

vCloud Director テナント ポータル ガイド

2019 年 9 月 19 日

VMware Cloud Director 10.0

最新の技術ドキュメントは、VMware の Web サイト (<https://docs.vmware.com/jp/>)

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

ヴィエムウェア株式会社
105-0013 東京都港区浜松町 1-30-5
浜松町スクエア 13F
www.vmware.com/jp

Copyright © 2017-2020 VMware, Inc. All rights reserved. 著作権および商標情報。

目次

vCloud Director テナント ポータル ガイド 10

1 vCloud Director テナント ポータルの概要 11

- VMware vCloud Director について 11
- vCloud Director テナント ポータルへのログイン 12
- vCloud Director テナント ポータルのロールと権限 13
- vCloud Director テナント ポータルの使用 13
- vCloud Director グローバル検索の使用 14
- タスクの表示 15
- 進行中のタスクの停止 16
- イベントの表示 17

2 仮想マシンの操作 18

- 仮想マシンのアーキテクチャ 19
- 仮想マシンの表示と編集 20
- 新しいスタンドアロン仮想マシンの作成 20
- 仮想マシン コンソールを開く 22
 - クライアントでの VMware Remote Console のインストール 22
 - 仮想マシンのリモート コンソールを開く 23
 - Web コンソールを開く 23
- 仮想マシンでの電源の操作の実行 24
 - 仮想マシンのパワーオン 24
 - 仮想マシンのパワーオフ 24
 - ゲスト OS のシャットダウン 25
 - 仮想マシンのリセット 25
 - 仮想マシンのサスペンド 26
 - 仮想マシンのサスペンド状態の破棄 26
- 仮想マシンでの VMware Tools のインストール 27
- 仮想マシンの仮想ハードウェア バージョンのアップグレード 28
- 仮想マシンのプロパティの編集 28
 - 仮想マシンの全般プロパティの変更 28
 - 仮想マシンのハードウェア プロパティの変更 30
 - 仮想マシンのゲスト OS のカスタマイズ プロパティの変更 32
 - 仮想マシンの詳細プロパティの変更 35
- メディアの挿入 38
- メディアの取り出し 38
- 異なる vApp への仮想マシンのコピー 39
- 異なる vApp への仮想マシンの移動 39

仮想マシンのアフィニティと非アフィニティ	40
アフィニティ ルールおよび非アフィニティ ルールの表示	41
アフィニティ ルールの追加	41
非アフィニティ ルールの追加	42
アフィニティ ルールまたは非アフィニティ ルールの編集	42
アフィニティ ルールまたは非アフィニティ ルールの削除	43
仮想マシンの監視	43
スナップショットの操作	44
仮想マシンのスナップショットの作成	45
仮想マシンをスナップショットに戻す	46
仮想マシンのスナップショットの削除	46
仮想マシンのリースの更新	47
仮想マシンの削除	47

3 vApp の操作 49

vApp の表示	50
新規 vApp の構築	50
OVF パッケージからの vApp フォームの作成	52
vApp テンプレートからの vApp の作成	54
vApp を開く	55
vApps での電源の操作の実行	56
vApp のパワーオン	56
vApp のパワーオフ	56
vApp の停止	57
vApp のリセット	57
vApp のサスペンド	57
vApp の一時停止状態の破棄	58
vApp のプロパティの編集	58
vApp の全般プロパティの編集	58
vApp の詳細プロパティの編集	59
vApp を共有	60
vApp ネットワーク図の表示	61
vApp でのネットワークの作業	62
vApp ネットワークの表示	62
vApp ネットワークのフェンス	63
vApp へのネットワークの追加	63
vApp ネットワークのネットワーク サービスの構成	64
vApp ネットワークの削除	69
スナップショットの操作	69
vApp のスナップショットの作成	70
vApp をスナップショットに戻す	71

vApp のスナップショットの削除	71
vApp の所有者の変更	72
別の仮想データセンターへの vApp の移動	72
別の仮想データセンターへの停止した vApp のコピー	73
パワーオン状態の vApp のコピー	73
仮想マシンの vApp への追加	74
vApp の vApp テンプレートとしてのカタログへの保存	75
OVF パッケージとしての vApp のダウンロード	76
vApp リースの更新	77
vApp の削除	77

4 組織仮想データセンター ネットワークの管理 78

使用可能な組織 VDC ネットワークの表示	79
隔離された組織仮想データセンター ネットワークの追加	80
経路指定された組織仮想データセンター ネットワークの追加	81
直接の組織仮想データセンター ネットワークの追加	83
インポートされた NSX-T 論理スイッチを使用した組織 VDC ネットワークの追加	84
組織仮想データセンター ネットワークの全般設定の編集	84
組織仮想データセンター ネットワークの変換	85
経路指定された組織仮想データセンター ネットワークのインターフェイスの変換	86
組織仮想データセンター ネットワークに使用されている IP アドレスの表示	86
組織仮想データセンター ネットワーク IP プールへの IP アドレスの追加	87
組織仮想データセンター ネットワークで使用される IP アドレス範囲の編集または削除	88
組織仮想データセンター ネットワークの DNS 設定の編集	88
隔離された組織仮想データセンター ネットワークの DHCP の設定	89
ネットワークの既存の DHCP プールの編集または削除	90
組織仮想データセンター ネットワークのリセット	91
組織仮想データセンター ネットワークの削除	91

5 クロス仮想データセンター ネットワークの管理 93

データセンター グループの管理	94
共通の出力方向が設定されたデータセンター グループの作成と設定	94
フォルト ドメインの出力方向が設定されたデータセンター グループの作成と設定	97
データセンター グループの表示	99
仮想データセンターのデータセンター グループへの追加	99
データセンター グループからの仮想データセンターの削除	100
データセンター グループの同期	100
データセンター グループ内の出力方向ポイントと共通の出力方向の設定のスワップ	101
出力方向ポイントの Edge Gateway の置き換え	102
出力方向ポイントの削除	102
ルートおよび出力方向ポイントの同期	103

拡張ネットワークの管理	104
拡張ネットワークの追加	104
拡張ネットワークの表示または編集	105
拡張ネットワークの削除	106
拡張ネットワークの同期	106

6 vCloud Director テナントの高度なネットワーク機能 108

vCloud Director の高度なネットワークの概要	109
テナント ポータルを使用したファイアウォール構成	109
Edge Gateway のファイアウォール	110
NSX Data Center for vSphere Edge Gateway ファイアウォールの管理	111
分散ファイアウォール	114
テナント ポータルを使用した、組織仮想データセンターでの分散ファイアウォールの有効化	115
テナント ポータルを使用した分散ファイアウォール ルールの管理	116
Edge Gateway の DHCP の管理	119
DHCP IP プールの追加	120
DHCP バインディングの追加	121
NSX Data Center for vSphere Edge Gateway の DHCP リレーの設定	122
NSX Data Center for vSphere Edge Gateway の DHCP リレー構成の指定	123
テナント ポータルを使用したネットワーク アドレス変換の管理	124
SNAT または DNAT ルールの追加	125
高度なルーティングの設定	127
NSX Data Center for vSphere Edge Gateway のデフォルトのルーティング設定の指定	127
スタティック ルートの追加	129
OSPF の設定	130
BGP の設定	132
ルート再配分の設定	134
ロード バランシング	135
ロード バランシングについて	135
仮想プライベート ネットワークを使用したセキュアなアクセス	147
SSL VPN-Plus の設定	147
IPsec VPN の構成	160
L2 VPN の構成	166
Edge ゲートウェイからの L2 VPN サービス構成の削除	170
SSL 証明書の管理	171
Edge Gateway の証明書署名リクエストの生成	171
Edge Gateway 用に生成された CSR に対応する CA 署名付き証明書のインポート	173
自己署名サービス証明書の構成	174
SSL 証明書の信頼性検証のための Edge Gateway への CA 証明書の追加	174
Edge Gateway への証明書失効リストの追加	175
Edge Gateway へのサービス証明書の追加	176

オブジェクトのグループ分け (カスタム)	177
ファイアウォール ルールと DHCP リレー設定で使用するための IP アドレス セットの作成	177
ファイアウォール ルールで使用するための MAC アドレス セットの作成	178
ファイアウォール ルールで使用可能なサービスの表示	179
ファイアウォール ルールで使用可能なサービス グループの表示	180
Edge Gateway の統計情報とログ	181
統計情報の表示	181
ログの有効化	181
SSH コマンドラインによる Edge Gateway へのアクセスの有効化	182
セキュリティ タグの操作	183
セキュリティ タグの作成および割り当て	183
セキュリティ タグの割り当ての変更	184
適用されているセキュリティ タグの表示	185
セキュリティ タグの編集	185
セキュリティ タグの削除	186
セキュリティ グループの操作	187
セキュリティ グループの作成	187
セキュリティ グループの編集	188
セキュリティ グループの削除	190

7 NSX-T Data Center Edge Gateway の管理 191

NSX-T Edge Gateway へのファイアウォール グループの追加	191
NSX-T Edge Gateway ファイアウォール ルールの追加	192
NSX-T Edge Gateway での SNAT ルールまたは DNAT ルールの追加	193
NSX-T Edge Gateway での DNS フォワーダ サービスの設定	194
カスタム アプリケーション ポート プロファイルの作成	195

8 名前付きディスクの使用およびストレージ ポリシーの確認 196

名前付きディスクの作成および使用	196
名前付きディスクの作成	196
名前付きディスクの編集	197
仮想マシンへの名前付きディスクの接続	197
名前付きディスクの削除	198
ストレージ ポリシーのプロパティの確認	198

9 仮想データセンターのプロパティの確認 199

仮想データセンターのプロパティの確認	199
仮想データセンターのメタデータの確認	199

10 専用 vCenter Server インスタンスおよびプロキシの操作 201

プロキシ設定を使用したブラウザの設定	201
--------------------	-----

プロキシが設定されたコンポーネントのユーザー インターフェイスへのログイン 202

11 vApp テンプレートの操作 204

vApp テンプレートの表示 204

OVF ファイルからの vApp テンプレートの作成 205

vApp テンプレートへの仮想マシン配置ポリシーと仮想マシン サイズ変更ポリシーの割り当て 206

vApp テンプレートのダウンロード 207

vApp テンプレートの削除 207

12 メディア ファイルの操作 208

メディア ファイルのアップロード 208

メディア ファイルの削除 209

メディア ファイルのダウンロード 209

13 カタログの操作 210

カタログの表示 211

カタログの作成 211

カタログを共有 212

カタログの削除 213

カタログのメタデータの管理 213

カタログを発行 214

外部カタログへのサブスクライブ 214

サブスクライブしたカタログの場所の URL とパスワードの更新 215

サブスクライブしたカタログの同期 215

14 組織仮想データセンター テンプレートの操作 217

使用可能な仮想データセンター テンプレートの表示 217

テンプレートからの仮想データセンターの作成 218

15 ユーザー、グループ、ロールの管理 219

ユーザーの管理 219

ユーザーの作成 219

ユーザーのインポート 220

ユーザーの変更 221

ユーザー アカウントの有効化または無効化 222

ユーザーの削除 222

ロックされたユーザー アカウントのロック解除 223

グループの管理 223

グループのインポート 223

グループの削除 224

グループの編集 224

ロールと権限 225

事前定義ロールとその権限 225

事前定義グローバル テナント ロールの権限 227

カスタム テナント ロールの作成 232

カスタム テナント ロールの編集 233

ロールの削除 233

16 組織での SAML の ID プロバイダの使用の有効化 234

17 組織の管理 236

組織の名前と説明の編集 236

電子メール設定の変更 237

SMTP 設定のテスト 237

組織内の仮想マシンのドメイン設定の変更 238

複数のサイトの操作 238

マルチサイト展開の設定と管理 239

リースについて 240

組織内の vApp および vApp テンプレートのリース ポリシーの変更 240

組織内の仮想マシンのデフォルトの割り当て容量の変更 241

組織内のパスワードおよびユーザー アカウントのポリシーの変更 242

18 サービス ライブラリの操作 243

サービスの検索 243

サービスの実行 243

19 カスタム エンティティ定義の操作 245

カスタム エンティティの検索 245

カスタム エンティティ定義の編集 246

カスタム エンティティ定義の追加 246

カスタム エンティティ インスタンス 247

カスタム エンティティへのアクションの関連付け 248

カスタム エンティティ定義からのアクションの関連付け解除 248

カスタム エンティティの公開 249

カスタム エンティティの削除 250

vCloud Director テナント ポータル ガイド

『VMware vCloud Director テナント ポータル ガイド』は、VMware vCloud Director テナント ポータルの使用方法を説明しています。このリリースでは、テナント ポータルを使用して組織を管理したり、仮想マシン、vApp、vApp 内のネットワークを作成および構成することができます。vCloud Director 環境内で VMware NSX[®] for vSphere[®] によって提供される高度なネットワーク機能を設定することもできます。vCloud Director テナント ポータルを使用して、カタログ、vApp、仮想データセンター テンプレートの作成と管理、およびクロス仮想データセンター ネットワークの作成と管理を行うことができます。

対象読者

このガイドは、vCloud Director テナント ポータルの機能を使用するすべての方を対象としています。ここで記載されている情報は、テナント ポータルを使用して組織を管理し、仮想マシン、vApp、ネットワークなどを管理する組織管理者を主な対象としています。

VMware の技術ドキュメントの用語集

『VMware Technical Publications Glossary (VMware テクニカル ドキュメント用語集)』は、専門的な技術用語に関する用語集です。VMware の技術ドキュメントで使用される用語の定義については、<http://www.vmware.com/support/pubs> をご覧ください。

vCloud Director テナント ポータル の概要

1

テナント ポータルにログインすると、仮想マシンおよび vApp の作成から高度なネットワークの設定、および vRealize Orchestrator ワークフローの実行まで、さまざまなタスクを実行できます。

この章には、次のトピックが含まれています。

- VMware vCloud Director について
- vCloud Director テナント ポータルへのログイン
- vCloud Director テナント ポータルのロールと権限
- vCloud Director テナント ポータルの使用
- vCloud Director グローバル検索の使用
- タスクの表示
- 進行中のタスクの停止
- イベントの表示

VMware vCloud Director について

VMware vCloud Director では、Web ベースのテナント ポータルへのロールベースのアクセスが提供されるため、組織のメンバーが組織のリソースと連携して vApp や仮想マシンを作成したり操作できます。

組織にアクセスするには、vCloud Director システム管理者によってその組織が作成され、リソースが割り当てられ、さらにテナント ポータルにアクセスするための URL が提供されなければなりません。各組織には組織管理者が 1 名以上含まれ、メンバーの追加とポリシー設定や環境設定を行うことによって組織をセットアップします。組織がセットアップされると、非管理者ユーザーは、仮想マシンと vApp を作成、使用、および管理するためにログインできるようになります。

組織

組織は、ユーザー、グループ、およびコンピューティング リソースの集合で構成される管理単位です。ユーザーは、ユーザーの作成時またはインポート時に組織管理者が設定した認証情報を入力して、組織レベルで認証を受けます。システム管理者が組織を作成してプロビジョニングするのに対し、組織管理者は、組織のユーザー、グループ、およびカタログを管理します。

ユーザーとグループ

組織には、任意の数のユーザーおよびグループを含めることができます。ユーザーを作成するには、組織管理者がローカルに作成するか、ディレクトリ サービスからインポートします。グループは、ディレクトリ サービスからインポートする必要があります。組織内の権限は、ユーザーおよびグループに権限とロールを割り当てることによって管理されます。

仮想データセンター

組織仮想データセンターは、組織にリソースを提供します。仮想データセンターは、仮想システムを格納、デプロイ、および運用できる環境を提供します。仮想 CD および DVD メディアのストレージも提供します。組織は複数の仮想データセンターを持つことができます。

組織仮想データセンター ネットワーク

組織仮想データセンター ネットワークは、vCloud Director 組織仮想データセンター内にあり、組織内のすべての vApp から使用できます。組織仮想データセンター ネットワークにより、組織内の vApp は相互に通信できます。組織仮想データセンター ネットワークは、外部ネットワーク、または組織の内部の隔離されたネットワークに接続できます。組織仮想データセンター ネットワークを作成できるのはシステム管理者のみですが、組織管理者は、自らが提供するネットワーク サービスを含め、組織仮想データセンター ネットワークを管理することができます。

vApp ネットワーク

vApp ネットワークは vApp 内に存在しており、これにより vApp 内の仮想マシンは相互に通信できるようになります。vApp ネットワークを組織仮想データセンター ネットワークに接続すると、vApp は、組織内の他の vApp と通信できるほか、組織仮想データセンター ネットワークが外部ネットワークに接続されている場合には組織外の他の vApp と通信できます。

カタログ

組織は、カタログを使用して vApp テンプレートとメディア ファイルを格納します。カタログにアクセスできる組織のメンバーは、カタログの vApp テンプレートとメディア ファイルを使用して、独自の vApp を作成できます。組織管理者は、公開カタログから組織カタログに項目をコピーできます。

専用 vCenter Server インスタンス (SDDC) およびプロキシ

Software-Defined Data Center (SDDC) によって vCenter Server 環境全体がカプセル化されます。専用 vCenter Server インスタンスに、基盤となる環境からさまざまなコンポーネントへのアクセスを可能にする 1 つ以上のプロキシを含めることができます。システム管理者は 1 つ以上の専用 vCenter Server インスタンスを組織に公開できます。ユーザーは含まれているプロキシを使用して、プロキシが設定されたコンポーネントのユーザー インターフェイスまたは API にアクセスできます。

vCloud Director テナント ポータルへのログイン

組織に固有の URL を使用して、vCloud Director テナント ポータルにアクセスできます。

組織のテナント ポータルの URL がわからない場合は、組織管理者にお問い合わせください。サポートされているブラウザおよび構成については、vCloud Director リリース ノート を参照してください。

手順

- 1 Web ブラウザで、組織のテナント ポータル URL に移動します。
たとえば、<https://vcloud.example.com/tenant/myOrg> などです。
- 2 ユーザー名とパスワードを入力し、[ログイン] をクリックします。

vCloud Director テナント ポータルのロールと権限

vCloud Director には、事前設定されたユーザー ロールとその権限のセットが含まれています。vCloud Director テナント ポータルにアクセスできるロールは、任意の組織内にデフォルトで作成されたロールまたは組織管理者によって作成されたその他のロールです。

以下の組織ロールが割り当てられているユーザーは、テナント ポータルにアクセスできます。表示される項目と実行できるアクションは、ロールに関連付けられている権限によって異なります。

- 組織管理者
- カタログ作成者
- vApp 作成者
- vApp ユーザー
- コンソールのアクセスのみ

事前定義のロールおよびその権限については、[事前定義ロールとその権限](#) を参照してください。

vCloud Director テナント ポータルの使用

複数の仮想データセンターがある場合は、vCloud Director テナント ポータルにログインすると [仮想データセンター] ダッシュボード画面が表示されます。仮想データセンターが 1 つしかない場合は、vCloud Director テナント ポータルにログインするとデータセンターに直接移動します。

[仮想データセンター] ダッシュボード画面は vCloud Director マルチサイト機能の一部であり、テナントの物理的に分散されたクラウド環境を単一のエンティティとして表示できます。マルチサイトの詳細については、[複数のサイトの操作](#) を参照してください。

このダッシュボードは、単一の組織に限定せずに、vCloud Director 仮想データセンターおよびサイトをまとめて表示する統合ビューです。複数セルおよび複数組織の環境では、関連する他のすべての組織の仮想データセンターも表示できます。

注： テナント ユーザーは、権限に応じて組織のすべてのメンバー サイトまたは一部のサイトのみを表示できます。

組織に関する情報が概要リボンの一番上に表示されます。

 1 Sites	 1 Organizations	 4 Virtual Datacenters	 1 Running vApps	 1 Running VMs
--	--	--	---	--

組織管理者としてログインすると、以下が表示されます。

- サイト、組織、仮想データセンターの数

- 実行中の vApp および仮想マシンの合計数
- 使用されている CPU、メモリ、ストレージなどのハードウェア リソース

仮想データセンターは、カード ビューに表示されます。各カードには、vCenter Server が属している組織、vApp の数、仮想マシンの合計数、実行中の状態にある仮想マシンの数に関する情報が含まれています。カードにはデータセンターの使用可能な CPU、メモリ、ストレージ容量のほか、現在のリソースの割り当てと予約に関するリアルタイム メトリックも表示されます。

メイン メニュー (☰) から別のメニュー項目に移動できます。

メニュー項目	説明
データセンター	組織内の仮想データセンターが表示される[仮想データセンター]画面に移動します。
データセンター グループ	クロス仮想データセンター ネットワークを管理するには、[データセンター グループ]画面に移動します。デフォルトでは、このメニュー項目を表示できるのはシステム管理者のみです。
ライブラリ	vApp テンプレート、カタログ、メディア、およびその他の種類のファイルに関する統合ビューに移動します。これらのテンプレートおよびファイルは、仮想マシンや vApp をデプロイするために使用します。
管理	組織管理者が別の組織との信頼関係を作成できる、マルチサイト管理画面に移動します。
タスク	vCloud Director によって報告されたタスクを表示する [タスク]画面に移動します。
イベント	vCloud Director によって報告されたイベントを表示する [イベント]画面に移動します。
操作	[サービス ライブラリ]画面に移動します。[サービス ライブラリ]には、vRealize Orchestrator ワークフローを実行できる vCloud Director コンポーネントのグループが含まれています。

Branding vCloud OpenAPI を使用して、vCloud Director テナント ポータルをカスタマイズできます。vCloud OpenAPI の使用方法については、<https://code.vmware.com> の『vCloud OpenAPI スタート ガイド』ドキュメントを参照してください。

vCloud Director グローバル検索の使用

vCloud Director グローバル検索を使用して、環境内のオブジェクト名に対して名前または名前の一部で検索を実行できます。仮想マシンの IP アドレスが固定されている場合は、この IP アドレスで仮想マシンを検索することもできます。



事前設定されたオブジェクトのリストは次のとおりです。

- データセンター
- vApp テンプレート
- vApp
- 仮想マシン
- vApp ネットワーク
- カタログ

仮想マシンが DHCP によって割り当てられた IP アドレスを使用している場合、検索では、この IP アドレスを返しませんが、DHCP によって割り当てられた IP アドレスを持つ仮想マシンを検索する場合は、名前で検索する必要があります。

デフォルトでは、ローカル サイト内のオブジェクト内のみを検索できます。マルチサイト環境を使用している場合は、複数のサイト間で検索できます。

手順

- 1 vCloud Director テナント ポータルの右上隅にある [検索] () アイコンをクリックします。
- 2 (オプション) [固定] () アイコンをクリックして、検索パネルを固定します。
- 3 [検索] テキスト ボックスに、一致するオブジェクト名または仮想マシンの固定 IP アドレスを検索するための記号、名前の一部、または IP アドレスを入力します。
- 4 マルチサイト環境を使用している場合は、検索を実行するサイトを選択します。
- 5 [Enter]キーを押します。

結果

オブジェクト タイプごとに上位 5 つの一致した結果が表示されます。結果はアルファベット順に表示されます。

次のステップ

- さらに結果がある場合、これを表示するには、各オブジェクト タイプの下にある [さらにロード] をクリックします。
- 検索結果から特定のオブジェクトに関する詳細を表示するには、そのオブジェクトをポイントします。
- オブジェクトの設定の表示または変更など、特定のオブジェクトを管理するには、このオブジェクトをクリックします。オブジェクトに関する詳細が左側に表示されます。

タスクの表示

テナント ポータルでは、最近のタスクのリストと、その詳細およびステータスを表示できます。さらに、すべてのタスクのリストも表示できます。

デフォルトで、[最近のタスク] パネルはテナント ポータルの下部に表示され、最近実行されたタスクのリストが示されます。仮想マシンを作成するなどの目的で処理を開始すると、このパネルにタスクが表示されます。[最近のタスク] パネルを最小化しても、実行中または失敗した最近のタスクの数は表示されます。二重矢印をクリックすると、いつでも [最近のタスク] パネルを再度開くことができます。

タスク ビューにはすべてのタスクのリストが表示され、その実行日時と、正常に完了したかどうかが表示されます。環境内の問題のトラブルシューティングは、このビューから開始します。タスク ビューには、仮想マシンや vApp の作成など、長時間の処理が含まれます。

手順

- 1 メイン メニュー (≡) で [タスク] を選択するか、[最近のタスク] パネルで [他のタスク] をクリックします。
すべてのタスクのリストが、タスクの実行された日時およびタスクのステータスと共に表示されます。
- 2 タスクについて表示する詳細を変更するには、エディタ アイコン (📄) をクリックします。
- 3 (オプション) タスクの詳細を表示するには、タスクの名前をクリックします。
タスクの詳細には、失敗の理由 (タスクが失敗したとき) などの情報が含まれます。

詳細	説明
操作	実行された処理の名前。
ジョブ ID	タスクの ID。
タイプ	タスクの実行対象となったオブジェクト。たとえば、仮想マシンを作成した場合、タイプは <code>vm</code> です。
組織	組織名。
ステータス	Succeeded、Running、Failed などのタスクのステータス。
開始元	処理を開始したユーザー。
開始時刻	処理が開始された日付と時刻。
完了日時	処理が成功または失敗した日付と時刻。
サービス名前空間	<code>com.vmware.vcloud</code> などのサービス名。
詳細	タスクが失敗した理由。たとえば、仮想マシンのスナップショットの作成を試み、ストレージが十分でないために処理が失敗すると、タスクの詳細は次のようになります。要求された操作は、vDC のストレージ割り当て容量を超えます: ストレージ ポリシー「*」で残り 8,693 MB、要求された量 41,472 MB。

進行中のタスクの停止

必要なすべての設定を適用または確認する前に誤って処理を開始した場合は、進行中のタスクを停止できます。

デフォルトでは、[最近のタスク] パネルはポータルの下部に表示されます。仮想マシンを作成するなどの目的で処理を開始すると、このパネルにタスクが表示されます。

前提条件

[最近のタスク] パネルが開いている必要があります。

手順

- 1 長時間の処理を開始します。
長時間の処理とは、仮想マシンまたは vApp の作成、仮想マシンや vApp に対して実行される電源操作などの処理です。
- 2 [最近のタスク] パネルで、[キャンセル] アイコン (✕) をクリックします。
- 3 [タスクのキャンセル] ダイアログ ボックスで [OK] をクリックして、タスクをキャンセルすることを確認します。

結果



処理が停止します。

イベントの表示

ポータルでは、すべてのイベントのリストと、その詳細およびステータスを表示できます。

ポータルでイベントのステータスを表示するには、イベント ビューを使用します。イベント ビューには、イベントが発生した日時と、イベントが成功したかどうかが表示されます。イベント ビューには、ユーザーのログイン、オブジェクトの作成や削除など、1 回だけ発生するものが含まれます。

手順

- 1 メイン メニュー () から、[イベント] を選択します。
すべてのイベントのリストが、イベントの発生した日時およびイベントのステータスと共に表示されます。
- 2 イベントについて表示する詳細を変更するには、エディタ アイコン () をクリックします。
- 3 (オプション) イベントをクリックして、イベントの詳細を表示します。

詳細	説明
イベント	イベントの名前。 たとえば、仮想マシンを含めるように vApp を変更する場合、その処理全体を開始するイベントは <i>Task 'Modify vApp' start</i> です。
イベント ID	タスクの ID。
タイプ	タスクの実行対象となったオブジェクト。たとえば、仮想マシンを作成した場合、タイプは <i>vm</i> です。
ターゲット	イベントのターゲット オブジェクト。 たとえば、仮想マシンを含めるように vApp を変更する場合、 <i>Task 'Modify vApp' start</i> イベントのターゲットは <i>vdcUpdateVapp</i> です。
ステータス	Succeeded、Failed など、イベントの状態。
サービス名前空間	<i>com.vmware.vcloud</i> などのサービス名。
組織	組織の名前。
所有者	イベントをトリガしたユーザー。
発生日時	イベントが発生した日付と時刻。

仮想マシンの操作

2

仮想マシンとは、物理コンピュータのようにオペレーティング システムとアプリケーションを実行するソフトウェア コンピュータです。仮想マシンは、一連の仕様および構成ファイルで構成され、ホストの物理リソースでバックアップされています。すべての仮想マシンには、物理ハードウェアと同一の機能を提供する仮想デバイスがあり、移植性、管理性、およびセキュリティの点で優れています。

vCloud Director 仮想マシンでは、物理マシン上で実行できる操作に加え、仮想マシンの状態のスナップショットの取得やホスト間での仮想マシンの移動などの仮想インフラストラクチャ操作がサポートされています。

vCloud Director 9.5 以降、仮想マシンは IPv6 接続をサポートします。IPv6 ネットワークに接続された仮想マシンには IPv6 アドレスを割り当てることができます。

重要： 仮想マシンを操作するためのすべての手順は、カード ビューに記載されています。これらの手順では、複数の仮想データセンターがあることが前提となります。グリッド ビューから同じ操作を実行することも可能ですが、手順は多少異なることがあります。

この章には、次のトピックが含まれています。

- 仮想マシンのアーキテクチャ
- 仮想マシンの表示と編集
- 新しいスタンドアロン仮想マシンの作成
- 仮想マシン コンソールを開く
- 仮想マシンでの電源の操作の実行
- 仮想マシンでの VMware Tools のインストール
- 仮想マシンの仮想ハードウェア バージョンのアップグレード
- 仮想マシンのプロパティの編集
- メディアの挿入
- メディアの取り出し
- 異なる vApp への仮想マシンのコピー
- 異なる vApp への仮想マシンの移動
- 仮想マシンのアフィニティと非アフィニティ
- 仮想マシンの監視

- スナップショットの操作
- 仮想マシンのリースの更新
- 仮想マシンの削除

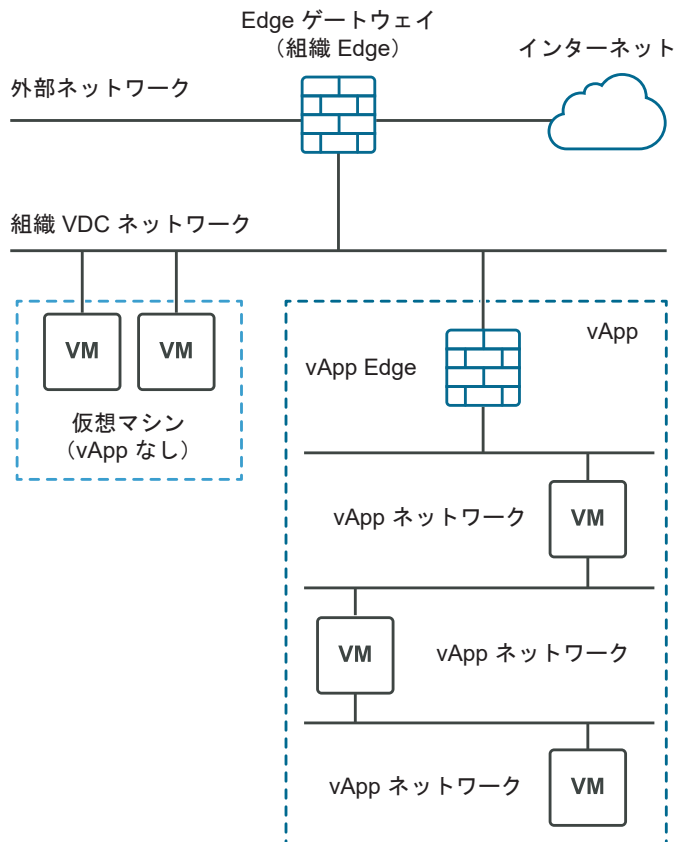
仮想マシンのアーキテクチャ

仮想マシンは、スタンドアロン マシンとして配置することも、vApp 内に配置することもできます。

仮想マシンとは、物理コンピュータのようにオペレーティング システムとアプリケーションを実行するソフトウェア コンピュータです。仮想マシンは、一連の仕様および構成ファイルで構成され、ホストの物理リソースでバックアップされています。すべての仮想マシンには、物理ハードウェアと同一の機能を提供する仮想デバイスがあり、移植性、管理性、およびセキュリティの点で優れています。仮想マシンは、スタンドアロンにすることも、vApp 内に配置することもできます。vApp は、1 台以上の仮想マシンと 1 つ以上のネットワークで構成される複合オブジェクトです。

次の図は、仮想マシンを作成する際のさまざまなオプションを示しています。vApp 内でスタンドアロン仮想マシンまたは仮想マシンを作成できます。スタンドアロン仮想マシンは、組織仮想データセンターに直接接続されています。vApp 内に仮想マシンを作成することもできます。vApp 内に仮想マシンを作成することで、複数台の仮想マシンとその関連するネットワークをグループ化できます。vApp を使用すると、複雑なアプリケーションを構築し、それらを将来の使用に備えてカタログに保存できます。

図 2-1. スタンドアロンまたは vApp 内の仮想マシン



仮想マシンの表示と編集

スタンドアロンまたは vApp の一部である仮想マシンを表示できます。仮想マシンはグリッド ビューまたはカード ビューで表示できます。

手順


- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [仮想マシン] を選択します。

- 2  をクリックしてカード ビュー内のリストを表示し、必要に応じて [検索先] ドロップダウン メニューから仮想マシンのリストをフィルタします。

- 3 グリッド ビューで仮想マシンを表示するには、 をクリックします。カード ビューに表示するには、 をクリックします。

仮想マシンのリストがグリッド ビューに、またはカードのリストとして表示されます。


- 4 (オプション) 各仮想マシンについて表示する詳細を含むようにグリッド ビューを設定します。

- a グリッド ビューから、[グリッド エディタ] アイコン () を選択します。
- b 仮想マシンの詳細のうち、グリッド ビューに表示する詳細の横にあるチェック ボックスをオンにして選択します。

詳細には、ハードウェアのバージョン、VMware Tools、メモリなどに関する情報が含まれます。

- c 変更内容を保存するには、[OK] をクリックします。

選択した詳細が、仮想マシンごとに列として表示されます。

- 5 (オプション) グリッド ビューで、仮想マシンの左側にある  をクリックして、仮想マシンに対して実行できるアクションを表示します。

たとえば、仮想マシンをシャットダウンすることができます。

- 6 仮想マシンのゲスト OS のインターフェイスにアクセスするには、カード ビューの右上にあるデスクトップ アイコンをクリックします。

新しいスタンドアロン仮想マシンの作成

新しいスタンドアロン仮想マシンを作成できます。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [仮想マシン] を選択します。

- 2  をクリックしてカード ビュー内のリストを表示し、必要に応じて [検索先] ドロップダウン メニューから仮想マシンのリストをフィルタします。

- 3 [新しい仮想マシン] をクリックします。
- 4 仮想マシンの名前とコンピュータ名を入力します。

重要： コンピュータ名には、英数字とハイフンのみを含めることができます。コンピュータ名は、数字のみで設定したり、スペースを含めたりすることはできません。

- 5 (オプション) わかりやすい説明を入力します。
- 6 仮想マシンを作成直後にパワーオンするかどうかを選択します。
- 7 仮想マシンを展開する方法を選択します。

オプション	アクション
新規	<p>カスタマイズ可能な設定で新しい仮想マシンを展開します。</p> <ol style="list-style-type: none"> a オペレーティング システム ファミリーとオペレーティング システムを選択します。 b (オプション) ブート イメージを選択します。 c (オプション) 仮想マシン配置ポリシーと仮想マシン サイズ変更ポリシーを選択します。 <p>仮想マシン配置ポリシーおよび仮想マシン サイズ変更ポリシーのドロップダウン メニューは、サービス プロバイダがこれらのポリシーを組織仮想データセンターに公開している場合にのみ表示されます。</p> <ol style="list-style-type: none"> d (オプション) 事前定義済みのサイズ変更オプションから仮想マシンのサイズを選択するか、[カスタム サイズ変更オプション] をクリックして、仮想 CPU の数、ソケットあたりのコア数、およびメモリ設定を手動で入力します。 <p>仮想マシンのサイズを定義する仮想マシン サイズ変更ポリシーを選択すると、このオプションは表示されません。</p> <p>仮想マシンの事前定義済みサイズには、[小]、[中]、[大] があります。</p> <ol style="list-style-type: none"> e ストレージ ポリシーや GB 単位のサイズなど、仮想マシンのストレージ設定を指定します。 f ネットワーク、IP モード、IP アドレス、プライマリ NIC など、仮想マシンのネットワーク設定を指定します。
テンプレートから	<p>テンプレート カタログで選択したテンプレートから仮想マシンを展開します。</p> <ol style="list-style-type: none"> a 使用可能なテンプレートのリストから仮想マシン テンプレートを選択します。 b (オプション) 仮想マシン配置ポリシーと仮想マシン サイズ変更ポリシーを選択します。 <p>仮想マシン配置ポリシーおよび仮想マシン サイズ変更ポリシーのドロップダウン メニューは、サービス プロバイダがこれらのポリシーを組織仮想データセンターに公開している場合にのみ表示されます。選択したテンプレートにポリシーが割り当てられている場合、事前定義済みのテンプレート ポリシーに制限されることがあります。</p> <ol style="list-style-type: none"> c (オプション) カスタム ストレージ ポリシーを使用するように選択し、[使用するカスタム ストレージ ポリシー] ドロップダウン メニューから使用するストレージ ポリシーを選択します。 d エンドユーザー使用許諾契約書がある場合は、確認のうえ、承諾してください。

- 8 [OK] をクリックして仮想マシンの設定を保存し、作成プロセスを開始します。

カタログで仮想マシンのカードを確認できます。仮想マシンが作成されるまで、状態はビジーと表示されます。

仮想マシン コンソールを開く

仮想マシン コンソールにアクセスすると、仮想マシンに関する情報の表示、ゲスト OS の操作、およびゲスト OS に影響を及ぼす操作の実行を行うことができます。

前提条件

仮想マシンはパワーオンされている必要があります。

クライアントでの VMware Remote Console のインストール

VMware Remote Console では、vCloud Director によってプロビジョニングおよび管理されるすべての仮想マシンに、組み込みのユーザー ゲスト インタラクションが用意されています。このセクションでは、Windows、Apple OS X、Linux に VMware Remote Console をインストールするために必要なタスクの詳細を説明します。

前提条件

この操作には、事前定義の vApp ユーザーロールに含まれている権限、またはそれに相当する権限が必要です。

手順

1 インストーラをダウンロードします。

- VMware Remote Console のダウンロード ページに移動し、現在のプラットフォームのリンクを選択します。

www.vmware.com/go/download-vmrc

- vCloud Director テナント ポータルの [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックします。仮想マシンを選択し、[アクション] メニューから [VMRC のダウンロード] を選択します。

2 現在のプラットフォームに応じてインストール手順を実行します。

- Windows

.msi インストーラをダブルクリックし、プロンプトの指示どおりに実行します。

- Linux

root 権限で .bundle インストーラを実行し、プロンプトの指示どおりに実行します。

- Mac

.dmg をダブルクリックして開き、含まれている VMware Remote Console アイコンをダブルクリックして、アプリケーション フォルダにコピーします。

結果

インストール後、`vmrc://` スキームで始まる Uniform Resource Identifier (URI) をクリックすると VMware Remote Console が起動します。VMware Workstation、Player、Fusion も `vmrc://` URI スキームを処理します。


仮想マシンのリモート コンソールを開く

vCloud Director テナント ポータルから VMware Remote Console を使用して仮想マシン コンソールを開くことができます。

前提条件

- ローカル システムに VMware Remote Console がインストールされていることを確認します。
- 選択した仮想マシンがパワーオン状態であることを確認してください。
- この操作には、事前定義の vApp ユーザーロールに含まれている権限、またはそれに相当する権限が必要です。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [仮想マシン] を選択します。
- 2  をクリックしてカード ビュー内のリストを表示し、必要に応じて [検索先] ドロップダウン メニューから仮想マシンのリストをフィルタします。
- 3 仮想マシンの [アクション] メニューから、[VMware Remote Console の起動] を選択します。

注： VMware Remote Console がインストールされていない場合は、ポップアップ ウィンドウが表示されて、VMware Remote Console をインストールするか、Web コンソールを使用するように求められます。

結果

仮想マシン コンソールが外部仮想リモート コンソールとして開きます。

注： VMware Remote Console を使用して vCloud Director 仮想マシンに接続した場合、実行できるのはコンソール操作 (Ctrl+Alt+Del の送信) のみです。デバイスの操作、電源の操作、または設定の管理を行うことはできません。


Web コンソールを開く

ローカル システムに VMware Remote Console がインストールされていない場合でも、仮想マシンのコンソールに接続できます。

前提条件

- 仮想マシンがパワーオン状態であることを確認します。
- この操作には、事前定義の vApp ユーザーロールに含まれている権限、またはそれに相当する権限が必要です。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [仮想マシン] を選択します。
- 2  をクリックしてカード ビュー内のリストを表示し、必要に応じて [検索先] ドロップダウン メニューから仮想マシンのリストをフィルタします。

3 仮想マシンの [アクション] メニューから、[Web コンソールの起動] を選択します。

結果

VMware HTML Console SDK を使用することで、仮想マシン コンソールがブラウザの新規タブに開きます。

次のステップ

コンソール ウィンドウ内の任意の場所をクリックすると、マウス、キーボード、およびその他の入力デバイスがコンソール内で使用できるようになります。

注： サポートされている国際キーボードについては、<https://www.vmware.com/support/developer/html-console/> にある VMware HTML Console SDK のドキュメントを参照してください。

仮想マシンでの電源の操作の実行

仮想マシンのパワーオンまたはパワーオフ、仮想マシンのサスペンドまたはリセット、あるいは仮想マシンのゲスト OS のシャットダウンなど、仮想マシンでの電源操作を実行できます。

仮想マシンのパワーオン


仮想マシンのパワーオンは、物理マシンのパワーオンと同じ操作です。

ゲストのカスタマイズが有効化されている仮想マシンは、その仮想マシンに現在のバージョンの VMware Tools がインストールされていないかぎり、パワーオンすることはできません。

前提条件

仮想マシンはパワーオフされている必要があります。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [仮想マシン] を選択します。
- 2  をクリックしてカード ビュー内のリストを表示し、必要に応じて [検索先] ドロップダウン メニューから仮想マシンのリストをフィルタします。
- 3 起動する仮想マシンの [アクション] メニューから [パワーオン] を選択します。

結果

パワーオンされた仮想マシンに緑でパワーオン状態が表示されます。


仮想マシンのパワーオフ

仮想マシンのパワーオフは、物理マシンのパワーオフと同じ操作です。

前提条件

仮想マシンはパワーオンされている必要があります。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [仮想マシン] を選択します。
- 2  をクリックしてカード ビュー内のリストを表示し、必要に応じて [検索先] ドロップダウン メニューから仮想マシンのリストをフィルタします。
- 3 パワーオフする仮想マシンの [アクション] メニューから [パワーオフ] を選択します。

結果

パワーオフされた仮想マシンに赤でパワーオフ状態が表示されます。


ゲスト OS のシャットダウン

仮想マシンのゲスト OS をシャットダウンすることは、物理マシンの電源を切ることに対応します。

前提条件

仮想マシンとゲスト OS がパワーオンされていること。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [仮想マシン] を選択します。
- 2  をクリックしてカード ビュー内のリストを表示し、必要に応じて [検索先] ドロップダウン メニューから仮想マシンのリストをフィルタします。
- 3 仮想マシンの [アクション] メニューから、[ゲスト OS をシャットダウン] を選択します。

結果

ゲスト OS がシャットダウンされます。

仮想マシンのリセット


仮想マシンをリセットすると状態（メモリ、キャッシュなど）はクリアされますが、仮想マシンは実行し続けます。仮想マシンをリセットすることは、物理マシンのリセット ボタンを押すことと同じです。仮想マシンの電源状態を変更することなく、オペレーティング システムのハード リセットを開始します。

前提条件

仮想マシンがパワーオンされていること。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [仮想マシン] を選択します。

- 2  をクリックしてカード ビュー内のリストを表示し、必要に応じて [検索先] ドロップダウン メニューから仮想マシンのリストをフィルタします。
- 3 リセットする仮想マシンの [アクション] メニューから、[リセット] を選択します。

結果

仮想マシンの状態がクリアされます。

仮想マシンのサスペンド


仮想マシンをサスペンドすると、メモリの内容をディスクに書き込むことによって現在の状態が保持されます。

サスペンドおよびレジューム機能は、仮想マシンの現在の状態を保存し、後で同じ状態から作業を再開する場合に便利です。

前提条件

仮想マシンはパワーオンされている必要があります。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [仮想マシン] を選択します。
- 2  をクリックしてカード ビュー内のリストを表示し、必要に応じて [検索先] ドロップダウン メニューから仮想マシンのリストをフィルタします。
- 3 サスペンドする仮想マシンの [アクション] メニューから、[サスペンド] を選択します。

結果

仮想マシンがサスペンドされますが、その状態は保持されます。


仮想マシンのサスペンド状態の破棄

仮想マシンがサスペンド状態で、仮想マシンの使用を再開する必要がなくなった場合は、サスペンド状態を破棄できます。サスペンド状態を破棄すると、保存済みメモリは削除され、マシンはパワーオフ状態に戻ります。

前提条件

サスペンド状態の仮想マシン。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [仮想マシン] を選択します。
- 2  をクリックしてカード ビュー内のリストを表示し、必要に応じて [検索先] ドロップダウン メニューから仮想マシンのリストをフィルタします。
- 3 仮想マシンの [アクション] メニューから、[サスペンド状態を破棄] を選択します。

結果

状態は破棄され、仮想マシンがパワーオフされます。

仮想マシンでの VMware Tools のインストール


vCloud Director は、VMware Tools を使用してゲスト OS をカスタマイズします。

VMware Tools は、汎用オペレーティング システム ドライバを仮想ハードウェア用に調整された VMware ドライバに置き換えることで仮想マシンの管理とパフォーマンスを向上させます。VMware Tools はゲスト OS にインストールします。ゲスト OS は VMware Tools がなくても動作しますが、重要な機能や便利な機能は利用できません。

前提条件

- 仮想マシンがパワーオン状態である必要があります。
- 新しく作成した仮想マシンにゲスト OS がインストールされていない場合は、まずゲスト OS をインストールしてから VMware Tools をインストールする必要があります。
- VMware Tools をインストールする前に、ゲストのカスタマイズを無効にする必要があります。
- vApp の仮想マシンにインストールされた VMware Tools のバージョンが 7299 より古い場合は、アップグレードする必要があります。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [仮想マシン] を選択します。
- 2  をクリックしてカード ビュー内のリストを表示し、必要に応じて [検索先] ドロップダウン メニューから仮想マシンのリストをフィルタします。
- 3 VMware Tools をインストールする仮想マシンの [アクション] メニューから、[VMware Tools のインストール] を選択します。

ターゲットのゲスト OS に VMware Tools がインストールされます。インストール中にエラーが発生すると、エラー メッセージが表示されます。[タスク] ウィンドウで、インストール処理の進行状況を確認することもできます。
- 4 仮想マシンの Web コンソールを開くには、[アクション] メニューから [Web コンソールの起動] を選択します。
- 5 特定のオペレーティング システム用の VMware Tools を設定するには、[VMware のナレッジベースの記事 KB1014294](#) の指示どおりに実行します。

結果

VMware Tools がゲスト OS 上にインストールおよび設定されます。

仮想マシンの仮想ハードウェア バージョンのアップグレード

仮想マシンに対して、仮想ハードウェア バージョンをアップグレードすることができます。仮想ハードウェア バージョンが高いほど、より多くの機能がサポートされます。

vApp 内の仮想マシンのハードウェア バージョンをダウングレードすることはできません。

vCloud Director は、バックアップ vSphere リソースに応じてハードウェア バージョンをサポートします。サポートされるハードウェア バージョンは、バックアップ プロバイダ VDC でサポートされている最新の仮想ハードウェア バージョンによって異なります。組織管理者またはシステム管理者は、基盤となるハードウェアでサポートされている最新バージョンよりも前のバージョンにハードウェア バージョンを設定できます。vCloud Director テナントポータルは、組織 VDC またはプロバイダ VDC がバックアップするハードウェアに基づいて、選択可能な仮想ハードウェア バージョンのリストを動的に設定します。


仮想マシンの互換性設定で使用するハードウェア機能については、『vSphere 仮想マシン管理』を参照してください。

VMware 製品とその仮想ハードウェア バージョンの詳細については、<https://kb.vmware.com/s/article/1003746> を参照してください。

前提条件

- 仮想マシンまたは仮想マシンを含む vApp を停止します。
- 仮想マシンに最新バージョンの VMware Tools がインストールされていることを確認します。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [仮想マシン] を選択します。
- 2  をクリックしてカード ビュー内のリストを表示し、必要に応じて [検索先] ドロップダウン メニューから仮想マシンのリストをフィルタします。
- 3 アップグレードする仮想マシンの [アクション] メニューから、[仮想ハードウェア バージョンをアップグレード] を選択します。
- 4 [OK] をクリックします。

結果

仮想マシンが最新バージョンにアップグレードされます。

仮想マシンのプロパティの編集

仮想マシンの名前と説明、ハードウェアとネットワークの設定、ゲスト OS の設定など、仮想マシンのプロパティを編集できます。


仮想マシンの全般プロパティの変更

仮想マシンの名前、説明、およびその他の全般プロパティは確認して変更することができます。

前提条件

オペレーティング システムなどのプロパティを変更するには、マシンがパワーオフ状態になっている必要があります。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [仮想マシン] を選択します。
- 2  をクリックしてカード ビュー内のリストを表示し、必要に応じて [検索先] ドロップダウン メニューから仮想マシンのリストをフィルタします。
- 3 編集する仮想マシンのカードで [詳細] をクリックします。
- 4 [全般] で表示または編集できるプロパティのリストは、デフォルトで展開されます。

オプション	アクション
仮想マシン名	仮想マシンの名前を編集します。 仮想マシンがパワーオン状態である間は、このプロパティを編集できます。
コンピュータ名	ネットワーク上の仮想マシンを識別するゲスト OS に設定されたコンピュータ名およびホスト名を編集します。コンピュータ名に対する Windows OS の制限により、このフィールドは 15 文字に制限されています。 仮想マシンがパワーオン状態である間は、このプロパティを編集できます。
説明	必要に応じて仮想マシンの説明を編集します。 仮想マシンがパワーオン状態である間は、このプロパティを編集できます。
オペレーティング システム ファミリー	ドロップダウン メニューからオペレーティング システム ファミリーを選択します。 仮想マシンがパワーオフ状態である間は、このプロパティを編集できます。また、仮想マシンにオペレーティング システムがすでに入っている場合は、このプロパティを編集することはできません。
オペレーティング システム	ドロップダウン メニューからオペレーティング システムを選択します。 仮想マシンがパワーオフ状態である間は、このプロパティを編集できます。また、仮想マシンにオペレーティング システムがすでに入っている場合は、このプロパティを編集することはできません。
起動遅延時間	起動動作を遅延させる時間（ミリ秒）を指定します。 仮想マシンをパワーオンしてから、BIOS を終了してゲスト OS ソフトウェアが起動されるまでの時間が短いことがあります。起動遅延時間を変更して、この時間を長くすることができます。
ストレージ ポリシー	ドロップダウン メニューから仮想マシンが使用するストレージ ポリシーを選択します。 仮想マシンがパワーオン状態である間は、このプロパティを編集できます。
仮想データセンター	この仮想マシンが属する仮想データセンターの名前を表示します。
VMware Tools	仮想マシンに VMware Tools がインストールされているかどうかを表示します。
仮想ハードウェア バージョン	仮想マシンの仮想ハードウェア バージョンを表示します。
アップグレード先:	アップグレードするには、ドロップダウン メニューからバージョンを選択します。


オプション	アクション
時間の同期	仮想マシンのゲスト OS と、それを実行している仮想データセンターとの間で、時間の同期を有効化するには、チェック ボックスをオンにします。
BIOS 設定の入力	次回仮想マシンを起動したときに、強制的に BIOS 設定画面にするかどうかを選択します。 仮想マシンがパワーオフ状態である間は、このプロパティを編集できます。

- 5 変更が完了したら、[保存] をクリックします。

仮想マシンのハードウェア プロパティの変更

仮想マシンのハードウェア プロパティは確認して変更することができます。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [仮想マシン] を選択します。
- 2  をクリックしてカード ビュー内のリストを表示し、必要に応じて [検索先] ドロップダウン メニューから仮想マシンのリストをフィルタします。
- 3 編集する仮想マシンのカードで [詳細] をクリックします。
- 4 [ハードウェア] をクリックすると、表示および編集できるハードウェア プロパティのリストが展開されます。

オプション	説明
仮想 CPU の数	CPU の数を編集します。 仮想マシンに割り当てることができる仮想 CPU の最大数は、ホストの論理 CPU 数、および仮想マシンにインストールされたゲスト OS の種類によって決まります。
ソケットあたりのコア数	ソケットあたりのコア数を編集します。 コアおよびソケットごとのコアに関する、仮想 CPU の割り当て方法を構成できます。シングルコア CPU、デュアルコア CPU、トライコア CPU などを使用するかどうかにより、仮想マシンの CPU コアの数指定してから、各ソケットに対するコアの数を選択します。
ゲスト OS に対するハードウェア支援 CPU 仮想化の公開	完全な CPU 仮想化をゲスト OS に公開できます。これにより、ハードウェア仮想化を必要とするアプリケーションが、バイナリ変換や準仮想化をせずに仮想マシンで稼働できます。
メモリの合計	仮想マシンのメモリ リソース設定を編集します。仮想マシンのメモリ サイズには、4 MB の倍数を指定する必要があります。 この設定は、仮想マシンに割り当てられる ESXi ホスト メモリの容量を決定します。仮想ハードウェアのメモリ サイズでは、仮想マシンで実行されるアプリケーションで使用可能なメモリの容量を決定します。仮想マシンは、仮想ハードウェアのメモリ サイズとして構成されたメモリ リソース以上のメモリ リソースを利用できません。
メモリ ホット アド	メモリ ホット アドを有効にすると、マシンがパワーオン状態の間仮想マシンにメモリ リソースを追加できます。この機能は、特定のゲスト OS と仮想マシン ハードウェア バージョン 7 以降のバージョンでのみサポートされています。
仮想 CPU ホット アド	仮想 CPU ホット アドを有効にすると、マシンがパワーオン状態の間仮想マシンに仮想 CPU を追加できます。ソケットごとに、コア数の倍数分のみを追加できます。この機能は、特定のゲスト OS と仮想マシン ハードウェアのバージョンでのみサポートされます。

オプション	説明
ソケットの数	ソケットの数を表示します。 ソケットの数は、使用可能な仮想 CPU の数によって決まります。仮想 CPU の数を更新すると、数が変わります。
リムーバブル メディア	接続された CD/DVD やフロッピー ドライブなど、使用可能なリムーバブル メディアを表示します。

5 [ハード ディスク] で [追加] をクリックして、ハード ディスクを追加します。

オプション	説明
サイズ	ハード ディスク サイズを MB 単位で入力します。後でハード ディスクのサイズを増やすことができます。 注： 仮想マシンがリンク クローンではなく、スナップショットを保持していない場合は、既存のハード ディスクのサイズを増やすことができます。
ポリシー	デフォルトで、仮想マシンのストレージ ポリシーが使用されます。 デフォルトでは、仮想マシンに接続されているすべてのハード ディスクは、その仮想マシンに指定されているストレージ ポリシーを使用します。これらのハード ディスクのデフォルトの設定は、仮想マシンの作成時、または仮想マシン プロパティの変更時にオーバーライドできます。各ハード ディスクの [サイズ] 列のドロップダウン メニューには、この仮想マシンで利用可能なすべてのストレージ ポリシーがリストされます。
IOPS	ディスクに特定の IOPS を選択します。 このオプションを使用して、1 秒あたりのディスクごとの I/O 処理数を制限します。
バス タイプ	バス タイプを選択します。 オプションは、[Paravirtual (SCSI)]、[LSI Logic パラレル (SCSI)]、[LSI Logic SAS (SCSI)]、[IDE]、および [SATA] です。ストレージ コントローラのタイプと互換性の詳細については、vSphere 仮想マシン管理ガイドを参照してください。
バス番号	バス番号を入力します。
ユニット番号	ハード ディスク ドライブの論理ユニット番号 (LUN) を入力します。

6 [NIC] で [追加] をクリックして、新しい NIC を追加します。

最大で 10 個の NIC を追加できます。仮想マシンのハードウェア バージョンに応じてサポートされている NIC の数については、<http://kb.vmware.com/s/article/2051652> を参照してください。vCloud Director では、仮想マシンの実行中に仮想マシン NIC を変更することができます。サポートされているネットワーク アダプタ タイプの詳細については、<http://kb.vmware.com/kb/1001805> を参照してください。

オプション	説明
プライマリ NIC	プライマリ NIC が選択されている場合は、フラグが表示されます。 プライマリ NIC を選択します。プライマリ NIC 設定によって、仮想マシンのデフォルトおよび唯一のゲートウェイが決まります。仮想マシンは、NIC を使用して、NIC と同じネットワークに直接接続されている仮想および物理マシンに接続できますが、ゲートウェイ接続が必要なネットワーク上のマシンへの接続に使用できるのはプライマリ NIC だけです。
NIC	NIC の数。
接続中	NIC を接続するチェック ボックスを選択します。
ネットワーク	ドロップダウン メニューからネットワークを選択します。

オプション	説明
IP モード	<p>IP モードを選択します。</p> <ul style="list-style-type: none"> ■ [固定 - IP プール] <p>ネットワークの IP プールから固定 IP アドレスを取得します。</p> <ul style="list-style-type: none"> ■ [固定 - 手動] <p>特定の IP アドレスを手動で指定することができます。このオプションを選択する場合は、[IP アドレス] 列に IP アドレスを入力する必要があります。</p> <ul style="list-style-type: none"> ■ [DHCP] <p>DHCP サーバから IP アドレスを取得します。</p>
MAC アドレス	ネットワーク インターフェイスの MAC アドレスを入力します。

7 [保存] をクリックします。

仮想マシンのゲスト OS のカスタマイズ プロパティの変更


vCloud Director におけるゲスト OS のカスタマイズは、すべてのプラットフォームでオプションです。Windows ドメインへの参加が必要な仮想マシンについては、必須です。

このメニューで指定する情報の一部は、Windows プラットフォームにのみ適用されます。[ゲスト OS のカスタマイズ] パネルには、Windows ドメインに参加する仮想マシンに必要な情報が含まれます。組織管理者は、組織内の Windows ゲストが参加できるドメインのデフォルト値を指定できます。すべての Windows 仮想マシンがドメインに参加する必要はありませんが、ほとんどの大規模企業のインストール環境では、ドメインのメンバーではない仮想マシンは多くの利用可能なネットワーク リソースにアクセスできません。

前提条件

- この操作には、事前定義の vApp 作成者ロールに含まれている権限、またはそれに相当する権限が必要です。
- ゲスト OS のカスタマイズには、VMware Tools を実行している仮想マシンが必要です。
- Windows ゲスト OS をカスタマイズする前に、システム管理者は vCloud Director サーバ グループに適切な Microsoft Sysprep ファイルをインストールしておく必要があります。『vCloud Director インストールおよびアップグレード ガイド』を参照してください。
- Linux ゲスト OS をカスタマイズするには、ゲストに Perl がインストールされている必要があります。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [仮想マシン] を選択します。
- 2  をクリックしてカード ビュー内のリストを表示し、必要に応じて [検索先] ドロップダウン メニューから仮想マシンのリストをフィルタします。
- 3 編集する仮想マシンのカードで [詳細] をクリックします。

4 [ゲスト OS のカスタマイズとプロパティ] をクリックしてゲスト OS の設定のリストを展開します。

オプション	説明
ゲストのカスタマイズの有効化	ゲストのカスタマイズを有効にするには、このオプションを選択します。
SID を変更	Windows セキュリティ ID (SID) を変更するには、このオプションを選択します。 このオプションは、Windows ゲスト OS を実行している仮想マシンに固有です。SID は、一部の Windows OS で、システムおよびユーザーを一意に識別するために使用されます。このオプションを選択しない場合、新規仮想マシンの SID は基になっている仮想マシンまたはテンプレートと同じになります。これらのコンピュータが1つのドメイン内にあり、ドメイン ユーザー アカウントのみが使用される場合、SID が重複していても問題が発生することはありません。しかし、これらのマシンがワークグループの一部であったり、ローカル ユーザー アカウントを使用したりする場合、SID が重複しているとファイル アクセス コントロールが危険にさらされる場合があります。詳細は、Microsoft Windows オペレーティング システムのドキュメントを参照してください。
ローカル管理者パスワードを許可	ゲスト OS で管理者パスワードの設定を許可するには、このオプションを選択します。 a ローカル管理者のパスワードを指定します。 [パスワードを指定] テキスト ボックスを空白にすると、パスワードが自動的に生成されます。 b 自動ログインを許可する回数を指定します。 値として 0 を入力すると、管理者としての自動ログインが無効になります。
初回ログイン時にパスワードの変更を管理者に要求	初回ログイン時にゲスト OS のパスワードの変更を管理者に要求するには、このオプションを選択します。セキュリティ上の理由から、選択することをお勧めします。
パスワードを自動生成	パスワードの自動生成を許可するには、このオプションを選択します。
この仮想マシンを有効化してドメインに参加させる	このオプションを選択すると、仮想マシンを Windows ドメインに参加させることができます。組織のドメインを使用するか、または組織のドメインをオーバーライドしてドメインのプロパティを入力することができます。 a ドメイン名を入力します。 b ユーザー名とパスワードを入力します。 c アカウント組織ユニットを入力します。
スクリプト	カスタマイズ スクリプトを使用して、仮想マシンのゲスト OS を変更することができます。カスタマイズ スクリプトを仮想マシンに追加すると、スクリプトは最初のカスタマイズと再カスタマイズの適用時にのみ呼び出されます。precustomization コマンド ライン パラメータを設定すると、ゲストのカスタマイズが開始する前にスクリプトが呼び出されます。postcustomization コマンド ライン パラメータを設定すると、ゲストのカスタマイズが終了した後にスクリプトが呼び出されます。 ■ スクリプト テキスト ボックスの下にあるアップロード ボタンをクリックして、ローカルマシンのカスタマイズ スクリプトに移動します。 ■ [スクリプト ファイル] テキスト ボックスに直接カスタマイズ スクリプトを入力します。 [スクリプト ファイル] テキスト ボックスに直接入力するカスタマイズ スクリプトは、1,500 文字を超えて入力することはできません。詳細については、VMware ナレッジベースの記事 https://kb.vmware.com/kb/1026614 を参照してください。

