

VMware Cloud Director Service Provider Admin Portal ガイド

変更日 : 2021 年 4 月 8 日

VMware Cloud Director 10.2

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
〒108-0023 東京都港区芝浦 3-1-1
田町ステーションタワー N 18 階
www.vmware.com/jp

Copyright © 2018-2021 VMware, Inc. All rights reserved. [著作権および商標情報](#)。

目次

1	VMware Cloud Director™ Service Provider Admin Portal ガイド	10
2	VMware Cloud Director Service Provider Admin Portal の概要	11
	VMware Cloud Director 管理の概要	11
	VMware Cloud Director Service Provider Admin Portal へのログイン	14
	VMware Cloud Director クイック検索の使用	15
	タスクの表示	16
	進行中のタスクの停止	16
	イベントの表示	16
	ユーザー環境設定の設定	17
	名前と説明に対する長さの制限	18
3	vSphere リソースの管理	19
	vCenter Server および NSX リソースの追加	20
	vCenter Server インスタンスを単独、または NSX Manager インスタンスと共に接続する	20
	vApp の検出および採用	24
	vCenter Server で NSX ライセンス キーを割り当てる	26
	NSX-T Manager インスタンスの登録	26
	NSX Advanced ロード バランシングの管理	27
	VMware Cloud Director エンドポイントとプロキシを使用した vSphere コンポーネントへのアクセス	31
	エンドポイントの作成	32
	基盤となる vCenter Server リソースにアクセスするためのプロキシの追加	33
	プロキシ証明書および CRL の管理	34
	クラウド リソースの追加	34
	プロバイダ仮想データセンター	35
	プロバイダ仮想データセンターの作成	35
	外部ネットワーク	39
	ネットワーク プール	42
	vCenter Server インスタンスの表示	46
	vCenter Server 設定の変更	47
	vCenter Server インスタンスの有効化または無効化	48
	vCenter Server インスタンスの再接続	48
	vCenter Server インスタンスの更新	49
	vCenter Server インスタンスのストレージ ポリシーの更新	49
	vCenter Server インスタンスの登録解除	49
	NSX Manager 設定の変更	50
	NSX-T Manager 設定の変更	51
	NSX-T Manager インスタンスの削除	51

マルチサイト展開の構成と管理	52
マルチサイト リソース リスト	54

4 プロバイダ仮想データセンターの管理 56

プロバイダ仮想データセンターの有効化または無効化	56
プロバイダ仮想データセンターの削除	57
プロバイダ仮想データセンターの全般設定の編集	57
プロバイダ仮想データセンターのマージ	58
プロバイダ仮想データセンターの組織仮想データセンターの表示	59
プロバイダ仮想データセンター上のデータストアの表示	59
プロバイダ仮想データセンターの外部ネットワークの表示	60
VMware Cloud Director での Kubernetes の使用	60
vSphere with VMware Tanzu クラスタの作成	64
ネイティブ Kubernetes クラスタの作成	70
VMware Tanzu Kubernetes Grid Integrated Edition クラスタの作成	72
プロバイダ仮想データセンターでの仮想マシン ストレージ ポリシーの管理	73
プロバイダ仮想データセンターのストレージ ポリシーでの仮想マシン暗号化の有効化	73
プロバイダ仮想データセンターへの仮想マシン ストレージ ポリシーの追加	75
プロバイダ仮想データセンター上の仮想マシン ストレージ ポリシーの有効化または無効化	75
プロバイダ仮想データセンターからの仮想マシン ストレージ ポリシーの削除	76
プロバイダ仮想データセンター上の仮想マシン ストレージ ポリシーのメタデータの変更	76
1 秒あたりの I/O 処理数の設定の有効化	77
プロバイダ VDC ストレージ ポリシーの設定の編集	79
ストレージ ポリシーがサポートするエンティティ タイプの編集	79
プロバイダ仮想データセンターでのリソース プールの管理	80
プロバイダ仮想データセンターへのリソース プールの追加	80
プロバイダ仮想データセンター上のリソース プールの有効化または無効化	81
プロバイダ仮想データセンターからのリソース プールの分離	82
プロバイダ仮想データセンターのメタデータの変更	82

5 組織の管理 84

リースについて	84
組織の作成	85
組織の有効化または無効化	85
組織の削除	86
組織のカatalogの設定	86
組織のポリシーの設定	86
テナント ストレージの移行	88
組織のリソース使用に対する割り当て容量の管理	89

6 組織仮想データセンターの管理 90

割り当てモデルについて	90
推奨される割り当てモデルの使用法	92
Flex 割り当てモデル	93
割り当てプール割り当てモデル	94
従量課金制の割り当てモデル	95
予約プール割り当てモデル	96
仮想マシン サイズ変更ポリシーと仮想マシン配置ポリシーについて	96
プロバイダ VDC 内での仮想マシン配置ポリシーの作成	100
グローバルな仮想マシン配置ポリシーの作成	102
仮想マシンの配置ポリシーの編集	103
組織 VDC への仮想マシン配置ポリシーの追加	103
仮想マシン配置ポリシーの削除	104
仮想マシン サイズ変更ポリシーの属性	105
仮想マシン サイズ変更ポリシーの作成	106
組織 VDC への仮想マシン サイズ変更ポリシーの追加	107
仮想マシン サイズ変更ポリシーの編集	107
仮想マシン サイズ変更ポリシーの削除	108
VMware Cloud Director での Kubernetes の使用	108
組織 VDC Kubernetes ポリシーの追加	112
組織 VDC Kubernetes ポリシーの編集	113
Tanzu Kubernetes クラスタの作成	114
ネイティブ Kubernetes クラスタの作成	115
VMware Tanzu Kubernetes Grid Integrated Edition クラスタの作成	117
組織仮想データセンターの作成	118
組織仮想データセンターの有効化または無効化	121
組織仮想データセンターの削除	121
仮想データセンター テンプレートの管理	121
組織仮想データセンター テンプレートの作成	122
テンプレートからの仮想データセンターのインスタンス化	125
組織 VDC テンプレートの編集	126
組織仮想データセンターの名前および説明の変更	129
組織仮想データセンターの割り当てモデルの設定の変更	129
組織仮想データセンターのストレージ設定の変更	130
組織仮想データセンターのストレージ ポリシーでの仮想マシン暗号化の有効化	130
組織仮想データセンターの仮想マシン プロビジョニング設定の変更	131
組織仮想データセンターへの仮想マシン ストレージ ポリシーの追加	132
組織仮想データセンターのデフォルト ストレージ ポリシーの変更	132
組織仮想データセンターのストレージ ポリシーの制限の編集	132
組織仮想データセンター上の仮想マシン ストレージ ポリシーのメタデータの変更	133
組織仮想データセンター上のストレージ ポリシーの有効化または無効化	134
組織仮想データセンターからの仮想マシン ストレージ ポリシーの削除	134

組織 VDC ストレージ ポリシーの設定の編集	134
組織仮想データセンターのネットワーク設定の編集	135
クロス仮想データセンター ネットワークの構成	136
組織仮想データセンターのメタデータの変更	138
組織仮想データセンターのリソース プールの表示	138
組織仮想データセンターの分散ファイアウォールの管理	138
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	139
分散ファイアウォール ルールの追加	139
分散ファイアウォール ルールの編集	142
オブジェクトのグループ分け (カスタム)	142
セキュリティ グループの操作	146
セキュリティ タグの操作	149

7 NSX Data Center for vSphere Edge Gateway の管理 154

NSX Data Center for vSphere Edge クラスタの操作	154
NSX Data Center for vSphere Edge Gateway の追加	156
NSX Data Center for vSphere Edge Gateway サービスの構成	158
NSX Data Center for vSphere Edge Gateway ファイアウォールの管理	158
NSX Data Center for vSphere Edge Gateway の DHCP の管理	162
SNAT または DNAT ルールの追加	166
高度なルーティングの設定	169
ロード バランシング	177
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	189
SSL 証明書の管理	214
オブジェクトのグループ分け (カスタム)	220
Edge Gateway のネットワーク使用と IP 割り当ての表示	224
Edge ゲートウェイのプロパティの編集	224
Edge Gateway での分散ルーティングの有効化または無効化	224
外部ネットワークと Edge Gateway 設定の変更	224
Edge Gateway の全般設定の編集	225
Edge Gateway のデフォルト ゲートウェイの編集	226
Edge Gateway の IP アドレスの設定の編集	226
Edge ゲートウェイ上の細分割り当てされた IP アドレス プールの編集	226
Edge ゲートウェイ上のレート制限の編集	227
Edge Gateway の再デプロイ	227
Edge ゲートウェイの削除	228
Edge Gateway の統計情報とログ	228
統計情報の表示	228
ログの有効化	229
SSH コマンドラインによる Edge Gateway へのアクセスの有効化	230

8 NSX-T Data Center Edge Gateway の管理 232

専用外部ネットワーク 232

NSX-T Data Center Edge Gateway の追加 233

NSX-T Data Center Edge Gateway への IP セットの追加 234

NSX-T Data Center Edge Gateway ファイアウォール ルールの追加 234

NSX-T Edge Gateway での SNAT ルールまたは DNAT ルールの追加 236

NSX-T Edge Gateway での DNS フォワーダ サービスの設定 238

NSX-T Edge Gateway の IP アドレスの割り当ての編集 239

迅速な IP アドレスの割り当て 240

カスタム アプリケーション ポート プロファイルの作成 240

NSX-T Data Center Edge Gateway のポリシーベースの IPsec VPN 241

NSX-T ポリシーベースの IPsec VPN の設定 242

IPsec VPN トンネルのセキュリティ プロファイルのカスタマイズ 243

専用の外部ネットワーク サービスの設定 244

ルート アドバタイズの管理 244

BGP の全般設定 245

IP アドレス プリフィックス リストの作成 246

BGP ネイバーの追加 247

NSX-T Data Center Edge Gateway での NSX Advanced ロード バランシングの管理 249

NSX-T Data Center Edge Gateway でのロード バランサの有効化 249

NSX-T Data Center Edge Gateway へのサービス エンジン グループの割り当て 249

サービス エンジン グループの設定の編集 250

ロード バランサ サーバ プールの追加 251

仮想サービスの作成 253

9 専用 vCenter Server インスタンスの管理 255

接続された vCenter Server のテナント アクセスの有効化 258

専用 vCenter Server の公開 258

10 システム管理者およびロールの管理 260

権限およびロールの管理 260

事前定義ロールとその権限 262

システム管理者の権限 264

事前定義グローバル テナント ロールの権限 277

権限バンドルの管理 283

グローバル テナント ロールの管理 285

プロバイダ ロールの管理 288

プロバイダ ユーザーおよびグループの管理 291

プロバイダ ユーザーの管理 291

プロバイダ グループの管理 294

11 システム設定の管理 296

- 全般システム設定の変更 296
- 全般システム設定 297
- サーバ グループのセルに対する FIPS モードの有効化 298
- システム メールの設定 300
- VMware Cloud Director ライセンスの変更 301
- カタログ同期の設定 301
- アドバイザリ ダッシュボードの作成 302
- ブロック タスクおよび通知の構成と監視 303
 - AMQP ブローカーの構成 303
 - ブロック タスク設定の構成 304
 - ブロックされているタスクの監視 305
- 公開アドレスの構成 305
- ID プロバイダの管理 307
 - LDAP 接続の管理 307
 - システムでの SAML ID プロバイダの使用を有効化 310
- 証明書の管理 312
 - 信頼されている証明書のインポート 312
 - 証明書ライブラリへの証明書のインポート 313
- プラグインの管理 314
 - プラグインのアップロード 314
 - プラグインの有効化または無効化 315
 - プラグインの削除 315
 - 組織からのプラグインの公開または公開解除 315
- VMware Cloud Director ポータルのカスタマイズ 316
- パスワード ポリシーの設定 317
- vSphere サービスの構成 318

12 VMware Cloud Director の監視 319

- VMware Cloud Director およびコスト レポート作成 319
- プロバイダ仮想データセンターの使用情報の表示 319

13 サービスの管理 321

- vRealize Orchestrator と VMware Cloud Director の統合 321
 - VMware Cloud Director への vRealize Orchestrator インスタンスの登録 322
- サービス カテゴリの作成 323
- サービス カテゴリの編集 323
- サービスのインポート 324
- サービスの検索 324
- サービスの実行 325
- サービス カテゴリの変更 326

サービスの登録解除 326

サービスの公開 326

14 定義済みエンティティの管理 328

定義済みエンティティの共有 329

カスタム エンティティの管理 331

 カスタム エンティティの検索 331

 カスタム エンティティ定義の編集 331

 カスタム エンティティ定義の追加 332

 カスタム エンティティ インスタンス 333

 カスタム エンティティへのアクションの関連付け 333

 カスタム エンティティからのアクションの関連付け解除 334

 カスタム エンティティの公開 334

 カスタム エンティティの削除 335

VMware Cloud Director™ Service Provider Admin Portal ガイド

1

『VMware Cloud Director Service Provider Admin Portal ガイド』には、Service Provider Admin Portal の使用方法に関する情報が示されています。service provider admin portal は、クラウド内の組織、権限、ロール、ユーザー、グループの管理と監視に使用します。NSX-T でバックアップされた組織仮想データセンター ネットワークの作成および管理も可能になります。

対象読者

このガイドは、VMware Cloud Director Service Provider Admin Portal の機能を使用するサービス プロバイダの管理者を対象としています。

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 のテクニカル ドキュメントで使用されている用語の定義については、<https://docs.vmware.com> をご覧ください。

VMware Cloud Director Service Provider Admin Portal の概要

2

VMware Cloud Director Service Provider Admin Portal は、サービス プロバイダ管理者の専用インターフェイスです。

この章には、次のトピックが含まれています。

- VMware Cloud Director 管理の概要
- VMware Cloud Director Service Provider Admin Portal へのログイン
- VMware Cloud Director クイック検索の使用
- タスクの表示
- 進行中のタスクの停止
- イベントの表示
- ユーザー環境設定の設定
- 名前と説明に対する長さの制限

VMware Cloud Director 管理の概要

VMware VMware Cloud Director を使用すると、仮想インフラストラクチャ リソースを仮想データセンターにプールし、Web ベースのポータルおよびプログラム インターフェイスを通じて完全に自動化されたカタログベースのサービスとしてリソースをユーザーに公開することで、安全なマルチテナントのクラウドを構築できます。

『VMware Cloud Director Service Provider Admin Portal Guide』では、システムへのリソースの追加、組織の作成とプロビジョニング、リソースと組織の管理、およびシステムの監視に関する情報を提供します。

vSphere および NSX リソース

VMware Cloud Director は、vSphere リソースを使用して、仮想マシンを実行するための CPU およびメモリを提供します。さらに、vSphere データストアは、仮想マシンの操作に必要な仮想マシン ファイルおよびその他のファイルのストレージを提供します。また、VMware Cloud Director は vSphere 分散スイッチ、vSphere ポートグループ、および NSX Data Center for vSphere も使用して仮想マシンのネットワークをサポートします。

VMware Cloud Director は NSX-T Data Center のリソースも使用できます。クラウドへの NSX-T Manager インスタンスの登録の詳細については、VMware Cloud Director Service Provider Admin Portal Guide または VMware Cloud Director API プログラミング ガイドを参照してください。

基盤となる vSphere および NSX リソースを使用して、クラウド リソースを作成できます。

バージョン 9.7 以降では、VMware Cloud Director は HTTP プロキシ サーバとして機能するため、組織が基盤となる vSphere 環境にアクセスできるように設定することが可能です。

クラウド リソース

クラウド リソースは、基盤となる vSphere リソースを抽象化したものです。VMware Cloud Director 仮想マシンおよび vApp のコンピューティング リソースとメモリ リソースを提供します。vApp は、1 台以上の個々の仮想マシンが、動作の詳細を定義するパラメータとともに含まれている仮想システムです。クラウド リソースからは、ストレージにアクセスし、ネットワークと接続することもできます。

クラウド リソースにはプロバイダおよび組織の仮想データセンター、外部ネットワーク、組織仮想データセンター ネットワーク、ネットワーク プールがあります。

クラウド リソースを VMware Cloud Director に追加するには、事前に vSphere リソースを追加する必要があります。

専用 vCenter Server インスタンスおよびプロキシ

専用 vCenter Server インスタンスは、vCenter Server インストール全体をカプセル化するクラウド リソースです。専用 vCenter Server インスタンスには、基盤となる vSphere 環境のさまざまなコンポーネントへのアクセスポイントとなるプロキシが 1 つ以上含まれています。プロバイダは、専用 vCenter Server インスタンスおよびプロキシを作成して有効にすることができます。プロバイダは、専用 vCenter Server インスタンスをテナントに公開できます。

専用 vCenter Server インスタンスおよびプロキシを作成および管理するには、Service Provider Admin Portal または vCloud OpenAPI を使用します。9 章 [専用 vCenter Server インスタンスの管理](#)、および <https://code.vmware.com> にある『VMware Cloud Director OpenAPI のスタート ガイド』を参照してください。

プロバイダ仮想データセンター

プロバイダ仮想データセンターでは、1 つの vCenter Server リソース プールのコンピューティング リソースとメモリ リソースを、そのリソース プールで使用可能な 1 つ以上のデータストアのストレージ リソースと結合します。

プロバイダ仮想データセンターは、vCenter Server インスタンスに関連付けられている NSX Manager インスタンス、またはクラウドに登録されている NSX-T Manager インスタンスのネットワーク リソースを使用できます。

場所やビジネス ユニットの異なるユーザーやパフォーマンス要件の異なるユーザーのために、複数のプロバイダ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

組織仮想データセンターは、組織にリソースを提供し、プロバイダ仮想データセンターからパーティションで区切られています。組織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。また、フロッピー ディスクや CD ROM などの仮想メディアのストレージともなります。

1 つの組織が複数の組織仮想データセンターを持つことができます。

VMware Cloud Director ネットワーク

VMware Cloud Director は 3 種類のネットワークをサポートします。

- 外部ネットワーク
- 組織仮想データセンター ネットワーク
- vApp ネットワーク

一部の組織仮想データセンター ネットワークとすべての vApp ネットワークは、ネットワーク プールによってバックアップされます。

外部ネットワーク

外部ネットワークは、vSphere ポート グループに基づいた、論理的で区別されているネットワークです。組織仮想データセンター ネットワークを外部ネットワークに接続すれば、vApp 内部の仮想マシンをインターネットに接続できます。

バージョン 9.5 以降、VMware Cloud Director は IPv6 外部ネットワークをサポートします。IPv6 外部ネットワークは IPv4 サブネットと IPv6 サブネットの両方をサポートし、IPv4 外部ネットワークは IPv4 サブネットと IPv6 サブネットの両方をサポートします。

デフォルトでは、外部ネットワークを作成および管理できるのは、システム管理者のみです。

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、VMware Cloud Director 組織仮想データセンターに属していて、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。外部接続を提供する場合は、組織仮想データセンター ネットワークを外部ネットワークに接続することができます。また、組織の内部に、隔離された組織仮想データセンター ネットワークを作成することもできます。

VMware Cloud Director 9.5 では、直接ネットワークおよび経路指定された組織仮想データセンター ネットワークに対する IPv6 サポートが導入されました。

VMware Cloud Director 9.5 以降、システム管理者は、NSX-T 論理スイッチによってバックアップされ、隔離された仮想データセンター ネットワークを作成することができます。組織管理者は、ネットワーク プールによってバックアップされ、隔離された仮想データセンター ネットワークを作成することができます。

VMware Cloud Director 9.5 では、仮想データセンター グループ内に拡張ネットワークを構成することによって、クロス仮想データセンター ネットワークも導入しています。

デフォルトでは、直接ネットワークおよびクロス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。システム管理者と組織管理者は組織仮想データセンター ネットワークを管理できますが、組織管理者が管理できる内容には制限があります。

vApp ネットワーク

vApp ネットワークは vApp に属していて、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 が組織内の他の vApp と通信できるようにするには、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します。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、vApp は他の組織の vApp と通信できます。vApp ネットワークは、ネットワーク プールによってバックアップされます。

vApp にアクセス可能なほとんどのユーザーは、独自の vApp ネットワークを作成して管理できます。vApp でのネットワークの操作方法については、『VMware Cloud Director Tenant Portal Guide』を参照してください。

ネットワーク プール

ネットワーク プールは、組織仮想データセンター内で使用可能な、区別されていないネットワークのグループです。ネットワーク プールは、VLAN ID やポート グループのような vSphere ネットワーク リソースによってバックイングされます。VMware Cloud Director はネットワーク プールを使用して、NAT を経由する内部組織仮想データセンター ネットワークおよびすべての vApp ネットワークを作成します。プールの各ネットワークにおけるネットワークトラフィックは、他のすべてのネットワークからレイヤ 2 で隔離されます。

VMware Cloud Director では各組織仮想データセンターに 1 つのネットワーク プールを指定できます。複数の組織仮想データセンターで 1 つのネットワーク プールを共有できます。組織仮想データセンターのネットワーク プールは、組織仮想データセンターのネットワーク割り当て容量を満たすために作成されるネットワークを提供します。ネットワーク プールを作成および管理できるのは、システム管理者のみです。

組織

VMware Cloud Director は組織を使用することでマルチテナントをサポートします。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。組織管理者のタスクについては『VMware Cloud Director Tenant Portal Guide』を参照してください。

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。組織管理者は、ユーザーを作成し、LDAP などのディレクトリ サービスからユーザーとグループをインポートできます。システム管理者は、各組織で使用可能な権限のセットを管理します。システム管理者は、作成し、グローバル テナントのロールを作成し、1 つ以上の組織に公開できます。組織管理者は、自分の組織のローカル ロールを作成できます。

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、カタログを含んでいる 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。システム管理者は、他の組織が利用できるようにするため、カタログの公開を組織に許可することができます。その後、組織管理者は、ユーザーに提供するカタログ項目を決定できます。

VMware Cloud Director Service Provider Admin Portal へのログイン

Web ブラウザを使用して VMware Cloud Director Service Provider Admin Portal にアクセスできます。

前提条件

VMware Cloud Director Service Provider Admin Portal にアクセスするには、システム管理者の権限が必要です。

手順

- 1 ブラウザで VMware Cloud Director サイトの Service Provider Admin Portal の URL を入力して、Enter を押します。

たとえば、**https://vcloud.example.com/provider** と入力します。

- 2 システム管理者のユーザー名とパスワードを使用してログインします。

VMware Cloud Director クイック検索の使用

VMware Cloud Director クイック検索を使用して、画面、エンティティ、およびアクションを検索できます。検索結果は、ユーザー インターフェイス内の位置に依存します。

結果はコンテキストや、エンティティが選択されているかどうか、特定のエンティティに対して使用可能なアクションに依存します。検索結果はセクションごとにグループ化されます。

- グローバル ナビゲーション - このセクションの結果は、Edge Gateway、LDAP、タスク、信頼されている証明書、仮想マシンなどの特定のエンティティに関係しません。これらの検索結果は、ユーザー インターフェイス内の位置には依存しません。
- コンテキスト ナビゲーション - このセクションの結果は、ユーザー インターフェイス内で選択したエンティティに依存します。たとえば、仮想マシン、ネットワーク図などの vApp 固有のビューなどが該当します。vApp のようなエンティティを選択した場合は、グローバル ナビゲーションとコンテキスト ナビゲーションの両方の結果、およびエンティティに適用可能なアクションが表示されます。
- コンテキスト アクション - このセクションの結果は、ユーザー インターフェイス内で選択したエンティティに依存します。ユーザー インターフェイス内の位置や選択したエンティティにより、クイック検索結果を使用することで、エンティティに関連するアクションを実行できることがあります。たとえば、仮想マシンの詳細ビューから検索すると、選択した仮想マシンで実行できるグローバル ビュー、コンテキスト ビュー、およびアクションの結果が表示されます。
- 名前によるエンティティ検索 - エンティティのリストを表示している場合、検索結果に、リスト内のエンティティと同じタイプのエンティティの名前を含めることもできます。たとえば、仮想マシンのリストを表示している場合、検索結果にはグローバル ナビゲーションの一致と仮想マシンの名前の一致が含まれます。表示しているリストにエンティティのページが複数含まれている場合は、検索によってエンティティの完全なリストがチェックされ、現在のページに表示されていない名前が表示されることがあります。

手順

- 1 [クイック検索] ウィンドウを開きます。
 - 上部ナビゲーション バーで、[ヘルプ] メニューをクリックし [クイック検索] を選択します。
 - オペレーティング システムに応じて Ctrl+. または Cmd+. を押します。
- 2 検索条件を入力します。
- 3 結果を参照してオプションを選択するか、Enter をクリックするか押して、アクションを実行します。

上矢印キーと下矢印キーを使用して、検索結果を参照できます。

タスクの表示

Service Provider Admin Portal から最近のタスクとそのステータスを表示できます。

最近のタスク ビューを使用して、Service Provider Admin Portal のタスクのステータスを監視できます。このビューは、環境内で発生する問題のトラブルシューティングを行う場合に、最初のステップとして利用できます。

[最近のタスク] ボタンの横に、実行中のタスクが青色で、失敗したタスクが赤色で表示されます。

手順

- 1 左下隅で、[最近のタスク] をクリックします。
- 2 (オプション) 最近のタスクのリストをソートおよびフィルタリングします。

結果

最近のタスクのリストが、タスクのステータス、タイプ、開始元、および開始時刻と完了時刻とともに表示されます。

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 上部ナビゲーション バーで、[監視] と [イベント] をクリックします。
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.cloud</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。

