグループまたは顧客組織を選択します。 |
| [ログイン名] フィールド | ユーザのログイン名。 |
| [パスワード] フィールド | ユーザのパスワード。<br>（注） ユーザに対して Lightweight Directory Access Protocol（LDAP）認証が設定されている場合、パスワードはローカル サーバではなく、LDAP サーバでのみ検証されます。 |
| [パスワードの確認] フィールド | 確認のために、ユーザのパスワードを再度入力します。 |
| [User Contact Email（ユーザの連絡先電子メール）] フィールド | ユーザの電子メール アドレス。<br>（注） 電子メール アドレスは、サービス リクエストのステータスをグループ所有者に通知し、承認を要求するために必要です。 |

| フィールド名 | 説明 |
|---|---|
| [名] フィールド | ユーザの名。 |
| [姓] フィールド | ユーザの姓。 |
| [電話] フィールド | ユーザの電話番号です。 |
| [住所] フィールド | ユーザの郵便住所です。 |

**ステップ 6** [Add] をクリックします。

## VMware ネットワーク ポリシーの作成

VMware ネットワーク ポリシーを作成するには、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** [Policies] > [Virtual/Hypervisor Policies] > [Network] の順に選択します。

**ステップ 3** [Network] ウィンドウで、[VMware Network Policy] タブをクリックします。

**ステップ 4** [VMware Network Policy] タブで、[Add] ボタンをクリックします。

**ステップ 5** 表示された [Network Policy Information] ウィンドウで、次のフィールドに値を入力します。

| 名前 | 説明 |
|---|---|
| [Policy Name] フィールド | ネットワーク ポリシーの名前。 |
| [ポリシーの説明] フィールド | ネットワーク ポリシーの説明。 |
| [Cloud Name] ドロップダウン リスト | ネットワーク ポリシーのクラウドの名前を選択します。 |
| [NICs] ドロップダウン リスト | 既存の NIC を選択するか、新しいポリシーを作成します。 |
| [NIC Name] フィールド | 仮想マシン ネットワークの NIC のエイリアス。 |
| [必須] チェックボックス | このチェックボックスをオンにすると、NIC が編集不可になります。 |

| 名前 | 説明 |
|---|---|
| [Port Groups] ボタン | クリックして、ポートプロファイルまたはポート グループを選択します。 |
| [Port Profile Name] チェックボックス | リストからポート プロファイルまたはポート グループを選択します。選択するポート グループが VMware vSwitch または Cisco Nexus 1000V スイッチのポート グループである場合、そのポート グループは Intercloud Fabric VSM で自動的に作成されます。<br>（注） Cisco Nexus 1000V スイッチを Intercloud Fabric に追加しておきます。ネットワーク要素の追加, （61 ページ）を参照してください。 |
| [Save NIC] ボタン | 保存する場合にクリックします。 |

**ステップ 6** [Submit] をクリックします。

## VMware コンピューティング ポリシーの作成

VMware コンピューティング ポリシーを作成するには、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** [Policies] > [Virtual/Hypervisor Policies] > [Computing] の順に選択します。

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

**ステップ 4** [VMware Computing Policy] タブで、[Add] ボタンをクリックします。

**ステップ 5** 表示された [Add Computing Policy] ウィンドウで、次のフィールドに値を入力します。

| 名前 | 説明 |
|---|---|
| [Policy Name] フィールド | ポリシーの名前。<br>（注） この名前は、カタログの定義で使用されます |
| [ポリシーの説明] フィールド | ポリシーの説明。 |

| 名前 | 説明 |
|---|---|
| [Cloud Name] ドロップダウン リスト | リソース割り当てを行うクラウドを選択します。 |
| [Selected Host NodesNodes] ボタン | ノードを選択するには、このチェックボックスをオンにして、[Select] をクリックします。 |

**ステップ 6** [Submit] をクリックします。

# Intercloud Fabric 仮想データセンターの作成

Intercloud Fabric 用の仮想データセンターを作成するには、次の手順を実行します。

### はじめる前に

Intercloud Fabric のポリシー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] > [IcfCloud] の順に選択します。

**ステップ 3** [IcfCloud] ウィンドウで、[IcfCloud] タブをクリックします。

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

**ステップ 5** [Policies] > [Virtual/Hypervisor Policies] > [Virtual Data Centers] > [Add vDC] の順に移動して、[Add vDC] ウィザードにアクセスすることもできます。

**ステップ 6** [Add vDC] ウィンドウで、次のフィールドに値を入力します。

| 名前 | 説明 |
|---|---|
| [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。 |

**ステップ 7** [Submit] をクリックします。

**ステップ 8** [Add Intercloud vDC] ウィンドウで、次のフィールドに値を入力します。

| 名前 | 説明 |
|---|---|
| 一般情報 | |

| 名前 | 説明 |
|---|---|
| [vDC Name] フィールド | 仮想データセンターの名前。 |
| [vDC Description] フィールド | 仮想データセンターの説明。 |
| [グループ] ドロップダウン リスト | 既存のユーザ グループを選択するか、[Add Group (+)] ボタンをクリックしてデータセンター用のユーザ グループを作成します。 |
| [Provider Account] ドロップダウン リスト | 仮想データセンターのプロバイダーアカウントを選択します。 |
| [Cloud Name] ドロップダウン リスト | 仮想データセンターの Intercloud Fabric Cloud を選択します。 |
| **承認者と連絡先** | |
| [Approver Username] フィールド | 承認者 のユーザ名。<br>このフィールドは、[Advanced] チェックボックスを選択した場合にのみ表示されます。 |
| **ポリシー** | |
| [System Policy] ドロップダウン リスト | 既存のシステム ポリシーを選択するか、仮想データセンター用のシステム ポリシーを作成することを選択します。<br>システム ポリシーを作成するには、Intercloud Fabric システム ポリシーの作成, （89 ページ）を参照してください。 |
| [Network Policy] ドロップダウン リスト | 既存のネットワーク ポリシーを選択するか、仮想データセンター用のネットワーク ポリシーを作成することを選択します。<br>ネットワーク ポリシーを作成するには、Intercloud Fabric ネットワーク ポリシーの作成, （87 ページ） を参照してください。 |
| [Advanced] チェックボックス | 詳細設定を表示するには、このチェックボックスをオンにします。<br>（注） このフィールドは、[VMware] 以外のクラウド タイプを選択した場合にのみ表示されます。 |

| 名前 | 説明 |
|---|---|
| [Allowed Active VMs for the vDC] チェックボックス | 仮想データセンターに対して許可するアクティブな仮想マシンの数を定義するには、このチェックボックスをオンにします。<br>（注） このフィールドは、[VMware] 以外のクラウドタイプを選択し、[Advanced] チェックボックスを選択した場合にのみ表示されます。 |
| [Define the number of active VMs allowed for this vDC] フィールド | 仮想データセンターに対して許可するアクティブな仮想マシンの数。<br>（注） このフィールドは、[Allowed Active VMs for the vDC] チェックボックスを選択した場合にのみ表示されます。 |
| **[Deployment and Resizing Options]** | 詳細設定を表示するには、[Advanced] チェックボックスをオンにします。 |
| [Override Template] チェックボックス | テンプレートの設定を上書きするには、このチェックボックスをオンにします。<br>（注） このフィールドは、[VMware] 以外のクラウドタイプを選択し、[Advanced] チェックボックスを選択した場合にのみ表示されます。 |
| [Define the number of CPUs] フィールド | テンプレートの CPU の数。<br>このフィールドは、[Override Template] チェックボックスを選択した場合にのみ表示されます。 |
| [Define the size of the Memory] フィールド | テンプレートのメモリ サイズ。<br>このフィールドは、[Override Template] チェックボックスを選択した場合にのみ表示されます。 |
| [Allow Resizing of VM] チェックボックス | 仮想データセンターの仮想マシンのサイズ変更を許可するには、このチェックボックスをオンにします。<br>（注） このフィールドは、[VMware] 以外のクラウドタイプを選択し、[Advanced] 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 |
|---|---|
| [Define the number of CPUs] フィールド | 仮想マシンの CPU の数。<br>このフィールドは、[Allow Resizing of VM] チェックボックスを選択した場合にのみ表示されます。 |
| [Define the size of the Memory] フィールド | 仮想マシンのメモリ サイズ。<br>このフィールドは、[Allow Resizing of VM] 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 9** [Add] をクリックして、パブリック Intercloud Fabric 仮想データセンターを追加します。

**ステップ 10** タスクの状態を表示するには、[Intercloud] > [Compute] の順に選択します。

**ステップ 11** クラウドを選択し、[vDC] タブをクリックします。
vDC のレポートが表示されます。 レポートの詳細については、『*Cisco Intercloud Fabric User Guide*』 を参照してください。

# プライベート仮想データセンターの作成

Intercloud Fabric 用のプライベート仮想データセンターを作成するには、次の手順を実行します。

### はじめる前に

Intercloud Fabric のポリシー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] > [IcfCloud] の順に選択します。

**ステップ 3** [IcfCloud] ウィンドウで、[IcfCloud] タブをクリックします。

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

**ステップ 5** [Policies] > [Virtual/Hypervisor Policies] > [Virtual Data Centers] > [Add vDC] の順に移動して、[Add vDC] ウィザードにアクセスすることもできます。

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

| 名前 | 説明 |
|---|---|
| [Cloud Type] ドロップダウン リスト | VMware のクラウド タイプを選択します。 |

**ステップ 7** [Submit] をクリックします。

**ステップ 8** [Add private vDC] の次のフィールドに値を入力します。

| 名前 | 説明 |
|---|---|
| **一般情報** | |
| [vDC Name] フィールド | 仮想データセンターの名前。 |
| [vDC Description] フィールド | 仮想データセンターの説明。 |
| [グループ] ドロップダウン リスト | 既存のユーザ グループを選択するか、[Add Group (+)] ボタンをクリックしてデータセンター用のユーザ グループを作成します。新しいユーザ グループの作成については、ユーザ グループの作成, （91 ページ） を参照してください。<br>仮想データセンターの作成後は、この値を変更できません。 |
| [Cloud Name] ドロップダウン リスト | 仮想データセンターのクラウドの名前を選択します。<br>仮想データセンターの作成後は、この値を変更できません。 |
| **ポリシー** | |
| [コンピューティングポリシー] ドロップダウン リスト | 既存のコンピューティング ポリシーを選択するか、仮想データセンター用のコンピューティング ポリシーを作成することを選択します。<br>ホスト/クラスタを選択する必要があります。デフォルトのコンピューティング ポリシーにはホスト/クラスタがありません。 |

| 名前 | 説明 |
|---|---|
| [Network Policy] ドロップダウン リスト | 既存のネットワーク ポリシーを選択するか、仮想データセンター用のネットワーク ポリシーを作成することを選択します。<br>ホスト/クラスタを選択する必要があります。デフォルトのネットワーク ポリシーにはホスト/クラスタがありません。<br>デフォルトのネットワーク ポリシーには NIC がありません。 デフォルト ポリシーを変更して NIC を追加することも、新しいネットワーク ポリシーを作成することもできます。<br>ネットワーク ポリシーを作成するには、Intercloud Fabric ネットワーク ポリシーの作成, （87 ページ） を参照してください。 |

**ステップ 9** [Add] をクリックして、プライベート仮想データセンターを追加します。

**ステップ 10** タスクの状態を表示するには、[Intercloud] > [Compute] の順に選択します。

**ステップ 11** クラウドを選択し、[vDC] タブをクリックします。
vDC のレポートが表示されます。 レポートの詳細については、『*Cisco Intercloud Fabric User Guide*』 を参照してください。

# Intercloud Fabric へのイメージのアップロード

Intercloud Fabric にイメージをアップロードするには、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] > [Compute] の順に選択します。

**ステップ 3** [Compute] ウインドウで、[Enterprise Template] タブを選択します。

**ステップ 4** [Enterprise Template] タブで、[Upload Image] ボタンをクリックします。
[Image Upload] ウィザードが表示されます。

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

| 名前 | 説明 |
|---|---|
| [Image Name] フィールド | Intercloud Fabric にアップロードするイメージの名前。 このイメージは、Intercloud Fabric Cloud のテンプレートの作成に使用されます。 |
| [Image Type] ドロップダウン リスト | イメージ タイプを選択します。 |
| [Image Source] ドロップダウン リスト | イメージ ソースを選択します。 |
| [Upload Protocol] ドロップダウン リスト | アップロードのプロトコルを選択します。<br>このフィールドは、イメージ ソースとして [Remote desktop] を選択した場合にのみ表示されます。 |
| [Remove Server IP] フィールド | リモート サーバの IP アドレス。<br>このフィールドは、イメージ ソースとして [Remote desktop] を選択した場合にのみ表示されます。 |
| [User Name] フィールド | ユーザ名。<br>このフィールドは、イメージ ソースとして [Remote desktop] を選択した場合にのみ表示されます。 |
| [Password] フィールド | ユーザ名のパスワード。<br>このフィールドは、イメージ ソースとして [Remote desktop] を選択した場合にのみ表示されます。 |
| [Filepath] フィールド | イメージのファイル パス。<br>このフィールドは、イメージ ソースとして [Remote desktop] を選択した場合にのみ表示されます。 |
| [Browse] ボタン | このボタンをクリックして、アップロードするファイルを選択します。 |

**ステップ 6** [Upload] をクリックして、イメージをアップロードします。

**ステップ 7** [Submit] をクリックします。

**ステップ 8** タスクの状態を表示するには、[Enterprise Image] 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 9** [Organizations] > [Service Requests] の順に選択します。

**ステップ 10** [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 11** [View Details] 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。

# Intercloud Fabric Cloud でのテンプレートの作成

Intercloud Fabric Cloud でテンプレートを作成するには、次の手順を実行します。

### はじめる前に

Intercloud Fabric にイメージをアップロードしておきます。

### 手順

**ステップ 1** Intercloud Fabric にログインします。

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

**ステップ 3** [Compute] ウインドウで、[Enterprise Template] タブを選択します。

**ステップ 4** [Enterprise Template] タブで、イメージを選択し、[Create Template in Cloud] ボタンをクリックします。
[Create Template in Cloud] ウィザードが表示されます。