5 変更が完了したら、[保存] をクリックします。

ゲストのカスタマイズについて

ゲスト OS をカスタマイズする場合には、いくつかの設定とオプションについて理解しておく必要があります。

[ゲストのカスタマイズを有効化] チェック ボックス

このチェック ボックスは、仮想マシンの [プロパティ] ページの [ゲスト OS のカスタマイズ] タブに表示されます。ゲストのカスタマイズの目標は、[プロパティ] ページで選択したオプションに基づいて構成することです。このチェック ボックスを選択すると、必要に応じて、ゲストのカスタマイズと再カスタマイズが実行されます。

このプロセスは、コンピュータ名、ネットワーク設定、管理者と root パスワードの設定および期限切れ、Windows オペレーティング システムの SID 変更などのゲストのカスタマイズ機能がすべて正常に動くようにするために必要です。[電源を入れて、再カスタマイズを適用] を正常に機能させるために、このオプションを選択してください。

このチェック ボックスが選択されている場合に vCloud Director の仮想マシンの構成パラメータがゲスト OS の設定と同期されていないと、仮想マシンの [プロパティ] 画面の [プロファイル] タブには、ゲスト OS との間で設定が同期されておらず、仮想マシンでゲストのカスタマイズが必要であることが表示されます。

vApp および仮想マシンでのゲストのカスタマイズの動作

チェック ボックスをオフにしておきます。

- [ゲストのカスタマイズを有効化]
- Windows ゲスト OS では、[SID を変更]
- [パスワードのリセット]

カスタマイズを実行する場合（または、ゲスト OS に反映が必要なネットワークの設定を変更した場合）は、[ゲストのカスタマイズを有効化] チェック ボックスを選択し、仮想マシンの [プロパティ] 画面の [ゲスト OS のカスタマイズ] タブでオプションを設定できます。vApp テンプレートの仮想マシンを使用して App を作成して仮想マシンを追加すると、その vApp テンプレートは構成要素として機能します。カタログから新規 vApp に仮想マシンを追加すると、その仮想マシンでは、ゲストのカスタマイズがデフォルトで有効になります。カタログから vApp テンプレートを vApp として保存すると、仮想マシンでは、[ゲストのカスタマイズを有効化しますか?] チェック ボックスがオンの場合にのみゲストのカスタマイズが有効になります。

以下に、ゲストのカスタマイズ設定のデフォルト値を示します。

- [ゲストのカスタマイズを有効化] チェック ボックスは、カタログ内のソース仮想マシンと同じです。
- Windows のゲスト仮想マシンの場合、[SID を変更] は、カタログ内のソース仮想マシンと同じです。
- パスワードのリセット設定は、カタログ内のソース仮想マシンと同じです。

必要に応じて、vApp を開始する前に [ゲストのカスタマイズを有効化] チェック ボックスを選択解除することができます。

ゲスト OS のインストールを保留しているブランクの仮想マシンを vApp に追加すると、それらの仮想マシンはカスタマイズの準備がまだできていないため、[ゲストのカスタマイズを有効化] チェック ボックスはデフォルトでオフに設定されます。

ゲスト OS と VMware Tools をインストールした後は、仮想マシンの電源を切り、vApp を停止し、[ゲストのカスタマイズを有効化] チェック ボックスをオンにして、vApp と仮想マシンを開始してゲストのカスタマイズを実行できます。

カスタマイズした仮想マシンで仮想マシン名とネットワーク設定を更新すると、その仮想マシンは次のパワーオン時に再カスタマイズされて、ゲストの仮想マシンと vCloud Director が再同期されます。

仮想マシンのパワーオンと再カスタマイズの適用

仮想マシンをパワーオンし、仮想マシンの再カスタマイズを適用することができます。

仮想マシンの設定が vCloud Director と同期していない場合や、ゲストのカスタマイズ実行の試みが失敗した場合、仮想マシンの再カスタマイズを適用できます。


仮想マシンで実行されているアプリケーションが、再カスタマイズをサポートしていることを確認します。

Microsoft Sysprep を使用してドメイン コントローラを変更し、SID も変更する場合は、仮想マシンが破損する可能性があります。仮想マシンが破損するリスクを回避するには、再カスタマイズを行う前にスナップショットを作成します。

前提条件

- 組織管理者である必要があります。
- 仮想マシンがパワーオフ状態である必要があります。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [仮想マシン] を選択します。
- 2  をクリックしてカード ビュー内のリストを表示し、必要に応じて [検索先] ドロップダウン メニューから仮想マシンのリストをフィルタします。
- 3 パワーオンしてカスタマイズする仮想マシンの [電源] メニューから [パワーオンして、再カスタマイズを適用] を選択します。

結果

仮想マシンが再カスタマイズされ、パワーオン状態になります。

仮想マシンの詳細プロパティの変更

[詳細設定] では、リソース割り当ての設定（共有、予約、および制限）を行い、仮想マシンに対して提供される CPU リソース、メモリ リソース、およびストレージ リソースの量を決定できます。

リソース割り当ての設定（共有、予約、および制限）を使用し、仮想マシンに対して提供される CPU リソース、メモリ リソース、およびストレージ リソースの量を決定します。

リソース割り当て共有

共有により、仮想データセンター内の仮想マシンの相対的な重要度が指定されます。仮想マシンでは、リソースの共有が別の仮想マシンの 2 倍であり、これらの 2 つの仮想マシンがリソースを競い合う場合は、2 倍のリソースを使用する権利があります。共有は通常、[高]、[標準]、または [低] として指定されます。これらの値は、共有の値をそれぞれ 4:2:1 の比率で指定します。[カスタム] を選択して、（比重を表す）特定の数の共有を各仮想マシンに割り当てることもできます。仮想マシンに共有を割り当てる場合は、常にその仮想マシンの優先度を、その他のパワーオンされた仮想マシンに対して相対的に指定します。

リソース割り当て予約

仮想マシンに確保される最小割り当てを指定します。vCloud Director では、仮想マシンの予約を達成するのに十分な未予約リソースが存在する場合にのみ、仮想マシンをパワーオンできます。仮想データセンターは、リソースが大量にロードされている場合でも、この量を確保します。予約は、具体的な単位（MHz または MB）で表されます。

たとえば、2 GHz が使用可能で、仮想マシン 1 に対して 1 GHz、仮想マシン 2 に対して 1 GHz のリソース割り当て予約をする場合を考えます。これで、必要な場合に各仮想マシンが 1GHz を獲得できます。ただし、仮想マシン 1 が 500 MHz しか使用していない場合には、仮想マシン 2 は 1.5 GHz を使用できます。

予約は、デフォルトで 0 に設定されます。最低限必要な量の CPU またはメモリを仮想マシンに対して常に利用可能にすることを約束する必要がある場合は、予約を指定できます。

リソース割り当て制限

仮想マシンに割り当てることができる CPU リソースとメモリ リソースに対する上限が指定されます。仮想データセンターは、予約より多くの量を仮想マシンに割り当てることができますが、システムに未使用のリソースがあっても、制限を超える割り当ては行いません。制限は、具体的な単位（MHz または MB）で表されます。


CPU リソースとメモリ リソースの制限は、デフォルトでは無制限です。メモリの制限が無制限である場合、通常は、作成時に仮想マシンに対して構成されたメモリの量が有効な制限になります。

ほとんどの場合、制限を指定する必要はありません。制限を指定すると、アイドル リソースを無駄にすることがあります。システムが活用されていない状態で、アイドル リソースが使用可能な場合でも、システムは、制限以上のリソースを仮想マシンが使用することを許可しません。制限の指定は、特別な理由がある場合にのみ行うようにしてください。

前提条件

- 予約プール仮想データセンターが必要です。
- 仮想マシンに対して特定量のメモリが仮想データセンターから提供されていることを確認します。
- 特定の仮想マシンには他の仮想マシンよりも高い割合の仮想データセンター リソースが常に割り当てられています。
- 仮想マシンに割り当てることができるリソースに上限を設定します。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [仮想マシン] を選択します。
- 2  をクリックしてカード ビュー内のリストを表示し、必要に応じて [検索先] ドロップダウン メニューから仮想マシンのリストをフィルタします。
- 3 編集する仮想マシンのカードで [詳細] をクリックします。
- 4 [詳細] をクリックします。

- 5 [優先度] ドロップダウン メニューからオプションを選択して、CPU 設定のリソース割り当て共有を設定します。

オプション	説明
低	仮想 CPU あたり 500 の共有を割り当てます。
標準	仮想 CPU あたり 1,000 の共有を割り当てます。
高	仮想 CPU あたり 2,000 の共有を割り当てます。
カスタム	共有の数を入力して、(比重を表す) 特定の数の共有を各仮想マシンに割り当てることができます。 仮想マシンに共有を割り当てるときは、常にその仮想マシンの優先度を、その他のパワーオンされた仮想マシンに対して相対的に指定します。

- 6 MHz 単位で予約を入力して CPU 設定の予約を指定し、必要に応じて CPU 設定の制限を MHz 単位で指定します。

オプション	説明
制限なし	デフォルトの CPU リソース オプションです。
最大値	仮想マシンに割り当てることができる CPU リソースの上限を MHz 単位で指定します。

- 7 [優先度] ドロップダウン メニューからオプションを選択して、メモリ設定のリソース割り当て共有を設定します。

オプション	説明
低	構成された仮想マシン メモリ 1 MB あたり 5 の共有を割り当てます。
標準	構成された仮想マシン メモリ 1 MB あたり 10 の共有を割り当てます。
高	構成された仮想マシン メモリ 1 MB あたり 20 の共有を割り当てます。
カスタム	共有の数を入力して、特定の数の共有を割り当てることができます。

- 8 メモリ設定の予約を MB 単位で指定し、必要に応じてメモリ設定の制限を MB 単位で指定します。

オプション	説明
制限なし	デフォルトの CPU リソース オプションです。
最大値	仮想マシンに割り当てることができる CPU リソースの上限を MHz 単位で指定します。

- 9 [メタデータ] の下にある [追加] をクリックして、メタデータを指定します。

たとえば、作成日や所有者に関するメタデータを追加できます。

- 10 変更が完了したら、[保存] をクリックします。


メディアの挿入

カタログから CD/DVD イメージなどのメディアを挿入し、仮想マシンのゲスト OS で使用できます。これらのメディア ファイルを使用して、仮想マシン、各種のアプリケーション、ドライバなどにオペレーティング システムをインストールできます。

前提条件

メディア ファイルのカタログにアクセスできる必要があります。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [仮想マシン] を選択します。
- 2  をクリックしてカード ビュー内のリストを表示し、必要に応じて [検索先] ドロップダウン メニューから仮想マシンのリストをフィルタします。
- 3 メディアを追加する仮想マシンを選択します。
- 4 [アクション] メニューで、[メディアを挿入] を選択します。
- 5 [CD を挿入] ウィンドウで、仮想マシンに挿入するメディア ファイルを選択します。
- 6 [挿入] をクリックします。


メディアの取り出し

仮想マシンで CD または DVD を使用し終わったら、メディア ファイルを取り出すことができます。

前提条件

メディア ファイルが仮想マシンに挿入されている状態。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [仮想マシン] を選択します。
- 2  をクリックしてカード ビュー内のリストを表示し、必要に応じて [検索先] ドロップダウン メニューから仮想マシンのリストをフィルタします。
- 3 メディアを取り出す仮想マシンを選択します。
- 4 [アクション] メニューで、[メディアの取り出し] を選択します。

結果

メディア ファイルが排出されます。

異なる vApp への仮想マシンのコピー


仮想マシンを別の vApp にコピーできます。仮想マシンをコピーする場合、コピー元の仮想マシンはソース vApp に残されます。

仮想マシンをコピーする場合、スナップショットはコピーに含まれません。

前提条件

- この操作には、事前定義の vApp 作成者ロールに含まれている権限、またはそれに相当する権限が必要です。
- 仮想マシンをパワーオフします。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [仮想マシン] を選択します。
- 2  をクリックしてカード ビュー内のリストを表示し、必要に応じて [検索先] ドロップダウン メニューから仮想マシンのリストをフィルタします。
- 3 コピーする仮想マシンの [アクション] メニューから [コピー] を選択します。
- 4 仮想マシンをコピーするターゲット vApp を選択し、[次へ] をクリックします。
- 5 仮想マシンの名前とコンピュータ名などのリソース、およびオプションでストレージ ポリシーと NIC を設定し、[次へ] をクリックします。

重要： コンピュータ名には、英数字とハイフンのみを含めることができます。数字のみで設定したり、スペースを含めたりすることはできません。

- 6 [設定内容の確認] 画面で設定内容を確認し、[終了] をクリックします。

異なる vApp への仮想マシンの移動

仮想マシンを別の vApp に移動できます。仮想マシンを移動すると、元の仮想マシンはソース vApp から削除されます。

仮想マシンを別の vApp に移動すると、作成したスナップショットが失われます。

vCloud Director 9.5 以降では、異なる vApp 間での仮想マシンの移動は、VMware vSphere[®] vMotion[®] および Enhanced vMotion Compatibility (EVC) に依存します。仮想マシンは、同じプロバイダ仮想データセンター内の同一または別の組織仮想データセンターに属する異なる vApp に移動できます。

仮想マシンを異なる vApp に移動する際に、ネットワークとストレージ プロファイルの変更などの再構成を実行できます。


表 2-1. 仮想マシン移動中の再構成と仮想マシンの状態

再構成	ターゲット vApp が同じ組織仮想データセンターにある場合の仮想マシンの状態	ターゲット vApp が同じプロバイダ 仮想データセンター内の別の組織仮想データセンターにある場合の仮想マシンの状態
ネットワークを変更	パワーオフ	該当なし
ネットワークを削除	パワーオンまたはパワーオフ	該当なし
ストレージ プロファイルを変更	パワーオンまたはパワーオフ	パワーオフ

前提条件

- この操作には、事前定義の vApp 作成者ロールに含まれている権限、またはそれに相当する権限が必要です。
- 基盤となる vSphere リソースが vMotion と EVC をサポートしていることを確認します。vMotion と EVC の要件と制限については、「vCenter Server およびホスト管理」を参照してください。
- 仮想マシン ネットワークまたはストレージ プロファイルを変更する場合は、仮想マシンをパワーオフする必要があるかどうかを確認します。「仮想マシンの移動中の再構成および仮想マシンの状態」の表を参照してください。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [仮想マシン] を選択します。
- 2  をクリックしてカード ビュー内のリストを表示し、必要に応じて [検索先] ドロップダウン メニューから仮想マシンのリストをフィルタします。
- 3 移動するマシンの [アクション] メニューから [移動] を選択します。
- 4 ターゲット vApp を選択して、[次へ] をクリックします。
- 5 仮想マシンの名前とコンピュータ名などのリソース、およびオプションでストレージ ポリシーと NIC を設定し、[次へ] をクリックします。

重要： コンピュータ名には、英数字とハイフンのみを含めることができます。数字のみで設定したり、スペースを含めたりすることはできません。

- 6 [設定内容の確認] 画面で設定内容を確認し、[終了] をクリックします。

仮想マシンのアフィニティと非アフィニティ

アフィニティ ルールおよび非アフィニティ ルールを使用すると、仮想マシンのグループを異なる ESXi ホスト間に分散させたり、特定の ESXi ホスト上に保持することができます。


アフィニティ ルールを指定すると、仮想マシンのグループが特定のホスト上に配置されるため、それらの仮想マシンの使用状況の監査を容易に行うことができます。非アフィニティ ルールを指定すると、仮想マシンのグループが異なるホストにまたがって配置されるため、特定のホストで障害が発生した場合にすべての仮想マシンが同時にダウンするのを防ぐことができます。

アフィニティまたは非アフィニティ ルールが満たされない場合、ルールに追加された仮想マシンのパワーオンができなくなります。

アフィニティ ルールおよび非アフィニティ ルールの表示

既存のアフィニティ ルールおよび非アフィニティ ルールとそのプロパティ（ルールによって影響を受ける仮想マシンやルールが有効にされているかどうかなど）を表示できます。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [アフィニティ ルール] を選択します。
- 2 （オプション） [グリッド エディタ] アイコン（）をクリックし、ルールの詳細のうち表示するものを選択します。

結果

既存のアフィニティ および非アフィニティ ルール、仮想マシン、および各ルールの有効ステータスをリストとして確認できます。

アフィニティ ルールの追加

アフィニティ ルールを作成して、特定の仮想マシンのグループを単一のホスト上に配置すると、それらの仮想マシンの使用状況を監査できます。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [アフィニティ ルール] を選択します。
- 2 [アフィニティ ルール] で [新規] をクリックします。
- 3 ルールの名前を入力します。
- 4 ルールを作成するだけで有効にしない場合は、[有効] を選択解除します。
デフォルトでは、チェック ボックスはオンの状態で、ルールは作成後に有効になります。
- 5 [必須] チェック ボックスを選択したままにします。
デフォルトでは、各アフィニティ ルールは必須です。これは、ルールを満たすことができない場合、ルールに追加された仮想マシンはパワーオンされないことを意味します。
- 6 アフィニティ ルールに追加する仮想マシンを選択します。
- 7 [保存] をクリックします。

結果

vCloud Director によって、アフィニティ ルールに関連付けられた仮想マシンが単一のホストに配置されます。

非アフィニティ ルールの追加

非アフィニティ ルールを作成して複数のホストに特定の仮想マシン グループを配置することで、1 台のホストで障害が発生した場合に、それらの仮想マシンが同時にダウンするのを防ぐことができます。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [アフィニティ ルール] を選択します。
- 2 [非アフィニティ ルール] で [新規] をクリックします。
- 3 ルールの名前を入力します。
- 4 ルールを作成するだけで有効にしない場合は、[有効] を選択解除します。
デフォルトでは、チェック ボックスはオンの状態で、ルールは作成後に有効になります。
- 5 [必須] チェック ボックスを選択したままにします。
デフォルトでは、各非アフィニティ ルールは必須です。これは、ルールを満たすことができない場合、ルールに追加された仮想マシンはパワーオンされないことを意味します。
- 6 非アフィニティ ルールに追加する仮想マシンを選択します。
- 7 [保存] をクリックします。

結果

vCloud Director によって、非アフィニティ ルールに関連付けられた仮想マシンが複数のホストに配置されます。

アフィニティ ルールまたは非アフィニティ ルールの編集

アフィニティ ルールまたは非アフィニティ ルールを編集して、ルールを有効化または無効化したり、仮想マシンを追加または削除したり、ルール名またはルール設定を変更したりすることができます。

前提条件

この操作では、Organization vDC: VM-VM Affinity Edit 権限が必要です。この権限は、事前定義のカatalog 作成者、vApp 作成者、および組織管理者ロールに含まれます。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [アフィニティ ルール] を選択します。
- 2 編集するルールの名前の横にあるラジオ ボタンをクリックして、[編集] をクリックします。
- 3 ルールのプロパティを編集します。
 - a 必要に応じてルールの名前を変更します。
 - b ルールを有効にするか無効にするかを選択します。

- c [必須] チェック ボックスを選択したままにします。
- d 仮想マシンを追加するか、削除します。

4 [保存] をクリックします。

アフィニティ ルールまたは非アフィニティ ルールの削除

アフィニティ ルールまたは非アフィニティ ルールを使用する必要がなくなったら、削除することができます。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [アフィニティ ルール] を選択します。
- 2 削除するルールの名前の横にあるラジオ ボタンをクリックして、[削除] をクリックします。
- 3 ルールの削除を確定するには、[OK] をクリックします。

結果

vCloud Director からアフィニティ ルールまたは非アフィニティ ルールが削除されます。

仮想マシンの監視


vCloud Director 管理者が仮想マシンを監視する機能を有効にした場合は、テナント ポータルで監視チャートを表示できます。

この機能を使用すると、特定の仮想マシンの状態を一定期間（日、週、または月単位）把握できます。

前提条件

この機能は、vCloud Director 管理者によって有効にされている場合にのみ使用できます。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [仮想マシン] を選択します。
- 2  をクリックしてカード ビュー内のリストを表示し、必要に応じて [検索先] ドロップダウン メニューから仮想マシンのリストをフィルタします。
- 3 監視する仮想マシンを選択し、[詳細] をクリックします。
- 4 [チャートの監視] をクリックして、監視ビューを展開します。
監視チャートが表示されます。

5

6 仮想マシンを監視するためのメトリック オプションを選択します。

[メトリック] ドロップダウン メニューのリストは、システム管理者の選択内容によって異なります。オプションの一部またはすべてが表示されます。

メトリック	説明
最新プロビジョニング ディスク	KB で指定されます。 日、週、または月のビューを選択します。
平均ディスク読み取り	% 値で指定されます。 日、週、または月のビューを選択します。
平均ディスク書き込み	% 値で指定されます。 日、週、または月のビューを選択します。
平均 CPU 使用率	% 値で指定されます。 日、週、または月のビューを選択します。
平均 CPU 使用率 (MHz)	MHz で指定されます。 日、週、または月のビューを選択します。
最大 CPU 使用率	% 値で指定されます。 日、週、または月のビューを選択します。
平均メモリ使用量	% 値で指定されます。 日、週、または月のビューを選択します。
最新使用ディスク	KB で指定されます。 日、週、または月のビューを選択します。

リストから選択する値が変わるたびに、新しいチャートが表示されます。

7 (オプション) メトリック収集のタイム フレームを変更します。

8 [更新] をクリックします。

9 変更内容を保存するには、[保存] をクリックします。

スナップショットの操作

スナップショットには、スナップショット作成時の仮想マシンの状態とデータが保存されます。仮想マシンのスナップショットを作成しても、その仮想マシンに影響はありません。特定の状態のその仮想マシンのイメージが、コピーされ、保存されるだけです。スナップショットは、繰り返し同じ状態の仮想マシンに戻る必要があるが、複数の仮想マシンを作成したくないという場合に便利です。

スナップショットは、未知の障害または有害な効果が発生する可能性のあるソフトウェアをテストするための、短期的なソリューションとして便利です。たとえば、線形処理、アップデート パッケージをインストールするような反復処理、または異なるバージョンのプログラムをインストールするような分岐処理において、スナップショットをリストア ポイントとして使用できます。

仮想マシンのオペレーティング システムをアップグレードするときにスナップショットを使用できます。たとえば、仮想マシンをアップグレードする前に、スナップショットを作成してアップグレード前の時点での状態を保持します。アップグレード中に問題が発生しなかった場合は、スナップショットを削除して、アップグレード中に行った変更をコミットできます。一方で問題が発生した場合は、スナップショットに戻すことにより、保存したアップグレード前の状態に仮想マシンを戻すことができます。

vCloud Director では、仮想マシンのスナップショットは 1 つのみ保持できます。仮想マシンの新しいスナップショットを作成するたびに、前のものが削除されます。

仮想マシンのスナップショットの作成

仮想マシンのスナップショットを作成することができます。スナップショットを作成したら、仮想マシンをスナップショットに戻すことができます。また、スナップショットを削除することもできます。

前提条件

仮想マシンが名前付きディスクに接続されていないことを確認します。

注： スナップショットでは NIC 構成はキャプチャされません。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [仮想マシン] を選択します。

- 2  をクリックしてカード ビュー内のリストを表示し、必要に応じて [検索先] ドロップダウン メニューから仮想マシンのリストをフィルタします。

- 3 スナップショットを作成する仮想マシンの [アクション] メニューから、[スナップショットの作成] を選択します。

仮想マシンのスナップショットを作成すると、既存のスナップショットがある場合には置き換えられます。

- 4 (オプション) 仮想マシンのメモリのスナップショットを作成するかどうかを選択します。

仮想マシンのメモリの状態を取得する場合、スナップショットは仮想マシンのライブ状態を維持します。メモリ スナップショットでは、稼働中のソフトウェアをアップグレードするときなど、ある特定の時点でのスナップショットが作成されます。メモリ スナップショットを作成しておけば、アップグレードが予想どおりに完了しなかったとき、またはソフトウェアが期待に添うものでなかったときに、仮想マシンを元の状態に戻すことができます。

メモリ状態の取得時に仮想マシンのファイルを静止させる必要はありません。メモリの状態を取得しない場合、スナップショットは仮想マシンのライブ状態を保存せず、ディスクは、静止しないかぎりクラッシュ時の整合性を保ちます。

5 (オプション) ゲスト ファイル システムを静止するかどうかを選択します。

この操作を行うには、仮想マシンに VMware Tools がインストールされている必要があります。仮想マシンを静止する場合、VMware Tools によって仮想システム内のファイル システムが静止されます。静止操作により、スナップショット ディスクはゲスト ファイル システムの一貫した状態を表します。静止スナップショットは、自動バックアップや定期バックアップに適しています。たとえば、仮想マシンのアクティビティを把握していなくとも、最新の復元用バックアップが欲しいという場合に、ファイルを静止することができます。

大容量ディスクがある仮想マシンを静止させることはできません。

6 [OK] をクリックします。

結果

スナップショットにより、仮想マシンを最新のスナップショットに戻すことができます。


仮想マシンをスナップショットに戻す

仮想マシンを、スナップショットを作成した時点の状態に戻すことができます。

前提条件

仮想マシンにスナップショットがあります。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [仮想マシン] を選択します。
- 2  をクリックしてカード ビュー内のリストを表示し、必要に応じて [検索先] ドロップダウン メニューから仮想マシンのリストをフィルタします。
- 3 スナップショットに戻す仮想マシンの [アクション] メニューから、[スナップショットに戻す] を選択します。
- 4 [OK] をクリックします。

結果

仮想マシンが保存されたスナップショットに戻されます。

仮想マシンのスナップショットの削除


仮想マシンのスナップショットを削除することができます。

スナップショットを削除すると、保存された仮想マシンの状態が削除されるため、二度とその状態には戻れなくなります。スナップショットを削除しても、仮想マシンの現在の状態に影響はありません。

前提条件

スナップショットが保存されている仮想マシン。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [仮想マシン] を選択します。
- 2  をクリックしてカード ビュー内のリストを表示し、必要に応じて [検索先] ドロップダウン メニューから仮想マシンのリストをフィルタします。
- 3 スナップショットを削除する仮想マシンの [アクション] メニューから、[スナップショットの削除] を選択します。
- 4 [OK] をクリックします。


仮想マシンのリースの更新

リースの有効期限が近い仮想マシンのリースを更新できます。

前提条件

この操作には、事前定義の組織管理者ロールに含まれている権限、またはそれに相当する権限が必要です。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [仮想マシン] を選択します。
- 2  をクリックしてカード ビュー内のリストを表示し、必要に応じて [検索先] ドロップダウン メニューから仮想マシンのリストをフィルタします。
- 3 リースの有効期限が近い仮想マシンの [アクション] メニューから、[リースの更新] を選択します。

結果

リースが更新されます。[リース] フィールドに新しいリース期間が表示されます。


仮想マシンの削除

仮想マシンを組織から削除できます。

前提条件

仮想マシンは電源を切っておく必要があります。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [仮想マシン] を選択します。
- 2  をクリックしてカード ビュー内のリストを表示し、必要に応じて [検索先] ドロップダウン メニューから仮想マシンのリストをフィルタします。

3 削除する仮想マシンの [アクション] メニューから [削除] を選択します。

4 削除を確認します。

結果

仮想マシンが削除されます。

vApp の操作

3

vApp は、ネットワークを介して通信し、デプロイされた環境でリソースとサービスを使用する 1 つ以上の仮想マシンによって構成されます。vApp には複数の仮想マシンを含めることができます。

vCloud Director 9.5 以降、vApp は IPv6 接続をサポートします。IPv6 ネットワークに接続された仮想マシンには IPv6 アドレスを割り当てることができます。

重要： vApp を操作するためのすべての手順は、カード ビューに記載されています。これらの手順では、複数の仮想データセンターがあることが前提となります。グリッド ビューから同じ操作を実行することも可能ですが、手順は多少異なることがあります。

この章には、次のトピックが含まれています。

- vApp の表示
- 新規 vApp の構築
- OVF パッケージからの vApp フォームの作成
- vApp テンプレートからの vApp の作成
- vApp を開く
- vApps での電源の操作の実行
- vApp のプロパティの編集
- vApp ネットワーク図の表示
- vApp でのネットワークの作業
- スナップショットの操作
- vApp の所有者の変更
- 別の仮想データセンターへの vApp の移動
- 別の仮想データセンターへの停止した vApp のコピー
- パワーオン状態の vApp のコピー
- 仮想マシンの vApp への追加
- vApp の vApp テンプレートとしてのカタログへの保存
- OVF パッケージとしての vApp のダウンロード



- vApp リースの更新
- vApp の削除

vApp の表示

グリッド ビューまたはカード ビューに vApp を表示できます。


手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [vApp] を選択します。


- 2 vApp をグリッド ビューで表示するには、 をクリックします。カード ビューで表示するには、 をクリックします。

vApp のリストがグリッドまたはカードのリストとして表示されます。

- 3 (オプション) 表示する詳細を含むようにグリッド ビューを設定します。

- a グリッド ビューから、[グリッド エディタ] アイコン () を選択します。
- b vApp の詳細のうち、グリッド ビューに表示する詳細の横にあるチェック ボックスをオンにして選択します。
- c 変更内容を保存するには、[OK] をクリックします。

選択した詳細が、vApp ごとに列として表示されます。

- 4 (オプション) グリッド ビューで、vApp の左側にある  をクリックして、vApp に対して実行できるアクションを表示します。

たとえば、vApp をシャットダウンすることができます。

新規 vApp の構築

vApp テンプレートに基づいて vApp を作成する代わりに、カタログの仮想マシン、新規仮想マシン、または両方の組み合わせを使用して新規 vApp を作成することもできます。

vApp を構築するには、vApp の名前と、オプションで説明を入力する必要があります。後から、元に戻って仮想マシンを vApp に追加することができます。

前提条件

この操作には、事前定義の vApp 作成者ロールに含まれている権限、またはそれに相当する権限が必要です。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [vApp] を選択します。
- 2 [新規 vApp] をクリックします。

3 vApp の名前と、必要に応じて説明を入力します。

4 (オプション) カタログからこの vApp に追加する仮想マシンを検索するか、[仮想マシンの追加] をクリックして新しい空の仮想マシンを追加します。

カタログに仮想マシンがない場合は、仮想マシンを作成して vApp に追加します。

a 仮想マシンの名前とコンピュータ名を入力します。

重要： コンピュータ名には、英数字とハイフンのみを含めることができます。コンピュータ名は、数字のみで設定したり、スペースを含めたりすることはできません。

b (オプション) わかりやすい説明を入力します。

c 仮想マシンを展開する方法を選択します。

オプション	アクション
新規	<p>カスタマイズ可能な設定で新しい仮想マシンを展開します。</p> <ol style="list-style-type: none"> オペレーティング システム ファミリーとオペレーティング システムを選択します。 (オプション) ブート イメージを選択します。 (オプション) 仮想マシン配置ポリシーと仮想マシン サイズ変更ポリシーを選択します。 <p>仮想マシン配置ポリシーおよび仮想マシン サイズ変更ポリシーのドロップダウン メニューは、サービス プロバイダがこれらのポリシーを組織仮想データセンターに公開している場合にのみ表示されます。</p> <ol style="list-style-type: none"> 仮想マシンのサイズを選択するか、または [カスタム サイズ変更オプション] をクリックして、コンピューティング、メモリ、およびストレージの設定を手動で入力します。 <p>仮想マシンの事前定義済みサイズには、小、中、大があります。</p> <ol style="list-style-type: none"> ストレージ ポリシーや GB 単位のサイズなど、ストレージ オプションを指定します。 ネットワーク、IP モード、IP アドレス、プライマリ NIC など、仮想マシンのネットワーク設定を指定します。
テンプレートから	<p>テンプレート カタログで選択したテンプレートから仮想マシンを展開します。</p> <ol style="list-style-type: none"> カタログから仮想マシン テンプレートを選択します。 (オプション) 仮想マシン配置ポリシーと仮想マシン サイズ変更ポリシーを選択します。 <p>仮想マシン配置ポリシーおよび仮想マシン サイズ変更ポリシーのドロップダウン メニューは、サービス プロバイダがこれらのポリシーを組織仮想データセンターに公開している場合にのみ表示されます。選択したテンプレートにポリシーが割り当てられている場合、事前定義済みのテンプレート ポリシーに制限されることがあります。</p> <ol style="list-style-type: none"> (オプション) カスタム ストレージ ポリシーを使用するように選択し、[使用するカスタム ストレージ ポリシー] からポリシーを選択します。 使用可能なエンドユーザー使用許諾契約書がある場合は、これを確認し、承諾する必要があります。

d 仮想マシンを vApp に追加するには、[OK] をクリックします。

カタログで追加された仮想マシンを確認できます。

5 (オプション) vApp 内に作成するその他の仮想マシンごとに、[手順 手順 4](#) を繰り返します。

6 vApp の作成を完了するには、[作成] をクリックします。

結果

vApp が作成され、パワーオフ状態になります。vApp をパワーオンすると、その仮想マシンが作成され、同じようにパワーオンされます。

OVF パッケージからの vApp フォームの作成

vApp テンプレートおよび対応するカタログ項目を作成せず、OVF パッケージから vApp を直接作成およびデプロイできます。

vCloud Director には、vCenter Server の制限とは異なる OVF デプロイに対する独自の制限があります。このため、vCenter Server で成功した OVF デプロイが vCloud Director では失敗する可能性があります。

vCloud Director は OVF 1.1 をサポートしていますが、OVF 1.1 スキーマのすべてのセクションをサポートしているわけではありません。たとえば、OVF の `DeploymentOptions` セクションはサポートされていません。

vCloud Director の OVF デプロイには、`TransferService`、NFS マウントのスプール領域、vCenter Server への NFC 接続、チェックサム検証などの多くのコンポーネントが含まれます。これらのコンポーネントのいずれかに障害が発生すると、OVF のアップロードに失敗します。


マニフェスト ファイルを含む OVF パッケージをアップロードすると、vCloud Director は OVF 記述子ファイルとすべての VMDK ファイルの SHA-1 ハッシュを `manifest.mf` ファイルの値に対して検証します。ハッシュが一致しない場合、アップロードは失敗します。システム管理者は、`CONFIG` プロパティを `ovf.manifest.check.disabled` に設定することで、このチェックを無効にできます。

前提条件

- アップロードする OVF パッケージがあり、OVF パッケージをアップロードし、vApp をデプロイする権限があることを確認します。
- OVF 記述子ファイルの OVF バージョンが 0.9 ではないことを確認します。
- vCloud Director でサポートされている OVF 記述子ファイルのデフォルトの最大サイズは 12 MB です。これをオーバーライドするには、`CONFIG` プロパティ `ovf.descriptor.size.max` を編集します。
- マニフェスト ファイル（.mf 拡張子）のデフォルトの最大許容サイズが 1 MB であることを確認します。
- OVF パッケージが OVF XSD スキーマに準拠していることを確認します。
- ハードウェア バージョンが OVF 記述子ファイルの `VirtualSystemType` 要素で指定されている場合は、そのバージョンが OVF をアップロードする仮想データセンターでサポートされている最新のハードウェア バージョンよりも低いことを確認します。
- OVF 記述子ファイルに `ExtraConfig` 要素が含まれている場合は、システム管理者がこれらの要素を `extraConfigs` 要素の `AllowedList` に含めていることを確認します。`AllowedList` に含まれていない要素があると、OVF のアップロードが検証エラーで失敗します。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [vApp] を選択します。
- 2 [OVF から vApp を追加] をクリックします。

- 3 [アップロード] () ボタンをクリックしてコンピュータからアクセス可能な場所を参照し、OVF/OVA テンプレート ファイルを選択します。

アクセス可能な場所にはローカルのハード ドライブ、ネットワーク共有、または CD/DVD ドライブなどがあります。サポートされているファイル拡張子は、.ova、.ovf、.vmdk、.mf、.cert、.strings です。アップロードするファイルよりも多くのファイル（たとえば VMDK ファイル）を参照する OVF ファイルをアップロードするように選択した場合は、すべてのファイルを参照して選択する必要があります。

- 4 [次へ] をクリックします。
- 5 デプロイする OVF/OVA テンプレートの詳細を確認し、[次へ] をクリックします。
- 6 vApp の名前と、必要に応じて説明を入力して、[次へ] をクリックします。
- 7 (オプション) vApp のコンピュータ名を変更して、英数字のみが含まれるようにします。

この手順は、vApp の名前にスペースまたは特殊文字が含まれている場合にのみ必要です。デフォルトでは、コンピュータ名に仮想マシンの名前があらかじめ入力されています。ただし、コンピュータ名には英数字のみを使用する必要があります。

- 8 [ストレージ ポリシー] ドロップダウン メニューから、vApp の各仮想マシンのストレージ ポリシーを選択し、[次へ] をクリックします。

- 9 各仮想マシンを接続するネットワークを選択します。

- [ネットワーク] ドロップダウン メニューから、各仮想マシンのネットワークを選択します。
- [詳細ネットワークのワークフローに切り替える] チェック ボックスを選択し、vApp 内の各仮想マシンのプライマリ NIC、ネットワーク アダプタ タイプ、ネットワーク、IP アドレスの割り当て、IP アドレスの設定などのネットワーク設定を手動で入力できます。

ウィザードを完了した後、仮想マシンの追加プロパティを構成することができます。

- 10 [次へ] をクリックします。
- 11 vApp 内の仮想マシンのハードウェアをカスタマイズし、[次へ] をクリックします。

オプション	説明
仮想 CPU の数	vApp 内の各仮想マシンの仮想 CPU の数を入力します。 仮想マシンに割り当てることができる仮想 CPU の最大数は、ホストの論理 CPU 数、および仮想マシンにインストールされたゲスト OS の種類によって決まります。
ソケットあたりのコア数	vApp 内の各仮想マシンのソケットあたりのコア数を入力します。 コアおよびソケットごとのコアに関する、仮想 CPU の割り当て方法を構成できます。シングルコア CPU、デュアルコア CPU、トライコア CPU などを使用するかどうかにより、仮想マシンの CPU コアの数指定してから、各ソケットに対するコアの数を選択します。
コアの数	vApp 内の各仮想マシンのコア数を表示します。 仮想 CPU の数を更新すると、数が変わります。
メモリの合計 (MB)	vApp 内の各仮想マシンのメモリを MB 単位で入力します。 この設定は、仮想マシンに割り当てられる ESXi ホスト メモリの容量を決定します。仮想ハードウェアのメモリ サイズでは、仮想マシンで実行されるアプリケーションで使用可能なメモリの容量を決定します。仮想マシンは、仮想ハードウェアのメモリ サイズとして構成されたメモリ リソース以上のメモリ リソースを利用できません。

12 [設定内容の確認] 画面で設定内容を確認し、[完了] をクリックします。

結果

新しい vApp がカード ビューに表示されます。

vApp テンプレートからの vApp の作成

アクセスできるカタログ内に保存されている vApp テンプレートに基づいて、新規 vApp を作成できます。

仮想マシンをカスタマイズするための OVF プロパティを含む OVF ファイルに vApp テンプレートに基づいている場合、これらのプロパティは vApp に渡されます。プロパティがユーザー構成可能な場合は、値を指定できます。

前提条件

- 公開カタログ内の vApp テンプレートには、組織管理者または vApp 作成者のみがアクセスできます。
- vApp ユーザー以上の権限を持っている場合、共有されている組織カタログ内の vApp テンプレートにアクセスできます。

手順

- 1** メイン メニュー (≡) で [ライブラリ] を選択し、左側のパネルで [vApp テンプレート] を選択します。
テンプレートのリストがグリッド ビューに表示されます。
- 2** vApp としてデプロイする vApp テンプレートの左側にあるリスト バー (⋮) をクリックし、[vApp の作成] を選択します。
- 3** ウィザードの [ライセンスを承諾] 画面でエンド ユーザー使用許諾契約書を読み、[承諾] をクリックします。
- 4** [次へ] をクリックします。
- 5** vApp の名前と、必要に応じて説明を入力します。
- 6** 自動的に停止する前にこの vApp が実行できる期間（時間または日単位）を指定します。
- 7** 自動的にクリーンアップされるまでに停止した vApp が使用可能な期間（時間または日単位）を指定します。
- 8** [次へ] をクリックします。
- 9** vApp を作成する仮想データセンターを選択します。
- 10** ストレージ ポリシーを選択します。
- 11** [次へ] をクリックします。
- 12** 各仮想マシンを接続するネットワークを選択します。
 - [ネットワーク] ドロップダウン メニューから、各仮想マシンのネットワークを選択します。
 - [詳細ネットワークのワークフローに切り替える] チェック ボックスを選択し、vApp 内の各仮想マシンのプライマリ NIC、ネットワーク アダプタ タイプ、ネットワーク、IP アドレスの割り当て、IP アドレスの設定などのネットワーク設定を手動で入力できます。

ウィザードを完了した後、仮想マシンの追加プロパティを構成することができます。

13 [次へ] をクリックします。

14 vApp 内の仮想マシンのハードウェアをカスタマイズし、[次へ] をクリックします。

オプション	説明
仮想 CPU の数	vApp 内の各仮想マシンの仮想 CPU の数を入力します。 仮想マシンに割り当てることができる仮想 CPU の最大数は、ホストの論理 CPU 数、および仮想マシンにインストールされたゲスト OS の種類によって決まります。
ソケットあたりのコア数	vApp 内の各仮想マシンのソケットあたりのコア数を入力します。 コアおよびソケットごとのコアに関する、仮想 CPU の割り当て方法を構成できます。シングルコア CPU、デュアルコア CPU、トライコア CPU などを使用するかどうかにより、仮想マシンの CPU コアの数を選択してから、各ソケットに対するコアの数を選択します。
コアの数	vApp 内の各仮想マシンのコア数を表示します。 仮想 CPU の数を更新すると、数が変わります。
メモリの合計 (MB)	vApp 内の各仮想マシンのメモリを MB 単位で入力します。 この設定は、仮想マシンに割り当てられる ESXi ホスト メモリの容量を決定します。仮想ハードウェアのメモリ サイズでは、仮想マシンで実行されるアプリケーションで使用可能なメモリの容量を決定します。仮想マシンは、仮想ハードウェアのメモリ サイズとして構成されたメモリ リソース以上のメモリ リソースを利用できません。
ハード ディスクのプロパティ	仮想マシンのハード ディスクのサイズを MB 単位で入力します。

15 [設定内容の確認] 画面で設定内容を確認し、[完了] をクリックします。


結果

新しい vApp がカード ビューに表示されます。

vApp を開く

vApp を開いて、含まれる仮想マシンとネットワークを表示できます。また、仮想マシンとネットワークがどのように接続されるかを示す図を表示することもできます。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [vApp] を選択します。
- 2  をクリックしてカード ビュー内の vApps を表示します。
- 3 カード ビューでは、vApp に関連付けられている仮想マシンの数、リース情報、総 CPU 数、ストレージとメモリの合計、関連付けられているネットワーク、およびスナップショットを作成したかどうか、などの全般的な情報を確認できます。
- 4 選択した vApp の詳細設定を表示するには、vApp カードの [詳細] をクリックします。

vApps での電源の操作の実行

vApp のパワーオンまたはパワーオフ、vApp のサスペンドまたはリセットなど、vApp での電源の操作を実行できます。


vApp のパワーオン

vApp をパワーオンすると、vApp 内でパワーオンされていない仮想マシンがすべてパワーオンされます。

前提条件

少なくとも vApp 作成者である必要があります。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [vApp] を選択します。
- 2  をクリックしてカード ビュー内の vApps を表示します。
- 3 パワーオンする vApp の [アクション] メニューから、[パワーオン] を選択します。

結果

vApp がパワーオンされます。


vApp のパワーオフ

vApp をパワーオフすると、vApp 内のすべての仮想マシンがパワーオフされます。特定のアクションを実行する前に vApp をパワーオフする必要があります。たとえば、vApp のカタログへの追加、コピー、別の VDC への移動などです。

前提条件

vApp が開始されている必要があります。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [vApp] を選択します。
- 2  をクリックしてカード ビュー内の vApps を表示します。
- 3 停止する vApp の [アクション] メニューから、[パワーオフ] を選択します。
- 4 [OK] をクリックします。

結果

vApp 内のすべての仮想マシンと vApp 自体がパワーオフ状態になります。


vApp の停止

vApp を停止すると、vApp 内の仮想マシンがすべてパワーオフまたはシャットダウンされます。特定のアクションを実行する前に vApp を停止する必要があります。たとえば、vApp のカタログへの追加、コピー、別の VDC への移動などです。

前提条件

vApp が開始されている必要があります。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [vApp] を選択します。
- 2  をクリックしてカード ビュー内の vApps を表示します。
- 3 停止する vApp の [アクション] メニューから、[停止] を選択します。
- 4 [OK] をクリックします。

結果

vApp 内のすべての仮想マシンと vApp 自体がパワーオフまたはシャットダウンされます。


vApp のリセット

vApp をリセットすると、状態（メモリ、キャッシュなど）はクリアされますが、vApp は実行し続けます。

前提条件

vApp が起動されていて、内部の仮想マシンがパワーオン状態になっている必要があります。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [vApp] を選択します。
- 2  をクリックしてカード ビュー内の vApps を表示します。
- 3 リセットする vApp の [アクション] メニューから、[リセット] を選択します。

結果

状態がクリアされ、vApp は引き続き実行されます。


vApp のサスペンド

vApp をサスペンドすると、メモリの内容をディスクに書き込むことによって現在の状態が保持されます。

前提条件

vApp が実行されている必要があります。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [vApp] を選択します。
- 2  をクリックしてカード ビュー内の vApps を表示します。
- 3 サスペンドする vApp の [アクション] メニューから、[サスペンド] を選択します。

結果

vApp はサスペンドされ、その状態が保持されます。


vApp の一時停止状態の破棄

vApp がサスペンド状態で、vApp の使用を再開する必要がなくなった場合は、サスペンド状態を破棄できます。サスペンド状態を破棄すると、保存済みメモリは削除され、vApp はパワーオフ状態に戻ります。

前提条件

vApp はサスペンド状態にする必要があります。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [vApp] を選択します。
- 2  をクリックしてカード ビュー内の vApps を表示します。
- 3 サスペンド状態の vApp の [アクション] メニューから、[サスペンド状態を破棄] を選択します。

結果

状態は破棄され、vApp がパワーオフされます。

vApp のプロパティの編集

vApp の名前と説明、リース設定、vApp で仮想マシンを起動する順序、共有設定、ネットワーク設定など、既存の vApp のプロパティを編集できます。

vApp の全般プロパティの編集

vApp の名前、説明、およびその他の全般プロパティは確認して変更することができます。

前提条件

vApp がパワーオフされていることを確認します。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [vApp] を選択します。

- 2  をクリックしてカード ビュー内の vApps を表示します。
- 3 選択した vApp のカードで、vApp のプロパティを表示および編集するために [詳細] をクリックします。
- 4 必要に応じてプロパティを確認して変更し、[保存] をクリックします。

オプション	アクション
名前	vApp の新しい名前を入力します。
説明	オプションで、vApp の説明を入力します。
仮想データセンター	vApp が属するデータセンターの名前。
スナップショット	スナップショットがある場合、その詳細が表示されます。
リース	<p>リースを更新するには、[更新] を選択します。</p> <p>a ランタイム リースの時間数または日数をスケジューリングします。</p> <p>自動的に停止する前に vApp が実行できる期間を定義します。</p> <p>b ストレージ リースの時間または日数をスケジューリングします。</p> <p>vApp が自動的に削除されるまでに使用可能な期間を定義します。</p>

結果

全般設定が保存されます。

vApp の詳細プロパティの編集


仮想マシンの起動および停止の順序を vApp 内で設定できます。特定の順序で起動および停止する必要がある仮想マシンにアプリケーションをインストールした際に、開始および停止の順序を構成します。

この設定は、仮想マシンを特定の順序で起動および停止する必要がある場合に便利です。たとえば、ある仮想マシンでデータベース サーバを、別の仮想マシンでアプリケーション サーバを、さらにもう 1 台の仮想マシンで Web サーバをホストするとします。関連する機能が正しく働くためには、最初にデータベース サーバを、次にアプリケーション サーバを、最後に Web サーバを起動する必要があります。

前提条件

vApp がパワーオフされていることを確認します。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [vApp] を選択します。
- 2  をクリックしてカード ビュー内の vApps を表示します。
- 3 選択した vApp のカードで [詳細] をクリックして、vApp の詳細プロパティまでスクロールダウンします。


4 各仮想マシンの起動および停止の順序プロパティを入力し、[保存] をクリックします。

オプション	アクション
起動の順序	仮想マシンを起動する順序を入力します。各マシンに対して、順番を表す値を入力する必要があります。
アクションを開始	起動アクションを選択します。 起動アクションは、仮想マシンを含んでいる vApp を開始した場合の仮想マシンの動作を決定します。デフォルトでは、このオプションは [パワーオン] に設定されます。
起動待機時間	起動待機時間を入力します。 起動待機時間とは、一連の仮想マシンの中で vCloud Director が次のマシンを起動するまで待機する時間の長さ（秒単位）です。
アクションを停止	停止アクションを選択します。 停止アクションとは、仮想マシンを含んでいる vApp を停止した場合に仮想マシンが実行するアクションです。[パワーオフ] を選択すると、仮想マシンは安定性を確保するためのシャットダウン アクションを実行することなくパワーオフします（ソケットからプラグを抜くことと同じです）。VMware Tools をインストールしていない場合は、このアクションを選択します。それ以外の場合は、シャットダウン時に安定性が確保される [シャットダウン] を選択します。
停止待機時間	停止待機時間を入力します。 停止待機時間とは、一連の仮想マシンの中で vCloud Director が次のマシンを停止するまで待機する時間の長さ（秒単位）です。

vApp を共有

vApp は、所属する組織内の他のグループまたはユーザーと共有することができます。共有 vApp で実行可能な操作は、アクセス コントロールの設定によって決まります。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [vApp] を選択します。
- 2  をクリックしてカード ビュー内の vApps を表示します。
- 3 選択した vApp のカードで [詳細] をクリックして、vApp の共有プロパティまでスクロールダウンします。

4 vApp を共有するユーザーを選択し、[保存] をクリックします。

オプション	アクション
組織内の全員で共有	<p>組織内のすべてのユーザーと共有するにはこのオプションを選択し、アクセス レベルを選択します。</p> <ul style="list-style-type: none"> ■ 完全コントロールを付与するには、[完全コントロール] を選択します。 <p>組織内のすべてのユーザーは、vApp を開く、起動する、vApp テンプレートとして保存する、テンプレートをカタログに追加する、vApp の所有者を変更する、カタログにコピーする、プロパティを変更するなどの操作を行うことができます。</p> <ul style="list-style-type: none"> ■ 読み取り専用アクセス権を付与するには、[読み取り専用] を選択します。
特定のユーザーおよびグループで共有	<p>指定したユーザーのみと共有するには、このオプションを選択します。</p> <ol style="list-style-type: none"> [アクセス権のないユーザーおよびグループ] パネルから名前を選択し、[アクセス権を持つユーザーおよびグループ] パネルに移動します。 指定されたユーザーおよびグループに対してアクセス レベルを選択します。 <ul style="list-style-type: none"> ■ 完全コントロールを付与するには、[完全コントロール] を選択します。 <p>完全コントロールが付与されたユーザーは、vApp を開く、起動する、vApp テンプレートとして保存する、テンプレートをカタログへ追加する、vApp の所有者を変更する、カタログをコピーする、プロパティを変更する、などの操作を行うことができます。</p> <ul style="list-style-type: none"> ■ 読み取り専用アクセス権を付与するには、[読み取り専用] を選択します。

結果

vApp は、指定されたユーザーまたはグループと共有されます。


vApp ネットワーク図の表示

vApp ネットワーク図により、vApp の仮想マシンとネットワークを視覚的に表示できます。

前提条件

vApp ネットワーク図を表示するには、vApp に含まれる仮想マシンを 40 台未満にする必要があります。vApp に 40 台を超える仮想マシンが含まれている場合、この図は使用できません。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [vApp] を選択します。
- 2  をクリックしてカード ビュー内の vApps を表示します。
- 3 選択した vApp のカードで、[詳細] をクリックします。
- 4 [ネットワーク図] タブをクリックします。

vApp 内の仮想マシンとネットワークの接続方法を示す図が表示されます。星印は、プライマリ NIC を表します。NIC が接続されている場合、該当する NIC は緑色に、NIC が接続されていない場合、白色になります。

- 5** (オプション) 接続されている仮想マシンとネットワークをハイライト表示するには、ネットワークまたは仮想マシンをクリックします。

接続されたオブジェクトとその間の接続がハイライト表示されます。

次のステップ

この画面から仮想マシンまたはネットワークを追加できます。

vApp でのネットワークの作業

vApp の仮想マシンは、vApp ネットワーク（隔離または経路指定）および組織仮想データセンター ネットワーク（直接またはフェンスあり）に接続できます。複数のネットワーク シナリオに対処するために、vApp へは異なるタイプのネットワークを追加できます。

vApp 内の仮想マシンは、vApp が使用できるネットワークに接続できます。仮想マシンを異なるネットワークに接続するには、そのネットワークを vApp にまず追加する必要があります。

vApp には、vApp ネットワークと組織仮想データセンター ネットワークを含めることができます。vApp ネットワークは、隔離または経路指定できます。隔離された vApp ネットワークは、vApp 内に含まれます。vApp ネットワークを組織仮想データセンター ネットワークに経路指定して、vApp 外の仮想マシンに対して接続を提供することもできます。経路指定された vApp ネットワークの場合、ファイアウォールや固定ルーティングなどのネットワーク サービスを構成できます。

vApp を組織仮想データセンター ネットワークに直接接続できます。同じ組織仮想データセンター ネットワークに接続されている同一仮想マシンを含む vApp が複数あり、これらの vApp を同時に開始させる場合は、vApp をフェンスできます。vApp をフェンスすると、MAC アドレスおよび IP アドレスを分離し、競合を起こさずに仮想マシンをパワーオンできるようになります。


vApp に追加するネットワークは、vApp を作成した組織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 プールを使用します。

vApp ネットワークの表示


vApp のネットワークにアクセスして表示することができます。

前提条件

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [vApp] を選択します。
- 2  をクリックしてカード ビュー内の vApps を表示します。
- 3 選択した vApp のカードで、[詳細] をクリックします。
- 4 [ネットワーク] タブをクリックします。

ネットワークのリストがある場合は表示されます。各ネットワークに関する情報として名前、ゲートウェイ、ネットマスク、接続などを表示し、IP アドレスと NAT リソースを保持できます。

- 5 (オプション) 表示する列を編集するには、[グリッド エディタ] アイコン () をクリックし、表示するか非表示にするかに応じてそれぞれの列のチェック ボックスを選択または選択解除します。

vApp ネットワークのフェンス


別の vApp に含まれている同一の仮想マシンをパワーオンすると、競合する可能性があります。競合することなく、別の vApp の同一の仮想マシンをパワーオンできるようにするには、vApp をフェンスする必要があります。

vApp をフェンスすると、仮想マシンの MAC アドレスおよび IP アドレスが隔離され、組織 VDC ネットワークの接続タイプが直接からフェンスありに変更されます。フェンスされたネットワーク上でファイアウォールが自動的に有効になり、発信トラフィックのみを許可するように設定されます。vApp をフェンスする際、フェンスされたネットワーク上で NAT ルールとファイアウォール ルールを設定することもできます。

前提条件

- 直接的な vApp ネットワークのみをフェンスできます。vApp が複数のネットワークを使用しており、他のネットワークが経路指定されているなどの場合では、直接ネットワークのみがフェンスされます。
- 直接的な vApp ネットワークが、この時点で使用されないよう、直接ネットワークを使用している vApp 内の仮想マシンを停止する必要があります。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [vApp] を選択します。
- 2  をクリックしてカード ビュー内の vApps を表示します。
- 3 選択した vApp のカードで、[詳細] をクリックします。
- 4 [ネットワーク] タブをクリックします。
- 5 vApp がフェンスされていない場合は、[編集] ボタンをクリックします。
- 6 [vApp のフェンス] オプションを有効にして、[OK] をクリックします。

結果

仮想マシンの IP アドレスおよび MAC アドレスが隔離されます。競合することなく、別の vApp で同一の仮想マシンをパワーオンすることができます。

vApp へのネットワークの追加

ネットワークを vApp に追加すると、vApp の仮想マシンに対してそのネットワークを使用可能にすることができます。vApp には、vApp ネットワークまたは組織仮想データセンター ネットワークを追加できます。


接続は、直接の場合もあれば、フェンスありの場合もあります。フェンスによって、異なる vApp にある同一の仮想マシンの MAC アドレスおよび IP アドレスを分離し、競合を起こさずにそれらの仮想マシンをパワーオンできます。

フェンスが有効になっていて vApp の電源が入っていると、組織仮想データセンターのネットワーク プールから隔離されたネットワークが作成されます。Edge Gateway が作成され、隔離されたネットワークおよび組織仮想データセンター ネットワークに関連付けられます。仮想マシンとの間で送受信されるトラフィックは Edge Gateway を通過し、ここで NAT およびプロキシ AR を使用して IP アドレスが変換されます。これにより、ルーターは同じ IP アドレス空間を使用して 2 つのネットワーク間のトラフィックを通過させることができます。

前提条件

組織仮想データセンター ネットワークを追加するには、管理者がそのようなネットワークを作成している必要があります。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [vApp] を選択します。
- 2  をクリックしてカード ビュー内の vApps を表示します。
- 3 選択した vApp のカードで [アクション] をクリックし、[ネットワークを追加] を選択します。
- 4 追加するネットワークのタイプを選択します。

オプション	アクション
組織 VDC ネットワーク	使用可能なネットワークのリストから組織仮想データセンター ネットワークを選択します。
vApp ネットワーク	<ol style="list-style-type: none"> a ネットワークの名前と、必要に応じて説明を入力します。 b ネットワークのゲートウェイ CIDR を入力します。 c (オプション) プライマリおよびセカンダリ DNS、および DNS サフィックスを入力します。 d (オプション) ゲスト VLAN を許可するかどうかを選択します。 e (オプション) IP アドレス範囲などの固定 IP アドレス プール設定を入力します。 f (オプション) 組織仮想データセンター ネットワークに接続できるようにするには、[組織 VDC ネットワークに接続] オプションを有効にして、リストからネットワークを選択します。

- 5 [追加] をクリックします。

結果

ネットワークが vApp に追加されます。

次のステップ

vApp の仮想マシンをネットワークに接続します。

vApp ネットワークのネットワーク サービスの構成

DHCP、ファイアウォール、ネットワーク アドレス変換 (NAT)、固定ルーティングなどのネットワーク サービスを、特定の vApp ネットワークに対して構成できます。

使用可能なネットワーク サービスは、vApp ネットワークのタイプによって異なります。


表 3-1. ネットワーク タイプ別の使用可能なネットワーク サービス

vApp ネットワークのタイプ	DHCP	ファイアウォール	NAT	固定ルーティング
直接				
経路指定	X	X	X	X
隔離	X			

ネットワーク全般の詳細の表示および編集

ネットワーク名や説明など、vApp ネットワーク全般の詳細を表示および編集することができます。


手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [vApp] を選択します。
- 2  をクリックしてカード ビュー内の vApps を表示します。
- 3 選択した仮想アプライアンスのカードで、[詳細] をクリックします。
- 4 [ネットワーク] タブで、ネットワークの詳細を表示するネットワークをクリックします。
- 5 [全般] タブでネットワーク情報を確認します。
- 6 [[編集]]をクリックします。
- 7 vApp ネットワークの名前および説明を編集します。
- 8 [保存] をクリックします。

vApp ネットワークの固定 IP アドレス プール設定の編集

固定 IP アドレス プールから固定 IP アドレスを取得することによって、vApp ネットワークを構成し、固定 IP アドレスを vApp 内の仮想マシンに提供することができます。


手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [vApp] を選択します。
- 2  をクリックしてカード ビュー内の vApps を表示します。
- 3 選択した仮想アプライアンスのカードで、[詳細] をクリックします。
- 4 [ネットワーク] タブで、ネットワークの詳細を表示するネットワークをクリックします。
- 5 [IP アドレス管理] タブで [固定プール] をクリックします。
- 6 [[編集]]をクリックします。
- 7 IP アドレス範囲を入力し、[追加] をクリックします。
- 8 [保存] をクリックします。

vApp ネットワークの DNS 設定の編集

vApp ネットワークを作成すると、DNS 設定をいつでも表示および編集できます。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [vApp] を選択します。
- 2  をクリックしてカード ビュー内の vApps を表示します。
- 3 選択した仮想アプライアンスのカードで、[詳細] をクリックします。
- 4 [ネットワーク] タブで、ネットワークの詳細を表示するネットワークをクリックします。
- 5 [IP アドレス管理] タブで [DNS] をクリックします。
DNS 設定が表示されます。
- 6 [[編集]]をクリックします。
- 7 プライマリ DNS、セカンダリ DNS、および DNS サフィックスを編集します。
- 8 [保存] をクリックします。

vApp ネットワークの DHCP の構成


vApp の仮想マシンに DHCP サービスを提供するために、特定の vApp ネットワークを構成できます。

vApp ネットワークに対して DHCP を有効にし、vApp の仮想マシンの NIC をネットワークに接続し、NIC の IP モードとして DHCP を選択します。vCloud Director は、仮想マシンをパワーオンしたときに、DHCP IP アドレスをその仮想マシンに割り当てます。

前提条件

経路指定されている vApp ネットワークまたは隔離されている vApp ネットワーク。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [vApp] を選択します。
- 2  をクリックしてカード ビュー内の vApps を表示します。
- 3 選択した仮想アプライアンスのカードで、[詳細] をクリックします。
- 4 [ネットワーク] タブで、ネットワークの詳細を表示するネットワークをクリックします。
- 5 [IP アドレス管理] タブで、[DHCP] をクリックします。
DHCP の状態が表示されます。
- 6 [[編集]]をクリックします。
- 7 [有効] をクリックします。

- 8 [IP プール] テキスト ボックスで、IP アドレスの範囲を入力します。


vCloud Director は、これらのアドレスを使用して DHCP 要求に対応します。DHCP IP アドレスの範囲は、vApp ネットワークの固定 IP プールと重複できません。

- 9 デフォルトの最大リース時間を秒単位で設定します。
- 10 [保存] をクリックします。

vApp ネットワークの IP の割り当ての表示

vApp のネットワークの IP 割り当ては、確認することができます。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [vApp] を選択します。
- 2  をクリックしてカード ビュー内の vApps を表示します。
- 3 選択した仮想アプライアンスのカードで、[詳細] をクリックします。
- 4 [ネットワーク] タブで、ネットワークの詳細を表示するネットワークをクリックします。
- 5 [IP アドレス管理] タブで [IP の割り当て] をクリックします。