ユーザー環境設定の設定

ユーザーがシステムにログインするたびに有効になる、特定の表示とシステム警告の環境設定を設定できます。

リースの詳細については、[リースについて](#)を参照してください。

手順

- 1 上部のナビゲーション バーで、ユーザー名をクリックし、[ユーザー環境設定] を選択します。
- 2 ログインしたときに表示するページを選択します。
 - a [開始ページ] の横にあるラジオ ボタンを選択し、[編集] をクリックします。
 - b ドロップダウン メニューからオプションを選択し、[保存] をクリックします。
- 3 ランタイム リースの有効期限に関する E メール通知を構成します。
 - a [展開リース アラート時間] の横にあるラジオ ボタンを選択し、[編集] をクリックします。
 - b 秒単位で値を入力し、[保存] をクリックします。

4 ストレージ リースの有効期限に関する E メール通知を構成します。

- a [ストレージ リース アラート時間] の横にあるラジオボタンを選択し、[編集] をクリックします。
- b 秒単位で値を入力し、[保存] をクリックします。

名前と説明に対する長さの制限

VMware Cloud Director で値を入力するときは、次のガイドラインに従ってください。

name 属性、Description 要素、および ComputerName 要素の文字列の値には、長さの制限があります。この制限は、文字列の値が添付されるオブジェクトによって異なります。

表 2-1. オブジェクトのプロパティに対する長さの制限

オブジェクト	プロパティ	最大文字長
Catalog	name	128
Catalog	Description	256
EdgeGateway	name	35
Media	name	128
Media	Description	256
VApp	name	128
VApp	Description	256
VAppTemplate	name	128
VAppTemplate	Description	256
Vdc	name	128
Vdc	Description	256
Vm	name	128
Vm	ComputerName	Windows の場合は 15、他のすべてのプラットフォームの場合は 63
Vm	Description	256

vSphere リソースの管理

3

VMware Cloud Director は、基盤となる vSphere 仮想インフラストラクチャからそのリソースを取得します。vSphere リソースを VMware Cloud Director に登録したら、これらのリソースを、vSphere インストール環境の組織で使用するために割り当てることができます。

VMware Cloud Director は、1 つ以上の vCenter Server 環境を使用して、その仮想データセンターをバックアップします。バージョン 9.7 以降、VMware Cloud Director は vCenter Server 環境を使用して、1 つ以上のプロキシと共に SDDC をカプセル化することもできます。ユーザーは、テナントが自身の VMware Cloud Director アカウントを使用して、VMware Cloud Director から基盤となる vSphere 環境へのアクセスポイントとしてこれらのプロキシを使用できるようにすることができます。

VMware Cloud Director で vCenter Server インスタンスを使用するには、事前にこの vCenter Server インスタンスを接続する必要があります。

接続された vCenter Server インスタンスによってバックアップされるプロバイダ仮想データセンターを作成すると、この vCenter Server インスタンスは、サービス プロバイダに公開済み（またはプロバイダによって範囲指定済み）として表示されます。プロバイダ仮想データセンターの作成に関する詳細については、『[プロバイダ仮想データセンターの作成](#)』を参照してください。

接続された vCenter Server インスタンスをカプセル化する SDDC を作成すると、その vCenter Server はテナント専用になります。この vCenter Server インスタンスはテナントに公開済み（またはテナントによって範囲指定済み）として表示されます。SDDC の作成方法の詳細については、[9 章 専用 vCenter Server インスタンスの管理](#) を参照してください。

注： デフォルトでは、vCenter Server インスタンスが接続されている場合、プロバイダ仮想データセンターまたは専用 vCenter Server インスタンスのいずれかを作成できます。vCenter Server インスタンスによってバックアップされるプロバイダ仮想データセンターを作成した場合、この vCenter Server インスタンスを使用して専用 vCenter Server インスタンスを作成したり、その逆を行ったりすることはできません。

一元化された SSL 管理

バージョン 10.1 以降の VMware Cloud Director は、証明書を管理するために、一元化されたテナント対応のストレージエリアに移動しています。そうすることで、VMware Cloud Director はすべての証明書を 1 か所に統合し、システム内のさまざまなコンポーネントで使用されているすべての証明書をシステム管理者および組織管理者が表示、監査、および管理できるようにします。VMware Cloud Director API を使用して、新しいテナント対応のストレージエリアの証明書を追加、更新、または削除できます。VMware Cloud Director API スキーマ リファレンスを参照してください。

新しい vCenter Server インスタンス、NSX Manager インスタンス、または NSX-T Manager インスタンスを追加または編集すると、VMware Cloud Director ユーザー インターフェイスによって、エンドポイントが提示する証明書が調査されます。VMware Cloud Director は、信頼される証明書を中央の証明書ストレージ エリアに追加します。

この章には、次のトピックが含まれています。

- vCenter Server および NSX リソースの追加
- VMware Cloud Director エンドポイントとプロキシを使用した vSphere コンポーネントへのアクセス
- クラウド リソースの追加
- vCenter Server インスタンスの表示
- vCenter Server 設定の変更
- vCenter Server インスタンスの有効化または無効化
- vCenter Server インスタンスの再接続
- vCenter Server インスタンスの更新
- vCenter Server インスタンスのストレージ ポリシーの更新
- vCenter Server インスタンスの登録解除
- NSX Manager 設定の変更
- NSX-T Manager 設定の変更
- NSX-T Manager インスタンスの削除
- マルチサイト展開の構成と管理
- マルチサイト リソース リスト

vCenter Server および NSX リソースの追加

VMware Cloud Director は、vSphere リソースを使用して、仮想マシンを実行するための CPU、メモリ、およびストレージを提供します。また、バージョン 9.7 以降では、VMware Cloud Director はテナントと基盤となる vSphere 環境の間で HTTP サーバとして機能することができます。

vCenter Server および ESXi の VMware Cloud Director システム要件およびサポート対象バージョンの詳細については、http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php にある「VMware 製品の相互運用性マトリックス」を参照してください。

vCenter Server インスタンスを単独、または NSX Manager インスタンスと共に接続する

vCenter Server インスタンスを接続して、そのリソースが VMware Cloud Director で使用可能になるようにできます。vCenter Server インスタンスは、関連付けられている NSX Manager インスタンスと一緒に接続できます。専用の vCenter Server インスタンス、または NSX-T Manager インスタンスに関連付けられているインスタンスの場合は、vCenter Server インスタンスを単独で接続できます。

VMware Cloud Director は、関連付けられた NSX Manager インスタンスまたは NSX-T Manager インスタンスと共に vCenter Server インスタンスを使用できます。

VMware Cloud Director で、この vCenter Server インスタンスを関連付けられた NSX Manager インスタンスと共に使用する場合は、vCenter Server および NSX Manager インスタンスを共に接続する必要があります。

VMware Cloud Director で、この vCenter Server インスタンスを NSX-T Manager インスタンスと共に使用する場合は、vCenter Server インスタンスを単独で接続する必要があります。vCenter Server インスタンスを単独で接続した後は、[NSX-T Manager インスタンスの登録](#)を実行する必要があります。

注： vCenter Server インスタンスを単独で接続した後は、関連付けられた NSX Manager インスタンスを後から追加することはできません。vCenter Server インスタンスを登録解除してから、関連付けられた NSX Manager インスタンスと共に再度接続することができます。

vCenter Server インスタンスは、VMware Cloud Director 環境から任意のサイトに接続できます。

直接アクセス可能な vCenter Server インスタンスを接続することも、プロキシの背後にある vCenter Server インスタンスを接続することもできます。vCloud OpenAPI を使用することにより、VMware Cloud Director 内のプロキシ設定を使用して、VMware Cloud Director インスタンスとそこに追加された vCenter Server インスタンスとの間にプロキシ接続を作成できます。この方法では、VMware Cloud Director インスタンスと vCenter Server インスタンスを異なる場所またはサイトに配置することができます。

プロキシの背後にある vCenter Server インスタンスを接続するには、まずプロキシ設定を宣言する必要があります。その後、vCenter Server インスタンスを接続し、vCenter Server インスタンスにアクセスするときにプロキシ設定を使用するように VMware Cloud Director を設定する必要があります。プロキシを介して NSX Data Center for vSphere ソリューションを接続することもできます。VMware Cloud Director は NSX-T Data Center のプロキシ設定をサポートしていません。vCenter Server インスタンスが登録されている Platform Services Controller に SSL 設定またはプロキシ設定を追加する必要はありません。

前提条件

- vCenter と vSphere の SSO 証明書を検証するように VMware Cloud Director を設定した場合は、vCenter Server の証明書を VMware Cloud Director にアップロードしたことを確認します。全般的なシステム設定の詳細については、『[全般システム設定の変更](#)』を参照してください。
- NSX Manager の証明書を検証するように VMware Cloud Director を設定した場合は、NSX Manager の証明書を VMware Cloud Director にアップロードしたことを確認します。全般的なシステム設定の詳細については、『[全般システム設定の変更](#)』を参照してください。

手順

1 [vCenter Server インスタンスの追加](#)

vCenter Server インスタンスを追加するには、vCenter Server アクセスの詳細を入力します。

2 (オプション) [関連付けられた NSX Manager インスタンスの追加](#)

VMware Cloud Director で、この vCenter Server インスタンスを関連付けられた NSX Manager インスタンスと共に使用する場合は、NSX Manager アクセス詳細を追加する必要があります。

vCenter Server インスタンスの追加

vCenter Server インスタンスを追加するには、vCenter Server アクセスの詳細を入力します。

手順

- 1 上部ナビゲーション バーの [リソース] で [インフラストラクチャ リソース] をクリックします。
- 2 左側のペインで、[vCenter Server インスタンス] をクリックし、[追加] をクリックします。
- 3 マルチサイト VMware Cloud Director デプロイを使用している場合は、[サイト] ドロップダウン メニューから、この vCenter Server インスタンスを追加するサイトを選択し、[次へ] をクリックします。
- 4 VMware Cloud Director の vCenter Server インスタンスの名前と、オプションで説明を入力します。
- 5 vCenter Server インスタンスの URL を入力します。

デフォルト ポートが使用されている場合は、ポート番号をスキップできます。カスタム ポートが使用されている場合は、ポート番号を含めます。

たとえば、**`https://FQDN_or_IP_address:<custom_port_number>`** のようになります。

- 6 vCenter Server 管理者アカウントのユーザー名とパスワードを入力します。
- 7 (オプション) 登録後に vCenter Server インスタンスを無効にするには、[有効] トグルをオフにします。
- 8 vCenter Server Web Client の URL を構成します。

オプション	説明
[vSphere サービスを利用して URL を指定]	このオプションを使用するには、vCloud API を使用して、vSphere Lookup Service を使用するように VMware Cloud Director を設定する必要があります。
[vSphere Web Client の URL]	このオプションを使用するには、vSphere Web Client の URL を入力する必要があります。 例： <code>https://example.vmware.com/vsphere-client</code> 。

- 9 [次へ] をクリックします。
- 10 エンドポイントに信頼されている証明書がない場合は、[信頼証明書] ウィンドウで、エンドポイントを信頼するかどうかを確認します。

マルチサイト環境で、vCloud Director 10.0 サイトにログインしている場合、または vCenter Server インスタンスを vCloud Director 10.0 サイトに登録する場合、VMware Cloud Director は中央の証明書ストレージ エリアにエンドポイントを追加しません。

- エンドポイントを中央の証明書ストレージ エリアに追加して続行するには、[信頼] をクリックします。
- このエンドポイントを信頼しない場合は、[キャンセル] をクリックし、信頼できるエンドポイントで **手順 5** から **手順 9** までを繰り返します。

- 11 (オプション) vCenter Server インスタンスに関連付けられている NSX Manager インスタンスの追加をスキップするには、[設定] を無効に切り替え、[次へ] をクリックします。

VMware Cloud Director で、この vCenter Server インスタンスを NSX-T Manager インスタンスと共に使用する場合は、vCenter Server インスタンスを単独で追加する必要があります。

注： 関連付けられた NSX Manager インスタンスを後から追加することはできません。vCenter Server インスタンスを登録解除してから、関連付けられた NSX Manager インスタンスと共に再度接続することができます。

- 12 プロバイダ VDC として使用されないテナント専用の vCenter Server を追加する場合は、[テナント アクセスの有効化] をオンに切り替えます。

vCenter Server インスタンスを VMware Cloud Director に追加すると、テナント関連情報がインスタンスの詳細ビューに表示されます。

- 13 VMware Cloud Director でデフォルトのプロキシが vCenter Server インスタンスと SSO サービスに対して生成されるようにする場合、[プロキシの生成] を有効に切り替えます。

vCenter Server インスタンスを VMware Cloud Director に追加すると、プロキシが [vSphere リソース] の [プロキシ] タブに表示されます。

- 14 [設定内容の確認] 画面で詳細を確認し、[完了] をクリックします。

(オプション) 関連付けられた NSX Manager インスタンスの追加

VMware Cloud Director で、この vCenter Server インスタンスを関連付けられた NSX Manager インスタンスと共に使用する場合は、NSX Manager アクセス詳細を追加する必要があります。

手順

- 1 [NSX-V Manager] 画面で、[設定] を有効のままにします。
- 2 NSX Manager インスタンスの URL を入力します。

デフォルト ポートが使用されている場合は、ポート番号をスキップできます。カスタム ポートが使用されている場合は、ポート番号を含めます。

たとえば、**`https://FQDN_or_IP_address:<custom_port_number>`** のようになります。

- 3 NSX 管理者アカウントのユーザー名とパスワードを入力します。

- 4 (オプション) この vCenter Server インスタンスによってバックアップされている仮想データセンターに対してクロス仮想データセンター ネットワークを有効にするには、[クロス VDC ネットワーク] をオンにして、コントロール仮想マシンのデプロイ プロパティとネットワーク プロバイダ範囲の名前を入力します。

コントロール仮想マシンのデプロイ プロパティは、ユニバーサル ルーターのようなクロス仮想データセンター ネットワーク コンポーネントの NSX Manager インスタンスにアプライアンスをデプロイする際に使用されます。

オプション	説明
ネットワーク プロバイダ範囲	データセンター グループのネットワーク トポロジ内のネットワーク フォルト ドメインに対応しています。例: boston-fault1 。 クロス仮想データセンター グループの管理については、『VMware Cloud Director Tenant Portal Guide』を参照してください。
リソース プール パス	クラスタから始まる vCenter Server インスタンスの特定のリソース プールへの階層パス (Cluster/Resource_Pool_Parent/Target_Resource)。例: TestbedCluster1/mgmt-rp 。 または、リソース プールの管理対象オブジェクト リファレンス ID を入力することもできます。例: resgroup-1476 。
データストア名	アプライアンスのファイルをホストするデータストアの名前。例: shared-disk-1 。
管理インターフェイス	HA 分散論理ルーター (DLR) 管理インターフェイスに使用されている vCenter Server またはポート グループ内のネットワーク名。例: TestbedPG1 。

- 5 [次へ] をクリックします。
- 6 エンドポイントに信頼されている証明書がない場合は、[信頼証明書] ウィンドウで、エンドポイントを信頼するかどうかを確認します。
- エンドポイントを中央の証明書ストレージ エリアに追加して続行するには、[信頼] をクリックします。
 - このエンドポイントを信頼しない場合は、[キャンセル] をクリックし、信頼できるエンドポイントで手順 2 から手順 4 までを繰り返します。
- 7 アクセス構成設定を有効または無効にします。
- 8 [設定内容の確認] 画面で詳細を確認し、[完了] をクリックします。

次のステップ

- vCenter Server で NSX ライセンス キーを割り当てる。
- プロバイダ仮想データセンターの作成。

vApp の検出および採用

デフォルト構成の場合、組織 VDC は、仮想データセンターをバックアップするいずれかの vCenter Server リソース プールで作成された仮想マシンを自動的に検出します。システムは簡単な vApp を作成して、検出された各仮想マシン (VM) を取り込みます。この vApp は、システム管理者が所有します。検出された vApp へのアクセス権がシステム管理者から付与されると、vApp の構成または再構成時に vApp 内の仮想マシンを参照できます。また、採用およびインポートする際に vApp を変更することもできます。

検出された vApp には、正確に 1 台の仮想マシンが含まれており、VMware Cloud Director で作成された vApp には適用されないいくつかの制約が課せられます。これらの vApp は、採用するかどうかにかかわらず、vApp の構成または再構成時に使用する仮想マシンのソースとして役立つ場合があります。

検出された各 vApp には、その中にある vCenter Server 仮想マシン名に由来する名前と、組織管理者が指定したプリフィックスが付与されます。

vApp を追加で検出する場合、システム管理者は VMware Cloud Director API を使用して、プロバイダ仮想データセンターにある指定したリソース プールを採用する組織仮想データセンターを作成できます。これらの採用されたリソース プール内の vCenter 仮想マシンは、検出された vApp として新しい仮想データセンターに表示され、採用の候補になります。

注： IDE ハード ドライブを搭載した仮想マシンは、パワーオフ状態の場合のみ検出されます。

1 台以上の vCenter 仮想マシンが VMware Cloud Director で検出されない場合、vCenter Server の仮想マシンの検出をデバッグすることにより、潜在的な原因を調査できます。詳細については、『VMware Cloud Director インストール、構成、およびアップグレード ガイド』を参照してください。

仮想マシンの検出の有効化

デフォルトでは、仮想マシンの検出は有効になっています。仮想マシンの検出を無効にするには、システム管理者が [システム設定] - [全般] タブにある [仮想マシンの検出を有効化] の選択を解除する必要があります。組織管理者は、VMware Cloud Director API を使用して、個々の VDC で仮想マシンの検出を無効にすることも、組織内のすべての VDC で仮想マシンの検出を無効にすることもできます。

検出された vApp からの仮想マシンの使用

検出された vApp へのアクセス権がシステム管理者から付与されると、他の vApp または vApp テンプレートに含まれる仮想マシンを使用すると同様の方法で、その仮想マシンを使用できます。たとえば、新しい vApp を作成するときに仮想マシンを指定できます。採用プロセスをトリガすることなく、検出された vApp のクローンを作成したり、その名前、説明、またはリース設定を変更したりできます。

検出された vApp の採用

検出された vApp を採用するには、vApp ネットワークを変更するか、この vApp に仮想マシンを追加します。検出された vApp を採用すると、その vApp は、VMware Cloud Director で作成された場合と同様にインポートおよび処理されます。採用された vApp が vCloud API 要求で取得された場合、この vApp には、autoNature という名前の要素が含まれます。検出された vApp が採用されていた場合、または VMware Cloud Director で作成されていた場合、この要素の値は false になります。採用された vApp を検出された vApp に戻すことはできません。

検出された vApp に含まれる仮想マシンを削除または移動すると、その仮想マシンを含んでいた vApp も削除されます。この動作は、採用された vApp には適用されません。

検出された vCenter 仮想マシンを含めるために作成される vApp は、仮想マシンを vApp として手動でインポートするときに作成される vApp と類似しています。ただし、この vApp よりも簡素化されており、vApp を変更しなければ仮想データセンターにデプロイできないようになっています。たとえば、そのネットワークとストレージのプロパティを編集し、組織の要件に固有のその他の調整を行う必要があります。

注： 仮想マシンを採用しても、vCenter Server で構成されている仮想マシンの予約、制限、および共有の設定は保持されません。インポートされた仮想マシンは、配置された組織仮想データセンターからリソース割り当ての設定を取得します。

vCenter Server で NSX ライセンス キーを割り当てる

vCenter Server インスタンスを関連付けられた NSX Manager インスタンスと共に接続した場合、vSphere Client を使用して、VMware Cloud Director ネットワークをサポートする NSX Manager インスタンスのライセンス キーを割り当てる必要があります。

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 vCenter Server システムに接続された vSphere Client ホストから、[ホーム] - [ライセンス] の順に選択します。
- 2 レポート ビューの場合、[資産] を選択します。
- 3 NSX Manager 資産を右クリックし、[ライセンス キーを変更] を選択します。
- 4 [このホストに新しいライセンス キーを割り当て] を選択し、[キーを入力] をクリックします。
- 5 ライセンス キーを入力し、キーの任意のラベルを入力して、[OK] をクリックします。

VMware Cloud Director を購入したときに受け取った NSX Manager ライセンス キーを使用します。このライセンス キーは複数の vCenter Server インスタンスで使用できます。

- 6 [OK] をクリックします。

NSX-T Manager インスタンスの登録

VMware Cloud Director がネットワーク リソースを使用できるように、NSX-T Manager インスタンスを VMware Cloud Director に登録することができます。プロバイダ仮想データセンターは、NSX Data Center for vSphere または NSX-T Data Center からネットワーク リソースを使用できます。

手順

- 1 上部ナビゲーション バーの [リソース] で [インフラストラクチャ リソース] をクリックします。
- 2 左側のペインで、[NSX-T Manager] をクリックし、[追加] をクリックします。
- 3 マルチサイト VMware Cloud Director デプロイを使用している場合は、[サイト] ドロップダウン メニューから、この NSX-T Manager インスタンスを追加するサイトを選択し、[次へ] をクリックします。
- 4 VMware Cloud Director の NSX-T Manager インスタンスの名前と、オプションで説明を入力します。

5 NSX-T Manager インスタンスの URL を入力します。

たとえば、**`https://FQDN_or_IP_address`** のようになります。

6 NSX-T Manager 管理者アカウントのユーザー名とパスワードを入力します。

7 [保存] をクリックします。

次のステップ

NSX-T Data Center によってバックアップされるプロバイダ仮想データセンターの作成に関する詳細については、<https://code.vmware.com> の『VMware Cloud Director API プログラミング ガイド』を参照してください。

NSX Advanced ロード バランシングの管理

バージョン 10.2 以降の VMware Cloud Director は、VMware NSX Advanced Load Balancer の機能を利用してロード バランシング サービスを提供します。

システム管理者は、NSX-T Data Center によってバックアップされている仮想データセンターのロード バランシング サービスへのアクセスを有効にし、構成することができます。

ロード バランシング サービスは NSX-T Data Center Edge Gateway に関連付けられ、この Edge Gateway の範囲は、NSX-T Data Center によってバックアップされている組織 VDC、または NSX-T Data Center ネットワーク プロバイダ タイプのデータセンター グループのいずれかに設定できます。

NSX Advanced Load Balancer をデプロイし、NSX-T Data Center 環境で使用するよう構成した後、コントローラを VMware Cloud Director に登録します。

NSX-T を使用して NSX Advanced Load Balancer を構成する方法については、[Avi と NSX-T の統合](#)を参照してください。

VMware Cloud Director を使用して NSX Advanced Load Balancer をデプロイする方法については、[VMware Cloud Director を使用する NSX Advanced Load Balancer のデプロイ](#)を参照してください。

NSX Advanced Load Balancer によって提供される仮想インフラストラクチャを使用するには、NSX-T Cloud インスタンスを VMware Cloud Director に登録します。コントローラはロード バランシング サービスの統合制御プレーンとして機能します。コントローラを登録した後、それらを VMware Cloud Director から直接管理できます。

NSX Advanced Load Balancer によって提供されるロード バランシング コンピューティング インフラストラクチャは、サービス エンジン グループに含まれています。VMware Cloud Director で NSX-T Data Center Edge Gateway に複数のサービス エンジン グループを割り当てることができます。単一の Edge Gateway に割り当てられているすべてのサービス エンジン グループは、同じネットワークを使用します。

サービス エンジン グループには、作成時に定義する独自のコンピューティング特性のセットがあります。

システム管理者がサービス エンジン グループを Edge Gateway に割り当てると、組織管理者は、特定のサービス エンジン グループで実行される仮想サービスを作成して構成できます。

コントローラ インスタンスの登録

VMware Cloud Director を NSX Advanced Load Balancer 環境と統合するには、コントローラ インスタンスを VMware Cloud Director インスタンスに登録します。

コントローラ インスタンスは、NSX Advanced Load Balancer によって提供されるロード バランシング サービスの統合制御プレーンとして機能します。

前提条件

NSX Advanced Load Balancer をインストールし、NSX-T Data Center インスタンスを使用して構成します。

NSX-T を使用して NSX Advanced Load Balancer を構成する方法については、[Avi と NSX-T の統合](#)を参照してください。

注： NSX-T Manager の NSX Advanced Load Balancer への登録に使用する FQDN または IP アドレスは、NSX-T Data Center の VMware Cloud Director への登録に使用した NSX-T Manager インスタンスの FQDN または IP アドレスと一致する必要があります。

手順

- 1 上部ナビゲーション バーの [リソース] で [インフラストラクチャ リソース] をクリックします。
- 2 [NSX-ALB] をクリックしてから、[コントローラ] をクリックします。
- 3 コントローラを追加するには、[追加] をクリックします。
- 4 マルチサイト環境を使用している場合は、ドロップダウン メニューから、コントローラを登録するサイトを選択します。
- 5 コントローラ インスタンスを登録します。
 - a コントローラ インスタンスのわかりやすい名前と、必要に応じて説明を入力します。
 - b コントローラの URL を入力します。
例: `https://FQDN-or-IP-address`
 - c コントローラのユーザー名とパスワードを入力します。
 - d [保存] をクリックします。

結果

コントローラ インスタンスがリストに有効と表示されます。

次のステップ

[NSX-T Cloud の登録](#)します。

NSX-T Cloud の登録

NSX Advanced Load Balancer によって提供される仮想インフラストラクチャを使用するには、NSX-T Cloud インスタンスを VMware Cloud Director に登録します。

NSX-T Cloud は、NSX-T Manager と NSX-T Data Center トランスポート ゾーンで構成されるサービス プロバイダ レベルの構成です。

NSX-T Manager は、システム ビューを提供する NSX-T Data Center の管理コンポーネントです。NSX-T Data Center トランスポート ゾーンは、特定のネットワークの使用に参加できるホストと仮想マシンを決定します。

同じ NSX-T Manager によって管理されている複数のトランスポートゾーンがある場合は、個別の NSX-T Cloud によって NSX-T Manager および NSX-T Data Center トランスポート ゾーンインスタンスの各ペアがカプセル化されます。