**ステップ 5** [Create Template in Cloud] の次のフィールドに値を入力します。

| 名前 | 説明 |
|---|---|
| [Template Name] フィールド | テンプレートの名前。 |
| [Cloud Name] ドロップダウン リスト | テンプレートの Intercloud Fabric Cloud 名。 |
| **Template Properties** | |
| [CPUコア] フィールド | テンプレートの CPU コアの値。 可能な値は 1 ～ 64 です。 |
| [Memory (MB)] フィールド | テンプレートのメモリの値。 可能な値は 32 ～ 1048576 です。 |

| 名前 | 説明 |
|---|---|
| [Disk (GB)] フィールド | テンプレートのディスクの値。 可能な値は 32 ～ 1048576 です。 |

**ステップ 6** [Submit] をクリックして、テンプレートを作成します。

**ステップ 7** タスクの状態を表示するには、[IcfTemplates] 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 8** [Organizations] > [Service Requests] の順に選択します。

**ステップ 9** [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 10** [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。

# テンプレートへのカタログの追加

テンプレートにカタログを追加するには、次の手順を実行します。

### はじめる前に

- Intercloud Fabric にイメージをアップロードしておきます。
- アップロードしたイメージに基づいてテンプレート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** [Policies] > [Catalogs] の順に選択します。

**ステップ 3** [Catalogs for all User Groups] ウィンドウで、[Catalog] タブを選択します。

**ステップ 4** [Catalog] タブで、テンプレートを選択し、[Add] ボタンをクリックします。

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

| 名前 | 説明 |
|---|---|
| [カタログタイプ] ドロップダウン リスト | カタログ タイプを選択します。これは Intercloud Fabric を選択する必要があります。 |

**ステップ 6** [Submit] をクリックします。
[Create Catalog] ウィザードが表示されます。

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

| 名前 | 説明 |
|---|---|
| **基本情報** | |
| [カタログ名] フィールド | カタログの名前。 |
| [カタログの説明] フィールド | カタログの説明。 |
| [カタログアイコン] ドロップダウン リスト | カタログのアイコンを選択します。 |
| [すべてのグループに適用] チェックボックス | すべてのユーザ グループがこのカタログを表示できるようにするには、チェックボックスをオンにします。 |
| [Selected Groups] ボタン | クリックして、このカタログのユーザ グループを選択します。 |
| [Cloud Name] ドロップダウン リスト | Intercloud Fabric Cloud を選択します。 |
| [イメージ] ドロップダウン リスト | Intercloud Fabric Cloud に関連付けられているテンプレートを選択します。 |

**ステップ 8** [Next] をクリックします。

**ステップ 9** [アプリケーションの詳細] ペインで、次のフィールドに値を入力します。

| 名前 | 説明 |
|---|---|
| [カテゴリ] ドロップダウン リスト | 仮想マシンのカテゴリを選択します。選択したカテゴリに定義済みのポリシーがある場合、それらのポリシーは VDC で定義されたポリシーに優先します。<br>アプリケーション カテゴリの管理, （108 ページ）を参照してください。 |
| [OSの指定] ドロップダウン リスト | 仮想マシンのオペレーティング システムを選択します。 |

**ステップ 10** [Next] をクリックします。
[Summary] ウィンドウにカタログ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、カタログを作成します。

**ステップ 12** タスクの状態を表示するには、[Catalog] 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。

# サービス要求の作成

サービス リクエストを作成するには、次の手順を実行します。仮想マシンをプロビジョニングするには、最初にサービス リクエストを作成する必要があります。 管理者または同等のユーザがサービス リクエストを承認すると、仮想マシンがプロビジョニングされます。仮想マシンは、ただちに承認することも、オリジナルのリクエストから 90 日以内に承認するようにスケジュールすることもできます。

### はじめる前に

- Intercloud Fabric にイメージをアップロードしておきます。
- Intercloud Fabric Cloud にアップロードしたイメージに基づいてテンプレートを作成しておきます。
- テンプレートにカタログを追加しておきます。

### 手順

**ステップ 1** Intercloud Fabric にログインします。

**ステップ 2** [Organizations] > [Service Requests] の順に選択します。

**ステップ 3** [Service Request] タブをクリックします。

**ステップ 4** [リクエストの作成] をクリックします。

**ステップ 5** [Create Request] 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 |
|---|---|
| [カタログタイプ] ドロップダウン リスト | カタログ タイプを選択します。これは Intercloud Fabric を選択する必要があります。 |

**ステップ 6** [Submit] をクリックします。
[Create Service Request] ウィザードが表示されます。

**ステップ 7** [Create Service Request] ウィザード で、[Catalog Selection] の次のフィールドに値を入力します。

| 名前 | 説明 |
|---|---|
| [グループの選択] ドロップダウン リスト | サービス リクエストのユーザ グループを選択します。 |
| [カタログの選択] ドロップダウン リスト | サービスリクエストのカタログを選択します。 |

**ステップ 8** [Next] をクリックします。

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

| 名前 | 説明 |
|---|---|
| [VDCの選択] ドロップダウン リスト | 仮想マシンをプロビジョニングする VDC。 |
| [Description] フィールド | VDC の説明。 |

**ステップ 10** [Custom Specification] の次のフィールドに値を入力します。

| 名前 | 説明 |
|---|---|
| [VM Networks] ペイン | 必要に応じて、vNIC を選択するか、鉛筆型アイコンをクリックして編集します。 |

**ステップ 11** [Edit VM Networks Entry] の次のフィールドに値を入力します。

| 名前 | 説明 |
|---|---|
| [NICエイリアス] フィールド | 仮想マシン ネットワークの NIC のエイリアス。 |
| [必須] チェックボックス | このチェックボックスをオンにすると、NIC が編集不可になります。 |
| [Port Groups] ペイン | ポート グループにエントリを追加するには、プラス アイコンをクリックします。 |

**ステップ 12** [Next] をクリックします。
[Summary] ウィンドウにサービス リクエストのサマリーが一覧表示されます。

**ステップ 13** [Submit] をクリックして、サービス リクエストを作成します。

**ステップ 14** タスクの状態を表示するには、[Catalog] 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 15** [Organizations] > [Service Requests] の順に選択します。

**ステップ 16** [Service Request] タブをクリックします。 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 17** [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。

# アプリケーション カテゴリの管理

アプリケーション カテゴリを管理するには、次の手順を実行します。 アプリケーション カテゴリを使用すると、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 ポリシーやシステム ポリシーを上書きすることができます。

### はじめる前に

### 手順

**ステップ 1** Intercloud Fabric にログインします。

**ステップ 2** [Policies] > [Virtual/Hypervisor Policies] > [Virtual Data Center] の順に選択します。

**ステップ 3** [vDC] タブで、仮想データセンターを選択し、[Management Categories] ボタンをクリックします。
[Virtual Data Centers for All User Groups] ウィンドウが表示されます。

**ステップ 4** アプリケーション カテゴリを選択し、[Edit] をクリックします。
[Edit App Category] ウィンドウが表示されます。

**ステップ 5** [Edit App Category] の次のフィールドに値を入力します。

| 名前 | 説明 |
|---|---|
| [Network Policy] ドロップダウン リスト | ネットワーク ポリシーを選択します。 |
| [System Policy] ドロップダウン リスト | システム ポリシーを選択します。 |

**ステップ 6** [Save（保存）] をクリックします。

# 仮想マシンの移行

## Intercloud Fabric Cloud への仮想マシンの移行

Intercloud Fabric Cloud に仮想マシンを移行するには、次の手順を実行します。

（注） アプリケーション カテゴリのポリシーは、仮想データセンターのポリシーに優先します。 アプリケーション カテゴリの管理, （108 ページ）を参照してください。

### はじめる前に

- Intercloud Fabric に仮想データセンターを作成しておきます。
- プライベート クラウドに仮想データセンターを作成しておきます。 管理ユーザの場合、これは任意です。

### 手順

**ステップ 1** Intercloud Fabric にログインします。

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

**ステップ 3** 仮想データセンターを選択します。

**ステップ 4** [Migrate VM to Cloud VM] タブをクリックします。

**ステップ 5** リストから仮想マシンを選択し、[Migrate VM to Cloud] ボタンをクリックします。

**ステップ 6** 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 |
|---|---|
| [Target VM Name] フィールド | 仮想マシンの名前。 |
| [VDCの選択] ドロップダウン リスト | 仮想マシンの移行先としてプロバイダー クラウドの仮想データセンターを選択します。 |
| [Select OS Version] ドロップダウン リスト | OS のバージョンを選択します。 |
| [コメント] フィールド | 必要に応じて、コメントを入力します。 |
| [Remove Source VM] チェックボックス | プライベート クラウド内の仮想データセンターからソース仮想マシンを削除するには、このチェックボックスをオンにします。 |

**ステップ 7** [Proceed] をクリックします。

# プライベート クラウドへの仮想マシンの移行

プライベート クラウドに仮想マシンを移行するには、次の手順を実行します。

（注） アプリケーション カテゴリのポリシーは、仮想データセンターのポリシーに優先します。 アプリケーション カテゴリの管理, （108 ページ）を参照してください。

## 手順

**ステップ 1** Intercloud Fabric にログインします。

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

**ステップ 3** クラウド内の仮想データセンターを選択します。

**ステップ 4** [VMs] タブを選択します。

**ステップ 5** リストから仮想マシンを選択し、[Migrate VM on Premise] ボタンをクリックします。

**ステップ 6** [Migrate VM on Premise] 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 |
|---|---|
| [Target VM Name] フィールド | 仮想マシンの名前。 |
| [VDCの選択] ドロップダウン リスト | 仮想マシンの移行先としてプライベート クラウドの仮想データセンターを選択します。 |
| [Select OS Version] ドロップダウン リスト | OS のバージョンを選択します。 |
| [コメント] フィールド | 必要に応じて、コメントを入力します。 |
| [Remove Source VM] チェックボックス | クラウド内のソース仮想マシンを削除するには、このチェックボックスをオンします。 |

**ステップ 7** [Proceed] をクリックします。

第 5 章

# クラウド仮想マシンのオンボード

This chapter contains the following sections:


- クラウド仮想マシンのオンボードについて，111 ページ
- 注意事項と制約事項，111 ページ
- 前提条件，112 ページ
- Intercloud Fabric へのクラウド仮想マシンのオンボード，113 ページ


## クラウド仮想マシンのオンボードについて

Intercloud Fabric を使用すると、プロバイダークラウドからIntercloud Fabric に仮想マシンをオンボードできます。 オンボード プロセスはプロバイダー クラウドで直接行われ、仮想マシンをプライベート クラウドに戻す必要はありません。 仮想マシンのオンボードは次のようなメリットをもたらします。

- Intercloud Fabric 内の 1 つの場所からすべての仮想マシンを管理できます。
- エンタープライズ IP アドレス空間を使用できます。
- プロバイダー インスタンスに対して Intercloud Fabric のすべのセキュリティ メカニズムを使用できます。
- プライベート サブネットをプロバイダー クラウドに拡張することによって、LDAP や DNS など、企業インフラストラクチャと管理フレームワークを使用できます。

## 注意事項と制約事項

- プロバイダー クラウドで動作する仮想マシンを Intercloud Fabric にオンボードすることは、Amazon Web Services EC2 Classic および Amazon Web Services EC2 VPC でのみサポートされます。

- オンボード処理はリージョン内に適用されます。つまり、仮想マシンと宛先VDCは同じリージョンにあります。
- 仮想マシンを Intercloud Fabric にオンボードすると、その仮想マシンにプライベート IP アドレスが割り当てられます。 新たに割り当てられるプライベート IP アドレスを使用してアプリケーションが通信することを想定している場合は、オンボードする前に、プロバイダーの IP アドレスを明示的に使用していたアプリケーションを手動で更新する必要があります。
- オンボードされる可能性がある、パーティショニングされていないディスクを備えた Linux 仮想マシンは、プライベート クラウドに移動できません。
- Windows 仮想マシンはオンボード可能ですが、プライベート クラウドには移動できません。
- プライベート クラウドに戻すことを想定している Linux 仮想マシンを参照する場合は、非永続名（/dev/xvda など）ではなく、永続名（UUID またはラベル）を /etc/fstab で使用する必要があります。 次に例を示します。
  - grub コンフィギュレーション ファイルでは、カーネル パラメータ root はラベルまたは ID を使用してルート パーティションを参照する必要があります。

    grub.conf でのラベル/ID の例：
    ```
    kernel /boot/vmlinuz-2.6.32-431.29.2.el6.x86_64 console=ttyS0
    ro root=UUID=9996863e-b964-47d3-a33b-3920974fdbd9
    rd_NO_LUKS  KEYBOARDTYPE=pc KEYTABLE=us
    LANG=en_US.UTF-8 xen_blkfront.sda_is_xvda=1
    console=ttyS0,115200n8 console=tty0 rd_NO_MD SYSFONT=latarcyrheb-sun16
    crashkernel=auto rd_NO_LVM rd_NO_DM
    ```
  - システム コンフィギュレーション ファイル /etc/fstab では、先頭カラムに、パーティション名ではなく、ラベルまたは ID が必要です。

    fstab でのラベル/ID の例：
    ```
    UUID=9996863e-b964-47d3-a33b-3920974fdbd9 /
    ext4
    defaults        1 1
    ```

# 前提条件

- Intercloud Fabric にオンボードする仮想マシンの資格情報を取得していることを確認します。
- プロバイダーのコンソールからオンボードした仮想マシンと Intercloud Fabric が通信できるように、仮想マシンについて以下が更新済みであることを確認します。
  - Amazon EC2 VPC の仮想マシンのセキュリティ グループを、Intercloud Fabric によって作成された仮想マシンのセキュリティ グループに変更。
  - UDP と TCP のポート 6644 と 6646、および TCP ポート 22 のインバウンド ルールを、Amazon EC2 Classic の仮想マシンのセキュリティ グループに追加。 セキュリティ グループは、Intercloud Fabric で作成された仮想マシンのセキュリティ グループと一致する必要があります。