割り当てられた IP アドレスが表示されます。

vApp ネットワークの固定ルーティングの設定


特定の vApp ネットワークを設定して、固定ルーティング サービスを提供し、異なる vApp ネットワーク上の仮想マシン間の通信を可能にすることができます。

作成するすべての固定ルートは自動的に有効になります。

前提条件

経路指定されている vApp ネットワーク。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [vApp] を選択します。
- 2  をクリックしてカード ビュー内の vApps を表示します。
- 3 選択した仮想アプライアンスのカードで、[詳細] をクリックします。
- 4 [ネットワーク] タブで、ネットワークの詳細を表示するネットワークをクリックします。
- 5 [ルーティング] タブで、[編集] をクリックします。

ネットワークの固定ルーティングを無効または有効にできます。

vApp ネットワークの固定ルーティングの追加

固定ルートは、同じ組織仮想データセンター ネットワークにルーティングされている 2 つの vApp ネットワーク間に追加できます。固定ルートにより、ネットワーク間のトラフィックが許可されます。


固定ルートは、フェンスされた vApp や重複しているネットワーク間に追加することはできません。固定ルートを vApp ネットワークに追加したら、固定ルートでトラフィックが許可されるようにネットワーク ファイアウォールルールを構成します。固定ルートを持つ vApp に対しては、この vApp または関連付けられているネットワークが削除されるまで割り当てられた IP アドレスを使用するように構成します。

固定ルートは、これらのルートを含む vApp が実行されている場合にのみ機能します。vApp の親ネットワークの変更、vApp の削除、または vApp ネットワークの削除を実行し、その vApp に固定ルートが含まれている場合、これらのルートは機能することができず、手動で削除しなければなりません。

前提条件

- 2 つの vApp ネットワークは、同じ組織仮想データセンター ネットワークにルーティングされています。
- vApp ネットワークは、少なくとも 1 回は開始された vApp にあります。
- 固定ルーティングは、両方の vApp ネットワークで有効化されています。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [vApp] を選択します。
- 2  をクリックしてカード ビュー内の vApps を表示します。
- 3 選択した仮想アプライアンスのカードで、[詳細] をクリックします。
- 4 [ネットワーク] タブで、ネットワークの詳細を表示するネットワークをクリックします。
- 5 [ルーティング] タブの [固定ルーティング] で [追加] をクリックします。
割り当てられた IP アドレスが表示されます。
- 6 固定ルートの名前を入力します。
- 7 ネットワーク アドレスを CIDR 形式で入力します。
ネットワーク アドレスは、固定ルートを追加する対象の vApp ネットワークに対するものです。
- 8 ネクスト ホップ IP アドレスを入力します。
次ホップ IP アドレスは、その vApp ネットワークのルーターの外部 IP アドレスです。
- 9 [保存] をクリックします。
- 10 2 つ目の vApp ネットワークに対しても同じ手順を繰り返します。

例：固定ルーティング例

vApp Network 1 および vApp Network 2 は両方とも、Org Network Shared に経路指定されています。各 vApp ネットワークで固定ルートを作成し、ネットワーク間のトラフィックを可能にします。固定ルートを作成するには、vApp ネットワークに関する情報を使用できます。

表 3-2. ネットワーク情報

ネットワーク名	ネットワーク仕様	ルーターの外部 IP アドレス
vApp Network 1	192.168.1.0/24	192.168.0.100
vApp Network 2	192.168.2.0/24	192.168.0.101
Org Network Shared	192.168.0.0/24	該当なし

vApp Network 1 で、vApp Network 2 への固定ルートを作成します。vApp Network 2 で、vApp Network 1 への固定ルートを作成します。

表 3-3. 固定ルーティング設定

vApp ネットワーク	ルート名	ネットワーク	次ホップ IP アドレス
vApp Network 1	tovapp2	192.168.2.0/24	192.168.0.101
vApp Network 2	tovapp1	192.168.1.0/24	192.168.0.100


vApp ネットワークの削除

vApp のネットワークが不要になったら、そのネットワークを削除できます。

前提条件

vApp は停止しており、vApp の仮想マシンはいずれもネットワークに接続されていません。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [vApp] を選択します。
- 2  をクリックしてカード ビュー内の vApps を表示します。
- 3 選択した仮想アプライアンスのカードで、[詳細] をクリックします。
- 4 [ネットワーク] タブで削除するネットワークを選択し、[削除] をクリックして削除を確定します。

スナップショットの操作

スナップショットを作成すると、特定の時点での vApp 内の仮想マシンの状態とデータが保持されます。スナップショットは、長期間にわたって使用したり、vApp をバックアップする代わりに使用するための機能ではありません。

vApp 内の仮想マシンをアップグレードするときにスナップショットを使用できます。たとえば、仮想マシンをアップグレードする前に、スナップショットを作成してアップグレード前の時点での状態を保持します。つまり、アップグレード前にスナップショットを保存し、それからアップグレードを実行します。アップグレード中に問題が発生しなかった場合は、スナップショットを削除して、アップグレード中に行った変更をコミットできます。一方で問題が発生した場合は、スナップショットの復帰を行うことにより、保存したアップグレード前の状態に vApp を戻すことができます。

vApp のスナップショットの作成


vApp のスナップショットを作成すると、vApp 内のすべての仮想マシンのスナップショットが作成されます。スナップショットを作成したら、vApp のすべての仮想マシンをスナップショットに戻すことができます。また、必要のないスナップショットを削除することもできます。

vApp スナップショットには、いくつかの制限事項があります。

- vApp スナップショットでは NIC 構成はキャプチャされません。
- vApp 内の仮想マシンのいずれかが名前付きディスクに接続されている場合、vApp スナップショットを作成することはできません。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [vApp] を選択します。

- 2  をクリックしてカード ビュー内の vApps を表示します。

- 3 スナップショットを作成する vApp の [アクション] メニューから、[スナップショットの作成] を選択します。

vApp のスナップショットを作成すると、既存のスナップショットがある場合には置き換えられます。

- 4 (オプション) vApp のメモリのスナップショットを作成するかどうかを選択します。

vApp のメモリの状態を取得する場合、スナップショットは vApp と vApp 内の仮想マシンのライブ状態を保持します。メモリ スナップショットでは、稼働中のソフトウェアをアップグレードするときなど、ある特定の時点でのスナップショットが作成されます。メモリ スナップショットを作成しておけば、アップグレードが予想どおりに完了しなかったとき、またはソフトウェアが期待に添うものでなかったときに、仮想マシンを元の状態に戻すことができます。

メモリ状態の取得時に vApp のファイルを静止させる必要はありません。メモリの状態を取得しない場合、スナップショットは vApp のライブ状態を保存せず、ディスクは、静止しないかぎりクラッシュ時の整合性を保ちます。

- 5 (オプション) ゲスト ファイル システムを静止するかどうかを選択します。

この操作を行うには、vApp 内の仮想マシンに VMware Tools がインストールされている必要があります。仮想マシンを静止する場合、VMware Tools によって仮想システム内のファイル システムが静止されます。静止操作により、スナップショット ディスクはゲスト ファイル システムの一貫した状態を表します。静止スナップショットは、自動バックアップや定期バックアップに適しています。たとえば、仮想マシンのアクティビティを把握していなくとも、最新の復元用バックアップが欲しいという場合に、ファイルを静止することができます。

大容量ディスクがある vApp を静止させることはできません。

- 6 [OK] をクリックします。

結果

vApp のスナップショットが作成されます。

次のステップ

vApp 内のすべての仮想マシンを最新のスナップショットに戻すことができます。


vApp をスナップショットに戻す

vApp のすべての仮想マシンを、vApp スナップショットを作成した時点の状態に戻すことができます。

前提条件

vApp に既存のスナップショットがあることを確認します。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [vApp] を選択します。
- 2  をクリックしてカード ビュー内の vApps を表示します。
- 3 元の状態に戻す vApp の [アクション] メニューから、[スナップショットに戻す] を選択します。
- 4 [OK] をクリックします。

結果

vApp 内のすべての仮想マシンがスナップショットの状態に戻されます。

vApp のスナップショットの削除


vApp のスナップショットを削除できます。

vApp のスナップショットを削除すると、その vApp のスナップショットに含まれている仮想マシンの状態が削除されるため、二度とその状態には戻れなくなります。スナップショットを削除しても、vApp の現在の状態に影響はありません。

前提条件

vApp のスナップショットを取得している。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [vApp] を選択します。
- 2  をクリックしてカード ビュー内の vApps を表示します。
- 3 スナップショットを削除する vApp の [アクション] メニューから、[スナップショットの削除] を選択します。
- 4 [OK] をクリックします。

結果

スナップショットが削除されます。


vApp の所有者の変更

たとえば、vApp 所有者が会社を退職したり、会社内でのロールが変わったりした場合は、vApp の所有者を変更できます。

前提条件

この操作には、事前定義の組織管理者ロールに含まれている権限、またはそれに相当する権限が必要です。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [vApp] を選択します。
- 2  をクリックしてカード ビュー内の vApps を表示します。
- 3 所有者を変更する vApp の [アクション] メニューから、[所有者を変更] を選択します。
- 4 リストからユーザーを選択します。
- 5 [OK] をクリックします。

結果

vApp の所有者が変更されます。


別の仮想データセンターへの vApp の移動

vApp を別の仮想データセンターに移動すると、その vApp はソース仮想データセンターから削除されます。

前提条件

- 少なくとも vApp 作成者である必要があります。
- vApp がパワーオフ状態である必要があります。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [vApp] を選択します。
- 2  をクリックしてカード ビュー内の vApps を表示します。
- 3 移動する vApp の [アクション] メニューから [移動] を選択します。
- 4 vApp を移動する仮想データセンターを選択し、[OK] をクリックします。
- 5 (オプション) ストレージ ポリシーを選択します。
- 6 [OK] をクリックします。

結果

vApp が元のデータセンターから削除され、選択したデータセンターに移動します。


別の仮想データセンターへの停止した vApp のコピー

vApp を別の仮想データセンターにコピーする場合、コピー元の vApp はソース仮想データセンターに残されます。

前提条件

- 少なくとも vApp 作成者である必要があります。
- vApp がパワーオフ状態である必要があります。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [vApp] を選択します。
- 2  をクリックしてカード ビュー内の vApps を表示します。
- 3 コピーする vApp の [アクション] メニューから [コピー] を選択します。
- 4 名前と説明を入力します。
- 5 vApp のコピーを作成する仮想データセンターを選択します。
- 6 (オプション) ストレージ ポリシーを選択します。
- 7 [OK] をクリックします。

結果

vApp は、指定した仮想データセンターに、指定した名前と説明でコピーされます。

パワーオン状態の vApp のコピー


既存の vApp に基づいて vApp を作成するには、vApp をコピーし、必要に応じてそのコピーを変更できます。vApp をコピーする前に、vApp の仮想マシンをパワーオフする必要はありません。実行中の仮想マシンのメモリ状態は、コピーされた vApp に保存されます。

前提条件

以下の条件を満たしていることを確認します。

- 少なくとも vApp ユーザー である必要があります。
- 組織仮想データセンターが、vCenter Server 5.5 以降によってバックアップされます。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [vApp] を選択します。
- 2  をクリックしてカード ビュー内の vApps を表示します。
- 3 コピーする vApp の [アクション] メニューから [コピー] を選択します。

- 4 名前と説明を入力します。
- 5 vApp のコピーを作成する仮想データセンターを選択します。
- 6 (オプション) ストレージ ポリシーを選択します。
- 7 [OK] をクリックします。

結果

vApp のコピーが作成され、vApp コピーがサスペンド状態になります。コピーされた vApp は、ネットワーク フェンスに対して有効化されます。

次のステップ

新しい vApp のネットワーク プロパティを変更するか、vApp をパワーオンします。


仮想マシンの vApp への追加

vApp に仮想マシンを追加できます。

前提条件

公開カタログの仮想マシンにアクセスするためには、組織管理者または vApp 作成者である必要があります。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [vApp] を選択します。
- 2  をクリックしてカード ビュー内の vApps を表示します。
- 3 仮想マシンを追加する vApp の [アクション] メニューから、[仮想マシンを追加] を選択します。
[仮想マシンを追加] ウィンドウで、vApp に関連付けられている仮想マシンのリストが表示されます。
- 4 新しい仮想マシンを作成して vApp に自動的に関連付けるには、[仮想マシンを追加] をクリックします。
- 5 仮想マシンの名前とコンピュータ名を入力します。

重要： コンピュータ名には、英数字とハイフンのみを含めることができます。コンピュータ名は、数字のみで設定したり、スペースを含めたりすることはできません。

- 6 (オプション) わかりやすい説明を入力します。
- 7 仮想マシンを作成直後にパワーオンするかどうかを選択します。

8 仮想マシンを展開する方法を選択します。

オプション	アクション
新規	<p>カスタマイズ可能な設定で新しい仮想マシンを展開します。</p> <ul style="list-style-type: none"> a オペレーティング システム ファミリーとオペレーティング システムを選択します。 b (オプション) ブート イメージを選択します。 c コンピューティング ポリシーを選択します。 d 仮想マシンのサイズを選択するか、または [カスタム サイズ変更オプション] をクリックして、コンピューティング、メモリ、およびストレージの設定を手動で入力します。 <p>事前定義済みのサイズ変更オプションには、小、中、大があります。</p> <ul style="list-style-type: none"> e ストレージ ポリシーや GB 単位のサイズなど、仮想マシンのストレージ設定を指定します。 f ネットワーク、IP モード、IP アドレス、プライマリ NIC など、仮想マシンのネットワーク設定を指定します。
テンプレートから	<p>テンプレート カタログで選択したテンプレートから仮想マシンを展開します。</p> <ul style="list-style-type: none"> a カタログから仮想マシン テンプレートを選択します。 b (オプション) カスタム ストレージ ポリシーを使用するように選択し、[使用するカスタム ストレージ ポリシー] からポリシーを選択します。 c 使用可能なエンド ユーザー使用許諾契約書がある場合は、これを確認し、承諾する必要があります。

9 [OK] をクリックして、仮想マシンを作成します。

10 [追加] をクリックして、仮想マシンを vApp に追加します。

vApp の vApp テンプレートとしてのカタログへの保存

vApp をカタログに追加することで、特定の vApp を vApp テンプレートに変換します。

前提条件

- この操作には、事前定義の vApp 作成者ロールに含まれている権限、またはそれに相当する権限が必要です。
- 組織には、1 つのカタログおよび使用可能な容量のある仮想データセンターが必要です。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [vApp] を選択します。

- 2  をクリックしてカード ビュー内の vApps を表示します。

- 3 カタログに追加する vApp の [アクション] メニューから [カタログに追加] を選択します。

注： vApp に属している仮想マシンが実行中の状態であるとしても、vApp をカタログに追加できます。実行中の vApp を選択すると、vApp テンプレートとしてカタログに追加され、すべての仮想マシンはサスペンド状態になります。

- 4 [カタログ] ドロップダウン メニューからターゲット カタログを選択します。

- 5 vApp テンプレートの名前と、オプションで説明を入力します。
- 6 (オプション) 既存の vApp テンプレートを新規のカタログ項目で上書きする場合は、[カタログ項目の上書き] を選択し、上書きするカタログ項目を選択します。

たとえば、新しいバージョンの vApp をカタログにアップロードする場合、古いバージョンを上書きすることができます。

- 7 テンプレートの使用方法を指定します。

この設定は、vApp テンプレートに基づいて vApp を作成するときに適用されます。このテンプレートから個々の仮想マシンを使用して vApp を構築する場合には、このオプションは無視されます。

オプション	説明
同一のコピーを作成	vApp テンプレートから vApp を作成する場合に、vApp の同一のコピーを作成するために選択します。
仮想マシン設定をカスタマイズ	vApp テンプレートから vApp を作成する場合に、仮想マシン設定のカスタマイズを有効にするときに選択します。

- 8 vApp テンプレートの作成を完了するには、[OK] をクリックします。

結果

vApp は vApp テンプレートとして保存され、指定されたカタログに表示されます。

OVF パッケージとしての vApp のダウンロード

vApp は OVF パッケージとしてダウンロードすることも、OVF パッケージを単一ファイルとして配布する OVA としてダウンロードすることもできます。

前提条件

- この操作には、事前定義の vApp 作成者ロールに含まれている権限、またはそれに相当する権限が必要です。
- vApp がパワーオフされており、デプロイ解除されていることを確認します。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [vApp] を選択します。



- 2  をクリックしてカード ビュー内の vApps を表示します。

- 3 ダウンロードする vApp の [アクション] メニューから [ダウンロード] を選択します。

- 4 vApp をダウンロードする形式を選択します。

- 5 (オプション) [ID 情報の保存] を選択すると、vApp 内にある仮想マシンの UUID および MAC アドレスがダウンロードされた OVF パッケージに含まれます。

これによりパッケージの移植性が制限されるため、必要な場合にのみ使用してください。

- 6 [OK] をクリックして、選択肢を確認し、ダウンロードを開始します。

結果

デフォルトでは、パッケージがブラウザのダウンロードフォルダにダウンロードされます。

vApp リースの更新

vApp のリースの有効期限が切れた場合、または有効期限が切れそうになっている場合は、更新することができます。

前提条件

この操作には、事前定義の vApp ユーザーロールに含まれている権限、またはそれに相当する権限が必要です。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [vApp] を選択します。
- 2 更新する vApp を選択します。
- 3 [アクション] メニューから、[リースの更新] を選択します。

結果

リースが更新されます。[リース] フィールドに新しいリース期間が表示されます。

vApp の削除

vApp を削除すると、組織からも削除されます。

前提条件

vApp は停止している必要があります。

少なくとも vApp 作成者である必要があります。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [vApp] を選択します。
- 2 削除する vApp を選択します。
- 3 [アクション] メニューから [削除] を選択します。
- 4 [OK] をクリックします。

結果

vApp が削除されます。

組織仮想データセンター ネットワークの管理

4

組織 VDC ネットワークは、システム管理者または組織管理者によって作成され、組織 VDC に割り当てられます。組織管理者は、ネットワークに関する情報の表示やネットワーク サービスの構成などを行うことができます。

NSX Data Center for vSphere でバックアップされた使用可能な組織仮想データセンター ネットワークのタイプには、直接、経路指定、内部、またはクロス VDC があります。

NSX-T Data Center でバックアップされた使用可能な組織データセンター ネットワークのタイプには、経路指定、内部、およびインポートがあります。

表 4-1. 組織 VDC ネットワークのタイプ

データセンター タイプのネットワーク	説明
直接	<p>システム管理者がプロビジョニングし、vSphere リソースによってバックアップされる外部ネットワークの 1 つに直接接続された組織 VDC ネットワーク。</p> <p>直接ネットワークは、NSX Data Center for vSphere によってバックアップされている組織 VDC でのみサポートされています。</p> <p>複数の組織 VDC からアクセスできます。異なる組織 VDC に属する仮想マシンがこのネットワークに接続して、トラフィックを確認できます。</p> <p>このネットワークは、組織 VDC 外の仮想マシンに対して直接レイヤー 2 接続を提供します。この組織 VDC 外の仮想マシンは、組織 VDC 内の仮想マシンに直接接続できます。</p> <p>注： 直接の組織 VDC ネットワークを追加できるのは、システム管理者のみです。</p> <p>IPv4 または IPv6 を選択します。</p>
隔離（内部）	<p>同じ組織 VDC のみからアクセスできます。この組織 VDC 内の仮想マシンのみが、内部組織 VDC ネットワークに接続して、トラフィックを表示できます。</p> <p>隔離ネットワークは、NSX-T Data Center によってバックアップされている組織 VDC と組織 VDC の NSX Data Center for vSphere でサポートされています。</p> <p>隔離された組織 VDC ネットワークは、組織 VDC に、複数の仮想マシンおよび vApp を接続できる隔離されたプライベート ネットワークを提供します。このネットワークは、この組織 VDC の外部にある仮想マシンへの接続は提供しません。この組織 VDC 外のマシンは、組織 VDC 内のマシンに接続できません。</p>
経路指定	<p>同じ組織 VDC のみからアクセスできます。この組織 VDC 内の仮想マシンのみがこのネットワークに接続できます。</p> <p>このネットワークは、外部ネットワークに対する制限されたアクセスも提供します。システム管理者または組織管理者は、外部ネットワークから特定の仮想マシンにアクセスできるようにネットワーク アドレス変換 (NAT)、ファイアウォール、および VPN を設定できます。</p> <p>IPv4 または IPv6 を選択します。</p>

表 4-1. 組織 VDC ネットワークのタイプ（続き）

データセンター タイプのネットワーク	説明
インポート済み	このネットワークは、既存の NSX-T 論理スイッチを使用します。ネットワークをインポートできるのは、システム管理者のみです。
クロス仮想データセンター	<p>このネットワークは、データセンター グループにまたがる拡張ネットワークの一部です。単一またはマルチサイトの vCloud Director 展開では、データセンター グループに 2 ～ 4 つの組織仮想データセンターを含めることができます。</p> <p>このネットワークに接続された仮想マシンは、基盤となる拡張ネットワークに接続されます。</p> <p>クロス VDC ネットワークには NSX Data Center for vSphere が必要です。</p> <p>IPv4 のみを選択できます。</p> <p>クロス VDC ネットワークの詳細については、5 章 クロス仮想データセンター ネットワークの管理を参照してください。</p>

組織 VDC ネットワークを管理する手順はすべて、環境内に複数の仮想データセンターがあるという前提で記載されています。

この章には、次のトピックが含まれています。

- [使用可能な組織 VDC ネットワークの表示](#)
- [隔離された組織仮想データセンター ネットワークの追加](#)
- [経路指定された組織仮想データセンター ネットワークの追加](#)
- [直接の組織仮想データセンター ネットワークの追加](#)
- [インポートされた NSX-T 論理スイッチを使用した組織 VDC ネットワークの追加](#)
- [組織仮想データセンター ネットワークの全般設定の編集](#)
- [組織仮想データセンター ネットワークの変換](#)
- [経路指定された組織仮想データセンター ネットワークのインターフェイスの変換](#)
- [組織仮想データセンター ネットワークに使用されている IP アドレスの表示](#)
- [組織仮想データセンター ネットワーク IP プールへの IP アドレスの追加](#)
- [組織仮想データセンター ネットワークで使用される IP アドレス範囲の編集または削除](#)
- [組織仮想データセンター ネットワークの DNS 設定の編集](#)
- [隔離された組織仮想データセンター ネットワークの DHCP の設定](#)
- [ネットワークの既存の DHCP プールの編集または削除](#)
- [組織仮想データセンター ネットワークのリセット](#)
- [組織仮想データセンター ネットワークの削除](#)

使用可能な組織 VDC ネットワークの表示

使用可能な組織仮想データセンター ネットワークを表示できます。

前提条件

この操作には、事前定義された組織管理者またはシステム管理者ロール、またはそれに相当する権限を含むロールが必要です。

手順

- ◆ [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [ネットワーク] を選択します。

結果

使用可能なネットワークのリストが表示され、名前ですべ替えることができます。

次のステップ

新しいネットワークを追加できます。また、既存のネットワークを編集、削除、またはリセットすることもできます。

隔離された組織仮想データセンター ネットワークの追加

この組織のみがアクセスできる、隔離された組織 VDC ネットワークを追加することができます。このネットワークは、この組織の外部にある仮想マシンへの接続は提供しません。この組織外の仮想マシンは、組織内の仮想マシンに接続できません。

組織 VDC ネットワークは、組織のニーズに応じて、隔離されたものと経路指定されたものを混在させることができます。たとえば、機密情報が含まれているネットワークを隔離し、それとは別に Edge ゲートウェイに関連付けてインターネットに接続したネットワークを使用することができます。

ネットワーク プールによってバックアップされている隔離された VDC ネットワークを作成できます。サービス プロバイダは、NSX-T 論理スイッチによってバックアップされている隔離された VDC ネットワークを作成することもできます。

IPv4 の隔離された組織 VDC ネットワークのみを作成できます。

前提条件

この操作には、事前定義の組織管理者ロールに含まれている権限、またはそれに相当する権限が必要です。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [ネットワーク] を選択します。
- 2 [追加] をクリックします。
- 3 [ネットワーク タイプの選択] 画面で、[隔離] を選択し、[次へ] をクリックします。
- 4 組織 VDC ネットワークのわかりやすい名前を入力します。
- 5 隔離ネットワークの Classless Inter-Domain Routing (CIDR) 設定を入力します。

`network_gateway_IP_address/subnet_prefix_length` (例: **192.167.1.1/24**) の形式を使用します。

6 (オプション) 組織 VDC ネットワークの説明を入力します。

7 (オプション) 組織 VDC ネットワークを同じ組織内の他の組織 VDC で使用できるようにするには、[共有済み] オプションに切り替えます。

このオプションを使用するのは、たとえば、アプリケーションがある組織 VDC で予約プールや割り当てプールが割り当てモデルとして設定されている場合です。この場合、十分な領域がないために、実行する仮想マシンをこれ以上増やせなくなることがあります。これを解決する策として、従量課金制のセカンダリ組織 VDC を作成し、そのネットワーク上で一時的に追加の仮想マシンを実行できます。

注： 組織 VDC は、同一のプロバイダ仮想データセンターによってバックアップされている必要があります。

8 [次へ] をクリックします。

9 (オプション) 固定 IP アドレスが必要な仮想マシンへの割り当て用に 1 つ以上の IP アドレスを予約するには、このネットワークの [固定 IP プール] を設定します。

a IP アドレスまたは IP アドレスの範囲を入力して [追加] をクリックします。

b 複数の固定 IP アドレスまたはアドレス範囲を追加するには、この手順を繰り返します。

c (オプション) IP アドレスおよび IP アドレス範囲を変更または削除するには、[変更] または [削除] をクリックします。

10 [次へ] をクリックします。

11 (オプション) DNS を設定します。

オプション	アクション
プライマリ DNS	プライマリ DNS サーバの IP アドレスを入力します。
セカンダリ DNS	セカンダリ DNS サーバの IP アドレスを入力します。
DNS サフィックス	DNS サフィックスを入力します。DNS サフィックスは、ホスト名を含めない DNS 名です。

12 [次へ] をクリックします。

13 [設定内容の確認] 画面で、指定した組織 VDC ネットワーク設定を確認し、[完了] をクリックします。

経路指定された組織仮想データセンター ネットワークの追加

外部ネットワークへのアクセスを制御するには、経路指定された組織 VDC ネットワークを追加できます。システム管理者および組織管理者は、外部ネットワークから特定の仮想マシンにアクセスできるようにネットワーク アドレス変換 (NAT)、ファイアウォール、および VPN を設定できます。

組織 VDC ネットワークは、組織のニーズに応じて、隔離されたものと経路指定されたものを混在させることができます。たとえば、Edge ゲートウェイに関連付けてインターネットに接続したネットワークを追加しつつ、機密情報が含まれているネットワークを隔離することができます。

IPv4 または IPv6 の経路指定された組織 VDC ネットワークを追加できます。

前提条件

この操作には、事前定義の組織管理者ロールに含まれている権限、またはそれに相当する権限が必要です。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [ネットワーク] を選択します。
- 2 [追加] をクリックします。
- 3 [ネットワーク タイプの選択] 画面で、[経路指定] を選択し、[次へ] をクリックします。
- 4 組織 VDC ネットワークのわかりやすい名前を入力します。
- 5 経路指定された組織 VDC ネットワークの Classless Inter-Domain Routing (CIDR) 設定を入力します。
network_gateway_ip_address/subnet_prefix_length (例: **192.167.1.1/24**) の形式を使用します。

- 6 (オプション) 組織 VDC ネットワークの説明を入力します。
- 7 (オプション) 組織 VDC ネットワークを同じ組織内の他の組織 VDC で使用できるようにするには、[共有済み] オプションに切り替えます。

このオプションを使用するのは、たとえば、組織 VDC 内のアプリケーションで予約プールや割り当てプールが割り当てモデルとして設定されている場合です。この場合、十分な領域がないために、実行する仮想マシンをこれ以上増やせなくなることがあります。これを解決する策として、従量課金制のセカンダリ組織 VDC を作成し、そのネットワーク上で一時的に追加の仮想マシンを実行できます。

注： 複数の組織 VDC で同じネットワーク プールを共有する必要があります。

- 8 [次へ] をクリックします。
- 9 [Edge 接続] 画面で、組織 VDC ネットワークと関連付ける Edge ゲートウェイを選択します。

組織 VDC に複数の Edge ゲートウェイが含まれる場合は、このネットワークが接続する Edge ゲートウェイを選択する必要があります。[使用可能なネットワークの数] 列に 1 以上の値が表示されていれば、Edge ゲートウェイは追加の経路指定されたネットワークをサポートできます。

- 10 [インターフェイス タイプ] ドロップダウン メニューから、インターフェイス タイプを選択します。

オプション	説明
内部	Edge ゲートウェイの内部インターフェイスのいずれかに接続します。 許可されるネットワークの最大数は 9 です。
分散	この Edge ゲートウェイに接続されている分散論理ルーター上にネットワークを作成します。 許可されるネットワークの最大数は 400 です。
サブインターフェイス	組織 VDC ネットワークを拡張します。vCloud Director は、L2 VPN による拡張に使用するネットワークを識別します。 vCloud Director は、NSX ネットワーク仮想化を利用して、このネットワークのトランク インターフェイス タイプを作成します。許可されるネットワークの最大数は 200 です。

- 11 (オプション) このネットワークでゲスト VLAN のタグ付けを有効にするには、[ゲスト VLAN の許可] オプションに切り替えます。
- 12 [次へ] をクリックします。

- 13 (オプション) 固定 IP アドレスが必要な仮想マシンへの割り当て用に 1 つ以上の IP アドレスを予約するには、このネットワークの [固定 IP プール] を設定します。
 - a IP アドレスまたは IP アドレスの範囲を入力して [追加] をクリックします。
 - b 複数の固定 IP アドレスまたはアドレス範囲を追加するには、この手順を繰り返します。
 - c (オプション) IP アドレスおよび IP アドレス範囲を変更または削除するには、[変更] または [削除] をクリックします。
- 14 [次へ] をクリックします。
- 15 (オプション) DNS を設定します。

オプション	アクション
プライマリ DNS	プライマリ DNS サーバの IP アドレスを入力します。
セカンダリ DNS	セカンダリ DNS サーバの IP アドレスを入力します。
DNS サフィックス	DNS サフィックスを入力します。DNS サフィックスは、ホスト名を含めない DNS 名です。

- 16 [次へ] をクリックします。
- 17 [設定内容の確認] 画面で、指定した組織 VDC ネットワーク設定を確認し、[完了] をクリックします。

直接の組織仮想データセンター ネットワークの追加

直接的なルートを使用して外部ネットワークに接続するには、システム管理者が直接接続を設定できます。

組織管理者として vCloud Director テナント ポータルにログインして、直接の組織仮想データセンター ネットワークを作成すると、適切な権限がないことを示す警告メッセージが表示されます。

前提条件

この操作は、システム管理者に制限されます。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [ネットワーク] を選択します。
- 2 [追加] をクリックします。
- 3 [ネットワーク タイプの選択] 画面で、[直接] を選択し、[次へ] をクリックします。
- 4 組織 VDC ネットワークのわかりやすい名前を入力します。
- 5 (オプション) 組織 VDC ネットワークの説明を入力します。
- 6 (オプション) 組織 VDC ネットワークを同じ組織内の他の組織 VDC で使用できるようにするには、[共有済み] オプションに切り替えます。
- 7 [外部ネットワーク接続] 画面で、新しい組織仮想データセンター ネットワークを直接接続する外部ネットワークを選択し、[次へ] をクリックします。
- 8 [設定内容の確認] 画面で、指定した組織 VDC ネットワーク設定を確認し、[完了] をクリックします。

インポートされた NSX-T 論理スイッチを使用した組織 VDC ネットワークの追加

システム管理者は、関連付けられた NSX-T Manager インスタンスから論理スイッチをインポートすることで、組織 VDC ネットワークを作成できます。

注： NSX-T 論理スイッチでは、IPv4 の隔離された組織ネットワークのみを作成することができます。NSX-T 論理スイッチに基づいた直接の組織ネットワークを作成することはできません。

前提条件

- この操作は、システム管理者に制限されます。
- ターゲット組織仮想データセンターをバックアップするプロバイダ仮想データセンターは、NSX-T Manager インスタンスに関連付けられている必要があります。
- システム管理者が、他の組織仮想データセンター ネットワークで使用されていない NSX-T 論理スイッチを 1 台以上作成している必要があります。

NSX-T 論理スイッチの作成および構成については、NSX-T 管理ガイドを参照してください。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [ネットワーク] を選択します。
- 2 [追加] をクリックします。
- 3 [ネットワーク タイプの選択] 画面で、[インポート] を選択し、[次へ] をクリックします。
- 4 新しい組織仮想データセンター ネットワークの名前と、オプションで説明を入力し、[次へ] をクリックします。
- 5 利用可能な NSX-T 論理スイッチのリストから、スイッチ名の横にあるラジオ ボタンをクリックしてターゲットスイッチを選択し、[次へ] をクリックします。
- 6 ネットワークの Classless Inter-Domain Routing (CIDR) 設定を入力します。
network_gateway_ip_address/subnet_prefix_length (例 : **192.167.1.1/24**) の形式を使用します。
スイッチがサブネット構成されている場合、この情報は自動入力されます。
- 7 (オプション) DNS 設定と固定 IP アドレス プールを指定します。
複数の IP アドレスおよび IP アドレス範囲を追加することができます。
- 8 [次へ] をクリックします。
- 9 [設定内容の確認] 画面の内容を確認し、[完了] をクリックします。

組織仮想データセンター ネットワークの全般設定の編集

組織 VDC ネットワークのプロパティを変更できます。

前提条件

これらの操作には、事前定義された組織管理者またはシステム管理者ロール、またはそれに相当する権限セットを含むロールが必要です。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [ネットワーク] を選択します。
- 2 表示または編集する組織 VDC ネットワークの名前をクリックします。
- 3 [全般] タブで、[編集] をクリックします。
 - a ネットワークの名前と説明を編集します。
 - b [共有済み] オプションを有効または無効に切り替えて、組織 VDC ネットワークを同じ組織内の他の仮想データセンターと共有するかどうかを指定します。
- 4 [保存] をクリックします。

組織仮想データセンター ネットワークの変換

組織 VDC ネットワークを作成すると、このネットワークを隔離から経路指定に、またはその逆に変換できます。

前提条件

これらの操作には、事前定義された組織管理者またはシステム管理者ロール、またはそれに相当する権限セットを含むロールが必要です。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [ネットワーク] を選択します。
- 2 変換する組織 VDC ネットワークの名前をクリックします。
- 3 [全般] タブで、[編集] をクリックします。
- 4 [接続] をクリックします。
- 5 Edge ゲートウェイに接続するか、またはこのネットワークを他のすべてのネットワークから隔離するには、[Edge ゲートウェイに接続] オプションを有効に切り替えるか、同じオプションを無効に切り替えます。

オプション	アクション
隔離されたネットワークを経路指定ネットワークに変換する。	<ol style="list-style-type: none"> 1 [Edge ゲートウェイに接続] オプションを有効にします。 2 使用可能な Edge ゲートウェイのリストから、接続する Edge ゲートウェイを選択します。 3 インターフェイス タイプを選択します。 4 ゲスト VLAN を許可するには、[ゲスト VLAN の許可] オプションを有効にします。
経路指定ネットワークを隔離されたネットワークに変換する。	[Edge ゲートウェイに接続] オプションを無効にします。

- 6 [保存] をクリックします。

結果

組織 VDC ネットワークが変換されました。

経路指定された組織仮想データセンター ネットワークのインターフェイスの変換

ネットワークのインターフェイスは、ネットワーク プロパティの編集などの方法で、内部インターフェイスからサブインターフェイスまたは分散ルーティングに変更できます。

注： クロス仮想データセンター ネットワークは変換できません。

前提条件

この操作には、事前定義の組織管理者ロールに含まれている権限、またはそれに相当する権限が必要です。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [ネットワーク] を選択します。
- 2 変換するネットワークの名前をクリックします。
- 3 編集する組織 VDC ネットワークの名前をクリックします。
- 4 [全般] タブで、[編集] をクリックします。
- 5 [接続] をクリックします。
- 6 [インターフェイス タイプ] ドロップダウン メニューから、インターフェイス タイプを選択します。

オプション	説明
内部	Edge ゲートウェイの内部インターフェイスのいずれかに接続します。 許可されるネットワークの最大数は 9 です。
分散	この Edge ゲートウェイに接続されている分散論理ルーター上にネットワークを作成します。 許可されるネットワークの最大数は 400 です。
サブインターフェイス	組織 VDC ネットワークを拡張します。vCloud Director は、L2 VPN による拡張に使用するネットワークを識別します。 vCloud Director は、NSX ネットワーク仮想化を利用して、このネットワークのトランク インターフェイス タイプを作成します。許可されるネットワークの最大数は 200 です。

- 7 [保存] をクリックします。

組織仮想データセンター ネットワークに使用されている IP アドレスの表示

現在使用中の組織仮想データセンター ネットワーク IP プールから、IP アドレスの一覧を表示できます。

前提条件

- これらの操作には、事前定義された組織管理者またはシステム管理者ロール、またはそれに相当する権限セットを含むロールが必要です。
- ネットワークが隔離されている、または経路指定された組織仮想データセンター ネットワークであることを確認します。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [ネットワーク] を選択します。
- 2 使用中の IP アドレスを確認するネットワーク名をクリックします。
- 3 [IP アドレス管理] タブをクリックします。
- 4 [IP の割り当て] をクリックして、現在使用中の IP アドレスを確認します。

組織仮想データセンター ネットワーク IP プールへの IP アドレスの追加

組織仮想データセンター ネットワークの IP アドレスが足りない場合は、IP プールにアドレスを追加できます。

直接接続する外部組織仮想データセンター ネットワークに IP アドレスを追加することはできません。

前提条件

- これらの操作には、事前定義された組織管理者またはシステム管理者ロール、またはそれに相当する権限セットを含むロールが必要です。
- ネットワークが隔離されている、または経路指定された組織仮想データセンター ネットワークであることを確認します。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [ネットワーク] を選択します。
- 2 編集するネットワークの名前をクリックします。
- 3 [IP アドレス管理] タブをクリックします。
[固定 IP プール] オプションがデフォルトで選択されています。
- 4 右側の [編集] ボタンをクリックします。
[ネットワークの編集] ウィンドウに、ゲートウェイ CIDR と IP アドレスの範囲がある場合は、それらが表示されます。

- 5 [固定 IP プール] テキスト ボックスに IP アドレスまたは IP アドレスの範囲を入力して、[追加] をクリックします。

注： クロス仮想データセンター ネットワークの場合、IP アドレスは、同一の拡張ネットワークから他の組織仮想データセンター ネットワークに割り当てられている IP アドレスと重複しないようにする必要があります。

- 6 [保存] をクリックします。

結果

IP アドレスまたは IP アドレス範囲がネットワーク IP プールに追加されます。

組織仮想データセンター ネットワークで使用される IP アドレス範囲の編集または削除

組織仮想データセンター ネットワークに、不要になった IP アドレスが含まれている場合は、アドレスを編集したり、IP アドレス プールからアドレスを削除することができます。

前提条件

- これらの操作には、事前定義された組織管理者またはシステム管理者ロール、またはそれに相当する権限セットを含むロールが必要です。
- ネットワークが隔離されている、または経路指定された組織仮想データセンター ネットワークであることを確認します。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [ネットワーク] を選択します。
- 2 編集するネットワークの名前をクリックします。
- 3 [IP アドレス管理] タブをクリックします。
[固定 IP プール] オプションがデフォルトで選択されています。
- 4 右側の [編集] ボタンをクリックします。
 - IP アドレス範囲を変更するには、範囲を選択して必要な編集を行い、[変更] をクリックします。
 - IP アドレス範囲を削除するには、範囲を選択して [削除] をクリックします。
- 5 [保存] をクリックします。

組織仮想データセンター ネットワークの DNS 設定の編集

組織仮想データセンター ネットワークの DNS 設定を編集できます。

前提条件

- これらの操作には、事前定義された組織管理者またはシステム管理者ロール、またはそれに相当する権限セットを含むロールが必要です。

- ネットワークが隔離されている、または経路指定された組織仮想データセンター ネットワークであることを確認します。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [ネットワーク] を選択します。
- 2 編集するネットワークの名前をクリックします。
- 3 [IP アドレス管理] タブをクリックします。
- 4 [DNS] を選択し、右側の [編集] ボタンをクリックします。
- 5 必要に応じて、プライマリ DNS、セカンダリ DNS、および DNS サフィックス情報を編集します。
- 6 [保存] をクリックします。

隔離された組織仮想データセンター ネットワークの DHCP の設定

隔離された組織 VDC ネットワークの DHCP 設定を編集できます。組織 VDC ネットワークの DHCP サービスは、DHCP からアドレスを要求するように設定されている仮想マシン NIC に、アドレス プールから IP アドレスを提供します。サービスは、仮想マシンがパワーオンされるとアドレスを提供します。

前提条件

- これらの操作には、事前定義された組織管理者またはシステム管理者ロール、またはそれに相当する権限セットを含むロールが必要です。
- ネットワークが隔離された組織仮想データセンター ネットワークであることを確認します。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [ネットワーク] を選択します。
- 2 編集するネットワークの名前をクリックします。
- 3 [IP アドレス管理] タブをクリックします。
- 4 [DHCP] を選択します。
DHCP 設定が右側に表示されます。
- 5 DHCP を有効にするには、[DHCP プール サービス] の右側にある [編集] をクリックします。
- 6 [DHCP プール サービス] を有効にして、[保存] をクリックします。
DHCP クライアントによって要求されたアドレスは、DHCP プールから取得されます。

7 ネットワークの DHCP プールを作成します。

a [追加] をクリックします。

b プールの IP アドレス範囲を入力します。

指定する IP アドレス範囲は、組織仮想データセンターの固定 IP アドレス プールと重複することはできません。

c DHCP アドレスのデフォルトのリース時間を秒単位で指定します。

デフォルト値は 3,600 秒です。

d DHCP アドレスの最大リース時間を秒単位で指定します。

これは、DHCP によって割り当てられた IP アドレスが仮想マシンにリースされる最大時間です。デフォルト値は 7,200 秒です。

8 [保存] をクリックします。

ネットワークの既存の DHCP プールの編集または削除

隔離された組織仮想データセンター ネットワーク内の DHCP プールが不要になった場合は、そのプールを削除するか、または編集することができます。

前提条件

- これらの操作には、事前定義された組織管理者またはシステム管理者ロール、またはそれに相当する権限セットを含むロールが必要です。
- ネットワークが隔離された組織仮想データセンター ネットワークであることを確認します。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [ネットワーク] を選択します。
- 2 編集するネットワークの名前をクリックします。
- 3 [IP アドレス管理] タブをクリックします。
- 4 [DHCP] を選択します。
DHCP 設定が右側に表示されます。

5 既存の DHCP プールを編集または削除します。

オプション	アクション
DHCP プールを編集する。	<ol style="list-style-type: none"> 1 編集する DHCP プールを選択します。 2 [編集] ボタンをクリックします。 3 プールの IP アドレス範囲を更新します。 4 DHCP アドレスのデフォルトのリース時間を秒単位で編集します。 5 DHCP アドレスの最大リース時間を秒単位で編集します。 6 [保存] をクリックします。
DHCP プールを削除する。	<ol style="list-style-type: none"> 1 削除する DHCP プールを選択します。 2 [削除] ボタンをクリックします。

組織仮想データセンター ネットワークのリセット

組織仮想データセンター ネットワークと関連付けられている、DHCP 設定やファイアウォール設定などのネットワーク サービスが期待どおりに機能しない場合は、ネットワークをリセットすることができます。

組織仮想データセンター ネットワークをリセットすると、ネットワークの DHCP サービス ゲートウェイが強制的に再デプロイされます。この操作により、DHCP サービスが一時的に中断され、ネットワークのリセット中はネットワーク サービスを使用することができません。

前提条件

- この操作には、事前定義の組織管理者ロールに含まれている権限、またはそれに相当する権限が必要です。
- ネットワークが、どの仮想マシン、vApp、またはその他のネットワークにも接続されていないこと。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [ネットワーク] を選択します。
- 2 組織 VDC ネットワークを選択します。
- 3 [リセット] をクリックして、リセット操作を確定します。

組織仮想データセンター ネットワークの削除

組織仮想データセンター ネットワークが不要になった場合は、このネットワークを削除できます。

前提条件

- この操作には、事前定義の組織管理者ロールに含まれている権限、またはそれに相当する権限が必要です。
- 仮想マシン、vApp、またはその他のネットワークに、ネットワークが接続されていないこと。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [ネットワーク] を選択します。

- 2 対象のネットワーク名の横にあるラジオ ボタンをクリックし、[削除] をクリックします。
- 3 確認するには、[OK] をクリックします。

クロス仮想データセンター ネットワークの管理

5

複数の組織仮想データセンター間でネットワークを構築するには、最初に仮想データセンターをグループ化してから、データセンター グループに拡張ネットワークを作成します。データセンター グループには、共通の出力方向ポイント構成または各ネットワーク フォルト ドメインの出力ポイント構成のいずれかを構成できます。

クロス仮想データセンター ネットワークには NSX Data Center for vSphere が必要です。

データセンター グループ

複数の出力方向ポイントを共有するように設定された、最大 4 つの仮想データセンターで構成されるグループです。データセンター グループには、次の出力方向ポイントのいずれかを設定できます。

出力方向ポイントの設定のタイプ	説明
共通の出力方向ポイントの設定	データセンター グループには、1 つのアクティブな出力方向ポイントと 1 つのスタンバイ出力方向ポイントを設定できます。この 2 つの出力方向ポイントは、データセンター グループ内のすべてのネットワーク フォルト ドメインにまたがる、参加しているすべての仮想データセンターに共通です。
フォルト ドメインあたりの出力方向ポイントの設定	データセンター グループには、データセンター グループ内のネットワーク フォルト ドメインごとに、1 つのアクティブな出力方向ポイントを設定できます。スタンバイ出力方向ポイントは作成できません。

組織には、複数のデータセンター グループを設定できます。組織仮想データセンターは、複数のデータセンターグループに参加できます。

参加している組織仮想データセンターは、異なる vCloud Director サイトに属することができます。[マルチサイト展開の設定と管理](#)を参照してください。

ネットワーク フォルト ドメイン

ネットワーク プロバイダの範囲。通常は、NSX Manager に関連付けられた、基盤となる vCenter Server インスタンスを指定します。

出力方向ポイント

データセンター グループまたはネットワーク フォルト ドメインをインターネットに接続する Edge Gateway。Edge Gateway は、データセンター グループ内の仮想データセンターに属している必要があります。仮想データセンター グループまたはネットワーク フォルト ドメインの出力方向ポイントおよびユニバーサル分散ルーターを指定する Edge Gateway に BGP ルートが設定されます。Edge Gateway 上の既存のルートには影響しません。

拡張ネットワーク

データセンター グループ内のすべての仮想データセンターをまたがるレイヤー 2 拡張ネットワークです。IPv4 のみを選択できます。

この章には、次のトピックが含まれています。

- [データセンター グループの管理](#)
- [拡張ネットワークの管理](#)

データセンター グループの管理

データセンター グループを作成すると、データセンター グループのネットワーク トポロジを編集できます。グループに仮想データセンターを追加または削除できます。出力方向ポイントはスワップ、置き換え、および削除することができます。さまざまな同期タスクを実行して、設定エラーを修正できます。

フォルト ドメインごとに共通の出力方向の設定を出力方向の設定に変換したり、逆方向の変換を行うことはできません。

共通の出力方向が設定されたデータセンター グループの作成と設定

共通の出力方向が設定された仮想データセンター グループを作成および設定し、Edge Gateway のペアが参加しているすべての仮想データセンターのアクティブおよびスタンバイ出力方向ポイントとして機能するように設定できます。

前提条件

- この操作を行うには、システム管理者ロール、または VDC グループ：VDC グループの設定権限を持つロールが組織に公開されている必要があります。
- システム管理者が、ターゲット仮想データセンターでクロス仮想データセンター ネットワークを有効にしていること。

手順

1 共通の出力方向が設定されたデータセンター グループの作成

2 ～ 4 つの仮想データセンターを、共通の出力方向が設定されたデータセンター グループにグループ化できます。

2 アクティブ出力方向ポイントの追加

データセンター グループをインターネットに接続するには、ネットワーク トポロジにアクティブ出力方向ポイントを追加する必要があります。

3 スタンバイ出力方向ポイントの追加

共通の出力方向が設定された仮想データセンター グループでは、フォルト トレランスの場合にスタンバイ出力方向ポイントとして機能するセカンダリ出力方向ポイントを追加できます。

共通の出力方向が設定されたデータセンター グループの作成

2 ～ 4 つの仮想データセンターを、共通の出力方向が設定されたデータセンター グループにグループ化できます。

手順

- 1 メイン メニュー (≡) で [データセンター グループ] を選択します。
データセンター グループのリストがカード ビューに表示されます。
- 2 [新しいデータセンター グループ] をクリックします。
- 3 新しいデータセンター グループの名前と、オプションで説明を入力します。
- 4 [共通の出力方向ポイント] を選択し、[次へ] をクリックします。
- 5 [データセンター] ページで新しいデータセンター グループのデータセンターを 2 つ以上、最大 4 つまで選択し、[次へ] をクリックします。
[データセンター] 画面には、システム管理者がクロス仮想データセンター ネットワークを有効にした仮想データセンターのリストが含まれています。
- 6 データセンター グループの詳細を確認し、[完了] をクリックします。

結果

新しく作成された仮想データセンター グループは、[データセンター グループ] ビューに表示されます。

アクティブ出力方向ポイントの追加

データセンター グループをインターネットに接続するには、ネットワーク トポロジにアクティブ出力方向ポイントを追加する必要があります。

前提条件

システム管理者が、データセンター グループに参加している仮想データセンターのいずれかに 1 つ以上の Edge Gateway を作成しています。

手順

- 1 メイン メニュー (≡) で [データセンター グループ] を選択します。
データセンター グループのリストがカード ビューに表示されます。
- 2 ターゲット データセンター グループのカードで、[詳細] をクリックします。
このデータセンター グループの [ネットワーク トポロジ] ビューにリダイレクトされます。現在のネットワーク トポロジが表示され、ネットワーク フォルト ドメイン、出力方向ポイント (設定されている場合)、およびトラフィック ルートと共に、参加中の仮想データセンターを確認できます。

- 3 [出力方向ポイントの追加] をクリックします。

[アクティブ出力方向ポイントの追加] ページが開き、参加している仮想データセンターに属する Edge Gateway のリストが表示されます。

- 4 このデータセンター グループのアクティブ出力方向ポイントとして機能させる Edge Gateway を選択し、[追加] をクリックします。

結果

BGP ルートが Edge Gateway 上に設定され、仮想データセンター グループの出力方向ポイントとユニバーサルルーターが示されます。Edge Gateway 上の既存のルートには影響しません。

ネットワーク トポロジ図が、新しく追加した出力方向ポイントで更新されます。参加している仮想データセンターからインターネットへのトラフィックは、青色の実線で表されます。

スタンバイ出力方向ポイントの追加

共通の出力方向が設定された仮想データセンター グループでは、フォルト トレランスの場合にスタンバイ出力方向ポイントとして機能するセカンダリ出力方向ポイントを追加できます。

前提条件

アクティブ出力方向ポイントとして機能している Edge Gateway とは別に、グループに参加している仮想データセンターのいずれかに 1 台以上の Edge Gateway が必要です。

手順

- 1 メイン メニュー (≡) で [データセンター グループ] を選択します。

データセンター グループのリストがカード ビューに表示されます。

- 2 ターゲット データセンター グループのカードで、[詳細] をクリックします。

このデータセンター グループの [ネットワーク トポロジ] ビューにリダイレクトされます。現在のネットワーク トポロジが表示され、ネットワーク フォルト ドメイン、出力方向ポイント（設定されている場合）、およびトラフィック ルートと共に、参加中の仮想データセンターを確認できます。

- 3 [スタンバイ出力方向ポイントの追加] をクリックします。

[スタンバイ出力方向ポイントの追加] ページが開き、参加中の仮想データセンターに属する未使用の Edge Gateway のリストが表示されます。この仮想データセンター グループのアクティブ出力方向ポイントで使用されている Edge Gateway は表示されません。

- 4 このデータセンター グループのスタンバイ出力方向ポイントとして機能させる Edge Gateway を選択し、[追加] をクリックします。

結果

BGP ルートが Edge Gateway 上に設定され、仮想データセンター グループの出力方向ポイントとユニバーサルルーターが示されます。Edge Gateway 上の既存のルートには影響しません。

ネットワーク トポロジ図が、新しく追加した出力方向ポイントで更新されます。フォルト トレランス発生時の、参加中の仮想データセンターからインターネットへのトラフィックは、青色の点線で表されます。

フォルト ドメインの出力方向が設定されたデータセンター グループの作成と設定

フォルト ドメインの出力方向が設定された仮想データセンター グループを作成および設定し、Edge Gateway がグループ内の各ネットワーク フォルト ドメインでアクティブ出力方向ポイントとして機能するように設定できます。フォルト ドメインの出力方向が設定されたデータセンター グループには、スタンバイ出力方向を作成することはできません。

前提条件

この操作を行うには、システム管理者ロール、または VDC グループ : VDC グループの設定権限を持つロールが組織に公開されている必要があります。

手順

1 フォルト ドメインの出力方向設定を使用したデータセンター グループの作成

2 ～ 4 つの仮想データセンターを、フォルト ドメインの出力方向設定を使用してデータセンター グループにグループ化できます。

2 フォルト ドメインへの出力方向ポイントの追加

仮想データセンターを、データセンター グループ内のネットワーク フォルト ドメインからインターネットに接続するには、ネットワーク フォルト ドメインに出力方向ポイントを追加する必要があります。出力方向ポイントは、データセンター グループ内の各ネットワーク フォルト ドメインに追加することができます。フォルト ドメインの出力方向が設定されたデータセンター グループでは、スタンバイ出力方向ポイントはサポートされません。


フォルト ドメインの出力方向設定を使用したデータセンター グループの作成

2 ～ 4 つの仮想データセンターを、フォルト ドメインの出力方向設定を使用してデータセンター グループにグループ化できます。

前提条件

システム管理者が、ターゲット仮想データセンターでクロス仮想データセンター ネットワークを有効にしていること。

手順

- 1 メイン メニュー () で [データセンター グループ] を選択します。
データセンター グループのリストがカード ビューに表示されます。
- 2 [新しいデータセンター グループ] をクリックします。
- 3 新しいデータセンター グループの名前と、オプションで説明を入力します。
- 4 [フォルト ドメインあたりの出力方向ポイント] を選択し、[次へ] をクリックします。

- 5 [データセンター] ページで新しいデータセンター グループのデータセンターを 2 つ以上、最大 4 つまで選択し、[次へ] をクリックします。

[データセンター] 画面には、システム管理者がクロス仮想データセンター ネットワークを有効にした仮想データセンターのリストが含まれています。

- 6 データセンター グループの詳細を確認し、[完了] をクリックします。

結果

新しく作成された仮想データセンター グループは、[データセンター グループ] ビューに表示されます。

フォルト ドメインへの出力方向ポイントの追加

仮想データセンターを、データセンター グループ内のネットワーク フォルト ドメインからインターネットに接続するには、ネットワーク フォルト ドメインに出力方向ポイントを追加する必要があります。出力方向ポイントは、データセンター グループ内の各ネットワーク フォルト ドメインに追加することができます。フォルト ドメインの出力方向が設定されたデータセンター グループでは、スタンバイ出力方向ポイントはサポートされません。

前提条件

このデータセンター グループ内で出力方向ポイントとして使用されている Edge Gateway とは別に、参加している仮想データセンターのいずれかに 1 つ以上の未使用の Edge Gateway が必要です。

手順

- 1 メイン メニュー (≡) で [データセンター グループ] を選択します。
データセンター グループのリストがカード ビューに表示されます。
- 2 ターゲット データセンター グループのカードで、[詳細] をクリックします。
このデータセンター グループの [ネットワーク トポロジ] ビューにリダイレクトされます。現在のネットワーク トポロジが表示され、ネットワーク フォルト ドメイン、出力方向ポイント (設定されている場合)、およびトラフィック ルートと共に、参加中の仮想データセンターを確認できます。
- 3 ネットワーク トポロジ図で、ターゲットのネットワーク フォルト ドメインをクリックします。
ネットワーク フォルト ドメインは実線で表され、図の下部に名前が表示されます。
選択したフォルト ドメインは、青色でマークされます。
- 4 [出力方向ポイントの追加] をクリックします。
[アクティブ出力方向ポイントの追加] 画面が開き、参加している仮想データセンターに属する Edge Gateway のリストが表示されます。
- 5 このフォルト ドメインの出力方向ポイントとして機能させる Edge Gateway を選択し、[追加] をクリックします。

結果

BGP ルートが Edge Gateway 上に設定され、ネットワーク フォルト ドメインの出力方向ポイントとユニバーサル ルーターが示されます。Edge Gateway 上の既存のルートには影響しません。

ネットワーク トポロジ図が、新しく追加した出力方向ポイントで更新されます。ネットワーク フォルト ドメイン内の仮想データセンターからインターネットへのトラフィックは、青色の実線で表されます。

データセンター グループの表示

組織内のデータセンター グループと、現在の構成に関する詳細を表示できます。

前提条件

この操作を行うには、システム管理者ロール、または VDC グループ : VDC グループの表示権限を持つロールが組織に公開されている必要があります。

手順

- 1 メイン メニュー (≡) で [データセンター グループ] を選択します。

データセンター グループのリストがカード ビューに表示されます。

- 2 ターゲット データセンター グループのカードで、[詳細] をクリックします。

このデータセンター グループの [ネットワーク トポロジ] ビューにリダイレクトされます。現在のネットワーク トポロジが表示され、ネットワーク フォルト ドメイン、出力方向ポイント (設定されている場合)、およびトラフィック ルートと共に、参加中の仮想データセンターを確認できます。

仮想データセンターのデータセンター グループへの追加

仮想データセンターをデータセンター グループに追加することで、既存のネットワークを新しい仮想データセンターに拡張することができます。

前提条件

- この操作を行うには、システム管理者ロール、または VDC グループ : VDC グループの設定権限を持つロールが組織に公開されている必要があります。
- データセンター グループに含まれている仮想データセンターが 4 つ未満であること。

手順

- 1 メイン メニュー (≡) で [データセンター グループ] を選択します。

データセンター グループのリストがカード ビューに表示されます。

- 2 ターゲット データセンター グループのカードで、[詳細] をクリックします。

このデータセンター グループの [ネットワーク トポロジ] ビューにリダイレクトされます。現在のネットワーク トポロジが表示され、ネットワーク フォルト ドメイン、出力方向ポイント (設定されている場合)、およびトラフィック ルートと共に、参加中の仮想データセンターを確認できます。

- 3 [データセンターの追加] をクリックします。

- 4 [データセンター] 画面で、データセンター グループに追加するデータセンターを選択し、[完了] をクリックします。

[データセンター] ページには、システム管理者によってクロス仮想データセンター ネットワーク構成が有効にされている仮想データセンターのリストが含まれています。

注： データセンター グループに含めることができる仮想データセンターは 4 つまでです。

データセンター グループからの仮想データセンターの削除

データセンター グループから仮想データセンターを削除して、この仮想データセンターから既存ネットワークを拡張しないようにすることができます。

前提条件

- この操作を行うには、システム管理者ロール、または VDC グループ：VDC グループの設定権限を持つロールが組織に公開されている必要があります。
- データセンター グループには、3 つ以上の仮想データセンターが含まれていること。
- 削除する仮想データセンターでデータセンター グループに出力方向ポイントが指定されていないこと。

手順

- 1 メイン メニュー (≡) で [データセンター グループ] を選択します。
データセンター グループのリストがカード ビューに表示されます。
- 2 ターゲット データセンター グループのカードで、[詳細] をクリックします。
このデータセンター グループの [ネットワーク トポロジ] ビューにリダイレクトされます。現在のネットワーク トポロジが表示され、ネットワーク フォルト ドメイン、出力方向ポイント（設定されている場合）、およびトラフィック ルートと共に、参加中の仮想データセンターを確認できます。
- 3 ターゲット仮想データセンターのカードの右上にある 3 つのドットをクリックし、[削除] をクリックします。
- 4 確認するには、[削除] をクリックします。

結果

データセンター グループのネットワーク トポロジ図から仮想データセンターが削除されます。

データセンター グループの同期


データセンター グループのネットワーク構成を再適用して、参加しているすべての仮想データセンターを確実にアクティブにするには、データセンター グループを同期します。

注： データセンター グループの同期中は、NSX でユニバーサル分散ルーターが同期するため、データセンター グループが数秒間使用できなくなります。

前提条件

この操作を行うには、システム管理者ロール、または VDC グループ : VDC グループの設定権限を持つロールが組織に公開されている必要があります。

手順

- 1 メイン メニュー () で [データセンター グループ] を選択します。

データセンター グループのリストがカード ビューに表示されます。

- 2 ターゲット データセンター グループのカードで、[詳細] をクリックします。

このデータセンター グループの [ネットワーク トポロジ] ビューにリダイレクトされます。現在のネットワーク トポロジが表示され、ネットワーク フォルト ドメイン、出力方向ポイント (設定されている場合)、およびトラフィック ルートと共に、参加中の仮想データセンターを確認できます。

- 3 [データセンター グループを同期] をクリックします。

- 4 確認するには、[OK] をクリックします。


データセンター グループ内の出力方向ポイントと共通の出力方向の設定のスイッチ

共通の出力方向ポイントの設定を使用してデータセンター グループ内のアクティブ出力方向ポイントとスタンバイ出力方向ポイントを設定した後に、出力方向ポイントのロールをスイッチすることができます。アクティブ出力方向ポイントをスタンバイ出力方向ポイントにしたり、スタンバイ出力方向ポイントをアクティブ出力方向ポイントにすることができます。