NSX-T Cloud は、NSX-T Data Center トランスポート ゾーンによってバックアップされているネットワーク プールと 1 対 1 の関係があります。

前提条件

[コントローラ インスタンスの登録](#)します。

手順

- 1 上部ナビゲーション バーの [リソース] で [インフラストラクチャ リソース] をクリックします。
- 2 [NSX-ALB] をクリックしてから、[NSX-T Cloud] をクリックします。
- 3 NSX-T Cloud を追加するには、[追加] をクリックします。
- 4 ドロップダウン メニューから、NSX-T Cloud を作成するコントローラ インスタンスを選択します。
- 5 NSX-T Cloud の名前と、必要に応じて説明を入力します。
- 6 リストから使用できるクラウドを選択します。
- 7 クラウドをインポートするには、[追加] をクリックします。

結果

インポートしたクラウドが、使用可能な NSX-T Cloud のリストに表示されます。

次のステップ

[サービス エンジン グループのインポート](#)します。

サービス エンジン グループのインポート

テナントに仮想サービス管理機能を提供するには、サービス エンジン グループを VMware Cloud Director 環境にインポートします。

サービス エンジン グループは、サイズ、ネットワーク アクセス、フェイルオーバーなどの共有サービス エンジンのプロパティも定義する隔離ドメインです。

サービス エンジン グループ内のリソースは、テナントのニーズに応じて、さまざまな仮想サービスに使用できます。これらのリソースを複数のサービス エンジン グループ間で共有することはできません。

サービス エンジン グループを管理および更新するには、NSX Advanced Load Balancer を使用します。NSX Advanced Load Balancer でサービス エンジン グループを更新したら、VMware Cloud Director ユーザー インターフェイスでサービス エンジン グループを同期し、設定を更新する必要があります。

Edge Gateway には、インポートされたサービス エンジン グループのみを割り当てることができます。

サービス エンジン グループをインポートするには、VMware Cloud Director インスタンスにすでに登録されている NSX-T Cloud に関連付けます。

前提条件

- [コントローラ インスタンス](#)の登録します。
- [NSX-T Cloud](#) の登録します。

手順

- 1 上部ナビゲーション バーの [リソース] で [インフラストラクチャ リソース] をクリックします。
- 2 [NSX-ALB] をクリックし、[サービス エンジン グループ] をクリックします。
- 3 サービス エンジン グループをインポートするには、[追加] をクリックします。
- 4 ドロップダウン メニューから NSX-T Cloud を選択します。
- 5 予約モデルを選択します。
 - サービス エンジン グループを単一の Edge Gateway に割り当てるには、[専用] を選択します。
 - 複数の Edge Gateway 間でサービス エンジン グループを共有するには、[共有] を選択します。
- 6 サービス エンジン グループの名前と、オプションで説明を入力します。
- 7 サービス エンジン グループのインスタンスを選択します。
- 8 [追加] をクリックします。

次のステップ

Edge Gateway でロード バランシングを有効にして、サービス エンジン グループを Edge Gateway に割り当てます。『[NSX-T Data Center Edge Gateway での NSX Advanced ロード バランシングの管理](#)』を参照してください。

サービス エンジン グループの同期

インポートされたサービス エンジン グループの設定を更新するには、NSX Advanced Load Balancer と同期する必要があります。

サービス エンジン グループを管理および更新するには、NSX Advanced Load Balancer を使用します。NSX Advanced Load Balancer でサービス エンジン グループを更新したら、VMware Cloud Director ユーザー インターフェイスでサービス エンジン グループを同期し、設定を更新する必要があります。

サービス エンジン グループを同期すると、グループの高可用性モードのローカル レコードと、サービス エンジン グループによってサポートされる仮想サービスの最大数が更新されます。

重要: サービス エンジン グループを同期した後に、サポートされている仮想サービスの新しい最大数の方が予約されている仮想サービスの数よりも少ない場合、サービス エンジン グループは割り当て超過としてマークされます。

サービス エンジン グループが過剰に割り当てられている場合は、仮想サービスを作成する Edge Gateway で十分に容量が予約されている場合でも、新しい仮想サービスの作成は失敗することがあります。

仮想サービスの作成の失敗を回避するには、サービス エンジン グループの設定を編集するときに、サポートされる仮想サービスの最大数が最初に予約された仮想サービスの数を下回らないようにします。

前提条件

サービス エンジン グループのインポート.

手順

- 1 上部ナビゲーション バーの [リソース] で [インフラストラクチャ リソース] をクリックします。
- 2 [NSX-ALB] を選択し、[サービス エンジン グループ] をクリックします。
- 3 サービス エンジン グループを選択し、[同期] をクリックします。

結果

サービス エンジン グループの設定が更新されます。

VMware Cloud Director エンドポイントとプロキシを使用した vSphere コンポーネントへのアクセス

VMware Cloud Director エンドポイントを使用して、基盤となる vSphere 環境にアクセスできます。エンドポイントがプロキシに接続されている場合、VMware Cloud Director は HTTP プロキシ サーバとして機能します。

エンドポイント

VMware Cloud Director エンドポイントは、データセンター コンポーネント（vCenter Server インスタンス、ESXi ホスト、または NSX Manager インスタンスなど）へのアクセス ポイントです。ユーザーは、VMware Cloud Director アカウントを使用して、プロキシ コンポーネントまたは非プロキシ コンポーネントのユーザー インターフェイスまたは API にログインできます。

専用の vCenter Server インスタンスを作成すると、そのインスタンスのデフォルト エンドポイントも作成されます。vCenter Server インスタンスの接続中に、プロキシを作成することもできます。ただし、デフォルトでは、デフォルト エンドポイントはどのプロキシにも接続されていません。プロキシに接続するには、デフォルトのエンドポイントを編集するか、新しいエンドポイントを作成する必要があります。

エンドポイントの作成、編集、および削除を行うには、専用 vCenter Server インスタンスの [エンドポイント] タブを使用します。『[エンドポイントの作成](#)』を参照してください。

プロキシ

VMware Cloud Director 提供のプロキシは VMware Cloud Director 内のプロキシ設定とは異なります。テナントを指定する VMware Cloud Director 提供のプロキシとは異なり、VMware Cloud Director 内のプロキシ設定はプロバイダ レベルで設定され、テナントは配置されません。

VMware Cloud Director によって提供されたプロキシを有効または無効にすると、そのプロキシを介したテナント アクセスを許可または停止できます。

プロキシは vCenter Server インスタンスを VMware Cloud Director に接続するときに作成するか、後で作成することができます。vCenter Server の接続中にプロキシを作成し、テナントがアクセスできるようにする場合は、プロキシをデフォルトのエンドポイントに手動で接続する必要があります。

vCenter Server インスタンスが外部 Platform Services Controller を使用している場合、VMware Cloud Director は Platform Services Controller のプロキシも作成します。親と子プロキシを使用すると、テナントから特定のプロキシを非表示にしたり、親プロキシを使用して子プロキシのグループを有効または無効にしたりできます。vCenter Server インスタンスを VMware Cloud Director に追加した後にプロキシを作成する方法については、[基盤となる vCenter Server リソースにアクセスするためのプロキシの追加](#)を参照してください。

[インフラストラクチャ リソース] の [プロキシ] タブでプロキシの編集、有効化、無効化、および削除ができます。

注： vCenter Server インスタンスにプロキシを追加するときは、証明書とサムプリントをアップロードする必要があります。これにより、プロキシ コンポーネントが自己署名証明書を使用する場合に、テナントが証明書とサムプリントを取得できるようになります。

証明書および証明書失効リスト (CRL) を表示および管理するには、[プロキシ証明書および CRL の管理](#)を参照してください。

エンドポイントの作成

管理者およびテナントが基盤となる vSphere 環境にアクセスする際に使用できるエンドポイントを作成できます。

エンドポイントは専用の vCenter Server インスタンスに接続する必要があります。また、エンドポイントは、テナントでは専用の vCenter Server インスタンスの [アクション] メニューを使用して表示できます。vCenter Server インスタンスを VMware Cloud Director に追加するときにテナントからのアクセスを有効にすると、VMware Cloud Director は、ターゲット URL として vCenter Server インスタンスの URL を持つデフォルトのエンドポイントを作成します。追加のエンドポイントを作成した場合は、デフォルトのエンドポイントを変更できます。

エンドポイントは、専用の vCenter Server インスタンスとプロキシ間のリンクとして機能することができます。エンドポイントは、1つのプロキシに接続できます。プロキシに接続されていない場合もあります。エンドポイントがプロキシに接続されている場合、エンドポイントのターゲットになるのは、接続されたプロキシのユーザー インターフェイスの URL ではなく、ターゲット URL です。

前提条件

エンドポイントを作成する vCenter Server インスタンスでテナントからのアクセスが有効になっていることを確認します。[接続された vCenter Server のテナント アクセスの有効化](#)を参照してください。

手順

- 1 上部ナビゲーション バーの [リソース] で [インフラストラクチャ リソース] をクリックします。
- 2 左側のパネルで [vCenter Server インスタンス] を選択します。
- 3 vCenter Server インスタンスを選択します。
- 4 vCenter Server の詳細情報が表示されている画面で、[エンドポイント] タブをクリックし、[新規] をクリックします。
- 5 エンドポイントの名前とターゲット URL を入力します。
- 6 (オプション) このエンドポイントを、この vCenter Server インスタンスのデフォルトのエンドポイントに設定します。

7 (オプション) プロキシとの接続を確立します。

8 [保存] をクリックします。

次のステップ

- エンドポイントの設定を編集します。
- エンドポイントを削除します。デフォルトのエンドポイントを削除する場合は、デフォルトとして別のエンドポイントを選択する必要があります。

基盤となる vCenter Server リソースにアクセスするためのプロキシの追加

VMware Cloud Director を vCenter Server インスタンスとそのコンポーネント用の HTTP プロキシ サーバとして機能させる場合は、プロキシを作成します。専用の vCenter Server インスタンスおよび目的が設定されていない vCenter Server インスタンスのプロキシを作成できます。

取得された証明書とサムプリントを使用して vCenter Server プロキシを自動的に生成する場合は、[vCenter Server インスタンス] グリッドまたは vCenter Server 詳細ビューから実行できます。vCenter Server に外部 Platform Services Controller がある場合、このオプションは SSO エンドポイントのプロキシも作成します。

この手順では、vCenter Server インスタンスのプロキシを手動で作成する方法、または ESXi ホスト、外部 Platform Services Controller インスタンス、または NSX Manager インスタンスのプロキシを作成する方法について説明します。

手順

- 1 上部ナビゲーション バーの [リソース] で [インフラストラクチャ リソース] をクリックします。
- 2 左側のパネルで [vCenter Server インスタンス] を選択します。
- 3 vCenter Server インスタンスを選択します。
- 4 vCenter Server の詳細情報が表示されている画面で、[プロキシ] タブをクリックし、[新規] をクリックします。
- 5 プロキシの名前を入力します。
- 6 VMware Cloud Director をプロキシにするコンポーネントに応じて、プロキシのタイプを選択します。

プロキシの作成後にこの設定を編集することはできません。

作成できる vCenter Server プロキシは 1 つのみです。既存の vCenter Server プロキシがあり、新規プロキシを作成する場合、[タイプ] ドロップダウン メニューに vCenter Server オプションは含まれていません。

- vCenter Server プロキシを作成する場合、[vCenter Server] を [タイプ] ドロップダウン メニューから選択し、[手順 10](#) に進みます。
 - プロキシを ESXi ホスト、NSX Manager、または SSO に対して作成する場合、ドロップダウン メニューから選択を行い、[手順 7](#) に進みます。
- 7 新しいプロキシの名前、ターゲット ホスト、およびユーザー インターフェイスの URL を入力します。

ターゲット ホストは、VMware Cloud Director をプロキシにするコンポーネントのホスト名または IP アドレスです。新しいプロキシのユーザー インターフェイス URL は、テナントがプロキシを開くときに、VMware Cloud Director ユーザー インターフェイスが転送される URL です。

- 8 テナントにプロキシが表示されるようにするには、[テナントの表示] オプションをオンにします。
- 9 (オプション) [親プロキシの選択] をクリックし、リストからプロキシを選択します。
- 10 [保存] をクリックします。

次のステップ

[プロキシ証明書および CRL の管理](#)。

プロキシ証明書および CRL の管理

プロキシ証明書および証明書失効リスト (CRL) を表示、ダウンロード、およびアップロードできます。

前提条件

1 つ以上の vCenter Server インスタンスに VMware Cloud Director 提供のプロキシがあることを確認します。[VMware Cloud Director エンドポイントとプロキシを使用した vSphere コンポーネントへのアクセス](#)を参照してください。

手順

- 1 上部ナビゲーション バーの [リソース] で [インフラストラクチャ リソース] をクリックします。
- 2 左側のパネルで、[プロキシ] をクリックし、プロキシを選択します。
- 3 [証明書の管理] をクリックします。
- 4 証明書および CRL をアップロードまたはダウンロードします。
- 5 [保存] をクリックします。

クラウド リソースの追加

クラウド リソースとは、基盤となる vSphere リソースを抽象化したもので、VMware Cloud Director 仮想マシンおよび vApp にコンピューティング リソースおよびメモリのリソースを提供し、ストレージおよびネットワーク 接続へのアクセスを可能にします。

クラウド リソースにはプロバイダおよび組織の仮想データセンター、外部ネットワーク、組織仮想データセンター ネットワーク、ネットワーク プールがあります。クラウド リソースを VMware Cloud Director に追加するには、事前に vSphere リソースを追加する必要があります。

組織仮想データセンターの詳細については、[6 章 組織仮想データセンターの管理](#)を参照してください。

組織仮想データセンター ネットワークの詳細については、『VMware Cloud Director Tenant Portal Guide』の「組織仮想データセンター ネットワークの管理」の章を参照してください。

VMware Cloud Director 9.7 には、vCenter Server インストール全体をカプセル化するクラウド リソースとして SDDC または専用 vCenter Server インスタンスが導入されています。プロバイダは、専用 vCenter Server インスタンスの作成と有効化、テナントへの公開、および基盤となる vSphere 環境のさまざまなコンポーネントに対するプロキシの作成と有効化を行うことができます。専用 vCenter Server インスタンスおよびプロキシの作成、テナントへの公開、および管理を行うには、Service Provider Admin Portal または vCloud OpenAPI を使用します。9 章 専用 vCenter Server インスタンスの管理 または <https://code.vmware.com> にある VMware Cloud Director OpenAPI のスタート ガイドを参照してください。

プロバイダ仮想データセンター

プロバイダ仮想データセンター (VDC) は、vCenter Server リソース プールのコンピューティング リソースおよびメモリ リソースと、単一の vCenter Server インスタンスの 1 つ以上のストレージ ポリシーのストレージ リソースを組み合わせ使用します。プロバイダ VDC は、ネットワーク リソースに NSX Data Center for vSphere または NSX-T Data Center のいずれかを使用できます。

- 接続された vCenter Server インスタンスと関連する NSX Manager インスタンスによってバックアップされたプロバイダ VDC を作成して、管理するには、Service Provider Admin Portal または vCloud API を使用します。
- 接続された vCenter Server インスタンスと NSX-T Manager インスタンスによってバックアップされたプロバイダ VDC を作成して、管理するには、Service Provider Admin Portal または vCloud API を使用します。

標準的な VMware Cloud Director システムには、さまざまなサービス レベルの要件を満たすために構成された複数のプロバイダ VDC が含まれています。プロバイダ VDC ごとに、プライマリ リソース プールがあります。プライマリ以外のリソース プールを追加および削除する場合は、バックアップしている vCenter Server インスタンスから操作します。プライマリ リソース プールを削除することはできません。

プロバイダ仮想データセンターの作成

vSphere のコンピューティング リソース、メモリ リソース、およびストレージ リソースを VMware Cloud Director で使用できるようにするには、プロバイダ仮想データセンター (VDC) を作成します。

組織が仮想マシンのデプロイを開始するか、カタログの作成を開始する前に、システム管理者はプロバイダ仮想データセンターと、そのリソースを使用する組織仮想データセンターを作成する必要があります。プロバイダ仮想データセンターと、サポートされる組織仮想データセンターとの関係は、管理上の決定事項です。決定は、サービス提供の範囲、vSphere インフラストラクチャのキャパシティと地理的分布、および同様の考慮事項に基づいて行うことができます。プロバイダ仮想データセンターによって、テナントが使用できる vSphere の容量とサービスが制限されるため、システム管理者は一般的に、パフォーマンス、容量、機能に基づいて測定された異なるクラスのサービスを備えたプロバイダ仮想データセンターを作成します。その後、テナントには、バックアップ プロバイダ仮想データセンターの設定で定義された、特定のサービス クラスを提供する組織仮想データセンターをプロビジョニングできます。

プロバイダ仮想データセンターを作成する際は、テナントに提供する vSphere 機能セットについて考慮します。これらの機能の一部は、プロバイダ仮想データセンターのプライマリ リソース プールに実装できます。また、特別に構成された vSphere クラスタに基づいて追加のリソース プールを作成し、[プロバイダ仮想データセンターへのリソース プールの追加](#)で説明されているように仮想データセンターへの追加が必要となる場合もあります。

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組織仮想データセンターにデプロイされた仮想マシンでは、使用可能なゲスト OS と仮想ハードウェア バージョンの組み合わせは、リソース プールをバックアップしているクラスタ内のホストにインストールされた ESXi リリースの範囲に基づいて決まります。

前提条件

- Service Provider Admin Portal にシステム管理者としてログインします。
- 自動化された DRS を使用するように構成されたクラスタ内に、使用可能な容量のあるターゲット プライマリ リソース プールが作成していることを確認します。リソース プールは、1 つのプロバイダ仮想データセンターに対してのみ使用できます。リソース プールを作成するには、vSphere Client を使用します。

vSphere High Availability (HA) を使用するクラスタの一部になっているリソース プールを使用する場合は、vSphere HA でのスロット サイズの計算方法をよく理解していることを確認します。スロット サイズおよび vSphere HA の動作のカスタマイズの詳細については、『vSphere 可用性』ドキュメントを参照してください。

- VMware Cloud Director で vSphere with VMware Tanzu を使用する場合は、スーパーバイザー クラスタが構成された vCenter Server 7.0 以降のインスタンスが使用可能であることを確認します。vSphere ドキュメントの『vSphere with Kubernetes の構成および管理』ガイドを参照してください。

- プロバイダ仮想データセンターのネットワーク リソースに NSX Data Center for vSphere を使用する場合：

- ターゲット プライマリ リソース プールを含む vCenter Server インスタンスが接続されていて、NSX Data Center for vSphere ライセンス キーを持っていることを確認します。
- NSX Manager で VXLAN インフラストラクチャを設定します。関連する『NSX 管理ガイド』を参照してください。

このプロバイダ仮想データセンターで、デフォルトの VXLAN ネットワーク プールの代わりに、カスタム VXLAN ネットワーク プールを使用する場合は、この段階でネットワーク プールを作成します。[NSX Data Center for vSphere トランスポート ゾーンによってバックアップされるネットワーク プールの作成](#)を参照してください。

- プロバイダ仮想データセンターのネットワーク リソースに NSX-T Data Center を使用する場合：

- [NSX-T Data Center Tier-0 ゲートウェイによってバックアップされる外部ネットワークの追加](#)
- [NSX-T Data Center トランスポート ゾーンによってバックアップされるネットワーク プールの作成](#)

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [プロバイダ VDC] を選択します。
- 3 [新規] をクリックします。
- 4 マルチサイト VMware Cloud Director デプロイを使用している場合は、[サイト] ドロップダウン メニューから、このプロバイダ仮想データセンター インスタンスを追加するサイトを選択し、[次へ] をクリックします。

- 5 プロバイダ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。

これらのテキスト ボックスを使用して、このプロバイダ仮想データセンターでバックアップされている組織仮想データセンターで利用可能な vSphere 機能を説明できます。たとえば、「**vSphere HA**」や「**IOPS サポートのあるストレージ ポリシー**」と入力します。

- 6 (オプション) 作成時にプロバイダ VDC を無効にするには、[状態] トグルをオフにします。

組織 VDC の作成に、無効な VDC のコンピューティング リソースとストレージ リソースを使用することはできません。

- 7 [次へ] をクリックします。

- 8 プロバイダ仮想データセンターのリソース プールを提供するには、vCenter Server インスタンスを選択して、[次へ] をクリックします。

このページには、VMware Cloud Director に登録されている vCenter Server インスタンスが一覧表示されます。vCenter Server インスタンスをクリックすると、使用可能なリソース プールが表示されます。

VMware Cloud Director で vSphere with VMware Tanzu を使用する場合は、スーパーバイザー クラスタが構成された vCenter Server 7.0 以降のインスタンスを選択する必要があります。

- 9 このプロバイダ仮想データセンターのプライマリ リソース プールとして機能するリソース プールを選択します。

1 つのプロバイダ仮想データセンターに対して 1 つのリソース プールを使用できます。リソース プールをプロバイダ仮想データセンターに追加すると、このリソース プールとその親チェーンは、その他のプロバイダ仮想データセンターでは選択できなくなります。

vSphere with VMware Tanzu を使用する場合は、スーパーバイザー クラスタを選択します。VMware Cloud Director では、スーパーバイザー クラスタによってバックアップされているリソース プールの横に、Kubernetes アイコンが表示されます。

- 10 スーパーバイザー クラスタによってバックアップされているリソース プールまたはクラスタを選択する場合に、Kubernetes 制御プレーンとの信頼関係を確立するには、Kubernetes 制御プレーン証明書を信頼する必要があります。

- 11 プロバイダ仮想データセンターでサポートする最新の仮想ハードウェア バージョンを選択して、[次へ] をクリックします。

システムは、リソース プールをバックアップするクラスタに含まれる、すべてのホストでサポートされている仮想ハードウェアの最も高いバージョンを判断し、これを [サポートされるハードウェアの最も高いバージョン] ドロップダウン メニューにデフォルトとして表示します。このデフォルトを使用することも、これより低いハードウェア バージョンをメニューから選択することもできます。指定したバージョンが、このプロバイダ仮想データセンターでバックアップされる組織仮想データセンターにおいて、デプロイされている仮想マシンで利用できる最新

の仮想ハードウェア バージョンになります。低い仮想ハードウェア バージョンを選択すると、これらの仮想マシンで一部のゲスト OS を使用できなくなる場合があります。選択したハードウェア バージョンでプロバイダ仮想データセンターを作成すると、そのバージョンはアップグレードのみ可能で、ダウングレードすることはできません。

注： プロバイダ仮想データセンターで使用可能なハードウェア バージョンは、ターゲット クラスタ内の ESXi ホストで使用可能な最新バージョンによって異なります。ESXi ホストでサポートされている最新のハードウェア バージョンを選択できない場合は、vSphere Client で、データセンターに仮想マシンを作成する場合のデフォルトの互換性が **[データセンター設定およびホスト バージョンを使用する]** に設定されていることを確認します。また、デフォルトの互換性設定を、クラスタに使用する最新のハードウェア バージョンに設定することもできます。

VMware Cloud Director 9.7 以降では、バックアップする vSphere インフラストラクチャがサポートする最新のハードウェア バージョンがサポートされます。VMware Cloud Director 10.2.2 以降では、vCenter Server インスタンスでデフォルトのハードウェア バージョンを手動で構成せずにハードウェア バージョンを設定することができます。

- 12 プロバイダ仮想データセンターのストレージ プロファイルを 1 つ以上選択し、[次へ] をクリックします。

選択したリソース プールでサポートされている、すべての vSphere ストレージ ポリシーが一覧表示されます。

- 13 このプロバイダ仮想データセンターのネットワーク プールを構成します。

すべてのプロバイダ仮想データセンターにはネットワーク プールが設定されている必要があります。デフォルトの範囲を使用して自動的に作成することも、特定の NSX Data Center for vSphere に基づいたカスタム VXLAN プールまたは NSX-T Data Center トランスポート ゾーンに基づいた Geneve プールを使用することもできます。

注： VMware Cloud Director で vSphere with VMware Tanzu を使用する場合は、[NSX-T Manager および Geneve ネットワーク プール] オプションを選択する必要があります。

オプション	説明
デフォルトの VXLAN ネットワーク プールを作成します	このプロバイダ仮想データセンターの VXLAN プールが作成されます。
リストから VXLAN ネットワーク プールを選択します	特定の NSX トランスポート ゾーンに基づいてカスタム VXLAN プールを使用できるように、リストからネットワーク プールを選択します。
NSX-T Manager および Geneve ネットワーク プールを選択します	NSX-T Data Center トランスポート ゾーンによってバックアップされたカスタム VXLAN プールを使用できるように、リストからネットワーク プールを選択します。

- 14 選択内容を確認し、[完了] をクリックすると、プロバイダ仮想データセンターが作成されます。

次のステップ

セカンダリ リソース プールを追加することで、Edge クラスタ、アフィニティ グループ、特別な設定のホストなど、一部の組織で必要となる特別な機能をプロバイダ仮想データセンターが提供するようにできます。[プロバイダ仮想データセンターへのリソース プールの追加](#)を参照してください。

外部ネットワーク

VMware Cloud Director 外部ネットワークは、システム内部のネットワークと仮想マシンをシステム外部のネットワーク、たとえば VPN、企業イントラネット、公開インターネットに接続するアップリンク インターフェイスです。外部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。

システムに登録されている vCenter Server インスタンスが複数ある場合は、複数の外部ネットワークを作成し、それぞれのネットワークを vSphere ネットワークまたは Tier-0 論理ルーターでバックアップできます。