- プロバイダー クラウドで Windows 仮想マシンのファイアウォールまたは IP テーブルが設定されている場合は、必要なポートが開いていることを確認します。
- プロバイダー クラウドにオンボードされている Windows 仮想マシンにオンボード パッケージをコピーできるように、必要なユーティリティ（Win SCP など）があることを確認します。
- Windows VM のオンボードを準備するために、次の手順を実行します。
  1. ZIP 圧縮されたバンドルを Windows VM にコピーします。
  2. c:\Program Files (x86)\ に `Cisco` という名前のフォルダを作成します。
  3. `Cisco` フォルダに ZIP 圧縮されたバンドルの内容を抽出します。
  4. `icf_onboard-*` 実行アプリケーションをダブルクリックします。

     これで、Intercloud Fabric に VM を展開する準備が整います。
- Linux 仮想マシンに SSH がインストール済みであることを確認します。
- オンボーディングの準備が整っている仮想マシンについて、次の情報を入手していることを確認します。
  - インスタンス ID
  - OS のバージョン
  - アーキテクチャ（32 ビットまたは 64 ビット）
  - CPU
  - メモリ
  - ディスク サイズ

# Intercloud Fabric へのクラウド仮想マシンのオンボード

Intercloud Fabric にクラウド仮想マシンをオンボードするには、次の手順を実行します。 同時に 1 台の仮想マシンのみを Intercloud Fabric にオンボードできます。

（注） このソフトウェア リリースでは、Intercloud Fabric へのクラウド仮想マシンのオンボードは、Amazon Web Service（AWS）EC2 Classic および Amazon Web Services（AWS）EC2-VPC でのみ実行できます。

Intercloud Fabric へのクラウド仮想マシンのオンボードは、以下の手順で行います。

1. クラウド VM へのコピー元となる場所にパッケージをダウンロードする。
2. クラウド VM にパッケージをコピーしてインストールする。

3 Intercloud Fabric に VM をオンボードする。

### 手順

**ステップ 1** Intercloud Fabricにログインします。

**ステップ 2** 次の手順でパッケージをダウンロードします。

a) [Intercloud] > [Compute] の順に選択します。

b) [Compute] ウィンドウで、プライベート クラウドを選択し、[VM] タブを選択します。

c) [VM] ウィンドウで、VM を選択し、[Onboard package] をクリックします。

d) Linux VM をオンボードするには、Linux パッケージ用の [Download] ボタンをクリックします。Windows VM をオンボードするには、Windows パッケージ用の [Download] ボタンをクリックします。

e) ローカル マシンにオンボード パッケージをダウンロードします。

**ステップ 3** 次の手順で、オンボード パッケージをコピーしてインストールします。

a) WinSCP または SSH を使用してプロバイダー クラウドの VM にログインし、ダウンロードしたオンボード パッケージを VM にコピーします。
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AccessingInstances.html を参照してください。

b) 次のコマンドを入力して、パッケージが VM にダウンロードされたことを確認します。
**# cd /root**

**# ls**

c) 次のコマンドを入力して、仮想マシン内のいずれかの場所にパッケージを抽出します。
**# unzip** *file_name*

d) 次のコマンドを入力して、パッケージをインストールします。
**# icf_onboard.sh**

例：
Linux VM パッケージのインストール出力

```
[root@ip-10-0-0-161 ec2-user]# cd /tmp/
[root@ip-10-0-0-161 tmp]# ls
lnx_ob_bundle_2.2.67.tgz
[root@ip-10-0-0-161 tmp]# tar -xzvf lnx_ob_bundle_2.2.67.tgz
authorized_keys
csw
ica-2.2.67.centos6_2.i686.rpm
ica-2.2.67.centos6_2.x86_64.rpm
ica-2.2.67.centos6_3.i686.rpm
ica-2.2.67.centos6_3.x86_64.rpm
ica-2.2.67.centos6_4.i686.rpm
ica-2.2.67.centos6_4.x86_64.rpm
ica-2.2.67.centos6_5.x86_64.rpm
ica-2.2.67.rhel6_0.i686.rpm
ica-2.2.67.rhel6_0.x86_64.rpm
ica-2.2.67.rhel6_1.i686.rpm
ica-2.2.67.rhel6_1.x86_64.rpm
ica-2.2.67.rhel6_2.i686.rpm
ica-2.2.67.rhel6_2.x86_64.rpm
ica-2.2.67.rhel6_3.i686.rpm
ica-2.2.67.rhel6_3.x86_64.rpm
```

```
ica-2.2.67.rhel6_4.i686.rpm
ica-2.2.67.rhel6_4.x86_64.rpm
ica-2.2.67.rhel6_5.x86_64.rpm
ica-2.2.67.sles11_2.x86_64.rpm
ica-2.2.67.sles11_3.x86_64.rpm
icf_onboard.sh
ssh_host_rsa_key
version.txt
[root@ip-10-0-0-161 tmp]# ./icf_onboard.sh
Found RHEL 6.5 x86_64
Image is now ICF ready.
```

**ステップ 4** Intercloud Fabric に VM をオンボードする手順：

a) Intercloud Fabric にログインします。

b) [Intercloud] > [Compute] の順に選択します。

c) [Compute] ウィンドウで、VMware クラウドを選択し、[VM] タブをクリックします。

d) [Onboard Cloud VM] をクリックします。
[Onboard Cloud VM] ウィンドウが表示されます。

e) [Onboard Cloud VM] の次のフィールドに値を入力します。

| 名前 | 説明 |
|---|---|
| [Instance ID] フィールド | オンボードする仮想マシンのインスタンス ID。 |
| [VM名] フィールド | オンボードする仮想マシンの名前。 |
| [VDCの選択] ドロップダウン リスト | 仮想マシンをオンボードする Intercloud Fabric 内の既存の VDC を選択します。<br>仮想マシンには、Intercloud Fabric VDC のネットワーク ポリシーに基づいて、ネットワーク情報（VLAN ID、静的 IP アドレス、DHCP IP アドレスなど）が割り当てられます。 |
| [Select OS Version] ドロップダウン リスト | オンボードする仮想マシンの OS のバージョンを選択します。 |
| [カテゴリ] ドロップダウン リスト | オンボードする仮想マシンのカテゴリを選択します。<br>アプリケーション カテゴリを使用すると、VDC に関連付けられているネットワーク ポリシーやシステム ポリシーを上書きすることができます。 |

f) [Proceed] をクリックして、Intercloud Fabric に仮想マシンをオンボードします。

g) タスクの状態を表示するには、次の手順を実行します。

1 [Organizations] > [Service Requests] の順に選択します。

2. [Service Request] タブを選択し、サービス リクエスト番号を検索するか、[Search] フィールドにサービス リクエスト番号を入力します。
3. [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。

h) [Onboard VM Cloud] レポートを表示するには、[Intercloud] > [Compute] > *[public-cloud-name]* > *[virtual-data-center]* の順に選択し、[VM] タブをクリックします。
次の情報が表示されます。

- インスタンス ID
- プロバイダー IP アドレス
- エンタープライズ IP アドレス
- VM の電源状態
- 仮想データセンターの名前
- クラウド内の Intercloud Fabric Switch とのトンネルのステータス

第 6 章

# Intercloud Fabric ファイアウォールのインストール

This chapter contains the following sections:


- Intercloud Fabric Firewall について，117 ページ
- 前提条件，118 ページ
- 注意事項と制約事項，118 ページ
- 基本的なトポロジ，119 ページ
- Intercloud Fabric Firewall のインストール ワークフロー，119 ページ


## Intercloud Fabric Firewall について

Intercloud Fabric Firewall（VSG）は、クラウド プロバイダー環境内のセキュアな仮想化データセンターへの信頼できるアクセスを実現する仮想アプライアンスであり、動的なポリシーベースの運用、トランスペアレント モビリティの強化、高密度マルチテナント機能のスケールアウト展開などの要件を満たしています。 Intercloud Fabric Firewall では、確立されたセキュリティ ポリシーによって信頼ゾーンへのアクセスを確実に制御および監視することができます。

Intercloud Fabric Firewall は、ワークロードの仮想化、企業のセキュリティ ポリシーと業界規制の順守の強化、簡素化されたセキュリティ監査など、さまざまなメリットをもたらします。

また、クラウド環境の仮想マシンを有害なネットワーク トラフィックから保護すると共に、Intercloud Fabric Router（CSR）またはクラウド仮想マシンのパブリック インターフェイスを介して仮想マシンへのアクセスを試みる不正なインターネットユーザや、サイト間のセキュア トンネルを介してアクセスを試みる不正な内部ユーザからも保護します。

Intercloud Fabric Firewall を展開することで、顧客はプライベート クラウドの セキュリティ ポリシーを拡張して、プロバイダー クラウドで実行する各自のアプリケーション ワークロードを保護することができます。 さらに、Intercloud Fabric Firewall は、Intercloud Fabric 環境で 3 層式アプリケーションをサポートすることによって、仮想マシン グループ間の論理的な分離を実現します。

セキュリティ要件に基づいて、仮想マシンを論理グループの一部として定義し、仮想マシン グループに Intercloud Fabric Firewall を適用することができます。

# 前提条件

- Intercloud Fabric Director がインストールされていること。
- インフラストラクチャのセットアップと Intercloud Fabric Cloud のセットアップが完了していること。
- Intercloud Fabric Extender トランク インターフェイスに対してポート グループを使用する場合は、Intercloud Fabric Extenderトランク ポートで無差別モードが有効になっていること。
- Intercloud Fabric Extender のトランク インターフェイスにバインドされているポート グループで全 VLAN 範囲が有効になっていること。

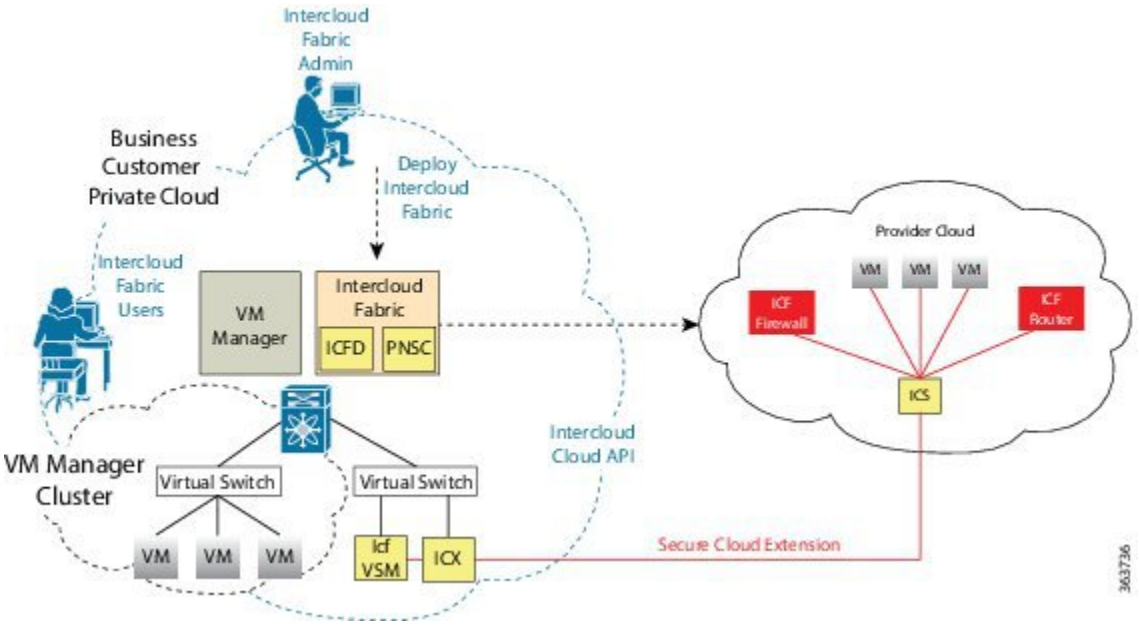
# 注意事項と制約事項

- Intercloud Fabric Cloud のインスタンスを作成した後で Intercloud Fabric Firewall サービスを追加することもできます。 サービスの管理, （72 ページ） を参照してください。

# 基本的なトポロジ

次の図は、Intercloud Fabric Firewall の基本的なトポロジを示しています。

**図 7 : *Intercloud Fabric Firewall* の基本的なトポロジ**




# Intercloud Fabric Firewall のインストール ワークフロー

Intercloud Fabric Firewall のインストール ワークフローには以下の手順が含まれます。

**手順**

**ステップ 1** Intercloud Fabric から Intercloud Fabric Firewall テンプレートとサービス インターフェイスを作成する。

- Intercloud Fabric Cloud の作成時にサービスを有効化する場合は、Intercloud Fabric Cloud の作成, （63 ページ） 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, （72 ページ） を参照してください。

**ステップ 2** Intercloud Fabric Firewall をインスタンス化する。
Intercloud Fabric Firewallのインスタンス化, （131 ページ）を参照してください。

**ステップ 3** コンピュート セキュリティ プロファイルを設定する。

コンピュート セキュリティ プロファイルの設定, （133 ページ）を参照してください。

**ステップ 4** サービス パスを作成する。
#unique_100を参照してください。

**ステップ 5** ポート プロファイルにサービス パスをバインドする。
ポート プロファイルへのサービス パスのバインド, （137 ページ）を参照してください。

**ステップ 6** クラウド仮想マシンのポート プロファイルを編集して、ファイアウォール サービスを有効化する。
Intercloud Fabric Firewall 用のポート プロファイルの編集, （138 ページ） を参照してください。

**ステップ 7** インストールを確認する。
Intercloud Fabric Firewall のインストールの確認, （139 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, （61 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。<br>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。 |

| 名前 | 説明 |
|---|---|
| [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。<br>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, （52 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。<br>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, （55 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。<br>新しい IP グループの作成については、IP グループの追加, （54 ページ） を参照してください。 |

| 名前 | 説明 |
|---|---|
| [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。<br>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, （53 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。<br>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。<br>Intercloud Fabric ファイアウォールのインストール, （117 ページ）を参照してください。 |
| [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。<br>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。<br>[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, （171 ページ）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。<br>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。<br>Intercloud Fabric Router（CSR）のインストールと設定, （141 ページ）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。<br>この VLAN は、Intercloud Fabric Router（CSR）を管理するために使用されます。<br>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。 |
| [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。<br>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。<br>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。<br>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。<br>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, （90 ページ） を参照してください。<br>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。<br>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。<br>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。<br>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。<br>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。<br>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。<br>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。<br>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, （90 ページ） を参照してください。<br>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。<br>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。<br>[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。 |

| 名前 | 説明 |
|---|---|
| [Host] ドロップダウン リスト | Intercloud Fabric Extender のホストを選択します。<br>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。<br>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。 |
| [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。<br>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。<br>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。<br>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。<br>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。<br>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, （90 ページ） を参照してください。 |

| 名前 | 説明 |
|---|---|
| **[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。<br>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。 |
| **[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。<br>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。<br>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。<br>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, （90 ページ） を参照してください。<br>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。<br>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。<br>（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。<br>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 Firewallのインスタンス化