前提条件

この操作を行うには、システム管理者ロール、または VDC グループ : VDC グループの設定権限を持つロールが組織に公開されている必要があります。

手順

- 1 メイン メニュー () で [データセンター グループ] を選択します。

データセンター グループのリストがカード ビューに表示されます。

- 2 ターゲット データセンター グループのカードで、[詳細] をクリックします。

このデータセンター グループの [ネットワーク トポロジ] ビューにリダイレクトされます。現在のネットワーク トポロジが表示され、ネットワーク フォルト ドメイン、出力方向ポイント (設定されている場合)、およびトラフィック ルートと共に、参加中の仮想データセンターを確認できます。

- 3 [出力方向ポイントのスイッチ] をクリックします。

- 4 確認するには、[OK] をクリックします。

結果

新しいトラフィック ルートを使用してネットワーク トポロジが更新されます。これで、インターネットへのトラフィックが新しいアクティブ出力方向ポイントにリダイレクトされるようになりました。

出力方向ポイントの Edge Gateway の置き換え

データセンター グループ内のアクティブまたはスタンバイ出力方向ポイントを表す Edge Gateway を置き換えることができます。

前提条件

- この操作を行うには、システム管理者ロール、または VDC グループ : VDC グループの設定権限を持つロールが組織に公開されている必要があります。
- 新しい Edge Gateway がデータセンター グループ内の他の出力方向ポイントで使用されていないこと。

手順

- 1 メイン メニュー (≡) で [データセンター グループ] を選択します。
データセンター グループのリストがカード ビューに表示されます。
- 2 ターゲット データセンター グループのカードで、[詳細] をクリックします。
このデータセンター グループの [ネットワーク トポロジ] ビューにリダイレクトされます。現在のネットワーク トポロジが表示され、ネットワーク フォルト ドメイン、出力方向ポイント (設定されている場合)、およびトラフィック ルートと共に、参加中の仮想データセンターを確認できます。
- 3 ネットワーク フォルト ドメイン構成内の出力方向ポイントを置き換える場合は、ネットワーク トポロジ図でターゲットの出力方向ポイントのネットワーク フォルト ドメインを選択します。
ネットワーク フォルト ドメインは実線で表され、図の下部にドメイン名が表示されます。
選択したネットワーク フォルト ドメインは、青色でマークされます。
- 4 ターゲットの出力方向ポイントのカードの右上にある 3 つのドットをクリックし、[置き換え] をクリックします。
[出力方向ポイントを置き換え] 画面が開き、参加している仮想データセンターに属する Edge Gateway のリストが表示されます。
- 5 新しい Edge Gateway を選択して、[置き換え] をクリックします。

結果

古い Edge Gateway から BGP ルートが削除され、仮想データセンター グループの出力方向ポイントおよびユニバーサル分散ルーターを指定する新しい Edge Gateway に BGP ルートが設定されます。

新しい Edge Gateway の名前で、ネットワーク トポロジ図が更新されます。

出力方向ポイントの削除

データセンター グループまたはネットワーク フォルト ドメインをインターネットから切断するには、出力方向ポイントを削除します。

前提条件

- この操作を行うには、システム管理者ロール、または VDC グループ : VDC グループの設定権限を持つロールが組織に公開されている必要があります。

- スタンバイ出力方向ポイントとベアになっているアクティブ出力方向ポイントを削除する場合は、出力方向ポイントをスワップするか、スタンバイ出力方向ポイントを削除する必要があります。

手順

- 1 メイン メニュー (≡) で [データセンター グループ] を選択します。
データセンター グループのリストがカード ビューに表示されます。
- 2 ターゲット データセンター グループのカードで、[詳細] をクリックします。
このデータセンター グループの [ネットワーク トポロジ] ビューにリダイレクトされます。現在のネットワーク トポロジが表示され、ネットワーク フォルト ドメイン、出力方向ポイント（設定されている場合）、およびトラフィック ルートと共に、参加中の仮想データセンターを確認できます。
- 3 ネットワーク フォルト ドメイン構成から出力方向ポイントを削除する場合は、ネットワーク トポロジ図でターゲットの出力方向ポイントのネットワーク フォルト ドメインを選択します。
ネットワーク フォルト ドメインは実線で表され、図の下部にドメイン名が表示されます。
選択したネットワーク フォルト ドメインは、青色でマークされます。
- 4 ターゲットの出力方向ポイントのカードの右上にある 3 つのドットをクリックし、[削除] をクリックします。
- 5 確認するには、[OK] をクリックします。

結果

他のユニバーサル分散ルーターで使用されていない場合は出力方向ポイントを指定する Edge Gateway から、BGP ルートが削除されます。

ネットワークのトポロジ図から出力方向ポイントが削除されます。

ルートおよび出力方向ポイントの同期

ルートを同期すると、データセンター グループまたはネットワーク フォルト ドメイン、および関連付けられた出力方向ポイントに動的ルーティングの設定を再適用できるようになります。出力方向ポイントを同期することで、出力方向ポイントをデータセンター グループに適切に接続できます。

前提条件

- この操作を行うには、システム管理者ロール、または VDC グループ : VDC グループの設定権限を持つロールが組織に公開されている必要があります。
- ターゲット データセンター グループまたはネットワーク フォルト ドメインの出力方向ポイントが設定されていること。

手順

- 1 メイン メニュー (≡) で [データセンター グループ] を選択します。
データセンター グループのリストがカード ビューに表示されます。

- 2 ターゲット データセンター グループのカードで、[詳細] をクリックします。

このデータセンター グループの [ネットワーク トポロジ] ビューにリダイレクトされます。現在のネットワーク トポロジが表示され、ネットワーク フォルト ドメイン、出力方向ポイント（設定されている場合）、およびトラフィック ルートと共に、参加中の仮想データセンターを確認できます。

- 3 データセンター グループ内のネットワーク フォルト ドメインを同期する場合は、ネットワーク トポロジ図でターゲットのネットワーク フォルト ドメインを選択します。

ネットワーク フォルト ドメインは実線で表され、図の下部にドメイン名が表示されます。

選択したネットワーク フォルト ドメインは、青色でマークされます。

- 4 グループまたはネットワーク フォルト ドメイン、および関連付けられた出力方向ポイントに動的ルーティングの設定を再適用するには、[ルートを同期] > [OK] の順にクリックします。

- 5 出力方向ポイントをデータセンター グループと同期するには、ターゲットの出力方向ポイントのカードの右上にある 3 つのドットをクリックし、[同期] > [OK] の順にクリックします。

拡張ネットワークの管理

データセンター グループを作成して設定すると、参加している仮想データセンターにまたがるレイヤー 2 拡張ネットワークを作成して、管理できます。

仮想データセンター レベルでは、拡張ネットワークはクロス仮想データセンター ルーティング タイプの組織仮想データセンター ネットワークとして表示されます。

拡張ネットワークの追加


データセンター グループに参加しているすべての仮想データセンターにまたがる拡張ネットワークを作成できます。

IPv4 の拡張ネットワークのみを追加することができます。

前提条件

この操作を行うには、事前定義済みの組織管理者ロール、または組織 VDC ネットワーク：プロパティの編集権限を持つロールが必要です。

手順

- 1 メイン メニュー () で [データセンター グループ] を選択します。

データセンター グループのリストがカード ビューに表示されます。

- 2 ターゲット データセンター グループのカードで、[詳細] をクリックします。

このデータセンター グループの [ネットワーク トポロジ] ビューにリダイレクトされます。現在のネットワーク トポロジが表示され、ネットワーク フォルト ドメイン、出力方向ポイント（設定されている場合）、およびトラフィック ルートと共に、参加中の仮想データセンターを確認できます。

- 3 左側のパネルで、[拡張ネットワーク] をクリックします。

拡張ネットワークのリストがグリッド ビューに表示されます。

- 4 [追加] をクリックします。
- 5 新しいネットワークの名前と、オプションで説明を入力します。
- 6 ネットワークの Classless Inter-Domain Routing (CIDR) 設定を入力し、[作成] をクリックします。

`network_gateway_IP_address/subnet_prefix_length` (例: **192.167.1.1/24**) の形式を使用します。

結果

データセンター グループの拡張ネットワークのリストで、新しく作成したネットワークを確認できます。

クロス仮想データセンター ルーティング タイプの組織仮想データセンター ネットワークが、参加している各仮想データセンターに作成されます。[ネットワーク] をクリックして、参加している仮想データセンターの [データセンター] ビューで新しく作成したネットワークを確認できます。仮想マシンまたは vApp がこの組織仮想データセンター ネットワークに接続する場合、仮想マシンまたは vApp は、拡張ネットワークに接続します。

次のステップ

対応する各クロス仮想データセンターの組織仮想データセンター ネットワークに対しても、固定 IP アドレスおよび IP アドレス プールを割り当てることができます。[組織仮想データセンター ネットワーク IP プールへの IP アドレスの追加](#)を参照してください。

拡張ネットワークに接続された仮想マシンの DNS および DHCP 構成の場合、vCloud OpenAPI を使用できます。

vCloud OpenAPI ドキュメントを確認するには、<https://>

`vCloud_Director_IP_address_or_host_name/docs` に移動します。コード サンプルを表示して

vCloud OpenAPI の呼び出しをテストするには、<https://>

`vCloud_Director_IP_address_or_host_name/api-explorer?scope=organization_name` に移動します。

拡張ネットワークの表示または編集


拡張ネットワークの名前、説明、CIDR 設定を表示できます。編集できるのは、拡張ネットワークの名前と説明のみです。

仮想データセンター レベルで拡張ネットワークの固定 IP アドレス プールの割り当てを編集する方法については、「[組織仮想データセンター ネットワーク IP プールへの IP アドレスの追加](#)」を参照してください。

前提条件

- 拡張ネットワークを表示するには、事前定義済みの組織管理者ロール、または組織 VDC ネットワーク：プロパティの表示権限を持つロールが必要です。
- 拡張ネットワークを編集するには、事前定義済みの組織管理者ロール、または組織 VDC ネットワーク：プロパティの編集権限を持つロールが必要です。

手順

- 1 メイン メニュー () で [データセンター グループ] を選択します。

データセンター グループのリストがカード ビューに表示されます。

- 2 ターゲット データセンター グループのカードで、[詳細] をクリックします。

このデータセンター グループの [ネットワーク トポロジ] ビューにリダイレクトされます。現在のネットワーク トポロジが表示され、ネットワーク フォルト ドメイン、出力方向ポイント（設定されている場合）、およびトラフィック ルートと共に、参加中の仮想データセンターを確認できます。

- 3 左側のパネルで、[拡張ネットワーク] をクリックします。

拡張ネットワークのリストがグリッド ビューに表示されます。

- 4 ターゲット ネットワーク名の横にあるラジオ ボタンをクリックして、[編集] をクリックします。
- 5 ネットワークの詳細を編集して、[保存] をクリックします。

拡張ネットワークの削除

不要になった拡張ネットワークは、削除することができます。

前提条件

- この操作を行うには、事前定義済みの組織管理者ロール、または組織 VDC ネットワーク：プロパティの編集権限を持つロールが必要です。
- 対応する組織仮想データセンター ネットワークが、いずれの仮想マシンまたは vApp にも接続されていないこと。

手順

- 1 メイン メニュー (≡) で [データセンター グループ] を選択します。

データセンター グループのリストがカード ビューに表示されます。

- 2 ターゲット データセンター グループのカードで、[詳細] をクリックします。

このデータセンター グループの [ネットワーク トポロジ] ビューにリダイレクトされます。現在のネットワーク トポロジが表示され、ネットワーク フォルト ドメイン、出力方向ポイント（設定されている場合）、およびトラフィック ルートと共に、参加中の仮想データセンターを確認できます。

- 3 左側のパネルで、[拡張ネットワーク] をクリックします。

拡張ネットワークのリストがグリッド ビューに表示されます。

- 4 対象のネットワーク名の横にあるラジオ ボタンをクリックし、[削除] をクリックします。

- 5 確定するには、[削除] をクリックします。

結果

対応する組織仮想データセンター ネットワークが、参加しているすべての仮想データセンターから削除されます。


拡張ネットワークの同期

参加しているすべての仮想データセンターが、拡張ネットワークに確実にアクセスできるようにするには、拡張ネットワークを同期します。

前提条件

この操作を行うには、事前定義済みの組織管理者ロール、または組織 VDC ネットワーク：プロパティの編集権限を持つロールが必要です。

手順

- 1 メイン メニュー () で [データセンター グループ] を選択します。
データセンター グループのリストがカード ビューに表示されます。
- 2 ターゲット データセンター グループのカードで、[詳細] をクリックします。
このデータセンター グループの [ネットワーク トポロジ] ビューにリダイレクトされます。現在のネットワーク トポロジが表示され、ネットワーク フォルト ドメイン、出力方向ポイント（設定されている場合）、およびトラフィック ルートと共に、参加中の仮想データセンターを確認できます。
- 3 左側のパネルで、[拡張ネットワーク] をクリックします。
拡張ネットワークのリストがグリッド ビューに表示されます。
- 4 ターゲット ネットワーク名の横にあるラジオ ボタンをクリックして、[同期] をクリックします。
- 5 確認するには、[OK] をクリックします。

vCloud Director テナントの高度なネットワーク機能

6

vCloud Director は、NSX ネットワーク仮想化ソフトウェアによる高度なネットワーク機能を備えており、クラウド環境でのセキュリティ制御、ルーティング、ネットワーク スケーリングの機能を拡張します。

これらのネットワーク機能を使用すると、組織仮想データセンター内で比類のないセキュリティと隔離を実現できます。これらの機能のメリットは次のとおりです。

- 動的ルーティング。vCloud Director 環境の NSX 機能は、Border Gateway Protocol (BGP) や Open Shortest Path First (OSPF) などのルーティング プロトコルをサポートしてシステム間のネットワーク統合を簡素化し、クラウド ホスト型アプリケーションのデプロイに冗長性と継続性をもたらします。
- きめ細かなネットワーク セキュリティと隔離。vCloud Director 環境の NSX 機能では、オブジェクト ベースのルール定義を使用できるため、複数の仮想ネットワークを用意しなくても、ステートフルにネットワーク トラフィックを隔離できます。このゼロトラスト セキュリティ モデルでは、アプリケーションや仮想マシンが侵害されても、侵入者がネットワークに完全にアクセスすることはできません。ネットワーク構成を簡素化するには、同一のネットワーク セキュリティ ポリシーを使用して、アプリケーションを vCloud Director 環境内の物理的に配置されている場所に関係なく保護し、アプリケーションがデプロイされている場所に関係なくセキュリティを移植できるようにゼロトラスト セキュリティ モデルを拡張します。
- NSX が備えるその他の機能には、ポイント対サイト接続用に拡張された VPN (IPSec VPN) とユーザー接続用に拡張された VPN (SSL VPN-Plus) のサポート、HTTPS 用に拡張されたロード バランシング、拡張されたネットワーク スケーラビリティがあります。

Edge Gateway ファイアウォールと分散ファイアウォールの 2 種類のファイアウォールを設定できます。これらのファイアウォールの違いの詳細については、[テナント ポータルを使用したファイアウォール構成](#)を参照してください。

これらの高度なネットワーク機能にアクセスするには、vCloud Director テナント ポータルまたは vCloud Director Service Provider Admin Portal を使用します。Edge Gateway は、詳細 Edge Gateway に変換する必要があります。『[Edge Gateway から詳細 Edge Gateway への変換](#)』を参照してください。

重要： IPv6 Edge Gateway ではサポートされるサービスが制限されます。IPv6 Edge Gateway は Edge ファイアウォール、分散ファイアウォール、スタティック ルーティングをサポートします。

この章には、次のトピックが含まれています。

- [vCloud Director の高度なネットワークの概要](#)
- [テナント ポータルを使用したファイアウォール構成](#)
- [Edge Gateway の DHCP の管理](#)

- テナント ポータルを使用したネットワーク アドレス変換の管理
- 高度なルーティングの設定
- ロード バランシング
- 仮想プライベート ネットワークを使用したセキュアなアクセス
- SSL 証明書の管理
- オブジェクトのグループ分け（カスタム）
- Edge Gateway の統計情報とログ
- SSH コマンドラインによる Edge Gateway へのアクセスの有効化
- セキュリティ タグの操作
- セキュリティ グループの操作

vCloud Director の高度なネットワークの概要

vCloud Director の高度なネットワークは、vCloud Director システムで組織の管理タスクを実行するために使用します。分散ファイアウォール、および VMware NSX[®] ソフトウェア コンポーネントによって提供されるその他の高度なネットワーク機能のうち、vCloud Director システム管理者が組織で利用できるようにしたものを管理できます。

高度なネットワークの一般的なユーザーは、次のとおりです。

- vCloud Director システム管理者。テナント ポータルを使用して、組織のために分散ファイアウォールやその他の高度なネットワーク機能を設定できます。
- 組織の管理者。テナント ポータルを使用して、システム管理者が組織で使えるようにした分散ファイアウォールやその他の高度なネットワーク機能を管理できます。

テナント ポータルを使用したファイアウォール構成

テナント ポータルを使用して、NSX ソフトウェアが提供するファイアウォール機能を vCloud Director 組織仮想データセンター内で構成できます。分散ファイアウォールのファイアウォール ルールを作成して、組織仮想データセンターの仮想マシン間でセキュリティを確保できます。また、外部のネットワーク トラフィックから組織仮想データセンター内の仮想マシンを保護するためのファイアウォール ルールを作成して Edge Gateway のファイアウォールに適用できます。

注： テナント ポータルでは、Edge Gateway のファイアウォールと分散ファイアウォールの両方を構成できません。

NSX 論理ファイアウォール テクノロジーは、さまざまなデプロイ事例に対応する 2 つのコンポーネントで構成されます。Edge Gateway のファイアウォールは North-South トラフィックの強制に重点を置き、分散ファイアウォールは East-West アクセスの制御に重点を置いています。

Edge Gateway のファイアウォールと分散ファイアウォールの主な相違点

Edge Gateway のファイアウォールは、North-South トラフィックを監視し、ファイアウォールやネットワーク アドレス変換 (NAT) を含む境界セキュリティ機能のほか、サイト間の IPSec および SSL VPN 機能を提供します。

分散ファイアウォールは、レイヤー 2 (L2) レベルまでの各仮想マシンとアプリケーションを隔離し、保護するための機能を提供します。分散ファイアウォールを構成すると、外部または内部ネットワークのあらゆるセキュリティ侵害を効果的に検疫できます。また、同じネットワーク セグメント上の仮想マシン間の East-West トラフィックを隔離できます。セキュリティ ポリシーは一元的に管理され、継承可能であり、入れ子構造にすることができます。このため、ネットワーク管理者とセキュリティ管理者はセキュリティ ポリシーを大きな規模で管理できます。また、デプロイ後に仮想マシンまたはアプリケーションが仮想データセンター間を移動しても、定義済みのセキュリティ ポリシーは仮想マシンまたはアプリケーションに付随します。

ファイアウォール ルールについて

NSX 製品ドキュメントで説明されているように、NSX では、一元的なレベルで定義されたファイアウォール ルールをプレルールと呼びます。また、個々の Edge Gateway レベルでルールを追加することもでき、このルールをローカル ルールと呼びます。

各トラフィック セッションは、ファイアウォール テーブルの一番上のルールと照合された後、テーブルの下位のルールに移動します。テーブル内のルールのうち、トラフィック パラメータと一致する最初のルールが適用されます。ルールは次の順序で表示されます。

- 1 ユーザー定義のプレルール。優先度が最も高く、仮想 NIC レベルごとの優先順位を使用して上から下の順序で適用されます。
- 2 自動組み込みルール (Edge Gateway サービスのトラフィックのフローを制御できるルール)。
- 3 Edge Gateway レベルで定義されたローカル ルール。
- 4 デフォルトの分散ファイアウォール ルール

NSX ソフトウェアでファイアウォール ルールを適用する方法の詳細については、『NSX 管理ガイド』で「ファイアウォール ルールの順序の変更」を参照してください。

Edge Gateway のファイアウォール

IP アドレス/VLAN 構成要素に基づいた DMZ の構築、マルチテナント仮想データセンターでのテナント間の隔離、ネットワーク アドレス変換 (NAT)、パートナー (エクストラネット) VPN、ユーザーベースの SSL VPN など、主な境界セキュリティ要件を満たすのに Edge Gateway のファイアウォールが役立ちます。

vCloud Director 環境の Edge Gateway ファイアウォール機能は、NSX ソフトウェアによって提供されます。NSX では、このファイアウォール機能は Edge ファイアウォールとも呼ばれます。Edge Gateway のファイアウォールは、North-South トラフィックを監視し、ファイアウォールやネットワーク アドレス変換 (NAT) を含む境界セキュリティ機能のほか、サイト間の IPSec および SSL VPN 機能を提供します。

NSX ソフトウェアの Edge Gateway ファイアウォールが提供する機能の詳細については、『NSX 管理ガイド』を参照してください。

NSX Data Center for vSphere Edge Gateway ファイアウォールの管理

Edge Gateway に送受信されるトラフィックを保護するには、その Edge Gateway にファイアウォール ルールを作成して、管理します。

組織仮想データセンター内の仮想マシン間で移動するトラフィックの保護方法については、[テナント ポータルを使用した分散ファイアウォール ルールの管理](#)を参照してください。

分散ファイアウォールの画面で作成され、[適用対象] 列で詳細 Edge ゲートウェイが指定されているルールは、その詳細 Edge ゲートウェイの [ファイアウォール] 画面に表示されません。

Edge Gateway の Edge Gateway ファイアウォール ルールは、[ファイアウォール] 画面に表示され、次の順序で適用されます。

- 1 内部ルール。自動配管ルールとも呼ばれます。これらの内部ルールにより、トラフィックが Edge ゲートウェイ サービスに流れるように制御できます。
- 2 ユーザー定義ルール。
- 3 デフォルト ルール。

デフォルト ルールの設定は、どのユーザー定義ファイアウォール ルールにも一致しないトラフィックに適用されます。デフォルト ルールは、[ファイアウォール] 画面の最下部に表示されます。

テナント ポータルで、Edge Gateway の [ファイアウォール ルール] 画面の [有効化] 切り替えを使用して、Edge Gateway ファイアウォールを無効または有効にします。

Edge Gateway から詳細 Edge Gateway への変換

テナント ポータルで Edge Gateway を使用するには、Edge Gateway を詳細 Edge Gateway に変換する必要があります。詳細 Edge Gateway に変換すると、テナント ポータルを使用して、NSX ソフトウェアが提供する固定および動的ルーティング機能をこれらの詳細 Edge Gateway 用に設定できます。

前提条件

Edge Gateway がすでにあることが必要です。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルから [エッジ] を選択します。
- 2 編集する Edge Gateway を選択します。
- 3 [詳細に変換] をクリックします。

結果

Edge Gateway が詳細 Edge Gateway に変換されます。

次のステップ

詳細 Edge Gateway に変換した後は、ゲートウェイを選択して [サービス] をクリックすることで設定できます。

NSX Data Center for vSphere Edge Gateway ファイアウォール ルールの追加

Edge Gateway のファイアウォール ルールを追加するには、この Edge Gateway の [ファイアウォール] タブを使用します。これらのファイアウォール ルールのソースおよびターゲットとして複数の NSX Edge インターフェイスと複数の IP アドレス グループを追加できます。

ルールのソースまたはターゲットに [内部] を指定すると、NSX Edge Gateway に接続されたポート グループ上のすべてのサブネットのトラフィックが指定されます。ソースとして [内部] を選択した場合は、NSX ゲートウェイに追加で内部インターフェイスを設定すると、ルールが自動的に更新されます。

注： Edge ゲートウェイを動的ルーティング用に設定すると、内部インターフェイスの Edge ゲートウェイ ファイアウォール ルールは機能しません。

手順

- Edge Gateway サービスを開きます。
 - [ネットワーク] > [エッジ] の順に選択します。
 - 編集する Edge Gateway を選択し、[サービス] をクリックします。
- [ファイアウォール ルール] 画面が表示されない場合は、[ファイアウォール] タブをクリックします。
- ファイアウォール ルール テーブルで既存のルールの下にルールを追加するには、その既存の行をクリックし、[作成] ボタンをクリックします。

新しいルールの行が選択したルールの下に追加され、デフォルトでは、すべてのターゲット、すべてのサービス、および [許可] アクションが割り当てられます。ファイアウォール テーブルにシステム定義のデフォルト ルールしかない場合、新しいルールはデフォルトのルールの上に追加されます。

- [名前] セルをクリックし、名前を入力します。
- [ソース] セルをクリックし、表示されているアイコンを使用して、ルールに追加するソースを選択します。

オプション	説明
[IP] アイコンをクリック	使用するソースの値を入力します。有効な値は、IP アドレス、CIDR、IP アドレス範囲、またはキーワード any です。Edge ゲートウェイ ファイアウォールは、IPv4 と IPv6 の両方の形式をサポートしています。
[+] アイコンをクリック	<p>[+] アイコンを使用し、特定の IP アドレス以外のオブジェクトをソースとして次のように指定します。</p> <ul style="list-style-type: none"> ■ [オブジェクトの選択] ウィンドウを使用し、選択内容に一致するオブジェクトを追加し、[保持] をクリックしてそれらをルールに追加します。 ■ ソースをルールから除外するには、[オブジェクトの選択] ウィンドウを使用してこのルールに追加し、次に除外の切り替えアイコンを選択してそのソースをこのルールから除外します。 <p>ソースで除外の切り替えを選択すると、すべてのソース（除外したソースを除く）から受信するトラフィックにルールが適用されます。除外の切り替えを選択しない場合、[オブジェクトの選択] ウィンドウで指定したソースから受信するトラフィックにルールが適用されます。</p>

- 6 [ターゲット] セルをクリックし、次のオプションのいずれかを実行します。

オプション	説明
[IP] アイコンをクリック	使用するターゲットの値を入力します。有効な値は、IP アドレス、CIDR、IP アドレス範囲、またはキーワード any です。Edge ゲートウェイ ファイアウォールは、IPv4 と IPv6 の両方の形式をサポートしています。
[+] アイコンをクリック	<p>[+] アイコンを使用し、特定の IP アドレス以外のオブジェクトをソースとして次のように指定します。</p> <ul style="list-style-type: none"> ■ [オブジェクトの選択] ウィンドウを使用し、選択内容に一致するオブジェクトを追加し、[保持] をクリックしてそれらをルールに追加します。 ■ ソースをルールから除外するには、[オブジェクトの選択] ウィンドウを使用してこのルールに追加し、次に除外の切り替えアイコンを選択してそのソースをこのルールから除外します。 <p>ソースで除外の切り替えを選択すると、すべてのソース（除外したソースを除く）から受信するトラフィックにルールが適用されます。除外の切り替えを選択しない場合、[オブジェクトの選択] ウィンドウで指定したソースから受信するトラフィックにルールが適用されます。</p>

- 7 新しいルールの [サービス] セルをクリックし、[+] アイコンをクリックして、そのサービスをポートとプロトコルの組み合わせとして指定します。

- サービス プロトコルを選択します。
- ソース ポートとターゲット ポートのポート番号を入力するか、**任意** を指定します。
- [保持] をクリックします。

- 8 新しいルールの [アクション] セルで、ルールのアクションを設定します。

オプション	説明
承諾	指定されたソース、ターゲット、およびサービスとの間のトラフィックを許可します。
拒否	指定されたソース、ターゲット、およびサービスとの間のトラフィックをブロックします。

- 9 [変更を保存] をクリックします。

保存操作が完了するまでに 1 分ほどかかることがあります。

NSX Data Center for vSphere Edge Gateway ファイアウォール ルールの変更

編集および削除できるのは、Edge ゲートウェイに追加されたユーザー定義のファイアウォール ルールのみです。自動生成されたルールまたはデフォルトのルールを編集または削除することはできません。ただし、デフォルト ルールのアクション設定は変更できます。ユーザー定義のルールは、優先順位を変更できます。

ルールが格納されている各セルで使用可能な設定の詳細については、[NSX Data Center for vSphere Edge Gateway ファイアウォール ルールの追加](#)を参照してください。

手順

- Edge Gateway サービスを開きます。
 - [ネットワーク] > [エッジ] の順に選択します。
 - 編集する Edge Gateway を選択し、[サービス] をクリックします。

2 [ファイアウォール] タブをクリックします。

3 ファイアウォール ルールを管理します。

- ルールを無効にする。これは、[いいえ]セルの緑色のチェック マークをクリックすることで行います。緑色のチェック マークは、無効を示す赤色のアイコンになります。無効にしたルールを有効にするには、無効を示す赤色のアイコンをクリックします。
- ルール名を編集する。これは、[名前] セルをダブルクリックして、新しい名前を入力することで行います。
- ルールの設定（ソース設定やアクション設定など）を変更する。これは、該当するセルを選択し、表示されたコントロールを使用することで行います。
- ルールを削除する。これは、ルール テーブルの上にある [削除] ボタンをクリックすることで行います。
- [ユーザー定義のルールのみを表示] 切り替えを使用して、システムによって生成されたルールを非表示にします。
- ルール テーブルでルールを上下に移動する。これは、ルールを選択して、ルール テーブルの上にある上下の矢印ボタンをクリックすることで行います。

4 [変更を保存] をクリックします。

分散ファイアウォール

分散ファイアウォールを使用すると、仮想マシンなどの組織仮想データセンター エンティティを仮想マシン名と属性に基づいてセグメント化できます。

vCloud Director は、NSX Data Center for vSphere によってバックアップされた組織仮想データセンターで分散ファイアウォール サービスをサポートしています。『NSX 管理ガイド』ドキュメントで説明されているように、この分散ファイアウォールは、ハイパーバイザー カーネルが組み込まれたファイアウォールであり、仮想化されたワークロードとネットワークを可視化および制御できます。仮想マシン名などのオブジェクトと、IP アドレスや IP セット アドレスなどのネットワーク構成要素に基づいて、アクセス制御ポリシーを作成できます。仮想マシンが vSphere vMotion によって新しい ESXi ホストに移動しても一貫したアクセス制御が提供されるようにファイアウォール ルールは各仮想マシンの vNIC レベルで適用されます。この分散ファイアウォールはマイクロセグメンテーション セキュリティ モデルをサポートし、East-West トラフィックを回線速度とほぼ同じ処理速度で検査できます。

『NSX 管理ガイド』ドキュメントで説明されているように、レイヤー 2 (L2) パケットの場合、分散ファイアウォールはキャッシュを作成し、パフォーマンスを向上させます。レイヤー 3 (L3) パケットは次の順序で処理されます。

- 1 すべてのパケットの既存の状態がチェックされます。
 - 2 状態の一致が見つかったら、そのパケットが処理されます。
 - 3 状態の一致が見つからない場合、そのパケットは一致が見つかるまでルールを介して処理されます。
- TCP パケットの場合、状態は、SYN フラグの付いたパケットに対してのみ設定されます。ただし、プロトコルを指定しないルール (service ANY) では、任意の組み合わせのフラグが付いた TCP パケットが一致する可能性があります。

- UDP パケットの場合、5-tuple の詳細がパケットから抽出されます。状態が状態テーブルにない場合、抽出された 5-tuple の詳細を使用して新しい状態が作成されます。その後受信したパケットは、この作成された状態と照合されます。
- ICMP パケットの場合、ICMP タイプ、コード、およびパケットの方向を使用して状態が作成されます。

分散ファイアウォールは、ID ベースのルールの作成にも役立つ可能性があります。管理者は、企業の Active Directory (AD) で定義された、ユーザーのグループ メンバーシップに基づいてアクセス制御を適用できます。ID ベースのファイアウォール ルールの使用事例を以下にいくつか示します。

- ユーザーがラップトップやモバイル デバイスを使用して仮想アプリケーションにアクセスする。ユーザー認証には Active Directory を使用する
- ユーザーが VDI インフラストラクチャを使用して仮想アプリケーションにアクセスする。仮想マシンは Microsoft Windows ベースである

NSX ソフトウェアの分散ファイアウォールが提供する機能の詳細については、『NSX 管理ガイド』ドキュメントを参照してください。

テナント ポータルを使用した、組織仮想データセンターでの分散ファイアウォールの有効化

組織仮想データセンターで分散ファイアウォール機能に対してテナント ポータルを使用するには、あらかじめこの組織仮想データセンターの分散ファイアウォールを有効にする必要があります。組織仮想データセンターで分散ファイアウォールを有効にすることができるのは、ORG_VDC_DISTRIBUTED_FIREWALL_ENABLE 権限を与えられている vCloud Director システム管理者またはユーザーです。

テナント ポータルの [分散ファイアウォール] 画面を使用して、組織仮想データセンターの分散ファイアウォールを有効にします。

前提条件

組織仮想データセンターが属している組織に、次の権限が割り当てられていることを確認します。

- 組織 VDC 分散ファイアウォール：有効化/無効化
- 組織 VDC 分散ファイアウォール：ルールの構成
- 組織 VDC 分散ファイアウォール：ルールの表示

vCloud Director システム管理者は、組織に権限を割り当てます。組織 vDC 分散ファイアウォール：有効化/無効化権限は、テナント ポータルのユーザー インターフェイスを使用して分散ファイアウォールを有効にするために必要です。組織 VDC 分散ファイアウォール：ルールの表示権限はテナント ポータルでルールを表示するために、また、組織 VDC 分散ファイアウォールのルールの構成権限はテナント ポータルを使用してファイアウォール ルールを構成するために必要です。

自身に割り当てられているロールに、組織 VDC 分散ファイアウォール：有効化/無効化権限が付与されていることを確認します。vCloud Director システムで事前定義されているロールのうちシステム管理者ロールだけが、デフォルトでこの権限を持っています。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、[ネットワーク] で[セキュリティ] を選択します。
- 2 分散ファイアウォール ルールを設定する組織仮想データセンターを選択します。
- 3 [サービスの構成] をクリックします。
- 4 [分散ファイアウォール] タブで分散ファイアウォールを有効にします。

次のステップ

デフォルトの分散ファイアウォール ルールについては、[テナント ポータルを使用した分散ファイアウォール ルールの管理](#)を参照してください。

テナント ポータルを使用した分散ファイアウォール ルールの管理

『NSX 管理ガイド』で説明されているように、デフォルトのファイアウォール設定は、ユーザー定義のどのファイアウォール ルールにも一致しないトラフィックに適用されます。vCloud Director Tenant Portal では、デフォルトの分散ファイアウォール ルールに [デフォルトの許可ルール] のラベルが付けられています。

vCloud Director Tenant Portal を使用して分散ファイアウォール設定を管理するには、組織仮想データセンターで分散ファイアウォール機能を有効にしておく必要があります。

デフォルトの分散ファイアウォール ルールは、レイヤー 3 とレイヤー 2 のすべてのトラフィックが組織仮想データセンターを通過できるように設定されています。この設定は、ユーザー インターフェイスの [アクション] 列に設定された [許可] で示されます。デフォルト ルールは常にルール テーブルの下部にあります。

重要： デフォルトの分散ファイアウォール ルールを削除または変更することはできません。

分散ファイアウォール ルールの追加

まず組織仮想データセンターの範囲に分散ファイアウォール ルールを追加します。次に、ルールを適用する範囲を絞り込むことができます。分散ファイアウォールでは、各ルールのソースおよびターゲットのレベルに複数のオブジェクトを追加して、追加する必要があるファイアウォール ルールの総数を減らすことができます。

ルール内で使用できる事前定義済みのサービスおよびサービス グループの詳細については、[ファイアウォール ルールで使用可能なサービスの表示およびファイアウォール ルールで使用可能なサービス グループの表示](#)を参照してください。

前提条件

- テナント ポータルを使用した、組織仮想データセンターでの分散ファイアウォールの有効化
- ルール内で送信元または宛先として IP セットを使用する場合は、[ファイアウォール ルールと DHCP リレー設定で使用するための IP アドレス セットの作成](#)を行います。
- ルール内で送信元または宛先として MAC セットを使用する場合は、[ファイアウォール ルールで使用するための MAC アドレス セットの作成](#)を行います。
- ルール内で送信元または宛先としてセキュリティ グループを使用する場合は、[セキュリティ グループの作成](#)を行います。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、[ネットワーク] で [セキュリティ] を選択します。
- 2 ファイアウォール ルールを変更するセキュリティ サービスの仮想データセンター ネットワークを選択し、[サービスの構成]をクリックします。

[セキュリティ サービス] 画面が表示されます。

- 3 作成するルールのタイプを選択します。一般的なルールまたはイーサネット ルールを作成するオプションがあります。

レイヤー 3 (L3) ルールは [全般] タブで構成されます。レイヤー 2 (L2) ルールは [イーサネット] タブで構成されます。

- 4 ファイアウォール テーブルの既存のルールの下にルールを追加するには、既存の行をクリックし、[作成]

() ボタンをクリックします。

新しいルールの行が選択したルールの下に追加され、デフォルトでは、すべてのターゲット、すべてのサービス、および [許可] アクションが割り当てられます。ファイアウォール テーブルにシステム定義のデフォルトの許可ルールしかない場合には、新しいルールはデフォルトのルールの上に追加されます。

- 5 [名前] セルをクリックし、名前を入力します。
- 6 [ソース] セルをクリックし、表示されているアイコンを使用して、ルールに追加するソースを選択します。

アクション	説明
[IP] アイコンをクリック	<p>[全般] タブで定義されたルールを適用します。</p> <p>使用するソースの値を入力します。有効な値は、IP アドレス、CIDR、IP アドレス範囲、またはキーワード any です。分散ファイアウォールは、IPv4 形式のみをサポートします。</p>
[+] アイコンをクリック	<p>[+] アイコンを使用し、特定の IP アドレス以外のオブジェクトをソースとして次のように指定します。</p> <ul style="list-style-type: none"> ■ [オブジェクトの選択] ウィンドウを使用し、選択内容に一致するオブジェクトを追加し、[保持] をクリックしてそれらをルールに追加します。 ■ ソースをルールから除外するには、[オブジェクトの選択] ウィンドウを使用してこのルールに追加し、次に除外の切り替えアイコンを選択してそのソースをこのルールから除外します。 <p>ソースで除外の切り替えを選択すると、すべてのソース（除外したソースを除く）から受信するトラフィックにルールが適用されます。除外の切り替えを選択しない場合、[オブジェクトの選択] ウィンドウで指定したソースから受信するトラフィックにルールが適用されます。</p>

7 [ターゲット] セルをクリックし、次のアクションのいずれかを実行します。

アクション	説明
[IP] アイコンをクリック	<p>[全般] タブで定義されたルールを適用します。</p> <p>使用するターゲットの値を入力します。有効な値は、IP アドレス、CIDR、IP アドレス範囲、またはキーワード any です。分散ファイアウォールは、IPv4 形式のみをサポートします。</p>
[+] アイコンをクリック	<p>[+] アイコンを使用し、特定の IP アドレス以外のオブジェクトをソースとして次のように指定します。</p> <ul style="list-style-type: none"> ■ [オブジェクトの選択] ウィンドウを使用し、選択内容に一致するオブジェクトを追加し、[保持] をクリックしてそれらをルールに追加します。 ■ ソースをルールから除外するには、[オブジェクトの選択] ウィンドウを使用してこのルールに追加し、次に除外の切り替えアイコンを選択してそのソースをこのルールから除外します。 <p>ソースで除外の切り替えを選択すると、すべてのソース（除外したソースを除く）から受信するトラフィックにルールが適用されます。除外の切り替えを選択しない場合、[オブジェクトの選択] ウィンドウで指定したソースから受信するトラフィックにルールが適用されます。</p>

8 新しいルールの [サービス] セルをクリックし、次のいずれかのアクションを実行します。

アクション	説明
[IP] アイコンをクリック	<p>サービスをポートとプロトコルの組み合わせとして指定します。</p> <ul style="list-style-type: none"> a サービス プロトコルを選択します。 b ソースとターゲット ポートのポート番号を入力するか、または 任意 を指定し、[保持] をクリックします。
[+] アイコンをクリック	<p>事前定義済みサービスまたはサービス グループを選択するか、または新規のものを定義するには、次のようにします。</p> <ul style="list-style-type: none"> a 1 つまたは複数のオブジェクトを選択し、フィルタに追加します。 b [保持] をクリックします。

9 新しいルールの [アクション] セルで、ルールのアクションを設定します。

オプション	説明
許可	指定されたソース、ターゲット、およびサービスとの間のトラフィックを許可します。
拒否	指定されたソース、ターゲット、およびサービスとの間のトラフィックをブロックします。

10 新しいルールの [方向] セルで、ルールを受信トラフィック、送信トラフィック、またはその両方のいずれに適用するかを選択します。

11 これが [全般] タブのルールである場合、新しいルールの [パケット タイプ] セルで、パケット タイプとして [任意]、[IPv4]、または [IPv6] のいずれかを選択します。

12 [適用対象] セルを選択し、[+] アイコンを使用してこのルールが適用されるオブジェクト範囲を定義します。

ルールに [ソース] と [ターゲット] セル内の仮想マシンが含まれている場合は、ルールが正常に機能するように、ソースとターゲットの両方の仮想マシンをルールの [適用対象] に追加する必要があります。

重要： IP アドレス グループ (IP セット)、MAC アドレス グループ (MAC セット)、および IP セットまたは MAC セットを含むセキュリティ グループは、有効な入力パラメータではありません。

13 [変更を保存] をクリックします。

分散ファイアウォール ルールの編集


vCloud Director 環境で組織仮想データセンターの既存の分散ファイアウォール ルールを変更するには、[分散ファイアウォール] 画面を使用します。

ルールが格納されている各セルで使用可能な設定の詳細については、[分散ファイアウォール ルールの追加](#)を参照してください。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、[ネットワーク] で [セキュリティ] を選択します。
- 2 ファイアウォール ルールを変更するセキュリティ サービスの仮想データセンター ネットワークを選択し、[サービスの構成] をクリックします。

[セキュリティ サービス] 画面が表示されます。
- 3 分散ファイアウォール ルールを管理するには、次のいずれかのアクションを実行します。
 - ルールを無効にする。これは、[いいえ] セルの緑色のチェック マークをクリックすることで行います。

緑色のチェック マークは、無効を示す赤色のアイコンになります。無効にしたルールを有効にするには、無効を示す赤色のアイコンをクリックします。
 - ルール名を編集する。これは、[名前] セルをダブルクリックして、新しい名前を入力することで行います。
 - ルールの設定（ソース設定やアクション設定など）を変更する。これは、該当するセルを選択し、表示されたコントロールを使用することで行います。
 - ルールを削除する。これは、ルール テーブルの上にある [削除] () ボタンをクリックすることで行います。
 - ルール テーブルでルールを上下に移動する。これは、ルールを選択して、ルール テーブルの上にある上下の矢印ボタンをクリックすることで行います。
- 4 [変更を保存] をクリックします。

Edge Gateway の DHCP の管理

関連する組織仮想データセンター ネットワークに接続された仮想マシンに Dynamic Host Configuration Protocol (DHCP) サービスを提供するように、Edge Gateway を設定します。

[NSX ドキュメント](#)で説明するとおり、NSX Edge Gateway 機能には、IP アドレスのプール化、1 対 1 の固定 IP アドレスの割り当て、および外部 DNS サーバ構成が含まれます。静的 IP アドレス バインディングは、管理対象オブジェクト ID と、要求側のクライアント仮想マシンのインターフェイス ID に基づきます。

NSX Edge ゲートウェイの DHCP サービスの特長は次のとおりです。

- DHCP 検出のために Edge Gateway の内部インターフェイスで待機します。

- すべてのクライアントのデフォルト ゲートウェイ アドレスとして、Edge Gateway の内部インターフェイスの IP アドレスを使用します。
- コンテナ ネットワークに対し、内部インターフェイスのブロードキャストとサブネット マスクの値を使用します。

次の状況では、DHCP が割り当てられた IP アドレスを持つクライアント仮想マシンで DHCP サービスを再起動する必要があります。

- DHCP プール、デフォルト ゲートウェイ、または DNS サーバを変更または削除した場合。
- Edge ゲートウェイ インスタンスの内部 IP アドレスを変更した場合。

注： DHCP 対応の Edge ゲートウェイ上の DNS 設定を変更すると、Edge ゲートウェイは DHCP サービスを提供しなくなります。このような状況が発生した場合は、[DHCP プール] 画面の [DHCP サービスのステータス] 切り替えを使用して、その Edge ゲートウェイの DHCP を無効にしてから再度有効にします。[DHCP IP プールの追加](#) を参照してください。

DHCP IP プールの追加

NSX Data Center for vSphere Edge Gateway の DHCP サービスに必要な IP プールを構成できます。DHCP は、組織仮想データセンター ネットワークに接続された仮想マシンへの IP アドレスの割り当てを自動化します。


『NSX 管理ガイド』に説明されているとおり、DHCP サービスには IP アドレスのプールが必要です。IP プールとは、ネットワーク内の連続した IP アドレスの範囲です。アドレス バインディングを持たない Edge ゲートウェイによって保護されている仮想マシンには、このプールから IP アドレスが割り当てられます。IP プールの範囲が互いに交わることはないため、1つの IP アドレスが属することができるのは1つの IP プールのみです。

注： DHCP サービスのステータスをオンにするには、少なくとも1つの DHCP IP プールを設定する必要があります。

手順

- 1 Edge Gateway サービスを開きます。
 - a [ネットワーク] > [エッジ] の順に選択します。
 - b 編集する Edge Gateway を選択し、[サービス] をクリックします。
- 2 [DHCP] - [プール] の順に移動します。
- 3 DHCP サービスが現在有効でない場合は、[DHCP サービスのステータス] の切り替えをオンにします。

注： [DHCP サービスのステータス] の切り替えをオンにした後には、変更を保存する前に少なくとも1つの DHCP IP アドレス プールを追加します。画面に DHCP IP プールが表示されておらず、[DHCP サービスのステータス] の切り替えをオンにして変更内容を保存する場合には、画面は切り替えがオフになって表示されます。

- 4 DHCP プールで、[作成] () ボタンをクリックし、DHCP プールの詳細を指定して [保持] をクリックします。

オプション	説明
IP の範囲	IP アドレスの範囲を入力します。
ドメイン名	DNS サーバのドメイン名。
DNS の自動構成	この IP プールの DNS バインディングに DNS サービス構成を使用するには、この切り替えを有効にします。 有効にすると、[プライマリ ネーム サーバ] と [セカンダリ ネーム サーバ] は [自動] に設定されます。
プライマリ ネーム サーバ	[DNS の自動構成] を有効にしない場合は、プライマリ DNS サーバの IP アドレスを入力します。 この IP アドレスは、ホスト名 - IP アドレス解決のために使用されます。
セカンダリ ネーム サーバ	[DNS の自動構成] を有効にしない場合は、セカンダリ DNS サーバの IP アドレスを入力します。 この IP アドレスは、ホスト名 - IP アドレス解決のために使用されます。
デフォルト ゲートウェイ	デフォルト ゲートウェイ アドレスを入力します。 デフォルト ゲートウェイ IP アドレスを指定しない場合は、Edge ゲートウェイ インスタンスの内部インターフェイスがデフォルト ゲートウェイとして使用されます。
サブネット マスク	Edge Gateway インターフェイスのサブネット マスクを入力します。
リースには有効期限がありません	このプールから割り当てられた IP アドレスが、割り当てられている仮想マシンに永続的にバインドされるようにするには、この切り替えを有効にします。 このオプションを選択すると、[リース時間] は無限に設定されます。
リース時間 (秒)	DHCP 割り当ての IP アドレスがクライアントにリースされる時間の長さ (秒単位)。 デフォルトのリース時間は、1 日 (86,400 秒) です。 注： [リースには有効期限がありません] を選択すると、リース時間を指定することはできません。

- 5 [変更を保存] をクリックします。

結果

vCloud Director は、DHCP サービスを提供するために Edge ゲートウェイを更新します。


DHCP バインディングの追加

サービスが動作中の仮想マシンで、IP アドレスが変更されないようにする場合は、仮想マシンの MAC アドレスを IP アドレスにバインドできます。バインドする IP アドレスは、DHCP IP プールと重複しないようにしてください。

前提条件

バインディングを設定する仮想マシンの MAC アドレスを手元に控えておきます。

手順

- 1 Edge Gateway サービスを開きます。
 - a [ネットワーク] > [エッジ] の順に選択します。
 - b 編集する Edge Gateway を選択し、[サービス] をクリックします。
- 2 [DHCP] - [バインディング] タブで [作成] () ボタンをクリックして、バインディングの詳細を指定し、[保持] をクリックします。

オプション	説明
MAC アドレス	IP アドレスにバインドする仮想マシンの MAC アドレスを入力します。
ホスト名	仮想マシンが DHCP リースを要求するときに、その仮想マシンに設定するホスト名を入力します。
IP アドレス	MAC アドレスにバインドする IP アドレスを入力します。
サブネット マスク	Edge Gateway インターフェイスのサブネット マスクを入力します。
ドメイン名	DNS サーバのドメイン名を入力します。
DNS の自動構成	この DNS バインディングに DNS サービス構成を使用するには、この切り替えを有効にします。 有効にすると、[プライマリ ネーム サーバ] と [セカンダリ ネーム サーバ] は [自動] に設定されます。
プライマリ ネーム サーバ	[DNS の自動構成] を選択しない場合は、プライマリ DNS サーバの IP アドレスを入力します。 この IP アドレスは、ホスト名 - IP アドレス解決のために使用されます。
セカンダリ ネーム サーバ	[DNS の自動構成] を選択しない場合は、セカンダリ DNS サーバの IP アドレスを入力します。 この IP アドレスは、ホスト名 - IP アドレス解決のために使用されます。
デフォルト ゲートウェイ	デフォルト ゲートウェイ アドレスを入力します。 デフォルト ゲートウェイ IP アドレスを指定しない場合は、Edge ゲートウェイ インスタンスの内部インターフェイスがデフォルト ゲートウェイとして使用されます。
リースには有効期限がありません	IP アドレスがその MAC アドレスに永続的にバインドされるようにするには、この切り替えを有効にします。 このオプションを選択すると、[リース時間] は無限に設定されます。
リース時間 (秒)	DHCP 割り当ての IP アドレスがクライアントにリースされる時間の長さ (秒単位)。 デフォルトのリース時間は、1 日 (86,400 秒) です。 注： [リースには有効期限がありません] を選択すると、リース時間を指定することはできません。

- 3 [変更を保存] をクリックします。

NSX Data Center for vSphere Edge Gateway の DHCP リレーの設定

vCloud Director 環境の NSX が提供する DHCP リレー機能により、既存の DHCP インフラストラクチャでの IP アドレス管理を中断せずに、vCloud Director 環境内で既存の DHCP インフラストラクチャを活用できます。DHCP メッセージは、仮想マシンから、物理 DHCP インフラストラクチャにある指定された DHCP サーバにリレ

ーされます。これにより、NSX ソフトウェアが制御する IP アドレスは、DHCP 制御された環境内にある他の IP アドレスと引き続き同期されます。

Edge Gateway の DHCP リレー構成では、複数の DHCP サーバをリストできます。要求は、リストされたすべてのサーバに送信されます。仮想マシンから DHCP 要求をリレーする間、Edge ゲートウェイはゲートウェイの IP アドレスを要求に追加します。外部 DHCP サーバはこのゲートウェイ アドレスを使用してプールを照合し、要求の IP アドレスを割り当てます。ゲートウェイ アドレスは、Edge Gateway のインターフェイスのサブネットに属している必要があります。

各 Edge ゲートウェイには異なる DHCP サーバを構成できるほか、各 Edge ゲートウェイでは、複数の IP アドレスのドメインに対応するため、複数の DHCP サーバを構成できます。

注：

- DHCP リレーでは、重複する IP アドレス空間はサポートされません。
 - DHCP リレーと DHCP サービスを同じ vNIC で同時に実行することはできません。vNIC にリレー エージェントが構成されている場合、その vNIC のサブネットで DHCP プールを構成することはできません。詳細については、『NSX 管理ガイド』を参照してください。
-

NSX Data Center for vSphere Edge Gateway の DHCP リレー構成の指定

vCloud Director 環境内の NSX ソフトウェアにより、Edge Gateway は vCloud Director 組織仮想データセンターの外部にある DHCP サーバに DHCP メッセージをリレーできます。Edge Gateway の DHCP リレー機能を設定できます。

『NSX 管理ガイド』で説明するように、既存の IP アドレス セット、IP アドレスのブロック、ドメイン、またはこれらのすべての組み合わせを使用して、DHCP サーバを指定できます。DHCP メッセージは、指定した各 DHCP サーバにリレーされます。

少なくとも1つの DHCP リレー エージェントを設定する必要があります。DHCP リレー エージェントは、DHCP リクエストを外部 DHCP サーバにリレーする Edge ゲートウェイ上のインターフェイスです。

前提条件


IP セットを使用して DHCP サーバを指定する場合は、その IP セットを Edge Gateway がオブジェクトのグループ分けに使用できることを確認します。[ファイアウォール ルール](#)と [DHCP リレー設定で使用するための IP アドレス セットの作成](#)を参照してください。

手順

- 1 Edge Gateway サービスを開きます。
 - a [ネットワーク] > [エッジ] の順に選択します。
 - b 編集する Edge Gateway を選択し、[サービス] をクリックします。
- 2 [DHCP] - [リレー] の順に移動します。

- 3 画面に表示されるフィールドを使用して、IP アドレス、ドメイン名、または IP アドレス セットで DHCP サーバを指定します。

[追加] () ボタンを使用して、既存の IP セットから利用できる IP セットを選択します。

- 4 DHCP リレー エージェントを設定し、その設定を画面上のテーブルに追加するには、[追加] () ボタンをクリックし、vNIC とそのゲートウェイ IP アドレスを選択し、[保持] をクリックします。

デフォルトで、ゲートウェイ IP アドレスは選択されている vNIC のプライマリ アドレスと一致します。デフォルトを保持できるほか、その vNIC で代替アドレスを使用可能な場合にはそれを選択できます。

- 5 [変更を保存] をクリックします。

テナント ポータルを使用したネットワーク アドレス変換の管理

vCloud Director 環境の NSX ソフトウェアにより、Edge Gateway はネットワーク アドレス変換 (NAT) サービスを提供できます。この機能を使用すると、コスト上およびセキュリティ上の目的で、組織で使用するパブリック IP アドレスの数を減らすことができます。

Edge Gateway の NAT サービスは、プライベート ネットワークの仮想マシンまたは仮想マシンのグループにパブリック アドレスを割り当てる機能を提供します。組織仮想データセンター内でプライベート アドレス設定された仮想マシンで実行されているサービスへのアクセスを Edge Gateway が提供できるようにするには、Edge Gateway で NAT ルールを設定する必要があります。一般に、vCloud Director 環境の Edge Gateway 上のアップリンク インターフェイスに NAT サービスを関連付けて、組織仮想データセンター ネットワーク上のアドレスが外部ネットワークに公開されないようにします。

NAT サービスの設定は、送信元 NAT (SNAT) ルールと宛先 NAT (DNAT) ルールに分けられます。vCloud Director 環境の Edge Gateway で SNAT ルールまたは DNAT ルールを設定する場合は、常に組織仮想データセンターの観点からルールを設定します。具体的には、次のようにルールを設定することを意味します。

- SNAT：トラフィックは組織仮想データセンターの内部ネットワーク上の仮想マシン（送信元）からインターネットを経由して外部ネットワーク（宛先）に移動します。SNAT ルールでは、組織仮想データセンター ネットワークから外部ネットワークまたは別の組織仮想データセンター ネットワークに送信されるパケットのソース IP アドレスを変換します。
- DNAT：トラフィックはインターネット（送信元）から組織仮想データセンターの仮想マシン（宛先）に移動します。DNAT ルールでは、外部ネットワークまたは別の組織仮想データセンター ネットワークから送信されて組織仮想データセンター ネットワークで受信されるパケットの IP アドレスを変換し、オプションでそのポートを変換します。

組織仮想データセンター内にプライベート IP アドレス空間を作成するための NAT ルールを設定できます。この設定を使用すると、プライベート IP アドレス空間を 1 つの組織仮想データセンターから別の組織仮想データセンターに移植することができます。NAT ルールを設定すると、別の組織仮想データセンターで使ったプライベート IP アドレスと同じプライベート IP アドレスを組織仮想データセンターの仮想マシンで使用できます。

vCloud Director 環境の NAT ルール機能では、次の操作がサポートされます。

- プライベート IP アドレス空間内でのサブネットの作成
- Edge Gateway の複数のプライベート IP アドレス空間の作成

- 複数の Edge Gateway インターフェイスに対する複数の NAT ルールの設定

重要: Edge Gateway ネットワーク上の仮想マシンにアクセスできるようにするには、Edge Gateway でファイアウォール ルールと NAT ルールの両方を設定する必要があります。デフォルトでは、Edge Gateway は、Edge Gateway ネットワーク上の仮想マシンとのネットワーク トラフィックをすべて拒否するようにファイアウォール ルールを設定した状態でデプロイされます。また、デフォルトでは Edge Gateway の NAT は無効です。このため、Edge Gateway で NAT を設定しない限り、Edge Gateway は受信および送信トラフィックの IP アドレスを変換できません。NAT ルールの設定後、対応するトラフィックを許可するようにファイアウォール ルールを追加しない限り、ネットワーク上の仮想マシンへの ping は失敗します。

SNAT または DNAT ルールの追加

ソース IP アドレスをパブリックからプライベート IP アドレスへ、またはその逆方向へ変更するには、ソース NAT (SNAT) ルールを作成します。ターゲット IP アドレスをパブリックからプライベート IP アドレスへ、またはその逆方向へ変更するには、ターゲット NAT (DNAT) ルールを作成します。

NAT ルールを作成するときには、次の形式を使用して、元の IP アドレスと変換先の IP アドレスを指定できます。

- IP アドレス。たとえば、192.0.2.0 とします。
- IP アドレス範囲。たとえば、192.0.2.0-192.0.2.24 とします。
- IP アドレス/サブネット マスク。たとえば、192.0.2.0/24 とします。
- any

vCloud Director 環境の Edge Gateway で SNAT ルールまたは DNAT ルールを設定する場合は、常に組織仮想データセンターの観点からルールを設定します。SNAT ルールでは、組織仮想データセンター ネットワークから外部ネットワークまたは別の組織仮想データセンター ネットワークに送信されるパケットのソース IP アドレスを変換します。DNAT ルールでは、外部ネットワークまたは別の組織仮想データセンター ネットワークから送信されて組織仮想データセンター ネットワークで受信されるパケットの IP アドレスを変換し、オプションでそのポートを変換します。

前提条件

パブリック IP アドレスを、ルールを追加する NSX Data Center for vSphere Edge Gateway インターフェイスに追加しておく必要があります。DNAT ルールの場合、元の (パブリック) IP アドレスを Edge ゲートウェイ インターフェイスに追加しておく必要があります。SNAT ルールの場合、変換先の (パブリック) IP アドレスを Edge ゲートウェイ インターフェイスに追加しておく必要があります。

手順

- 1 Edge Gateway サービスを開きます。
 - a [ネットワーク] > [エッジ] の順に選択します。
 - b 編集する Edge Gateway を選択し、[サービス] をクリックします。
- 2 [NAT] をクリックして、[NAT ルール] 画面を表示します。
- 3 どのタイプの NAT ルールを作成しているかに応じて、[DNAT ルール] または [SNAT ルール] をクリックします。

4 ターゲット NAT ルール（外部から内部へ）を設定します。

オプション	説明
適用対象	ルールを適用するインターフェイスを選択します。
元の IP/範囲	必要な IP アドレスを入力します。 このアドレスは、DNAT ルールを設定する Edge ゲートウェイのパブリック IP アドレスにする必要があります。検査対象のパケットでは、この IP アドレスまたはアドレス範囲がパケットのターゲット IP アドレスとして表示されます。これらのパケット ターゲット アドレスは、この DNAT ルールによって変換されたものです。
プロトコル	ルールを適用するプロトコルを選択します。このルールをすべてのプロトコルに適用するには、[任意] を選択します。
元のポート	(オプション) 仮想マシンが接続されている内部ネットワークに接続するために Edge ゲートウェイで受信トラフィックが使用するポートまたはポート範囲を選択します。これは、[プロトコル] が [ICMP] または [任意] に設定されているときには選択できません。
ICMP タイプ	[プロトコル] に [ICMP] (デバイス間でエラー情報を通信するために使用されるエラー報告と診断のユーティリティ) を選択する場合は、ドロップダウン メニューから [ICMP タイプ] を選択します。 ICMP メッセージは、タイプのフィールドで識別されます。デフォルトで、[ICMP タイプ] は [任意] に設定されています。
変換された IP/範囲	着信パケット上のターゲット アドレスの変換先となる IP アドレスまたは IP アドレス範囲を入力します。 これらのアドレスは、外部ネットワークからトラフィックを受信できるように DNAT を設定している 1 台以上の仮想マシンの IP アドレスです。
変換されたポート	(オプション) 内部ネットワークの仮想マシン上で着信トラフィックが接続しているポートまたはポート範囲を選択します。仮想マシンに着信したパケットは、DNAT ルールによってこれらのポートに変換されます。
説明	(オプション) このルールで何を識別するのがわかるように説明を入力します。
有効	このルールを有効にするには、オンに切り替えます。
ログの有効化	このルールによって実行されたアドレス変換をログに記録するには、オンにします。

5 ソース NAT ルール（内部から外部へ）を設定します。

オプション	説明
適用対象	ルールを適用するインターフェイスを選択します。
元のソース IP/範囲	このルールに適用する元の IP アドレスまたは IP アドレス範囲を入力します。 これらのアドレスは、外部ネットワークにトラフィックを送信できるように SNAT ルールを設定している 1 台以上の仮想マシンの IP アドレスです。
変換されたソース IP/範囲	必要な IP アドレスを入力します。 このアドレスは、常に SNAT ルールを設定するゲートウェイのパブリック IP アドレスにする必要があります。外部ネットワークにトラフィックを送信するときに、発信パケット上のソース アドレス (仮想マシン) が変換される IP アドレスを指定します。
説明	(オプション) このルールで何を識別するのがわかるように説明を入力します。
有効	このルールを有効にするには、オンに切り替えます。
ログの有効化	このルールによって実行されたアドレス変換をログに記録するには、オンにします。

- 6 [保持] をクリックして、画面上のテーブルにルールを追加します。
- 7 設定するルールごとに、この手順を繰り返します。
- 8 [変更を保存] をクリックして、システムにルールを保存します。

次のステップ

設定した SNAT ルールまたは DNAT ルールに対応する Edge ゲートウェイ ファイアウォール ルールを追加します。 [NSX Data Center for vSphere Edge Gateway ファイアウォール ルールの追加](#) を参照してください。