VMware Cloud Director は、IPv4 および IPv6 の外部ネットワークをサポートします。

注： 外部ネットワークの作成時に定義した IP アドレスの範囲は、Edge Gateway、またはこのネットワークに直接接続されている仮想マシンのいずれかに割り当てられます。このため、IP アドレスを VMware Cloud Director の外部で使わないでください。

vSphere ネットワークでバックアップされる外部ネットワーク

外部ネットワークは、単一の vSphere ネットワークまたは複数の vSphere ネットワークによってバックアップできます。

- 単一の vSphere インスタンスでバックアップされる外部ネットワーク。

外部ネットワークの各ユーザーに、vSphere ネットワーク上の重複しない IP アドレス セットを提供するには、システム管理者が、基盤となる VLAN の IP アドレス範囲を手動で設定する必要があります。

- 複数の vSphere ネットワークでバックアップされる外部ネットワーク。

外部ネットワークは、複数の vSphere ネットワークでバックアップできます。この方法を使用すると、VMware Cloud Director で IP アドレスを簡単に管理できます。外部ネットワークのプロパティを変更して、そのネットワーク バックアップを変更することが可能です。

複数の vSphere ネットワークによってバックアップされている外部ネットワークには、いくつかの制約があります。

- ネットワークは、システムに登録された各 VMware Cloud Director インスタンス上で最大 1 つのバックアップ vSphere ネットワークを所有できます。
- バックアップ ネットワークのスイッチは、すべて同じタイプにする必要があります (vSphere Distributed Switch または標準スイッチのいずれかを使用します)。

Tier-0 論理ルーターによってバックアップされる外部ネットワーク

外部ネットワークは、NSX-T Data Center Tier-0 論理ルーターによってバックアップできます。

NSX-T Data Center の VRF-Lite Tier-0 ゲートウェイによってバックアップされている外部ネットワークを作成することもできます。

仮想ルーティング/転送 (VRF) ゲートウェイは、親 Tier-0 ゲートウェイから作成されます。このゲートウェイには独自のルーティング テーブルがあります。

同じ Tier-0 ゲートウェイ内に複数の VRF ゲートウェイが同時に存在することができます。そのため、VRF によってバックアップされた外部ネットワークを作成すると、NSX-T Data Center の Tier-0 ゲートウェイをスケールアウトすることによって、VDC 内に完全に経路指定されたネットワーク トポロジを作成できるようになります。

VRF ゲートウェイの詳細については、NSX-T Data Center 管理ガイドを参照してください。

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追加

外部ネットワークを追加すると、VMware Cloud Director で使用する vSphere ネットワーク リソースを登録できます。外部ネットワークに接続する組織 VDC ネットワークを作成できます。

IPv4 または IPv6 外部ネットワークを追加できます。IPv6 外部ネットワークは IPv4 サブネットと IPv6 サブネットの両方をサポートし、IPv4 外部ネットワークは IPv4 サブネットと IPv6 サブネットの両方をサポートします。

前提条件

VLAN トランクの有無にかかわらず、vSphere ポート グループが使用可能であることを確認します。固定ポートのバインドを備えた、柔軟性に優れたポート グループによって、最適なパフォーマンスが確保されます。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のペインで、[外部ネットワーク] をクリックし、[新規] をクリックします。
- 3 [vSphere リソース] を選択してから、ネットワークをバックアップするポート グループのタイプを選択して、[次へ] をクリックします。
- 4 新しい外部ネットワークの名前と、オプションで説明を入力します。
- 5 外部ネットワークをバックアップするポート グループを選択し、[次へ] をクリックします。
- 6 1 つ以上のサブネットを設定し、[次へ] をクリックします。
 - a サブネットを追加するには、[追加] をクリックします。
 - b 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。
 - c (オプション) DNS 設定を入力します。
 - d 1 つ以上の IP アドレス範囲または IP アドレスを追加することによって、固定 IP アドレス プールを設定します。
 - e [OK] をクリックします。
 - f (オプション) 別のサブネットを追加するには、この手順を繰り返します。
- 7 ネットワーク設定を確認し、[完了] をクリックします。

次のステップ

これで、外部ネットワークに接続する組織 VDC ネットワークを作成できます。

NSX-T Data Center Tier-0 ゲートウェイによってバックアップされる外部ネットワークの追加

VMware Cloud Director が使用する NSX-T Data Center ネットワーク リソースを登録するには、Tier-0 ゲートウェイによってバックアップされる外部ネットワークを追加します。

前提条件

NSX-T Data Center Tier-0 ゲートウェイによってバックアップされる外部ネットワークを作成するには、まず Tier-0 ゲートウェイを作成する必要があります。Tier-0 ゲートウェイは、NSX-T Manager ユーザー インターフェイスまたは NSX ポリシー API を使用して作成できます。

NSX-T Data Center 内の VRF ゲートウェイによってバックアップされる外部ネットワークを作成する場合は、Tier-0 ゲートウェイにリンクされた VRF ゲートウェイも作成する必要があります。

- NSX-T Manager ユーザー インターフェイスで、Tier-0 ゲートウェイを作成します。
 - a 管理者権限を使用して、NSX-T Manager インスタンスにログインします。
 - b [ネットワーク] をクリックし、[Tier-0 ゲートウェイ] をクリックして、[ゲートウェイの追加] - [Tier-0] の順にクリックします。
 - c Tier-0 ルーターの名前を入力します。
 - d 高可用性モードを選択します。

注： デフォルトでは、アクティブ/アクティブ モードが使用されます。アクティブ/アクティブ モードでは、トラフィックはすべてのメンバー間で負荷分散されます。アクティブ/スタンバイ モードでは、選択されたアクティブなメンバーがすべてのトラフィックを処理します。アクティブなメンバーに障害が発生した場合は、新しいメンバーがアクティブになります。

- e ドロップダウン メニューから既存の NSX-T Edge クラスターを選択してこの Tier-0 論理ルーターをバックアップし、[保存] をクリックします。
- NSX-T Data Center 内の VRF ゲートウェイによってバックアップされる外部ネットワークを作成する場合は、Tier-0 ゲートウェイにリンクされた VRF ゲートウェイを作成します。
 - a 管理者権限を使用して、NSX-T Manager インスタンスにログインします。
 - b [ネットワーク] をクリックしてから [Tier-0 ゲートウェイ] をクリックし、[ゲートウェイの追加] - [VRF] の順にクリックします。
 - c VRF ゲートウェイの名前を入力します。
 - d VRF ゲートウェイの接続先となる Tier-0 ゲートウェイを選択します。
 - e [保存] をクリックします。

手順

- 1 VMware Cloud Director Service Provider Admin Portal にログインします。
- 2 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 3 左側のペインで、[外部ネットワーク] をクリックし、[新規] をクリックします。
- 4 新しい外部ネットワークを登録するサイトを選択し、[次へ] をクリックします。
- 5 [バックアップ タイプ] ページで [NSX-T リソース (Tier-0 ルーター)] を選択し、ネットワークをバックアップする登録済みの NSX-T Manager を選択して、[次へ] をクリックします。
- 6 新しい外部ネットワークの名前と、オプションで説明を入力します。

- 7 外部ネットワークに接続する Tier-0 ゲートウェイまたは VRF ゲートウェイを選択し、[次へ] をクリックします。
- 8 1つ以上のサブネットを設定し、[次へ] をクリックします。
 - a サブネットを追加するには、[追加] をクリックします。
 - b ネットワークの Classless Inter-Domain Routing (CIDR) 設定を入力します。
 - c (オプション) DNS 設定を入力します。
 - d 1つ以上の IP アドレス範囲または IP アドレスを追加することによって、固定 IP アドレス プールを構成します。
 - e [OK] をクリックします。
 - f (オプション) 別のサブネットを追加するには、手順 8.a ~ 8.e を繰り返します。
- 9 ネットワーク設定を確認し、[完了] をクリックします。

次のステップ

Tier-0 ゲートウェイを使用して、外部ネットワークへのアップリンクを作成します。

ネットワーク プール

ネットワーク プールとは、組織 VDC 内で vApp ネットワークおよび特定のタイプの組織 VDC ネットワークを作成するために使用できる、区別されていないネットワークのグループです。

ネットワーク プールは、VLAN ID やポート グループのような vSphere ネットワーク リソース、NSX Data Center for vSphere リソース、または NSX-T Data Center リソースによってバックアップされます。

VMware Cloud Director はネットワーク プールを使用して、NAT を経由する内部組織 VDC ネットワークおよびすべての vApp ネットワークを作成します。プールの各ネットワークにおけるネットワーク トラフィックは、他のすべてのネットワークからレイヤ 2 で隔離されます。

VMware Cloud Director では各組織 VDC に 1 つのネットワーク プールを指定できます。複数の組織 VDC で 1 つのネットワーク プールを共有できます。組織 VDC のネットワーク プールは、組織 VDC のネットワーク割り当て容量を満たすために作成されるネットワークを提供します。

VXLAN ネットワーク プール

NSX Data Center for vSphere によってバックアップされているすべてのプロバイダ VDC には、VXLAN ネットワーク プールが含まれています。

NSX Data Center for vSphere によってバックアップされるプロバイダ VDC を作成する場合は、プロバイダ VDC を既存の VXLAN ネットワーク プールに関連付けるか、プロバイダ VDC 用の VXLAN ネットワーク プールを作成します。

新しく作成された VXLAN ネットワーク プールには、作成時に、含まれるプロバイダ VDC の名前から派生する名前が与えられ、その VDC に接続されます。このネットワーク プールの削除または編集を行うことはできません。プロバイダ VDC の名前を変更すると、VXLAN ネットワーク プールの名前も自動的に変更されます。

注： インフラストラクチャ全体でネットワーク パフォーマンスを最適化するには、1 つの VXLAN ネットワーク プールを作成し、作成時にすべてのプロバイダ VDC に関連付けます。

VMware Cloud Director VXLAN ネットワークは、IETF VXLAN 標準に基づいており、さまざまな利点があります。

- レイヤ 3 の境界をまたぐ論理ネットワーク
- 単一のレイヤ 2 上の複数のラックをまたぐ論理ネットワーク
- ブロードキャストの抑制
- 高パフォーマンス
- 規模の拡大 (最高で 1,600 万のネットワーク アドレス)

VMware Cloud Director 環境における VXLAN ネットワークの詳細については、『NSX 管理ガイド』を参照してください。

NSX Data Center for vSphere トランスポート ゾーンによってバックアップされるネットワーク プールの作成

VMware Cloud Director が使用する NSX Data Center for vSphere トランスポート ゾーンを登録するには、VXLAN でバックアップされるネットワーク プールを追加します。

前提条件

VMware Cloud Director に登録されている任意の vCenter Server で NSX Data Center for vSphere トランスポート ゾーンを作成します。『NSX 管理ガイド』を参照してください。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [ネットワーク プール] を選択し、[新規] をクリックします。
- 3 新しいネットワーク プールの名前と、必要に応じて説明を入力し、[次へ] をクリックします。
- 4 [VXLAN にバックアップされている] を選択し、[次へ] をクリックします。
- 5 このネットワーク プールで使用される VXLAN トランスポート ゾーンを指定する vCenter Server インスタンスを選択し、[次へ] をクリックします。
- 6 新しいネットワーク プールをバックアップする NSX Data Center for vSphere トランスポート ゾーンを選択し、[次へ] をクリックします。

注： クロス仮想データセンター ネットワーク用のユニバーサル ネットワーク プールを作成するには、UNIVERSAL_VXLAN タイプのトランスポート ゾーンを選択します。

- 7 ネットワーク プール設定を確認し、[完了] をクリックします。

次のステップ

ネットワーク プールによってバックアップされる組織 VDC ネットワークを作成するか、ネットワーク プールを組織 VDC に関連付けて vApp ネットワークを作成します。

Geneve ネットワーク プール

NSX-T Data Center によってバックアップされるすべてのプロバイダ VDC には、Geneve ネットワーク プールが含まれています。

Geneve は、NSX-T Data Center でオーバーレイ機能を提供するネットワーク仮想化の標準です。

NSX-T Data Center によってバックアップされるプロバイダ VDC を作成する場合は、プロバイダ VDC を既存の Geneve ネットワーク プールに関連付けるか、プロバイダ VDC 用の Geneve ネットワーク プールを作成します。

注： VMware Cloud Director は、VLAN トランスポート ゾーンによってバックアップされている NSX-T Data Center ネットワーク プールをサポートしていません。

VMware Cloud Director Geneve ネットワークには複数の利点があります。

- レイヤ 3 の境界をまたぐ論理ネットワーク
- 単一のレイヤ 2 上の複数のラックをまたぐ論理ネットワーク
- ブロードキャストの抑制
- 高パフォーマンス
- 規模の拡大 (最高で 1,600 万のネットワーク アドレス)

NSX-T Data Center トランスポート ゾーンによってバックアップされるネットワーク プールの作成

VMware Cloud Director が使用する NSX-T Data Center トランスポート ゾーンを登録するには、Geneve でバックアップされるネットワーク プールを作成します。

前提条件

オーバーレイにバックアップされている NSX-T Data Center トランスポート ゾーンを作成します。

注： VMware Cloud Director は、VLAN トランスポート ゾーンによってバックアップされている NSX-T Data Center ネットワーク プールをサポートしていません。

トランスポート ゾーンの作成および Geneve オーバーレイと呼ばれる汎用ネットワーク仮想化カプセル化の詳細については、『NSX-T Data Center 製品のドキュメント』を参照してください。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [ネットワーク プール] を選択し、[新規] をクリックします。
- 3 新しいネットワーク プールの名前と、必要に応じて説明を入力し、[次へ] をクリックします。
- 4 [Geneve にバックアップされている] を選択し、[次へ] をクリックします。

- 5 このネットワーク プールのトランスポート ゾーンを提供する NSX-T Manager インスタンスを選択し、[次へ] をクリックします。
- 6 NSX-T トランスポート ゾーンを選択し、[次へ] をクリックします。
- 7 ネットワーク プール設定を確認し、[完了] をクリックします。

次のステップ

ネットワーク プールによってバックアップされる組織 VDC ネットワークを作成するか、ネットワーク プールを組織 VDC に関連付けて vApp ネットワークを作成します。

VLAN ID によってバックアップされるネットワーク プールの作成

VMware Cloud Director が使用する vSphere VLAN ID を登録するには、VLAN でバックアップされるネットワーク プールを追加します。VLAN によってバックアップされるネットワーク プールは、組織 VDC ネットワークにセキュリティ、スケーラビリティ、パフォーマンスを提供します。

前提条件

一定範囲の VLAN ID と 1 つの vSphere Distributed Switch が vSphere で使用可能であることを確認します。VLAN ID は、ESXi サーバが接続される物理スイッチ内で構成される有効な ID である必要があります。

注意： VLAN はレイヤ 2 レベルで隔離される必要があります。VLAN を適切に隔離できないと、ネットワークが中断されることがあります。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [ネットワーク プール] を選択し、[新規] をクリックします。
- 3 新しいネットワーク プールの名前と、必要に応じて説明を入力し、[次へ] をクリックします。
- 4 [VLAN にバックアップされている] を選択し、[次へ] をクリックします。
- 5 このネットワーク プールで使用される分散仮想スイッチを指定する vCenter Server インスタンスを選択し、[次へ] をクリックします。
- 6 VLAN ID の範囲を入力し、[次へ] をクリックします。
- 7 ネットワーク プールの Distributed Switch を選択し、[次へ] をクリックします。
- 8 ネットワーク プール設定を確認し、[完了] をクリックします。

次のステップ

ネットワーク プールによってバックアップされる組織 VDC ネットワークを作成するか、ネットワーク プールを組織 VDC に関連付けて vApp ネットワークを作成します。

vSphere ポート グループによってバックアップされるネットワーク プールの作成

VMware Cloud Director が使用する vSphere ポート グループを登録するには、ポート グループによってバックアップされるネットワーク プールを追加します。他のタイプのネットワーク プールとは異なり、ポート グループによ

ってバックアップされたネットワーク プールでは vSphere Distributed Switch が不要であり、サードパーティの Distributed Switch に関連付けられたポート グループをサポートできます。

注意： ポート グループは、レイヤー 2 で他のすべてのポート グループから隔離される必要があります。ポート グループは、物理的に隔離されるか、VLAN タグを使用して隔離される必要があります。ポート グループを適切に隔離できない場合は、ネットワークが中断されることがあります。

前提条件

1 つ以上のポート グループが vSphere 環境で使用可能であることを確認します。ポート グループはクラスタ内の各 ESXi ホストで使用する必要があり、各ポート グループは単一の VLAN のみを使用する必要があります。ポート グループは、VLAN トランクを含むものと、含まないものがサポートされます。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [ネットワーク プール] を選択し、[新規] をクリックします。
- 3 新しいネットワーク プールの名前と、必要に応じて説明を入力し、[次へ] をクリックします。
- 4 [ポートグループにバックアップされている] を選択し、[次へ] をクリックします。
- 5 このネットワーク プールで使用されるポート グループを提供する vCenter Server インスタンスを選択し、[次へ] をクリックします。
- 6 ポート グループを 1 つ以上選択し、[次へ] をクリックします。
各ポート グループに 1 つのネットワークを作成できます。
- 7 ネットワーク プール設定を確認し、[完了] をクリックします。

次のステップ

ネットワーク プールによってバックアップされる組織 VDC ネットワークを作成するか、ネットワーク プールを組織 VDC に関連付けて vApp ネットワークを作成します。

vCenter Server インスタンスの表示

VMware Cloud Director インストール内のすべてのサイトの vCenter Server インスタンスのリストを表示できます。VMware Cloud Director での各 vCenter Server インスタンスの使用方法を確認できます。

手順

- 1 上部ナビゲーション バーの [リソース] で [インフラストラクチャ リソース] をクリックします。
- 2 左側のパネルで [vCenter Server インスタンス] を選択します。

結果

接続されているすべての vCenter Server インスタンスのリストが表示されます。リストには、各 vCenter Server インスタンスについて次の情報が含まれています。

	説明
[名前]	VMware Cloud Director 内の vCenter Server インスタンスの名前。
[ステータス]	vCenter Server ステータスは、正常、警告、および重大です。
[状態]	有効または無効。 vCenter Server インスタンスの有効化または無効化 を参照してください。
[接続]	VMware Cloud Director に接続されているかどうか。 vCenter Server インスタンスの再接続 を参照してください。
[VC ホスト]	vCenter Server インスタンスの FQDN。
[バージョン]	vCenter Server のバージョン。
[使用量]	専用の vCenter Server インスタンスによってテナント アクセスが有効になりました。プロバイダは、複数のプロバイダ VDC にまたがる共有 vCenter Server インスタンスのさまざまなリソース プールを使用し、それらのリソース プールを複数のテナントに割り当てることができます。『 9 章 専用 vCenter Server インスタンスの管理 』を参照してください。
[クラスタの健全性]	vCenter Server インスタンス内のすべてのクラスタの健全性の集計。クラスタの健全性を集計すると、健全性が最も低いクラスタの健全性が表示されます。
[クラスタ]	vCenter Server インスタンス内のクラスタの数。
[仮想マシン]	vCenter Server インスタンス内の仮想マシンの数。
[実行中の仮想マシン]	vCenter Server インスタンスで実行中の仮想マシンの数。
[CPU]	使用中の仮想 CPU 量を、利用可能な vCenter Server CPU 合計量のパーセンテージで表したもの。
[メモリ]	使用中の仮想メモリ量を、利用可能な vCenter Server メモリ合計量のパーセンテージで表したもの。
[ストレージ]	使用中の仮想ストレージ量を、利用可能な vCenter Server ストレージ合計量のパーセンテージで表したもの。

vCenter Server 設定の変更

接続済み vCenter Server インスタンスの接続情報が変更された場合や、VMware Cloud Director での名前と説明またはそのコンピューティング プロバイダ範囲を変更する場合は、その設定を変更できます。

vCenter Server インスタンスを追加したときの設定を変更できます。[vCenter Server インスタンスの追加](#)を参照してください。

手順

- 1 上部ナビゲーション バーの [リソース] で [インフラストラクチャ リソース] をクリックします。
- 2 左側のペインで [vCenter Server インスタンス] をクリックし、変更する vCenter Server インスタンスの名前をクリックします。

- 3 [vCenter Server 情報] セクションの右上隅にある [編集] をクリックします。
- 4 (オプション) インスタンスの名前と説明を編集します。
- 5 (オプション) vCenter Server のコンピューティング プロバイダ範囲を編集します。

コンピューティング プロバイダ範囲は、コンピューティング フォルト ドメインを表すか、テナントに表示される、ワークロードのあるアベイラビリティ ゾーンを表します。デフォルトでは、プロバイダ仮想データセンターのコンピューティング プロバイダ範囲は、バックアップ vCenter Server インスタンスから継承されます。単一の vCenter Server インスタンスによってバックアップされる複数のプロバイダ VDC のコンピューティング プロバイダ範囲を区別できます。たとえば、vCenter Server にコンピューティング プロバイダ範囲 **Germany** を設定し、プロバイダ VDC に範囲 **Munich** を設定することができます。

- 6 (オプション) vCenter Server インスタンスの URL を編集します。
- 7 (オプション) vCenter Server 管理者アカウントのユーザー名とパスワードを編集します。
- 8 (オプション) [有効] トグル ボタンをオン/オフにします。
- 9 (オプション) vCenter Server Web クライアントの URL を設定します。
- 10 [保存] をクリックします。

次のステップ

接続情報を変更した場合は、[vCenter Server インスタンスの再接続](#)を実行する必要があります。

vCenter Server インスタンスの有効化または無効化

メンテナンスを実行する前、または vCenter Server インスタンスの登録を解除する前に、ターゲット vCenter Server インスタンスを無効にする必要があります。VMware Cloud Director の仮想データセンターに、このリソースを提供するには、vCenter Server インスタンスを有効にする必要があります。

手順

- 1 上部ナビゲーション バーの [リソース] で [インフラストラクチャ リソース] をクリックします。
- 2 左側のパネルで [vCenter Server インスタンス] を選択します。
- 3 ターゲット vCenter Server インスタンスの名前の横にあるラジオ ボタンをクリックして、[有効化] または [無効化] をクリックします。
- 4 確認するには、[OK] をクリックします。

vCenter Server インスタンスの再接続

vCenter Server インスタンスが切断として表示される場合、または接続設定を変更した場合は、接続のリセットを試行することができます。

注： 新しい接続を確立する間は、vCenter Server インスタンスは操作できません。

手順

- 1 上部ナビゲーション バーの [リソース] で [インフラストラクチャ リソース] をクリックします。
- 2 左側のパネルで [vCenter Server インスタンス] を選択します。
- 3 ターゲット vCenter Server インスタンスの名前の横にあるラジオ ボタンをクリックして、[再接続] をクリックします。
- 4 確認するには、[OK] をクリックします。

vCenter Server インスタンスの更新

基盤となる vCenter Server リソースに関する VMware Cloud Director データベース内の情報を更新するには、vCenter Server インスタンスを更新する必要があります。

VMware Cloud Director 10.2.2 以降では、Kubernetes を使用している場合に vCenter Server インスタンスを更新すると、組織仮想データセンターの外部ネットワークから Tanzu Kubernetes クラスタへのアクセスをブロックするデフォルトのファイアウォール ポリシーと NAT ルールがリストアされます。

手順

- 1 上部ナビゲーション バーの [リソース] で [インフラストラクチャ リソース] をクリックします。
- 2 左側のパネルで [vCenter Server インスタンス] を選択します。
- 3 ターゲット vCenter Server インスタンスの名前の横にあるラジオ ボタンをクリックして、[更新] をクリックします。
- 4 確認するには、[OK] をクリックします。

vCenter Server インスタンスのストレージ ポリシーの更新

基盤となる vSphere 環境の仮想マシン ストレージ ポリシーに関する VMware Cloud Director データベース内の情報を更新するには、vCenter Server インスタンスのストレージ ポリシーを更新する必要があります。

手順

- 1 上部ナビゲーション バーの [リソース] で [インフラストラクチャ リソース] をクリックします。
- 2 左側のパネルで [vCenter Server インスタンス] を選択します。
- 3 ターゲット vCenter Server インスタンスの名前の横にあるラジオ ボタンをクリックして、[ポリシーの更新] をクリックします。
- 4 確認するには、[OK] をクリックします。

vCenter Server インスタンスの登録解除

vCenter Server インスタンスのリソースの使用を停止するには、VMware Cloud Director インストールからこの vCenter Server インスタンスを削除します。

前提条件

- vCenter Server インスタンスを無効にします。[vCenter Server インスタンスの有効化または無効化](#)を参照してください。
- この vCenter Server インスタンスのリソース プールを使用するすべてのプロバイダ仮想データセンターを削除します。[プロバイダ仮想データセンターの削除](#)を参照してください。

手順

- 1 上部ナビゲーション バーの [リソース] で [インフラストラクチャ リソース] をクリックします。
- 2 左側のパネルで [vCenter Server インスタンス] を選択します。
- 3 ターゲット vCenter Server インスタンスの名前の横にあるラジオ ボタンをクリックして、[登録解除] をクリックします。
- 4 確認するには、[OK] をクリックします。

NSX Manager 設定の変更

登録済み NSX Manager インスタンスの接続情報が変更された場合や、VMware Cloud Director での名前と説明を変更する場合は、この設定を変更できます。

NSX Manager インスタンスを追加したときの設定を変更できます。[\(オプション\)関連付けられた NSX Manager インスタンスの追加](#)を参照してください。

手順

- 1 上部ナビゲーション バーの [リソース] で [インフラストラクチャ リソース] をクリックします。
- 2 左側のペインで [vCenter] をクリックして、ターゲット NSX Manager インスタンスに関連付けられている vCenter Server インスタンスの名前をクリックします。
- 3 [NSX-V Manager 情報] セクションの右上隅にある [編集] をクリックします。
- 4 NSX Manager のホスト名と管理者の認証情報を変更し、[保存] をクリックします。
- 5 (オプション) この vCenter Server インスタンスによってバックアップされている仮想データセンターに対してクロス仮想データセンター ネットワークを有効にするには、トグルを有効にして、コントロール仮想マシンのプロパティとネットワーク プロバイダ範囲の名前を入力します。