Intercloud Fabric Cloud を設定して Intercloud Fabric Firewallテンプレートを導入すると、PNSC からインスタンス化できるようになります。 Intercloud Fabric Firewall, をインスタンス化するには、次の作業を実行します。

### Before You Begin

次の条件が満たされていることを確認します。

- Intercloud Fabric Cloudを作成して設定した。
- Intercloud Fabric Firewall テンプレートを導入した。

### Procedure

**Step 1** Intercloud Fabricにログインします。

**Step 2** [Intercloud] > [Infrastructure]の順に選択します。

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

**Step 4** [Resource Management] タブをクリックします。

**Step 5** ルート構造をナビゲートして、インスタンス化するテナントを選択しますIntercloud Fabric Firewall。

**Step 6** [tenant] ペインで、[Actions] ドロップダウン リストから [Add Compute Firewall] を選択します。

**Step 7** [Add Compute Firewall] ダイアログ ボックスで、次を入力します。

| Name | Description |
|---|---|
| [Name]フィールド | Intercloud Fabric Firewallの名前。 |
| [Description] フィールド | Intercloud Fabric Firewallの説明。 |
| [Host Name]フィールド | Intercloud Fabric Firewallのホスト名。 |

**Step 8** [Select] をクリックしてデバイス プロファイルを選択し、[OK] をクリックします。

**Step 9** [Next] をクリックします。

**Step 10** [Select Service Device] ページで、[Instantiate in Cloud] オプションを選択します。

**Step 11** リストから Intercloud Fabric Firewall テンプレートを選択します。

**Step 12** [VM Access] セクションで、管理者アクセス用のパスワードを入力して確認します。

**Step 13** [Next] をクリックします。

**Step 14** [VPC] ページの [Select Intercloud Link] セクションで、適切な Intercloud Fabric Cloudをナビゲートして選択します。

**Step 15** [Next] をクリックします。

**Step 16** [Configure Service VM Interfaces] ページで、[Add Interface] をクリックします。

**Step 17** [Add Interface] ダイアログ ボックスで、インターフェイス タイプとして [Management] を選択し、次の詳細を入力します。

| Name | Description |
|---|---|
| [IP Addressフィールド | 管理インターフェイスの IP アドレス。 |
| [Subnet] フィールド | 管理インターフェイスのサブネット マスク。 |
| Gateway] フィールド | 管理インターフェイスのゲートウェイ。 |
| [Port Group] ドロップダウン リスト | Intercloud Fabric から作成したファイアウォール管理ポート プロファイル。<br>**Note** ファイアウォール管理ポート プロファイルは、 Intercloud Fabricから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 |

**Step 18** [OK] をクリックして、[Add Interface]ダイアログ ボックスを閉じます。

**Step 19** [Configure Service VM Interfaces] ページで、[Add Interface] をクリックします。

**Step 20** [Add Interface] ダイアログ ボックスで、インターフェイス タイプとして [Data] を選択し、次の詳細を入力します。

| Name | Description |
|---|---|
| [IP Address] フィールド | データ インターフェイスの IP アドレス。 |
| [Subnet] フィールド | データインターフェイスのサブネットマスク。 |

| Name | Description |
|---|---|
| [Port Group]ドロップダウン リスト | Intercloud Fabricから作成したファイアウォール データ ポート プロファイル。<br>**Note** ファイアウォール データ ポート プロファイルは、Intercloud Fabricから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_Data_710 |

**Step 21** [OK] をクリックします。

**Step 22** [Next]をクリックします。

**Step 23** [Summary] ページで詳細を確認し、[Finish] をクリックして Intercloud Fabric Firewallをインスタンス化します。

# コンピュート セキュリティ プロファイルの設定

Cisco Prime Network Services Controller（PNSC）では、テナント レベルでコンピュート セキュリティ プロファイルを作成することができます。

### 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、[Policy Management] > [Service Profiles] > [root] > [tenant] > [Compute Firewall] > [Compute Security Profiles] の順に選択します。

**ステップ 5** [General] タブで、[Add Compute Security Profile] をクリックします。

**ステップ 6** [Add Compute Security Profile] の次のフィールドに値を入力します。

（注） 次の属性は Intercloud Fabric にのみ対応しています。

- VM name
- Port profile name
- Operating system name
- User-defined (custom)

**表 5**：***[General]*** タブ

| フィールド | 説明 |
|---|---|
| Name | プロファイル名。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 | プロファイルの簡単な説明。識別子として 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。 |
| Policy Set | ポリシー セットのドロップダウン リスト。 |
| Add ACL Policy Set | このリンクをクリックすると、ACL ポリシー セットを追加できます。 |
| Resolved Policy Set | このリンクをクリックすると、解決されたポリシー セットを編集できます。 |
| **[Resolved Policies] 領域** | |
| (Un)assign Policy | このリンクをクリックすると、ポリシーを割り当てまたは割り当て解除できます。 |
| Name | ルール名。 |
| Source Condition | ルールの送信元条件。 |
| Destination Condition | ルールの宛先条件。 |
| Service/Protocol | ルールが適用されるプロトコルまたはサービス。 |
| EtherType | ルールが適用される、カプセル化されているプロトコル。 |
| Action | ルール条件が満たされた場合に実行するアクション。 |

| フィールド | 説明 |
|---|---|
| Description | ルールの説明。 |

表 *6* : *[Attributes]* タブ

| フィールド | 説明 |
|---|---|
| Add User Defined Attribute | 属性を追加するダイアログボックスが開きます。 |
| Name | 属性名。 |
| Value | 属性値。 |

**ステップ 7** [OK] をクリックします。

# サービス パスの作成

サービス パスを作成するには、次の手順を実行します。

（注） サービス パスではサービス ノードを複数回使用できません。

**手順**

| | コマンドまたはアクション | 目的 |
|---|---|---|
| **ステップ 1** | 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]> tenant > [Policies] > [Service Path]の順に選択し、[Add Service Path] | |
| **ステップ 5** | [Add Service Path] ダイアログボックスで、サービス パスの名前と | |

<table>
<tr><th></th><th>コマンドまたはアクション</th><th>目的</th></tr>
<tr><td></td><td>説明を入力し、[Add Service Entry]をクリックします。</td><td></td></tr>
<tr><td>ステップ 6</td><td>次の詳細を入力します。</td><td>
<table>
<tr><th>名前</th><th>説明</th></tr>
<tr><td>[Service Type]オプション ボタン</td><td>サービス タイプを選択します。</td></tr>
<tr><td>[Service Node]ドロップダウン リスト</td><td>既存のサービス ノードを選択するか、新しいサービス ノードを作成します。</td></tr>
<tr><td>[Name]フィールド</td><td>サービス ノードの名前。<br>このフィールドは、新しいサービス ノードを作成する場合にのみ表示されます。</td></tr>
<tr><td>[Service Type]オプション ボタン</td><td>サービス タイプを選択します。<br>このフィールドは、新しいサービス ノードを作成する場合にのみ表示されます。</td></tr>
<tr><td>[Network Service]ドロップダウン リスト</td><td>論理サービス デバイスの名前。<br>このフィールドは、新しいサービス ノードを作成する場合にのみ表示されます</td></tr>
<tr><td>[Fail Mode]オプション ボタン</td><td>サービス ノードが接続を失った場合に実行するアクション。<br>このフィールドは、新しいサービス ノードを作成する場合にのみ表示されます。</td></tr>
<tr><td>[Adjacency Type]オプション ボタン</td><td>レイヤ 3 隣接タイプを選択します。<br>このフィールドは、新しいサービス ノードを作成する場合にのみ表示されます。</td></tr>
</table>
</td></tr>
</table>

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | [Service Profile]ドロップダウン リスト: サービス プロファイルを選択します。サービス プロファイルは、サービス パスを使用しているトラフィックに適用するポリシーを識別します。 |
| ステップ 7 | サービス パスでの必要に応じて、追加のサービス エントリを入力し、[OK]をクリックします。 | |

# ポート プロファイルへのサービス パスのバインド

ポート プロファイルにサービス パスをバインドすると、そのポート プロファイルを使用するすべてのトラフィックが、設定されているサービス パスに従うようになります。

### はじめる前に

サービス パスが存在することを確認します。

### 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、[Resource Management] > [Resources] > [VSMs] > *[vsm]* > [Edit] の順に選択します。

**ステップ 5** [Port Profiles] テーブルで、サービス パスをバインドするポート プロファイルを選択し、[Edit] をクリックします。

**ステップ 6** [Service Path] フィールドで、[Select] をクリックします。

**ステップ 7** [Select Service Path] ダイアログボックスで 、必要なサービス パスを選択し、[OK] をクリックします。

**ステップ 8** [Edit Port Profile] ダイアログボックスで、[Apply]、[OK] の順にクリックし、変更を適用して保存します。

# Intercloud Fabric Firewall 用のポート プロファイルの編集

Intercloud Fabric Firewall 用のポート プロファイルを編集するには、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** [Port Profile] タブで、ポート プロファイルを選択します。

**ステップ 5** [Edit] ボタンをクリックします。
[Edit Port Profile] ウィンドウが表示されます。

**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 |
|---|---|
| [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するには、このチェックボックスをオンにします。<br>（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。 |
| [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。<br>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。 |

| 名前 | 説明 |
|---|---|
| [New Org Name] フィールド | 組織の名前。<br>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** [Submit] をクリックします。

# Intercloud Fabric Firewall のインストールの確認

Intercloud Fabric Firewall 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、[Resource Management] > [Managed Resources] の順に選択します。

**ステップ 5** icfCloud を選択し、[Network Services] を選択します。
テーブルで Intercloud Fabric Firewall のインストールのステータスを確認できます。

第 7 章

# 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，141 ページ
- 注意事項と制約事項，142 ページ
- 前提条件，143 ページ
- Intercloud Fabric Router（CSR）のインストールと設定に関するワークフロー，143 ページ


## Intercloud Fabric Router（CSR）について

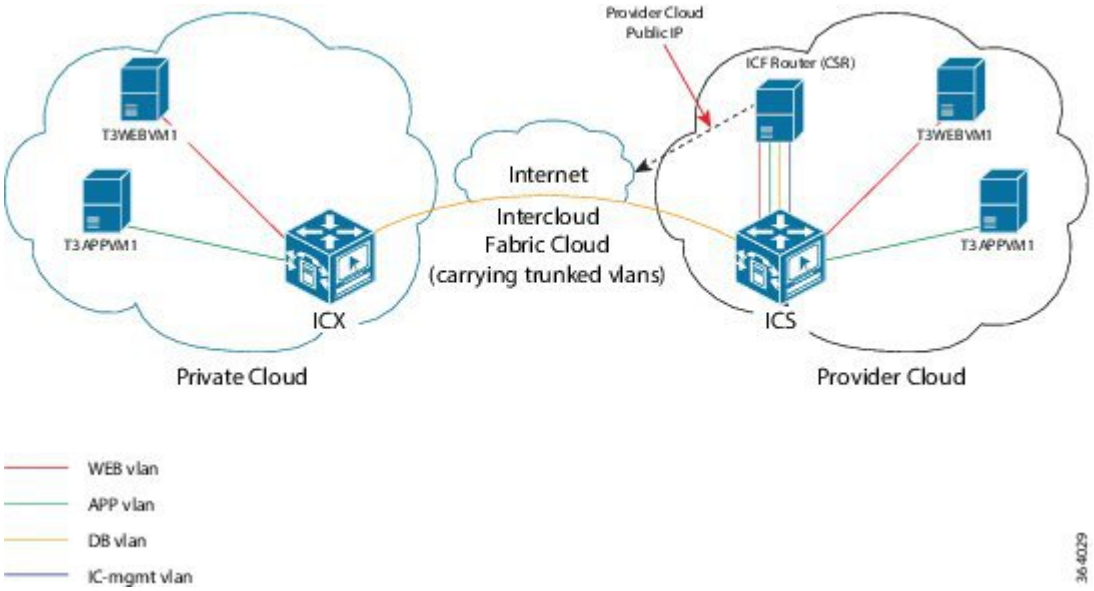
Intercloud Fabric Router（CSR）は、x86 サーバ ハードウェア上の仮想マシン（VM）インスタンスに配置されるクラウドベースの仮想ルータを提供します。 Intercloud Fabric Router（CSR）は、指定された Cisco IOS XE セキュリティ機能とスイッチング機能を仮想化プラットフォーム上で提供する仮想プラットフォームです。