高度なルーティングの設定

NSX ソフトウェアによって提供されるスタティック ルーティングおよび動的ルーティング機能を Edge Gateway に設定できます。

動的ルーティングを有効にするには、Border Gateway Protocol (BGP) または Open Shortest Path First (OSPF) プロトコルを使用して詳細 Edge ゲートウェイを設定します。

NSX が提供するルーティング機能の詳細については、『NSX 管理ガイド』の「ルーティング」を参照してください。

詳細 Edge ゲートウェイごとにスタティック ルーティングおよび動的ルーティングを指定できます。動的ルーティング機能は、レイヤー 2 ブロードキャスト ドメイン間で必要な転送情報を提供します。これにより、レイヤー 2 ブロードキャスト ドメインを削減し、ネットワークの効率を高め、規模を拡大することができます。NSX は、このインテリジェンスを East-West ルーティングのワークロードがある場所まで拡張します。この機能により、余分なコストや時間をかけずにホップを拡張して、仮想マシン間でより直接的な通信を実現できます。

NSX Data Center for vSphere Edge Gateway のデフォルトのルーティング設定の指定

Edge ゲートウェイに対して、スタティック ルーティングおよび動的ルーティングのデフォルト設定を指定できます。

注： 設定されているすべてのルーティング設定を削除するには、[ルーティング設定] 画面の下部にある [グローバル構成をクリア] ボタンを使用します。このアクションにより、デフォルトのルーティング設定、スタティック ルート、OSPF、BGP、ルート再配分の各サブ画面で現在指定されているすべてのルーティング設定が削除されます。

手順

- 1 Edge Gateway サービスを開きます。
 - a [ネットワーク] > [エッジ] の順に選択します。
 - b 編集する Edge Gateway を選択し、[サービス] をクリックします。
- 2 [ルーティング] - [ルーティング設定] の順に選択します。

- 3 この Edge ゲートウェイで等価コスト マルチパス (ECMP) ルーティングを有効にするには、[ECMP] 切り替えをオンにします。

『NSX 管理』ドキュメントで説明されているとおり、ECMP は、単一のターゲットへのネクスト ホップ パケット転送が複数のベスト パスで行われるようにするルーティング戦略です。NSX は、これらのベスト パスの決定を、統計に基づくか、設定済みのスタティック ルートを使用するか、または OSPF や BGP などの動的ルーティング プロトコルによるメトリック計算の結果として行います。[スタティック ルート] 画面で複数のネクスト ホップを指定することで、スタティック ルートに対する複数のパスを指定できます。

ECMP と NSX の詳細については、『NSX トラブルシューティング ガイド』のルーティングに関するトピックを参照してください。

- 4 デフォルトのルーティング ゲートウェイの設定を指定します。

- a [適用対象] ドロップ ダウン リストを使用して、ターゲット ネットワークに向かうネクスト ホップに到達できるインターフェイスを選択します。

選択したインターフェイスの詳細を表示するには、青い情報アイコンをクリックします。

- b ゲートウェイ IP アドレスを入力します。
- c MTU を入力します。
- d (オプション) オプションで、説明を入力します。
- e [変更を保存] をクリックします。

- 5 デフォルトの動的ルーティング設定を指定します。

注： 環境で IPsec VPN を設定してある場合は、動的ルーティングを使用しないでください。

- a ルーター ID を選択します。

リストからルーター ID を選択するか、[+] アイコンを使用して新しいルーター ID を入力します。このルーター ID は、動的ルーティングのためにルートをカーネルにプッシュする Edge ゲートウェイの最初のアップリンク IP アドレスになります。

- b [ログの有効化] 切り替えをオンにし、ログ レベルを選択することにより、ログ記録を設定します。
- c [OK] をクリックします。

- 6 [変更を保存] をクリックします。

次のステップ

スタティック ルートを追加します。[スタティック ルートの追加](#)を参照してください。

ルート再配分を設定します。[ルート再配分の設定](#)を参照してください。

動的ルーティングを設定します。次のトピックを参照してください。

- [BGP の設定](#)
- [OSPF の設定](#)

スタティック ルートの追加


宛先のサブネットまたはホストにスタティック ルートを追加できます。

デフォルトのルーティング設定で ECMP が有効になっている場合は、スタティック ルートに複数のネクスト ホップを指定できます。ECMP を有効にする手順については、[NSX Data Center for vSphere Edge Gateway のデフォルトのルーティング設定の指定](#)を参照してください。

前提条件

NSX のドキュメントで説明されているとおり、スタティック ルートのネクスト ホップ IP アドレスは、NSX Data Center for vSphere Edge Gateway のインターフェイスのいずれかに関連付けられているサブネット内に存在する必要があります。異なる場合、そのスタティック ルートの設定は失敗します。

手順

- 1 Edge Gateway サービスを開きます。
 - a [ネットワーク] > [エッジ] の順に選択します。
 - b 編集する Edge Gateway を選択し、[サービス] をクリックします。
- 2 [ルーティング] - [スタティック ルート] の順に移動します。
- 3 [作成] () ボタンをクリックします。
- 4 スタティック ルートの次のオプションを設定します。

オプション	説明
ネットワーク	ネットワークを CIDR 表記で入力します。
ネクスト ホップ	ネクスト ホップの IP アドレスを入力します。 ネクスト ホップ IP アドレスは、Edge Gateway のインターフェイスのいずれかに関連付けられているサブネット内に存在する必要があります。 ECMP が有効になっている場合は、複数のネクスト ホップを入力できます。
MTU	データ パケットの最大転送値を編集します。 MTU 値は、選択された Edge ゲートウェイ インターフェイスに設定された MTU 値を超える値にすることはできません。デフォルトでは、[ルーティング設定] 画面に、Edge ゲートウェイ インターフェイスで設定された MTU を表示できます。
インターフェイス	オプションで、スタティック ルートを追加する Edge ゲートウェイ インターフェイスを選択します。デフォルトで、ネクスト ホップのアドレスに一致するインターフェイスが選択されます。
説明	オプションで、スタティック ルートの説明を入力します。

- 5 [変更を保存] をクリックします。

次のステップ

スタティック ルートの NAT ルールを設定します。[SNAT または DNAT ルールの追加](#)を参照してください。

トラフィックがスタティック ルートを經由することを許可するファイアウォール ルールを追加します。[NSX Data Center for vSphere Edge Gateway ファイアウォール ルールの追加](#)を参照してください。

OSPF の設定

NSX Data Center for vSphere Edge Gateway の動的ルーティング機能を使用するように、Open Shortest Path First (OSPF) ルーティング プロトコルを設定できます。vCloud Director 環境に置かれた Edge ゲートウェイの OSPF は、一般に、vCloud Director の Edge ゲートウェイ間でルーティング情報を交換する目的に使用されます。

NSX Edge ゲートウェイがサポートする OSPF は、単一のルーティング ドメイン内のみで IP パケットをルーティングする Interior Gateway Protocol です。『NSX 管理ガイド』に記載されているように、NSX Edge Gateway に OSPF を設定すると、Edge Gateway はルートを学習して通知できるようになります。Edge ゲートウェイは OSPF を使用して、使用可能な Edge ゲートウェイからリンク状態に関する情報を収集し、ネットワークのトポロジ マッピングを構築します。このトポロジによって、インターネット レイヤーに提供されるルーティング テーブルが決まり、IP パケット内にあるターゲット IP アドレスに基づいてルーティングに関する決定が行われます。

その結果、OSPF ルーティング ポリシーはコストが等しいルート間でトラフィックのロード バランシングを動的に処理できるようになります。OSPF ネットワークは、トラフィック フローを最適化して、ルーティング テーブルのサイズを制限するために、複数のルーティング領域に分割されています。領域とは、同じ領域 ID を持つ OSPF ネットワーク、ルーター、およびリンクの論理的な集合のことです。領域は領域 ID で識別されます。

前提条件


ルーター ID を設定する必要があります。[NSX Data Center for vSphere Edge Gateway のデフォルトのルーティング設定の指定](#)。

手順

- 1 Edge Gateway サービスを開きます。
 - a [ネットワーク] > [エッジ] の順に選択します。
 - b 編集する Edge Gateway を選択し、[サービス] をクリックします。
- 2 [ルーティング] - [OSPF] の順に移動します。
- 3 OSPF が現在有効でない場合は、[OSPF の有効化] 切り替えを使用して、OSPF を有効にします。
- 4 組織のニーズに合わせて OSPF 設定を行います。

オプション	説明
グレースフル リスタートの有効化	OSPF サービスの再起動時にパケット転送が中断されないように指定します。
デフォルトの広告の有効化	Edge ゲートウェイが OSPF ピアに自分自身をデフォルト ゲートウェイとして通知できるようにします。


- 5 (オプション) [変更を保存] をクリックするか、または引き続き領域の定義やインターフェイス マッピングを設定することができます。

- 6 [追加] () ボタンをクリックし、OSPF エリア定義を追加します。ダイアログ ボックスでマッピングの詳細を指定し、[保持] をクリックします。

注： デフォルトでは、領域 ID が 51 の Not-So-Stubby Area (NSSA) が設定されます。この領域は OSPF 画面の領域定義テーブルに自動的に表示されます。NSSA 領域を変更または削除できます。

オプション	説明
領域 ID	領域 ID を IP アドレスまたは 10 進数の形式で入力します。
領域タイプ	<p>[標準] または [NSSA] を選択します。</p> <p>NSSA は、AS 外部の Link-State Advertisement (LSA) が NSSA に大量に送信されるのを防ぎます。NSSA は外部ターゲットへのデフォルト ルーティングを利用します。そのため、NSSA は OSPF ルーティング ドメインのエッジに配置する必要があります。NSSA は外部ルートを OSPF ルーティング ドメインにインポートできます。これにより、OSPF ルーティング ドメインに属さない小規模なルーティング ドメインにトランジット サービスを提供することができます。</p>
領域認証	<p>OSPF が領域レベルで実行する認証タイプを選択します。</p> <p>領域内のすべての Edge ゲートウェイに、同一の認証と対応するパスワードを設定しておく必要があります。MD5 認証を有効にするには、レシーバとトランスミッタの両方に同じ MD5 キーが必要です。</p> <p>選択肢は次のとおりです。</p> <ul style="list-style-type: none"> ■ [なし] <p>認証は不要です。</p> ■ [パスワード] <p>このオプションを選択した場合は、[領域認証値] フィールドで指定したパスワードが送信パケットに含まれます。</p> ■ [MD5] <p>このオプションを選択した場合、認証には MD5 (Message Digest type 5) 暗号化が使用されます。MD5 チェックサムが送信パケットに含まれます。[領域認証値] フィールドに MD5 キーを入力します。</p>

- 7 [変更を保存] をクリックして、インターフェイス マッピングを追加するときに、新たに設定した領域定義を選択できるようにします。

- 8 [追加] () ボタンをクリックし、インターフェイスのマッピングを追加します。ダイアログ ボックスでマッピングの詳細を指定し、[保持] をクリックします。

これらのマッピングによって、Edge Gateway のインターフェイスが領域にマップされます。

- a ダイアログ ボックスで、領域定義にマッピングするインターフェイスを選択します。

このインターフェイスによって、両方の Edge ゲートウェイの接続先となる外部ネットワークが指定されます。

- b 選択したインターフェイスにマッピングする領域の領域 ID を選択します。

- c (オプション) OSPF の設定をデフォルト値から変更し、このインターフェイスのマッピングに合わせてカスタマイズします。

新しいマッピングを設定するときには、これらの設定のデフォルト値が表示されます。通常は、デフォルト設定をそのまま使用することをお勧めします。設定を変更する場合は、OSPF ピアで同じ設定が使用されることを確認してください。

オプション	説明
Hello 間隔	インターフェイスに送信される Hello パケットの間隔 (秒) です。
Dead 間隔	少なくとも 1 つの Hello パケットをネイバーから受信してから、ネイバーが停止していると宣言されるまでの間隔 (秒) です。
優先度	インターフェイスの優先度です。優先順位が最高のインターフェイスが、Edge ゲートウェイ ルーターに指定されます。
コスト	該当するインターフェイスを越えてパケットを送信するために必要なオーバーヘッドです。インターフェイスのコストは、そのインターフェイスのバンド幅に反比例します。バンド幅が大きくなるほど、コストは小さくなります。

- d [保持] をクリックします。

9 OSPF 画面で [変更を保存] をクリックします。

次のステップ

ルーティング情報の交換相手となる他の Edge ゲートウェイで、OSPF を設定します。

OSPF 対応 Edge ゲートウェイ間のトラフィックを許可するファイアウォール ルールを追加します。[NSX Data Center for vSphere Edge Gateway ファイアウォール ルールの追加](#)を参照してください。

ルートの再分散およびファイアウォール設定を使用して正しいルートを通知できることを確認します。[ルート再配分の設定](#)を参照してください。

BGP の設定

NSX Data Center for vSphere Edge Gateway の動的ルーティング機能を使用するように Border Gateway Protocol (BGP) を設定できます。


『NSX 管理ガイド』に記載されているように、BGP は、複数の自律システム間のネットワーク到達可能性を指定する IP ネットワークまたはプレフィックスのテーブルを使用することでルーティングを決定します。ネットワークの分野では、BGP スピーカーという用語は、BGP を実行しているネットワーク デバイスを表します。2 つの BGP スピーカーが接続を確立してから、ルーティング情報が交換されます。BGP ネイバーという用語は、接続などを確立した BGP スピーカーを表します。接続を確立すると、デバイスはルートを交換して、テーブルを同期させます。各デバイスはキープ アライブ メッセージを送信して、この関係を維持します。

手順

- 1 Edge Gateway サービスを開きます。
 - a [ネットワーク] > [エッジ] の順に選択します。
 - b 編集する Edge Gateway を選択し、[サービス] をクリックします。

- 2 [ルーティング] - [BGP] の順に移動します。
- 3 BGP が現在有効でない場合は、[BGP の有効化] 切り替えを使用して、BGP を有効にします。
- 4 組織のニーズに応じて BGP 設定を行います。

オプション	説明
グレースフル リスタートの有効化	BGP サービスの再起動時にパケット転送が中断されないように指定します。
デフォルトの広告の有効化	Edge ゲートウェイが BGP ネイバーに自分自身をデフォルト ゲートウェイとして通知できるようにします。
ローカル AS	<p>必須項目です。プロトコルのローカルの自律システム (AS) 機能に使用するための AS ID 番号を指定します。指定する値は 1 ～ 65534 の数字で、グローバルで一意的な値にする必要があります。</p> <p>ローカル AS は、BGP の機能です。設定している Edge ゲートウェイにシステムからローカル AS 番号が割り当てられます。Edge ゲートウェイが他の自律システム内の BGP ネイバーとピアリングする場合は、この ID を通知します。ターゲットの最適パスの選択時、ルートが経由する自律システムのパスは、動的ルーティング アルゴリズムのメトリックの 1 つとして使用されます。</p>

- 5 [変更を保存] をクリックするか、BGP ルーティング ネイバーを引き続き設定することができます。
- 6 [追加] () ボタンをクリックし、BGP ネイバー設定を追加します。ダイアログ ボックスでネイバーの詳細を指定し、[保持] をクリックします。

オプション	説明
IP アドレス	この Edge ゲートウェイの BGP ネイバーの IP アドレスを入力します。
リモート AS	この BGP ネイバーが属している自律システムのグローバルに一意的な番号を 1 ～ 65534 の範囲内で入力します。このリモート AS の番号は、システムの BGP ネイバー テーブル内の BGP ネイバー エントリに使用されます。
ウェイト	ネイバー接続のデフォルトのウェイトです。組織の要求に合わせて調整します。
キープ アライブ時間	ソフトウェアがピアにキープ アライブ メッセージを送信する頻度です。デフォルトの頻度は 60 秒です。組織の要求に合わせて調整します。
ホールド ダウン時間	<p>ソフトウェアがキープ アライブ メッセージを受信しなくなってから、ピアが停止していると宣言するまでの間隔です。この間隔は、キープ アライブ間隔の 3 倍にする必要があります。デフォルトの間隔は 180 秒です。組織の要求に合わせて調整します。</p> <p>2 つの BGP ネイバー間でピアリングが確立されると、Edge ゲートウェイはホールド ダウン タイマーを開始します。Edge ゲートウェイがネイバーからキープ アライブ メッセージを受信するたびに、ホールド ダウン タイマーは 0 にリセットされます。Edge ゲートウェイがキープ アライブ メッセージの受信を 3 回連続で失敗し、ホールド ダウン タイマーがキープ アライブ間隔の 3 倍に到達すると、Edge ゲートウェイはネイバーが停止していると見なし、このネイバーからルートを削除します。</p>

オプション	説明
パスワード	<p>この BGP ネイバーが認証を必要としている場合は、認証パスワードを入力します。</p> <p>ネイバー間の接続で送信されるセグメントごとに検証が行われます。MD5 認証を設定するには、両方の BGP ネイバーで同じパスワードを設定する必要があります。使用しない場合、これらの間に接続が確立されません。</p>
BGP フィルタ	<p>このテーブルを使用して、この BGP ネイバーのプレフィックス リストを使用したルート フィルタリングを指定します。</p> <p>注意： フィルタの最後で、block all ルールが適用されます。</p> <p>[+] アイコンをクリックし、オプションを設定して、テーブルにフィルタを追加します。[保持] をクリックして、各フィルタを保存します。</p> <ul style="list-style-type: none"> ■ 方向を選択して、ネイバーへの受信トラフィックと送信トラフィックのいずれかをフィルタするかを指定します。 ■ アクションを選択して、トラフィックの許可または拒否のいずれかを指定します。 ■ ネイバーへの送受信をフィルタするネットワークを入力します。ANY を入力するか、またはネットワークを CIDR 形式で入力します。 ■ [IP プリフィックス GE] および [IP プリフィックス LE] に入力して、IP プリフィックス リストで le および ge キーワードを使用します。

7 [変更を保存] をクリックして、システムに設定を保存します。

次のステップ

ルーティング情報の交換相手となる他の Edge ゲートウェイで、BGP を設定します。

BGP が設定された Edge ゲートウェイへの送受信トラフィックを許可するファイアウォール ルールを追加します。詳細については、[NSX Data Center for vSphere Edge Gateway ファイアウォール ルールの追加](#)を参照してください。


ルート再配分の設定

デフォルトでは、ルーターは同じプロトコルを実行している他のルーターとのみルートを共有します。マルチプロトコル環境を設定した場合は、クロスプロトコル ルート共有を使用するようにルート再配分を設定する必要があります。ルート再配分は NSX Data Center for vSphere Edge Gateway に対して設定できます。

手順

- Edge Gateway サービスを開きます。
 - [ネットワーク] > [エッジ] の順に選択します。
 - 編集する Edge Gateway を選択し、[サービス] をクリックします。
- [ルーティング] - [ルートの再分散] に移動します。
- プロトコルの切り替えを使用して、ルートの再分散を有効にするプロトコルをオンにします。

4 画面上のテーブルに IP プリフィックスを追加します。

- a [追加] () ボタンをクリックします。
- b ネットワークの名前および IP アドレスを CIDR 形式で入力します。
- c [保持] をクリックします。

5 [追加] () ボタンをクリックして各 IP プリフィックスに再分散基準を指定します。ダイアログ ボックスで基準を指定し、[保持] をクリックします。

テーブル内のエントリは順番に処理されます。上下の矢印を使用して順番を調整します。

オプション	説明
プリフィックス名	特定の IP プリフィックスを選択してこの基準を適用するか、または [任意] を選択してすべてのネットワーク ルートに基準を適用します。
学習者プロトコル	この再分散基準で他のプロトコルからルートを学習するプロトコルを選択します。
次からの学習を許可	[学習者プロトコル] リストで選択したプロトコルでルートを学習できるネットワークのタイプを選択します。
アクション	選択したネットワーク タイプからの再分散の許可または拒否のいずれかを選択します。

6 [変更を保存] をクリックします。

ロード バランシング

ロード バランサーは、ユーザーに対してロードの分散が透過的に行われるように、受信サービス リクエストを複数のサーバに均等に分散します。ロード バランシングは、最適なリソース使用率の達成、スループットの最大化、応答時間の最小化、過負荷の回避に役立ちます。

ロード バランシングについて

NSX ロード バランサーは、2 つのロード バランシング エンジンをサポートします。レイヤー 4 ロード バランサーはパケット ベースであり、高速パス処理を提供します。レイヤー 7 ロード バランサーはソケット ベースであり、パケット エンド サービスの高度なトラフィック管理戦略と DDOS 緩和をサポートします。

Edge Gateway は外部ネットワークからの受信トラフィックのロード バランシングを行うため、Edge Gateway のロード バランシングを外部インターフェイスで設定します。ロード バランシング用の仮想サーバを構成する場合、組織仮想データセンターにある使用可能な IP アドレスのいずれかを指定します。

ロード バランシングの戦略と概念

パケット ベースのロード バランシング戦略は TCP および UDP レイヤーに実装されます。パケット ベースのロード バランシングでは、接続の停止または要求全体のバッファリングを行いません。代わりに、パケットの操作後に、選択したサーバに直接パケットを送信します。1 つのセッションのパケットが同じサーバに送信されるように TCP および UDP セッションはロード バランサー内で維持されます。グローバル構成および関連する仮想サーバ構成の両方で [アクセラレーションが有効] を選択し、パケット ベースのロード バランシングを有効にできます。

ソケット ベースのロード バランシング戦略はソケット インターフェイス上に実装されます。1つの要求に対してクライアント側の接続とサーバ側の接続の2つの接続が確立されます。サーバ側の接続は、サーバの選択後に確立されます。HTTP ソケット ベースの実装の場合、要求全体を受信した後、オプションの L7 操作によって選択されたサーバに要求を送信します。HTTPS ソケット ベースの実装の場合、クライアント側の接続またはサーバ側の接続のいずれかで認証情報を交換します。ソケット ベースのロード バランシングは、TCP、HTTP、および HTTPS 仮想サーバのデフォルト モードです。

NSX ロード バランサーの主な概念は、仮想サーバ、サーバ プール、サーバ プール メンバー、およびサービス監視です。

仮想サーバ

アプリケーション サービスの抽象概念。IP アドレス、ポート、プロトコル、およびアプリケーション プロファイル (TCP、UDP など) の一意の組み合わせで表されます。

サーバ プール

バックエンド サーバのグループ。

サーバ プール メンバー

バックエンド サーバをプール内のメンバーとして表します。

サービス モニター

バックエンド サーバの健全性ステータスを調べる方法を定義します。

アプリケーション プロファイル

特定のアプリケーションの TCP、UDP、永続性、および証明書設定を表します。

設定の概要

最初に、ロード バランサーのグローバル オプションを設定します。バックエンド サーバ メンバーで構成されるサーバ プールを作成し、サービス モニターをプールに関連付けて、バックエンド サーバを効率的に管理および共有します。

次に、アプリケーション プロファイルを作成し、クライアント SSL、サーバ SSL、X-Forwarded-For、永続性など、ロード バランサーでアプリケーションの共通の動作を定義します。永続性では、同様の特性 (送信元の IP アドレスまたは Cookie を同じプール メンバーに送信する必要があるなど) を持つ後続の要求が、ロード バランシング アルゴリズムを実行せずに送信されます。アプリケーション プロファイルは、仮想サーバ全体で再利用できます。

オプションのアプリケーション ルールを作成し、トラフィックの操作に関するアプリケーション固有の設定を行います。たとえば、特定の URL またはホスト名と照合し、異なる要求を異なるプールで処理できるようにします。次に、アプリケーションに固有のサービス モニターを作成します。既存のサービス モニターがニーズを満たしている場合はそのサービス モニターを使用することもできます。

必要に応じて、L7 仮想サーバの高度な機能をサポートするアプリケーション ルールを作成できます。アプリケーション ルールの使用事例として、コンテンツの切り替え、ヘッダーの操作、セキュリティ ルール、DOS 保護があります。

最後に、サーバ プール、アプリケーション プロファイル、およびあらゆるアプリケーション ルールをまとめて接続する仮想サーバを作成します。

仮想サーバが要求を受信すると、ロード バランシング アルゴリズムはプール メンバーの設定とランタイム ステータスを考慮します。次に、アルゴリズムは、1 つ以上のメンバーで構成される、トラフィックを分散するための適切なプールを計算します。プール メンバーの設定には、ウェイト、最大接続、および状態ステータスなどの設定が含まれます。ランタイム ステータスには、現在の接続、応答時間、および健全性チェックのステータス情報が含まれます。計算方法として、ラウンドロビン、重み付きラウンドロビン、最小接続、送信元 IP アドレス ハッシュ、重み付き最小接続、URL、URI、または HTTP ヘッダーを使用できます。

各プールは、関連付けられたサービス モニターで監視されます。ロード バランサーがプール メンバーの問題を検出すると、メンバーは DOWN としてマークされます。サーバ プールからサーバを選択するときは、UP のサーバのみが選択されます。サーバ プールがサービス モニターと共に構成されていない場合、すべてのプール メンバーが UP とみなされます。

ロード バランサー サービスの設定

ロード バランサーのグローバル設定パラメータには、全体の有効化、レイヤー 4 エンジンまたはレイヤー 7 エンジンの選択、およびログに記録するイベント タイプの仕様などがあります。

手順

- 1 Edge Gateway サービスを開きます。
 - a [ネットワーク] > [エッジ] の順に選択します。
 - b 編集する Edge Gateway を選択し、[サービス] をクリックします。
- 2 [ロード バランサー] > [グローバル構成] の順に移動します。
- 3 有効にするオプションを選択します。

オプション	アクション
ステータス	<p>切り替えアイコンをクリックして、ロード バランサーを有効にします。</p> <p>[アクセラレーションが有効] を有効にして、L7 エンジンではなく、より高速な L4 エンジンを使用するようにロード バランサーを設定します。L4 TCP VIP は Edge ゲートウェイのファイアウォールの前に処理されるため、[許可] ファイアウォール ルールは必要ありません。</p> <p>注： HTTP および HTTPS 用の L7 VIP はファイアウォールの後に処理されるため、アクセラレーションが有効でない場合は、これらのプロトコルについて、L7 VIP へのアクセスを許可するための Edge ゲートウェイファイアウォール ルールが必要です。アクセラレーションが有効であり、サーバ プールが非透過モードの場合は、SNAT ルールが追加されるため、Edge ゲートウェイでファイアウォールを有効であることを確認する必要があります。</p>
ログの有効化	Edge ゲートウェイのロード バランサーでトラフィック ログを収集するように、ログを有効にします。
ログ レベル	ログに収集するイベントの重要度を選択します。

- 4 [変更を保存] をクリックします。
- 保存操作が完了するまでに 1 分ほどかかることがあります。

次のステップ

ロード バランサーのアプリケーション プロファイルを設定します。[アプリケーション プロファイルの作成](#)を参照してください。


アプリケーション プロファイルの作成

アプリケーション プロファイルは、特定のタイプのネットワーク トラフィックに関するロード バランサーの動作を定義します。プロファイルを設定したら、仮想サーバに関連付けます。関連付けられた仮想サーバは、プロファイルに指定した値に基づいてトラフィックを処理します。プロファイルを使用すると、ネットワーク トラフィックの管理機能を強化し、トラフィック管理タスクをより簡単に、効率的に行うことができます。

HTTPS トラフィックのプロファイルを作成するときは、次の HTTPS トラフィック パターンを使用できます。

- クライアント -> HTTPS -> LB (SSL を終了) -> HTTP -> サーバ
- クライアント -> HTTPS -> LB (SSL を終了) -> HTTPS -> サーバ
- クライアント -> HTTPS -> LB (SSL パススルー) -> HTTPS -> サーバ
- クライアント -> HTTP -> LB-> HTTP -> サーバ

手順

- 1 Edge Gateway サービスを開きます。
 - a [ネットワーク] > [エッジ] の順に選択します。
 - b 編集する Edge Gateway を選択し、[サービス] をクリックします。
- 2 [ロード バランサー] > [アプリケーション プロファイル] の順に移動します。
- 3 [作成] () ボタンをクリックします。
- 4 プロファイルの名前を入力します。
- 5 アプリケーション プロファイルを設定します。

オプション	説明
タイプ	サーバに要求を送信するためのプロトコルの種類を選択します。必須パラメータのリストは、選択したプロトコルによって変わります。選択したプロトコルに当てはまらないパラメータは入力できません。その他のパラメータはすべて必須です。
SSL パススルーの有効化	クリックすると、仮想サーバに対し、SSL 認証のパススルーが有効になります。 それ以外の場合は、ターゲット アドレスで SSL 認証が実行されます。
HTTP リダイレクト URL	(HTTP および HTTPS) ターゲット アドレスに届いたトラフィックのリダイレクト先 URL を入力します。

オプション	説明
永続性	<p>プロファイルの永続性メカニズムを指定します。</p> <p>永続性により、セッション データ（クライアント要求を処理した特定のプール メンバーなど）が追跡および格納されます。その結果、セッション中または後続のセッション中、クライアント要求は同じプール メンバーに転送されます。次のオプションがあります。</p> <ul style="list-style-type: none"> ■ [ソース IP] <p>ソース IP パーシステンスは、ソース IP アドレスに基づいてセッションを追跡します。ソース アドレスのアフィニティの永続性をサポートする仮想サーバへの接続をクライアントが要求すると、ロード バランサーはそのクライアントの過去の接続を確認し、過去の接続が見つかりそのクライアントを同じプール メンバーに返します。</p> ■ [MSRDP] <p>(TCP のみ) Microsoft Remote Desktop Protocol (MSRDP) パーシステンスは、Microsoft Remote Desktop Protocol (RDP) サービスを実行する Windows クライアントと Windows サーバ間の永続性セッションを維持します。MSRDP による永続性を有効にする推奨シナリオは、Windows Server ゲスト OS を実行中のメンバーで構成するロード バランシング プールを作成し、すべてのメンバーが Windows クラスタに属し、Windows セッション ディレクトリに参加するようにすることです。</p> ■ [SSL セッション ID] <p>SSL パススルーを有効にすると、SSL セッション ID の永続性が使用可能になります。SSL セッション ID の永続性を使用すると、同じクライアントからの繰り返し接続が同じサーバに送信されます。セッション ID の永続性により、SSL セッションのレジュームを使用できるため、クライアントとサーバの両方の処理時間を節約できます。</p>
Cookie 名	<p>(HTTP および HTTPS) 永続性メカニズムとして [Cookie] を指定した場合は、Cookie 名を入力します。[Cookie] は、Cookie を使用して、クライアントが最初にサイトにアクセスするときのセッションを一意に識別します。ロード バランサーは、セッションで後続の要求を接続するときに、この Cookie を参照してすべての要求を同じ仮想サーバに送ります。</p>
モード	<p>Cookie の挿入に使用するモードを選択します。次のモードがサポートされています。</p> <ul style="list-style-type: none"> ■ [挿入] <p>Edge ゲートウェイが Cookie を送信します。サーバが 1 つ以上の Cookie を送信すると、クライアントはもう 1 つ Cookie を受信します（サーバの Cookie と Edge ゲートウェイの Cookie）。サーバが Cookie を送信しない場合、クライアントは Edge ゲートウェイの Cookie のみを受信します。</p> ■ [プレフィックス] <p>クライアントが複数の Cookie をサポートしていない場合は、このオプションを選択します。</p> <p>注： すべてのブラウザは、複数の Cookie を受け付けます。ただし、1 つの Cookie のみをサポートする専用クライアントを使用した専用アプリケーションを使用している場合があります。その場合、Web サーバは Cookie を通常通り送信します。Edge ゲートウェイは、その Cookie 情報を（プレフィックスとして）サーバの Cookie 値に挿入します。この Cookie が追加された情報は、Edge ゲートウェイがサーバに送信したときに削除されます。</p> ■ [アプリケーション セッション] このオプションでは、サーバは Cookie を送信しません。代わりに、ユーザー セッション情報を URL として送信します。たとえば、<code>http://example.com/admin/UpdateUserServlet;jsessionid=OI24B9ASD7BSSD</code> の場合、<code>jsessionid</code> がユーザー セッション情報で、永続性のために使用されています。トラブルシューティングのためにアプリケーション セッションの永続性テーブルを見ることはできません。

オプション	説明
有効期限 (秒)	<p>永続性の有効期間を秒単位で入力します。1 ~ 86,400 の正の整数を指定します。</p> <p>注： TCP でソース IP アドレスによる永続性を使用する L7 ロード バランシングでは、一定期間に新規の TCP 接続がない場合、接続が継続中であっても永続性エントリがタイムアウトになります。</p>
X-Forwarded-For HTTP ヘッダーの挿入	<p>(HTTP および HTTPS) ロード バランサーを介して Web サーバに接続するクライアントの送信元 IP アドレスを識別するには、[X-Forwarded-For HTTP ヘッダーの挿入] を選択します。</p> <p>注： SSL バススルーを有効にした場合、このヘッダーの使用はサポートされません。</p>
プール側の SSL の有効化	<p>(HTTPS のみ) サーバ側からのロード バランサーの認証に使用する証明書、CA、または CRL を定義するには、[プール証明書] タブの [プール側の SSL の有効化] を選択します。</p>

- 6 (HTTPS のみ) アプリケーション プロファイルで使用する証明書を構成します。必要な証明書がない場合は、[証明書] タブから作成できます。

オプション	説明
仮想サーバ証明書	HTTPS トラフィックの復号化に使用する証明書、CA、または CRL を選択します。
プール証明書	<p>サーバ側からのロード バランサーの認証に使用する証明書、CA、または CRL を定義します。</p> <p>注： このタブを有効にするには、[プール側の SSL の有効化] を選択します。</p>
暗号	SSL/TLS ハンドシェイク時にネゴシエートされる暗号アルゴリズム (または暗号スイート) を選択します。
クライアント認証	<p>クライアント認証を無視するか、必須にするかどうかを指定します。</p> <p>注： [必須] に設定すると、クライアントは、要求またはハンドシェイクがキャンセルされた後、証明書を提供する必要があります。</p>

- 7 変更内容を維持するには、[保持] をクリックします。

この操作は完了するまでに 1 分かかることがあります。

次のステップ

さまざまなタイプのネットワーク トラフィックの健全性チェックを定義するには、ロード バランサーのサービス監視を追加します。[サービス監視の作成](#)を参照してください。

サービス監視の作成

特定のタイプのネットワーク トラフィックの健全性チェック パラメータを定義するには、サービス監視を作成します。サービス監視をプールに関連付けると、サービス監視パラメータに基づいてプール メンバーが監視されます。

手順

- Edge Gateway サービスを開きます。
 - [ネットワーク] > [エッジ] の順に選択します。
 - 編集する Edge Gateway を選択し、[サービス] をクリックします。

2 [ロード バランサー] > [サービス監視] の順に移動します。

3 [作成] () ボタンをクリックします。

4 サービス監視の名前を入力します。

5 (オプション) サービス監視に関する次のオプションを設定します。

オプション	説明
間隔	指定した [メソッド] を使用してサーバが監視する間隔を入力します。
タイムアウト	サーバからの応答を受信する必要がある期間の最大値 (秒) を入力します。
最大試行回数	指定した監視の [メソッド] が連続して失敗できる回数を入力します。この回数を超えるとサーバは停止状態と判断されます。
タイプ	健全性チェック要求をサーバに送信する方法 (HTTP、HTTPS、TCP、ICMP、または UDP) を選択します。 選択したタイプに応じて、[新規サービス監視] ダイアログの他のオプションが有効または無効になります。
予測	(HTTP および HTTPS) 監視が HTTP または HTTPS 応答のステータス行で照合する文字列を入力します (HTTP/1.1 など)。
メソッド	(HTTP および HTTPS) サーバ ステータスの検出に使用するメソッドを選択します。
URL	(HTTP および HTTPS) サーバ ステータス要求で使用する URL を入力します。 注: メソッドとして POST を選択した場合は、[送信] の値を指定する必要があります。
送信	(HTTP、HTTPS、UDP) 送信するデータを入力します。
受信	(HTTP、HTTPS、および UDP) 応答コンテンツで照合する文字列を入力します。 注: [予測] が一致しない場合、監視は [受信] のコンテンツを照合しません。
拡張	(すべて) サービス監視の詳細パラメータをキーと値のペアで入力します。たとえば、「warning=10」は、10 秒以内にサーバが応答しない場合に、そのステータスを警告に設定することを示します。拡張項目はすべて、キャリッジ リターン文字で区切る必要があります。以下にその例を挙げます。 <pre><extension>delay=2 critical=3 escape</extension></pre>

6 変更内容を維持するには、[保持] をクリックします。

この操作は完了するまでに 1 分かかることがあります。

例：各プロトコルでサポートされる拡張機能

表 6-1. HTTP/HTTPS プロトコルの拡張機能

監視の拡張機能	説明
no-body	ドキュメントの本文を待たずに、HTTP/HTTPS ヘッダーの後で読み取りを停止します。 注： HTTP GET または HTTP POST は送信されますが、HEAD メソッドは送信されません。
max-age=SECONDS	ドキュメントが SECONDS より古い場合は警告します。数値は、分の場合は 10m、時間の場合は 10h、日の場合は 10d の形式で指定します。
content-type=STRING	POST 呼び出しでの Content-Type ヘッダーのメディア タイプを指定します。
linespan	正規表現で改行記号を許可します (-r または R より前に指定する必要があります)。
regex=STRING または ereg=STRING	正規表現の STRING をページで検索します。
eregi=STRING	大文字小文字を区別して正規表現の STRING をページで検索します。
invert-regex	見つかった場合は CRITICAL、見つからなかった場合は OK を返します。
proxy-authorization=AUTH_PAIR	基本認証を使用するプロキシ サーバのユーザー名とパスワード (username:password) を指定します。
useragent=STRING	HTTP ヘッダーの文字列を User Agent として送信します。
header=STRING	HTTP ヘッダー内のその他のタグを送信します。追加のヘッダーで複数回使用できます。
onredirect=ok warning critical follow sticky stickyport	リダイレクト ページの処理方法を示します。 sticky は follow に似ていますが、指定した IP アドレスと連携します。stickyport は、ポートが同じであることを確認します。
pagesize=INTEGER:INTEGER	必要なページ サイズの最小値と最大値をバイト単位で指定します。
warning=DOUBLE	警告ステータスになる応答時間を秒単位で指定します。
critical=DOUBLE	重大ステータスになる応答時間を秒単位で指定します。

表 6-2. HTTPS プロトコルのみを対象とした拡張機能

監視の拡張機能	説明
sni	SSL/TLS のホスト名拡張機能のサポート (SNI) を有効にします。
certificate=[INTEGER]	証明書の最低有効日数を指定します。ポートのデフォルト値は 443 です。このオプションを使用すると、URL はチェックされません。
authorization=AUTH_PAIR	基本認証を使用するサイトのユーザー名とパスワード (username:password) を指定します。

表 6-3. TCP プロトコルの拡張機能

監視の拡張機能	説明
escape	send または quit 文字列で、\n、\r、\t、または \ の使用を許可します。send または quit オプションの前に指定する必要があります。デフォルトでは、send には何も追加されず、quit の最後には \r\n が追加されます。
all	すべての expect 文字列がサーバ応答に含まれている必要があることを指定します。デフォルトでは、any が使用されます。
quit=STRING	接続を正常に終了するため、サーバに文字列を送信します。
refuse=ok warn crit	ok、warn、または crit の状態で TCP 拒否を受け入れます。デフォルトでは、crit の状態を使用します。
mismatch=ok warn crit	ok、warn、または crit の状態で、想定される文字列の不一致を受け入れます。デフォルトでは、warn の状態を使用します。
jail	TCP ソケットからの出力を非表示にします。
maxbytes=INTEGER	指定数より多いバイト数を受信すると、接続を閉じます。
delay=INTEGER	文字列の送信から応答のポーリングまで、指定秒数を待機します。
certificate=INTEGER[,INTEGER]	証明書の最低有効日数を指定します。最初の値は警告まで、2 番目の値は重大までの #days です（指定されない場合は 0）。
ssl	接続に SSL を使用します。
warning=DOUBLE	警告ステータスになる応答時間を秒単位で指定します。
critical=DOUBLE	重大ステータスになる応答時間を秒単位で指定します。


次のステップ

ロード バランサーのサーバ プールを追加します。[ロード バランシングのサーバ プールの追加](#)を参照してください。

ロード バランシングのサーバ プールの追加

バックエンド サーバを柔軟かつ効率的に管理および共有するために、サーバ プールを追加できます。プールはロード バランサーの分散メソッドを管理し、健全性チェック パラメータのためにサービス モニターが接続されています。

手順

- Edge Gateway サービスを開きます。
 - [ネットワーク] > [エッジ] の順に選択します。
 - 編集する Edge Gateway を選択し、[サービス] をクリックします。
- [ロード バランサー] > [プール] の順に移動します。
- [作成] () ボタンをクリックします。
- ロード バランサー プールの名前と、必要に応じて説明を入力します。

5 [アルゴリズム] ドロップダウン メニューから、サービスのバランシング メソッドを選択します。

オプション	説明
ROUND_ROBIN	各サーバーは、割り当てられたウェイトに従って、順に使用されます。これは、サーバーの処理時間が等しく分散されたままである場合に、最もスムーズで公平なアルゴリズムです。
IP_HASH	各バケットのソースおよびターゲット IP アドレスのハッシュに基づいてサーバーを選択します。
LEASTCONN	クライアントの要求を、サーバー上の既存の接続数に基づいて複数のサーバーに分散させます。新しい接続は、オープン接続数が最も少ないサーバーに送信されます。
URI	URI の左側の部分（クエスチョン マークの前）は、ハッシュされ、実行中のサーバーの全体のウェイトで割られます。その結果により、要求を受け取るサーバーが指定されます。このオプションにより、サーバーが停止しない限り、URI は必ず同じサーバーに転送されます。
HTTPHEADER	HTTP ヘッダー名が各 HTTP 要求で検索されます。カッコで囲まれているヘッダー名は大文字小文字が区別されません。これは ACL 'hdr()' 関数と同様です。ヘッダーが存在しないか、どの値も含まれていない場合には、ラウンド ロビン アルゴリズムが適用されます。HTTP HEADER アルゴリズム パラメータには、1 つのオプション <code>headerName=<name></code> があります。たとえば、HTTP HEADER アルゴリズム パラメータとして host を使用できます。
URL	引数で指定した URL パラメータが、各 HTTP GET 要求のクエリ文字列内で検索されます。パラメータに等号 (=) と値が続く場合、値はハッシュされ、実行中のサーバーの重みの合計で除算されます。結果により、要求を受信するサーバーが指定されます。このプロセスを使用して要求内のユーザー ID を追跡し、サーバーが起動したり停止したりしない限り、同じユーザー ID が常に同じサーバーに確実に送信されるようにします。値またはパラメータが見つからない場合、ラウンド ロビン アルゴリズムが適用されます。URL アルゴリズム パラメータには、1 つのオプション <code>urlParam=<url></code> があります。

6 メンバーをプールに追加します。

a [追加] () ボタンをクリックします。

b プール メンバーの名前を入力します。

c プール メンバーの IP アドレスを入力します。

d メンバーがロード バランサーからトラフィックを受信するポートを入力します。

e メンバーが健全性モニターの要求を受信する監視ポートを入力します。

f [ウェイト] テキスト ボックスに、このメンバーが処理するトラフィックの割合を入力します。1 ～ 256 の範囲の整数にする必要があります。

g (オプション) [最大接続数] テキスト ボックスに、メンバーが処理できる同時接続の最大数を入力します。
受信要求の数が最大を超えた場合、要求はキューに入れられ、ロード バランサーは接続が解放されるのを待機します。

h (オプション) [最小接続数] テキスト ボックスに、メンバーが必ず受け入れなければならない同時接続数の最小数を入力します。

i [保持] をクリックして、新しいメンバーをプールに追加します。

この操作は完了するまでに 1 分かかることがあります。

- 7 (オプション) クライアント IP アドレスをバックエンド サーバに表示するには、[透過的] を選択します。

[透過的] が選択されていない場合 (デフォルト値)、バックエンド サーバは、ロード バランサーの内部 IP アドレスとして、トラフィック ソースの IP アドレスを参照します。

[透過的] が選択されている場合、ソース IP アドレスは、クライアントの実際の IP アドレスであり、Edge ゲートウェイをデフォルト ゲートウェイとして設定し、戻りパケットが Edge ゲートウェイを確実に経由するようにします。

- 8 変更内容を維持するには、[保持] をクリックします。

この操作は完了するまでに 1 分かかることがあります。

次のステップ

ロード バランサーの仮想サーバを追加します。仮想サーバには公開 IP アドレスがあり、すべての受信クライアント要求を処理します。 [仮想サーバの追加](#) を参照してください。

アプリケーション ルールの追加

アプリケーション ルールを作成して、IP アプリケーション トラフィックの操作と管理を直接行うことができます。

手順

- 1 Edge Gateway サービスを開きます。
 - a [ネットワーク] > [エッジ] の順に選択します。
 - b 編集する Edge Gateway を選択し、[サービス] をクリックします。
- 2 [ロード バランサー] > [アプリケーション ルール] の順に移動します。

- 3 [追加] () ボタンをクリックします。

- 4 アプリケーション ルールの名前を入力します。
- 5 アプリケーション ルールのスクリプトを入力します。

アプリケーション ルールの構文については、<http://cbonte.github.io/haproxy-dconv/configuration-1.5.html> を参照してください。

- 6 変更内容を維持するには、[保持] をクリックします。

この操作は完了するまでに 1 分かかることがあります。

次のステップ


ロード バランサーに追加する仮想サーバに新しいアプリケーション ルールを関連付けます。 [仮想サーバの追加](#) を参照してください。

仮想サーバの追加


仮想サーバとして NSX Data Center for vSphere Edge Gateway 内部インターフェイスまたはアップリンク インターフェイスを追加します。仮想サーバには公開 IP アドレスがあり、すべての受信クライアント要求を処理します。

デフォルトでは、ロード バランサーは、各クライアント要求の後にサーバ TCP 接続を閉じます。

手順

- 1 Edge Gateway サービスを開きます。
 - a [ネットワーク] > [エッジ] の順に選択します。
 - b 編集する Edge Gateway を選択し、[サービス] をクリックします。
- 2 [ロード バランサー] > [仮想サーバ] の順に移動します。
- 3 [追加] () ボタンをクリックします。
- 4 [全般] タブで、仮想サーバの次のオプションを設定します。

オプション	説明
仮想サーバの有効化	クリックして、仮想サーバを有効にします。
アクセラレーションの有効化	クリックしてアクセラレーションを有効にします。
アプリケーション プロファイル	仮想サーバに関連付けるアプリケーション プロファイルを選択します。
名前	仮想サーバの名前を入力します。
説明	必要に応じて仮想サーバの説明を入力します。
IP アドレス	ロード バランサーがリスンする IP アドレスを入力するか、参照して選択します。
プロトコル	仮想サーバが受け入れるプロトコルを選択します。選択した [アプリケーション プロファイル] により使用されるものと同じプロトコルを選択する必要があります。
ポート	ロード バランサーが待機するポート番号を入力します。
デフォルトのプール	ロード バランサーが使用するサーバ プールを選択します。
接続制限	(オプション) 仮想サーバが処理できる最大同時接続数を入力します。
接続速度の制限 (CPS)	(オプション) 1 秒あたり最大の受信新規接続要求を入力します。

- 5 (オプション) アプリケーション ルールを仮想サーバに関連付けるために、[詳細] タブをクリックし、次の手順を実行します。
 - a [追加] () ボタンをクリックします。
 ロード バランサー用に作成されたアプリケーション ルールが表示されます。必要に応じて、ロード バランサーのアプリケーション ルールを追加します。 [アプリケーション ルールの追加](#)を参照してください。
- 6 変更内容を維持するには、[保持] をクリックします。
 この操作は完了するまでに 1 分かかることがあります。

次のステップ

新しい仮想サーバ (ターゲット IP アドレス) へのトラフィックを許可する、Edge ゲートウェイ ファイアウォール ルールを作成します。 [NSX Data Center for vSphere Edge Gateway ファイアウォール ルールの追加](#)を参照してください。

仮想プライベート ネットワークを使用したセキュアなアクセス

Edge Gateway の NSX ソフトウェアによって提供される VPN 機能を設定できます。組織仮想データセンターに VPN 接続を設定する際は、SSL VPN-Plus トンネル、IPsec VPN トンネル、または L2 VPN トンネルを使用します。

『NSX 管理ガイド』で説明されているように、NSX Edge ゲートウェイは以下の VPN サービスをサポートしています。

- SSL VPN Plus。リモート ユーザーがプライベートの企業アプリケーションにアクセスできます。
- IPsec VPN。NSX Edge ゲートウェイと、同じく NSX を備えているサードパーティ製ハードウェア ルーターまたは VPN ゲートウェイを備えているリモート サイトとの間に、サイト間接続を提供します。
- L2 VPN。仮想マシンが地理的境界を越えて同じ IP アドレスを維持しながらネットワーク接続を保持できるよう許可することにより、組織仮想データセンターの拡張を実現します。

vCloud Director 環境では、以下の組み合わせの間に VPN トンネルを作成できます。

- 同じ組織内の組織仮想データセンター ネットワーク
- 異なる組織内の組織仮想データセンター ネットワーク
- 組織仮想データセンター ネットワークと外部ネットワーク

注： vCloud Director は、2 つの同じ Edge ゲートウェイ間の複数の VPN トンネルをサポートしていません。2 つの Edge ゲートウェイ間に既存のトンネルがあり、そのトンネルに別のサブネットを追加する場合は、既存の VPN トンネルを削除して、新しいサブネットを含む新しい VPN トンネルを作成してください。

Edge Gateway の VPN トンネルを構成した後は、リモートの場所から VPN クライアントを使用して、その Edge Gateway によってバックアップされている組織仮想データセンターに接続できます。

SSL VPN-Plus の設定

vCloud Director 環境の Edge Gateway に SSL VPN-Plus サービスを使用すると、リモート ユーザーはこの Edge Gateway でバックアップされている組織仮想データセンター内のプライベート ネットワークおよびアプリケーションに安全に接続できるようになります。Edge Gateway にさまざまな SSL VPN-Plus サービスを設定できます。

vCloud Director 環境の場合は、Edge Gateway の SSL VPN-Plus 機能によってネットワーク アクセス モードがサポートされます。リモート ユーザーが安全に接続して、Edge ゲートウェイの背後にあるネットワークおよびアプリケーションにアクセスできるようにするには、SSL クライアントをインストールする必要があります。Edge Gateway の SSL VPN-Plus 設定の一部として、オペレーティング システムに対応したインストール パッケージを追加し、特定のパラメータを設定します。詳細については、[SSL VPN-Plus クライアントのインストール パッケージの追加](#)を参照してください。

Edge ゲートウェイで SSL VPN-Plus を設定するには、複数の手順を実行します。

前提条件

SSL VPN-Plus に必要なすべての SSL 証明書が、[証明書] 画面に追加されていることを確認します。[SSL 証明書の管理](#)を参照してください。

注： Edge ゲートウェイで HTTPS に使用されるデフォルト ポートは、ポート 443 です。SSL VPN 機能を使用するには、Edge Gateway の HTTPS ポートに外部ネットワークからアクセスできる必要があります。SSL VPN クライアントが機能するには、[SSL VPN-Plus] タブの [サーバー設定] 画面で設定された Edge Gateway の IP アドレスおよびポートに、クライアント システムからアクセスできる必要があります。[SSL VPN サーバの設定](#)を参照してください。

手順

1 SSL-VPN Plus 画面への移動

SSL-VPN Plus 画面に移動して、NSX Data Center for vSphere Edge Gateway に SSL-VPN Plus サービスを設定することができます。

2 SSL VPN サーバの設定

このサーバ設定では、サービスがリスンする IP アドレスとポート、サービスの暗号リスト、およびそのサービス証明書など、SSL VPN サーバの設定を行います。Edge Gateway に接続するときに、リモート ユーザーはこれらのサーバ設定と同じ IP アドレスとポートを指定します。

3 Edge Gateway 上で SSL VPN-Plus と使用するための IP アドレス プールの作成

[SSL VPN-Plus] タブの [IP プール] 画面を使用して設定した固定 IP アドレス プールに含まれる仮想 IP アドレスが、リモート ユーザーに割り当てられます。

4 Edge Gateway 上で SSL VPN-Plus とともに使用するためのプライベート ネットワークの追加

プライベート ネットワークを構成するには、[SSL VPN-Plus] タブにある [プライベート ネットワーク] 画面を使用します。プライベート ネットワークは、リモート ユーザーが VPN クライアントと SSL VPN トンネルを使用して接続するときに、VPN クライアントがアクセスするネットワークです。有効なプライベート ネットワークは、VPN クライアントのルーティング テーブルに組み込まれます。

5 Edge Gateway での SSL VPN-Plus の認証サービスの設定

[SSL VPN-Plus] タブにある [認証] 画面を使用して、Edge Gateway の SSL VPN サービスのローカル認証サーバを設定し、オプションでクライアント証明書の認証を有効にします。この認証サーバを使用して、接続しているユーザーを認証します。ローカル認証サーバに設定されているすべてのユーザーが認証されます。

6 ローカルの SSL VPN-Plus 認証サーバへの SSL VPN-Plus ユーザーの追加

[SSL VPN-Plus] タブの [ユーザー] 画面を使用して、Edge Gateway の SSL VPN サービスのローカル認証サーバに、リモート ユーザーのアカウントを追加します。

7 SSL VPN-Plus クライアントのインストール パッケージの追加

[SSL VPN-Plus] タブにある [インストール パッケージ] 画面を使用して、リモート ユーザー用の SSL VPN-Plus クライアントの名前付きインストール パッケージを作成します。

8 SSL VPN-Plus クライアント構成の編集

[SSL VPN-Plus] タブの [クライアント構成] 画面を使用して、リモート ユーザーが SSL VPN にログインしたときの SSL VPN クライアント トンネルの応答方法をカスタマイズします。

9 Edge Gateway での SSL VPN-Plus の全般設定のカスタマイズ

vCloud Director 環境の Edge Gateway では、一部の SSL VPN-Plus 設定がデフォルトで設定されています。vCloud Director テナント ポータルの [SSL VPN-Plus] タブの [全般設定] を使用して、これらの設定をカスタマイズします。

SSL-VPN Plus 画面への移動

SSL-VPN Plus 画面に移動して、NSX Data Center for vSphere Edge Gateway に SSL-VPN Plus サービスを設定することができます。

手順

- 1 Edge Gateway サービスを開きます。
 - a [ネットワーク] > [エッジ] の順に選択します。
 - b 編集する Edge Gateway を選択し、[サービス] をクリックします。
- 2 [SSL VPN-Plus] タブをクリックします。

次のステップ

[全般] 画面で、SSL VPN-Plus のデフォルト設定を行います。[Edge Gateway での SSL VPN-Plus の全般設定のカスタマイズ](#)を参照してください。

SSL VPN サーバの設定

このサーバ設定では、サービスがリスンする IP アドレスとポート、サービスの暗号リスト、およびそのサービス証明書など、SSL VPN サーバの設定を行います。Edge Gateway に接続するときに、リモート ユーザーはこれらのサーバ設定と同じ IP アドレスとポートを指定します。

Edge Gateway がその外部インターフェイス上の複数のオーバーレイ IP アドレス ネットワークで構成されている場合、SSL VPN サーバに対して選択した IP アドレスが、Edge Gateway のデフォルトの外部インターフェイスとは異なる可能性があります。

SSL VPN サーバの設定時に、SSL VPN トンネルで使用する暗号化アルゴリズムを選択する必要があります。1 つ以上の暗号を選択できます。選択した暗号の長所と短所を照らし合わせながら、慎重に選択します。

デフォルトでは、Edge Gateway ごとに SSL VPN トンネルのデフォルトのサーバ ID 証明書として生成されたデフォルトの自己署名証明書が使用されます。このデフォルトの証明書ではなく、[証明書] 画面でシステムに追加したデジタル証明書を使用することもできます。

前提条件

- [SSL VPN-Plus の設定](#)で説明されている前提条件を満たしていることを確認します。
- デフォルトとは異なるサービス証明書を使用する場合は、必要な証明書をシステムにインポートします。[Edge Gateway へのサービス証明書の追加](#)を参照してください。
- [SSL-VPN Plus 画面への移動](#)。

手順

- 1 [SSL VPN-Plus] 画面で、[サーバ設定] をクリックします。

- 2 [有効] をクリックします。
- 3 ドロップダウン メニューから IP アドレスを選択します。
- 4 (オプション) TCP のポート番号を入力します。

この TCP ポート番号は、SSL クライアント インストール パッケージで使用されます。デフォルトでは、HTTPS/SSL トラフィックのデフォルト ポートのポート 443 が使用されます。ポート番号が必要な場合でも、通信用の任意の TCP ポートを設定できます。

注： SSL VPN クライアントでは、ここで設定した IP アドレスとポートにリモート ユーザーのクライアント システムからアクセスできる必要があります。ポート番号をデフォルトから変更する場合は、変更後の IP アドレスとポートに対象ユーザーのシステムから確実にアクセスできるようにします。

- 5 暗号リストから暗号化方式を選択します。
- 6 サービスの Syslog のログ ポリシーを設定します。

デフォルトではログは有効です。ログに記録するメッセージのレベルを変更するか、ログを無効にできます。
- 7 (オプション) システムが生成したデフォルトの自己署名証明書ではなくサービス証明書を使用する場合は、[サービス証明書を変更] をクリックし、証明書を選択して [OK] をクリックします。
- 8 [変更を保存] をクリックします。

次のステップ

注： 設定した Edge Gateway の IP アドレスと TCP ポート番号にリモート ユーザーがアクセスできる必要があります。この手順で設定した SSL VPN-Plus の IP アドレスとポートへのアクセスを許可する、Edge Gateway のファイアウォール ルールを追加します。[NSX Data Center for vSphere Edge Gateway ファイアウォール ルールの追加](#)を参照してください。

リモート ユーザーが SSL VPN-Plus を使用して接続したときにリモート ユーザーに IP アドレスが割り当てられるように IP プールを追加します。[Edge Gateway 上で SSL VPN-Plus と使用するための IP アドレス プールの作成](#)を参照してください。

Edge Gateway 上で SSL VPN-Plus と使用するための IP アドレス プールの作成

[SSL VPN-Plus] タブの [IP プール] 画面を使用して設定した固定 IP アドレス プールに含まれる仮想 IP アドレスが、リモート ユーザーに割り当てられます。

この画面で追加された各 IP アドレス プールは、Edge Gateway に設定される IP アドレス サブネットになります。これらの IP アドレス プールで使用する IP アドレスの範囲は、Edge Gateway で設定されている他のすべてのネットワークとは異なっている必要があります。

注： SSL VPN は、IP アドレス プールの IP アドレスを、画面上のテーブルに表示される IP アドレス プールの順に、リモート ユーザーに割り当てます。IP アドレス プールを画面上のテーブルに追加した後は、上下の矢印を使用して、テーブル内のアドレス プールの位置を調整できます。

前提条件

- [SSL-VPN Plus 画面への移動](#)。

■ SSL VPN サーバの設定。

手順

1 [SSL VPN-Plus] タブで、[IP プール] をクリックします。

2 [作成] () ボタンをクリックします。

3 IP プールを設定します。

オプション	アクション
IP の範囲	127.0.0.1-127.0.0.9. のように、この IP アドレス プールの IP アドレスの範囲を入力します。 VPN クライアントを認証し、SSL VPN トンネルに接続するときに、これらの IP アドレスが割り当てられます。
ネットマスク	255.255.255.0 など、IP アドレス プールのネットマスクを入力します。
ゲートウェイ	Edge Gateway でこの IP アドレス プールのゲートウェイ アドレスとして作成して割り当てる IP アドレスを入力します。 IP アドレス プールが作成されると、Edge Gateway 仮想マシンで仮想アダプタが作成され、この IP アドレスはその仮想インターフェイスに設定されます。この IP アドレスには、[IP の範囲] フィールドで指定した範囲に含まれないサブネットの任意の IP アドレスも指定できます。
説明	(オプション) この IP アドレス プールの説明を入力します。
ステータス	この IP アドレス プールを有効にするか無効にするかを選択します。
プライマリ DNS	(オプション) これらの仮想 IP アドレスの名前解決のために使用するプライマリ DNS サーバの名前を入力します。
セカンダリ DNS	(オプション) 使用するセカンダリ DNS サーバの名前を入力します。
DNS サフィックス	(オプション) ドメインベースのホスト名解決のために、クライアント システムがホストされているドメインの DNS サフィックスを入力します。
WINS サーバ	(オプション) 組織のニーズに合わせて、WINS サーバ アドレスを入力します。

4 [保持] をクリックします。

結果

IP アドレス プールの構成が画面上のテーブルに追加されます。

次のステップ

SSL VPN-Plus を使用して接続するリモート ユーザーにアクセスを許可するプライベート ネットワークを追加します。[Edge Gateway 上で SSL VPN-Plus とともに使用するためのプライベート ネットワークの追加](#)を参照してください。

Edge Gateway 上で SSL VPN-Plus とともに使用するためのプライベート ネットワークの追加

プライベート ネットワークを構成するには、[SSL VPN-Plus] タブにある [プライベート ネットワーク] 画面を使用します。プライベート ネットワークは、リモート ユーザーが VPN クライアントと SSL VPN トンネルを使用し

て接続するときに、VPN クライアントがアクセスするネットワークです。有効なプライベート ネットワークは、VPN クライアントのルーティング テーブルに組み込まれます。


プライベート ネットワークは、VPN クライアントのトラフィックを暗号化する、または暗号化から除外する Edge Gateway の背後にあるすべてのアクセス可能な IP アドレス ネットワークのリストです。SSL VPN トンネル経由でアクセスする必要がある各プライベート ネットワークは、個別のエントリとして追加する必要があります。エントリの数は、ルート要約の手法を使用して制限できます。

- SSL VPN-Plus は、リモート ユーザーによるプライベート ネットワークへのアクセスを、画面上のテーブルに表示される IP アドレス プールの順（上から下）に許可します。プライベート ネットワークを画面上のテーブルに追加した後は、上下の矢印を使用して、テーブル内のネットワークの位置を調整できます。
- プライベート ネットワークに対して TCP 最適化の有効化を選択すると、アクティブ モードの FTP などの一部のアプリケーションがそのサブネット内で動作しない場合があります。アクティブ モードで構成されている FTP サーバを追加するには、その FTP サーバ用に別のプライベート ネットワークを追加し、そのプライベート ネットワークの TCP 最適化を無効にする必要があります。また、その FTP サーバのプライベート ネットワークを有効にし、画面上のテーブルで、TCP が最適化されたプライベート ネットワークより上に表示されるようにする必要があります。