コントロール仮想マシンのプロパティは、ユニバーサル ルーターなどのクロス仮想データセンター ネットワーク コンポーネントの NSX Manager インスタンスにアプライアンスを展開する際に使用されます。

パラメータ	説明
リソース プール バス	クラスタから始まる vCenter Server インスタンスの特定のリソース プールへの階層パス (<i>Cluster/Resource_Pool_Parent/Target_Resource</i>)。例： TestbedCluster1/mgmt-rp 。 または、リソース プールの管理対象オブジェクト リファレンス ID を入力することもできます。例： resgroup-1476 。
データストア名	アプライアンスのファイルをホストするデータストアの名前。例： shared-disk-1 。

パラメータ	説明
管理インターフェイス	HA 分散論理ルーター (DLR) 管理インターフェイスに使用されている vCenter Server またはポート グループ内のネットワーク名。例: TestbedPG1 。
ネットワーク プロバイダ範囲	データセンター グループのネットワーク トポロジ内のネットワーク フォルト ドメインに対応しています。例: boston-fault1 。 クロス仮想データセンター グループの管理については、『VMware Cloud Director Tenant Portal Guide』を参照してください。

NSX-T Manager 設定の変更

登録済み NSX-T Manager インスタンスの接続情報が変更された場合や、VMware Cloud Director での名前と説明を変更する場合は、この設定を変更できます。

vCenter Server インスタンスを追加したときの設定を変更できます。[NSX-T Manager インスタンスの登録](#)を参照してください。

手順

- 1 上部ナビゲーション バーの [リソース] で [インフラストラクチャ リソース] をクリックします。
- 2 左側のペインで [NSX-T Manager] をクリックし、変更する NSX-T Manager インスタンスの名前をクリックします。
- 3 [全般] タブの右上隅にある [編集] をクリックします。
- 4 NSX-T Manager 設定を編集して、[保存] をクリックします。

NSX-T Manager インスタンスの削除

NSX-T Manager インスタンスのリソースの使用を停止するには、VMware Cloud Director インストールからこの vCenter Server インスタンスを削除します。

前提条件

この NSX-T Manager インスタンスのリソースを使用するすべてのプロバイダ仮想データセンターを削除します。[プロバイダ仮想データセンターの削除](#)を参照してください。

手順

- 1 上部ナビゲーション バーの [リソース] で [インフラストラクチャ リソース] をクリックします。
- 2 左側のペインで、[NSX-T Manager] をクリックします。
- 3 削除する NSX-T Manager インスタンス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 確定するには、[削除] をクリックします。

マルチサイト展開の構成と管理

地理的に分散された複数の VMware Cloud Director インストール環境またはサーバ グループとその組織を単一のエンティティとして管理および監視するには、サービス プロバイダとテナントが VMware Cloud Director マルチサイト機能を使用します。

マルチサイトの効果的な実装

2 つの VMware Cloud Director サイトを関連付けると、これらのサイトを単一のエンティティとして管理できます。これらのサイトにある複数の組織を相互に関連付けることもできます。組織が関連付けのメンバーである場合、組織ユーザーは VMware Cloud Director Tenant Portal を使用して、任意のメンバーのサイトにある組織の資産にアクセスできます。ただし、各メンバー組織とその資産は使用するサイトにローカルに配置されます。

注： サイトを関連付けるには、VMware Cloud Director API を使用する必要があります。サイトの VMware Cloud Director API バージョンは同じであるか、メジャー バージョンの差が 1 である必要があります。たとえば、VMware Cloud Director 10.1 (API バージョン 34.0) のサイトを VMware Cloud Director サイト バージョン 10.0、10.1、10.2、または 10.2.2 (それぞれ API バージョンは 33.0、34.0、35.0、または 35.2) に関連付けることができます。

2 つのサイトを関連付けた後、VMware Cloud Director API または VMware Cloud Director Tenant Portal を使用して、それらのサイトを使用する組織を関連付けることができます。『VMware Cloud Director API プログラミング ガイド』または『VMware Cloud Director Tenant Portal Guide』の[マルチサイト展開の構成と管理](#) トピックを参照してください。

サイトまたは組織がピアと作成できる関連付けの数には上限がありませんが、各関連付けには必ず 2 つのメンバーを含めます。各サイトまたは組織には、独自のプライベート キーを設定する必要があります。関連付けの各メンバーはパブリック キーを交換して信頼関係を確立します。パブリック キーはメンバー間の署名要求を確認するために使用されます。

関連付けられた各サイトは、VMware Cloud Director サーバ グループ (VMware Cloud Director データベースを共有するサーバのグループ) の範囲によって定義されます。関連付けられた各組織は、1 つのサイトを使用します。組織管理者は、各メンバー サイトにある資産への組織ユーザーおよびグループによるアクセスを制御します。

サイトのオブジェクトとサイトの関連付け

インストールまたはアップグレード プロセスでは、ローカルの VMware Cloud Director サーバ グループを表す site オブジェクトが作成されます。複数の VMware Cloud Director サーバ グループで管理権限を持つシステム管理者は、VMware Cloud Director サイトの関連付けとして、これらのサーバ グループを構成できます。

組織の関連付け

サイトの関連付けが完了したら、メンバー サイトの組織管理者は組織の関連付けを開始できます。

注： テナントの組織に system 組織を関連付けることはできません。任意のサイトにある system 組織は、別のサイトにある system 組織にのみ関連付けることができます。

ユーザーおよびグループの ID

サイトおよび組織の関連付けでは、同じ ID プロバイダ (IDP) を使用することに同意する必要があります。関連付けられたすべての組織のユーザーおよびグループの ID は、この IDP が管理する必要があります。

システム組織では例外として VMware Cloud Director 統合 IDP を使用する必要がありますが、関連付けメンバーは各自に適した IDP を自由に選択できます。

組織のユーザーおよびグループのサイト アクセス コントロール

組織管理者は、各自の IDP を設定して、ユーザーまたはグループのアクセス トークンを生成できます。このアクセス トークンはすべてのメンバー サイトで有効にすることも、一部のメンバー サイトのみで有効にすることもできます。ユーザーおよびグループの ID は、すべてのメンバー組織で同じにする必要がありますが、ユーザーおよびグループの権限は、各メンバー組織内でユーザーおよびグループが割り当てられているロールによって制約されます。ユーザーまたはグループへのロールは、作成したカスタム ロールと同様に、メンバー組織にローカルで割り当てられます。

ロード バランサの要件

マルチサイト展開を効果的に実装するには、ロード バランサを設定して、組織のエンドポイント (`https://vcloud.example.com` など) に送信される要求を、サイト関連付けの各メンバーのエンドポイント (`https://us.vcloud.example.com` や `https://uk.vcloud.example.com` など) に分散する必要があります。サイトに複数のセルがある場合は、受信する要求をすべてのセルで分散するロード バランサも設定する必要があります。これにより、`https://us.vcloud.example.com` への要求を、`https://cell1.us.vcloud.example.com`、`https://cell2.us.vcloud.example.com` などで処理できます。

注： グローバル ロード バランサ (この場合は `https://vcloud.example.com`) は、ユーザー インターフェイスへのアクセス専用にする必要があります。REST API を使用する独自のスクリプトまたはプログラムを開発する場合、この呼び出しは特定のサイトをターゲットにする必要があります。

ネットワーク接続の要件

マルチサイト機能を使用する場合は、各サイトの各セルが、すべてのサイトの REST API エンドポイントに REST API 要求を実行できる必要があります。「ロード バランサの要件」セクションの例を使用する場合は、`cell1.us.vcloud.example.com` および `cell2.us.vcloud.example.com` から `uk.example.com` の REST API エンドポイントにアクセスする必要があります。その逆は、`uk.example.com` のすべてのセルで成立します。つまり、セルは自身の REST API エンドポイントに REST API 呼び出しを実行できる必要があるため、`cell1.us.vcloud.example.com` から `https://us.vcloud.example.com` への REST API 呼び出しが可能である必要があります。

REST API のファンアウトを行うには、すべてのサイトの REST API エンドポイントに対して REST API 要求を行う必要があります。たとえば、ユーザー インターフェイスまたは API クライアントがマルチサイト要求を行い、すべてのサイトから組織のページを取得して、`cell1.us.vcloud.example.com` で要求を処理する場合を考えます。セル `cell1` は REST API 呼び出しを行って、各サイトに構成された REST API エンドポイントを使用してサイトから組織のページを取得する必要があります。すべてのサイトから組織のページが返されたら、`cell1` は結果を照合し、他のすべてのサイトのデータを含む結果を 1 ページにまとめて返します。

サイトと証明書

サイトが他のサイトに関連付けられている場合に、証明書を更新する場合、他のサイトへの変更の通知が必要になることがあります。他のサイトに証明書の変更を知らせない場合、マルチサイトのファンアウトが影響を受ける可能性があります。

サイトの証明書を適切に署名された有効な証明書に置き換える場合は、他のサイトに通知する必要はありません。証明書は有効で、適切に署名されているため、他のサイトのセルは中断することなく、安全な方法で接続し続けることができます。

サイトの証明書を自己署名証明書に置き換える場合、または自動信頼の妨げとなる他の問題が証明書にある場合は、他のサイトに通知する必要があります。たとえば、証明書が期限切れの場合は、他のサイトに通知する必要があります。他の各サイトで、Service Provider Admin Portal の [信頼されている証明書] に証明書をアップロードする必要があります。[信頼されている証明書のインポート](#)を参照してください。証明書をインポートすると、証明書がアップロードされたサイトは新しい証明書を取得してサイトを信頼できます。

注： これらの証明書は、リモート サイトにインストールする前に、他のサイトの [信頼されている証明書] にインポートできます。これにより、古い証明書と新しい証明書の両方が信頼されている証明書プールに配置されるため、通信が中断されなくなります。サイトを再び関連付ける必要はありません。

関連付けメンバーのステータス

サイトまたは組織の関連付けを作成した後、ローカル システムは定期的にリモートの各関連付けメンバーのステータスを取得し、ローカル サイトの VMware Cloud Director データベースでステータスを更新します。メンバーのステータスは、SiteAssociationMember または OrgAssociationMember の Status 要素で確認できます。この要素には、以下の 3 つの値のいずれかが含まれます。

ACTIVE

両者の間で関連付けが確立され、リモート側との通信が正常に行われました。

ASYMMETRIC

ローカル サイトでの関連付けが確立されましたが、リモート サイトからの応答がありません。

UNREACHABLE

両者の間で関連付けが確立されましたが、現在リモート サイトがネットワーク上でアクセスできません。

メンバー ステータスの「ハートビート」は、マルチサイト システムのユーザー ID、つまり VMware Cloud Director のインストール中にシステム組織で作成したローカルの VMware Cloud Director ユーザー アカウントを使用して実行されます。このアカウントはシステム組織のメンバーですが、システム管理者の権限はありません。このアカウントには、Multisite: System Operations 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 VMware Cloud Director API 要求を行うことができます。

マルチサイト リソース リスト

複数の場所で VMware Cloud Director 環境を使用している場合は、接続されたすべてのサイトのオブジェクトに関する情報を含むリソース リストを表示できます。

Service Provider Admin Portal から vSphere およびクラウド リソースを介した移動を容易にするために、バージョン 9.7 以降の VMware Cloud Director にはマルチサイト リソース リストが導入されています。バージョン 10.0 以降の VMware Cloud Director は、組織を含むマルチサイト リソース リストをサポートしています。

リソース リストにアクセスするには、[vSphere リソース] メニューと [クラウド リソース] メニューを使用します。

複数のサイトのオブジェクトの詳細にアクセスできるほかに、ローカル サイトとリモート サイトの両方にオブジェクトを作成することもできます。

マルチサイト vSphere リソース リストは、vCenter Server インスタンス、NSX-T Manager インスタンス、リソース プール、データストア、ホスト、Distributed Switch、ポート グループ、取り残されたアイテム、およびストレージ ポリシーでサポートされます。

マルチサイト クラウド リソース リストは、組織、組織 VDC、組織 VDC テンプレート、プロバイダ VDC、クラウド セル、Edge Gateway、外部ネットワーク、ネットワーク プール、および仮想マシン サイズ変更ポリシーでサポートされます。

プロバイダ仮想データセンターの管理

4

プロバイダ仮想データセンターを作成すると、プロバイダ仮想データセンターのプロパティの変更、プロバイダ仮想データセンター自体の無効化/削除、プロバイダ仮想データセンターのストレージ ポリシーやリソース プールの管理を実行できます。

プロバイダ仮想データセンターを作成するには、Service Provider Admin Portal または vCloud API を使用する必要があります。Service Provider Admin Portal の使用の詳細については、[プロバイダ仮想データセンターの作成](#)を参照してください。vCloud API の使用の詳細については、「VMware Cloud Director API プログラミング ガイド」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。

- [プロバイダ仮想データセンターの有効化または無効化](#)
- [プロバイダ仮想データセンターの削除](#)
- [プロバイダ仮想データセンターの全般設定の編集](#)
- [プロバイダ仮想データセンターのマージ](#)
- [プロバイダ仮想データセンターの組織仮想データセンターの表示](#)
- [プロバイダ仮想データセンター上のデータストアの表示](#)
- [プロバイダ仮想データセンターの外部ネットワークの表示](#)
- [VMware Cloud Director での Kubernetes の使用](#)
- [プロバイダ仮想データセンターでの仮想マシン ストレージ ポリシーの管理](#)
- [プロバイダ仮想データセンターでのリソース プールの管理](#)
- [プロバイダ仮想データセンターのメタデータの変更](#)

プロバイダ仮想データセンターの有効化または無効化

プロバイダ仮想データセンター (VDC) のリソースを使用する既存のすべての組織 VDC を無効にするには、このプロバイダ VDC を無効にすることができます。無効にされたプロバイダ VDC のリソースを使用する組織 VDC を作成することはできません。

実行中の vApp およびパワーオンされた仮想マシンは、このプロバイダ VDC によってバックアップされている既存の組織 VDC で引き続き実行されますが、追加の vApp または仮想マシンを作成または起動することはできません。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [プロバイダ VDC] を選択します。
- 3 ターゲット プロバイダ VDC の名前の横にあるラジオ ボタンをクリックして、[有効化] または [無効化] をクリックします。
- 4 確認するには、[OK] をクリックします。

プロバイダ仮想データセンターの削除

プロバイダ仮想データセンターのリソースを VMware Cloud Director から削除するには、このプロバイダ仮想データセンターを削除します。

vSphere の基盤となるリソースは影響を受けません。

前提条件

- ターゲット プロバイダ仮想データセンターを無効にします。 [プロバイダ仮想データセンターの有効化または無効化](#)を参照してください。
- このプロバイダ仮想データセンターのリソースを使用するすべての組織仮想データセンターを削除します。 [組織仮想データセンターの削除](#)を参照してください。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [プロバイダ VDC] を選択します。
- 3 削除するプロバイダ仮想データセンター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 確認するには、[OK] をクリックします。

プロバイダ仮想データセンターの全般設定の編集

プロバイダ仮想データセンターの名前および説明を変更できます。バックアップ リソース プールでサポートされている仮想ハードウェアのバージョンの方が新しい場合は、プロバイダ仮想データセンターでサポートされる最新の仮想ハードウェアをアップグレードできます。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [プロバイダ VDC] をクリックし、変更するプロバイダ仮想データセンターの名前をクリックします。
- 3 [設定] - [全般] タブで、右上隅にある [編集] をクリックします。
- 4 (オプション) プロバイダ仮想データセンターの名前および説明を変更します。

- 5 (オプション) プロバイダ仮想データセンターのコンピューティングプロバイダ範囲を入力します。

コンピューティング プロバイダ範囲は、コンピューティング フォルト ドメインを表すか、テナントに表示される、ワークロードのあるアベイラビリティ ゾーンを表します。デフォルトでは、プロバイダ仮想データセンターのコンピューティング プロバイダ範囲は、バックアップ vCenter Server インスタンスから継承されます。単一の vCenter Server インスタンスによってバックアップされる複数のプロバイダ VDC のコンピューティング プロバイダ範囲を区別できます。たとえば、vCenter Server にコンピューティング プロバイダ範囲 **Germany** を設定し、プロバイダ VDC に範囲 **Munich** を設定することができます。

- 6 (オプション) ドロップダウン メニューから、このプロバイダ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 バージョンを選択し、[保存] をクリックします。

選択できる最新バージョンは、プロバイダ仮想データセンターをバックアップするリソース プール内の ESXi ホストによって決まります。

注： プロバイダ仮想データセンターでサポートされるハードウェア バージョンのみをアップグレードできます。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。VMware Cloud Director 10.2 でサポートされている仮想マシン ハードウェアの最大バージョンは、バージョン 17 です。ハードウェア バージョン 17 は、クラスタまたはデータセンター レベルの vCenter Server インスタンスで有効にした場合に使用できます。

- 7 [保存] をクリックします。

プロバイダ仮想データセンターのマージ

2 つのプロバイダ仮想データセンターのリソースを統合するには、これらのプロバイダ仮想データセンターを単一のプロバイダ仮想データセンターにマージします。

前提条件

- ターゲット プロバイダ仮想データセンターが、同じ vCenter Server データセンターに属していること。
- ターゲット プロバイダ仮想データセンターに、柔軟性に優れた組織仮想データセンターのみが含まれていること。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [プロバイダ VDC] を選択します。
- 3 拡張するプロバイダ仮想データセンターの名前の横にあるラジオ ボタンをクリックして、[マージ] をクリックします。
- 4 リソースをマージするプロバイダ仮想データセンターの名前の横にあるラジオ ボタンをクリックして、[マージ] をクリックします。

プロバイダ仮想データセンターの組織仮想データセンターの表示

プロバイダ仮想データセンターのリソースを使用している組織仮想データセンター (VDC) のリストを表示できます。


手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [プロバイダ VDC] を選択し、ターゲット プロバイダ仮想データセンターの名前をクリックします。
- 3 [組織 VDC] タブをクリックします。

結果

このプロバイダ仮想データセンターのリソースを使用している組織仮想データセンターのリストが表示されます。リストには、各組織 VDC のステータス、状態、割り当てモデル、組織、vCenter Server インスタンス、ネットワーク数、vApp の数、ストレージ ポリシーの数、およびリソース プールの数に関する情報が含まれています。

次のステップ

- VMware Cloud Director Tenant Portal の組織仮想データセンター ビューに移動するには、ターゲット組織仮想データセンターの名前の横にある [ポップアウト] アイコン () をクリックします。
- 組織仮想データセンターの名前の横にあるラジオ ボタンをクリックすると、[6 章 組織仮想データセンターの管理](#)に記載されている操作と同様の管理操作を実行できます。

プロバイダ仮想データセンター上のデータストアの表示

プロバイダ仮想データセンターにストレージ容量を提供するデータストアに関する詳細を表示できます。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [プロバイダ VDC] を選択し、ターゲット プロバイダ仮想データセンターの名前をクリックします。
- 3 [データストア] タブをクリックします。

プロバイダ仮想データセンター内のすべてのデータストアのリストが表示されます。リストには、各データストアについて次の情報が含まれています。

タイトル	説明
[名前]	データストアの名前
[状態]	有効または無効
[タイプ]	データストアが使用するファイル システムのタイプ (仮想マシン ファイル システム (VMFS) またはネットワーク ファイル システム (NFS))

タイトル	説明
[使用済み]	ログ ファイル、スナップショットおよび仮想ディスクなど、仮想マシン ファイルに使用されているデータストア領域。仮想マシンをパワーオンすると、使用済みストレージ領域にログ ファイルも含まれます。
[プロビジョニング済み]	仮想マシンに保証されているデータストア領域。仮想マシンがシンプロビジョニングを使用している場合、プロビジョニング済み容量の一部は使用されていないため、他の仮想マシンが使用されていない容量を使用できる場合があります。シン プロビジョニングを使用する場合、この値が実際のデータストア容量を超える場合があります。
[要求されたストレージ]	<p>データストア上で VMware Cloud Director オブジェクトによってのみ使用されているプロビジョニング済みのストレージで、以下を含みます。</p> <ul style="list-style-type: none"> ■ VMware Cloud Director でプロビジョニングされた仮想マシン ■ カタログ アイテム (テンプレートとメディア) ■ NSX Edge ■ 仮想マシンの使用済みおよび未使用のメモリ スワップ要件 <p>この値には、シャドウ仮想マシンまたはリンク クローン ツリー内の中間ディスクに要求されるストレージは含まれません。</p>
[vCenter Server]	データストアに関連付けられた vCenter Server インスタンス。

プロバイダ仮想データセンターの外部ネットワークの表示

プロバイダ仮想データセンターからアクセス可能な外部ネットワークのリストを表示できます。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [プロバイダ VDC] を選択し、ターゲット プロバイダ仮想データセンターの名前をクリックします。
- 3 [外部ネットワーク] タブをクリックします。

結果

使用可能な外部ネットワークのリストと、そのゲートウェイの CIDR 設定および IP アドレス プールの使用についての情報を表示できます。

VMware Cloud Director での Kubernetes の使用

VMware Cloud Director で Kubernetes を使用することにより、テナントにマルチテナントの Kubernetes サービスを提供できます。

Container Service Extension

Kubernetes Container Clusters は VMware Cloud Director 用の Container Service Extension プラグインです。サービス プロバイダおよびテナントが Kubernetes クラスタを作成するには、Kubernetes Container Clusters プラグインを使用する必要があります。VMware Cloud Director 10.2 以降では、プラグインの手動ダウンロードや、VMware Cloud Director Service Provider Admin Portal へのアップロードを行う必要はありません。VMware Cloud Director では、デフォルトでこのプラグインを使用できますが、Kubernetes クラスタを作成できるようにするには、テナントにプラグインを公開する必要があります。

ネイティブ クラスタと VMware Tanzu Kubernetes Grid Integrated Edition (TKGI) クラスタを作成するには、サービス プロバイダとテナントの両方が Container Service Extension バージョン 3.0 を使用する必要があります。Container Service Extension 3.0 サーバのセットアップを完了し、Container Service Extension ネイティブ配置ポリシーを 1 つ以上の組織 VDC に公開する必要があります。

VMware Cloud Director の vSphere with VMware Tanzu

VMware Cloud Director の vSphere with VMware Tanzu を使用すると、スーパーバイザー クラスタによってバックアップされているプロバイダ仮想データセンター (VDC) を作成できます。vSphere with VMware Tanzu が有効になっているホスト クラスタは、スーパーバイザー クラスタと呼ばれます。リソースの使用に制限を設定し、組織、ユーザー、グループあたりの Kubernetes クラスタの数など、使用可能なリソースを制限することができます。詳細については、[組織のリソース使用に対する割り当て容量の管理](#)を参照してください。

VMware Cloud Director で vSphere with VMware Tanzu を使用するには、まず vSphere 7.0 以降のクラスタで vSphere with VMware Tanzu 機能を有効にして、そのクラスタをスーパーバイザー クラスタとして構成する必要があります。vSphere ドキュメントの『vSphere with Kubernetes の構成および管理』ガイドを参照してください。使用する vCenter Server インスタンスには、ホスト クラスタとスーパーバイザー クラスタを両方含めることができます。

クラスタを作成するには、Tanzu Kubernetes プロバイダ VDC Kubernetes ポリシーを組織に公開し、作成時に組織 VDC Kubernetes ポリシーを適用する必要があります。ネイティブ クラスタおよび TKGI クラスタは、プロバイダ VDC Kubernetes ポリシーと組織 VDC Kubernetes ポリシーを使用しません。

Kubernetes クラスタ タイプ

- ネイティブ クラスタ - Kubernetes Container Clusters プラグインは、ネイティブの Kubernetes ランタイムを使用してクラスタを管理します。これらのクラスタは制御プレーン ノードが 1 台で、High Availability 機能は削減されています。また、パーシステント ボリュームの選択肢は少なく、ネットワークの自動化機能もありません。ただし、コストが低くなる場合があります。ネイティブの Kubernetes クラスタ環境では、Container Service Extension サーバをセットアップする必要があります。Container Service Extension (CSE) のドキュメントの「[CSE サーバ管理](#)」の章を参照してください。
- Tanzu Kubernetes クラスタ - vSphere with Tanzu ランタイム オプションを使用して、vSphere with VMware Tanzu で管理される Tanzu Kubernetes クラスタを作成できます。このオプションを使用すると、機能は増えますが、コストが高くなる可能性があります。詳細については、vSphere ドキュメントの『vSphere with Kubernetes の構成および管理』ガイドを参照してください。

- TKGI クラスタ - VMware Tanzu Kubernetes Grid Integrated Edition は、マルチクラウドのエンタープライズ プロバイダおよびサービス プロバイダが運用できる Kubernetes を対象とする、専用のコンテナ ソリューションです。これらの機能には、Kubernetes クラスタの高可用性、自動拡張、健全性チェック、自己修復、ローリング アップグレードなどがあります。TKGI クラスタの詳細については、VMware Tanzu Kubernetes Grid Integrated Edition のドキュメントを参照してください。

Tanzu Kubernetes クラスタ作成用のワークフロー

- 1 vSphere with VMware Tanzu 機能が有効になっている vCenter Server 7.0 以降のインスタンスを VMware Cloud Director に追加します。『[vCenter Server インスタンスを単独、または NSX Manager インスタンスと共に接続する](#)』を参照してください。
- 2 各スーパーバイザー クラスタのネットワーク設定を確認して、Kubernetes のワークロードを実行できるようにします。