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 *8*：*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, （63 ページ）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, （63 ページ）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, （72 ページ） 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, （156 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, （161 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, （165 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, （61 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。 |

| 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。<br>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。<br>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, （52 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。<br>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, （55 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。<br>新しい IP グループの作成については、IP グループの追加, （54 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。<br>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, （53 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。<br>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。<br>Intercloud Fabric ファイアウォールのインストール, （117 ページ） 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。<br>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。<br>[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, （171 ページ）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。<br>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。<br>Intercloud Fabric Router（CSR）のインストールと設定, （141 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。<br>この VLAN は、Intercloud Fabric Router（CSR）を管理するために使用されます。<br>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。<br>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。<br>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。<br>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。<br>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，（90 ページ） を参照してください。<br>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。<br>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。<br>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。<br>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。<br>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。<br>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。<br>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。<br>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，（90 ページ） を参照してください。<br>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。<br>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。<br>[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。<br>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。<br>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。<br>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。<br>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。<br>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。<br>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。<br>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, （90 ページ） 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。<br>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。<br>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。<br>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。<br>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，（90 ページ） を参照してください。<br>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。<br>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。<br>（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。<br>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。<br>[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。<br>新しい条件を追加するには、[Add Rule Condition] をクリックします。<br>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。<br>新しい条件を追加するには、[Add Rule Condition] をクリックします。<br>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。<br>• 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。<br>• 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。<br>1 [Any] チェックボックスをオフにします。<br>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。<br>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。<br>• Resolved Source IP Pool<br>• Resolved Source Port Pool<br>• Resolved Source IP PAT Pool<br>• Resolved Destination IP Pool<br>• Resolved Destination Port Pool<br>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。<br>[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。<br>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。<br>• [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。<br>• [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。<br>• [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。<br>• [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。<br>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。<br>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<br>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
```

第 8 章

# Intercloud Fabric Router（統合型）のインストールと設定

This chapter contains the following sections:


- Intercloud Fabric Router (Integrated)について，169 ページ
- 注意事項と制約事項，170 ページ
- 前提条件，171 ページ
- Intercloud Fabric Router (Integrated) のインストールと設定に関するワークフロー，171 ページ


## Intercloud Fabric Router (Integrated)について

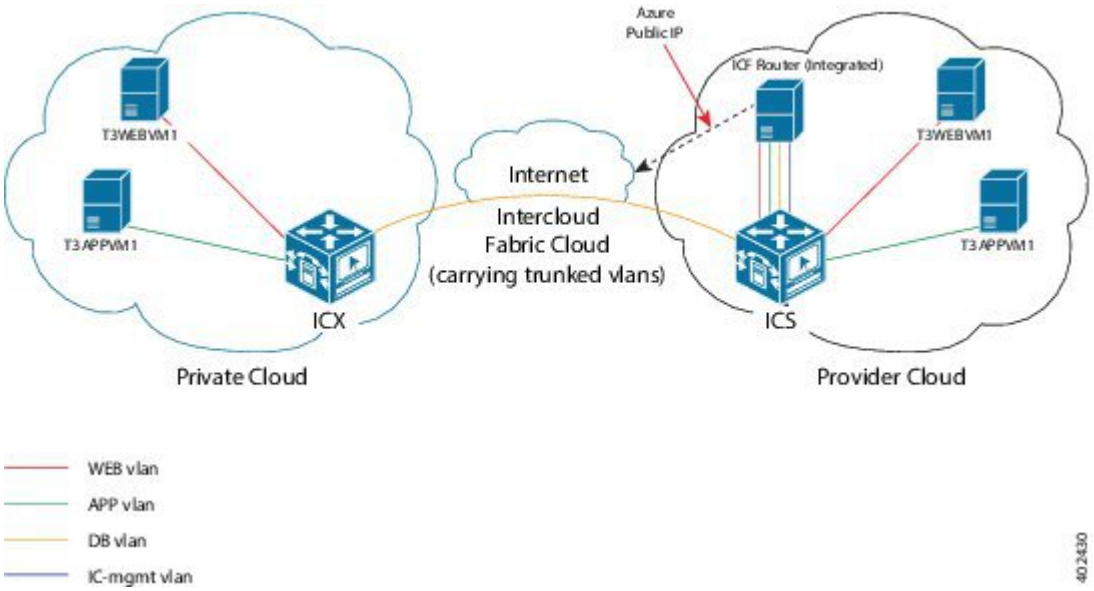
Intercloud Fabric Router (Integrated)は統合されたルータ機能を Intercloud Fabric にもたらします。 これは、Intercloud Fabric スイッチのコンテナとしてオンデマンドで作成されます。 Intercloud Fabric Cloud がインスタンス化されるときや、既存の Intercloud Fabric インスタンス上にあるときに作成できます。

Intercloud Fabric Router (Integrated) は Intercloud Fabric のエッジ デバイスとして動作し、次の機能を提供します。

- プロバイダー クラウドの仮想マシン用の VLAN 間ルーティング。
- 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。
- スタティック ルートの設定。これによって、プロバイダー クラウドに拡張されていない企業ネットワークにプロバイダー クラウドの VM が到達できるようになります。

- プロバイダー クラウドの VM 用 NAT によるインターネットへの直接アクセス。

**図 *9*：*Intercloud Fabric Router (Integrated)* のトポロジ**




# 注意事項と制約事項

Intercloud Fabric Router (Integrated) には次のような制約事項があります。

- Intercloud Fabric Router (Integrated) は、Microsoft Azure でのみサポートされます。
- Intercloud Fabric Cloud インスタンスがハイ アベイラビリティ（HA）モードの場合は、Intercloud Fabric Router (Integrated) を作成できません。
- Intercloud Fabric Cloud インスタンスを Intercloud Fabric Router (Integrated) で作成する場合、HA モードを選択するオプションは無効になります。
- ルーティングは管理 VLAN サブネットで暗黙的に使用できるので、Intercloud Fabric Router (Integrated) でインターフェイスを設定する際は、管理 VLAN のインターフェイスを設定しないでください。

Intercloud Fabric Router (Integrated) には次のような注意事項があります。

- Intercloud Fabric Router (Integrated) は、常に、PNSC 内の icfCloud という名前のテナント組織の下に作成されます。
- Intercloud Fabric Router (Integrated) の名前は自動的に選択され、関連する Intercloud Fabric Cloud と同じ名前になります。 たとえば、Intercloud Fabric Cloud インスタンスの名前が Icf-Azure-Link1 である場合、対応する Intercloud Fabric Router (Integrated) も同じ名前になります。

# 前提条件

各 Intercloud Fabric Cloud ごとに Intercloud Fabric Router (Integrated) 用の特別な IP アドレスが必要であるため、管理サブネットワークに十分な数の IP アドレスを確保してください。

# Intercloud Fabric Router (Integrated) のインストールと設定に関するワークフロー

Intercloud Fabric Router (Integrated) のインストールと設定には、概略的に見て次のタスクが関係します。

**手順**

**ステップ 1** Intercloud Fabric から Intercloud Fabric Router (Integrated) サービスを作成する、または Intercloud Fabric Cloud の作成後に Intercloud Fabric Router (Integrated) サービスを有効化する。

- Intercloud Fabric Cloud の作成, （63 ページ）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, （72 ページ） を参照してください。

**ステップ 2** 以下について、Cisco Prime Network Services Controller を使用して Intercloud Fabric Router (Integrated) を設定する。

a) ルータ インターフェイスの設定。
Intercloud Fabric Router (Integrated) のルータ インターフェイスの設定, （181 ページ） を参照してください。

b) （オプション）スタティック ルーティングの設定。
スタティック ルーティングの設定, （186 ページ）を参照してください。

c) （オプション）ネットワーク アドレス変換（NAT）ポリシーの設定。
Intercloud Fabric Router (Integrated) の NAT ポリシーの設定, （189 ページ）を参照してください。

**ステップ 3** Intercloud Fabric Router (Integrated) のインストールを確認する。
Intercloud Fabric Router (Integrated) のインストールの確認, （194 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, （61 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。<br>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。 |
| [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。<br>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, （52 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。<br>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, （55 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。<br>新しい IP グループの作成については、IP グループの追加, （54 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。<br>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, （53 ページ） を参照してください。 |
| **サービス** | |

| 名前 | 説明 |
|---|---|
| [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。<br>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。<br>Intercloud Fabric ファイアウォールのインストール, （117 ページ）を参照してください。 |
| [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。<br>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。<br>[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, （171 ページ）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。<br>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。<br>Intercloud Fabric Router（CSR）のインストールと設定, （141 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。<br>この VLAN は、Intercloud Fabric Router（CSR）を管理するために使用されます。<br>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。 |
| [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。<br>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。<br>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。<br>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。<br>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, （90 ページ） を参照してください。<br>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。<br>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。<br>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。<br>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。<br>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。<br>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。<br>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。<br>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, （90 ページ） を参照してください。<br>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。<br>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。<br>[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。<br>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。<br>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。<br>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。<br>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。<br>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。<br>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。<br>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, （90 ページ） 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。<br>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。

# Intercloud Fabric Router (Integrated) のサービスの有効化

Intercloud Fabric Cloud を作成した後、[Manage Services] オプションを使用して Intercloud Fabric Router (Integrated) のインスタンスを作成できます。

### はじめる前に

Intercloud Fabric Cloud を作成しておきます。

### 手順

**ステップ 1** Intercloud Fabric GUI にログインし、[Intercloud] > [IcfCloud] の順に選択します。

**ステップ 2** [IcfCloud] ウィンドウで、[IcfCloud] タブを選択します。

**ステップ 3** Intercloud Fabric Cloud を選択し、[Manage Services] をクリックします。

**ステップ 4** [Manage Services] ウィンドウで、[ICF Router (Integrated)] チェックボックスをオンにして、選択した Intercloud Fabric Cloud 上に Intercloud Fabric Router (Integrated) のインスタンスを作成します。Intercloud Fabric Router (Integrated) をインスタンス化した後、Prime Network Services Controller GUI を使用してそれを設定できます。

# Intercloud Fabric Router (Integrated) のルータ インターフェイスの設定

Intercloud Fabric Router (Integrated) を作成または有効化すると、Intercloud Fabric によって Intercloud Fabric Router (Integrated) の管理インターフェイスとトランク インターフェイスが作成されます。VLAN 間ルーティング、NAT と PAT のポリシー、およびスタティック ルーティング用のインターフェイスを設定する必要があります。 Intercloud Fabric Router (Integrated) のルータ インターフェイスを設定するには、次の手順を実行します。

一般的に、VLAN 間通信には 2 つのインターフェイスが必要です。 ただし、Intercloud Fabric Router (Integrated) の場合、管理 VLAN はルーティング可能なので、1 つのルータ インターフェイスのみ追加する必要があります。

### はじめる前に

- Intercloud Fabric Cloud を作成し、Intercloud Fabric Router (Integrated) サービスを有効にしておきます。
- PNSC GUI で、Intercloud Fabric Router (Integrated) が *Running* 状態であることを確認します。

### 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] 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、[Resource Management] > [Managed Resources] の順に選択します。

**ステップ 5** [IcfCloud] という名前のテナント組織を選択します。

**ステップ 6** [Network Services] タブを選択します。
さまざまな Intercloud Fabric Router (Integrated) インスタンスで実行中のすべての Intercloud Fabric Cloud インスタンスが一覧表示されます。

**ステップ 7** インスタンス を選択し、[Edit Edge Router] を選択します。
[Edit Edge Router] ウィザードが表示されます。

**ステップ 8** [Edit Edge Router] に次のフィールドを表示します。

| 名前 | 説明 |
|---|---|
| [Name] フィールド | ルータの名前。 親のIntercloud Fabric Cloud インスタンスと同じ名前です。 |
| [Description] フィールド | ルータの説明。 |
| [Host Name] フィールド | ホスト名。 親のIntercloud Fabric Cloud インスタンスと同じ名前です。 |
| [Maangement IP] フィールド | 管理インターフェイスの IP アドレス。 |
| [Platform Type] フィールド | 統合ゲートウェイ。 このフィールドには、Intercloud Fabric Router (Integrated) の機能を提供する基盤のプラットフォームが表示されます |
| [Device Profile] ボタン | ルータのデフォルトのデバイス プロファイル。<br>（注） デフォルトでは、[defaultIG] という名前のデバイス プロファイルが選択されます。 [Device Profile] への参照および実際の [defaultIG] プロファイルを変更しないでください。 どちらかを変更すると、Intercloud Fabric Router (Integrated) インスタンスの *Config Status* が *failed-to-apply* に変更される可能性があります。 これは、Intercloud Fabric Router (Integrated) が [Device Profile] のポリシーをサポートしていないためです。 |
| [Device Service Profile] ボタン | ルータのデフォルトのデバイス サービス プロファイル。<br>このルータ インスタンス固有のスタティック ルーティング ポリシーと NAT ポリシーの組み合わせをサポートするには、各自が作成した別のデバイス サービス プロファイルを選択する必要があります。 |
| **Status（ステータス）** | |

| 名前 | 説明 |
|---|---|
| [Association Status] フィールド | ステータス値 [associating] は、ルータ インスタンスがまだ作成されていないことを示します。このステータスは、ルータインスタンスを作成するために、PNSC が関連する ICF クラウドインスタンスに接続を試みていることを示しています。 このステータスは、ICF クラウドインスタンスの電源がオンになり、サイト間トンネルのステータスが *[UP]* になるまで続く場合があります。<br>ステータス値 [associated] は、ルータ インスタンスが作成済みであることを示します。 |
| [Config Status] フィールド | ステータス値 [ok] は、ルータが正しく設定されていることを示します。<br>ステータス値 [failed to apply] は、ルータが正しく設定されていないことを示します。 設定に失敗した原因を調べるには、[Fault] タブをクリックします。 |
| [Reachable] フィールド | ステータス値 [Yes] は、PNSC がルータと通信可能であることを示します。<br>ステータス値 [No] は、PNSC がルータと通信できないことを示します。 |
| **[VM Access]** | |
| [User Name] フィールド | ルータにアクセスするための [admin] ユーザ名。 |
| [Password] フィールド | Intercloud Fabric で使用されるパスワード。 すべての Intercloud Fabric Router (Integrated) のパスワードが、Intercloud Fabric 用のパスワードと同じです。 Intercloud Fabric Router (Integrated) のパスワードを変更しないことをお勧めします。 |
| [Confirm Password] フィールド | パスワード。 |