前提条件

- [SSL-VPN Plus 画面への移動](#)。
- [Edge Gateway 上で SSL VPN-Plus と使用するための IP アドレス プールの作成](#)。

手順

- 1 [SSL VPN-Plus] タブで、[プライベート ネットワーク] をクリックします。
- 2 [追加] () ボタンをクリックします。
- 3 プライベート ネットワークを構成します。

オプション	アクション
ネットワーク	プライベート ネットワークの IP アドレスを、 192169.1.0/24 などの CIDR 形式で入力します。
説明	(オプション) ネットワークの説明を入力します。
トラフィックを送信	<p>VPN クライアントでプライベート ネットワークとインターネット トラフィックを送信する方法を指定します。</p> <ul style="list-style-type: none"> ■ [トンネルを経由] <p>VPN クライアントは、プライベート ネットワークとインターネット トラフィックを SSL VPN-Plus が有効な Edge Gateway を経由して送信します。</p> ■ [トンネルを迂回] <p>VPN クライアントは Edge Gateway をバイパスし、トラフィックをプライベート サーバに直接送信します。</p>

オプション	アクション
TCP 最適化を有効化	<p>(オプション) インターネットの速度を最適化するには、トラフィックの送信に [トンネルを経由] を選択した際に、[TCP 最適化を有効化] も選択する必要があります。</p> <p>このオプションを選択すると、VPN トンネルでの TCP パケットのパフォーマンスが向上しますが、UDP トラフィックのパフォーマンスは向上しません。</p> <p>従来のフルアクセス SSL VPN トンネルは、インターネット上の暗号化で、2 番目の TCP/IP スタックの TCP/IP データを送信します。この従来の方法では、アプリケーション レイヤーのデータを 2 つの別々の TCP ストリームにカプセル化します。パケット ロスは最適なインターネット条件下でも発生しますが、これが起こると、TCP-over-TCP メルトダウンと呼ばれるパフォーマンス劣化効果が生じます。TCP-over-TCP メルトダウンでは、2 つの TCP 計測ツールが 1 つの IP アドレス データ パケットを修正することにより、ネットワークのスループットが低下し、接続がタイムアウトになります。[TCP 最適化を有効化] を選択すると、この TCP-over-TCP の問題が発生するリスクを回避できます。</p> <p>注： TCP 最適化を有効にする際には、以下を考慮する必要があります。</p> <ul style="list-style-type: none"> ■ インターネット トラフィックを最適化するポート番号を入力する必要があります。 ■ SSL VPN サーバは、VPN クライアントの代わりに TCP 接続を開始します。SSL VPN サーバが TCP 接続を開始すると、最初に自動生成される Edge ファイアウォール ルールが適用されます。このルールは、Edge Gateway から開始されたすべての接続の通過を許可します。最適化されていないトラフィックは、通常の Edge ファイアウォール ルールによって評価されます。デフォルトで生成された TCP ルールでは、任意の接続が許可されます。
ポート	<p>[トンネルを経由] を選択した場合は、リモート ユーザーが内部サーバにアクセスするために開くポート番号の範囲を入力します。FTP トラフィックの場合は 20-21、HTTP トラフィックの場合は 80-81 のようになります。</p> <p>ユーザーに無制限のアクセス権を付与する場合は、このフィールドを空白のままにします。</p>
ステータス	プライベート ネットワークの有効/無効を切り替えます。

4 [保持] をクリックします。

5 [変更を保存] をクリックして、システムに設定を保存します。

次のステップ

認証サーバを追加します。 [Edge Gateway での SSL VPN-Plus の認証サービスの設定](#) を参照してください。

重要： この画面で追加したプライベート ネットワークへのネットワーク トラフィックを許可するため、対応するファイアウォール ルールを追加します。 [NSX Data Center for vSphere Edge Gateway ファイアウォール ルールの追加](#) を参照してください。

Edge Gateway での SSL VPN-Plus の認証サービスの設定

[SSL VPN-Plus] タブにある [認証] 画面を使用して、Edge Gateway の SSL VPN サービスのローカル認証サーバを設定し、オプションでクライアント証明書の認証を有効にします。この認証サーバを使用して、接続しているユーザーを認証します。ローカル認証サーバに設定されているすべてのユーザーが認証されます。

1 台のローカル SSL VPN-Plus 認証サーバのみを Edge Gateway に設定できます。[+ ローカル] をクリックして追加の認証サーバを指定した場合、設定の保存を試みるとエラー メッセージが表示されます。

SSL VPN 経由での認証の最大時間は、3 分です。この最大数は認証以外のタイムアウトによって決定されます。この値を設定することはできず、デフォルト値は 3 分です。このため、チェーン認証に複数の認証サーバがあり、ユーザー認証に 3 分を超える時間がかかる場合、ユーザーは認証されません。

前提条件

- [SSL-VPN Plus 画面への移動](#)。
- [Edge Gateway 上で SSL VPN-Plus とともに使用するためのプライベート ネットワークの追加](#)。
- クライアント証明書認証を有効にする場合は、CA 証明書が Edge Gateway に追加されていることを確認します。[SSL 証明書の信頼性検証のための Edge Gateway への CA 証明書の追加](#) を参照してください。

手順

- 1 [SSL VPN-Plus] タブおよび [認証] をクリックします。
- 2 [ローカル] をクリックします。

3 認証サーバを設定します。

- a (オプション) パスワード ポリシーを有効にして設定します。

オプション	説明
パスワード ポリシーを有効化	ここで設定するパスワード ポリシーを適用します。
パスワードの長さ	パスワードの長さで許可される最大文字数と最小文字数を入力します。
英字の最小数	(オプション) パスワードに必要な英字の最小数を入力します。
数字の最小数	(オプション) パスワードに必要な数字の最小数を入力します。
特殊文字の最小数	(オプション) アンバサンド (&)、ハッシュ タグ (#)、パーセント記号 (%) など、パスワードに必要な特殊文字の最小数を入力します。
パスワードにはユーザー ID を含めないでください	(オプション) パスワードにユーザー ID を含めることを禁止するには、このオプションを有効にします。
パスワードの有効期間	(オプション) ユーザーによる変更が必要になるまでパスワードが存続できる最大日数を入力します。
有効期限の通知 (期限切れになるまでの日数を指定)	(オプション) [パスワードの有効期間] の値の何日前に、パスワードの有効期限が近づいていることをユーザーに通知するかを入力します。

- b (オプション) アカウントのロックアウト ポリシーを有効にして設定します。

オプション	説明
アカウントのロックアウト ポリシーを有効化	ここで設定するアカウント ロックアウト ポリシーを適用します。
再試行の回数	ユーザーが自分のアカウントへのアクセスを再試行できる回数を入力します。
再試行の期間	ログインが成功しなかった場合にユーザー アカウントがロックされる期間を分単位で入力します。 たとえば、[再試行の回数] を 5 に、[再試行の期間] を 1 分間に設定した場合、1 分間のうちにログインに 5 回失敗すると、ユーザーのアカウントがロックされることになります。
ロックアウトの期間	ユーザー アカウントをロック状態にする期間を入力します。 この期間が経過すると、アカウントのロックは自動的に解除されます。

- c [ステータス] セクションでこの認証サーバを有効にします。

- d (オプション) セカンダリ認証を設定します。

オプション	説明
このサーバをセカンダリ認証に使用	(オプション) 認証の第 2 レベルとしてサーバを使用するかどうかを指定します。
認証が失敗した場合はセッションを終了	(オプション) 認証の失敗時に VPN セッションを終了するかどうかを指定します。

- e [保持] をクリックします。

- 4 (オプション) クライアント認定の認証を有効にするは、[証明書を変更] をクリックして有効/無効の切り替えをオンにし、使用する CA 証明書を選択して [OK] をクリックします。

次のステップ

ローカル認証サーバにローカル ユーザーを追加し、これらのユーザーが SSL VPN-Plus を使用して接続できるようにします。[ローカルの SSL VPN-Plus 認証サーバへの SSL VPN-Plus ユーザーの追加](#) を参照してください。

リモート ユーザーがローカル システムにインストールできるようにするために、SSL クライアントを含むインストール パッケージを作成します。[SSL VPN-Plus クライアントのインストール パッケージの追加](#) を参照してください。

ローカルの SSL VPN-Plus 認証サーバへの SSL VPN-Plus ユーザーの追加

[SSL VPN-Plus] タブの [ユーザー] 画面を使用して、Edge Gateway の SSL VPN サービスのローカル認証サーバに、リモート ユーザーのアカウントを追加します。


注： ローカル認証サーバがまだ構成されていない場合、[ユーザー] 画面でユーザーを追加すると、ローカル認証サーバがデフォルト値で自動的に追加されます。[認証] 画面の編集ボタンを使用して、デフォルト値を表示して編集します。[認証] 画面の使用の詳細については、「[Edge Gateway での SSL VPN-Plus の認証サービスの設定](#)」を参照してください。

前提条件

[SSL-VPN Plus 画面への移動](#)。

手順

1 [SSL VPN-Plus] タブで、[ユーザー] をクリックします。

2 [作成] () ボタンをクリックします。

3 ユーザーの次のオプションを設定します。

オプション	説明
ユーザー ID	ユーザー ID を入力します。
パスワード	ユーザーのパスワードを入力します。
パスワードを再入力	パスワードを再入力します。
名	(オプション) ユーザーの名を入力します。
姓	(オプション) ユーザーの姓を入力します。
説明	(オプション) ユーザーの説明を入力します。
有効	ユーザーを有効にするか無効にするかを指定します。
パスワードを無期限にする	(オプション) このユーザーに対して常に同じパスワードを保持するかどうかを指定します。
パスワードの変更を許可	(オプション) ユーザーがパスワードを変更できるようにするかどうかを指定します。
次のログインでパスワードを変更	(オプション) このユーザーの次回ログイン時に、パスワードを変更するように依頼するかどうかを指定します。

4 [保持] をクリックします。

5 ユーザーを追加するには、手順を繰り返します。

次のステップ

ローカル認証サーバにローカル ユーザーを追加し、これらのユーザーが SSL VPN-Plus を使用して接続できるようにします。[ローカルの SSL VPN-Plus 認証サーバへの SSL VPN-Plus ユーザーの追加](#) を参照してください。

リモート ユーザーがローカル システムにインストールできるようにするために、SSL クライアントを含むインストール パッケージを作成します。[SSL VPN-Plus クライアントのインストール パッケージの追加](#) を参照してください。

SSL VPN-Plus クライアントのインストール パッケージの追加

[SSL VPN-Plus] タブにある [インストール パッケージ] 画面を使用して、リモート ユーザー用の SSL VPN-Plus クライアントの名前付きインストール パッケージを作成します。


SSL VPN-Plus クライアント インストール パッケージは、Edge Gateway に追加できます。新しいユーザーは、最初に VPN 接続を使用してログインする際に、このパッケージをダウンロードしてインストールするように求められます。これらのクライアント インストール パッケージを追加すると、Edge Gateway のパブリック インターフェイスの FQDN からダウンロードできるようになります。

Windows、Linux、および Mac オペレーティング システムで実行するインストール パッケージを作成することができます。SSL VPN クライアントごとに異なるインストール パラメータを必要とする場合は、構成ごとにインストール パッケージを作成します。

前提条件

SSL-VPN Plus 画面への移動

手順

- 1 このテナント ポータルの [SSL VPN-Plus] タブで、[インストール パッケージ] をクリックします。
- 2 [追加] () ボタンをクリックします。
- 3 インストール パッケージを設定します。

オプション	説明
プロファイル名	このインストール パッケージのプロファイル名を入力します。 この名前は、Edge Gateway へのこの SSL VPN 接続を識別するためにリモート ユーザーに表示されます。
ゲートウェイ	Edge Gateway のパブリック インターフェイスの IP アドレスまたは FQDN を入力します。 入力した IP アドレスまたは FQDN は、SSL VPN クライアントにバインドされます。クライアントがリモート ユーザーのローカル システムにインストールされている場合、この IP アドレスまたは FQDN が SSL VPN クライアントに表示されます。 この SSL VPN クライアントに追加の Edge Gateway アップリンク インターフェイスをバインドするには、[追加] () ボタンをクリックして行を追加し、インターフェイスの IP アドレスまたは FQDN とポートを入力します。
ポート	(オプション) 表示されるデフォルトの値からポート値を変更するには、値をダブルクリックして新しい値を入力します。

オプション	説明
Windows	インストール パッケージを作成するオペレーティング システムを選択します。
Linux	
Mac	
説明	(オプション) ユーザーの説明を入力します。
有効	このパッケージを有効にするか無効にするかを指定します。

4 Windows のインストール パラメータを選択します。

オプション	説明
ログイン時にクライアントを起動	リモート ユーザーがローカル システムにログインするときに、SSL VPN クライアントを起動します。
パスワードの保存を許可	ユーザーのパスワードをクライアントで記憶できるようにします。
サイレント モードのインストールを有効化	リモート ユーザーに対してインストール コマンドを表示しません。
SSL クライアント ネットワーク アダプタを非表示	VMware SSL VPN-Plus アダプタを非表示にします。このアダプタは、SSL VPN クライアント インストール パッケージと一緒にリモート ユーザーのコンピュータにインストールされます。
クライアント システム トレイ アイコンを非表示	VPN 接続がアクティブかアクティブでないかを示す SSL VPN トレイ アイコンを非表示にします。
デスクトップアイコンを作成	ユーザー デスクトップに SSL クライアントを起動するアイコンを作成します。
サイレント モードの操作を有効化	インストールが完了したことを示すウィンドウを非表示にします。
サーバセキュリティ証明書の検証	SSL VPN クライアントが安全な接続を確立する前に SSL VPN サーバ証明書を検証します。

5 [保持] をクリックします。

次のステップ

クライアントの設定を編集します。 [SSL VPN-Plus クライアント構成の編集](#) を参照してください。

SSL VPN-Plus クライアント構成の編集

[SSL VPN-Plus] タブの [クライアント構成] 画面を使用して、リモート ユーザーが SSL VPN にログインしたときの SSL VPN クライアント トンネルの応答方法をカスタマイズします。

前提条件

[SSL-VPN Plus 画面への移動](#)

手順

- 1 [SSL VPN-Plus] タブで、[クライアント構成] をクリックします。
- 2 [トンネリング モード] を選択します。
 - 分割トンネル モードでは、VPN トラフィックのみが Edge Gateway を通過します。

- フル トンネル モードでは、Edge Gateway がリモート ユーザーのデフォルト ゲートウェイとなり、すべてのトラフィック（VPN、ローカル、インターネットなど）が Edge Gateway を通過します。
- 3 フル トンネル モードを選択した場合、リモート ユーザーのクライアントで使用するデフォルト ゲートウェイの IP アドレスを入力します。また、必要に応じて、ローカル サブネットのトラフィックのフローを VPN トンネルから除外するかどうかを選択できます。
 - 4 （オプション） 自動再接続を無効にします。

デフォルトでは [自動再接続を有効化] は有効です。自動再接続が有効な場合は、ユーザーが切断されると、SSL VPN クライアントによって自動的に再接続します。
 - 5 （オプション） 必要に応じて、クライアントのアップグレードが利用可能な場合にリモート ユーザーに通知するためのクライアントの機能を有効にします。

デフォルトではこのオプションは無効です。このオプションを有効にした場合、リモート ユーザーはアップグレードのインストールを選択できます。
 - 6 [変更を保存] をクリックします。

Edge Gateway での SSL VPN-Plus の全般設定のカスタマイズ

vCloud Director 環境の Edge Gateway では、一部の SSL VPN-Plus 設定がデフォルトで設定されています。vCloud Director テナント ポータルの [SSL VPN-Plus] タブの [全般設定] を使用して、これらの設定をカスタマイズします。

前提条件

[SSL-VPN Plus 画面への移動](#)。

手順

- 1 [SSL VPN-Plus] タブで、[全般設定] をクリックします。
- 2 組織のニーズに合わせて、必要に応じて全般設定を編集します。

オプション	説明
同じユーザー名を使用した複数のログインを禁止する	オンにすると、リモート ユーザーが同じユーザー名で利用できるアクティブなログイン セッションが 1 つのみに制限されます。
圧縮	オンにすると、TCP ベースのインテリジェント データ圧縮が有効になり、データ転送速度が向上します。
ログの有効化	オンにすると、SSL VPN ゲートウェイを通過するトラフィックのログが保持されます。デフォルトではログは有効です。
仮想キーボードを強制する	オンにすると、リモート ユーザーは画面上の仮想キーボードのみを使用してログイン情報を入力する必要があります。
仮想キーボードのキーをランダム化する	オンにすると、仮想キーボードでランダムなキー レイアウトが使用されます。
セッション アイドル タイムアウト	セッション アイドル タイムアウトを分単位で入力します。 指定された期間、ユーザーのセッションでアクティビティがない場合、ユーザーのセッションを切断します。システムのデフォルトは 10 分です。
ユーザー通知	リモート ユーザーがログインした後、リモート ユーザーに表示するメッセージを入力します。

オプション	説明
パブリック URL アクセスを有効化	オンにすると、リモート ユーザーは、リモート ユーザー アクセスが明示的に設定されていないサイトにアクセスできます。
強制タイムアウトを有効化	オンにすると、[強制タイムアウト] フィールドで指定した期間の経過後にリモート ユーザーを切断します。
強制タイムアウト	タイムアウト時間を分単位で入力します。 [強制タイムアウトを有効化] をオンに切り替えると、このフィールドが表示されます。

3 [変更を保存] をクリックします。

IPsec VPN の構成

vCloud Director 環境に置かれた NSX Data Center for vSphere Edge Gateway は、組織仮想データセンター ネットワーク間、または組織仮想データセンター ネットワークと外部 IP アドレス間の VPN トンネルを保護するために、サイト間の Internet Protocol Security (IPsec) をサポートしています。IPsec VPN サービスは Edge Gateway に設定できます。

最も一般的なシナリオは、リモート ネットワークから組織仮想データセンターへの IPsec VPN 接続を設定することです。NSX ソフトウェアでは、証明書認証、事前共有キー モード、自身とリモート VPN ルーター間の IP ユニキャストトラフィックのサポートなどの Edge Gateway の IPsec VPN 機能が提供されます。複数のサブネットが Edge Gateway の背後にある内部ネットワークに IPsec トンネル経由で接続するような設定も可能です。IPsec トンネルを経由して内部ネットワークに接続するように複数のサブネットを設定する場合は、これらのサブネットおよび Edge Gateway の背後にある内部ネットワークのアドレス範囲が重複しないようにする必要があります。

注： IPsec トンネルの両側にあるローカル ピアとリモート ピアで IP アドレスが重複している場合は、ローカルに接続されたルートおよび自動配管ルートの有無に応じて、このトンネルを通して転送されるトラフィックに一貫性がなくなることがあります。

次の IPsec VPN アルゴリズムがサポートされています。

- AES (AES128 CBC)
- AES256 (AES256-CBC)
- トリプル DES (3DES192-CBC)
- AES-GCM (AES128 GCM)
- DH-2 (Diffie-Hellman グループ 2)
- DH-5 (Diffie-Hellman グループ 5)
- DH-14 (Diffie-Hellman グループ 14)

注： IPsec VPN では、動的ルーティング プロトコルはサポートされていません。組織仮想データセンターの Edge Gateway とリモート サイトの物理ゲートウェイ VPN の間に IPsec VPN トンネルを構成する場合は、その接続の動的ルーティングを構成できません。リモート サイトの IP アドレスを、Edge Gateway のアップリンク上の動的ルーティングによって学習することはできません。

『NSX 管理ガイド』のトピック「IPsec VPN の概要」に記載されているように、Edge Gateway でサポートされている最大トンネル数は、構成されているサイズ（コンパクト、大、特大、超特大）によって決まります。

Edge Gateway 構成のサイズを表示するには、Edge Gateway に移動し、Edge Gateway 名をクリックします。

Edge Gateway で IPsec VPN を設定するには、複数の手順を実行します。

注： トンネルのエンドポイント間にファイアウォールが配置されている場合は、IPsec VPN サービスを設定した後、次の IP プロトコルおよび UDP ポートを許可するようにルールを更新します。

- IP プロトコル ID 50 (ESP)
- IP プロトコル ID 51 (AH)
- UDP ポート 500 (IKE)
- UDP ポート 4500

手順

1 [IPsec VPN] 画面への移動

[IPsec VPN] 画面で、NSX Data Center for vSphere Edge Gateway の IPsec VPN サービスの設定を開始できます。

2 Edge ゲートウェイの IPsec VPN サイト接続の設定

Edge Gateway の IPsec VPN 機能を使用して、組織仮想データセンターと別のサイトの間に IPsec VPN 接続を確立するために必要な設定を行うには、vCloud Director テナント ポータルで [IPsec VPN サイト] 画面を使用します。

3 Edge ゲートウェイでの IPsec VPN サービスの有効化

1 つ以上の IPsec VPN 接続が設定されている場合は、Edge Gateway で IPsec VPN サービスを有効にできます。

4 グローバル IPsec VPN 設定の指定

[グローバル構成] 画面を使用して、IPsec VPN の認証を Edge Gateway レベルで設定します。この画面では、グローバルの事前共有キーを設定し、証明書認証を有効にすることができます。

[IPsec VPN] 画面への移動

[IPsec VPN] 画面で、NSX Data Center for vSphere Edge Gateway の IPsec VPN サービスの設定を開始できます。

手順

1 Edge Gateway サービスを開きます。

- a [ネットワーク] > [エッジ] の順に選択します。
- b 編集する Edge Gateway を選択し、[サービス] をクリックします。

2 [VPN] - [IPsec VPN] の順に選択します。

次のステップ

[IPsec VPN サイト] 画面を使用して、IPsec VPN 接続を設定します。Edge ゲートウェイで IPsec VPN サービスを有効にするには、少なくとも 1 つの接続を事前に設定する必要があります。[Edge ゲートウェイの IPsec VPN サイト接続の設定](#)を参照してください。

Edge ゲートウェイの IPsec VPN サイト接続の設定

Edge Gateway の IPsec VPN 機能を使用して、組織仮想データセンターと別のサイトの間に IPsec VPN 接続を確立するために必要な設定を行うには、vCloud Director テナント ポータルで [IPsec VPN サイト] 画面を使用します。


サイト間に IPsec VPN 接続を設定する場合は、現在の場所から見て接続を設定します。接続の設定には、VPN 接続を正しく設定できるように、vCloud Director 環境のコンテキスト内での接続の概念について理解する必要があります。

- ローカル サブネットおよびピア サブネットによって、VPN の接続先ネットワークが指定されます。IPsec VPN サイトの設定内でこれらのサブネットを指定する場合は、特定の IP アドレスではなく、ネットワーク範囲を入力します。**192.168.99.0/24** などの CIDR 形式を使用します。
- ピア ID は、VPN 接続を終端するリモート デバイスを一意に識別する ID のことで、通常はパブリック IP アドレスです。証明書認証を使用するピアの場合、この ID はピアの証明書で設定された識別名である必要があります。PSK ピアの場合、この ID には任意の文字列を指定できます。NSX のベスト プラクティスは、リモート デバイスのパブリック IP アドレスまたは完全修飾ドメイン名 (FQDN) をピア ID として使用することです。ピア IP アドレスが別の組織仮想データセンター ネットワークから取得されている場合は、ピアのネイティブ IP アドレスを入力します。ピアに NAT が設定されている場合は、ピアのプライベート IP アドレスを入力します。
- ピア エンドポイントは、ユーザーが接続しているリモート デバイスのパブリック IP アドレスを指定します。ピアのゲートウェイにインターネットから直接アクセスできず、別のデバイスを介して接続されている場合は、ピア エンドポイントのアドレスがピアの ID と異なることがあります。ピアに NAT が設定されている場合は、デバイスが NAT に使用しているパブリック IP アドレスを入力します。
- ローカル ID は、組織仮想データセンターの Edge Gateway のパブリック IP アドレスを指定します。Edge Gateway のファイアウォールと、IP アドレスまたはホスト名を入力することができます。
- ローカル エンドポイントは、Edge Gateway が送信を行う組織仮想データセンター内のネットワークを指定します。通常は、Edge Gateway の外部ネットワークがローカル エンドポイントになります。

前提条件

- [\[IPsec VPN\] 画面への移動](#)。
- [IPsec VPN の構成](#)。
- 認証方法としてグローバル証明書を使用する場合は、[\[グローバル構成\] 画面で証明書認証が有効になっていることを確認](#)します。[グローバル IPsec VPN 設定の指定](#)を参照してください。

手順

- 1 Edge Gateway サービスを開きます。
 - a [ネットワーク] > [エッジ] の順に選択します。
 - b 編集する Edge Gateway を選択し、[サービス] をクリックします。
- 2 [IPsec VPN] タブで、[IPsec VPN サイト] をクリックします。
- 3 [追加] () ボタンをクリックします。
- 4 IPsec VPN 接続を設定します。

オプション	アクション
有効	この接続を 2 台の VPN エンドポイント間で有効にします。
Perfect Forward Secrecy (PFS) の有効化	<p>このオプションを有効にすると、システムはユーザーが開始したすべての IPsec VPN セッションに対して一意のパブリック キーを生成します。</p> <p>PFS を有効にすると、Edge Gateway のプライベート キーと各セッション キーの間にリンクが作成されなくなります。</p> <p>セッション キーが危険にさらされても、このキーによって保護された特定のセッション内で交換されたデータ以外に影響はありません。サーバのプライベート キーが危険にさらされると、アーカイブされたセッションまたは今後のセッションの復号化にこのキーを使用できなくなります。</p> <p>PFS が有効な場合は、この Edge ゲートウェイとの IPsec VPN 接続を処理するときに、若干のオーバーヘッドが発生します。</p> <p>重要： 追加キーの取得元として、一意のセッション キーを使用しないでください。また、IPsec VPN トンネルが機能するには、トンネルの両側で PFS をサポートする必要があります。</p>
名前	(オプション) 接続の名前を入力します。
ローカル ID	<p>Edge Gateway インスタンスの外部 IP アドレスを入力します。これは、Edge Gateway のパブリック IP アドレスです。</p> <p>この IP アドレスは、リモート サイトの IPsec VPN 設定でピア ID に使用されます。</p>
ローカル エンドポイント	<p>この接続のローカル エンドポイントであるネットワークを入力します。</p> <p>ローカル エンドポイントは、Edge Gateway が送信を行う組織仮想データセンター内のネットワークを指定します。通常は、外部ネットワークがローカル エンドポイントになります。事前共有キーを使用して IP 間トンネルを追加する場合は、ローカル ID とローカル エンドポイントの IP アドレスを同じにすることができます。</p>
ローカル サブネット	<p>サイト間で共有するネットワークを入力します。複数のサブネットを入力するには、区切り文字にカンマを使用します。</p> <p>特定の IP アドレスではなく、IP アドレスを CIDR 形式 (192.168.99.0/24 など) で指定してネットワーク範囲を入力します。</p>

オプション	アクション
ピア ID	<p>ピア サイトを一意に識別するピア ID を入力します。</p> <p>ピア ID は、VPN 接続を終端するリモート デバイスを一意に識別する ID のことで、通常はパブリック IP アドレスです。</p> <p>証明書認証を使用するピアの場合、この ID はピアの証明書に含まれている識別名である必要があります。PSK ピアの場合、この ID には任意の文字列を指定できます。NSX のベスト プラクティスは、リモート デバイスのパブリック IP アドレスまたは完全修飾ドメイン名 (FQDN) をピア ID として使用することです。</p> <p>ピア IP アドレスが別の組織仮想データセンター ネットワークから取得されている場合は、ピアのネイティブ IP アドレスを入力します。ピアに NAT が設定されている場合は、ピアのプライベート IP アドレスを入力します。</p>
ピア エンドポイント	<p>接続先リモート デバイスのパブリック側アドレスである、ピア サイトの IP アドレスまたは完全修飾ドメイン名 (FQDN) を入力します。</p> <p>注： ピアに NAT が設定されている場合は、デバイスが NAT に使用しているパブリック IP アドレスを入力します。</p>
ピア サブネット	<p>VPN の接続先となるリモート ネットワークを入力します。複数のサブネットを入力するには、区切り文字にカンマを使用します。</p> <p>特定の IP アドレスではなく、IP アドレスを CIDR 形式 (192.168.99.0/24 など) で指定してネットワーク範囲を入力します。</p>
暗号化アルゴリズム	<p>ドロップダウン メニューから暗号化アルゴリズムのタイプを選択します。</p> <p>注： 選択する暗号化タイプは、リモート サイトの VPN デバイスで設定されている暗号化タイプと一致する必要があります。</p>
認証	<p>認証を選択します。次のオプションがあります。</p> <ul style="list-style-type: none"> ■ [PSK] <p>事前共有キー (PSK) を選択すると、Edge Gateway とピア サイト間で共有されるプライベート キーを認証に使用するように指定されます。</p> ■ [証明書] <p>証明書の認証では、グローバル レベルで定義された証明書を認証に使用するように指定されます。このオプションは、[IPsec VPN] タブの [グローバル構成] 画面でグローバル証明書が設定されている場合以外は使用できません。</p>
共有キーを変更	<p>(オプション) 既存の接続の設定を更新している場合は、このオプションを有効にして [事前共有キー] フィールドを使用可能にし、共有キーを更新できるようにします。</p>
事前共有キー	<p>認証タイプに [PSK] を選択した場合、英数字のシークレット文字列を入力します。これは、最大長が 128 バイトの文字列です。</p> <p>注： 共有キーは、リモート サイトの VPN デバイスで設定されたキーと一致する必要があります。ベスト プラクティスは、匿名サイトが VPN サービスに接続するときに共有キーを設定することです。</p>
共有キーの表示	<p>(オプション) このオプションを有効にすると、共有キーを画面に表示できるようになります。</p>

オプション	アクション
Diffie-Hellman グループ	<p>ピア サイトおよびこの Edge Gateway が、セキュアでない通信チャネルを介して共有シークレットを確立できるようにする暗号化スキームを選択します。</p> <p>注： [Diffie-Hellman グループ] は、リモート サイトの VPN デバイスで設定された内容と一致する必要があります。</p>
拡張	<p>(オプション) 次のオプションのいずれかを入力します。</p> <ul style="list-style-type: none"> ■ <code>securelocaltrafficbyip=IPAddress</code> : IPsec VPN トンネルを介して Edge Gateway のローカル トラフィックをリダイレクトします。 <p>これはデフォルト値です。</p> <ul style="list-style-type: none"> ■ <code>passthroughSubnets=PeerSubnetIPAddress</code> : 重複するサブネットをサポートします。

5 [保持] をクリックします。

6 [変更を保存] をクリックします。

保存操作が完了するまでに 1 分ほどかかることがあります。

次のステップ

リモート サイトの接続を設定します。接続の両側（組織仮想データセンターおよびピア サイト）で、IPsec VPN 接続を設定する必要があります。

この Edge ゲートウェイで IPsec VPN サービスを有効にします。少なくとも 1 つの IPsec VPN 接続が設定されている場合は、サービスを有効にできます。[Edge ゲートウェイでの IPsec VPN サービスの有効化](#) を参照してください。

Edge ゲートウェイでの IPsec VPN サービスの有効化

1 つ以上の IPsec VPN 接続が設定されている場合は、Edge Gateway で IPsec VPN サービスを有効にできます。

前提条件

- [\[IPsec VPN\] 画面への移動](#)。
- この Edge ゲートウェイに、少なくとも 1 つの IPsec VPN 接続が設定されていることを確認します。[Edge ゲートウェイの IPsec VPN サイト接続の設定](#)で説明されている手順を参照してください。

手順

- 1 [IPsec VPN] タブで、[アクティベーションのステータス] をクリックします。
- 2 [IPsec VPN サービス ステータス] をクリックして、IPsec VPN サービスを有効にします。
- 3 [変更を保存] をクリックします。

結果

Edge ゲートウェイの IPsec VPN サービスがアクティブになります。

グローバル IPsec VPN 設定の指定

[グローバル構成] 画面を使用して、IPsec VPN の認証を Edge Gateway レベルで設定します。この画面では、グローバルの事前共有キーを設定し、証明書認証を有効にすることができます。

グローバルの事前共有キーは、ピア エンドポイントが **any** に設定されたサイトで使用されます。

前提条件

- 証明書認証を有効にする場合は、1 つ以上のサービス証明書と、それに対応する CA 署名付き証明書を保持していることを [証明書] 画面で確認します。IPsec VPN には、自己署名証明書は使用できません。[Edge Gateway へのサービス証明書の追加](#)を参照してください。
- [\[IPsec VPN\] 画面への移動](#)。

手順

- 1 Edge Gateway サービスを開きます。
 - a [ネットワーク] > [エッジ] の順に選択します。
 - b 編集する Edge Gateway を選択し、[サービス] をクリックします。
- 2 [IPsec VPN] タブで、[グローバル構成] をクリックします。
- 3 (オプション) 次のようにして、グローバル事前共有キーを設定します。
 - a [共有キーを変更] オプションを有効にします。
 - b 事前共有キーを有効にします。

グローバルの事前共有キー (PSK) は、ピア エンドポイントが「any」に設定されたすべてのサイトによって共有されます。グローバルの PSK がすでに設定されている場合、PSK を空の値に変更して保存しても既存の設定には影響しません。

- c (オプション) 必要に応じて [共有キーの表示] を有効にして、事前共有キーを表示します。
 - d [変更を保存] をクリックします。
- 4 証明書認証を設定します。
 - a [証明書認証の有効化] を有効にします。
 - b 適切なサービス証明書、CA 証明書、CRL を選択します。
 - c [変更を保存] をクリックします。

次のステップ

必要に応じて、Edge Gateway の IPsec VPN サービスのログを有効にできます。[Edge Gateway の統計情報とログ](#)を参照してください。

L2 VPN の構成

vCloud Director 環境の Edge Gateway では、L2 VPN がサポートされます。L2 VPN により、地理的境界を越えて同じ IP アドレスを保持しながら仮想マシンを常にネットワークに接続できるようになるため、組織仮想データセンターの拡張が可能になります。L2 VPN サービスを Edge Gateway に設定できます。

NSX Data Center for vSphere は、Edge Gateway の L2 VPN 機能を提供します。L2 VPN により、2 つのサイト間のトンネルを設定できます。これらのサイト間で移動した場合も、仮想マシンは同じサブネット上にとどまるため、L2 VPN を使用してネットワークを拡張することにより、組織仮想データセンターを拡張することができます。一方のサイトの Edge Gateway から、他方のサイトの仮想マシンにすべてのサービスを提供できます。

L2 VPN トンネルを作成するには、L2 VPN サーバおよび L2 VPN クライアントを設定します。『NSX 管理ガイド』に記載されているように、L2 VPN サーバがターゲット Edge Gateway に、L2 VPN クライアントがソース Edge Gateway になります。各 Edge Gateway で L2 VPN を設定した後に、サーバとクライアントの両方で L2 VPN サービスを有効にする必要があります。

注： サブインターフェイスとして作成された経路指定済みの組織仮想データセンター ネットワークは、Edge Gateway 上になければなりません。

[L2 VPN] 画面への移動

NSX Data Center for vSphere Edge Gateway の L2 VPN サービスの設定を開始するには、[L2 VPN] 画面に移動する必要があります。

手順

- 1 Edge Gateway サービスを開きます。
 - a [ネットワーク] > [エッジ] の順に選択します。
 - b 編集する Edge Gateway を選択し、[サービス] をクリックします。
- 2 [VPN] - [L2 VPN] の順に選択します。

次のステップ

L2 VPN サーバを設定します。[L2 VPN サーバとしての Edge Gateway の構成](#)を参照してください。

L2 VPN サーバとしての Edge Gateway の構成

L2 VPN サーバは、L2 VPN クライアントが接続するターゲット NSX Edge です。

『NSX 管理ガイド』に記載されているように、複数のピア サイトをこの L2 VPN サーバに接続できます。

注： サイトの構成を変更すると、Edge Gateway は既存のすべての接続から切断され、再接続されます。


前提条件

- Edge Gateway に、Edge Gateway のサブインターフェイスとして構成されている、経路指定された組織仮想データセンター ネットワークがあることを確認してください。
- [\[L2 VPN\] 画面への移動](#)。
- サービス証明書を L2 VPN 接続にバインドする場合は、サーバ証明書が Edge Gateway にすでにアップロードされていることを確認します。[Edge Gateway へのサービス証明書の追加](#)を参照してください。
- L2 VPN サービスを有効にするには、サーバのリスナー IP アドレス、リスナー ポート、暗号化アルゴリズム、および少なくとも 1 つのピア サイトを構成しておく必要があります。

手順

- 1 [L2 VPN] タブで、L2 VPN モードの [サーバ] を選択します。
- 2 [サーバー グローバル] タブで、L2 VPN サーバのグローバル構成の詳細を設定します。

オプション	アクション
リスナー IP アドレス	Edge Gateway の外部インターフェイスのプライマリまたはセカンダリ IP アドレスを選択します。
リスナー ポート	組織のニーズに合わせて、表示される値を編集します。 L2 VPN サービスのデフォルト ポートは 443 です。
暗号化アルゴリズム	サーバとクライアント間の通信に使用する暗号化アルゴリズムを選択します。
サービス証明書の詳細	[サーバ証明書を変更] をクリックして、L2 VPN サーバにバインドする証明書を選択します。 [サーバ証明書を変更] ウィンドウで、[サーバ証明書の検証] を有効にし、リストからサーバ証明書を選択して [OK] をクリックします。

- 3 ピア サイトを構成するには、[サーバー サイト] タブをクリックします。
- 4 [追加] () ボタンをクリックします。
- 5 L2 VPN ピア サイトの設定をします。

オプション	アクション
有効	このピア サイトを有効にします。
名前	ピア サイトの一意の名前を入力します。
説明	(オプション) 説明を入力します。
ユーザー ID	ピア サイトの認証に使用するユーザー名とパスワードを入力します。
パスワード	ピア サイトのユーザー認証情報は、クライアント側の認証情報と同じにする必要があります。
パスワードを確認	
拡張インターフェイス	クライアントで拡張されるサブインターフェイスを 1 つ以上選択します。 選択できるサブインターフェイスは、Edge Gateway でサブインターフェイスとして構成された組織仮想データセンター ネットワークのサブインターフェイスです。
出力方向最適化ゲートウェイ アドレス	(オプション) 仮想マシンのデフォルト ゲートウェイが 2 つのサイトで同じである場合は、L2 VPN トンネルを介してトラフィックをローカルに経路指定またはブロックするサブインターフェイスのゲートウェイ IP アドレスを入力します。

- 6 [保持] をクリックします。
 - 7 [変更を保存] をクリックします。
- 保存操作が完了するまでに 1 分ほどかかることがあります。

次のステップ

この Edge Gateway で L2 VPN サービスを有効にします。 [Edge Gateway での L2 VPN サービスの有効化](#) を参照してください。

L2 VPN クライアントとしての Edge Gateway の構成

L2 VPN クライアントは、ターゲット NSX Edge（L2 VPN サーバ）との通信を開始するソース NSX Edge です。

前提条件

- [\[L2 VPN\] 画面への移動。](#)
- この L2 VPN クライアントが、サーバ証明書を使用する L2 VPN サーバに接続している場合は、この L2 VPN クライアントのサーバ証明書を検証できるようにするために、対応する認証局 (CA) 証明書が Edge Gateway にアップロードされていることを確認します。[SSL 証明書の信頼性検証のための Edge Gateway への CA 証明書の追加](#)を参照してください。

手順

- 1 [L2 VPN] タブで、L2 VPN モードの [クライアント] を選択します。
- 2 [クライアント グローバル] タブで、L2 VPN クライアントのグローバル構成の詳細を設定します。

オプション	説明
サーバ アドレス	このクライアントが接続する L2 VPN サーバの IP アドレスを入力します。
サーバ ポート	クライアントが接続する L2 VPN サーバのポートを入力します。 デフォルト ポートは 443 です。
暗号化アルゴリズム	サーバと通信するための暗号化アルゴリズムを選択します。
拡張インターフェイス	サーバに拡張するサブインターフェイスを選択します。 選択できるサブインターフェイスは、Edge Gateway でサブインターフェイスとして構成された組織仮想データセンター ネットワークのサブインターフェイスです。
出力方向最適化ゲートウェイ アドレス	(オプション) 仮想マシンのデフォルト ゲートウェイが 2 つのサイト間で同じ場合、サブインターフェイスのゲートウェイ IP アドレスか、トラフィックをトンネル経由でフローさせない IP アドレスを入力します。
ユーザー詳細	サーバ認証で使用するユーザー ID とパスワードを入力します。

- 3 [変更を保存] をクリックします。
保存操作が完了するまでに 1 分ほどかかることがあります。
- 4 (オプション) 詳細オプションを設定するには、[クライアント詳細] タブをクリックします。
- 5 この L2 VPN クライアント Edge がインターネットに直接アクセスできず、プロキシ サーバを使用して L2 VPN サーバ Edge にアクセスする必要がある場合は、プロキシ設定を指定します。

オプション	説明
セキュア プロキシの有効化	選択してセキュアなプロキシを有効にします。
アドレス	プロキシ サーバの IP アドレスを入力します。
ポート	プロキシ サーバ ポートを入力します。
ユーザー名 パスワード	プロキシ サーバの認証情報を入力します。

6 サーバ認定の検証を有効にするには、[CA 証明書を変更] をクリックし、適切な CA 証明書を選択します。

7 [変更を保存] をクリックします。

保存操作が完了するまでに 1 分ほどかかることがあります。

次のステップ

この Edge ゲートウェイで L2 VPN サービスを有効にします。[Edge Gateway での L2 VPN サービスの有効化](#) を参照してください。

Edge Gateway での L2 VPN サービスの有効化

必要な L2 VPN 設定が行われている場合は、Edge Gateway で L2 VPN サービスを有効にできます。

注： この Edge Gateway で HA がすでに構成されている場合、Edge Gateway に 1 つ以上の内部インターフェイスを確実に構成します。1 つのインターフェイスだけがあり、そのインターフェイスが HA 機能によってすでに使用されている場合、同じ内部インターフェイス上の L2 VPN 構成は機能しません。

前提条件

- この Edge Gateway が L2 VPN サーバ（宛先の NSX Edge）の場合、L2 VPN サーバの必要な設定が行われており、1 つ以上の L2 VPN ピア サイトが構成されていることを確認します。[L2 VPN サーバとしての Edge Gateway の構成](#) で説明されている手順を参照してください。
- この Edge Gateway が L2 VPN クライアント（送信元 NSX Edge）の場合、L2 VPN クライアントが設定されていることを確認します。[L2 VPN クライアントとしての Edge Gateway の構成](#) で説明されている手順を参照してください。
- [\[L2 VPN\] 画面への移動](#)。

手順

1 [L2 VPN] タブで [有効化] 切り替えボタンをクリックします。

2 [変更を保存] をクリックします。

結果

Edge Gateway の L2 VPN サービスがアクティブになります。

次のステップ

ファイアウォールのインターネット側で NAT またはファイアウォール ルールを作成し、L2 VPN サーバが L2 VPN クライアントに接続できるようにします。

Edge ゲートウェイからの L2 VPN サービス構成の削除

Edge Gateway の既存の L2 VPN サービス構成は削除することができます。このアクションにより、Edge ゲートウェイの L2 VPN サービスも無効になります。

前提条件

[\[L2 VPN\] 画面への移動](#)

手順

- 1 [L2 VPN] 画面の一番下までスクロールし、[構成の削除] をクリックします。
- 2 削除を確定するには、[OK] をクリックします。

結果

L2 VPN サービスが無効になり、構成の詳細が Edge ゲートウェイから削除されます。

SSL 証明書の管理

vCloud Director 環境内の NSX ソフトウェアは、Edge ゲートウェイに設定した SSL VPN-Plus および IPsec VPN トンネルで Secure Sockets Layer (SSL) 証明書を使用する機能を提供します。

vCloud Director 環境の Edge ゲートウェイでは、自己署名証明書、認証局 (CA) 署名付き証明書、および CA によって生成、署名された証明書がサポートされます。証明書署名リクエスト (CSR) の生成、証明書のインポート、インポートした証明書の管理、証明書失効リスト (CRL) の作成を実行できます。

組織仮想データセンターでの証明書の使用について

vCloud Director 組織仮想データセンターの以下のネットワーク領域について、証明書を管理できます。

- 組織仮想データセンター ネットワークとリモート ネットワークの間の IPsec VPN トンネル
- プライベート ネットワークのリモート ユーザーと組織仮想データセンター内の Web リソースの間の SSL VPN-Plus 接続
- 2 つの NSX Edge ゲートウェイの間の L2 VPN トンネル
- 組織仮想データセンターでロード バランシングが設定されている仮想サーバおよびプール サーバ

クライアント証明書の使用方法

CAI コマンドまたは REST 呼び出しを通じてクライアント証明書を作成できます。その後、この証明書をリモートユーザーに配布し、リモート ユーザーが証明書を各自の Web ブラウザにインストールできます。

クライアント証明書の導入の主なメリットは、各リモート ユーザーに関するリファレンス クライアント証明書を保存し、リモート ユーザーが提示するクライアント証明書に照らして確認できるという点にあります。特定のユーザーからの今後の接続を防ぐために、セキュリティ サーバのクライアント証明書のリストからリファレンス証明書を削除することができます。証明書を削除すると、そのユーザーからの接続が拒否されます。

Edge Gateway の証明書署名リクエストの生成

認証局 (CA) に署名付き証明書を要求するか、自己署名証明書を作成するには、Edge Gateway の証明書署名リクエスト (CSR) を生成しておく必要があります。

CSR は、SSL 証明書を必要とする NSX Edge Gateway で生成する必要があるエンコードされたファイルです。CSR を使用すると、会社名とドメイン名を識別する情報とともにパブリック キーを送信する方法が標準化されます。

Edge Gateway に保存しておく必要がある、一致するプライベート キーのファイルを使用して CSR を生成します。CSR には、一致するパブリック キーと他の情報（組織の名前、場所、ドメイン名など）が含まれます。

手順

- 1 Edge Gateway サービスを開きます。
 - a [ネットワーク] > [エッジ] の順に選択します。
 - b 編集する Edge Gateway を選択し、[サービス] をクリックします。
- 2 [証明書] タブをクリックします。
- 3 [証明書] タブで [CSR] をクリックします。
- 4 CSR の次のオプションを設定します。

オプション	説明
コモン ネーム	使用する証明書の対象組織の完全修飾ドメイン名 (FQDN) を入力します (www.example.com など)。 コモン ネームに http:// または https:// のプリフィックスを含めないでください。
組織単位	このフィールドは、この証明書が関連付けられている vCloud Director 組織内の部門を区別する場合に使用します。「エンジニアリング」や「販売」などを入力します。
組織名	どの名前で会社が法的に登録されているかを入力します。 記載する組織は、証明書要求内のドメイン名の法的登録者でなければなりません。
地域	会社が法的に登録されている市または地域を入力します。
都道府県名	会社が法的に登録されている都道府県の完全な名前を入力します (短縮形を使用しない)。
国コード	会社が法的に登録されている国の名前を入力します。
プライベート キー アルゴリズム	証明書のキー タイプ (RSA または DSA) を入力します。 通常は RSA を使用します。キー タイプは、ホスト間の通信の暗号化アルゴリズムを定義します。 注： SSL VPN-Plus は RSA 証明書のみをサポートします。
キーのサイズ	キー サイズをビット数で入力します。 最小サイズは、2,048 ビットです。
説明	(オプション) 証明書の説明を入力します。

- 5 [保持] をクリックします。

CSR が生成され、CSR タイプの新しいエントリが画面上のリストに追加されます。

結果

画面上のリストで CSR タイプのエントリを選択すると、その CSR の詳細が画面に表示されます。表示された、CSR の PEM 形式のデータをコピーし、それを認証局 (CA) に送信して CA 署名付き証明書を取得できます。

次のステップ

CSR を使用してサービス証明書を作成するには、次の 2 つのオプションのいずれかを使用します。

- CSR を CA に送信して、CA 署名付き証明書を取得します。認証局 (CA) から署名付き証明書を受け取ったら、署名付き証明書をシステムにインポートします。Edge Gateway 用に生成された CSR に対応する CA 署名付き証明書のインポートを参照してください。

- CSR を使用して、自己署名証明書を作成します。[自己署名サービス証明書の構成](#) を参照してください。

Edge Gateway 用に生成された CSR に対応する CA 署名付き証明書のインポート

証明書署名リクエスト (CSR) を生成し、その CSR に基づく CA 署名付き証明書を取得した後、CA 署名付き証明書をインポートして Edge Gateway で使用できます。

前提条件

CSR に対応する CA 署名付き証明書を取得していることを確認します。CA 署名付き証明書内のプライベート キーが、選択した CSR のプライベート キーと一致しない場合、インポート プロセスは失敗します。

手順

- Edge Gateway サービスを開きます。
 - [ネットワーク] > [エッジ] の順に選択します。
 - 編集する Edge Gateway を選択し、[サービス] をクリックします。
- [証明書] タブをクリックします。
- 画面上のテーブルで、インポートする CA 署名付き証明書の対象の CSR を選択します。
- 署名付き証明書をインポートします。
 - [CSR 用に生成された署名付き証明書] をクリックします。
 - CA 署名証明書の PEM データを指定します。
 - 参照可能なシステム上の PEM ファイルにデータがある場合は、[アップロード] ボタンをクリックしてそのファイルを参照し、選択します。
 - PEM データをコピーして貼り付けることができる場合、[署名付き証明書 (PEM 形式)] フィールドに PEM データを貼り付けます。

-----BEGIN CERTIFICATE----- と -----END CERTIFICATE----- の行を含めます。
 - (オプション) 説明を入力します。
 - [保持] をクリックします。

注： CA 署名付き証明書内のプライベート キーが、[証明書] 画面で選択した CSR のプライベート キーと一致しない場合、インポート プロセスは失敗します。

結果

サービス証明書タイプの CA 署名付き証明書が画面上のリストに表示されます。

次のステップ

必要に応じて、SSL VPN-Plus トンネルまたは IPsec VPN トンネルに CA 署名付き証明書を接続します。[SSL VPN サーバの設定](#) および [グローバル IPsec VPN 設定の指定](#) を参照してください。

自己署名サービス証明書の構成

Edge Gateway の VPN 関連の機能で使用するために、Edge Gateway に自己署名サービス証明書を構成できます。また、自己署名証明書を作成、インストール、および管理できます。

サービス証明書が [証明書] 画面で使用可能な場合は、Edge Gateway の VPN 関連の設定を行うときにそのサービスの証明書を指定できます。VPN は、その VPN にアクセスするクライアントに指定されたサービス証明書を提示します。

前提条件

1 つ以上の CSR が Edge Gateway の [証明書] 画面で使用可能になっていること。[Edge Gateway の証明書署名リクエストの生成](#)を参照してください。

手順

- 1 Edge Gateway サービスを開きます。
 - a [ネットワーク] > [エッジ] の順に選択します。
 - b 編集する Edge Gateway を選択し、[サービス] をクリックします。
- 2 [証明書] タブをクリックします。
- 3 この自己署名証明書に使用する CSR をリストから選択し、[CSR を自己署名] をクリックします。
- 4 自己署名証明書の有効日数を入力します。
- 5 [保持] をクリックします。

システムが自己署名証明書を生成し、[サービス証明書] タイプの新しいエントリを画面上のリストに追加します。

結果

自己署名証明書は、Edge Gateway で使用可能です。画面上のリストで [サービス証明書] タイプのエントリを選択すると、その詳細が画面に表示されます。

SSL 証明書の信頼性検証のための Edge Gateway への CA 証明書の追加

Edge Gateway に CA 証明書を追加すると、認証のために Edge Gateway に提示された SSL 証明書（通常は Edge Gateway への VPN 接続で使用されるクライアント証明書）の信頼性を検証できます。

通常は、会社または組織のルート証明書を CA 証明書として追加します。一般的な用途は、証明書を使用して VPN クライアントを認証する際の SSL VPN です。クライアント証明書は VPN クライアントに配布でき、VPN クライアントからの接続時にそのクライアント証明書が CA 証明書に対して検証されます。

注： CA 証明書を追加する際、通常は関連する証明書失効リスト (CRL) を設定します。CRL は、失効した証明書を提示するクライアントを阻止します。[Edge Gateway への証明書失効リストの追加](#)を参照してください。

前提条件

PEM 形式の CA 証明書のデータがあることを確認します。ユーザー インターフェイスで、CA 証明書の PEM データを貼り付けるか、そのデータが格納されている、ネットワークで利用可能なファイルをローカル システム内で参照することができます。

手順

- 1 Edge Gateway サービスを開きます。
 - a [ネットワーク] > [エッジ] の順に選択します。
 - b 編集する Edge Gateway を選択し、[サービス] をクリックします。
- 2 [証明書] タブをクリックします。
- 3 [CA 証明書] をクリックします。
- 4 CA 証明書のデータを提供します。
 - 参照可能なシステム上の PEM ファイルにデータがある場合は、[アップロード] ボタンをクリックしてそのファイルを参照し、選択します。
 - PEM データのコピーと貼り付けが可能な場合は、[CA 証明書 (PEM 形式)] フィールドに貼り付けます。
 -----BEGIN CERTIFICATE----- と -----END CERTIFICATE----- の行を含めます。
- 5 (オプション) 説明を入力します。
- 6 [保持] をクリックします。

結果

[CA 証明書] タイプの CA 証明書が画面上のリストに表示されます。Edge Gateway の VPN 関連の設定を行うときに、この CA 証明書を指定できるようになりました。

Edge Gateway への証明書失効リストの追加

証明書失効リスト (CRL) は、発行元の証明書機関 (CA) から失効と主張されているデジタル証明書のリストです。これを使用すると、失効した証明書を提示するユーザーを信頼しないように、システムを更新できます。Edge Gateway に CRL を追加できます。

『NSX 管理ガイド』の説明のように、CRL には次の項目が含まれます。

- 失効した証明書と失効の理由
- 証明書の発行日
- 証明書を発行した機関
- 次のリリースの提案日

ある潜在的ユーザーがサーバへのアクセスを試みた場合、サーバは、その特定のユーザーに関する CRL エントリに基づいてアクセスの許可または拒否を行います。

手順

- 1 Edge Gateway サービスを開きます。
 - a [ネットワーク] > [エッジ] の順に選択します。
 - b 編集する Edge Gateway を選択し、[サービス] をクリックします。
- 2 [証明書] タブをクリックします。
- 3 [CRL] をクリックします。
- 4 CRL のデータを提供します。
 - 参照可能なシステム上の PEM ファイルにデータがある場合は、[アップロード] ボタンをクリックしてそのファイルを参照し、選択します。
 - PEM データのコピーと貼り付けが可能な場合は、[CRL (PEM 形式)] フィールドに貼り付けます。
 -----BEGIN X509 CRL----- と -----END X509 CRL----- の行を含めます。
- 5 (オプション) 説明を入力します。
- 6 [保持] をクリックします。

結果

CRL が画面上のリストに表示されます。

Edge Gateway へのサービス証明書の追加

Edge Gateway にサービス証明書を追加すると、これらの証明書が Edge Gateway の VPN 関連設定で使用できるようになります。[証明書] 画面にサービス証明書を追加できます。

前提条件

サービス証明書とそのプライベート キーが PEM 形式になっていることを確認します。ユーザー インターフェイスで、PEM データを貼り付けるか、そのデータを格納する、ローカル システムから利用可能なネットワーク内のファイルを参照できます。

手順

- 1 Edge Gateway サービスを開きます。
 - a [ネットワーク] > [エッジ] の順に選択します。
 - b 編集する Edge Gateway を選択し、[サービス] をクリックします。
- 2 [証明書] タブをクリックします。
- 3 [サービス証明書] をクリックします。
- 4 サービス証明書のデータを PEM 形式で入力します。
 - 参照可能なシステム上の PEM ファイルにデータがある場合は、[アップロード] ボタンをクリックしてそのファイルを参照し、選択します。

- PEM データのコピーと貼り付けが可能な場合は、[サービス証明書 (PEM 形式)] フィールドに貼り付けます。

-----BEGIN CERTIFICATE----- と -----END CERTIFICATE----- の行を含めます。

5 証明書プライベート キーのデータを PEM 形式で入力します。

- 参照可能なシステム上の PEM ファイルにデータがある場合は、[アップロード] ボタンをクリックしてそのファイルを参照し、選択します。
- PEM データのコピーと貼り付けが可能な場合は、[プライベート キー (PEM 形式)] フィールドに貼り付けます。

-----BEGIN RSA PRIVATE KEY----- と -----END RSA PRIVATE KEY----- の行を含めます。

6 プライベート キーのパスフレーズを入力して確認します。

7 (オプション) 説明を入力します。

8 [保持] をクリックします。

結果

[サービス証明書] タイプの証明書が画面上のリストに表示されます。Edge Gateway の VPN 関連の設定を行うときに、このサービス証明書を選択できるようになりました。

オブジェクトのグループ分け (カスタム)

NSX 環境の vCloud Director ソフトウェアは、特定のエンティティのセットおよびグループを定義する機能を提供します。これは、他のネットワーク関連の設定 (ファイアウォール ルールの設定など) を指定するときに使用できます。

ファイアウォール ルールと DHCP リレー設定で使用するための IP アドレス セットの作成

IP セットは、組織仮想データセンター レベルで作成できる IP アドレスのグループのことです。IP セットは、ファイアウォール ルールまたは DHCP リレー設定で送信元または宛先として使用することができます。

IP セットは、vCloud Director テナント ポータルの [オブジェクトのグループ分け] 画面を使用して作成します。[オブジェクトのグループ分け] 画面は、[サービス] 画面と [Edge ゲートウェイ] 画面の両方にあります。


手順

- 1 [オブジェクトのグループ分け] ページを開きます。

オプション	アクション
Edge Gateway サービスから開く	<ol style="list-style-type: none"> a [ネットワーク] - [エッジ] の順に選択します。 b 編集する Edge ゲートウェイを選択し、[サービスの構成] をクリックします。 c [オブジェクトのグループ分け] をクリックします。
セキュリティ サービスから開く	<ol style="list-style-type: none"> a [ネットワーク] - [セキュリティ] の順に選択します。 b 編集するセキュリティ サービスを選択し、[サービスの構成] をクリックします。 c [オブジェクトのグループ分け] をクリックします。

- 2 [IP アドレス セット] タブをクリックします。

定義済みの IP アドレス セットが画面に表示されます。

- 3 IP アドレス セットを追加するには、[作成] () ボタンをクリックします。
- 4 IP セットに含める IP アドレスの他に、IP セットの名前と、オプションで IP セットの説明を入力します。
- 5 (オプション) [サービス] 画面の [オブジェクトのグループ分け] 画面を使用して IP セットを指定する場合は、[継承] 切り替えを使用して継承を有効にし、基盤となるスコープでの表示を許可します。

継承はデフォルトでは有効です。

- 6 この IP セットを保存するには、[保持] をクリックします。

結果

これで、新しい IP セットをファイアウォール ルールまたは DHCP リレー構成でソースまたはターゲットとして選択できます。

ファイアウォール ルールで使用するための MAC アドレス セットの作成

MAC セットは、組織仮想データセンター レベルで作成できる MAC アドレスのグループです。ファイアウォール ルールの送信元または宛先として MAC セットを使用できます。

MAC アドレス セットは、vCloud Director テナント ポータルの [オブジェクトのグループ分け] 画面を使用して作成します。[オブジェクトのグループ分け] 画面は、[サービス] 画面と [Edge ゲートウェイ] 画面の両方にあります。


手順

- 1 [オブジェクトのグループ分け] ページを開きます。

オプション	アクション
Edge Gateway サービスから開く	<ol style="list-style-type: none"> a [ネットワーク] - [エッジ] の順に選択します。 b 編集する Edge ゲートウェイを選択し、[サービスの構成] をクリックします。 c [オブジェクトのグループ分け] をクリックします。
セキュリティ サービスから開く	<ol style="list-style-type: none"> a [ネットワーク] - [セキュリティ] の順に選択します。 b 編集するセキュリティ サービスを選択し、[サービスの構成] をクリックします。 c [オブジェクトのグループ分け] をクリックします。

- 2 [MAC アドレス セット] タブをクリックします。

定義済みの MAC アドレス セットが画面に表示されます。

- 3 MAC アドレス セットを追加するには、[作成] () ボタンをクリックします。
- 4 セット名を入力し、オプションで説明、および MAC アドレス セットに含める MAC アドレスを入力します。
- 5 (オプション) [サービス] 画面の [オブジェクトのグループ分け] ページを使用して MAC アドレス セットを指定する場合は、[継承] 切り替えを使用して継承を有効にし、基盤となるスコープでの表示を許可します。

継承はデフォルトでは有効です。

- 6 MAC アドレス セットを保存するには、[保持] をクリックします。

結果

これで、新しい MAC アドレス セットをファイアウォール ルールでソースまたはターゲットとして選択できます。

ファイアウォール ルールで使用可能なサービスの表示

ファイアウォール ルールで利用できるサービスのリストを表示できます。この場合、サービスとはプロトコルとポートの組み合わせです。

vCloud Director テナント ポータルの [オブジェクトのグループ分け] ページを使用して、使用可能なサービスを表示できます。[オブジェクトのグループ分け] ページは、[サービス] 画面と [Edge ゲートウェイ] 画面の両方にあります。

テナント ポータルを使用して、リストに新しいサービスを追加することはできません。使用可能なサービスのセットは、vCloud Director システム管理者によって管理されます。

手順

- 1 [オブジェクトのグループ分け] ページを開きます。

オプション	アクション
Edge Gateway サービスから開く	a [ネットワーク] - [エッジ] の順に選択します。 b 編集する Edge ゲートウェイを選択し、[サービスの構成] をクリックします。 c [オブジェクトのグループ分け] をクリックします。
セキュリティ サービスから開く	a [ネットワーク] - [セキュリティ] の順に選択します。 b 編集するセキュリティ サービスを選択し、[サービスの構成] をクリックします。 c [オブジェクトのグループ分け] をクリックします。

- 2 [サービス] タブをクリックします。

結果

使用可能なサービスが画面に表示されます。

ファイアウォール ルールで使用可能なサービス グループの表示

ファイアウォール ルールで使用できるサービス グループのリストを表示できます。この場合、サービスとはプロトコルとポートの組み合わせであり、サービス グループとはサービスまたは他のサービス グループから成るグループです。

vCloud Director テナント ポータルの [オブジェクトのグループ分け] ページを使用して、使用可能なサービス グループを表示できます。[オブジェクトのグループ分け] ページは、[サービス] 画面と [Edge ゲートウェイ] 画面の両方にあります。