重要： Ingress CIDRs および Services CIDR パラメータの IP アドレス範囲が、services および pods パラメータのデフォルトの vSphere の値である IP アドレス 10.96.0.0/12 および 192.168.0.0/192.16 と重複することはできません。『[vSphere with Kubernetes の構成および管理](#)』ガイドの Tanzu Kubernetes クラスタの構成パラメータに関する情報を参照してください。

注： VMware Cloud Director 10.2.2 以降で、初期セットアップ後にスーパーバイザー クラスタのネットワーク設定を変更した場合は、vCenter Server インスタンスを更新して、クラスタが作成された組織仮想データセンターの外部にある Tanzu Kubernetes クラスタからのアクセスをブロックする自動ファイアウォール ポリシーおよび NAT ルールを調整する必要があります。

- 3 スーパーバイザー クラスタによってバックアップされるプロバイダ VDC を作成します。『[プロバイダ仮想データセンターの作成](#)』を参照してください。

または、既存のプロバイダ VDC にスーパーバイザー クラスタを追加することもできます。vSphere 6.7 以前の環境を使用している場合は、環境をバージョン 7.0 にアップグレードして、既存のクラスタで vSphere with VMware Tanzu を有効にすることもできます。

スーパーバイザー クラスタによってバックアップされているプロバイダ VDC は、すべてのプロバイダ VDC が表示されているグリッド内に、名前の横に Kubernetes アイコンが付いた状態で表示されます。

- 4 (オプション) VMware Cloud Director によって、スーパーバイザー クラスタでバックアップされているプロバイダ VDC のデフォルトのプロバイダ VDC Kubernetes ポリシーが自動的に生成されます。Tanzu Kubernetes クラスタに対して、追加のプロバイダ VDC Kubernetes ポリシーを作成できます。『[プロバイダ VDC Kubernetes ポリシーの作成](#)』を参照してください。
- 5 [プロバイダ VDC] タブの [プロバイダ VDC Kubernetes ポリシーの組織 VDC への公開](#) または [組織 VDC] タブの [組織 VDC Kubernetes ポリシーの追加](#)。
- 6 サービス プロバイダに Kubernetes Container Clusters プラグインを公開します。『[組織からのプラグインの公開または公開解除](#)』を参照してください。テナントで Kubernetes クラスタを作成できるようにするには、これらの組織に Kubernetes Container Clusters プラグインを公開する必要があります。VMware Cloud Director プラグインの管理の詳細については、[プラグインの管理](#)を参照してください。

- 7 Tanzu Kubernetes クラスタを作成および管理する権限をテナントに付与する場合は、クラスタを使用する組織に `vmware : tkgcluster` 資格権限バンドルを公開する必要があります。権限バンドルを共有したら、Tanzu Kubernetes クラスタを作成および変更するロールに編集 : Tanzu Kubernetes ゲスト クラスタ権限を追加する必要があります。ユーザーがクラスタの削除を行う場合は、ロールに完全コントロール : Tanzu Kubernetes ゲスト クラスタ権限を追加する必要があります。さらに、組織内のすべての Tanzu Kubernetes クラスタを表示するユーザーや、サイト間でクラスタを管理するユーザーに、管理者権限を割り当てることもできます。ランタイム定義エンティティ (RDE) の権限およびアクセス レベルの詳細については、[14 章 定義済みエンティティの管理](#)を参照してください。
- 8 アクセス コントロール リスト (ACL) エントリを作成して、テナントまたはシステム管理者にアクセス権を付与します。ランタイム定義エンティティ (RDE) の共有の詳細については、[定義済みエンティティの共有](#)を参照してください。
- 9 [Tanzu Kubernetes クラスタの作成](#)

ネイティブ クラスタおよび TKGI クラスタ作成のワークフロー

- 1 サービス プロバイダに Kubernetes Container Clusters プラグインを公開します。『[組織からのプラグインの公開または公開解除](#)』を参照してください。テナントで Kubernetes クラスタを作成できるようにするには、これらの組織に Kubernetes Container Clusters プラグインを公開する必要があります。VMware Cloud Director プラグインの管理の詳細については、[プラグインの管理](#)を参照してください。
- 2 Container Service Extension サーバをセットアップし、Container Service Extension ネイティブ配置ポリシーまたは TKGI 有効化メタデータを組織 VDC に公開します。CSE サーバの設定の詳細については、Container Service Extension (CSE) のドキュメントの[CSE サーバ管理](#)の章を参照してください。
- 3 ネイティブ クラスタを作成および管理する権限をテナントに付与する場合は、ネイティブ クラスタを使用する組織に `cse : nativeCluster` 資格権限バンドルを公開する必要があります。権限バンドルを共有したら、ネイティブ クラスタを作成および変更するロールに 編集 : CSE : NATIVECLUSTER 権限を追加する必要があります。ユーザーがクラスタの削除を行う場合は、ロールに完全コントロール : CSE : NATIVECLUSTER 権限を追加する必要があります。さらに、組織内のすべての Tanzu Kubernetes クラスタを表示するユーザーや、サイト間でクラスタを管理するユーザーに、管理者権限を割り当てることもできます。ランタイム定義エンティティ (RDE) の権限およびアクセス レベルの詳細については、[14 章 定義済みエンティティの管理](#)を参照してください。
- 4 TKGI クラスタを作成および管理する権限をテナントに付与する場合は、特定の組織に `{cse} : PKS DEPLOY RIGHT` 権限を公開し、TKGI クラスタを作成および管理するロールに `{cse} : PKS DEPLOY RIGHT` 権限を追加する必要があります。`{cse} : PKS DEPLOY RIGHT` は、Container Service Extension サーバのインストール中に作成されます。
- 5 ネイティブ クラスタのアクセス コントロール リスト (ACL) エントリを作成して、テナントまたはシステム管理者にアクセス権を付与します。ランタイム定義エンティティ (RDE) の共有の詳細については、[定義済みエンティティの共有](#)を参照してください。
- 6 [ネイティブ Kubernetes クラスタの作成または VMware Tanzu Kubernetes Grid Integrated Edition クラスタの作成](#)。

vSphere with VMware Tanzu クラスタの作成

プロバイダ VDC と組織 VDC の Kubernetes ポリシーを使用すると、vSphere with VMware Tanzu クラスタを作成できます。

VMware Cloud Director の vSphere with VMware Tanzu

vSphere クラスタで vSphere with VMware Tanzu を有効にすると、Kubernetes ワークロードを ESXi ホストで直接実行し、専用リソース プール内にアップストリーム Kubernetes クラスタを作成できるようになります。詳細については、vSphere ドキュメントの『vSphere with Kubernetes の構成および管理』ガイドを参照してください。

VMware Cloud Director の vSphere with VMware Tanzu を使用すると、スーパーバイザー クラスタによってバックアップされているプロバイダ仮想データセンター (VDC) を作成できます。vSphere with VMware Tanzu が有効になっているホスト クラスタは、スーパーバイザー クラスタと呼ばれます。リソースの使用に制限を設定し、組織、ユーザー、グループあたりの Kubernetes クラスタの数など、使用可能なリソースを制限することができます。詳細については、[組織のリソース使用に対する割り当て容量の管理](#)を参照してください。

VMware Cloud Director で vSphere with VMware Tanzu を使用するには、まず vSphere 7.0 以降のクラスタで vSphere with VMware Tanzu 機能を有効にして、そのクラスタをスーパーバイザー クラスタとして構成する必要があります。vSphere ドキュメントの『vSphere with Kubernetes の構成および管理』ガイドを参照してください。使用する vCenter Server インスタンスには、ホスト クラスタとスーパーバイザー クラスタを両方含めることができます。

テナントは、組織 VDC Kubernetes ポリシーの 1 つを適用することによって Tanzu Kubernetes クラスタを作成できます。システム管理者は、Service Provider Admin Portal または VMware Cloud Director Tenant Portal を使用して組織 VDC の Kubernetes ポリシーを編集および削除できます。ネイティブ クラスタおよび TKGI クラスタは、プロバイダ VDC Kubernetes ポリシーと組織 VDC Kubernetes ポリシーを使用しません。

VMware Cloud Director は、PodSecurityPolicy アドミッション コントローラが有効な状態で Tanzu Kubernetes クラスタをプロビジョニングします。ワークロードをデプロイするには、ポッドのセキュリティ ポリシーを作成する必要があります。ポッドのセキュリティ ポリシーを Kubernetes で使用する実装の詳細については、『vSphere with Kubernetes の構成および管理』ガイドの「Tanzu Kubernetes クラスタでのポッドのセキュリティ ポリシーの使用」を参照してください。

ワークフロー

- 1 vSphere with VMware Tanzu 機能が有効になっている vCenter Server 7.0 以降のインスタンスを VMware Cloud Director に追加します。『[vCenter Server インスタンスを単独、または NSX Manager インスタンスと共に接続する](#)』を参照してください。
- 2 スーパーバイザー クラスタによってバックアップされるプロバイダ VDC を作成します。『[プロバイダ仮想データセンターの作成](#)』を参照してください。

または、既存のプロバイダ VDC にスーパーバイザー クラスタを追加することもできます。vSphere 6.7 以前の環境を使用している場合は、環境をバージョン 7.0 にアップグレードして、既存のクラスタで vSphere with VMware Tanzu を有効にすることもできます。

スーパーバイザー クラスタによってバックアップされているプロバイダ VDC は、すべてのプロバイダ VDC が表示されているグリッド内に、名前の横に Kubernetes アイコンが付いた状態で表示されます。

- 3 (オプション) VMware Cloud Director によって、スーパーバイザー クラスタでバックアップされているプロバイダ VDC のデフォルトのプロバイダ VDC Kubernetes ポリシーが自動的に生成されます。Tanzu Kubernetes クラスタに対して、追加のプロバイダ VDC Kubernetes ポリシーを作成できます。『[プロバイダ VDC Kubernetes ポリシーの作成](#)』を参照してください。
- 4 [プロバイダ VDC] タブの[プロバイダ VDC Kubernetes ポリシーの組織 VDC への公開](#) または [組織 VDC] タブの [組織 VDC Kubernetes ポリシーの追加](#)。
- 5 サービス プロバイダに Kubernetes Container Clusters プラグインを公開します。『[組織からのプラグインの公開または公開解除](#)』を参照してください。テナントで Kubernetes クラスタを作成できるようにするには、これらの組織に Kubernetes Container Clusters プラグインを公開する必要があります。VMware Cloud Director プラグインの管理の詳細については、[プラグインの管理](#)を参照してください。
- 6 Tanzu Kubernetes クラスタを使用する組織に、vmware : tkgcluster 資格権限バンドルを公開します。
- 7 Tanzu Kubernetes クラスタを作成するロールに編集 : Tanzu Kubernetes ゲスト クラスタ権限を追加します。ユーザーがクラスタの削除も行う場合は、ロールに完全コントロール : Tanzu Kubernetes ゲスト クラスタ権限を追加する必要があります。さらに、組織内のすべての Tanzu Kubernetes クラスタを表示するユーザーや、サイト間でクラスタを管理するユーザーに、管理者権限を割り当てることもできます。ランタイム定義エンティティ (RDE) の権限およびアクセス レベルの詳細については、[14 章 定義済みエンティティの管理](#)を参照してください。
- 8 アクセス コントロール リスト (ACL) エントリを作成して、テナントまたはシステム管理者にアクセス権を付与します。ランタイム定義エンティティ (RDE) の共有の詳細については、[定義済みエンティティの共有](#)を参照してください。
- 9 [Tanzu Kubernetes クラスタの作成](#)

プロバイダ VDC Kubernetes ポリシーの作成

VMware Cloud Director では、スーパーバイザー クラスタにバックアップされているプロバイダ VDC のデフォルトのプロバイダ VDC Kubernetes ポリシーが自動的に生成されます。Tanzu Kubernetes クラスタに対して、追加のプロバイダ VDC Kubernetes ポリシーを作成できます。

プロバイダ VDC Kubernetes ポリシーと組織 VDC Kubernetes ポリシーは、Tanzu Kubernetes クラスタを作成する場合、またはテナントで作成できるようにする場合にのみ必要になります。ネイティブ クラスタおよび TKGI クラスタでは、これらの Kubernetes ポリシーは使用されません。

前提条件

スーパーバイザー クラスタによってバックアップされているプロバイダ VDC が 1 つ以上あることを確認するか、既存のプロバイダ VDC にスーパーバイザー クラスタを追加します。[VMware Cloud Director での Kubernetes の使用](#)を参照してください。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
 - 2 左側のパネルで [プロバイダ VDC] を選択し、プロバイダ VDC の名前をクリックします。
 - 3 [ポリシー] で [Kubernetes] を選択し、[新規] をクリックします。
- [VDC Kubernetes ポリシーの作成] ウィザードが表示されます。

- 4 プロバイダ VDC Kubernetes ポリシー名前と説明を入力し、[次へ] をクリックします。
- 5 Kubernetes 対応スーパーバイザー クラスタによってバックアップされているリソース プールを選択します。
- 6 このポリシーで作成された Kubernetes クラスタ ノードの CPU とメモリを予約するかどうかを選択します。
 クラス タイプごとに、保証型とベスト エフォート型の 2 つのエディションがあります。保証型クラス エディションでは構成済みリソースが完全に予約されますが、ベスト エフォート型エディションではリソースのオーバーコミットが許可されます。選択内容に応じて、ウィザードの次のページで、仮想マシンのクラス タイプを、保証型エディションまたはベスト エフォート型エディションの中から選択できます。
 - CPU とメモリを完全に予約する保証型エディションの仮想マシンクラス タイプを指定するには、[はい] を選択します。
 - CPU とメモリが予約されていないベスト エフォート型エディションの仮想マシン クラス タイプを指定するには、[いいえ] を選択します。
- 7 このポリシーで作成された Kubernetes クラスタの CPU およびメモリの制限を選択します。
 ポリシーを組織 VDC に公開すると、選択した制限は、新しく作成された組織 VDC Kubernetes ポリシーの最大値として機能します。
- 8 [次へ] をクリックします。
- 9 ウィザードの [マシン クラス] 画面で、このポリシーで使用可能な 1 つ以上の仮想マシン クラス タイプを選択し、[次へ] をクリックします。
 組織 VDC へのポリシーの公開の際にテナントで使用可能なクラス タイプは、ここで選択したマシン クラスに限定されます。
- 10 1 つ以上のストレージ ポリシーを選択します。
- 11 選択内容を確認し、[完了] をクリックします。

次のステップ

[プロバイダ VDC Kubernetes ポリシーの組織 VDC への公開](#)

vSphere Kubernetes ポリシーの編集

組織 VDC Kubernetes ポリシーと Tanzu Kubernetes クラスタの作成に使用される、プロバイダ VDC Kubernetes ポリシーの設定を編集できます。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [プロバイダ VDC] を選択し、プロバイダ VDC の名前をクリックします。
- 3 (オプション) [ポリシー] で [Kubernetes] を選択し、公開するポリシーを選択して、[編集] をクリックします。
 [VDC Kubernetes ポリシーの編集] ウィザードが表示されます。
- 4 (オプション) プロバイダ VDC Kubernetes ポリシー名前と説明を編集して、[次へ] をクリックします。

- 5 (オプション) このポリシーで作成された Kubernetes クラスターの CPU およびメモリの制限を変更して、[次へ] をクリックします。

ポリシーを組織 VDC に公開すると、選択した制限は、新しく作成された組織 VDC Kubernetes ポリシーの最大値として機能します。

- 6 (オプション) ウィザードの [マシン クラス] 画面で、このポリシーで使用可能な 1 つ以上の仮想マシン クラス タイプを追加し、[次へ] をクリックします。

組織 VDC へのポリシーの公開の際にテナントで使用可能なクラス タイプは、ここで選択したマシン クラスに限定されます。

- 7 (オプション) 1 つ以上のストレージ ポリシーを追加します。

- 8 選択内容を確認し、[保存] をクリックします。

次のステップ

プロバイダ VDC Kubernetes ポリシーの組織 VDC への公開

プロバイダ VDC Kubernetes ポリシーの組織 VDC への公開

プロバイダ VDC Kubernetes ポリシーをテナントが使用できるようにするには、Flex 組織 VDC に公開します。プロバイダ VDC Kubernetes ポリシーを公開する場合は、テナントによる Kubernetes クラスターの作成に使用可能な組織 VDC Kubernetes ポリシーを作成します。

プロバイダ VDC Kubernetes ポリシーを組織 VDC に追加または公開する場合は、そのポリシーをテナントが使用できるようにします。テナントは、利用可能な組織 VDC Kubernetes ポリシーを使用して、Kubernetes クラスターを作成するときに Kubernetes キャパシティを利用できます。Kubernetes ポリシーによって、配置、インフラストラクチャの品質、パーシステント ボリュームのストレージ クラスがカプセル化されます。Kubernetes ポリシーには、コンピューティングに関するさまざまな制限を設定できます。

1 つの組織 VDC に複数のプロバイダ VDC Kubernetes ポリシーを公開できます。1 つのプロバイダ VDC Kubernetes ポリシーを組織 VDC に複数回公開できます。組織 VDC Kubernetes ポリシーは、サービス品質のインジケータとして使用できます。たとえば、保証型マシン クラスと高速ストレージ クラスを選択できるゴールド Kubernetes ポリシー、またはベスト エフォート型マシン クラスと低速ストレージ クラスを選択できるシルバー Kubernetes ポリシーを公開できます。

前提条件

- スーパーバイザー クラスターによってバックアップされているプロバイダ VDC を作成するか、既存のプロバイダ VDC にスーパーバイザー クラスターを追加します。[VMware Cloud Director での Kubernetes の使用](#)を参照してください。
- 環境内に 1 つ以上の Flex 組織 VDC があることを確認します。[組織仮想データセンターの作成](#)を参照してください。
- Tanzu Kubernetes クラスターの仮想マシン クラス タイプについて理解しておきます。vSphere ドキュメントの『vSphere with Kubernetes の構成および管理』ガイドを参照してください。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。

- 2 左側のパネルで [プロバイダ VDC] を選択し、プロバイダ VDC の名前をクリックします。
- 3 [ポリシー] で [Kubernetes] を選択し、公開するポリシーを選択して、[公開] をクリックします。
[組織 VDC に公開] ウィザードが表示されます。
- 4 テナントに表示される、組織 VDC Kubernetes ポリシーの名前と説明を入力し、[次へ] をクリックします。
- 5 ポリシーを公開する Flex 組織 VDC を選択して、[次へ] をクリックします。
- 6 このポリシーで作成された Kubernetes クラスターの CPU およびメモリの制限を選択します。
上限は、組織 VDC の CPU とメモリの割り当てによって異なります。ポリシーを公開すると、選択した制限はテナントの最大値として機能します。
- 7 このポリシーで作成された Kubernetes クラスター ノードの CPU とメモリを予約するかどうかを選択して、[次へ] をクリックします。
クラス タイプごとに、保証型とベスト エフォート型の 2 つのエディションがあります。保証型クラス エディションでは構成済みリソースが完全に予約されますが、ベスト エフォート型エディションではリソースのオーバーコミットが許可されます。選択内容に応じて、ウィザードの次のページで、仮想マシンのクラス タイプを、保証型エディションまたはベスト エフォート型エディションの中から選択できます。
 - CPU とメモリを完全に予約する保証型エディションの仮想マシンクラス タイプを指定するには、[はい] を選択します。
 - CPU とメモリが予約されていないベスト エフォート型エディションの仮想マシン クラス タイプを指定するには、[いいえ] を選択します。
- 8 ウィザードの [マシン クラス] 画面で、このポリシーで使用可能な仮想マシン クラス タイプを 1 つ以上選択します。
組織 VDC へのポリシーの公開の際にテナントで使用可能なクラス タイプは、ここで選択したマシン クラスに限定されます。
- 9 1 つ以上のストレージ ポリシーを選択します。
- 10 選択内容を確認し、[公開] をクリックします。

結果

公開されたポリシーに関する情報は、Flex 組織 VDC の [ポリシー] セクションに表示されます。公開されたポリシーによって、スーパーバイザー クラスター上に、指定されたリソース制限を持つスーパーバイザー ネームスペースが作成されます。

テナントは、Kubernetes ポリシーを使用して、Kubernetes クラスターを作成できます。VMware Cloud Director は、作成された各 Kubernetes を、同じスーパーバイザー ネームスペース内のこの Kubernetes ポリシーの下に配置します。ポリシーのリソース制限が、スーパーバイザー ネームスペースのリソース制限になります。スーパーバイザー ネームスペースの、テナントで作成されたすべての Kubernetes クラスターは、これらの制限内のリソースについて競合します。

Tanzu Kubernetes クラスターの作成

Kubernetes Container Clusters プラグインを使用して Tanzu Kubernetes クラスターを作成できます。

クラスタ作成に関するさまざまな Kubernetes ランタイム オプションの詳細については、[VMware Cloud Director での Kubernetes の使用](#)を参照してください。

コンテナ サービス拡張機能 CLI を使用して、Kubernetes クラスタを管理することもできます。[Container Service Extension](#) のドキュメントを参照してください。

VMware Cloud Director は、PodSecurityPolicy アドミSSION コントローラが有効な状態で Tanzu Kubernetes クラスタをプロビジョニングします。ワークロードをデプロイするには、ポッドのセキュリティ ポリシーを作成する必要があります。ポッドのセキュリティ ポリシーを Kubernetes で使用する実装の詳細については、『vSphere with Kubernetes の構成および管理』ガイドの「Tanzu Kubernetes クラスタでのポッドのセキュリティ ポリシーの使用」を参照してください。

前提条件

- Tanzu Kubernetes クラスタを管理するすべての組織に Kubernetes Container Clusters プラグインを公開します。
- 組織 VDC 内に 1 つ以上の組織 VDC Kubernetes ポリシーがあることを確認します。組織 VDC Kubernetes ポリシーを追加するには、[組織 VDC Kubernetes ポリシーの追加](#)を参照してください。
- クラスタを使用する組織に、vmware : tkgcluster 資格権限バンドルを公開する必要があります。権限バンドルを共有したら、Tanzu Kubernetes クラスタを作成および変更するロールに編集 : Tanzu Kubernetes ゲスト クラスタ権限を追加する必要があります。ユーザーがクラスタの削除も行う場合は、ロールに完全コントロール : Tanzu Kubernetes ゲスト クラスタ権限を追加する必要があります。さらに、組織内のすべての Tanzu Kubernetes クラスタを表示するユーザーや、サイト間でクラスタを管理するユーザーに、管理者権限を割り当てることもできます。ランタイム定義エンティティ (RDE) の権限およびアクセス レベルの詳細については、[14 章 定義済みエンティティの管理](#)を参照してください。
- アクセス コントロール リスト (ACL) エントリを作成して、テナントまたはシステム管理者にアクセス権を付与します。ランタイム定義エンティティ (RDE) の共有の詳細については、[定義済みエンティティの共有](#)を参照してください。

手順

- 1 上部ナビゲーション バーで、[詳細] - [Kubernetes Container Clusters] の順に選択します。
- 2 (オプション) TKGI クラスタを作成する際に組織 VDC が有効になっている場合は、[Kubernetes Container Clusters] 画面で [vSphere with Tanzu およびネイティブ] タブを選択します。
- 3 [新規] をクリックします。
- 4 [vSphere with Tanzu] ランタイム オプションを選択して、[次へ] をクリックします。
- 5 新しい Kubernetes クラスタの名前を入力して、[次へ] をクリックします。
- 6 Tanzu Kubernetes クラスタをデプロイする組織 VDC を選択して、[次へ] をクリックします。

- 7 組織 VDC Kubernetes ポリシーと Kubernetes バージョンを選択して、[次へ] をクリックします。

VMware Cloud Director に、組織 VDC または Kubernetes ポリシーにも関連付けられていないデフォルトの Kubernetes バージョン セットが表示されます。これらのバージョンはグローバル設定です。使用可能なバージョンのリストを変更するには、セル管理ツールを使用して、`./cell-management-tool manage-config --name wcp.supported.kubernetes.versions -v version_numbers` コマンドにカンマ区切りのバージョン番号を指定して実行します。

- 8 新しいクラスタの制御プレーンおよびワーカー ノードの数を選択します。
- 9 制御プレーンおよびワーカー ノードのマシン クラスを選択して、[次へ] をクリックします。
- 10 制御プレーンおよびワーカー ノードの Kubernetes ポリシー ストレージ クラスを選択して、[次へ] をクリックします。
- 11 (オプション) VMware Cloud Director 10.2.2 以降の場合は、Kubernetes サービスの IP アドレスの範囲と Kubernetes ポッドの範囲を指定して、[次へ] をクリックします。

Classless Inter-Domain Routing (CIDR) は、IP ルーティングと IP アドレス割り当ての方法です。

オプション	説明
Pods CIDR	Kubernetes ポッドで使用する IP アドレスの範囲を指定します。デフォルト値は 192.168.0.0/16 です。ポッドのサブネット サイズは /24 以上にする必要があります。この値はスーパーバイザー クラスタの設定と重複することはできません。1 つの IP アドレス範囲を入力できます。
Services CIDR	Kubernetes サービスで使用する IP アドレスの範囲を指定します。デフォルト値は 10.96.0.0/12 です。この値はスーパーバイザー クラスタの設定と重複することはできません。1 つの IP アドレス範囲を入力できます。

- 12 クラスタの設定を確認し、[終了] をクリックします。

次のステップ

- ワーカー ノードの数を変更する場合は、Kubernetes クラスタのサイズを変更します。
- kubeconfig ファイルをダウンロードします。kubectl コマンドライン ツールは、kubeconfig ファイルを使用して、クラスタ、ユーザー、名前空間、および認証メカニズムに関する情報を取得します。
- Kubernetes クラスタを削除します。

ネイティブ Kubernetes クラスタの作成

Kubernetes Container Clusters プラグインを使用して、Container Service Extension 3.0 管理対象の Kubernetes クラスタを作成できます。