**ステップ 9** [Network Interfaces] タブをクリックします。

**ステップ 10** [Add Interfaces] をクリックします。

**ステップ 11** [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 | インターフェイスの名前。 名前は 15 文字までです。 |
| [Description] フィールド | 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。<br>（注） ルータ インスタンスで NAT 設定をサポートするには、[Public Cloud] タイプが必要です。 1 つの [Public Cloud] タイプのインスタンスだけがサポートされます。<br>（注） [Ethernet] タイプのインターフェイスを作成した後は、Admin State、Use As Default Gateway、IP Address、Extend Default Gateway、Enterprise Gateway などの属性のみ変更できます。<br>[Public Cloud] タイプのインターフェイスを作成した後は、Admin State などの属性のみ変更できます。 [Public Cloud] タイプのインターフェイスは、インターネットへの接続が不要な場合にのみ削除する必要があります。 |
| [Admin State] オプション ボタン | インターフェイスの管理状態を選択します。<br>[Public Cloud] タイプのインターフェイスのデフォルト値は、[Enabled] です。 ステータスを [Disabled] に変更するとルータ インターフェイスがシャット ダウンするため、そのインターフェイスを介したトラフィックのルーティングと NAT 変換が無効になります。 |

| 名前 | 説明 |
|---|---|
| [Interface Service Profile] ボタン | デフォルトのインターフェイス サービス プロファイルが選択されます。<br>（注） デフォルトでは、[defaultIG] という名前のインターフェイス サービス プロファイルが選択されます。 [Device Profile] への参照および実際の [defaultIG] プロファイルを変更しないでください。 どちらかを変更すると、Intercloud Fabric Router (Integrated) インスタンスの *Config Status* が *failed-to-apply* に変更される可能性があります。 これは、Intercloud Fabric Router (Integrated) が [Interface Service Profile] のポリシーをサポートしていないためです。 |
| [Mode] オプション ボタン | デフォルトでは、[Trunk] が選択され、変更できません。 |
| [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 プロファイルが選択されます。 ポート プロファイルは、親の Intercloud Fabric Cloudインスタンスと同じポートプロファイルが使用され、変更できません。 |
| [Category] オプション ボタン | デフォルトでは、[Tagged Interface] が選択されます。 |
| [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。<br>管理 VLAN ではインターフェイスを作成できません。 |
| [Use As Default Gateway] チェックボックス | 関連するサブネットワークで起動するクラウド仮想マシンのデフォルト ゲートウェイとしてインターフェイスを設定するには、[Use As Default Gateway] チェックボックスをオンにします。 |

| 名前 | 説明 |
|---|---|
| [IP Address] フィールド | プライマリ IPアドレス。 Intercloud Fabric Router (Integrated) ではセカンダリの設定サポートされません。<br>このオプションは、[Use As Default Gateway] チェックボックスをオンにした場合に使用できます。 |
| [Subnet Mask] フィールド | IP アドレスのサブネット マスク。<br>このオプションは、[Use As Default Gateway] チェックボックスをオンにした場合に使用できます。 |
| [Extend Default Gateway] チェックボックス | プロバイダークラウドに移行された仮想マシンのデフォルト ゲートウェイとしてルータ インスタンスが動作できるようにするには、このチェックボックスをオンにします。<br>.<br>このオプションは、[Use As Default Gateway] チェックボックスをオンにした場合に使用できます。 |
| [Gateway] フィールド | ゲートウェイ IP アドレス。<br>このオプションは、[Use As Default Gateway] チェックボックスをオンにした場合に使用できます。 |

**ステップ 12** [OK] をクリックします。

# スタティック ルーティングの設定

Intercloud Fabric では、Intercloud Fabric Router (Integrated) のスタティック ルートを設定できます。

スタティック ルートのルーティング ポリシーを設定すると、対象となるルータ インスタンスに存在するエッジ ルータ デバイス プロファイルからそのルーティング ポリシーを選択して、ルータ インスタンスに適用できます。

### はじめる前に

対象となる Intercloud Fabric Router (Integrated) のエッジ ルータ デバイス プロファイルが存在すること。

### 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。
Prime Network Services Controller GUI が表示されます。

**ステップ 4** Prime Network Services Controller GUI で、[Policy Management] > [Service Policies] > [root] > [icfCloud] > [Policies] > [Routing] の順に選択します。

**ステップ 5** [Add Routing Policy] をクリックします。
[Add Routing Policy] ウィンドウが表示されます。

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

（注） Intercloud Fabric Router (Integrated) に対して [Static Route] オプションのみがサポートされています。

| 名前 | 説明 |
|---|---|
| [Name] フィールド | ルーティング ポリシーの名前。 |
| [Description] フィールド | ルーティング ポリシーの説明。 |
| [Static Route] ドロップダウン リスト | 既存のスタティック ルートを選択するか、新しいスタティック ルートを作成します。 |

**ステップ 7** スタティック ルート ルーティング ポリシーを作成するには、次の手順を実行します。

a) [Add Static Route] をクリックします。

b) [Add Static Route] の次のフィールドに値を入力します。

| 名前 | 説明 |
|---|---|
| [Destination Network] フィールド | 宛先の IP ルート プレフィックスおよびプレフィックス マスク。<br>このフィールドには「0.0.0.0」を入力できますが、Intercloud Fabric Router (Integrated) に関連付けると、ポリシーは失敗します。 |

| 名前 | 説明 |
|---|---|
| [Forwarding (Next Hop)] フィールド | 宛先ネットワークに到達するために使用可能なネクスト ホップの IP アドレス。<br>Intercloud Fabric Router (Integrated) に対して [Forwarding Interface] フィールドはサポートされていません。 |
| [Distance Metric] フィールド | ディスタンス メトリック。 |

**ステップ 8** [OK] をクリックします。

**ステップ 9** Prime Network Services Controller GUI で、[Policy Management] > [Service Policies] > [root] > [icfCloud] > [Edge Router] > [Device Service Profiles] の順に選択します。

**ステップ 10** [Add Router Device Service Profile] をクリックします。
[Add Router Device Service Profile] ウィンドウが表示されます。

**ステップ 11** [Add Router Device Service Profile] 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 | デバイス サービス プロファイルの名前。 |
| [Description] フィールド | デバイス サービス プロファイルの説明。 |
| [Routing Policy] ドロップダウン リスト | 既存のルーティング ポリシー セットを選択するか、新しいポリシー セットを作成します。 |

**ステップ 12** プロファイルを Intercloud Fabric Router (Integrated) に関連付けるには、[Resource Management] > [Managed Resources] > [tenant] の順に選択します。

**ステップ 13** Intercloud Fabric Router (Integrated) を選択し、[Edit Edge Router] を選択します。
[Edit Edge Router] ウィザードが表示されます。

**ステップ 14** [Edit Edge Router] で、[Device Service Profile] ボタンをクリックします。 [Select Router Device Profile] ウィンドウでデバイス プロファイルを選択します。

**ステップ 15** [OK] をクリックします。

**ステップ 16** 設定を確認するには、次の手順を実行します。

a) Intercloud Fabric Router (Integrated) の [Config Status] が *Running* であることを確認します。

b) [Config Status] が *failed-to-apply* である場合は、[Edit Edge Router] > [Faults] の順に選択し、[Description] フィールドで、設定が失敗した原因を調べます。

# Intercloud Fabric Router (Integrated) のネットワーク アドレス変換について

Intercloud Fabric 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ネットワーク アドレス変換（NAT）ポリシーをサポートしています。 これらのポリシーは、両方の IP アドレス変換方式（スタティックとダイナミック）をサポートしています

（注） Intercloud Fabric Router (Integrated) は、Microsoft Azure クラウドでのみサポートされます。

Intercloud Fabric では、次に示すポリシー項目を設定できます。

- NAT ポリシー セット：エッジ ルータ デバイス サービス プロファイルに関連付けることができるゼロ個以上の NAT ポリシー グループ。 ルータ インスタンスに対してデバイス サービス プロファイルの NAT ポリシー セットを使用すると、ポリシー セットのすべての NAT ポリシーがルータ インスタンスに適用されます。
- NAT ポリシー：ゼロ個以上の NAT ルール。それぞれのアクション タイプは Static または Dynamic になります。

Intercloud Fabric Router (Integrated) の NAT を設定する際は、次のガイドラインに従ってください。

- 宛先 NAT を設定する場合は、次のようにスタティック NAT ルールを作成します。
  1. IP アドレス、プロトコル、およびポートに対して EQ 演算子を使用して、宛先のみ一致条件を設定します。
  2. 変換された宛先 IP アドレスに対して、親 Intercloud Fabric Switch に割り当てられているプロバイダー プライベート IP アドレスを使用します。
- 送信元 NAT を設定する場合は、次のようにダイナミック NAT ルールを作成します。
  1. インターネット アクセスが必要なクラウド VM のサブネットワークに対応する、送信元のみ一致条件を設定します。
  2. アドレス変換を設定する場合は、[Interface Overload] チェックボックスをクリックし、[Public Cloud Interface] を選択します。

## Intercloud Fabric Router (Integrated) の NAT ポリシーの設定

Intercloud Fabric Router (Integrated) の NAT ポリシーを設定するには、次の手順を実行します。

### はじめる前に

- Intercloud Fabric Router (Integrated) でパブリック クラウド インターフェイスを作成します。

- NAT の設定対象となる Intercloud Fabric Router (Integrated) インスタンスのエッジ ルータ デバイス サービス プロファイルを作成します。

### 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。
Prime Network Services Controller GUI が表示されます。

**ステップ 4** [Policy Management] > [Service Profiles] > [root] > [icfCloud] > [Edge Router] > [Device Service Profiles] の順に選択します。

**ステップ 5** Intercloud Fabric Router (Integrated) 用に作成したデバイス サービス プロファイルを選択し、[Edit] をクリックします。

**ステップ 6** [Edit Router Device Service Profile] ウインドウで、[NAT Policy Set] ドロップダウン リストから既存の NAT ポリシーセットを選択するか、[Add NAT Policy Set] をクリックして NAT ポリシーセットを作成します。

**ステップ 7** （任意） [Add NAT Policy Set] をクリックして、NAT ポリシー セットを作成します。

**ステップ 8** （任意） [Add NAT Policy Set] 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 | 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 NAT Policy] アイコン | NAT ポリシーを追加するには、既存の NAT ポリシーを選択するか、または [Add NAT Policy] をクリックします。 |

**ステップ 9** （任意） [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 | 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。 |

| 名前 | 説明 |
|---|---|
| [Add Rule] アイコン | NAT ポリシーにルールを追加するには、既存のルールを選択するか、[Add Rule] をクリックします。 |

**ステップ 10** （任意） [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 | Description |
|---|---|
| 名前 | 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。<br>新しい条件を追加するには、[Add Rule Condition] をクリックします。<br>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。<br>（注） Source Match（送信元の一致）条件は、送信元 NAT の使用に対して Dynamic タイプの NAT Action を指定する場合にのみ使用します。<br>IP アドレスに対してサポートされている演算子は、EQ および PREFIX です。 ネットワーク ポートに対してサポートされている演算子は EQ、NEQ、GT、LT ですが、送信元の一致条件に対してネットワーク ポートを使用することは想定されていません。 |

| フィールド | Description |
|---|---|
| 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。<br>新しい条件を追加するには、[Add Rule Condition] をクリックします。<br>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。<br>（注） Destination Match（宛先の一致）条件は、宛先 NAT の使用に対して Static タイプの NAT Action を指定する場合にのみ使用します。<br>IP アドレスおよびポートに対してサポートされている演算子は、EQ だけです。 宛先 NAT の使用においては、IPアドレスとポートの両方の一致条件が必要です。 |
| Protocol | ルールが適用されるプロトコルを指定します。<br>• 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。<br>• 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。<br>1 [Any] チェックボックスをオフにします。<br>2 [Operator] ドロップダウン リストから [Equal] を選択します。<br>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** | |
| 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。 |

| フィールド | Description |
|---|---|
| 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。<br>• Resolved Source IP Pool<br>• Resolved Source Port Pool<br>• Resolved Destination IP Pool<br>• Resolved Destination Port Pool<br>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。<br>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 11 を参照してください。<br>Intercloud Fabric Router (Integrated) でダイナミック NAT を使用する場合は、[Overload Interface] チェックボックスをオンにして、使用するパブリック クラウド インターフェイスを選択します。 |
| NAT Options | Intercloud Fabric Router (Integrated) では使用できません。 |

**ステップ 11** （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。<br>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。<br>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。 |

| フィールド | 説明 |
|---|---|
| Attribute Type | 使用可能な属性タイプ（読み取り専用）。<br>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。 |
| Attribute Name | 選択した属性タイプに対して使用可能な属性名（読み取り専用）。 |
| **[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 12** [OK] をクリックします。

**ステップ 13** プロファイルを Intercloud Fabric Router (Integrated) に関連付けるには、[Resource Management] > [Managed Resources] > *[tenant]* の順に選択します。

**ステップ 14** Intercloud Fabric Router (Integrated) を選択し、[Edit Edge Router] を選択します。
[Edit Edge Router] ウィザードが表示されます。

**ステップ 15** [Edit Edge Router] で、[Device Service Profile] ボタンをクリックします。 [Select Router Device Profile] ウィンドウでデバイス プロファイルを選択します。

**ステップ 16** [OK] をクリックします。

**ステップ 17** 設定を確認するには、Intercloud Fabric Router (Integrated) CLI にログインし、**show intercloud ig tech-support** コマンドを入力します。

# Intercloud Fabric Router (Integrated) のインストールの確認

Intercloud Fabric Router (Integrated) 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 の CLI にログインします。

**ステップ 2** **show intercloud ig tech-support** コマンドを入力して、インストールを確認します。

第 9 章

# Cisco Intercloud Fabric のアップグレード

This chapter contains the following sections:


- Cisco Intercloud Fabric のアップグレードについて，195 ページ
- 前提条件，195 ページ
- Intercloud Fabric のアップグレード ワークフロー，196 ページ


## Cisco Intercloud Fabric のアップグレードについて

Cisco Intercloud Fabric リリース 2.2.1 へのアップグレードは、Cisco Intercloud Fabric 2.1.2 から 2.2.1 へのアップグレードのみがサポートされています。

Cisco Intercloud Fabric 用のアップグレード ソフトウェアは、Cisco.com の Intercloud Fabric Download Software ページから入手できます。

## 前提条件

- アップグレード中にサービス リクエストが一切実行されないようにします。 アップグレードを開始する前に、すべてのサービス リクエストを完了させる必要があります。
- HA モードで展開されている Intercloud Fabric Cloud の場合は、Intercloud Fabric スイッチと Intercloud Fabric Extender をアクティブまたはスタンバイ 状態にしておく必要があります。これらが到達可能であることも確認してください。
- HA モードで展開されている Intercloud Fabric VSM の場合は、HA ペアが正常であること、VSM がアクティブまたはスタンバイ状態であること、およびどちらもオンライン状態であることを確認します。
- Intercloud Fabric Director の管理者パスワードを変更して Prime Network Services Controller の管理者パスワードと同一にします。 パスワードを変更するには、Intercloud Fabric Cloud GUI にログインし、[Admin] > [Password] の順に選択します。

# Intercloud Fabric のアップグレード ワークフロー

Intercloud Fabricのアップグレードには、次のタスクが含まれます。

手順

**ステップ 1** Intercloud Fabric Directorアップグレードの前提条件を満たしていることを確認する。
前提条件, （195 ページ） を参照してください。

**ステップ 2** Intercloud Fabric のアップグレード ソフトウェア バンドルをダウンロードする。
Intercloud Fabric アップグレード ソフトウェア バンドルのダウンロード, （196 ページ） を参照してください。

**ステップ 3** Upgrade VM を VMware 5.1 または 5.5 ESXi ホストに展開する。
VM の展開とアップグレード, （197 ページ） を参照してください。

**ステップ 4** Upgrade VM のネットワークを設定する。
Upgrade VM のネットワークの設定, （198 ページ） を参照してください。

**ステップ 5** Intercloud Fabric 2.2.1 の1 つの VM ファイルをダウンロードする。
1 つの Intercloud Fabric VM イメージのダウンロード, （199 ページ） を参照してください。

**ステップ 6** `setup_info` ファイルを設定する。
setup_info ファイルの設定, （200 ページ） を参照してください。

**ステップ 7** Intercloud Fabric のアップグレード スクリプトを実行する。
Intercloud Fabric のアップグレード, （202 ページ） を参照してください。

**ステップ 8** Intercloud Fabric のコンポーネントをアップグレードする。
Intercloud Fabric コンポーネントのアップグレード, （204 ページ） を参照してください。

**ステップ 9** サービス VM をアップグレードする。
サービス VM のアップグレード, （205 ページ） を参照してください。

# Intercloud Fabric アップグレード ソフトウェア バンドルのダウンロード

Cisco.com から Intercloud Fabric アップグレード ソフトウェア バンドルをダウンロードするには、次の手順を実行します。

### 手順

**ステップ 1** ブラウザを使用して https://software.cisco.com/download/navigator.html に移動し、[Cloud and Systems Management] > [Cloud Management] > [Intercloud Fabric] > [Intercloud Fabric for Business] の順に選択します。

**ステップ 2** Intercloud Fabric のアップグレードイメージをダウンロードします（`icfb-k9-upgrade-2.2.1-pkg.zip`）。

**ステップ 3** ダウンロードしたアップグレードイメージファイルを解凍し、`icfb-k9-upgrade-2.2.1.zip` ファイルを取得します。

**ステップ 4** `icfb-k9-upgrade-2.2.1.zip` ファイルを解凍し、次のファイルを取得します。

- `ICF_UPGRADE_VM.ova`：Intercloud Fabric のアップグレードを補助する Upgrade VM を VMware 上に展開します。
- `upgrade-icfb-infra-2.2.1.tar`：Intercloud Fabric をアップグレードした後、Intercloud Fabric のコンポーネントのアップグレードに使用されます。

**ステップ 5** VMware vCenter クライアントが存在するホストに `ICF_UPGRADE_VM.ova` ファイルをコピーします。

**ステップ 6** 同じホストに `upgrade-icfb-infra-2.2.1.tar` ファイルをコピーします。

# VM の展開とアップグレード

ここでは、Intercloud Fabric をアップグレードする手順の一部として、VMware ESXi ホストに Upgrade VM を展開する方法について説明します。

### はじめる前に

`ICF_UPGRADE_VM.ova` ファイルに VMware ホストからアクセスできることを確認します。

### 手順

**ステップ 1** VMware vSphere クライアントで、Upgrade VM を展開する ESXi ホストを選択します。

**ステップ 2** [File] > [Deploy OVF Template] を選択します。

**ステップ 3** `ICF_UPGRADE_VM.ova` ファイルを参照して選択し、[Next] をクリックします。

**ステップ 4** Upgrade VM 用のネットワークを選択する際は、Cisco Intercloud Fabric Director と Prime Network Services Controller が存在しているネットワークに、選択したポート グループが到達可能であることを確認します。

**ステップ 5** VM の残りの情報を入力し、[Summary] 画面の [Power on after deployment] チェックボックスをオンにします。

**ステップ 6** [Finish] をクリックします。
Upgrade VM が展開され、その電源がオンになります。

# Upgrade VM のネットワークの設定

Upgrade VM のネットワークを設定するには、次の手順を実行します。

### はじめる前に

Upgrade VM が展開され、実行していること。

### 手順

**ステップ 1** VMware vSphere クライアントで、Upgrade VM を右クリックして [Open Console] を選択します。

**ステップ 2** 次の資格情報を使用して VM にログインします。

- ユーザ名：root
- パスワード：sfish123

**ステップ 3** root プロンプトで、**ifconfig -a** コマンドを入力し、イーサネット インターフェイス名を取得します。
次のような情報が表示されます。