テナント ポータルを使用して、サービス グループを作成することはできません。使用可能なサービス グループのセットは、vCloud Director システム管理者によって管理されます。

手順

- 1 [オブジェクトのグループ分け] ページを開きます。

オプション	アクション
Edge Gateway サービスから開く	a [ネットワーク] - [エッジ] の順に選択します。 b 編集する Edge ゲートウェイを選択し、[サービスの構成] をクリックします。 c [オブジェクトのグループ分け] をクリックします。
セキュリティ サービスから開く	a [ネットワーク] - [セキュリティ] の順に選択します。 b 編集するセキュリティ サービスを選択し、[サービスの構成] をクリックします。 c [オブジェクトのグループ分け] をクリックします。

- 2 [サービス グループ] タブをクリックします。

結果

使用可能なサービス グループが画面に表示されます。[説明] 列には、サービス グループごとにグループ分けされたサービスが表示されます。

Edge Gateway の統計情報とログ

Edge Gateway の統計情報およびログを表示できます。

統計情報の表示

[Edge ゲートウェイ サービス] 画面に統計情報を表示できます。

手順

- 1 Edge Gateway サービスを開きます。
 - a [ネットワーク] > [エッジ] の順に選択します。
 - b 編集する Edge Gateway を選択し、[サービス] をクリックします。
- 2 [統計情報] タブをクリックします。
- 3 表示する統計情報のタイプに応じて、タブを移動します。

オプション	説明
接続	[接続] 画面に運用状況が示されます。この画面には、選択した Edge ゲートウェイのインターフェイスを流れるトラフィックのグラフと、ファイアウォール サービスとロード バランサー サービスの接続統計が表示されます。 ステータスを表示する期間を選択します。
IPsec VPN	[IPsec VPN] 画面には、IPsec VPN のステータスと統計情報、および各トンネルのステータスと統計情報が表示されます。
L2 VPN	[L2 VPN] 画面には、L2 VPN のステータスと統計情報が表示されます。

ログの有効化

Edge Gateway のログを有効にできます。設定を完了するには、ログ データを収集する機能のログ設定を有効にするだけでなく、Syslog サーバが収集したログ データを受信できるように設定する必要があります。[Edge 設定] 画面で Syslog サーバをすると、その Syslog サーバから記録されたデータにアクセスできるようになります。

前提条件

この操作には、事前定義の組織管理者ロールに含まれている権限、またはそれに相当する権限が必要です。

手順

- 1 Edge Gateway サービスを開きます。
 - a [ネットワーク] > [エッジ] の順に選択します。
 - b 編集する Edge Gateway を選択し、[サービス] をクリックします。
- 2 [Edge 設定] タブで [Syslog サーバの編集] ボタンをクリックします。
 ログが有効なサービスに対して Edge Gateway のネットワーク関連ログが記録されるように、Syslog サーバをカスタマイズできます。

vCloud Director システム管理者が vCloud Director 環境用に Syslog サーバを構成した場合は、デフォルトでこの Syslog サーバが使用され、[Edge 設定] 画面にその IP アドレスが表示されます。

3 機能ごとにログを有効にします。

- [NAT] タブで [DNAT ルール] ボタンをクリックし、[ログの有効化] 切り替えを有効にします。
アドレス変換のログを記録します。
- [NAT] タブで [SNAT ルール] ボタンをクリックし、[ログの有効化] 切り替えを有効にします。
アドレス変換のログを記録します。
- [ルーティング] タブで [ルーティング設定] をクリックし、[動的ルーティングの設定] で [ログの有効化] 切り替えを有効にします。
動的ルーティングのアクティビティのログを記録します。[ログ レベル] ドロップダウン メニューで、ログを記録するメッセージ ステータス レベルの下限を選択します。
- [ロード バランサー] タブで [グローバル構成] をクリックし、[ログの有効化] 切り替えを有効にします。
ロード バランサーのトラフィック フローのログを記録します。[ログ レベル] ドロップダウン メニューで、ログを記録するメッセージ ステータス レベルの下限を選択します。
- [VPN] タブで [IPSec VPN] - [ログ設定] の順に選択し、[ログの有効化] 切り替えを有効にします。
ローカル サブネットとピア サブネットの間のトラフィック フローのログを記録します。[ログ レベル] ドロップダウン メニューで、ログを記録するメッセージ ステータス レベルの下限を選択します。
- [SSL VPN-Plus] タブで [全般設定] をクリックし、[ログの有効化] 切り替えを有効にします。
SSL VPN ゲートウェイを通過するトラフィックのログを保持します。
- [SSL VPN-Plus] タブで [サーバー設定] をクリックし、[ログの有効化] 切り替えを有効にします。
SSL VPN サーバで発生するアクティビティのログを Syslog に記録します。[ログ レベル] ドロップダウン メニューで、ログを記録するメッセージ ステータス レベルの下限を選択します。

SSH コマンドラインによる Edge Gateway へのアクセスの有効化

SSH コマンドラインによる Edge Gateway へのアクセスを有効にすることができます。

手順

- 1 Edge Gateway サービスを開きます。
 - a [ネットワーク] > [エッジ] の順に選択します。
 - b 編集する Edge Gateway を選択し、[サービス] をクリックします。
- 2 [Edge 設定] タブをクリックします。

3 SSH を設定します。

オプション	説明
ユーザー名	SSH がこの Edge Gateway にアクセスする場合に使用する認証情報を入力します。
パスワード	デフォルトでは、SSH のユーザー名は admin です。
パスワードを再入力	
パスワードの有効期限	パスワードの有効期間を日数で入力します。
ログイン バナー	Edge Gateway への SSH 接続を開始するときにユーザーに表示されるテキストを入力します。

4 [有効] 切り替えをオンにします。

次のステップ

SSH によるこの Edge Gateway へのアクセスを許可するように、該当する NAT またはファイアウォール ルールを設定します。

セキュリティ タグの操作

セキュリティ タグとは、仮想マシンまたは仮想マシンのグループに関連付けることができるラベルです。セキュリティ タグは、セキュリティ グループと共に使用することを想定して設計されています。セキュリティ タグを作成したら、それをファイアウォール ルールで使用するセキュリティ グループに関連付けます。ユーザー定義セキュリティ タグの作成、編集、割り当てを行うことができます。また、特定のセキュリティ タグが適用されている仮想マシンやセキュリティ グループを表示することもできます。

セキュリティ タグは、通常はオブジェクトを動的にグループ化してファイアウォール ルールを簡素化するために使用します。たとえば、任意の仮想マシンで発生することが予想されるアクティビティの種類に基づき、いくつかの異なるセキュリティ タグを作成できます。セキュリティ タグを、1 つはデータベース サーバ用、もう 1 つはメール サーバ用に作成します。その後、データベース サーバまたはメール サーバを収容する仮想マシンに適切なタグを適用します。後でセキュリティ グループにタグを割り当て、それに対するファイアウォール ルールを記述すれば、仮想マシンで実行されているのがデータベース サーバかメール サーバかによって異なるセキュリティ 設定を適用できます。仮想マシンの機能を後で変更する場合は、ファイアウォール ルールを編集するのではなく、セキュリティ タグから仮想マシンを削除して行えます。

セキュリティ タグの作成および割り当て

セキュリティ タグを作成して、仮想マシンまたは仮想マシン グループに割り当てることができます。

セキュリティ タグを作成してから、それを仮想マシンまたは仮想マシン グループに割り当てます。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、[ネットワーク] で [セキュリティ] を選択します。
- 2 セキュリティ サービスを選択し、[サービスの構成] をクリックします。
- 3 [セキュリティ タグ] タブをクリックします。

4 [作成] () ボタンをクリックし、セキュリティ タグの名前を入力します。

5 (オプション) セキュリティ タグの説明を入力します。

6 (オプション) セキュリティ タグを仮想マシンまたは仮想マシン グループに割り当てます。

[次のタイプのオブジェクトを参照] ドロップダウン メニューでは、[仮想マシン] がデフォルトで選択されています。

a 左側のパネルから仮想マシンを選択します。

b 右矢印をクリックして、選択した仮想マシンにセキュリティ タグを割り当てます。

仮想マシンは右側のパネルに移動し、セキュリティ タグが割り当てられます。

7 選択した仮想マシンへのタグの割り当てが完了したら、[保持] をクリックします。

結果

セキュリティ タグが作成され、(事前に選択してある場合は) 選択した仮想マシンに割り当てられます。

次のステップ

セキュリティ タグは、セキュリティ グループを操作するように設計されています。セキュリティ グループの作成の詳細については、[セキュリティ グループの作成](#)を参照してください。

セキュリティ タグの割り当ての変更

セキュリティ タグを作成すると、仮想マシンに手動で割り当てることができます。セキュリティ タグを編集して、セキュリティ タグをすでに割り当てた仮想マシンからタグを削除することもできます。


セキュリティ タグを作成済みの場合、それらを仮想マシンに割り当てることができます。セキュリティ タグを使用すると、ファイアウォール ルールを記述するための仮想マシンをグループ化できます。たとえば、機密性の高いデータがある仮想マシンのグループにセキュリティ タグを割り当てます。

手順

1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、[ネットワーク] で[セキュリティ] を選択します。

2 セキュリティ サービスを選択し、[サービスの構成] をクリックします。

3 [セキュリティ タグ] タブをクリックします。

4 セキュリティ タグのリストから、編集するセキュリティ タグを選択し、[編集] () ボタンをクリックします。

5 左側のパネルから仮想マシンを選択し、右矢印をクリックしてセキュリティ タグを割り当てます。

右側のパネルの仮想マシンには、セキュリティ タグが割り当てられます。

6 右側のパネルで仮想マシンを選択し、左矢印をクリックしてタグを削除します。

左側のパネルの仮想マシンには、セキュリティ タグが割り当てられていません。

7 変更の追加を完了した後、[保持] をクリックします。

結果

セキュリティ タグが、選択した仮想マシンに割り当てられます。

次のステップ

セキュリティ タグは、セキュリティ グループを操作するように設計されています。セキュリティ グループの作成の詳細については、[セキュリティ グループの作成](#)を参照してください。

適用されているセキュリティ タグの表示

環境内の仮想マシンに適用されているセキュリティ タグを表示できます。また、環境内のセキュリティ グループに適用されているセキュリティ タグを表示することもできます。

前提条件

セキュリティ タグが作成され、仮想マシンまたはセキュリティ グループに適用されている必要があります。

手順

- 1** [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、[ネットワーク] で [セキュリティ] を選択します。
- 2** セキュリティ サービスを選択し、[サービスの構成] をクリックします。
- 3** [セキュリティ タグ] タブから、割り当てられているタグを表示します。
 - a [セキュリティ タグ] タブで割り当てを確認するセキュリティ タグを選択して、[編集] アイコンをクリックします。
 - b [仮想マシンの割り当て/割り当て解除] で、セキュリティ タグに割り当てられている仮想マシンのリストを確認できます。
 - c [破棄] をクリックします。
- 4** [セキュリティ グループ] タブで、割り当てられているタグを表示します。
 - a [オブジェクトのグループ分け] タブをクリックし、[セキュリティ グループ] をクリックします。
 - b セキュリティ グループを選択します。
 - c [メンバーを含める] のリストから、セキュリティ グループに割り当てられているセキュリティ タグを確認できます。

結果


既存のセキュリティ タグのほか、関連付けられている仮想マシンおよびセキュリティ グループを表示できます。この方法で、セキュリティ タグとセキュリティ グループに基づき、ファイアウォール ルールの作成方針を決めることができます。

セキュリティ タグの編集

ユーザー定義のセキュリティ タグを編集できます。

仮想マシンの環境または機能を変更した場合は、別のセキュリティ タグを使用して、新しいマシン構成に対してファイアウォール ルールが適切となるようにすることもできます。たとえば、仮想マシンがある状態で、これ以上機密データを保存しない場合は、別のセキュリティ タグを割り当てて、機密データに適用されるファイアウォール ルールが仮想マシンに対して実行されないようにすることができます。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、[ネットワーク] で [セキュリティ] を選択します。
- 2 セキュリティ サービスを選択し、[サービスの構成] をクリックします。
- 3 [セキュリティ タグ] タブをクリックします。
- 4 セキュリティ タグのリストで、編集するセキュリティ タグを選択します。
- 5 [編集] () ボタンをクリックします。
- 6 セキュリティ タグの名前と説明を編集します。
- 7 選択した仮想マシンにタグを割り当てるか、割り当てを削除します。
- 8 変更内容を保存するには、[保持] をクリックします。

次のステップ


セキュリティ タグを編集すると、関連するセキュリティ グループまたはファイアウォール ルールの編集も必要になる場合があります。セキュリティ グループの詳細については、[セキュリティ グループの操作](#)を参照してください。

セキュリティ タグの削除

ユーザー定義のセキュリティ タグを削除できます。

仮想マシンの機能または環境が変わった場合は、セキュリティ タグを削除できます。たとえば、Oracle データベースのセキュリティ タグがある状態で別のデータベース サーバを使用することにした場合にセキュリティ タグを削除できます。その場合、Oracle データベースに適用されるファイアウォール ルールは、仮想マシンに対して実行されなくなります。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、[ネットワーク] で [セキュリティ] を選択します。
- 2 セキュリティ サービスを選択し、[サービスの構成] をクリックします。
- 3 [セキュリティ タグ] タブをクリックします。
- 4 セキュリティ タグのリストから、削除するセキュリティ タグを選択します。
- 5 [削除] () ボタンをクリックします。
- 6 削除を確定するには、[OK] をクリックします。

結果

セキュリティ タグが削除されます。

次のステップ

セキュリティ タグを削除すると、関連するセキュリティ グループまたはファイアウォール ルールの編集も必要になる場合があります。セキュリティ グループの詳細については、「[セキュリティ グループの操作](#)」を参照してください。

セキュリティ グループの操作

セキュリティ グループとは、仮想マシン、組織仮想データセンター ネットワーク、セキュリティ タグなどのアセットまたはグループ分けオブジェクトの集合です。

セキュリティ グループには、セキュリティ タグ、仮想マシン名、仮想マシンのゲスト OS 名、または仮想マシンのゲスト ホスト名に基づく動的なメンバーシップ基準を設定できます。たとえば、「web」というセキュリティ タグのある仮想マシンは、いずれも Web サーバ向けの特定のセキュリティ グループに自動的に追加されます。セキュリティ グループを作成すると、そのグループにセキュリティ ポリシーが適用されます。



セキュリティ グループの作成

ユーザー定義のセキュリティ グループを作成できます。

前提条件

セキュリティ グループでセキュリティ タグを使用する場合は、[セキュリティ タグの作成および割り当て](#)を行います。

手順

- 1 セキュリティ サービスを開きます。
 - a [ネットワーク] - [セキュリティ] の順に選択します。
 - b セキュリティ設定を適用する組織仮想データセンターを選択し、[サービスの構成] をクリックします。
テナント ポータルにセキュリティ サービスが表示されます。
- 2 [オブジェクトのグループ分け] - [セキュリティ グループ] の順に選択します。
[セキュリティ グループ] ページが開きます。
- 3 [作成] () ボタンをクリックします。
- 4 セキュリティ グループの名前と、オプションで説明を入力します。
この説明はセキュリティ グループのリスト内に表示されます。わかりやすい説明を追加することにより、セキュリティ グループを簡単に識別できます。
- 5 (オプション) 動的なメンバー セットを追加します。
 - a 動的なメンバー セットの下にある [追加] () ボタンをクリックします。
 - b ステートメントの条件の [任意]の一部または[すべて] に一致させるかどうかを選択します。

- c 一致する最初のオブジェクトを入力します。
オプションには、[セキュリティ タグ]、[仮想マシンのゲスト OS の名前]、[仮想マシン名]、[仮想マシンのゲスト ホストの名前] があります。
 - d [次を含む]、[次の値で始まる]、[次の値で終わる]などの演算子を選択します。
 - e 値を入力します。
 - f (オプション) 別のステートメントを追加するには、ブール演算子の [And] または [Or] を使用します。
- 6** (オプション) メンバーを含めます。
- a [次のタイプのオブジェクトを参照] ドロップダウン メニューで、[仮想マシン]、[組織 VDC ネットワーク]、[IP アドレス セット]、[MAC アドレス セット]、[セキュリティ タグ]などのオブジェクト タイプを選択します。
 - b [メンバーを含める] リストにオブジェクトを含めるには、左側のパネルでオブジェクトを選択し、右矢印をクリックして右側のパネルに移動します。
- 7** (オプション) メンバーを除外します。
- a [次のタイプのオブジェクトを参照] ドロップダウン メニューで、[仮想マシン]、[組織 VDC ネットワーク]、[IP アドレス セット]、[MAC アドレス セット]、[セキュリティ タグ]などのオブジェクト タイプを選択します。
 - b [メンバーを除外] リストにオブジェクトを含めるには、左側のパネルでオブジェクトを選択し、右矢印をクリックして右側のパネルに移動します。
- 8** 変更内容を維持するには、[保持] をクリックします。
この操作は完了するまでに 1 分かかることがあります。

結果

これで、セキュリティ グループを、ファイアウォール ルールなどのルールで使用できるようになりました。

セキュリティ グループの編集


ユーザー定義のセキュリティ グループを編集できます。

手順

- 1** セキュリティ サービスを開きます。
 - a [ネットワーク] - [セキュリティ] の順に選択します。
 - b セキュリティ設定を適用する組織仮想データセンターを選択し、[サービスの構成] をクリックします。
テナント ポータルにセキュリティ サービスが表示されます。
- 2** [オブジェクトのグループ分け] - [セキュリティ グループ] の順に選択します。
[セキュリティ グループ] ページが開きます。
- 3** 編集するセキュリティ グループを選択します。
セキュリティ グループの詳細は、セキュリティ グループのリストの下に表示されます。


4 (オプション) セキュリティ グループの名前と説明を編集します。

5 (オプション) 動的なメンバー セットを追加します。


- a [動的なメンバー セット] の下にある [追加] () ボタンをクリックします。
- b ステートメントの条件の [任意]の一部または[すべて] に一致させるかどうかを選択します。
- c 一致する最初のオブジェクトを入力します。


オプションには、[セキュリティ タグ]、[仮想マシンのゲスト OS の名前]、[仮想マシン名]、[仮想マシンのゲスト ホストの名前] があります。

- d [次を含む]、[次の値で始まる]、[次の値で終わる]などの演算子を選択します。
- e 値を入力します。
- f (オプション) 別のステートメントを追加するには、ブール演算子の [And] または [Or] を使用します。


6 (オプション) 編集するメンバー セットの横にある [編集] () アイコンをクリックして、動的なメンバー セットを編集します。

- a 動的なメンバー セットに必要な変更を適用します。
- b [OK] をクリックします。

7 (オプション) 削除するメンバー セットの横にある [削除] () アイコンをクリックして、動的なメンバー セットを削除します。

8 (オプション) [メンバーを含める] リストの横にある [編集] () アイコンをクリックして、含まれているメンバーのリストを編集します。

- a [次のタイプのオブジェクトを参照] ドロップダウン メニューで、[仮想マシン]、[組織 VDC ネットワーク]、[IP アドレス セット]、[MAC アドレス セット]、[セキュリティ タグ]などのオブジェクト タイプを選択します。
- b [メンバーを含める] リストにオブジェクトを含めるには、左側のパネルでオブジェクトを選択し、右矢印をクリックして右側のパネルに移動します。
- c [メンバーを含める] リストからオブジェクトを除外するには、右側のパネルでオブジェクトを選択し、左矢印をクリックして左側のパネルに移動します。

9 (オプション) [メンバーを除外] リストの横にある [編集] () アイコンをクリックして、除外されたメンバーのリストを編集します。

- a [次のタイプのオブジェクトを参照] ドロップダウン メニューで、[仮想マシン]、[組織 VDC ネットワーク]、[IP アドレス セット]、[MAC アドレス セット]、[セキュリティ タグ]などのオブジェクト タイプを選択します。
- b [メンバーを除外] リストにオブジェクトを含めるには、左側のパネルでオブジェクトを選択し、右矢印をクリックして右側のパネルに移動します。
- c [メンバーを除外] リストからオブジェクトを除外するには、右側のパネルでオブジェクトを選択し、左矢印をクリックして左側のパネルに移動します。

10 [変更を保存] をクリックします。

セキュリティ グループへの変更が保存されます。

セキュリティ グループの削除

ユーザー定義のセキュリティ グループを削除できます。

手順

1 セキュリティ サービスを開きます。

a [ネットワーク] - [セキュリティ] の順に選択します。

b セキュリティ設定を適用する組織仮想データセンターを選択し、[サービスの構成] をクリックします。

テナント ポータルにセキュリティ サービスが表示されます。

2 [オブジェクトのグループ分け] - [セキュリティ グループ] の順に選択します。

[セキュリティ グループ] ページが開きます。

3 削除するセキュリティ グループを選択します。

4 [削除] () ボタンをクリックします。

5 削除を確定するには、[OK] をクリックします。

結果

セキュリティ グループが削除されます。

NSX-T Data Center Edge Gateway の管理

7

NSX-T Data Center Edge Gateway は経路指定された組織 VDC ネットワークに対して、外部ネットワークとの接続および IP 管理プロパティを提供します。また、ファイアウォール、ネットワーク アドレス変換 (NAT)、DNS 転送、DHCP（デフォルトで有効）などのサービスも提供します。

この章には、次のトピックが含まれています。

- NSX-T Edge Gateway へのファイアウォール グループの追加
- NSX-T Edge Gateway ファイアウォール ルールの追加
- NSX-T Edge Gateway での SNAT ルールまたは DNAT ルールの追加
- NSX-T Edge Gateway での DNS フォワーダ サービスの設定
- カスタム アプリケーション ポート プロファイルの作成

NSX-T Edge Gateway へのファイアウォール グループの追加

ファイアウォール ルールを作成して NSX-T Edge Gateway に追加するには、まずファイアウォール グループを作成する必要があります。ファイアウォール グループは、ファイアウォール ルールが適用されるオブジェクトのグループです。複数のオブジェクトをファイアウォール グループにまとめると、作成するファイアウォール ルールの合計数を減らすことができます。

手順

- 1 [ネットワーク] > [エッジ] の順に選択します。
- 2 NSX-T Edge Gateway をクリックして、[セキュリティ] をクリックします。
- 3 [グループ] タブをクリックし、[新規] をクリックします。
- 4 ファイアウォール グループの名前と、オプションで説明を入力します。
- 5 グループに含める仮想マシンの IP アドレスまたは IP アドレス範囲を入力し、[追加] をクリックします。
- 6 ファイアウォール グループを保存するために、[保存] をクリックします。

結果

ファイアウォール グループが作成され、NSX-T Edge Gateway に追加されました。

次のステップ

NSX-T Edge Gateway ファイアウォール ルールの追加

NSX-T Edge Gateway ファイアウォール ルールの追加

NSX-T Edge Gateway との間で送受信されるネットワーク トラフィックを制御するには、ファイアウォール ルールを作成します。

手順

- 1 [ネットワーク] > [エッジ] の順に選択します。
- 2 Edge Gateway をクリックし、[サービス] をクリックします。
- 3 [ファイアウォール] 画面が表示されていない場合は、[ファイアウォール] タブをクリックします。
- 4 [ルールの編集] をクリックします。
- 5 ファイアウォール ルールを選択し、[上に追加] ボタンをクリックします。

新しいルールの行が、選択したルールの上に追加されます。

- 6 ファイアウォール ルールを設定します。

オプション	説明
名前	ルールの名前を入力します。
状態	作成時にルールを有効にするには、[状態] 切り替えを有効にします。
アプリケーション	(オプション) ルールが適用される特定のポート プロファイルを選択するには、[アプリケーション] 切り替えを有効にして、[保存] をクリックします。
ソース	<p>オプションを選択し、[保持] をクリックします。</p> <ul style="list-style-type: none"> ■ 任意のソース アドレスからのトラフィックを許可または拒否するには、[任意のソース] 切り替えをオンにします。 ■ 特定のファイアウォール グループからのトラフィックを許可または拒否するには、リストからファイアウォール グループを選択します。
ターゲット	<p>オプションを選択し、[保持] をクリックします。</p> <ul style="list-style-type: none"> ■ 任意のターゲット アドレスへのトラフィックを許可または拒否するには、[任意のターゲット] を有効に切り替えます。 ■ 特定のファイアウォール グループからのトラフィックを許可または拒否するには、リストからファイアウォール グループを選択します。
アクション	<p>[アクション] ドロップダウン メニューからオプションを選択します。</p> <ul style="list-style-type: none"> ■ 指定されたソース、ターゲット、およびサービスとの間のトラフィックを許可するには、[承諾] を選択します。 ■ 指定されたソース、ターゲット、およびサービスとの間のトラフィックをブロックするには、[拒否] を選択します。
IP プロトコル	IPv4 または IPv6 のトラフィックにルールを適用するかどうかを選択します。
方向	ルールを適用するトラフィックの方向を選択します。
ログの有効化	このルールによって実行されたアドレス変換をログに記録するには、[ログの有効化] 切り替えをオンにします。

7 [保存] をクリックします。

8 追加のルールを設定するには、これらの手順を繰り返します。

結果

ファイアウォール ルールが作成されると、Edge Gateway のファイアウォール ルールのリストに表示されます。必要に応じて、ルールを上に移動、下に移動、編集、または削除できます。

NSX-T Edge Gateway での SNAT ルールまたは DNAT ルールの追加

ソース IP アドレスをプライベート IP アドレスからパブリック IP アドレスに変更するには、ソース NAT (SNAT) ルールを作成します。ターゲット IP アドレスをパブリック IP アドレスからプライベート IP アドレスに変更するには、ターゲット NAT (DNAT) ルールを作成します。

vCloud Director 環境の Edge Gateway で SNAT ルールまたは DNAT ルールを設定する場合は、常に組織 VDC の観点からルールを設定します。SNAT ルールでは、組織 VDC ネットワークから送信されたパケットのソース IP アドレスを外部ネットワークまたは別の組織 VDC ネットワークに変換します。DNAT ルールでは、外部ネットワークまたは別の組織 VDC ネットワークから発信されて組織 VDC ネットワークが受信したパケットの IP アドレスとオプションでポートを変換します。

前提条件

パブリック IP アドレスを、ルールを追加する Edge Gateway インターフェイスに追加しておく必要があります。

手順

- 1 [ネットワーク] > [エッジ] の順に選択します。
- 2 Edge Gateway をクリックして、[NAT] をクリックします。
- 3 ルールを追加するには、[追加] をクリックします。
- 4 ソース NAT ルール（内部から外部へ）を構成します。

オプション	説明
名前	ルールの名前を入力します。
状態	作成時にルールを有効にするには、[状態] トグルをオンにします。
インターフェイス タイプ	ルールを適用するインターフェイスを選択します。
外部 IP	SNAT ルールを設定する Edge Gateway のパブリック IP アドレスを入力します。
内部 IP	SNAT を設定する仮想マシンの IP アドレスまたは IP アドレス範囲を入力し、外部ネットワークにトラフィックを送信できるようにします。
ログの有効化	このルールによって実行されたアドレス変換をログに記録するには、[ログの有効化] 切り替えをオンにします。

5 ターゲット NAT ルール（外部から内部へ）を構成します。

オプション	説明
名前	ルールの名前を入力します。
状態	作成時にルールを有効にするには、[状態] トグルをオンにします。
インターフェイス タイプ	ルールを適用するインターフェイスを選択します。
外部 IP	DNAT ルールを設定する Edge Gateway のパブリック IP アドレスを入力します。 入力した IP アドレスは、Edge Gateway の細分割り当てされた IP アドレス範囲に属している必要があります。
アプリケーション	(オプション) ルールを適用する特定のアプリケーション ポート プロファイルを選択します。 アプリケーション ポート プロファイルには、内部ネットワークに接続するために、Edge Gateway で受信トラフィックが使用するポートとプロトコルが含まれています。
内部 IP	DNAT を設定する仮想マシンの IP アドレスまたは IP アドレス範囲を入力し、外部ネットワークからトラフィックを受信できるようにします。
内部ポート	(オプション) DNAT ルールが仮想マシンで受信したパケットの変換先としているポートまたはポート範囲を選択します。
ログの有効化	このルールによって実行されたアドレス変換をログに記録するには、[ログの有効化] 切り替えをオンにします。

6 [保存] をクリックします。

7 追加のルールを設定するには、これらの手順を繰り返します。

NSX-T Edge Gateway での DNS フォワーダ サービスの設定

DNS クエリを外部 DNS サーバに転送するには、DNS フォワーダを設定します。

DNS フォワーダ サービスを設定するときに、条件付きフォワーダ ゾーンを追加することもできます。条件付きフォワーダ ゾーンは、最大 5 つの FQDN DNS ゾーンを含むリストとして設定されます。DNS クエリがこのリスト内のドメイン名と一致する場合、クエリは対応するフォワーダ ゾーンからサーバに転送されます。

手順

- 1 [ネットワーク] > [エッジ] の順に選択します。
- 2 Edge Gateway をクリックし、[サービス] をクリックします。
- 3 [DNS] をクリックし、[DNS フォワーダ] セクションで [編集] をクリックします。
- 4 DNS フォワーダ サービスを有効にするには、[状態] 切り替えを有効にします。
- 5 デフォルト DNS ゾーンの名前と、オプションで説明を入力します。
- 6 1 つ以上のアップストリーム サーバの IP アドレスをカンマで区切って入力します。
- 7 [保存] をクリックします。

- 8 (オプション) 条件付きフォワーダ ゾーンを追加します。
 - a [条件付きフォワーダ ゾーン] セクションで、[追加] をクリックします。
 - b フォワーダ ゾーンの名前を入力します。
 - c 1つ以上のアップストリーム サーバの IP アドレスをカンマで区切って入力します。
 - d 1つ以上のドメイン名をカンマで区切って入力し、[保存] をクリックします。

カスタム アプリケーション ポート プロファイルの作成

ファイアウォール ルールと NAT ルールを作成するには、事前構成されたアプリケーション ポート プロファイルとカスタム アプリケーション ポート プロファイルを使用します。

アプリケーション ポート プロファイルには、プロトコルと、ポートまたはポートのグループの組み合わせが含まれます。ポート グループは、Edge Gateway のファイアウォール サービスおよび NAT サービスに使用されます。NSX-T Data Center に事前設定されたデフォルトのポート プロファイルに加えて、カスタム アプリケーション ポート プロファイルを作成できます。

Edge Gateway にカスタム アプリケーション ポート プロファイルを作成すると、同じ組織 VDC 内にある他のすべての NSX-T Data Center Edge Gateway からそのプロファイルを表示できるようになります。

手順

- 1 [ネットワーク] > [エッジ] の順に選択します。
- 2 Edge Gateway をクリックし、[セキュリティ] タブをクリックします。
- 3 [アプリケーション ポート プロファイル] をクリックします。
- 4 [カスタム アプリケーション] セクションで [新規] をクリックします。
- 5 アプリケーション ポート プロファイルの名前と、オプションで説明を入力します。
- 6 ドロップダウン メニューからプロトコルを選択します。
- 7 ポートまたはポートの範囲をカンマ区切りで入力し、[保存] をクリックします。

次のステップ

アプリケーション ポート プロファイルを使用して、ファイアウォール ルールと NAT ルールを作成します。[NSX-T Edge Gateway ファイアウォール ルールの追加](#)および[NSX-T Edge Gateway での SNAT ルールまたは DNAT ルールの追加](#)を参照してください。

名前付きディスクの使用およびストレージ ポリシーの確認

8

vCloud Director テナント ポータルを使用して名前付きディスクを作成および管理し、組織仮想データセンターのストレージ ポリシーを確認することができます。

この章には、次のトピックが含まれています。

- 名前付きディスクの作成および使用
- ストレージ ポリシーのプロパティの確認

名前付きディスクの作成および使用

名前付きディスクとは、組織 VDC 内に作成されたスタンドアローンの仮想ディスクのことです。組織管理者およびそれぞれの権限を持つユーザーは、名前付きディスクを作成、削除、および更新したり、仮想マシンに接続したりできます。

名前付きディスクを作成すると、作成したディスクには仮想マシンでなく、組織 VDC が関連付けられます。VDC 内にディスクを作成した後、ディスクの所有者または管理者はこのディスクを VDC 内にデプロイされた任意の仮想マシンに接続できます。ディスクの所有者はディスク プロパティの変更、仮想マシンからの切断、および VDC からの削除を行うこともできます。システム管理者と組織管理者は、ディスクの所有者と同じ権限を持ち、ディスクを使用および変更することができます。

名前付きディスクの作成

名前付きディスクを作成し、後の段階で仮想マシンに接続することができます。

名前付きディスクを作成するには、名前とサイズを指定する必要があります。必要に応じて説明を追加し、ディスクで使用するストレージ プロファイルを選択できます。

前提条件

組織管理者ロール、またはディスク所有者の権限が必要です。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルの [ストレージ] で [名前付きディスク] を選択します。
- 2 [新規] をクリックします。
- 3 ディスクの名前と、必要に応じて説明を入力します。

- 4 [ストレージ ポリシー] ドロップダウン メニューから、ストレージ ポリシーを選択します。
- 5 名前付きディスクのサイズをバイト単位で入力します。
- 6 [バス タイプ] および [バス サブタイプ] ドロップダウン メニューでバス タイプおよびサブタイプをそれぞれ選択し、[保存] をクリックします。

次のステップ

vCloud API を使用して、仮想マシンに独立ディスクを接続します。VMware `{code}` の「サービス プロバイダ向け vCloud API プログラミング ガイド」を参照してください。

名前付きディスクの編集

ディスクを作成した後に、ディスクの名前、説明、ストレージ ポリシー、およびサイズを変更できます。

前提条件

組織管理者ロール、またはディスク所有者の権限が必要です。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルの [ストレージ] で [名前付きディスク] を選択します。
- 2 変更するディスクを選択して、[編集] をクリックします。
- 3 名前、説明、ストレージ ポリシー、およびサイズ（バイト単位）などの設定を編集します。
- 4 [保存] をクリックします。

仮想マシンへの名前付きディスクの接続

VDC 内に名前付きディスクを作成した後に、そのディスクを VDC にデプロイされている任意の仮想マシンに接続できます。

前提条件

組織管理者ロール、またはディスク所有者の権限が必要です。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルの [ストレージ] で [名前付きディスク] を選択します。
- 2 仮想マシンに接続する名前付きディスクの名前の横にあるラジオ ボタンをクリックして、[接続] をクリックします。
- 3 ドロップダウン メニューから名前付きディスクを接続する仮想マシンを選択し、[適用] をクリックします。

結果

名前付きディスクが仮想マシンに接続されます。

次のステップ

仮想マシンに接続する名前付きディスクは、必要に応じて追加や接続解除をすることが可能です。

名前付きディスクの削除

名前付きディスクが不要な場合は、削除できます。

前提条件

組織管理者ロール、またはディスク所有者の権限が必要です。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックし、左側のパネルの [ストレージ] で [名前付きディスク] を選択します。
- 2 削除するディスクを選択して、[削除] をクリックします。
- 3 [OK] をクリックします。

ストレージ ポリシーのプロパティの確認

ストレージ ポリシーおよびストレージ ポリシーの詳細を確認できます。

前提条件

この操作には、事前定義の組織管理者ロールに含まれている権限、またはそれに相当する権限が必要です。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックします。
- 2 [ストレージ] で [ストレージ ポリシー] をクリックします。
使用可能なストレージ ポリシーのリストが表示されます。
- 3 ストレージ ポリシーの詳細を表示するには、ストレージ ポリシーの名前をクリックします。
- 4 [全般] タブおよび [メタデータ] タブで詳細を確認し、[OK] をクリックします。

仮想データセンターのプロパティの確認

9

組織管理者として、仮想データセンターのプロパティを確認できます。

この章には、次のトピックが含まれています。

- 仮想データセンターのプロパティの確認
- 仮想データセンターのメタデータの確認

仮想データセンターのプロパティの確認

組織に割り当てられた仮想データセンターのプロパティを確認できます。

前提条件

この操作には、事前定義の組織管理者ロールに含まれている権限、またはそれに相当する権限が必要です。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックします。
- 2 [設定] で、[全般] をクリックします。

結果

名前、説明、ステータスなど、仮想データセンターのプロパティを確認できます。データセンターに関するメトリック情報には、割り当てモデル、vCPU のほか、CPU、およびメモリ使用率も含まれます。

仮想データセンターのメタデータの確認

vCloud Director には、ユーザー定義メタデータをオブジェクトに関連付けるための汎用機能があります。システム管理者が組織仮想データセンターのメタデータを作成した場合は、組織データセンターのメタデータを確認できます。

前提条件

この操作には、事前定義の組織管理者ロールに含まれている権限、またはそれに相当する権限が必要です。

手順

- 1 [仮想データセンター] ダッシュボード画面で、確認する仮想データセンターのカードをクリックします。

2 [設定] で [メタデータ] をクリックします。

使用可能なメタデータのリストが表示されます。

専用 vCenter Server インスタンスおよびプロキシの操作

10

vCloud Director 9.7 以降では、vCloud Director から専用 vCenter Server 環境にアクセスできます。vCloud Director は HTTP プロキシ サーバとして機能し、基盤となる vSphere 環境からコンポーネントにアクセスできるようにします。

vCloud Director では、Software-Defined Data Center (SDDC) によって専用 vCenter Server 環境全体がカプセル化されます。専用 vCenter Server インスタンスに、基盤となる環境からさまざまなコンポーネントへのアクセスを可能にする 1 つ以上のプロキシを含めることができます。

[システム管理者]は 1 つ以上の専用 vCenter Server インスタンスを組織に公開できます。ユーザーは含まれているプロキシを使用して、プロキシが設定されたコンポーネントのユーザー インターフェイスまたは API にアクセスできます。

この章には、次のトピックが含まれています。

- [プロキシ設定を使用したブラウザの設定](#)
- [プロキシが設定されたコンポーネントのユーザー インターフェイスへのログイン](#)

プロキシ設定を使用したブラウザの設定

プロキシが設定された vSphere コンポーネントのユーザー インターフェイスにアクセスするには、組織に公開されるプロキシを設定しておく必要があります。

公開されたプロキシを使用するようにブラウザを設定するには、プロキシの自動設定 (PAC) ファイルの URL をブラウザにコピーします。

注： システム管理者が専用の vSphere データセンターを組織に公開する場合、または専用の vSphere データセンターの 1 つにプロキシを追加する場合、指定された URL から PAC をブラウザが再度取得するまで数分かかる可能性があります。ブラウザを強制的に更新するには、この手順を繰り返します。

前提条件

- システム管理者が、1 つ以上の有効な専用 vCenter Server インスタンスを組織に公開していることを確認します。
- システム管理者が組織に SDDC_VIEW 権限およびトークン: 管理権限を公開していて、自分のロールにこれらの権限が含まれていることを確認します。

- システム管理者が [CPOM 拡張機能] プラグインを組織に公開し、有効にしていることを確認します。このプラグインは、vCloud Director Tenant Portal で専用 vSphere データセンターを表示して使用するための機能を提供します。

手順

- 1 メイン メニュー (≡) で [データセンター] を選択します。
- 2 [専用 vSphere データセンター] ペインで、[ここをクリックしてプロキシ設定ガイドを表示] をクリックします。
- 3 PAC の URL をコピーし、[次へ] をクリックします。
- 4 指示に従って、PAC の URL を参照するようにブラウザを構成します。
- 5 プロキシが設定されたコンポーネントで自己署名証明書が使用されている場合は、ブラウザに証明書をインポートします。
 - a ターゲットの vSphere データセンター カードで [アクション] をクリックし、[証明書のインポート] をクリックします。
 - b 証明書と証明書失効リスト (CRL) をダウンロードします。
 - c ダウンロードした証明書をブラウザにインポートします。

ご使用のブラウザに関するユーザー手順を参照してください。

プロキシが設定されたコンポーネントのユーザー インターフェイスへのログイン

vCloud Director アカウントを使用して、プロキシが設定されたコンポーネントのユーザー インターフェイスにアクセスできます。

前提条件

プロキシが設定されたコンポーネントのユーザー インターフェイスにログインする前に、プロキシへのアクセスを設定する必要があります。 [プロキシ設定を使用したブラウザの設定](#) を参照してください。

手順

- 1 メイン メニュー (≡) で [データセンター] を選択します。
- 2 [専用 vSphere データセンター] タブをクリックします。
- 3 専用 vCenter Server インスタンスのプロキシを開きます。
 - デフォルトのプロキシを開くには、[vSphere を開く] をクリックします。
 - デフォルト以外のプロキシを開くには、次の手順を実行します。
 - [アクション] をクリックし、[プロキシの表示] をクリックします。

- プロキシの URL をクリックします。

プロキシ認証情報を含む新しいカードが開きます。

- 4 ユーザー名とパスワードをコピーします。
- 5 プロキシを有効にするには、[開く] をクリックします。

新しいカードが開き、プロキシに対して認証するよう求めるプロンプトが表示されます。

- 6 [ユーザー名] テキスト ボックスに、コピーしたユーザー名を貼り付けます。
- 7 [パスワード] テキスト ボックスにコピーしたパスワードを貼り付けて、[OK] をクリックします。

結果

プロキシされたコンポーネントのユーザー インターフェイスが開きます。

vApp テンプレートの操作

11

vApp テンプレートとは、オペレーティング システム、アプリケーション、およびデータと共に読み込まれる仮想マシンのイメージです。これらのテンプレートにより、組織全体で仮想マシンの構成に一貫性を持たせることができます。vApp テンプレートはカタログに追加されます。

この章には、次のトピックが含まれています。

- vApp テンプレートの表示
- OVF ファイルからの vApp テンプレートの作成
- vApp テンプレートへの仮想マシン配置ポリシーと仮想マシン サイズ変更ポリシーの割り当て
- vApp テンプレートのダウンロード
- vApp テンプレートの削除

vApp テンプレートの表示


カタログで使用可能な、アクセス権のある vApp テンプレートのリストを表示できます。vApp テンプレートを表示し、そこに含まれる仮想マシンを確認することができます。

カタログ項目として含まれている vApp テンプレートのうち、自分に共有されているもののみにアクセスできます。カタログの共有の詳細については、[カタログを共有](#)を参照してください。


前提条件

この操作には、事前定義の vApp 作成者ロールに含まれている権限、またはそれに相当する権限が必要です。

手順

- 1 メイン メニュー () で [ライブラリ] を選択し、左側のパネルで [vApp テンプレート] を選択します。
テンプレートのリストがグリッド ビューに表示されます。

2 (オプション) 表示する要素を含むようにグリッド ビューを設定します。

- a グリッド ビューで、vApp テンプレートのリストの下にあるグリッド エディタ アイコン () をクリックします。
- b バージョン、ステータス、カタログ、所有者など、グリッド ビューに追加する要素を選択します。
- c [OK] をクリックします。

グリッドには、リスト内の各 vApp テンプレートについて選択した要素が表示されます。

3 vApp テンプレートに含まれている仮想マシンを表示するには、vApp テンプレートの名前をクリックします。

vApp テンプレートに含まれている仮想マシンがグリッドに表示されます。

4 (オプション) グリッド ビューに表示する要素を選択するには、仮想マシンのリストの下にあるグリッド エディタ アイコン () をクリックします。

- a グリッド ビューに追加する要素を選択します。
- b [OK] をクリックします。

OVF ファイルからの vApp テンプレートの作成



OVF パッケージをアップロードして、カタログに vApp テンプレートを作成できます。

vCloud Director は Open Virtualization Format (OVF) および Open Virtualization Appliance (OVA) の仕様をサポートします。仮想マシンをカスタマイズするための OVF プロパティを含む OVF ファイルをアップロードする場合、これらのプロパティは vApp テンプレートに保存されます。OVF パッケージの作成については、『OVF Tool User Guide』および『VMware vCenter Converter User's Guide』を参照してください。

前提条件

この操作には、事前定義のカタログ作成者ロールに含まれている権限、またはそれに相当する権限が必要です。

手順

- 1 メイン メニュー () で [ライブラリ] を選択し、左側のパネルで [vApp テンプレート] を選択します。
テンプレートのリストがグリッド ビューに表示されます。
- 2 [追加] をクリックします。
- 3 OVF ファイルの URL アドレスを入力するか、[アップロード] アイコン () をクリックしてコンピュータからアクセス可能な場所を参照し、OVF/OVA テンプレート ファイルを選択します。

アクセス可能な場所にはローカルのハード ドライブ、ネットワーク共有、または CD/DVD ドライブなどがあります。サポートされているファイル拡張子は、.ova、.ovf、.vmdk、.mf、.cert、.strings です。アップロードするファイルよりも多くのファイル (たとえば VMDK ファイル) を参照する OVF ファイルをアップロードするように選択した場合は、すべてのファイルを参照して選択する必要があります。
- 4 デプロイする OVF/OVA テンプレートの詳細を確認し、[次へ] をクリックします。

- 5 vApp テンプレートの名前と、必要に応じて説明を入力して、[次へ] をクリックします。
- 6 [カタログ] ドロップダウン メニューから、テンプレートを追加するカタログを選択します。
- 7 vApp テンプレートの設定を確認し、[終了] をクリックします。

結果

新しい vApp テンプレートがテンプレート グリッド ビューに表示されます。

vApp テンプレートへの仮想マシン配置ポリシーと仮想マシン サイズ変更ポリシーの割り当て

vApp テンプレートの仮想マシンを特定の仮想マシン配置ポリシーおよび仮想マシン サイズ設定ポリシーに関連付けるには、割り当てるポリシーを vApp テンプレートの個々の仮想マシンにタグ付けします。

vCloud Director 10.0 以降では、ユーザーが仮想マシンの編集集中に事前定義された仮想マシン配置ポリシーまたは仮想マシン サイズ変更ポリシーを変更できるようになりました。

注： vCloud Director 10.0 にアップグレードすると、すべての既存のテンプレート タグ付けを変更できるようになります。事前定義された仮想マシン配置ポリシーまたは仮想マシン サイズ変更ポリシーの変更を許可しない場合は、変更を許可しないポリシーの [変更可能] チェックボックスの選択を解除する必要があります。

前提条件

- この操作には、vApp テンプレートを編集する権限が必要です。
- vCloud Director 環境内に 1 つ以上の vApp テンプレートがあることを確認します。

手順

- 1 メイン メニュー (≡) で [ライブラリ] を選択し、左側のパネルで [vApp テンプレート] を選択します。
テンプレートのリストがグリッド ビューに表示されます。
- 2 タグを付ける vApp テンプレートの横にあるラジオ ボタンを選択し、[コンピューティング ポリシーを使用したタグ付け] をクリックします。
- 3 仮想マシン配置ポリシーを vApp テンプレートの仮想マシンに割り当てる場合は、仮想マシンに対応する行の [仮想マシン配置ポリシー] ドロップダウン メニューからポリシーを選択します。
- 4 仮想マシン サイズ変更ポリシーを vApp テンプレートの仮想マシンに割り当てる場合は、仮想マシンに対応する行の [仮想マシン サイズ変更ポリシー] ドロップダウン メニューからポリシーを選択します。
- 5 (オプション) 仮想マシンの編集集中にユーザーが事前定義済みの仮想マシン配置ポリシーまたは仮想マシン サイズ変更ポリシーを変更できるようにするには、ポリシーのドロップダウン メニューの下にある [変更可能] チェックボックスをオンにします。
- 6 [タグ] をクリックします。

vApp テンプレートのダウンロード

カタログから vApp テンプレートを OVA ファイルとしてローカル マシンにダウンロードできます。

前提条件

この操作には、事前定義のカタログ作成者ロールに含まれている権限、またはそれに相当する権限が必要です。

手順

- 1 メイン メニュー (≡) で [ライブラリ] を選択し、左側のパネルで [vApp テンプレート] を選択します。
テンプレートのリストがグリッド ビューに表示されます。

- 2 ダウンロードする vApp テンプレートの左側にあるリスト バー (⋮) をクリックして、[ダウンロード] を選択します。

注： 組織のカタログから vApp テンプレートをダウンロードできます。組織の管理者は、公開カタログから vApp テンプレートをダウンロードできます。それ以外のユーザーには [ダウンロード] ボタンがグレイアウトで表示されます。

- 3 (オプション) ダウンロードされた OVA パッケージ内の仮想マシンの UUID および MAC アドレスを保存するには、[ID 情報の保存] チェックボックスを選択します。

- 4 [OK] をクリックして、インストールが完了するのを待ちます。

OVA ファイルは、Web ブラウザのデフォルトのダウンロード場所に保存されます。

vApp テンプレートの削除

組織カタログから vApp テンプレートを削除できます。カタログが公開されている場合は、公開カタログからも vApp テンプレートが削除されます。

前提条件

この操作には、事前定義の vApp 作成者ロールに含まれている権限、またはそれに相当する権限が必要です。

手順

- 1 メイン メニュー (≡) で [ライブラリ] を選択し、左側のパネルで [vApp テンプレート] を選択します。
テンプレートのリストがグリッド ビューに表示されます。

- 2 削除する vApp テンプレートの左側にあるリスト バー (⋮) をクリックして、[削除] を選択します。

- 3 削除を確認します。

削除した vApp テンプレートは、グリッド ビューから削除されます。

メディア ファイルの操作

12

カタログを使用して、メディア ファイルのアップロード、コピー、移動、プロパティの編集ができます。

この章には、次のトピックが含まれています。

- メディア ファイルのアップロード
- メディア ファイルの削除
- メディア ファイルのダウンロード

メディア ファイルのアップロード

新しいメディア ファイルや、既存のメディア ファイルの新しいバージョンをカタログにアップロードできます。カタログにアクセスできるユーザーは、その仮想マシンでメディア ファイルを開くことができます。

前提条件

この操作には、事前定義のカタログ作成者ロールに含まれている権限、またはそれに相当する権限が必要です。

手順

- 1 メイン メニュー (≡) で [ライブラリ] を選択し、左側のパネルで [メディアとその他] を選択します。
メディア ファイルのリストがグリッド ビューに表示されます。
- 2 [追加] をクリックします。
- 3 [カタログ] ドロップダウン メニューから、メディア ファイルをアップロードするカタログを選択します。
- 4 メディア ファイルの名前を入力します。
名前を入力しない場合は、メディア ファイルの名前を基に [名前] テキスト ボックスに自動的に入力されます。
- 5 アップロード アイコン (↑) をクリックして、ディスク イメージ ファイル (.iso ファイルなど) を参照し、選択します。
- 6 [OK] をクリックします。
アップロードが開始すると、メディア ファイルがグリッドに表示されます。

次のステップ

ファイルのサイズによっては、アップロードが完了するまでしばらくかかる場合があります。ダウンロードのステータスは、[最近のタスク] ビューで監視できます。詳細については、[タスクの表示](#)を参照してください。


メディア ファイルの削除

不要になったメディア ファイルをカタログから削除できます。


前提条件

この操作には、事前定義のカタログ作成者ロールに含まれている権限、またはそれに相当する権限が必要です。

手順

- 1 メイン メニュー () で [ライブラリ] を選択し、左側のパネルで [メディアとその他] を選択します。

メディア ファイルのリストがグリッド ビューに表示されます。

- 2 削除するメディア ファイルの左側にあるリスト バー () をクリックして、[削除] を選択します。

- 3 削除を確認します。

削除したメディア ファイルは、グリッド ビューから削除されます。

メディア ファイルのダウンロード

メディア ファイルをカタログからダウンロードできます。

前提条件

この操作には、事前定義のカタログ作成者ロールに含まれている権限、またはそれに相当する権限が必要です。

手順

- 1 メイン メニュー () で [ライブラリ] を選択し、左側のパネルで [メディアとその他] を選択します。

メディア ファイルのリストがグリッド ビューに表示されます。

- 2 ダウンロードするメディア ファイルの左側にあるリスト バー () をクリックして、[ダウンロード] を選択します。

ダウンロード タスクが開始し、Web ブラウザのデフォルトのダウンロード場所にファイルが保存されます。

次のステップ

ファイルのサイズによっては、ダウンロードが完了するまでしばらくかかる場合があります。ダウンロードのステータスは、[最近のタスク] パネルで監視できます。詳細については、[タスクの表示](#)を参照してください。

カタログとは、組織内の vApp テンプレートおよびメディア ファイルのコンテナです。組織管理者およびカタログ作成者は組織内でカタログを作成できます。カタログ コンテンツは、vCloud Director インストール環境内のその他のユーザーまたは組織と共有したり、vCloud Director インストール環境外の組織がアクセスできるよう、外部公開したりできます。

vCloud Director には、プライベート カatalog、共有カタログ、および外部からアクセス可能なカタログが含まれています。プライベート カatalog には、組織の他のユーザーと共有できる vApp テンプレートおよびメディア ファイルが含まれます。システム管理者が組織に対してカタログ共有を有効にすると、組織カタログを共有し、vCloud Director インストール環境内の他の組織がアクセスできるカタログを作成できます。システム管理者が組織に対してカタログの外部公開を有効にすると、vCloud Director インストール環境外の組織がアクセスできるよう、組織カタログを公開することができます。vCloud Director インストール環境外の組織が外部に公開されたカタログのコンテンツにアクセスするには、そのカタログをサブスクライブする必要があります。

OVF パッケージは、カタログに直接アップロードすることができます。また、vApp を vApp テンプレートとして保存したり、vApp テンプレートを vSphere からインポートすることもできます。[OVF ファイルからの vApp テンプレートの作成](#) および [vApp の vApp テンプレートとしてのカタログへの保存](#) を参照してください。

組織のメンバーは、所有または共有の vApp テンプレートおよびメディア ファイルにアクセスできます。組織管理者とシステム管理者は、組織内の全ユーザーとカタログを共有したり、組織内の特定のユーザーおよびグループとカタログを共有したりすることができます。[カタログを共有](#) を参照してください。

この章には、次のトピックが含まれています。



- [カタログの表示](#)
- [カタログの作成](#)
- [カタログを共有](#)
- [カタログの削除](#)
- [カタログのメタデータの管理](#)
- [カタログを発行](#)
- [外部カタログへのサブスクライブ](#)
- [サブスクライブしたカタログの場所の URL とパスワードの更新](#)
- [サブスクライブしたカタログの同期](#)

カタログの表示

組織内で共有されているカタログにアクセスできます。公開カタログには、組織管理者が組織内でのアクセスを許可している場合にアクセスできます。

カタログへのアクセスは、各自のロールの権限ではなく、カタログの共有によって制御されます。共有されているカタログまたはカタログ項目のみにアクセスできます。詳細については、[カタログを共有](#)を参照してください。

手順

- 1 メイン メニュー (≡) で [ライブラリ] を選択し、左側のパネルで [カタログ] を選択します。
カタログのリストがグリッド ビューに表示されます。
- 2 (オプション) 表示する要素を含むようにグリッド ビューを設定します。
 - a グリッド ビューから、カタログのリストの下に表示されるグリッド エディタのアイコン () をクリックします。
 - b バージョン、説明、ステータスなど、グリッド ビューに含める要素を選択します。
 - c [OK] をクリックします。
 グリッドには、各カタログについて選択した要素が表示されます。
- 3 (オプション) 各カタログで実行できるアクションを表示するには、グリッド ビューでリスト バー () を使用します。
たとえば、カタログを共有したり削除したりできます。

カタログの作成

新規カタログを作成し、ストレージ ポリシーに関連付けることができます。

前提条件

この操作には、事前定義のカタログ作成者ロールに含まれている権限、またはそれに相当する権限が必要です。

手順

- 1 メイン メニュー (≡) で [ライブラリ] を選択し、左側のパネルで [カタログ] を選択します。
カタログのリストがグリッド ビューに表示されます。
- 2 [新規] をクリックして、新規カタログを作成します。
- 3 カatalogの名前と、必要に応じて説明を入力します。
- 4 (オプション) カatalogにストレージ ポリシーを割り当てるかどうかを選択し、ストレージ ポリシーを選択します。
- 5 [OK] をクリックします。

結果

新規カタログは、[カタログ] タブで、グリッド ビューに表示されます。

カタログを共有

カタログは、組織のすべてのメンバーまたは特定のメンバーと共有できます。

前提条件

- この操作には、事前定義のカタログ作成者ロールに含まれている権限、またはそれに相当する権限が必要です。
- カatalogの所有者である必要があります。

手順

- 1 メイン メニュー (≡) で [ライブラリ] を選択し、左側のパネルで [カタログ] を選択します。
カタログのリストがグリッド ビューに表示されます。
- 2 共有するカタログの左側にあるリスト バー (⋮) をクリックして、[共有] を選択します。
[カタログを共有] ウィンドウのグリッド ビューに、カタログにアクセスできるユーザーのリストが表示されます。
- 3 他のユーザーとカタログを共有するには、[追加] をクリックします。

オプション	説明
この組織内の全員で共有	組織内のすべてのユーザーおよびグループにアクセス権を付与します。
特定のユーザーおよびグループで共有	カタログへのアクセス権を付与するユーザーまたはグループを選択して、[追加]をクリックします。

- 4 アクセス レベルを選択します。

オプション	説明
読み取り専用	このカタログにアクセスできるユーザーは、カタログの vApp テンプレートおよび ISO ファイルへの読み取りアクセス権を有します。
読み取り/書き込み	このカタログにアクセスできるユーザーは、カタログの vApp テンプレートおよび ISO ファイルへの読み取りアクセス権を所有し、vApp テンプレートおよび ISO ファイルをカタログに追加することができます。
完全コントロール	このカタログにアクセスできるユーザーは、カタログのコンテンツおよび設定を完全にコントロールすることができます。

- 5 [OK] をクリックします。
[カタログを共有] ダイアログ ボックスのグリッド ビューに、カタログにアクセスできるようになったユーザーまたはグループが表示されます。
- 6 (オプション) その他のすべての組織の管理者と読み取り専用アクセス権を共有するように選択します
- 7 [保存] をクリックします。

結果

[カタログ] タブのグリッド ビューで、このカタログの [共有] ステータスが変更されます。

カタログの削除

組織からカタログを削除できます。

前提条件

この操作には、事前定義のカタログ作成者ロールに含まれている権限、またはそれに相当する権限が必要です。

注： カatalogには、vApp テンプレートやメディア ファイルが含まれていないようにする必要があります。これらの項目は、別のカタログに移動するか、削除することができます。

手順

- 1 メイン メニュー (≡) で [ライブラリ] を選択し、左側のパネルで [カタログ] を選択します。
カタログのリストがグリッド ビューに表示されます。
- 2 削除するカタログの左側にあるリスト バー (⋮) をクリックして、[削除] を選択します。
- 3 削除を確認します。
削除したカタログ項目は、グリッド ビューから削除されます。

カタログのメタデータの管理

組織管理者またはカタログの所有者は、所有するカタログのメタデータを作成または更新できます。

手順

- 1 メイン メニュー (≡) で [ライブラリ] を選択し、左側のパネルで [カタログ] を選択します。
カタログのリストがグリッド ビューに表示されます。
- 2 カatalogの左側にあるリスト バー (⋮) をクリックし、[メタデータ] を選択します。
選択したカタログのメタデータは、グリッド ビューに表示されます。
- 3 (オプション) メタデータを追加するには、[追加] をクリックします。
 - a メタデータ名を入力します。
名前は、このオブジェクトに関連付けられているメタデータ名内で一意にする必要があります。
 - b [テキスト]、[番号]、[日付と時刻]、[「はい」または「いいえ」] などのメタデータ タイプを選択します。
 - c メタデータ値を入力します。
 - d [保存] をクリックします。

4 (オプション) 既存のメタデータを更新します。

メタデータ名を更新することはできません。

- a メタデータ タイプを更新します。
- b 新しいメタデータ値を入力します。
- c [保存] をクリックします。

5 (オプション) 既存のメタデータを削除します。

- a 削除アイコンをクリックします。
- b [保存] をクリックします。

カタログを発行

システム管理者からカタログへのアクセスを許可された場合、カタログを外部に公開し、そのカタログの vApp テンプレートとメディア ファイルを、vCloud Director インストール環境外の組織のサブスクリプションで使用できます。

前提条件

システム管理者によって組織に対するカタログの外部公開が有効になっていて、カタログへのアクセス権が与えられていることを確認します。

手順

- 1 メイン メニュー (≡) で [ライブラリ] を選択し、左側のパネルで [カタログ] を選択します。
カタログのリストがグリッド ビューに表示されます。
- 2 公開するカタログの左側にあるリスト バー (⋮) をクリックして、[公開設定] を選択します。
- 3 [公開を有効化] を選択し、オプションでカタログ アクセス用のパスワードを入力します。
ASCII 文字のみがサポートされています。
- 4 [保存] をクリックします。

外部カタログへのサブスクライブ

外部カタログにサブスクライブして、外部に公開されたカタログの読み取り専用コピーを作成することができます。サブスクライブされたカタログは変更できません。

前提条件

- この操作には、事前定義の組織管理者ロールに含まれている権限、またはそれに相当する権限が必要です。
- システム管理者は、外部カタログにサブスクライブする権限を組織に付与する必要があります。

手順

- 1 メイン メニュー (☰) で [ライブラリ] を選択し、左側のパネルで [カタログ] を選択します。
カタログのリストがグリッド ビューに表示されます。
- 2 [新規] をクリックして、新規カタログを作成します。
- 3 カatalogの名前と、必要に応じて説明を入力します。
- 4 外部カタログへのサブスクライブを選択して、サブスクリプション URL を指定します。
- 5 パスワード（省略可）を入力して、カタログにアクセスします。
- 6 外部カタログからコンテンツを自動的にダウンロードするかどうかを選択します。
- 7 [OK] をクリックします。

サブスクライブしたカタログの場所の URL とパスワードの更新

サブスクライブしたカタログを作成してから、サブスクライブしたカタログの場所の URL とパスワードを更新できます。

前提条件

- この操作には、事前定義の組織管理者ロールに含まれている権限、またはそれに相当する権限が必要です。
- サブスクライブしたカタログが作成されている必要があります。
- システム管理者は、外部カタログにサブスクライブする権限を組織に付与する必要があります。

手順

- 1 メイン メニュー (☰) で [ライブラリ] を選択し、左側のパネルで [カタログ] を選択します。
カタログのリストがグリッド ビューに表示されます。
- 2 サブスクライブしたカタログの左側にあるリスト バー (⋮) をクリックして、[サブスクライブ設定] を選択します。
カタログをサブスクライブしていない場合、オプションはグレーアウトで表示されます。
- 3 サブスクライブしたこのカタログの場所の URL とパスワードを更新します。
- 4 外部カタログからコンテンツを自動的にダウンロードするかどうかを選択します。
- 5 [保存] をクリックします。