クラスタ作成に関するさまざまな Kubernetes ランタイム オプションの詳細については、[VMware Cloud Director での Kubernetes の使用](#)を参照してください。

コンテナ サービス拡張機能 CLI を使用して、Kubernetes クラスタを管理することもできます。[Container Service Extension](#) のドキュメントを参照してください。

前提条件

- サービス プロバイダが、Kubernetes Container Clusters プラグインを組織に公開していることを確認します。Kubernetes Container Clusters は VMware Cloud Director 用の Container Service Extension プラグインです。このプラグインは、上部ナビゲーション バーの [詳細] - [Kubernetes Container Clusters] で確認できます。
- ネイティブ Kubernetes クラスタ環境で組織 VDC を有効にするには、Container Service Extension サーバを設定します。Container Service Extension (CSE) のドキュメントの [CSE サーバ管理](#) の章を参照してください。
- CSE サーバのセットアップ中に作成された CSE ネイティブ ポリシーを組織 VDC に公開します。ユーザー インターフェイスを使用するには、[組織 VDC への仮想マシン配置ポリシーの追加](#)を参照してください。CSE 3.0 CLI を使用してポリシーを発行するには、`vcd cse ovdc enable Organization_VDC_Name --org Organization_Name --native` コマンドを実行します。
- `cse: nativeCluster` 資格権限バンドルを、ネイティブ クラスタを使用する組織に公開する必要があります。権限バンドルを共有したら、Tanzu Kubernetes クラスタを作成および変更するロールに編集 : CSE : NATIVECLUSTER 権限を追加する必要があります。ユーザーがクラスタの削除も行う場合は、ロールに完全コントロール : CSE : NATIVECLUSTER 権限を追加する必要があります。さらに、組織内のすべての Tanzu Kubernetes クラスタを表示するユーザーや、サイト間でクラスタを管理するユーザーに、管理者権限を割り当てることもできます。ランタイム定義エンティティ (RDE) の権限およびアクセス レベルの詳細については、[14 章 定義済みエンティティの管理](#)を参照してください。
- アクセス コントロール リスト (ACL) エントリを作成して、テナントまたはシステム管理者にアクセス権を付与します。ランタイム定義エンティティ (RDE) の共有の詳細については、[定義済みエンティティの共有](#)を参照してください。

手順

- 1 上部ナビゲーション バーで、[詳細] - [Kubernetes Container Clusters] の順に選択します。
- 2 (オプション) TKGI クラスタを作成する際に組織 VDC が有効になっている場合は、[Kubernetes Container Clusters] 画面で [vSphere with Tanzu およびネイティブ] タブを選択します。
- 3 [新規] をクリックします。
- 4 [ネイティブ] Kubernetes ランタイム オプションを選択します。
- 5 名前を入力し、リストから Kubernetes テンプレートを選択します。
- 6 (オプション) 新しい Kubernetes クラスタおよび SSH パブリック キーの説明を入力します。
- 7 [次へ] をクリックします。
- 8 ネイティブ クラスタをデプロイする組織 VDC を選択して、[次へ] をクリックします。
- 9 制御プレーンおよびワーカー ノードの数を選択し、必要に応じてノードのサイズ変更ポリシーを選択します。
- 10 [次へ] をクリックします。
- 11 NFS ソフトウェアを使用して追加の仮想マシンをデプロイする場合は、[NFS を有効化] をオンにします。
- 12 (オプション) 制御プレーンおよびワーカー ノードのストレージ ポリシーを選択します。

13 [次へ] をクリックします。

14 Kubernetes クラスタのネットワークを選択して、[次へ] をクリックします。

15 クラスタの設定を確認し、[終了] をクリックします。

次のステップ

- ワーカー ノードの数を変更する場合は、Kubernetes クラスタのサイズを変更します。
- kubeconfig ファイルをダウンロードします。kubectl コマンドライン ツールは、kubeconfig ファイルを使用して、クラスタ、ユーザー、名前空間、および認証メカニズムに関する情報を取得します。
- Kubernetes クラスタを削除します。

VMware Tanzu Kubernetes Grid Integrated Edition クラスタの作成

Container Service Extension を使用して VMware Tanzu Kubernetes Grid Integrated Edition (TKGI) クラスタを作成できます。

クラスタ作成に関するさまざまな Kubernetes ランタイム オプションの詳細については、[VMware Cloud Director での Kubernetes の使用](#)を参照してください。

コンテナ サービス拡張機能 CLI を使用して、Kubernetes クラスタを管理することもできます。[Container Service Extension](#) のドキュメントを参照してください。

TKGI の有効化メタデータを使用することで、TKGI クラスタを作成し、TKGI 対応の組織 VDC にアクセスするためのアクセス権をテナントに提供することができます。TKGI クラスタを作成するテナントの機能を制限する場合は、組織 VDC へのアクセス権のみを提供します。この場合、テナントは既存の TKGI クラスタを管理することはできませんが、新しいクラスタを作成することはできません。

前提条件

- サービス プロバイダが、Kubernetes Container Clusters プラグインを組織に公開していることを確認します。Kubernetes Container Clusters は VMware Cloud Director 用の Container Service Extension プラグインです。このプラグインは、上部ナビゲーション バーの [詳細] - [Kubernetes Container Clusters] で確認できます。
- TKGI Kubernetes クラスタ環境で組織 VDC を有効にするには、Container Service Extension サーバを設定します。CSE CLI を使用して TKGI の組織 VDC を有効にする方法については、Container Service Extension (CSE) ドキュメントの [CSE サーバ管理](#) の章を参照してください。
- TKGI の作成と管理にテナントからアクセスできるようにする場合は、特定の組織に {cse} : PKS DEPLOY RIGHT 権限を公開し、TKGI クラスタを作成および管理するロールに {cse} : PKS DEPLOY RIGHT を追加する必要があります。{cse} : PKS DEPLOY RIGHT は、Container Service Extension サーバのインストール中に作成されます。

手順

- 1 上部ナビゲーション バーで、[詳細] - [Kubernetes Container Clusters] の順に選択します。
- 2 [Kubernetes Container Clusters] 画面で [TKGI] タブを選択し、[新規] をクリックします。
[新しい TKGI クラスタの作成] ウィザードが開きます。

- 3 TKGI クラスタをデプロイする組織 VDC を選択して、[次へ] をクリックします。

VMware Cloud Director から CSE サーバ内の情報が要求されるため、リストがロードされるまで時間がかかることがあります。

- 4 新しい TKGI クラスタの名前を入力し、ワーカー ノードの数を選択します。

TKGI クラスタには、1 台以上のワーカー ノードが必要です。

- 5 [次へ] をクリックします。

- 6 クラスタの設定を確認し、[終了] をクリックします。

- 7 (オプション) 新しい TKGI クラスタをクラスタ リストに表示するには、ページの右側にある [更新] ボタンをクリックします。

次のステップ

- ワーカー ノードの数を変更する場合は、Kubernetes クラスタのサイズを変更します。
- kubeconfig ファイルをダウンロードします。kubectl コマンドライン ツールは、kubeconfig ファイルを使用して、クラスタ、ユーザー、名前空間、および認証メカニズムに関する情報を取得します。
- Kubernetes クラスタを削除します。

プロバイダ仮想データセンターでの仮想マシン ストレージ ポリシーの管理

プロバイダ仮想データセンター (VDC) から仮想マシン ストレージ ポリシーの追加、有効化、無効化、および削除ができます。プロバイダ仮想データセンター上の仮想マシン ストレージ ポリシーのメタデータを追加、編集、または削除することもできます。

VMware Cloud Director 10.2.2 以降では、ストレージ ポリシーで許可されるエンティティを制限できます。[ストレージ ポリシーがサポートするエンティティ タイプの編集](#) を参照してください。

プロバイダ仮想データセンターのストレージ ポリシーでの仮想マシン暗号化の有効化

暗号化が有効なストレージ ポリシーをプロバイダ VDC に追加できます。仮想マシンおよびディスクを暗号化するには、仮想マシンの暗号化機能を備えたストレージ ポリシーに関連付けます。

VMware Cloud Director 10.1 以降では、仮想マシンの暗号化を使用してデータのセキュリティを強化できます。暗号化により、仮想マシンだけでなく仮想マシンのディスクやファイルも保護することができます。API およびユーザー インターフェイスで、ストレージ ポリシーの機能や、仮想マシンとディスクの暗号化ステータスを表示できます。それぞれの vCenter Server バージョンでサポートされている暗号化された仮想マシンとディスクには、すべての操作を実行できます。

仮想マシンの暗号化の有効化

VMware Cloud Director で仮想マシンを暗号化するには、vCenter Server インスタンスに 1 つ以上のキー管理サーバ (KMS) を設定し、仮想マシンとディスクに仮想マシン暗号化機能を備えたストレージ ポリシーを関連付ける必要があります。

- 1 vCenter Server に KMS クラスタを追加します。vCenter Server インスタンスに複数の KMS クラスタを含めることができます。キー管理サーバ クラスタの設定の詳細については、『vSphere のセキュリティ』ガイドの [キー管理サーバ クラスタの設定](#) を参照してください。
- 2 vCenter Server で、ストレージ ポリシーの暗号化を有効にします。『vSphere のセキュリティ』ガイドの [暗号化ストレージ ポリシーの作成](#) トピックを参照してください。
- 3 VMware Cloud Director Service Provider Admin Portal で、暗号化が有効なポリシーをプロバイダ VDC に追加します。『[プロバイダ仮想データセンターへの仮想マシン ストレージ ポリシーの追加](#)』を参照してください。
- 4 VMware Cloud Director Service Provider Admin Portal で、暗号化が有効なポリシーを組織 VDC に追加します。『[組織仮想データセンターへの仮想マシン ストレージ ポリシーの追加](#)』を参照してください。
- 5 テナントは VMware Cloud Director Tenant Portal で、仮想マシンまたはディスクに仮想マシンの暗号化が有効なストレージ ポリシーを関連付けることができます。
- 6 仮想マシンまたはディスクを復号するには、仮想マシンまたはディスクに暗号化が有効になっていないストレージ ポリシーをテナントが関連付けます。

仮想マシンの暗号化に関する制限事項

VMware Cloud Director では、次のアクションはサポートされていません。

- パワーオン状態の仮想マシンまたはそのディスクを暗号化または復号化します。
- 暗号化された仮想マシンの OVF をエクスポートします。
- 仮想マシンのディスクがスナップショットに含まれている場合に、このスナップショットを使用してディスクを暗号化および復号します。
- 仮想マシンのディスクが暗号化されたポリシーに含まれている場合に、仮想マシンを復号します。
- 暗号化されたディスクを暗号化されていない仮想マシンに追加します。
- 暗号化されていない仮想マシン上の既存のディスクを暗号化します。
- 暗号化された名前付きディスクを暗号化されていない仮想マシンに追加します。
- 暗号化されたリンク クローンを作成します。
- リンク クローン仮想マシンまたはそのディスクを暗号化します。
- ソース仮想マシンが暗号化されている場合に、vCenter Server インスタンス間で仮想マシンのインスタンス化、移動、またはクローン作成を行います。

注： 高速プロビジョニング済みの組織 VDC でソースまたはターゲット仮想マシンが暗号化されている場合に、クローンを作成すると、VMware Cloud Director は常にフル クローンを作成します。

仮想マシンの暗号化ストレージ機能の識別

システム管理者と組織管理者には、デフォルトで、組織 VDC のストレージ機能を表示し、仮想マシンとディスクが暗号化されているかどうかを参照するために必要な権限が設定されています。vApp 作成者は、仮想マシンとディスクの暗号化ステータスを参照できます。ロールおよび権限の詳細については、[事前定義ロールとその権限](#)を参照してください。

すべてのストレージ機能は、[リソース] - [vSphere リソース] - [ストレージ ポリシー] の [機能] 列で確認できます。この列には、仮想マシンの暗号化、タグベースの関連付け、vSAN、IOPS 制限ストレージ機能が表示されます。ストレージ機能の完全なリストを表示するには、ストレージ ポリシー名の左側にある矢印をクリックして行を展開します。

プロバイダ VDC の [ストレージ ポリシー] タブで、ストレージ機能の情報を表示することもできます。

プロバイダ仮想データセンターへの仮想マシン ストレージ ポリシーの追加

仮想マシン ストレージ ポリシーをプロバイダ仮想データセンターに追加できます。その後、こ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る組織仮想データセンターを構成して、追加されたストレージ ポリシーをサポートすることができます。

前提条件

- vSphere 管理者によって、ターゲット仮想マシン ストレージ ポリシーが作成されていること。ストレージ ポリシー ベース管理 (SPBM) の詳細については、『vSphere ストレージ』ドキュメントを参照してください。
- [vCenter Server インスタンスのストレージ ポリシーの更新](#)。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [プロバイダ VDC] を選択し、ターゲット プロバイダ仮想データセンターの名前をクリックします。
- 3 [ポリシー] で [ストレージ] を選択し、[追加] をクリックします。
- 4 追加する 1 個以上のストレージ ポリシーを選択し、[追加] をクリックします。

[* (任意)] を選択すると、VMware Cloud Director は、データストアがプロバイダ仮想データセンターのデータストア クラスタに追加されるか、またはクラスタから削除されるときに、動的にそれらを追加および削除します。

次のステップ

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組織仮想データセンターを構成し、ストレージ ポリシーをサポートします。[組織仮想データセンターへの仮想マシン ストレージ ポリシーの追加](#)を参照してください。

プロバイダ仮想データセンター上の仮想マシン ストレージ ポリシーの有効化または無効化

プロバイダ仮想データセンターで仮想マシン ストレージ ポリシーを無効にすると、この組織仮想データセンターは、この仮想マシン ストレージ ポリシーを使用できなくなります。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [プロバイダ VDC] を選択し、ターゲット プロバイダ仮想データセンターの名前をクリックします。
- 3 [ポリシー] で [ストレージ] を選択します。
- 4 ターゲット仮想マシン ストレージ ポリシーの横にあるラジオ ボタンをクリックして、[有効化] または [無効化] をクリックします。
- 5 確認するには、[OK] をクリックします。

プロバイダ仮想データセンターからの仮想マシン ストレージ ポリシーの削除

プロバイダ仮想データセンターから仮想マシン ストレージ ポリシーを削除できます。

前提条件

ターゲット仮想マシン ストレージ ポリシーを無効にします。 [プロバイダ仮想データセンター上の仮想マシン ストレージ ポリシーの有効化または無効化](#)を参照してください。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [プロバイダ VDC] を選択し、ターゲット プロバイダ仮想データセンターの名前をクリックします。
- 3 [ポリシー] で [ストレージ] を選択します。
- 4 ターゲット仮想マシン ストレージ ポリシーの横にあるラジオ ボタンをクリックして、[削除] をクリックします。
- 5 確認するには、[削除] をクリックします。

プロバイダ仮想データセンター上の仮想マシン ストレージ ポリシーのメタデータの変更

プロバイダ仮想データセンター上のストレージ ポリシーのメタデータを追加、編集、または削除できます。

オブジェクト メタデータを使用すると、プロバイダ仮想データセンター上でユーザー定義の `name=value` ペアとストレージ ポリシーを関連付けることができます。vCloud API クエリのフィルタ式内でオブジェクト メタデータを使用できます。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [プロバイダ VDC] を選択し、ターゲット プロバイダ仮想データセンターの名前をクリックします。
- 3 [ポリシー] で [ストレージ] を選択します。

- 4 ターゲット仮想マシン ストレージ ポリシーの横にあるラジオ ボタンをクリックして、[メタデータ] をクリックします。
- 5 [[編集]]をクリックします。
- 6 (オプション) キーと値のペアを追加するには、[追加] をクリックして、名前と値を入力し、新しいキーと値のペアのタイプを選択します。
- 7 (オプション) キーと値のペアを編集するには、新しい名前と値を入力し、キーと値のペアに新しいタイプを選択します。
- 8 (オプション) キーと値のペアを削除するには、行の右端にある [削除] アイコンをクリックします。
- 9 [保存] をクリックし、[OK] をクリックします。

1 秒あたりの I/O 処理数の設定の有効化

テナントがディスクごとの IOPS の上限を設定できるように、ストレージ ポリシーの 1 秒あたりの I/O 処理数 (IOPS) の設定を有効にできます。

物理ストレージ デバイスおよび仮想ディスクで管理される読み取りと書き込みのパフォーマンスは IOPS と呼ばれる単位を使用して定義されます。この単位は 1 秒あたりの読み書き操作の回数を表します。I/O パフォーマンスを制限するには、IOPS 割り当てが有効なストレージ デバイスを含むプロバイダ VDC ストレージ ポリシーは、組織 VDC ストレージ ポリシーをバックアップしている必要があります。その後、テナントは、指定されたレベルの I/O パフォーマンスを要求するように、IOPS を使用するディスクを構成できます。IOPS をサポートするように構成されたストレージ プロファイルは、IOPS を使用するすべてのディスクにデフォルトの IOPS 値を提供します。これには、特定の IOPS 値を要求するように構成されていないディスクも含まれます。特定の IOPS 値を要求するように構成されたハード ディスクでは、要求されている値よりも最大 IOPS 値のほうが低いストレージ ポリシー、または IOPS をサポートするように構成されていないストレージ ポリシーを使用できません。

注： 仮想マシンに表示される実際の I/O スループットは、ブロック サイズと IOPS の組み合わせです。仮想マシンで異なるブロック サイズが使用されている場合、IOPS が同じ数に制限されていても、スループットは異なります。ストレージ I/O リソースの管理の詳細については、『vSphere のリソース管理ガイド』を参照してください。

VMware Cloud Director IOPS ストレージ ポリシー

このオプションで編集できるデフォルトの IOPS 設定があります。ディスクあたりの IOPS またはストレージ ポリシーあたりの IOPS に制限を設定できます。ディスク サイズ (GB) に基づいてディスクあたりの IOPS 制限を設定することにより、ディスク サイズの増大に伴い、許可する IOPS を大きくすることができます。テナントは、これらの制限内でディスクにカスタム IOPS を設定できます。配置するときに IOPS のキャパシティを考慮するかどうかに関係なく、IOPS の制限を使用できます。

Storage DRS クラスタによってバックアップされているストレージ ポリシーで IOPS を有効にすることはできません。

- 1 ディスクをデータストアに配置するときに VMware Cloud Director が IOPS を考慮するように設定するには、vCenter Server で、変更するストレージ ポリシーに関連付けられているすべてのデータストアに IOPS キャパシティを追加します。

- 2 ディスクをデータストアに配置するときに VMware Cloud Director が IOPS を考慮するように設定するには、vCenter Server で、IOPS キャパシティが追加されたデータストアを使用するストレージ ポリシーを作成します。
- 3 VMware Cloud Director Service Provider Admin Portal または VMware Cloud Director API を使用して、1 つ以上のプロバイダ VDC にストレージ ポリシーを追加します。
- 4 Service Provider Admin Portal または VMware Cloud Director API を使用して、1 つ以上の組織 VDC にストレージ ポリシーを公開します。ストレージ ポリシーを公開した組織 VDC は、ポリシーの IOPS 設定を継承します。
- 5 継承されたストレージポリシーの IOPS 設定を編集する場合は、Service Provider Admin Portal または VMware Cloud Director API を使用して組織 VDC ストレージ ポリシーを更新します。

このポリシー タイプは、ストレージ ポリシーの VCD/IOPS 機能として表示されます。

vCenter Server IOPS ストレージ ポリシー

このオプションを使用すると、このポリシーを使用するすべてのディスクに 1 つの IOPS が設定されます。

VMware Cloud Director でこの設定を編集することはできません。テナントは、これらのポリシーを使用してディスクにカスタム IOPS を設定することはできません。このオプションでは、ディスクのサイズやデータストア間のロード バランシングに応じて IOPS をスケーリングすることはありません。

- 1 vCenter Server で、カスタムの予約、制限、および共有を使用して、VC-IOPS 対応のストレージ ポリシーを作成します。
- 2 vCenter Server または VMware Cloud Director Service Provider Admin Portal で、ディスクをストレージ ポリシーに割り当てます。

このポリシー タイプは、ストレージ ポリシーの vSphere/IOPS 機能として表示されます。ソースまたはターゲット仮想マシンに vSphere/IOPS 機能がある場合は、高速プロビジョニングされた仮想マシンを作成できません。

vCenter Server のディスクに関する IOPS の設定

vCenter Server で IOPS 設定を変更するには、ディスクの IOPS を手動で更新します。VMware Cloud Director でこれらの IOPS 設定を編集することはできません。

既存のストレージ ポリシーでの IOPS 制限の有効化

注： vSphere/IOPS 機能がすでに設定されているポリシーで、VMware Cloud Director IOPS の制限を有効にすることはできません。

- VCD/IOPS ストレージ ポリシーで IOPS 制限を有効にします。
 - a ディスクをデータストアに配置するときに VMware Cloud Director が IOPS キャパシティを考慮するように設定するには、vCenter Server で、変更するストレージ ポリシーに関連付けられているすべてのデータストアに IOPS キャパシティを追加します。
 - b ディスクをデータストアに配置するときに VMware Cloud Director が IOPS キャパシティを考慮するように設定するには、VMware Cloud Director Service Provider Admin Portal または VMware Cloud Director API を使用して、対応するプロバイダ VDC ストレージ ポリシーから IOPS キャパシティがゼロでないと報告されることを確認します。

- c VMware Cloud Director Service Provider Admin Portal または VMware Cloud Director API を使用して、VCD/IOPS 機能を有効にし、最大 IOPS 値、デフォルト IOPS 値などを設定するように、組織 VDC ストレージ ポリシーを更新します。

- vCenter Server の vSphere/IOPS ストレージ ポリシーで IOPS 制限を有効にします。

組織 VDC ストレージ ポリシーの IOPS 制限を有効にすると、テナントは VMware Cloud Director Tenant Portal を使用して、ディスクごとの IOPS 制限を設定できます。

プロバイダ VDC ストレージ ポリシーの設定の編集

プロバイダ VDC ストレージ ポリシーの 1 秒あたりの I/O 処理数 (IOPS) の設定を変更できます。デフォルトでは、ポリシーが公開されている組織 VDC は、プロバイダ VDC ストレージ ポリシーの設定を継承します。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [プロバイダ VDC] を選択し、ターゲット プロバイダ仮想データセンターの名前をクリックします。
- 3 [ポリシー] で [ストレージ] を選択します。
- 4 ターゲット ストレージ ポリシーの横にあるラジオ ボタンをクリックして、[設定の編集] をクリックします。
- 5 1 秒あたりの I/O 処理数を制限する場合は、[IOPS 制限が有効] トグルをオンにします。
- 6 配置中に IOPS が考慮されるようにする場合は、[影響のある配置] トグルをオンにします。

[影響のある配置] トグルがオンになっている場合、VMware Cloud Director はデータストア間で IOPS のロード バランシングを行います。ディスクの IOPS 設定を行うときに、VMware Cloud Director は選択したディスクに必要な IOPS キャパシティを持つデータストアを考慮します。[影響のある配置] トグルがオフになっている場合は、データストアごとに IOPS キャパシティを設定する必要はありません。Storage DRS クラスタを使用することができます。
- 7 最大およびデフォルトの IOPS 設定を行い、[保存] をクリックします。

結果

新しいストレージ ポリシー設定は、このポリシーが公開されるすべての組織 VDC に適用されます。

ストレージ ポリシーがサポートするエンティティ タイプの編集

VMware Cloud Director 10.2.2 以降で、プロバイダ VDC ストレージ ポリシーが特定のタイプの VMware Cloud Director エンティティをサポートしないようにする場合は、ポリシーに関連付けられているエンティティのリストを編集して制限することができます。

プロバイダ VDC ストレージ ポリシーを作成すると、デフォルトでは、使用可能なすべてのエンティティ タイプがサポートされます。デフォルトのエンティティ タイプは次のとおりです。

- 仮想マシン
- 名前付きディスク
- カタログ メディア

- vApp および仮想マシン テンプレート
- Tanzu Kubernetes クラスタ
- Edge ゲートウェイ

ストレージ ポリシーがサポートするエンティティ タイプを、このリスト内の1つ以上のタイプに制限できます。エンティティを作成する場合は、そのタイプをサポートするストレージ ポリシーのみを使用できます。たとえば、カタログを作成する場合は、カタログ メディアと App テンプレート、または両方をサポートするストレージ ポリシーのみが表示されます。エンティティがストレージ ポリシーを使用している場合に、サポート対象のエンティティ タイプのリストからこのエンティティ タイプを削除しても、エンティティはこのストレージ ポリシーを引き続き使用します。ただし、新しいストレージ ポリシーを選択しないかぎり、このポリシーに変更を加えることはできません。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [プロバイダ VDC] を選択し、ターゲット プロバイダ仮想データセンターの名前をクリックします。
- 3 [ポリシー] で [ストレージ] を選択します。
- 4 ターゲット ストレージ ポリシーの横にあるラジオ ボタンをクリックして、[サポートされているタイプの編集] をクリックします。
- 5 [エンティティ タイプのサポート] ドロップダウン メニューで [特定のエンティティの選択] を選択します。
- 6 ストレージ ポリシーでサポートするエンティティを選択して、[保存] をクリックします。

次のステップ

- [組織仮想データセンターへの仮想マシン ストレージ ポリシーの追加](#)
- 「サポートされているストレージ エンティティ タイプ：管理」権限を持つユーザーは、VMware Cloud Director OpenAPI を使用することで、すべてのストレージ ポリシーで使用可能なタイプのリストで、エンティティ タイプの追加/削除ができます。たとえば、リストにランタイム定義エンティティ (RDE) を追加または削除できます。テナントに追加の VMware Cloud Director 機能を提供する拡張機能の作成方法については、[14 章 定義済みエンティティの管理](#)を参照してください。