```
eth0   Link encap:Ethernet HWaddr 00:50:56:A1:68:5D
       inet addr:209.165.201.25 Bcast:209.165.201.31 Mask:255.255.255.224
       inet6 addr: fe80::250:56ff:fea1:685d/64 Scope:Link
       UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
       RX packets:7789859 errors:0 dropped:0 overruns:0 frame:0
       TX packets:759319 errors:0 dropped:0 overruns:0 carrier:0
```

```
        collisions:0 txqueuelen:1000
        RX bytes:5961703905 (5.5 GiB) TX bytes:6777958552 (6.3 GiB)
```

**ステップ 4** 編集用に /etc/sysconfig/network-scripts/ifcfg-ethX ファイルを開きます。 このファイルが存在しない場合は作成してください。

**ステップ 5** 必要なネットワーク情報（IP アドレス、ネットマスク、ゲートウェイ IP アドレスなど）を入力し、ファイルを保存して終了します。
入力は次の例のようになります。

```
DEVICE=eth0
TYPE=Ethernet
ONBOOT=yes
NM_CONTROLLED=yes
BOOTPROTO=static
IPADDR=209.165.201.25
NETMASK=255.255.255.224
GATEWAY=209.165.201.1
```

**ステップ 6** **ifconfig** コマンドを入力して、インターフェイスに正しい IP アドレスが割り当てられていることを確認します。

**ステップ 7** 編集用に /etc/resolv.conf ファイルを開き、次の情報を入力します。

- ドメイン名
- DNS サーバの IP アドレス。

**ステップ 8** **service network restart** コマンドを入力して、ネットワークを再開します。

**ステップ 9** Upgrade VM の IP アドレスをメモします。 このアドレスは Intercloud Fabric のアップグレードで必要になります。

# 1 つの Intercloud Fabric VM イメージのダウンロード

Cisco.com から Intercloud Fabric の 1 つの VM イメージをダウンロードするには、次の手順を実行します。

### 手順

**ステップ 1** ブラウザを使用して https://software.cisco.com/download/navigator.html に移動し、[Cloud and Systems Management] > [Cloud Management] > [Intercloud Fabric] > [Intercloud Fabric for Business] の順に選択します。

**ステップ 2** Intercloud Fabric の 1 つの VM イメージをダウンロードします（icfb-k9-2.2.1-pkg.zip）。

**ステップ 3** イメージファイルを解凍し、1 つの Intercloud Fabric 2.2.1 VM の展開に使用される icf-2.2.1.ova ファイルを取得します。

**ステップ 4** 次のようにして、Upgrade VM に icf-2.2.1.ova ファイルをコピーします。

a) Upgrade VM コンソールにログインします。
b) /var/www/html/patch ディレクトリに移動します。
c) SCP または FTP を使用して、/var/www/html/patch ディレクトリに icf-2.2.1.ova ファイルをコピーします。

# setup_info ファイルの設定

この手順では、アップグレードの準備として setup_info ファイルを設定する方法について説明します。

### 手順

**ステップ 1** Upgrade VM コンソールにログインします。 資格情報は次のとおりです。

- ユーザ名：root
- パスワード：sfish123

**ステップ 2** /root ディレクトリに移動します。

**ステップ 3** 次の表の情報を使用して、setup_info ファイルを編集します。

| パラメータ | 説明 | 例 |
|---|---|---|
| **[ICF] セクション**<br>このセクションでは VMware vCenter のパラメータを入力します。 | | |
| vc_ip | vCenter クライアントの IP アドレス。 | vc_ip = 209.165.201.20 |
| vc_user | vCenter クライアントのユーザ名。 | vc_user = root |
| vc_passwd | vCenter クライアントのパスワード。 | vc_passwd = *mypassword* |
| esx_host | Intercloud Fabric VM を展開するホストの IP アドレス。 | esx_host = 209.165.201.21 |
| datastore | Intercloud Fabric VM のデータ ストアの名前。 | datastore = "datastore1 (2)" |
| vm_name | Intercloud Fabric VM の名前。 | vm_name = "icf_209_165_201_25" |
| ip_addr | Intercloud Fabric VM に使用される IP アドレス。 | ip_addr = 209.165.201.25 |

| パラメータ | 説明 | 例 |
|---|---|---|
| network | Intercloud Fabric VM のイーサネット インターフェイスネットワークにアタッチするためのネットワーク名。 | network - "ICF Network" |
| subnet | Intercloud Fabric VM のサブネット マスク。 | subnet = "255.255.0.0" |
| gateway | Intercloud Fabric VM のゲートウェイ IP アドレス。 | gateway = "209.165.201.2" |
| domain_name | Intercloud Fabric VM のドメイン名。 | domain_name = "cisco.com" |
| dns_ip | Intercloud Fabric VM の DNS サーバの IP アドレス。 | dns_ip = "209.165.201.10" |
| ntp_ip | Intercloud Fabric VM の NTP サーバの IP アドレス。 | ntp_ip = "209.165.201.11" |
| timezone | Intercloud Fabric VM のタイム ゾーン。 | timezone = "America/Los_Angeles" |
| **[ICFD] セクション**<br>既存の Intercloud Fabric 2.1.2 のインストールから Intercloud Fabric Director の情報を入力します。新しい Intercloud Fabric Director VM はこれらと同じ値を使用します。 | | |
| icfd_vm_name | Intercloud Fabric 2.1.2 での Intercloud Fabric Director VM の名前。 | icfd_vm_name = abc-icfd |
| ip_addr | Intercloud Fabric 2.1.2 での Intercloud Fabric Director VM の IP アドレス。 | ip_addr = 209.165.201.24 |
| username | Intercloud Fabric 2.1.2 での Intercloud Fabric Director VM のユーザ名。 | username = admin |
| password | Intercloud Fabric 2.1.2 での Intercloud Fabric Director VM のパスワード。 | password = "*admin_password*" |
| **[PNSC] Section**<br>既存の Intercloud Fabric 2.1.2 のインストールから Prime Network Services Controller の情報を入力します。 新しい Prime Network Services Controller VM はこれらと同じ値を使用します。 | | |
| pnsc_hostname | Intercloud Fabric 2.1.2 での Prime Network Services Controller VM のホスト名。 | pnsc_hostname =123-pnsc |
| pnsc_vm_name | Intercloud Fabric 2.1.2 での Prime Network Services Controller VM の名前。 | pnsc_vm_name = 123-pnsc |

| パラメータ | 説明 | 例 |
|---|---|---|
| ip_addr | Intercloud Fabric 2.1.2 での Prime Network Services Controller VM の IP アドレス。 | ip_addr = 209.165.201.25 |
| username | Intercloud Fabric 2.1.2 での Prime Network Services Controller VM のユーザ名。 | username = admin |
| password | Intercloud Fabric 2.1.2 での Prime Network Services Controller VM のパスワード。 | password = "*pnsc_password*" |

**ステップ 4** `setup_info` ファイルを保存して終了します。

# Intercloud Fabric のアップグレード

Intercloud Fabric をアップグレードするには、次の作業を行うアップグレード スクリプトを実行します。

- 必要なサービス、ネットワーク、ポートプロファイル、および接続が利用可能であることを確認する。
- パッチを Intercloud Fabric Director に適用する。
- Intercloud Fabric Director と Prime Network Services Controller のデータベースをバックアップする。
- Cisco Intercloud Fabric の新しいバージョンをインストールする。
- Intercloud Fabric Director と Prime Network Services Controller のデータベースをリストアし、サービスを再起動する。
- 必要に応じて、`upgrade.log` ファイルを作成し、参照のためにそれを `/root` ディレクトリに格納する。

アップグレードを開始して、その進行状況を Upgrade VM コンソールでモニタできます。

## はじめる前に

次の内容を確認します。

- `setup_info` ファイルの値が正しいこと。
- `icf-2.2.1.ova` ファイルが Upgrade VM にコピーされ、`/var/www/html/patch` ディレクトリに存在していること。
- Upgrade VM の IP アドレスを入手していること。

### 手順

**ステップ 1** Upgrade VM コンソールにログインします。

**ステップ 2** /root ディレクトリに移動します。

**ステップ 3** 次のコマンドを入力して、Intercloud Fabric をアップグレードします。

```
./ICF_Upgrade.py
```

アップグレード スクリプトが起動し、その進行状況をコンソールでモニタできます。 アップグレードが完了すると、成功メッセージが表示されます。 出力例については、Intercloud Fabric のアップグレードの出力例, （203 ページ） を参照してください。
スクリプトが失敗し、エラー メッセージが表示された場合は、エラーを確認して、特定された問題を修復し、スクリプトを再実行します。

### 次の作業

Intercloud Fabric コンポーネントのアップグレード, （204 ページ）に進みます。

## Intercloud Fabric の アップグレードの出力例

以下は、Intercloud Fabric アップグレード スクリプトの実行中に表示される出力の例です。