サブスクライブしたカタログの同期

サブスクライブしたカタログを作成してから、元のカatalogとの同期を行い、変更があるかどうかを確認することができます。たとえば、元のカatalogのメタデータが変更されている場合は、同期を実行すると、サブスクライブしたカタログのメタデータが更新されます。

前提条件

- この操作には、事前定義の組織管理者ロールに含まれている権限、またはそれに相当する権限が必要です。
- サブスクライブしたカタログが作成されている必要があります。
- システム管理者は、外部カタログにサブスクライブする権限を組織に付与する必要があります。

手順

- 1 メイン メニュー () で [ライブラリ] を選択し、左側のパネルで [カタログ] を選択します。
カタログのリストがグリッド ビューに表示されます。
- 2 サブスクライブしたカタログの左側にあるリスト バー () をクリックして、[同期] を選択します。
カタログをサブスクライブしていない場合、オプションはグレーアウトで表示されます。
サブスクライブしたカタログが元のカタログと同期されます。

組織仮想データセンター テンプレートの操作

14

組織管理者、または組織仮想データセンター テンプレートを表示してインスタンス化する権限を持つすべてのロールでは、追加の組織仮想データセンターを作成できます。

組織仮想データセンター テンプレートは、組織仮想データセンターと、オプションで Edge Gateway と組織仮想データセンター ネットワークの構成を指定します。システム管理者は、組織仮想データセンター テンプレートを作成して組織と共有することにより、組織管理者が組織内でこれらのリソースを作成できるようにします。

仮想データセンター テンプレートを作成して共有することで、システム管理者は、プロバイダ仮想データセンターや外部ネットワークなど、システム リソースの割り当てにおける管理制御を保持しながら、組織仮想データセンターのセルフサービス プロビジョニングを可能にできます。

システム管理者は、組織仮想データセンター テンプレートを作成し、さまざまな組織にテンプレートにアクセスする権限を付与します。

組織に仮想データセンター テンプレートへのアクセス権が付与されている場合は、vCloud Director Tenant Portal を使用して、使用可能なテンプレートから仮想データセンターを作成することができます。

この章には、次のトピックが含まれています。

- 使用可能な仮想データセンター テンプレートの表示
- テンプレートからの仮想データセンターの作成

使用可能な仮想データセンター テンプレートの表示

システム管理者が作成した組織仮想データセンター テンプレートを表示できます。

仮想データセンター テンプレートから新しい組織仮想データセンターを作成する前に、仮想データセンター テンプレートを表示します。

前提条件

この操作には、事前定義済みの組織管理者ロール、または組織仮想データセンター テンプレートを表示およびインスタンス化することができるロールに含まれている権限が必要になります。

手順

- ◆ メイン メニュー (≡) で [ライブラリ] を選択し、左側のパネルで [VDC テンプレート] を選択します。
仮想データセンター テンプレートのリストがグリッド ビューに表示されます。

次のステップ

組織仮想データセンター テンプレートの説明を確認して、新しい組織仮想データセンターの作成元になるテンプレートを選択します。

テンプレートからの仮想データセンターの作成

システム管理者が作成した仮想データセンター テンプレートから、組織仮想データセンターを作成することができます。

前提条件

この操作には、事前定義済みの組織管理者ロール、または組織仮想データセンター テンプレートを表示およびインスタンス化することができるロールに含まれている権限が必要になります。

手順

- 1 メイン メニュー (≡) で [ライブラリ] を選択し、左側のパネルで [VDC テンプレート] を選択します。
仮想データセンター テンプレートのリストがグリッド ビューに表示されます。
- 2 テンプレートを選択し、[新規の VDC] をクリックします。
- 3 仮想データセンターの名前と、オプションで説明を入力します。
- 4 [作成] をクリックします。

結果

新しい組織仮想データセンターの作成がインスタンス化されます。これには数分かかることがあります。[最近のタスク] パネルでタスクの進行状況を確認できます。

次のステップ

新しく作成した組織仮想データセンターは、ネットワークおよびセキュリティ設定などを管理する仮想マシン、vApp を作成して管理することができます。

ユーザー、グループ、ロールの管理

15

組織管理者は、個々に vCloud Director に追加することも、LDAP グループの一部として追加することもできます。また、組織内でユーザーが所有する権限を決定するロールを、追加したり変更したりすることもできます。

重要： 組織内のユーザー、グループ、およびロールを管理するには、組織管理者である必要があります。システム管理者は、1 つ以上のグローバル テナント ロールをテナントに公開できます。組織管理者は、公開されたロールをロールのリストで確認できます。たとえば、カタログ作成者、vApp 作成者、vApp ユーザー、組織管理者などのロールがあります。事前定義されたグローバル テナント ロールは変更できませんが、同様のカスタム テナント ロールを作成および更新して、テナント内のユーザーに割り当てることはできます。

この章には、次のトピックが含まれています。

- ユーザーの管理
- グループの管理
- ロールと権限

ユーザーの管理

テナント ポータルから、ユーザーを作成、編集、インポート、および削除することができます。また、ユーザーが無効なパスワードでログインを試みてユーザー アカウントがロックされた場合に、ユーザー アカウントのロックを解除することもできます。

ユーザーの作成

vCloud Director 組織内でユーザーを作成することができます。

前提条件

この操作には、事前定義の組織管理者ロールに含まれている権限、またはそれに相当する権限が必要です。

手順

- 1 メイン メニュー (☰) から、[管理] を選択します。
- 2 左側のパネルの [アクセス コントロール] で、[ユーザー] をクリックします。
ユーザーのリストが表示されます。
- 3 [作成] をクリックします。

4 (オプション) ユーザーのユーザー名とパスワード設定を入力します。

パスワードの最小文字数は 6 文字です。

5 作成時にユーザーを有効にするかどうかを選択します。

6 ユーザーに割り当てるロールを選択します。

[使用可能なロール] メニューは、事前定義ロール、およびユーザーまたはシステム管理者が作成したカスタムのロールのリストで構成されています。

事前定義ロール	説明
vApp 作成者	事前定義の vApp 作成者ロールに関連付けられた権限を持つユーザーは、カタログを使用し、vApp を作成できます。
コンソールのアクセスのみ	事前定義のコンソールのアクセスのみロールに関連付けられた権限を持つユーザーは、仮想マシンの状態およびプロパティを表示し、ゲスト OS を使用できます。
vApp ユーザー	事前定義の vApp ユーザーロールに関連付けられた権限を持つユーザーは、既存の vApp を使用できます。
組織管理者	事前定義の組織管理者ロールを持つユーザーは、vCloud Director テナント ポータルまたは vCloud API を使用して、組織内のユーザーとグループを管理し、(事前定義の組織管理者ロールを含む) ロールを割り当てることができます。組織管理者は、vCloud API を使用して、組織にローカルなロール オブジェクトを作成または更新できます。組織管理者によって作成または変更されたロールは、他の組織には表示されません。
ID プロバイダに準拠	事前定義の ID プロバイダに従うロールに関連付けられた権限は、ユーザーの OAuth または SAML ID プロバイダから受信した情報に基づいて決定されます。ユーザーに ID プロバイダに従うロールが割り当てられているときに包含の資格を得るには、ID プロバイダによって提供されたロール名が、組織内で定義されたロール名と大文字小文字も含めて完全に一致する必要があります。
カタログ作成者	事前定義のカタログ作成者ロールに関連付けられた権限を持つユーザーは、カタログを作成および公開できます。[]

7 (オプション) 名前、メール アドレス、電話番号、インスタント メッセージ ID などの連絡先情報を入力します。

8 (オプション) ユーザーの仮想マシン割り当て容量を入力します。

割り当て容量によって、ユーザーが管理できる仮想マシンと稼働中の仮想マシンの数が決定されます。ユーザーに提供する仮想マシンの数を制限しない場合は、[制限なし] を選択します。

9 [保存] をクリックします。

ユーザーのインポート

ユーザーを組織に追加するには、LDAP ユーザーまたは SAML ユーザーをインポートして特定のロールを割り当てます。

前提条件

- この操作には、事前定義の組織管理者ロールに含まれている権限、またはそれに相当する権限が必要です。
- LDAP サーバへの有効な接続があること、または [16 章 組織での SAML の ID プロバイダの使用の有効化](#) ことを確認します。

手順

- 1 メイン メニュー (≡) から、[管理] を選択します。
- 2 左側のパネルの [アクセス コントロール] で、[ユーザー] をクリックします。
ユーザーのリストが表示されます。
- 3 [ユーザーのインポート] をクリックします。
- 4 ユーザーをインポートするソースを選択します。
表示されるのは、ID プロバイダとして設定したソース LDAP サーバまたは SAML サーバのみです。

ソース	アクション
LDAP	LDAP サーバからユーザーをインポートします。 a テキスト ボックスに名前の全部または一部を入力し、[検索] をクリックします。 b インポートするユーザーを選択し、[追加] をクリックします。
SAML	SAML サーバからユーザーをインポートします。インポートするユーザーのユーザー名を入力します。 ユーザー名は、この組織に構成された SAML ID プロバイダがサポートする名前の識別子の形式でなければなりません。 注： vCenter Single Sign-On を SAML ID プロバイダとして使用している場合、vCenter Single Sign-On ドメインからインポートするユーザー名は、jdoe@mydomain.com のようなユーザー プリンシパル名 (UPN) 形式である必要があります。 ユーザー名ごとに新しい行を使用します。

- 5 インポートするユーザーに割り当てるロールを選択します。
- 6 [保存] をクリックします。

ユーザーの変更

組織の管理者は、既存のユーザーのパスワード、連絡先、および仮想マシンの割り当て容量の設定を変更できます。また、ユーザーのロールを変更することもできます。

前提条件

この操作には、事前定義の組織管理者ロールに含まれている権限、またはそれに相当する権限が必要です。

手順

- 1 メイン メニュー (≡) から、[管理] を選択します。
- 2 左側のパネルの [アクセス コントロール] で、[ユーザー] をクリックします。
ユーザーのリストが表示されます。
- 3 編集するユーザーの名前の横にあるラジオ ボタンをクリックして、[変更] をクリックします。

4 変更する設定を更新します。

- a 必要に応じてパスワードを変更します。
- b ユーザーを有効にするか無効にするかを選択します。
- c ユーザー ロールを更新します。
- d 名前、メール アドレス、電話番号、インスタント メッセージ ID などの連絡先情報を更新します。
- e ユーザーの仮想マシン割り当て容量を編集します。

5 [保存] をクリックします。

ユーザー アカウントの有効化または無効化

ユーザーが vCloud Director にログインできないようにするには、そのユーザーのアカウントを無効にします。ユーザーを削除するには、事前にそのアカウントを無効にする必要があります。

前提条件

この操作には、事前定義の組織管理者ロールに含まれている権限、またはそれに相当する権限が必要です。

手順

- 1 メイン メニュー (≡) から、[管理] を選択します。
- 2 左側のパネルの [アクセス コントロール] で、[ユーザー] をクリックします。
ユーザーのリストが表示されます。
- 3 ユーザー アカウントを無効にするには、ユーザー名の横にあるラジオ ボタンをクリックし、[無効化] をクリックして、アカウントを無効することを確認します。
- 4 すでに無効化されたユーザーアカウントを有効にするには、ユーザー名の横にあるラジオ ボタンをクリックし、[有効化] をクリックします。

ユーザーの削除

vCloud Director 組織からユーザーを削除するには、ユーザー アカウントを削除します。

前提条件

- この操作には、事前定義の組織管理者ロールに含まれている権限、またはそれに相当する権限が必要です。
- 削除するアカウントを無効にします。

手順

- 1 メイン メニュー (≡) から、[管理] を選択します。
- 2 左側のパネルの [アクセス コントロール] で、[ユーザー] をクリックします。
ユーザーのリストが表示されます。
- 3 削除するユーザーの名前の横にあるラジオ ボタンをクリックして、[削除] をクリックします。

- 4 ユーザー アカウントの削除を確定するには、[OK] をクリックします。

ロックされたユーザー アカウントのロック解除

vCloud Director 組織でロックアウト ポリシーを有効にしている場合、無効なログイン試行が一定の回数実行されると、そのユーザー アカウントはロックされます。ロックされたユーザー アカウントのロックは解除することができます。ベスト プラクティスは、ユーザーのパスワードを変更してから、アカウントのロックを解除することです。

前提条件

この操作には、事前定義の組織管理者ロールに含まれている権限、またはそれに相当する権限が必要です。

手順

- 1 メイン メニュー (≡) から、[管理] を選択します。
- 2 左側のパネルの [アクセス コントロール] で、[ユーザー] をクリックします。
ユーザーのリストが表示されます。
- 3 ユーザー名の横にあるラジオ ボタンをクリックし、[ロックを解除] をクリックします。

グループの管理

LDAP サーバへの有効な接続がある場合や、SAML ID プロバイダを使用できるように組織が設定されている場合は、LDAP グループまたは SAML グループをインポートできます。インポートされたグループを編集または削除することもできます。

グループのインポート

ユーザーのグループを追加するには、LDAP グループまたは SAML グループをインポートします。

前提条件

- この操作には、事前定義の組織管理者ロールに含まれている権限、またはそれに相当する権限が必要です。
- LDAP サーバへの有効な接続があること、または [16 章 組織での SAML の ID プロバイダの使用の有効化](#) ことを確認します。

手順

- 1 メイン メニュー (≡) から、[管理] を選択します。
- 2 左側のパネルの [アクセス コントロール] で、[グループ] をクリックします。
ユーザー グループのリストが表示されます。
- 3 [グループのインポート] をクリックします。

4 ユーザー グループをインポートするソースを選択します。

表示されるのは、ID プロバイダとして設定したソース LDAP サーバまたは SAML サーバのみです。

ソース	アクション
LDAP	LDAP サーバからユーザー グループをインポートします。 a テキスト ボックスに名前の全部または一部を入力し、[検索] をクリックします。 b インポートするユーザー グループを選択し、[追加] をクリックします。
SAML	SAML サーバからユーザー グループをインポートします。インポートするグループの名前を入力します。 グループ名ごとに新しい行を使用します。

5 インポートするユーザーのグループに割り当てるロールを選択します。

6 [保存] をクリックします。

グループの削除

グループの LDAP グループを削除することで、グループを vCloud Director 組織から削除できます。

LDAP グループを削除すると、そのグループのメンバーシップのみに基づく vCloud Director アカウントを所有するユーザーはログインできなくなります。

前提条件

この操作には、事前定義の組織管理者ロールに含まれている権限、またはそれに相当する権限が必要です。

手順

- 1 メイン メニュー (≡) から、[管理] を選択します。
- 2 左側のパネルの [アクセス コントロール] で、[グループ] をクリックします。
ユーザー グループのリストが表示されます。
- 3 削除するグループ名の横にあるラジオ ボタンをクリックして、[削除] をクリックします。
- 4 グループの削除を確定するには、[OK] をクリックします。

グループの編集

vCloud Director テナント ポータルからグループを編集できます。

前提条件

この操作には、事前定義の組織管理者ロールに含まれている権限、またはそれに相当する権限が必要です。

手順

- 1 メイン メニュー (≡) から、[管理] を選択します。
- 2 左側のパネルの [アクセス コントロール] で、[グループ] をクリックします。
ユーザー グループのリストが表示されます。

- 3 編集するグループ名の横にあるラジオ ボタンをクリックして、[編集] をクリックします。
- 4 必要に応じてグループを編集します。
 - a 説明を変更します。
 - b 必要に応じてグループのメンバーのロールを変更します。
- 5 [保存] をクリックします。

ロールと権限

vCloud Director はロールと権限を使用して、ユーザーが組織内で実行できる操作を決定します。vCloud Director には、それぞれの権限を持つ多数の事前定義済みロールが含まれています。

システム管理者および組織管理者は、各ユーザーまたはグループにロールを割り当てる必要があります。同じユーザーが、異なる組織で異なるロールを所有することもできます。システム管理者は、システム全体にわたってロールの作成と、既存のロールの変更が可能です。それに対して組織管理者は、自分が管理する組織についてのみ、ロールを作成し、ロールを変更できます。

vCloud Director テナント ポータルでは、組織管理者が自分の担当する組織のロールを管理できます。システム管理者が 1 つ以上の事前定義済みテナント ロールを組織に公開した場合は、組織管理者としてこれらのロールを表示できますが、変更することはできません。ただし、同様な権限を持つカスタム テナント ロールを作成し、組織内のユーザーに割り当てることはできます。

事前定義のロールおよびその権限については、[事前定義ロールとその権限](#)を参照してください。

事前定義ロールとその権限

vCloud Director の各事前定義ロールには、共通ワークフロー内の操作の実行に必要な一連のデフォルト権限が含まれています。デフォルトで、事前定義済みのすべてのグローバル テナント ロールは、システムのすべての組織に公開されます。

事前定義済みのプロバイダ ロール

デフォルトでは、プロバイダ組織のみにローカルなプロバイダ ロールは、システム管理者ロールとマルチサイト システムロールです。システム管理者は、追加のカスタム プロバイダ ロールを作成できます。

システム管理者

システム管理者ロールは、プロバイダ組織にのみ設定されています。システム管理者ロールには、システムのすべての権限が含まれています。システム管理者ロールでのみ使用可能な権限のリストについては、vCloud Director Service Provider Admin Portal Guide を参照してください。システム管理者の認証情報は、インストールおよび構成時に確立されます。システム管理者は、プロバイダ組織に追加のシステム管理者およびユーザー アカウントを作成できます。

マルチサイト システム

マルチサイト展開のためのハートビート プロセスを実行する場合に使用します。このロールには、マルチサイト システムの操作 という権限のみが付与されています。これにより、サイト関連付けのリモート メンバーのステータスを取得する vCloud API 要求を行うことができます。

事前定義済みのグローバル テナント ロール

デフォルトでは、事前定義済みのグローバル テナント ロールおよびそこに含まれている権限がすべての組織に公開されます。システム管理者は、個別の組織で権限およびグローバル テナント ロールの公開を解除することができます。システム管理者は、事前定義済みのグローバル テナント ロールを編集または削除できます。システム管理者は、追加のグローバル テナント ロールを作成および公開できます。

組織管理者

組織の作成後、システム管理者は、組織管理者ロールを組織内のどのユーザーにでも割り当てることができます。事前定義の組織管理者ロールを持つユーザーは、組織内のユーザーとグループを管理し、(事前定義の組織管理者ロールを含む) ロールを割り当てることができます。組織管理者によって作成または変更されたロールは、他の組織には表示されません。

カタログ作成者

事前定義済みのカタログ作成者ロールに関連付けられた権限を持つユーザーは、カタログを作成および公開できます。

vApp 作成者

事前定義の vApp 作成者ロールに関連付けられた権限を持つユーザーは、カタログを使用し、vApp を作成できます。

vApp ユーザー

事前定義の vApp ユーザーロールに関連付けられた権限を持つユーザーは、既存の vApp を使用できます。

コンソールのアクセスのみ

事前定義のコンソールのアクセスのみロールに関連付けられた権限を持つユーザーは、仮想マシンの状態およびプロパティを表示し、ゲスト OS を使用できます。

ID プロバイダに従う

事前定義の ID プロバイダに従うロールに関連付けられた権限は、ユーザーの OAuth または SAML ID プロバイダから受信した情報に基づいて決定されます。ユーザーまたはグループに ID プロバイダに従うロールが割り当てられているときに包含の資格を得るには、ID プロバイダによって提供されたロールまたはグループ名が、組織内で定義されたロールまたはグループ名と大文字小文字も含めて完全に一致する必要があります。

- ユーザーが OAuth ID プロバイダによって定義されている場合、ユーザーには、ユーザーの OAuth トークンの `roles` アレイで指定されたロールが割り当てられます。
- ユーザーが SAML ID プロバイダによって定義されている場合、ユーザーには、名前が組織の `OrgFederationSettings` にある `SamlAttributeMapping` 要素内の `RoleAttributeName` 要素に表示される SAML 属性で指定されたロールが割り当てられます。

ユーザーに ID プロバイダに従うロールが割り当てられているが、一致するロールまたはグループ名が組織内で利用できない場合、ユーザーは組織にログインすることができますが、権限はありません。ID プロバイダがユーザーをシステム管理者などのシステムレベルのロールに関連付けている場合、ユーザーは組織にログインすることができますが、権限はありません。このようなユーザーにはロールを手動で割り当てる必要があります。

ID プロバイダに従うロールは例外として、事前定義ロールにはすべてデフォルトの権限セットが含まれています。システム管理者のみが、事前定義ロールの権限を変更できます。システム管理者が事前定義ロールを変更すると、変更内容がシステム内のロールのすべてのインスタンスに反映されます。

事前定義グローバル テナント ロールの権限

複数の事前定義済みグローバル ロールには、さまざまな共通の権限があります。これらの権限はデフォルトですべての新しい組織に付与されるほか、組織管理者が作成するその他のロールで使用できます。事前定義されたテナント ロールの権限のリストについては、[事前定義グローバル テナント ロールの権限](#)を参照してください。

事前定義グローバル テナント ロールの権限

複数の事前定義済みグローバル ロールには、さまざまな共通の権限があります。これらの権限はデフォルトですべての新しい組織に付与されるほか、組織管理者が作成するその他のロールで使用できます。

vCloud Director のグローバル テナント ロールに含まれる権限

このリリースの 新機能	権限名	組織管理 者	カタログ作成者	vApp 作成者	vApp ユーザ ー	コンソールのア クセスのみ
	すべての組織 VDC へのアクセス	✓				
	カタログ：マイ クラウドからの vApp の追加	✓	✓	✓		
	カタログ：所有者を変更	✓				
	カタログ：CLSP 公開のサブスクリ プション	✓	✓			
	カタログ：カタログを作成/削除	✓	✓			
	カタログ：プロパティの編集	✓	✓			
	カタログ：公開	✓	✓			
	カタログ：共有	✓	✓			
	カタログ：ACL の表示	✓	✓			
	カタログ：非公開および共有カタロ グの表示	✓	✓	✓		
	カタログ：公開カタログの表示	✓				
	カスタム エンティティ：組織内の すべてのカスタム エンティティ イ ンスタンスを表示	✓				
	カスタム エンティティ：カスタム エンティティ インスタンスの表示	✓				
	ディスク：所有者を変更	✓	✓			
	ディスク：作成	✓	✓	✓		
	ディスク：削除	✓	✓	✓		

このリリースの新機能	権限名	組織管理者	カタログ作成者	vApp 作成者	vApp ユーザー	コンソールのアクセスのみ
	ディスク：プロパティの編集	✓	✓	✓		
	ディスク：プロパティの表示	✓	✓	✓	✓	
	全般：管理者のコントロール	✓				
	全般：管理者の表示	✓				
	全般：通知の送信	✓				
	グループ/ユーザー：表示	✓				
	ハイブリッド クラウドの運用：コントロール チケットを取得	✓				
	ハイブリッド クラウドの運用：クラウドからのトンネル チケットを取得	✓				
	ハイブリッド クラウドの運用：クラウドへのトンネル チケットを取得	✓				
	ハイブリッドクラウドの運用：クラウドからのトンネルを作成	✓				
	ハイブリッド クラウドの運用：クラウドへのトンネルを作成	✓				
	ハイブリッド クラウドの運用：クラウドからのトンネルを削除	✓				
	ハイブリッド クラウドの運用：クラウドへのトンネルを削除	✓				
	ハイブリッド クラウドの運用：クラウドからのトンネルのエンドポイント タグを更新	✓				
	ハイブリッド クラウドの運用：クラウドからのトンネルを表示	✓				
	ハイブリッド クラウドの運用：クラウドへのトンネルを表示	✓				
	組織ネットワーク：プロパティの編集	✓				
	組織ネットワーク：表示	✓				
	組織 VDC コンピューティング ポリシー：表示	✓	✓	✓	✓	
	組織 VDC 分散ファイアウォール：ルールの構成	✓				
	組織 VDC 分散ファイアウォール：ルールの表示	✓				

このリリースの 新機能	権限名	組織管理 者	カタログ作成者	vApp 作成者	vApp ユーザ ー	コンソールのア クセスのみ
	組織 VDC ゲートウェイ : DHCP の構成	✓				
✓	組織 VDC ゲートウェイ : DNS の 構成	✓				
✓	組織 VDC ゲートウェイ : ECMP ルーティングの構成	✓				
	組織 VDC ゲートウェイ : ファイア ウォールの設定	✓				
	組織 VDC ゲートウェイ : IPsec VPN の構成	✓				
	組織 VDC ゲートウェイ : ロード バランサの構成	✓				
	組織 VDC ゲートウェイ : NAT の 構成	✓				
	組織 VDC ゲートウェイ : 固定ルー ティングの設定	✓				
	組織 VDC ゲートウェイ : Syslog の構成	✓				
	組織 VDC ゲートウェイ : 詳細ネッ トワークに変換	✓				
	組織 VDC ゲートウェイ : 表示	✓				
	組織 VDC ゲートウェイ : DHCP の表示	✓				
✓	組織 VDC ゲートウェイ : DNS の 表示	✓				
	組織 VDC ゲートウェイ : ファイア ウォールの表示	✓				
	組織 VDC ゲートウェイ : IPsec VPN の表示	✓				
	組織 VDC ゲートウェイ : ロード バランサの表示	✓				
	組織 VDC ゲートウェイ : NAT の 表示	✓				
	組織 VDC ゲートウェイ : 固定ルー ティングの表示	✓				
	組織 VDC ネットワーク : プロパテ ィの編集	✓				
	組織 VDC ネットワーク : プロパテ ィの表示	✓		✓		
	組織 VDC ストレージ プロファイ ル : デフォルトの設定	✓				

このリリースの 新機能	権限名	組織管理 者	カタログ作成者	vApp 作成者	vApp ユーザ ー	コンソールのア クセスのみ
	組織 VDC : 編集	✓				
	組織 VDC : ACL の編集	✓				
	組織 VDC : ファイアウォールの管 理	✓				
	組織 VDC : 表示	✓	✓			
	組織 VDC : ACL の表示	✓				
	組織 VDC : メトリックの表示	✓				
	組織 VDC : 仮想マシン - 仮想マシ ン アフィニティの編集	✓	✓	✓		
	組織 : 関連付け設定の編集	✓				
	組織 : 連携設定の編集	✓				
	組織 : LDAP 設定の編集	✓				
	組織 : リース ポリシーの編集	✓				
	組織 : OAuth 設定の編集	✓				
	組織 : パスワード ポリシーの編集	✓				
	組織 : プロパティの編集	✓				
	組織 : 割り当て容量ポリシーの編集	✓				
	組織 : SMTP 設定の編集	✓				
	組織 : VDC ACL の編集に IdP からユーザー/グループを暗黙的に インポート	✓				
	組織 : 表示	✓	✓	✓		
	組織 : メトリックの表示	✓				
	ロール : 作成、編集、削除、または コピー	✓				
	サービス ライブラリ : サービス ラ イブラリの表示	✓				
	ユーザー インターフェイス プラグ イン : 表示	✓	✓	✓	✓	
	vApp テンプレート/メディア : コ ピー	✓	✓	✓		
	vApp テンプレート/メディア : 作 成/アップロード	✓	✓			

このリリースの 新機能	権限名	組織管理 者	カタログ作成者	vApp 作成者	vApp ユーザ ー	コンソールのア クセスのみ
	vApp テンプレート/メディア：編 集	✓	✓	✓		
	vApp テンプレート/メディア：表 示	✓	✓	✓	✓	
	vApp テンプレート：所有者の変 更	✓	✓			
	vApp テンプレート：チェックア ウト	✓	✓	✓	✓	
	vApp テンプレート ダウンロード	✓	✓			
	vApp：所有者を変更	✓				
	vApp：コピー	✓	✓	✓	✓	
	vApp：作成/再構成	✓	✓	✓		
	vApp：削除	✓	✓	✓	✓	
	vApp：ダウンロード	✓	✓	✓		
	vApp：プロパティの編集	✓	✓	✓	✓	
	vApp：仮想マシンのコンピュー ティング ポリシーを編集	✓	✓	✓		
	vApp：仮想マシンの CPU を編集	✓	✓	✓		
	vApp：仮想マシンのハード ディ スクを編集	✓	✓	✓		
	vApp：仮想マシンのメモリを編集	✓	✓	✓		
	vApp：仮想マシンのネットワーク を編集	✓	✓	✓	✓	
	vApp：仮想マシンのプロパティを 編集	✓	✓	✓	✓	
	vApp：仮想マシンのパスワード設 定を管理	✓	✓	✓	✓	✓
	vApp：パワー操作	✓	✓	✓	✓	
	vApp：共有	✓	✓	✓	✓	
	vApp：スナップショット操作	✓	✓	✓	✓	
	vApp：アップロード	✓	✓	✓		
	vApp：コンソールの使用	✓	✓	✓	✓	✓
	vApp：ACL の表示	✓	✓	✓	✓	
	vApp：仮想マシンのメトリックを 表示	✓		✓	✓	

このリリースの新機能	権限名	組織管理者	カタログ作成者	vApp 作成者	vApp ユーザー	コンソールのアクセスのみ
	vApp : 仮想マシンのブート オプション	✓	✓	✓		
	vApp : vCenter Server への仮想マシンのメタデータ	✓	✓	✓		
	VDC テンプレート : インスタンス化	✓				
	VDC テンプレート : 表示	✓				

カスタム テナント ロールの作成

組織管理者は、テナント ポータルを使用して、管理対象の組織のカスタム テナント ロール オブジェクトを作成できます。

前提条件

この操作には、事前定義の組織管理者ロールに含まれている権限、またはそれに相当する権限が必要です。

手順

- 1 メイン メニュー (☰) から、[管理] を選択します。
- 2 左側のパネルの [アクセス コントロール] で、[ロール] をクリックします。
ロールのリストが表示されます。
- 3 [追加] をクリックします。
- 4 ロールの名前と、必要に応じて説明を入力します。
- 5 ロールの権限を展開し、ロールの権限を選択します。

権限は、オブジェクトを表示または管理できるカテゴリおよびサブカテゴリにグループ化されています。

オプション	説明
アクセス コントロール	特定のオブジェクトを表示および管理するためのアクセスを制御する権限。
管理	管理者権限を制御する権限。
コンピュート	組織仮想データセンターおよびプロバイダ仮想データセンター、vApp、組織仮想データセンターのテンプレート、仮想マシン グループ、および仮想マシンの監視のアクセスと管理を制御する権限。
拡張機能	追加のプラグインおよび vCloud Director 拡張機能へのアクセスを制御する権限。
インフラストラクチャ	データストア、ディスク、ホストなどのインフラストラクチャ オブジェクトのアクセスと管理を制御する権限。
ライブラリ	カタログおよびカタログ項目のアクセスと管理を制御する権限。
ネットワーク	ネットワーク設定のアクセスと管理を制御する権限。

- 6 [保存] をクリックします。


カスタム テナント ロールの編集

組織管理者は、テナント ポータルを使用して、管理対象の組織のカスタム テナント ロール オブジェクトを編集できます。組織管理者は、システム管理者が組織に公開したグローバル テナント ロールのみを表示できます。グローバル テナント ロールを編集することはできません。

前提条件

この操作には、事前定義の組織管理者ロールに含まれている権限、またはそれに相当する権限が必要です。

手順

- 1 メイン メニュー () から、[管理] を選択します。
- 2 左側のパネルの [アクセス コントロール] で、[ロール] をクリックします。
ロールのリストが表示されます。
- 3 編集するロールの横にあるラジオ ボタンをクリックして、[編集] をクリックします。
- 4 必要に応じてロールの設定を変更します。
 - a ロールの名前と説明（説明はオプション）を変更します。
 - b ロールの権限を編集します。
- 5 [保存] をクリックします。


ロールの削除

組織管理者は、テナント ポータルを使用して、管理対象の組織のロール オブジェクトを削除できます。

前提条件

この操作には、事前定義の組織管理者ロールに含まれている権限、またはそれに相当する権限が必要です。

手順

- 1 メイン メニュー () から、[管理] を選択します。
- 2 左側のパネルの [アクセス コントロール] で、[ロール] をクリックします。
ロールのリストが表示されます。
- 3 削除するロールの横にあるラジオ ボタンをクリックして、[削除] をクリックします。
- 4 ロールの削除を確定するには、[OK] をクリックします。

組織での SAML の ID プロバイダの使用の有効化

16

Security Assertion Markup Language (SAML) の ID プロバイダからユーザーおよびグループをインポートし、インポートされたユーザーが SAML の ID プロバイダで設定した認証情報を使用して組織にログインできるようにするには、組織での SAML の ID プロバイダ（シングル サインオンとも呼ばれる）の使用を有効にします。

ユーザーおよびグループをインポートすると、SAML トークンから属性のリストが抽出され（使用できる場合）、ユーザーのログイン試行に関する情報の対応箇所を解釈する際に使用されます。

- `email address = "EmailAddress"`
- `user name = "UserName"`
- `full name = "FullName"`
- `user's groups = "Groups"`
- `user's roles = "Roles"`

ロールの属性は設定可能です。

ユーザーを直接インポートする代わりに、インポートしたグループのメンバーシップによってユーザーがログインできるようにする場合は、グループ情報が必要です。ユーザーは複数のグループに所属することができるため、1 人のユーザーがセッションの実行中に複数のロールを持つ場合があります。

インポートしたユーザーまたはグループに ID プロバイダに従うロールが割り当てられている場合は、トークンの Roles 属性から収集された情報に基づいてロールが割り当てられます。別の属性が使用されている場合、この属性名は API を使用した場合のみ設定可能です。また、設定できるのは Roles 属性のみとなります。ID プロバイダに従うロールが使用されているにもかかわらずロール情報を抽出できない場合、ユーザーはログインできますが、操作を実行する権限はありません。


前提条件

- この操作には、事前定義の組織管理者ロールに含まれている権限、またはそれに相当する権限が必要です。
- SAML 2.0 に準拠した ID プロバイダへのアクセス権があることを確認します。
- SAML の ID プロバイダから必要なメタデータを受信していることを確認します。メタデータを vCloud Director に手動でインポートするか、XML ファイルとしてインポートする必要があります。メタデータには、次の情報を含める必要があります。
 - Single Sign-On サービスの場所
 - シングル ログアウト サービスの場所

■ サービスの X.509 証明書の場所

構成方法および SAML プロバイダからのメタデータの取得方法については、SAML ID プロバイダのドキュメントを参照してください。

手順

- 1 メイン メニュー () から、[管理] を選択します。
- 2 [ID プロバイダ] で [SAML] をクリックします。
- 3 [[編集]] をクリックします。
- 4 [サービス プロバイダ] タブでエンティティ ID を入力します。

エンティティ ID は、ID プロバイダに対して一意となる組織の識別子です。組織名、または SAML ID プロバイダの要件を満たす他の任意の文字列を使用できます。

重要： エンティティ ID は、指定した後に削除することはできません。エンティティ ID を変更するには、組織の SAML を完全に再設定する必要があります。エンティティ ID の詳細については、『[Assertions and Protocols for the OASIS Security Assertion Markup Language \(SAML\) 2.0](#)』を参照してください。

- 5 [メタデータ] リンクをクリックして、組織の SAML メタデータをダウンロードします。
ダウンロードされたメタデータを ID プロバイダにそのまま提供する必要があります。
- 6 [証明書の有効期限] の日付を確認し、必要な場合は、再生成 をクリックして、連携メッセージの署名に使用される証明書を再生成します。
証明書は SAML メタデータに含まれ、暗号化と署名の両方に使用されます。組織と SAML ID プロバイダ間の信頼の確立方法によっては、暗号化と署名のいずれかまたは両方が必要になることがあります。
- 7 [ID プロバイダ] タブで [SAML の ID プロバイダを使用する] 切り替えを有効にします。
- 8 ID プロバイダから受信した SAML メタデータをコピーして、テキスト ボックスに貼り付けるか、[アップロード] をクリックして XML ファイル内のメタデータを参照し、アップロードします。
- 9 [保存] をクリックします。

次のステップ

- vCloud Director メタデータを使用して SAML プロバイダを設定します。SAML ID プロバイダのドキュメントおよび『vCloud Director インストールおよびアップグレード ガイド』を参照してください。
- SAML ID プロバイダからユーザーおよびグループをインポートします。[15 章 ユーザー、グループ、ロールの管理](#)を参照してください。

組織管理者は、組織の名前、Eメールの設定、ドメインの設定、メタデータ、ポリシーなど、組織内の多くの設定を変更できます。

この章には、次のトピックが含まれています。

- 組織の名前と説明の編集
- 電子メール設定の変更
- SMTP 設定のテスト
- 組織内の仮想マシンのドメイン設定の変更
- 複数のサイトの操作
- マルチサイト展開の設定と管理
- リースについて
- 組織内の vApp および vApp テンプレートのリース ポリシーの変更
- 組織内の仮想マシンのデフォルトの割り当て容量の変更
- 組織内のパスワードおよびユーザー アカウントのポリシーの変更

組織の名前と説明の編集

組織の完全な名前および説明を編集できます。

前提条件

この操作には、事前定義の組織管理者ロールに含まれている権限、またはそれに相当する権限が必要です。

手順

- 1 メイン メニュー (≡) から、[管理] を選択します。
- 2 [設定] で、[全般] をクリックします。
組織名、デフォルトの URL、完全な名前、説明などの全般設定のリストが表示されます。
- 3 組織の完全な名前および説明を変更するには、[編集] をクリックします。
- 4 必要な変更を適用して、[保存] をクリックします。

電子メール設定の変更

システム管理者が組織を作成したときに設定した E メールデフォルト設定は、確認して変更することができます。

データ ストアの容量不足など、重要な情報をレポートする場合、vCloud Director はアラート メールを送信します。デフォルトでは、システム レベルで指定される SMTP サーバを使用して、システム レベルで指定されるメールアドレスのリストまたはシステム管理者宛てに、組織からアラート メールが送信されます。システム レベルで指定したものと異なるメール アドレス セットにこの組織に対するアラートを送信するよう vCloud Director を設定する場合、またはシステム レベルで指定したものと異なる SMTP サーバを使用して組織からアラートを送信する場合は、組織レベルで E メール設定を修正することができます。

前提条件

この操作には、事前定義の組織管理者ロールに含まれている権限、またはそれに相当する権限が必要です。

手順

- 1 メイン メニュー (≡) から、[管理] を選択します。
- 2 [設定] で [E メール] をクリックします。
組織の E メール設定が表示されます。
- 3 [[編集]] をクリックします。
- 4 [SMTP サーバ] タブで、SMTP サーバの設定を編集します。
 - a カスタムの SMTP サーバを使用するか、デフォルトを使用するかを選択します。
 - b カスタムの SMTP サーバを使用する場合は、[SMTP サーバ名] テキスト ボックスに DNS ホスト名または SMTP サーバの IP アドレスを入力します。
 - c (オプション) SMTP サーバ ポートを入力します。
 - d (オプション) 認証を要求してユーザー名とパスワードを入力するかどうかを選択します。
- 5 通知設定を編集するには、[通知設定] タブをクリックします。
 - a カスタム通知設定を使用するように選択します。
 - b 組織の Eメールの送信者として表示されるメール アドレスを入力します。
 - c (オプション) Eメールの件名のプリフィックスとして使用するテキストを入力します。
 - d (オプション) すべての組織管理者に通知を送信するのか、それとも特定のメール アドレスに通知を送信するのかを選択します。
 - e (オプション) 特定のメール アドレスに通知を送信する場合は、メール アドレスをカンマで区切って入力します。
- 6 [保存] をクリックします。

SMTP 設定のテスト

組織の E メール設定を変更した後に、SMTP 設定をテストできます。

前提条件

この操作には、事前定義の組織管理者ロールに含まれている権限、またはそれに相当する権限が必要です。

手順

- 1 メイン メニュー (≡) から、[管理] を選択します。
- 2 [設定] で [E メール] をクリックします。
組織の E メール設定が表示されます。
- 3 [テスト] をクリックします。
- 4 SMTP 設定をテストするための宛先メール アドレスおよび SMTP サーバのパスワードを入力して、[テスト] ボタンをクリックします。

組織内の仮想マシンのドメイン設定の変更

組織で作成された仮想マシンが参加できるデフォルト Windows ドメインを設定できます。仮想マシンは、デフォルトのドメインを指定しているかどうかにかかわらず、認証情報を持っているドメインにいつでも参加できます。

前提条件

この操作には、事前定義の組織管理者ロールに含まれている権限、またはそれに相当する権限が必要です。

手順

- 1 メイン メニュー (≡) から、[管理] を選択します。
- 2 [設定] で [ゲストのカスタマイズ] をクリックします。
- 3 選択して組織内の仮想マシンのドメイン参加を有効にします。
- 4 ドメイン名、ユーザー名、およびパスワードを入力します。
入力した認証情報は、ドメイン管理者ではなく、通常のドメイン ユーザーに適用されます。
- 5 (オプション) アカウント組織ユニットを入力します。
- 6 [保存] をクリックします。

複数のサイトの操作

vCloud Director マルチサイト機能を使用すると、サービス プロバイダ、または地理的に分散した複数の vCloud Director インストール (サーバ グループ) のテナントが、これらのインストールおよびその組織を単一エンティティとして管理および監視できます。

vCloud Director テナント ポータルでは、組織管理者が、関連付けられているサイト上で組織の関連付けを行うことができます。

サイトの関連付けの詳細については、『vCloud Director Service Provider Admin Portal Guide』を参照してください。

マルチサイト展開の設定と管理

システム管理者が 2 つのサイトを関連付けた後に、任意のメンバー サイトの組織管理者が自分の組織の関連付けを開始することができます。

2 つの組織（ここでは組織 A および組織 B と表記）間の関連付けを作成するには、両方の組織の組織管理者が操作を行う必要があります。こうすることで、各組織にログインし、ローカルな関連付けデータを取得して、取得したデータを他の組織に送信できるようになります。

重要： 2 つの組織を関連付けるプロセスは、2 つの補助的なペアリング操作に論理的に分割することができます。（この例の）最初の操作では、サイト A の組織 A にサイト B の組織 B をペアリングします。次に、サイト B の組織 B にサイト A の組織 A をペアリングします。両方のペアリングが完了するまで、関連付けは完了しません。

前提条件

- 組織で占有されているサイトを関連付ける必要があります。
- この操作は、両方のサイトのシステム管理者、または両方の組織の組織管理者が行う必要があります。

手順

- 1 サイト A で組織 A の vCloud Director テナント ポータルにログインして、そのローカルの関連付けデータを取得します。
 - a [管理] をクリックします。
 - b [設定] で [マルチサイト] をクリックします。
 - c XML 形式でデータをダウンロードするには、[ローカルの関連付けデータをエクスポート] をクリックします。
ブラウザのダウンロード フォルダ内のファイルにデータが保存されます。
- 2 サイト A の組織 A からローカルの関連付けデータを送信するには、サイト B の組織 B の vCloud Director テナント ポータルにログインします。
 - a [管理] をクリックします。
 - b [設定] で [マルチサイト] をクリックします。
 - c [組織の関連付けを新規作成] をクリックします。
[新しい関連付け XML] テキスト ボックスの下にある上矢印をクリックし、[手順 手順 1](#) でダウンロードしたローカルの関連付けデータを選択して、[手順 手順 1](#) でダウンロードした関連付けデータを組織 B に送信します。
 - d [次へ] をクリックして、データを確認し、送信します。
サイト A の組織 A にサイト B の組織 B がペアリングされます。
 - e 関連付けられた組織を表示するには、[完了] をクリックします。
 - f 関連付けられた組織の詳細を表示するか、または関連付けを削除するには、[組織名] カードをクリックします。

- 3 組織 B からローカルの関連付けデータを取得し、それを組織 A に送信するためには、手順 1 と手順 2 を繰り返して、関連付けを完了します。

リースについて

組織を作成するときにはリースを指定します。リースでは、vApp を実行できる最大時間、およびその vApp と vApp テンプレートを格納できる最大時間を指定することで、組織のストレージ リソースおよびコンピューティング リソースに対するコントロールのレベルを提供します。

ランタイム リースの目的は、非アクティブの vApp がコンピューティング リソースを消費するのを防ぐことです。たとえば、ユーザーが vApp を開始してその vApp を停止しないまま休暇に入った場合、vApp はリソースを使用し続けます。

ランタイム リースは、ユーザーが vApp を開始したときに始まります。ランタイム リースの期限が切れると、vCloud Director は vApp を停止します。

ストレージ リースの目的は、使用されていない vApp および vApp テンプレートがストレージ リソースを消費するのを防ぐことです。vApp ストレージ リースは、ユーザーが vApp を停止したときに始まります。ストレージ リースは、実行中の vApp には影響を及ぼしません。vApp テンプレートのストレージ リースは、ユーザーが vApp テンプレートを vApp に追加したとき、vApp テンプレートをワークスペースに追加したとき、vApp テンプレートのダウンロード、コピー、移動を行ったときに始まります。

ストレージ リースの期限が切れると、vCloud Director は設定された組織ポリシーに沿って、その vApp または vApp テンプレートを期限切れとしてマークするか、その vApp または vApp テンプレートを削除します。

組織内の vApp および vApp テンプレートのリース ポリシーの変更

システム管理者が組織を作成したときに設定されたデフォルトのポリシーを確認および変更できます。

前提条件

この操作には、事前定義の組織管理者ロールに含まれている権限、またはそれに相当する権限が必要です。

手順

- 1 メイン メニュー (≡) から、[管理] を選択します。

- 2 [設定] で [ポリシー] をクリックします。

システム管理者が設定したデフォルトのポリシーを表示できます。

- 3 [[編集]] をクリックします。

- 4 vApp リースを編集します。

vApp リースでは、vApp を実行できる最大時間、およびその vApp を格納できる最大時間を指定することで、組織のストレージ リソースおよびコンピューティング リソースに対するコントロールのレベルを提供します。また、ストレージ リースの有効期限が切れた場合の vApp の動作も指定できます。

- a vApp が自動的に停止するまでの実行可能な時間を定義するには、最大ランタイム リースを入力します。
- b パワーオフ状態やサスペンドなど、ランタイムの有効期限切れアクションを選択します。

- c 停止した vApp が自動的にクリーンアップされるまでの使用可能な時間を定義するには、最大ストレージ リースを入力します。
- d vApp を永久に削除する、vApp を期限切れのアイテムに移動するなどのストレージ クリーンアップ アクションを選択します。

5 vApp テンプレート リースを編集します。

vApp テンプレート リースでは、vApp テンプレートを格納できる最大時間を指定することで、組織のストレージ リソースおよびコンピューティング リソースに対するコントロールのレベルを提供します。また、ストレージ リースの有効期限が切れた場合の vApp テンプレートの動作も指定できます。

- a vApp テンプレートが自動的にクリーンアップされるまでの使用可能な時間を定義するには、最大ストレージ リースを入力します。
- b vApp テンプレートを永久に削除する、vApp を期限切れのアイテムに移動するなどのストレージ クリーンアップ アクションを選択します。

6 [OK] をクリックします。

組織内の仮想マシンのデフォルトの割り当て容量の変更


組織を作成したときにシステム管理者によって設定されたデフォルトの割り当てポリシーを確認および変更できます。

割り当て容量により、組織内の各ユーザーが組織の仮想データセンターで格納およびパワーオンすることができる仮想マシンの数が決まります。指定する割り当て容量は、組織に追加されるすべての新規ユーザーにとってのデフォルト設定となります。ユーザー レベルで設定された割り当て容量は、組織レベルで設定された割り当て容量よりも優先されます。

前提条件

この操作には、事前定義の組織管理者ロールに含まれている権限、またはそれに相当する権限が必要です。

手順

- 1 メイン メニュー () から、[管理] を選択します。
- 2 [設定] で [ポリシー] をクリックします。
システム管理者が設定したデフォルトのポリシーを表示できます。
- 3 [[編集]]をクリックします。
- 4 仮想マシンの数を、無制限から指定した値までの範囲内で選択します。
- 5 パワーオン状態の仮想マシンの数を、無制限から指定した値までの範囲内で選択します。
- 6 [OK] をクリックします。

組織内のパスワードおよびユーザー アカウントのポリシーの変更


組織を作成したときにシステム管理者によって設定されたデフォルトのパスワード ポリシーおよびユーザー アカウント ポリシーを確認および変更できます。

パスワード ポリシーおよびユーザー アカウント ポリシーによって、ユーザーが無効なパスワードを入力した場合の vCloud Director の動作を定義します。[]

前提条件

この操作には、事前定義の組織管理者ロールに含まれている権限、またはそれに相当する権限が必要です。

手順

- 1 メイン メニュー () から、[管理] を選択します。
- 2 [設定] で [ポリシー] をクリックします。
システム管理者が設定したデフォルトのポリシーを表示できます。
- 3 [[編集]] をクリックします。
- 4 何度かの無効なログイン試行の後にユーザー アカウントをロックできるようにします。
- 5 アカウントがロックされるまでに許可される、無効なログインの試行回数を入力します。
- 6 ロックされたアカウントのユーザーが再ログインできない時間を分単位で入力します。
- 7 [OK] をクリックします。

サービス ライブラリの操作

18

vCloud Director のサービス ライブラリ項目は、クラウド管理機能を拡張して、プロバイダまたはテナントの管理者がさまざまなサービスを監視および操作できるようにする vRealize Orchestrator ワークフローのことです。

この章には、次のトピックが含まれています。

- サービスの検索
- サービスの実行

サービスの検索

vCloud Director テナント ポータルの [サービス ライブラリ] ページには、vCloud Director にインポートされて組織に公開された一連の vRealize Orchestrator ワークフローが表示されます。

前提条件

この操作を行うには、事前定義されたユーザー ロールにサービス ライブラリに関する権限を含める必要があります。

手順

- 1 メイン メニュー (≡) で [ライブラリ] を選択し、[サービス] で [サービス ライブラリ] を選択します。

サービス項目のリストがカード ビューで表示されます。カード ビューにはページあたり 12 個の項目が、名前を基準としてアルファベット順に表示されます。各カードには、サービスの名前、および vRealize Orchestrator がインポートされたサービス カテゴリに対応するタグが表示されます。

- 2 ページ上部の [検索] テキスト ボックスに、サービスの名前またはサービスが属するカテゴリの名前の最初の語句を入力します。

- a サービスの名前で検索するのか、それともサービス カテゴリで検索するかを選択します。

検索結果がカード ビューで表示されます。カード ビューにはページあたり 12 個の項目が、名前を基準としてアルファベット順に表示されます。

サービスの実行

vCloud Director テナント ポータルの [サービス ライブラリ] ページからサービスを実行できます。

前提条件

この操作を行うには、事前定義されたユーザー ロールにサービス ライブラリに関する権限を含める必要があります。

手順

- 1 メイン メニュー (≡) で [ライブラリ] を選択し、[サービス] で [サービス ライブラリ] を選択します。

サービス項目のリストがカード ビューで表示されます。カード ビューにはページあたり 12 個の項目が、名前を基準としてアルファベット順に表示されます。各カードには、サービスの名前、および vRealize Orchestrator がインポートされたサービス カテゴリに対応するタグが表示されます。

- 2 実行するサービスを検索します。
- 3 サービスのカードで、[実行] をクリックします。

新しいダイアログが開きます。サービスの必須入力パラメータの値を入力する必要があります。

- 4 [完了] をクリックして、サービスの実行を確認します。

次のステップ

実行のステータスは、[最近のタスク] ビューで監視できます。詳細については、[タスクの表示](#)を参照してください。

カスタム エンティティ 定義の操作

19

vCloud Director のカスタム エンティティ定義は、vRealize Orchestrator オブジェクト タイプにバインドされているオブジェクト タイプです。vCloud Director 組織内のユーザーは、必要に応じてこれらのタイプを所有、管理、変更できます。組織のユーザーは、サービスを実行することでカスタム エンティティをインスタンス化し、オブジェクトのインスタンスにアクションを適用することができます。

この章には、次のトピックが含まれています。

- カスタム エンティティの検索
- カスタム エンティティ定義の編集
- カスタム エンティティ定義の追加
- カスタム エンティティ インスタンス
- カスタム エンティティへのアクションの関連付け
- カスタム エンティティ定義からのアクションの関連付け解除
- カスタム エンティティの公開
- カスタム エンティティの削除

カスタム エンティティの検索

組織に公開されたカスタム エンティティを検索できます。

前提条件

この操作を行うには、事前定義されたユーザー ロールにカスタム エンティティに関する権限を含める必要があります。

手順

- 1 メイン メニュー (≡) で [ライブラリ] を選択し、[サービス] で [カスタム エンティティ定義] を選択します。

カスタム エンティティのリストがカード ビューで表示されます。カード ビューにはページあたり 12 個の項目が、名前を基準としてアルファベット順に表示されます。各カードには、カスタム エンティティの名前、エンティティがマッピングされている vRealize Orchestrator タイプ、エンティティのタイプ、および説明が表示されます（これらの情報を入手できる場合）。

- 2 ページ上部の [検索] テキスト ボックスに、検索するエンティティの名前を表す語句または文字を入力します。
検索結果がカード ビューで表示されます。カード ビューにはページあたり 12 個の項目が、名前を基準としてアルファベット順に表示されます。

カスタム エンティティ定義の編集

カスタム エンティティの名前および説明を変更できます。エンティティのタイプ、またはエンティティがバインドされる vRealize Orchestrator オブジェクト タイプを変更することはできません。これらは、カスタム エンティティのデフォルト プロパティです。デフォルト プロパティを変更する場合は、カスタム エンティティ定義を削除して、再作成する必要があります。

前提条件

この操作を行うには、事前定義されたユーザー ロールにカスタム エンティティに関する権限を含める必要があります。

手順

- 1 メイン メニュー (≡) で [ライブラリ] を選択し、[サービス] で [カスタム エンティティ定義] を選択します。
カスタム エンティティのリストがカード ビューで表示されます。カード ビューにはページあたり 12 個の項目が、名前を基準としてアルファベット順に表示されます。各カードには、カスタム エンティティの名前、エンティティがマッピングされている vRealize Orchestrator タイプ、エンティティのタイプ、および説明が表示されます（これらの情報を入手できる場合）。
- 2 選択したカスタム エンティティのカードで、[アクション] - [編集] の順に選択します。
新しいダイアログが開きます。
- 3 カスタム エンティティ定義の名前または説明を変更します。
- 4 [OK] をクリックして、変更を確定します。

カスタム エンティティ定義の追加


カスタム エンティティを作成して、既存の vRealize Orchestrator オブジェクト タイプにマッピングできます。

前提条件

この操作を行うには、事前定義されたユーザー ロールにカスタム エンティティに関する権限を含める必要があります。


手順

- 1 メイン メニュー (≡) で [ライブラリ] を選択し、[サービス] で [カスタム エンティティ定義] を選択します。
カスタム エンティティのリストがカード ビューで表示されます。カード ビューにはページあたり 12 個の項目が、名前を基準としてアルファベット順に表示されます。各カードには、カスタム エンティティの名前、エンティティがマッピングされている vRealize Orchestrator タイプ、エンティティのタイプ、および説明が表示されます（これらの情報を入手できる場合）。

- 2  アイコンをクリックして、新しいカスタム エンティティを追加します。

新しいダイアログが開きます。

- 3 [カスタム エンティティ定義] ウィザードの手順に沿って処理を進めます。

手順	
名前と説明	新しいエンティティの名前と、オプションで説明を入力します。
明	エンティティ タイプの名前 (sshHost など) を入力します。
vRO	ドロップダウン メニューで、カスタム エンティティ定義のマッピングに使用する vRealize Orchestrator を選択します。
	注： 複数の vRealize Orchestrator サーバがある場合は、それぞれにカスタム エンティティ定義を個別に作成する必要があります。
タイプ	リストの表示アイコン () をクリックして、使用可能な vRealize Orchestrator オブジェクト タイプをプラグイン別にグループ化して参照します。たとえば、[SSH] - [ホスト] の順に選択します。 タイプの名前がわかっている場合は、テキスト ボックスに直接入力できます。例：SSH:Host。
確認	指定した詳細を確認し、[完了] をクリックして作成を完了します。

結果

カード ビューに新しいカスタム エンティティ定義が表示されます。


カスタム エンティティ インスタンス


vCloud Director でカスタム エンティティ定義としてすでに定義されているオブジェクト タイプを入力パラメータとして指定して、vRealize Orchestrator ワークフローを実行すると、出力パラメータにカスタム エンティティのインスタンスが表示されます。

前提条件

この操作を行うには、事前定義されたユーザー ロールにカスタム エンティティに関する権限を含める必要があります。

手順

- 1 メイン メニュー () で [ライブラリ] を選択し、[サービス] で [カスタム エンティティ定義] を選択します。
カスタム エンティティのリストがカード ビューで表示されます。カード ビューにはページあたり 12 個の項目が、名前を基準としてアルファベット順に表示されます。各カードには、カスタム エンティティの名前、エンティティがマッピングされている vRealize Orchestrator タイプ、エンティティのタイプ、および説明が表示されます (これらの情報を入手できる場合)。
- 2 選択したカスタム エンティティのカードで、[インスタンス] をクリックします。
使用可能なインスタンスがグリッド ビューで表示されます。

- 3 各エンティティの左側にあるリスト バー () をクリックして、関連付けられたワークフローを表示します。
- ワークフローをクリックすると、入力パラメータとしてエンティティのインスタンスを使用するワークフローが実行されます。


カスタム エンティティへのアクションの関連付け

カスタム エンティティ定義にアクションを関連付けると、特定のカスタム エンティティのインスタンス上で一連の vRealize Orchestrator ワークフローを実行できるようになります。

前提条件

この操作を行うには、事前定義されたユーザー ロールにカスタム エンティティに関する権限を含める必要があります。

手順

- 1 メイン メニュー () で [ライブラリ] を選択し、[サービス] で [カスタム エンティティ定義] を選択します。
カスタム エンティティのリストがカード ビューで表示されます。カード ビューにはページあたり 12 個の項目が、名前を基準としてアルファベット順に表示されます。各カードには、カスタム エンティティの名前、エンティティがマッピングされている vRealize Orchestrator タイプ、エンティティのタイプ、および説明が表示されます（これらの情報を入手できる場合）。
- 2 選択したカスタム エンティティのカードで、[アクション] - [アクションの関連付け] の順に選択します。
新しいダイアログが開きます。
- 3 [カスタム エンティティを VRO ワークフローに関連付け] ウィザードの手順に沿って処理を進めます。

手順	詳細
vRO ワークフローの選択	表示されたワークフローのいずれかを選択します。これらは、[サービス ライブラリ] ページで使用可能なワークフローです。
ワークフローの入力パラメータの選択	リストから使用できる入力パラメータを選択します。vRealize Orchestrator ワークフローのタイプにカスタム エンティティ定義のタイプを関連付けます。
関連付けの確認	指定した詳細を確認し、[完了] をクリックして関連付けを完了します。

例

たとえば、タイプが SSH:Host のカスタム エンティティがある場合は、カスタム エンティティのタイプと一致する sshHost 入力パラメータを選択して、このエンティティを Add a Root Folder to SSH Host ワークフローに関連付けることができます。

カスタム エンティティ定義からのアクションの関連付け解除

関連付けられたアクションのリストから vRealize Orchestrator ワークフローを削除できます。

前提条件

この操作を行うには、事前定義されたユーザー ロールにカスタム エンティティに関する権限を含める必要があります。

手順

- 1 メイン メニュー (≡) で [ライブラリ] を選択し、[サービス] で [カスタム エンティティ定義] を選択します。
 カスタム エンティティのリストがカード ビューで表示されます。カード ビューにはページあたり 12 個の項目が、名前を基準としてアルファベット順に表示されます。各カードには、カスタム エンティティの名前、エンティティがマッピングされている vRealize Orchestrator タイプ、エンティティのタイプ、および説明が表示されます（これらの情報を入手できる場合）。
- 2 選択したカスタム エンティティのカードで、[アクション] - [アクションの関連付け解除] の順に選択します。
 新しいダイアログが開きます。
- 3 削除するワークフローを選択して、[アクションの関連付け解除] をクリックします。
 vRealize Orchestrator ワークフローとカスタム エンティティの関連付けが解除されました。

カスタム エンティティの公開

他のテナントまたはサービス プロバイダのユーザーが、入力パラメータとしてカスタム エンティティのインスタンスを使用してワークフローを実行できるようにするには、カスタム エンティティを公開する必要があります。

前提条件

この操作を行うには、事前定義されたユーザー ロールにカスタム エンティティに関する権限を含める必要があります。

手順

- 1 メイン メニュー (≡) で [ライブラリ] を選択し、[サービス] で [カスタム エンティティ定義] を選択します。
 カスタム エンティティのリストがカード ビューで表示されます。カード ビューにはページあたり 12 個の項目が、名前を基準としてアルファベット順に表示されます。各カードには、カスタム エンティティの名前、エンティティがマッピングされている vRealize Orchestrator タイプ、エンティティのタイプ、および説明が表示されます（これらの情報を入手できる場合）。
- 2 選択したカスタム エンティティのカードで、[アクション] - [公開] の順に選択します。
 新しいダイアログが開きます。
- 3 カスタム エンティティ定義をサービス プロバイダに公開するのか、すべてのテナントに公開するのか、または選択したテナントのみに公開するのかを選択します。
- 4 [保存] をクリックして、変更を確定します。
 選択した公開先がカスタム エンティティ定義を使用できるようになります。


カスタム エンティティの削除

カスタム エンティティが使用されなくなった場合、正しく設定されていなかった場合、または vRealize Orchestrator タイプを別のカスタム エンティティにマッピングする場合は、カスタム エンティティ定義を削除できます。

前提条件

この操作を行うには、事前定義されたユーザー ロールにカスタム エンティティに関する権限を含める必要があります。

手順

- 1 メイン メニュー () で [ライブラリ] を選択し、[サービス] で [カスタム エンティティ定義] を選択します。

カスタム エンティティのリストがカード ビューで表示されます。カード ビューにはページあたり 12 個の項目が、名前を基準としてアルファベット順に表示されます。各カードには、カスタム エンティティの名前、エンティティがマッピングされている vRealize Orchestrator タイプ、エンティティのタイプ、および説明が表示されます（これらの情報を入手できる場合）。

- 2 選択したカスタム エンティティのカードで、[アクション] - [削除] の順に選択します。

- 3 削除を確認します。

カード ビューからカスタム エンティティが削除されます。