```
[root@localhost ~]# ./ICF_Upgrade.py
2015-04-24 10:53:08,396 - __main__ - INFO - ################Upgrade procedure################
2015-04-24 10:53:08,396 - __main__ - INFO - Verfying whether all required images are present
 to start the upgrade...
2015-04-24 10:53:08,867 - __main__ - INFO - verifying FTP and HTTP services running
2015-04-24 10:53:08,884 - __main__ - INFO - Logging into ICFD and checking services
/root/.ssh/known_hosts updated.
Original contents retained as /root/.ssh/known_hosts.old
2015-04-24 10:53:21,812 - __main__ - INFO - All services are running on icfd after 10 seconds
2015-04-24 10:53:21,813 - __main__ - INFO - Logging into PNSC and checking services
/root/.ssh/known_hosts updated.
Original contents retained as /root/.ssh/known_hosts.old
2015-04-24 10:53:28,304 - __main__ - INFO - verfying PNSC API connect (required for PNSC
DB backup)
2015-04-24 10:53:28,624 - __main__ - INFO - Verifying gateway ip is pingable
2015-04-24 10:53:35,674 - __main__ - INFO - 209.165.201.1 is pingable in 5 seconds
2015-04-24 10:53:35,674 - __main__ - INFO - Verifying domain name is pingable, which means
 dns ip is right
2015-04-24 10:53:42,754 - __main__ - INFO - cisco.com is pingable in 5 seconds
2015-04-24 10:53:42,754 - __main__ - INFO - Verifying ICF VM ip is not in use already
2015-04-24 10:54:06,803 - __main__ - INFO - Verifying there is no VM/Folder/ResourcePool
with same name as ICF on Vcenter
2015-04-24 10:54:07,325 - __main__ - INFO - Verifying the ICFD, PNSC VM names are correct
on Vcenter
2015-04-24 10:54:07,691 - __main__ - INFO - Verifying the ESX hostname and Datastore are
correct on Vcenter
2015-04-24 10:54:07,756 - __main__ - INFO - Verifying OVFTOOL not returning any error with
 given config to create the ICF VM
2015-04-24 10:54:11,829 - __main__ - INFO - Logging into ICFD...
.
.
.
.
.
```

```
Original contents retained as /root/.ssh/known_hosts.old
2015-04-24 12:27:59,167 - __main__ - INFO - All services in PNSC are running now after 5
seconds
2015-04-24 12:27:59,167 - __main__ - INFO - Stopping ICFD services...
2015-04-24 12:28:00,078 - __main__ - INFO - Starting ICFD services...
2015-04-24 12:29:43,882 - __main__ - INFO - All services are running on icfd after 100
seconds
2015-04-24 12:29:43,882 - __main__ - INFO - Upgrade operation completed successfully...
Please login to ICFD UI to start upgrade of infra components
```

# Intercloud Fabric コンポーネントのアップグレード

Intercloud Fabric VSM、Intercloud Fabric Extender、Intercloud Fabric など、Intercloud Fabric Switch コンポーネントをアップグレードするには、次の手順を実行します。 サービス VM のアップグレードについては、サービス VM のアップグレード, （205 ページ） を参照してください。

## はじめる前に

- Cisco.com からアップグレード ソフトウェアをダウンロードしておきます（Intercloud Fabric アップグレード ソフトウェア バンドルのダウンロード, （196 ページ） を参照）。
- `upgrade-icfb-infra-2.2.1.tar` ファイルをホストにコピーしておきます（Intercloud Fabric アップグレード ソフトウェア バンドルのダウンロード, （196 ページ） を参照）。
- Intercloud Fabric をアップグレードしておきます（Intercloud Fabric のアップグレード, （202 ページ） を参照）。

## 手順

**ステップ 1** Intercloud Fabric 2.2.1 GUI 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、[Upgrade ICFD Components] をクリックします。
[Upgrade ICFD Components] ウィンドウが表示されます。

**ステップ 4** [Browse] をクリックして、デスクトップにダウンロードした `upgrade-icfb-infra-2.2.1.tar` ファイルを選択し、[Upload] をクリックしてそのファイルをアップロードします。
ファイルのアップロードが完了すると、確認メッセージが表示されます。

**ステップ 5** [Process Bundle] をクリックします。
[Upgrade ICFD Components] ウィンドウに、アップグレードした Intercloud Fabric コンポーネントが一覧表示されます。

**ステップ 6** [Upgrade] をクリックして、Intercloud Fabric コンポーネントをアップグレードします。
アップグレードの進行中は、他のサービス リクエストを作成しないでください。

**ステップ 7** タスクの状態を表示するには、次の手順を実行します。

a) [Infrastructure] タブで、タスクのサービス リクエスト番号を検索します。

b) [Organizations] > [Service Requests] の順に選択します。

c) [Service Request] タブをクリックし、サービス リクエスト番号を検索するか、[Search] フィールドにサービス リクエスト番号を入力します。

d) [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 VM のアップグレード

次の項での説明に従ってサービス VM をアップグレードできます。


- Intercloud Fabric Router（CSR）のアップグレード, （205 ページ）
- Intercloud Fabric Firewall（VSG）のアップグレード, （206 ページ）


## Intercloud Fabric Router（CSR）のアップグレード

Intercloud Fabric Director を正常にアップグレード した後、次の手順に従って Intercloud Fabric Router（CSR）をアップグレードできます。

（注） Intercloud Fabric Router（CSR）にアタッチされている仮想マシンのトラフィックは、ルータのアップグレード中に影響を受けます。

### はじめる前に

Amazon クラウドのアカウントを持っている場合は、以下の手順を実行します。

1. Prime Network Services Controller GUI にログインし、[Intercloud Management] > [Infrastructure] > *[vpc]* の順に選択します。
2. VPC で、必要な Intercloud リンクを選択します。
3. 右側のペインで、[Network Services Templates] を選択し、CSR テンプレートと同期させます。応答として、v3.14.01 または CSR が表示されます。
4. CSR テンプレートとの同期後に v3.14.01 または CSR が表示されない場合は、資格情報を使用して Amazon からインスタンスをインスタンス化します。

### 手順

**ステップ 1** 管理者資格情報を使用して Prime Network Services Controller の GUI にログインします。

**ステップ 2** 次の手順で、既存の Intercloud Fabric Router（CSR）の設定の詳細をすべて記録します。 この情報は、アップグレードした Intercloud Fabric Router（CSR）を設定する際に必要になります。

a) GUI で、[Resource Management] > [Managed Resources] > *[tenant]* > *[csr]* の順に選択し、[Edit] をクリックします。
b) [Edit] ダイアログボックスの各タブの情報をすべて記録します。これには、各インターフェイスの名前、ホスト名、インターフェイス名、IP アドレス、VLAN とサブネット マスク、および各インターフェイスにアタッチされているデバイス サービス プロファイル、ルータのデバイス プロファイル、インターフェイス サービス プロファイルなどが含まれます。

**ステップ 3** [Resource Management] > [Managed Resources] > *[tenant]* の順に選択します。

**ステップ 4** 右側のペインで、アップグレードする Intercloud Fabric Router（CSR）を選択します。

**ステップ 5** [Delete] をクリックして、削除を確認します。

（注） この削除は Intercloud Fabric Router（CSR）にのみ影響を与えます。 Prime Network Services Controller のルータに関連付けられているポリシーには影響しません。

**ステップ 6** Prime Network Services Controller GUI からログアウトし、再度ログインします。

**ステップ 7** [Resource Management] > [Managed Resources] > *[tenant]* の順に選択します。

**ステップ 8** [Actions] > [Add Edge Router] の順に選択します。

**ステップ 9** ウィザードの [Properties] 画面で、Intercloud Fabric Router（CSR）名、デバイスとデバイス サービス プロファイル、ホスト名、パスワードなど、この手順の前半で収集した情報を追加します。

**ステップ 10** [Service Device] 画面で、[Instantiate in Cloud] を選択して、バージョン 03.14.01 のイメージを選択します。

**ステップ 11** 次の画面で、以前の Intercloud Fabric Router（CSR）が展開されていたクラウドを選択します。

**ステップ 12** [Interfaces] 画面で、この手順の前半で収集したインターフェイス情報を各インターフェイスに設定します。 この情報には、インターフェイス名、IP アドレス、サブネット マスク、VLAN タギング、インターフェイス サービス プロファイルなど含まれます。

**ステップ 13** [Summary] 画面で、情報が正確であることを確認し、[Finish] をクリックしてルータを展開します。

**ステップ 14** 展開が完了したら、Intercloud Fabric Router（CSR）のステータスとして「*Running*」と表示されていることを確認します。

**ステップ 15** NAT が設定されている場合は、新たに展開したルータのパブリック IP アドレスを取得し、既存の NAT の設定を更新してパブリック IP アドレスの変更を反映させます。

**ステップ 16** 次の手順で、設定がルータに適用されたことを確認します。

a) Prime Network Services Controller CLI から、管理 IP アドレスを使用し、管理者として Intercloud Fabric Router（CSR）コンソールにログインします。
b) **show run** コマンドを入力し、応答を検証して、設定が正しいことを確認します。

## Intercloud Fabric Firewall（VSG）のアップグレード

Intercloud Fabric Director を正常にアップグレードした後、次の手順に従って Intercloud Fabric Firewall（VSG）をアップグレードできます。

### 手順

**ステップ 1** 管理者資格情報を使用して Prime Network Services Controller の GUI にログインします。

**ステップ 2** 次の手順で、既存の Intercloud Fabric Firewall（VSG）の詳細をすべて記録します。 この情報は、アップグレードした Intercloud Fabric Firewall（VSG）を設定する際に必要になります。

a) GUI で、[Resource Management] > [Managed Resources] > *[tenant]* > *[vsg]* の順に選択し、[Edit] をクリックします。

b) セキュリティプロファイル、各（管理およびデータ）インターフェイスの名前、インターフェイス名、IP アドレス、サブネットマスク、ゲートウェイ、ポートグループなど、[Edit] ダイアログボックスの各タブの情報をすべて記録します。

c) [Security Profiles] タブで、セキュリティ プロファイルが表示されていることを確認します。

**ステップ 3** [Resource Management] > [Managed Resources] > *[tenant]* の順に選択します。

**ステップ 4** 右側のペインで、アップグレードする Intercloud Fabric Firewall（VSG）を選択します。

**ステップ 5** [Delete] をクリックして、削除を確認します。

**ステップ 6** Prime Network Services Controller GUI からログアウトし、再度ログインします。

**ステップ 7** [Resource Management] > [Managed Resources] > *[tenant]* の順に選択します。

**ステップ 8** [Actions] > [Add Compute Firewall] の順に選択します。

**ステップ 9** ウィザードで、この手順の前半で収集した情報を使用して、新しいIntercloud Fabric Firewall（VSG）を展開します。

**ステップ 10** Intercloud Fabric Firewall（VSG）が展開され、*Running* というステータスが表示されたら、次の手順で、ファイアウォールの設定が適切であることを確認します。

a) Prime Network Services Controller CLI から、管理 IP アドレスを使用し、管理者として Intercloud Fabric Firewall（VSG）コンソールにログインします。

b) [show running-config] コマンドを入力します。

c) 出力で次の点を確認します。

- 表示されたバージョンがアップグレードしたバージョンであること。
- ホスト名、IP アドレス、管理およびデータ インターフェイスの設定、セキュリティ プロファイルの情報が正確であること。
- `nsc-policy-agent` セクションに、正しい Prime Network Services Controller サーバ情報が表示されていること。

d) 次のように **show nsc-pa status** コマンドを入力して、NSC ポリシー エージェントが正常にインストールされたことを確認します。

```
firewall(config)# show nsc-pa status
NSC Policy-Agent status is - Installed Successfully. Version 2.0(0.72)-vsg
```

**ステップ 11** VSM コンソールにログインし、**show vservice brief** コマンドを入力して、サービス ノードのバインディングを確認します。

応答として、Intercloud Fabric Firewall（VSG）に関する情報、サービス パス、ファイアウォールにアタッチされている VM が表示されます。

第 10 章

# その他の情報


- Cisco Intercloud Fabric の関連資料，209 ページ
- マニュアルの入手方法およびテクニカル サポート，210 ページ
- マニュアルに関するフィードバック，211 ページ


## Cisco Intercloud Fabric の関連資料

ここでは、Cisco Intercloud Fabric に付属のマニュアルと次の URL から入手可能なマニュアルを列挙します。

http://www.cisco.com/c/en/us/support/cloud-systems-management/intercloud-fabric/tsd-products-support-series-home.html

### 一般情報

『*Cisco Intercloud Fabric Release Notes*』

### インストール & アップグレード

『*Cisco Intercloud Fabric* スタートアップ ガイド』

### ユーザ ガイド

『*Cisco Intercloud Fabric User Guide*』

### コンフィギュレーション ガイド

『*Cisco Intercloud Fabric Configuration Guide*』

『*Cisco Intercloud Fabric Firewall Configuration Guide*』

『*Cisco vPath and vServices Reference Guide for Intercloud Fabric*』

### プログラミング

『*Cisco Intercloud Fabric Director REST API Guide*』

### トラブルシューティング & アラート

『*Cisco Intercloud Fabric Troubleshooting Guide*』

### Cisco Intercloud Fabric Provider Platform

下記の Cisco Intercloud Fabric Provider Platform 用ドキュメントは、次の URL から入手可能です。

http://www.cisco.com/c/en/us/support/cloud-systems-management/intercloud-fabric/tsd-products-support-series-home.html

『*Cisco Intercloud Fabric Provider Platform Release Notes*』

『*Cisco Intercloud Fabric Provider Platform Installation Guide*』

『*Cisco Intercloud Fabric Provider Platform Administrator Guide*』

『*Cisco Intercloud Fabric Provider Platform Troubleshooting Guide*』

### Cisco Nexus 1000V のマニュアル

Cisco Nexus 1000V for VMware vSphere

Cisco Nexus 1000V for KVM

Cisco Nexus 1000V for Microsoft Hyper-V

### Cisco Virtual Security Gateway に関するマニュアル

Cisco Virtual Security Gateway

### Cisco Prime Network Services Controller のマニュアル

Cisco Prime Network Services Controller

### Cisco Cloud Services Router のマニュアル

Cisco Cloud Services Router 1000V

# マニュアルの入手方法およびテクニカル サポート

マニュアルの入手、Cisco Bug Search Tool（BST）の使用、サービス要求の送信、追加情報の収集の詳細については、『*What's New in Cisco Product Documentation*』を参照してください。このドキュメントは、http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html から入手できます。

『*What's New in Cisco Product Documentation*』では、シスコの新規および改訂版の技術マニュアルの一覧を、RSS フィードとして購読できます。また、リーダー アプリケーションを使用して、コンテンツをデスクトップに配信することもできます。 RSS フィードは無料のサービスです。

# マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載もれなどお気づきの点がございましたら、HTML ドキュメント内のフィードバック フォームよりご連絡ください。intercloud-fabric-doc-feedback@cisco.com。

ご協力をよろしくお願いいたします。