VMware Cloud Director により、すべてのエンティティをサポートするストレージ ポリシーに変更が自動的に適用されます。1つ以上のストレージ ポリシーで特別に選択されているエンティティは削除できません。

プロバイダ仮想データセンターでのリソース プールの管理

プロバイダ仮想データセンターからセカンダリ リソース プールの追加、有効化、無効化、および分離を実行できます。プロバイダ仮想データセンターでは、プライマリ リソース プールの無効化または分離はできません。

プロバイダ仮想データセンターへのリソース プールの追加

プロバイダ仮想データセンターに1つ以上のセカンダリ リソース プールを追加すると、プロバイダ仮想データセンターの従量課金制および割り当てプールの組織仮想データセンターを拡張できます。

複数のリソース プールでバックアップされているコンピューティング リソースは、より多くの仮想マシンに対応するよう拡張できます。

VLAN アップリンクを持つ NSX Edge をホストするために最適に設定された vSphere クラスタによってバックアップされる、リソース プールを追加できます。VMware Cloud Director では、メタデータを使用して、これらのクラスタによってバックアップされるリソース プールに組織 VDC Edge Gateway をシステム上配置する必要がありますを示すことができます。詳細については、VMware ナレッジベースの記事 (<https://kb.vmware.com/kb/2151398>) を参照してください。

前提条件

vSphere 管理者によって、プロバイダ仮想データセンターのプライマリ リソース プールをバックアップする vCenter Server インスタンスにターゲットのセカンダリ リソース プールが作成されていること。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [プロバイダ VDC] を選択し、ターゲット プロバイダ仮想データセンターの名前をクリックします。
- 3 [リソース プール] タブで [追加] をクリックします。
- 4 追加するリソース プールを選択し、[追加] をクリックします。

vSphere with VMware Tanzu を使用する場合は、スーパーバイザー クラスタを選択します。VMware Cloud Director では、スーパーバイザー クラスタによってバックアップされているリソース プールの横に、Kubernetes アイコンが表示されます。

- 5 スーパーバイザー クラスタによってバックアップされているリソース プールまたはクラスタを選択する場合に、Kubernetes 制御プレーンとの信頼関係を確立するには、Kubernetes 制御プレーン証明書を信頼する必要があります。
- 6 リソース プールを追加する場合は、[手順 1](#) ~ [手順 5](#) を繰り返します。

結果

VMware Cloud Director では、リソース プールをプロバイダ仮想データセンターで使えるよう追加し、そのプロバイダ仮想データセンターでバックアップされる従量課金制と割り当てプールの組織仮想データセンターすべてに柔軟性を持たせます。

VMware Cloud Director は、新しいリソース プールの下に システム VDC リソース プールも追加します。このリソース プールは、NSX Edge 仮想マシンや、リンク クローンのテンプレートとして機能する仮想マシンなどのシステム リソースの作成に使用されます。

重要： システム VDC リソース プールの編集または削除を行わないでください。

プロバイダ仮想データセンター上のリソース プールの有効化または無効化

リソース プールを無効にすると、プロバイダ仮想データセンターがリソース プールのメモリおよびコンピューティング リソースを使用できなくなります。

すでに進行中のプロセスは、無効なリソース プールのリソースの使用を停止しません。

注： プロバイダ仮想データセンターでプライマリ リソース プールを無効にすることはできません。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [プロバイダ VDC] を選択し、ターゲット プロバイダ仮想データセンターの名前をクリックします。
- 3 [リソース プール] タブをクリックします。
- 4 ターゲット リソース プールの横にあるラジオ ボタンをクリックして、[有効化] または [無効化] をクリックします。
- 5 確認するには、[OK] をクリックします。

プロバイダ仮想データセンターからのリソース プールの分離

プロバイダ仮想データセンターに複数のリソース プールがある場合は、プロバイダ仮想データセンターからセカンダリ リソース プールを分離することができます。プロバイダ仮想データセンターからプライマリ リソース プールを分離することはできません。

前提条件

- プロバイダ仮想データセンターのターゲット リソース プールを無効にします。 [プロバイダ仮想データセンター上のリソース プールの有効化または無効化](#)を参照してください。
- 無効化されたリソース プールの影響を受けるネットワークを再デプロイします。
- 無効化されたリソース プールの影響を受ける Edge Gateway を再デプロイします。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [プロバイダ VDC] を選択し、ターゲット プロバイダ仮想データセンターの名前をクリックします。
- 3 [リソース プール] タブをクリックします。
- 4 ターゲット リソース プールの横にあるラジオ ボタンをクリックして、[分離] をクリックします。
- 5 確認するには、[OK] をクリックします。

プロバイダ仮想データセンターのメタデータの変更

プロバイダ仮想データセンターのメタデータを追加、編集、または削除できます。

オブジェクト メタデータを使用すると、ユーザー定義の `name=value` ペアに、プロバイダ仮想データセンターを関連付けることができます。vCloud API クエリのフィルタ式内でオブジェクト メタデータを使用できます。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [プロバイダ VDC] を選択し、ターゲット プロバイダ仮想データセンターの名前をクリックします。
- 3 [設定] - [メタデータ] タブで、右上隅にある [編集] をクリックします。
- 4 (オプション) キーと値のペアを追加するには、[追加] をクリックして、名前と値を入力し、新しいキーと値のペアのタイプを選択します。
- 5 (オプション) キーと値のペアを編集するには、新しい名前と値を入力し、キーと値のペアに新しいタイプを選択します。
- 6 (オプション) キーと値のペアを削除するには、行の右端にある [削除] アイコンをクリックします。
- 7 [保存] をクリックし、[OK] をクリックします。

組織の管理

5

VMware Cloud Director Service Provider Admin Portal では、VMware Cloud Director 組織を作成、設定、および管理することができます。

VMware Cloud Director Service Provider Admin Portal を使用して、組織の管理、組織に割り当てられたリソースのユーザーによる使用方法を決定するポリシーの設定、およびカタログの公開と共有組織の管理を実行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。

- リースについて
- 組織の作成
- 組織の有効化または無効化
- 組織の削除
- 組織のカタログの設定
- 組織のポリシーの設定
- テナント ストレージの移行
- 組織のリソース使用に対する割り当て容量の管理

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 はリソースを消費し続けます。

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、VMware Cloud 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、VMware Cloud 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。

組織の作成

VMware Cloud Director Service Provider Admin Portal から新しい組織を作成できます。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。

- a 左側のパネルで [組織] を選択します。

既存の組織のリストがグリッド ビューで表示されます。

- 2 [新規] をクリックします。

[新しい組織] ダイアログが開きます。

- 3 以下の値を入力します。

オプション	説明
組織名	組織のテナント ポータルへのアクセス用 URL を形成する一意の識別子。
組織の完全な名前	組織の完全な名前。
説明	オプションの組織の説明。

- 4 [作成] ボタンをクリックして、作成を完了します。

組織の有効化または無効化

組織を無効にすると、ユーザーは組織にログインできなくなり、現在ログイン中のユーザーのセッションも終了されます。組織内で実行されている vApp は引き続き実行されます。

システム管理者は、組織が無効にされていても、リソースの割り当て、ネットワークの追加などを行うことができます。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。

- a 左側のパネルで [組織] を選択します。

既存の組織のリストがグリッド ビューで表示されます。

- 2 組織の名前の横にあるラジオ ボタンをクリックして、[有効化] または [無効化] をクリックします。

組織の削除

組織を削除して、VMware Cloud Director から完全に削除します。

前提条件

組織を削除するには、組織を無効にし、組織内のすべての組織仮想データセンター、テンプレート、メディア ファイル、および vApp を削除する必要があります。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
 - a 左側のパネルで [組織] を選択します。

既存の組織のリストがグリッド ビューで表示されます。
- 2 組織の名前の横にあるラジオ ボタンをクリックし、[削除] をクリックします。
- 3 確定するには、[はい] をクリックします。

組織のカatalogの設定

組織がサービス カatalogを共有する方法を設定できます。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
 - a 左側のパネルで [組織] を選択します。

既存の組織のリストがグリッド ビューで表示されます。
- 2 組織を選択し、[構成] タブで [カatalog] を選択します。
- 3 共有および公開の設定を変更するには、[編集] をクリックします。

オプション	説明
共有	組織管理者がこの組織のカatalogを、VMware Cloud Director のこのインスタンス内の他の組織と共有することを許可します。このオプションを選択しなくても、組織管理者が組織内でカatalogを共有することはできます。
外部カatalogへの公開を許可	組織管理者が VMware Cloud Director のこのインスタンスの外部の組織にカatalogを公開することを許可します。
外部カatalogのサブスクライブを許可	組織管理者が VMware Cloud Director のこのインスタンスの外部のカatalogをサブスクライブすることを許可します。

組織のポリシーの設定

リース、割り当て容量、および制限によって、組織のユーザーがストレージおよび処理のリソースを使用する能力が制限されます。これらの設定を変更して、ユーザーが組織のリソースを使い果たしたり、独占したりするのを防ぎます。

前提条件

[リースについて](#)を参照してください。

手順

- 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
 - 左側のパネルで [組織] を選択します。
既存の組織のリストがグリッド ビューで表示されます。
- 組織を選択し、[ポリシー] タブを選択します。
- 組織のリース、割り当て容量、リソース制限、およびパスワード ポリシーを編集するには、[編集] をクリックします。
- 次の内容で、vApp のリースを設定します。

オプション	説明
最大ランタイム リース	vApp を実行できる期間。この期間を過ぎると、自動的に停止されます。
ランタイムの有効期限アクション	期限切れの実行中の vApp の処理方法。 vApp をサスペンドすると、その仮想マシンがすべてサスペンドされ、メモリがディスクに書き込まれて現在の状態が保持されます。[パワーオフ] により、そのすべての仮想マシンおよび子 vApp がただちに停止します。
最大ストレージ リース	停止した vApp を使用できる期間。この期間を過ぎると、自動的にクリーンアップされます。
ストレージ クリーンアップ	vApp を停止してクリーンアップした後の処理方法。

- 次の内容で、vApp テンプレートのリースを設定します。

オプション	説明
最大ストレージ リース	vApp テンプレートを使用できる期間。この期間を過ぎると、自動的にクリーンアップされます。
ストレージ クリーンアップ	期限切れの vApp テンプレートをクリーンアップした後の処理方法。

- 次の内容で、割り当て容量を設定します。

オプション	説明
すべての仮想マシンの割り当て容量	この組織内でユーザーが保存できる使用可能な仮想マシンの合計数。
実行中の仮想マシンの割り当て容量	この組織内でユーザーがパワーオンできる仮想マシンの合計数。

- 次の内容で、制限を設定します。

オプション	説明
ユーザーごとのリソースを大量に消費する操作数	ユーザー 1 人あたりのリソースを大量に使用する操作の最大数を入力するか、[システム制限の継承] を選択します。
ユーザーごとのキューに入れられるリソースを大量に消費する操作数	ユーザー 1 人あたりのリソースを大量に使用するキュー登録対象操作の最大数を入力するか、[システム制限の継承] を選択します。
組織ごとのリソースを大量に消費する操作数	組織あたりのリソースを大量に使用する同時操作の最大数を入力するか、[システム制限の継承] を選択します。

オプション	説明
組織ごとのキューに入れられるリソースを大量に消費する操作数	組織あたりのリソースを大量に使用するキュー登録対象操作の最大数を入力するか、[システム制限の継承] を選択します。
仮想マシンごとの同時接続数	仮想マシンあたりの同時コンソール接続の最大数を入力するか、[システム制限の継承] を選択します。
組織ごとの仮想データセンターの数	組織あたりの仮想データセンターの最大数を入力するか、[システム割り当て容量の継承] を選択します。

8 次の内容で、パスワード ポリシーを設定します。

オプション	説明
アカウント ロックアウトが有効	無効なログインを複数回試行したユーザーのアカウントをロックアウトできます。
ロックアウトまでの無効なログイン回数	ユーザー 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。
アカウント ロックアウト間隔	ロックされたユーザー アカウントがログインできない期間。

テナント ストレージの移行

1 つ以上の組織に含まれるすべての vApp、独立したディスク、およびカタログ項目を、1 つ以上のデータストアから別のデータストアに移行できます。

データストアを廃止する前に、このデータストアに格納されているすべてのアイテムを新しいデータストアに移行する必要があります。ストレージ容量の大きい新しいデータストアや、VMware vSAN などの最新のストレージ技術を使用する新しいデータストアに組織を移行することもできます。

重要： テナントのストレージ移行は、リソースを大量に消費する処理であり、特に多数の資産を移行する場合は、長時間にわたって実行される可能性があります。テナント ストレージの移行の詳細については、<https://kb.vmware.com/kb/2151086> を参照してください。

前提条件

- ターゲット組織の組織 VDC で使用されているストレージ ポリシーを判別します。[組織仮想データセンターへの仮想マシン ストレージ ポリシーの追加](#)を参照してください。
- 移行するソース データストアが含まれているストレージ ポリシーごとに、移行先のターゲット データストアが 1 つ以上あることを確認します。ターゲット データストアを作成するか、既存のデータストアを使用することができます。ターゲット組織で使用されるストレージ ポリシーのデータストアを決定することの詳細については、『vSphere ストレージ』のドキュメントを参照してください。

手順

- 1 VMware Cloud Director Service Provider Admin Portal に システム管理者としてログインするか、組織: テナント ストレージの移行 権限を持つロールを使用してログインします。
- 2 [テナント ストレージの移行] ウィザードを開始します。
 - [クラウド リソース] で [組織] を選択し、[テナント ストレージの移行] をクリックします。
 - [vSphere リソース] で [データストア] を選択し、[テナント ストレージの移行] をクリックします。

- 3 移行するストレージ アイテムがある 1 つ以上の組織を選択し、[次へ] をクリックします。
- 4 移行するソース データストアを 1 つ以上選択し、[次へ] をクリックします。
ウィザードには、システム内のすべてのデータストアが一覧表示されます。
- 5 1 つ以上のターゲット データストアを選択し、[次へ] をクリックします。
- 6 [設定内容の確認] 画面を確認し、[完了] をクリックして移行を開始します。

組織のリソース使用に対する割り当て容量の管理

組織全体のリソース使用量の制限を管理できます。仮想マシン、Tanzu Kubernetes クラスタ、CPU、メモリ、またはストレージに対する組織の割り当て容量を追加、編集、削除できます。

ユーザーまたはグループが使用できるリソースの制限については、[ユーザーのリソース割り当ての管理](#)または[グループのリソース割り当ての管理](#)を参照してください。

前提条件

組織の作成

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [組織] を選択します。
- 3 割り当て容量に設定する組織の名前を選択します。
- 4 [構成] セクションで [割り当て容量] を選択します。
デフォルトでは、組織に割り当て容量は設定されていません。
- 5 [[編集]] をクリックします。
- 6 選択した組織の割り当て容量を変更します。

Tanzu Kubernetes クラスタの数、組織内のすべての仮想マシンまたは実行中の仮想マシンの数、使用された CPU、メモリ、およびストレージに関する割り当て容量を追加、編集、または削除できます。選択したタイプのリソースを無制限に組織に割り当てる場合は、[制限なし] を選択します。

- 7 [保存] をクリックします。

組織仮想データセンターの管理

6

組織にリソースを提供するには、この組織用の組織仮想データセンター (VDC) を 1 つ以上作成します。組織 VDC の作成後、組織 VDC のプロパティの変更、組織 VDC 自体の無効化/削除、組織 VDC の割り当てモデル、ストレージ、ネットワーク設定の管理を実行できます。

この章には、次のトピックが含まれています。

- [割り当てモデルについて](#)
- [仮想マシン サイズ変更ポリシーと仮想マシン配置ポリシーについて](#)
- [VMware Cloud Director での Kubernetes の使用](#)
- [組織仮想データセンターの作成](#)
- [組織仮想データセンターの有効化または無効化](#)
- [組織仮想データセンターの削除](#)
- [仮想データセンター テンプレートの管理](#)
- [組織仮想データセンターの名前および説明の変更](#)
- [組織仮想データセンターの割り当てモデルの設定の変更](#)
- [組織仮想データセンターのストレージ設定の変更](#)
- [組織仮想データセンターのネットワーク設定の編集](#)
- [クロス仮想データセンター ネットワークの構成](#)
- [組織仮想データセンターのメタデータの変更](#)
- [組織仮想データセンターのリソース プールの表示](#)
- [組織仮想データセンターの分散ファイアウォールの管理](#)

割り当てモデルについて

割り当てモデルは、割り当てられたプロバイダ仮想データセンター (VDC) のコンピューティング リソースとメモリ リソースが組織 VDC にコミットされる方法とタイミングを決定します。

次の表に、組織 VDC の割り当てモデルに基づいて、仮想マシン (VM) レベルまたはリソース プール レベルでの vSphere リソース展開の設定を示します。

	Flex 割り当てモデル	柔軟性のある割り当て プール モデル	柔軟性のない割り 当てプール モデル	従量課金制モデル	予約プール モデル
柔軟性	組織 VDC の設定に基づきます。	はい	いいえ	はい	いいえ
vCPU 速度	仮想マシンの CPU 制限が仮想マシン サイズ変更ポリシーで定義されていない場合、vCPU 速度が VDC 内の仮想マシンの CPU 制限に影響することがあります。	組織 VDC 内で実行中の vCPU の数に影響します。	該当なし	仮想マシンの CPU 制限に影響する	該当なし
リソース プールの CPU 制限	組織 VDC の CPU 制限は、リソース プール内の仮想マシンの数に基づいて分配されます。	組織 VDC の CPU 割り当て	組織 VDC の CPU 割り当て	制限なし	組織 VDC の CPU 割り当て
リソース プールの CPU 予約	組織 VDC の CPU 予約は、リソース プール内の vCPU の数に基づいて分配されます。組織 VDC の CPU 予約は、組織 VDC の CPU 割り当てに CPU 保証率を掛けた値に等しくなります。	パワーオン状態の仮想マシン数の合計は、CPU 保証率に vCPU 速度および vCPU の数を掛けた値に等しくなります。	組織 VDC CPU の割り当てに CPU 保証率を掛けた値	なし、拡張可能	組織 VDC の CPU 割り当て
リソース プールのメモリ制限	組織 VDC のメモリ制限は、リソース プール内の仮想マシンの数に基づいて分配されます。	制限なし	組織 VDC の RAM 割り当て	制限なし	組織 VDC の RAM 割り当て
リソース プールのメモリ予約	組織 VDC の RAM 予約は、リソース プール内の仮想マシンの数に基づいて分配されます。組織 VDC の RAM 予約は、組織 VDC の RAM 割り当てに RAM 保証率を掛けた値に等しくなります。	RAM 保証率にリソース プール内のパワーオン状態のすべての仮想マシンの vRAM を掛けた値の合計リソース プールの RAM 予約は拡張可能です。	組織 VDC の RAM 割り当てに RAM 保証率を掛けた値	なし、拡張可能	組織 VDC の RAM 割り当て
仮想マシンの CPU 制限	仮想マシンの仮想マシン サイズ変更ポリシーに基づきます。	制限なし	制限なし	vCPU の速度に vCPU の数を掛けた値	カスタム
仮想マシンの CPU 予約	仮想マシンの仮想マシン サイズ変更ポリシーに基づきます。	0	0	CPU 速度に vCPU の速度、および vCPU の数を掛けた値に等しくなります。	カスタム
仮想マシンの RAM 制限	仮想マシンの仮想マシン サイズ変更ポリシーに基づきます。	制限なし	制限なし	vRAM	カスタム
仮想マシンの RAM 予約	仮想マシンの仮想マシン サイズ変更ポリシーに基づきます。	0	vRAM に、RAM の保証率および RAM のオーバーヘッドを掛けた値に等しくなります。	vRAM に、RAM の保証率および RAM のオーバーヘッドを掛けた値に等しくなります。	カスタム

レガシーの VDC 割り当てモデルから Flex 割り当てモデルへの変換

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を、柔軟性のある割り当てプール モデル、柔軟性のない割り当てプール モデル、従量課金モデル、または予約プール モデルの VDC に追加します。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が既存の VDC の割り当てモデルと互換性がない場合は、VDC を Flex 組織 VDC に変換するかどうかを決定できます。

仮想マシン ポリシーのコンプライアンス

レガシー VDC 変換によって仮想マシンがコンプライアンス非準拠になることはありません。管理者が仮想マシンのコンピューティング値または仮想マシン グループ メンバーシップを vCenter Server インスタンスで直接変更すると、割り当てられた仮想マシン サイズ変更ポリシーまたは仮想マシン配置ポリシーに対し、仮想マシンがコンプライアンスに準拠しない状態になる可能性があります。必要な権限を持つユーザーが vCloud API を使用して仮想マシンの予約および制限の値を変更した場合も、仮想マシンがコンプライアンスに準拠しない状態になる可能性があります。コンプライアンスに準拠しない仮想マシンがある場合は、VMware Cloud Director Tenant Portal のユーザー インターフェイスに警告メッセージが表示されます。テナントは、コンプライアンス非準拠の原因に関する詳細情報を確認して、仮想マシンを準拠状態に戻すことができます。これにより、仮想マシンにポリシーが再適用されます。

推奨される割り当てモデルの使用法

各割り当てモデルは、さまざまなレベルのパフォーマンス制御および管理に使用できます。

次の表に、各割り当てモデルの推奨される使用法についての情報を示します。

割り当てモデル	推奨される使用法
Flex 割り当てモデル	Flex 割り当てモデルを使用すると、ワークロード レベルでパフォーマンスを詳細に制御できます。VMware Cloud Director システム管理者は Flex 割り当てモデルを使用して、個々の組織仮想データセンター (VDC) の柔軟性を管理できます。Flex 割り当てモデルでは、ポリシーベースのワークロード管理が使用されます。Flex 割り当てモデルが有効な場合、クラウド プロバイダは組織 VDC のメモリのオーバーヘッドを詳細に制御し、テナントに厳密なバースト容量の使用を適用することができます。
割り当てプール割り当てモデル	割り当てプール割り当てモデルは、長期にわたる、安定したワークロードに対して使用します。このモデルでは、テナントがサブスクリブしたコンピューティング リソースの使用量が固定されるため、クラウド プロバイダはコンピューティング リソースのキャパシティを予測して管理することができます。割り当てプール割り当てモデルは、さまざまなパフォーマンス要件を持つワークロードに最適です。割り当てプール割り当てモデルでは、すべてのワークロードで vCenter Server のリソース プール内の割り当て済みリソースが共有されます。柔軟性の有効/無効にかかわらず、テナントに配分されるコンピューティング リソースは制限されます。割り当てプール割り当てモデルでは、クラウド プロバイダはシステム レベルで柔軟性を有効または無効にして、設定をすべての割り当てプール組織 VDC に適用します。柔軟性のない割り当てプール割り当てを使用している場合、組織 VDC は VDC リソース プールを事前に予約します。テナントは vCPU をオーバーコミットできませんが、メモリをオーバーコミットすることはできません。柔軟性のあるプール割り当てを使用している場合、組織 VDC はコンピューティング リソースを事前に予約しないため、キャパシティが複数のクラスタに分散することがあります。クラウド プロバイダは物理コンピューティング リソースのオーバーコミットメントを管理しますが、テナントは vCPU とメモリをオーバーコミットできません。

割り当てモデル	推奨される使用法
従量課金制	vCenter Server にコンピューティング リソースを事前に割り当てる必要がない場合は、従量課金制モデルを使用します。予約、制限、およびシェアは、テナントが VDC にデプロイしたすべてのワークロードに適用されます。従量課金制の割り当てモデルでは、組織 VDC 内のすべてのワークロードに、設定済みのコンピューティング リソースが同じ割合で予約されます。VMware Cloud Director では、すべてのワークロードで vCPU の CPU 速度は同じと見なされるため、ユーザーは組織 VDC レベルでの CPU 速度のみを定義します。パフォーマンスの観点から、個々のワークロードの予約設定を変更することはできないため、すべてのワークロードに同じ設定が適用されます。従量課金制の割り当てモデルは、同じ組織 VDC 内で実行するためのパフォーマンス要件が異なる複数のワークロードを実行する必要があるテナントに最適です。従量課金制モデルには柔軟性があるため、自動スケール アプリケーションの一部である短時間の汎用ワークロードに適しています。従量課金制では、テナントは組織 VDC 内のコンピューティング リソースに対する需要の急増に対応することができます。
予約プール	組織 VDC で実行されているワークロードのパフォーマンスをきめ細かく制御する必要がある場合は、予約プール割り当てモデルを使用します。クラウド プロバイダの観点からすると、予約プール割り当てモデルでは、vCenter Server のすべてのコンピューティング リソースを事前に割り当てる必要があります。予約プール割り当てモデルには柔軟性がありません。予約プール割り当てモデルは、特定のテナント専用のハードウェアで実行されるワークロードに最適です。このような場合、テナント ユーザーは、コンピューティング リソースの使用とオーバーコミットメントを管理できます。

Flex 割り当てモデル

VMware Cloud Director 9.7 以降では、システム管理者は Flex 割り当てモデルを使用して組織仮想データセンター (VDC) を作成できます。システム管理者は Flex 割り当てと仮想マシン サイジング ポリシーを組み合わせ、VDC レベルと個々の仮想マシン (VM) レベルの両方で CPU および RAM の使用量を制御できます。Flex 割り当てモデルは、既存の割り当てモデルで使用可能なすべての割り当て設定をサポートします。

VMware Cloud Director 10.0 以降では、Flex 以外の組織 VDC をすべて Flex VDC に変換できます。

Flex 組織 VDC を作成する場合、システム管理者は組織 VDC の次のパラメータを制御します。

パラメータ	説明
Elasticity	柔軟性のあるプール機能を有効または無効にします。
Include VM Memory Overhead	この VDC でメモリのオーバーヘッドを追加または除外します。true に設定すると、すべてのパワーオン状態の仮想マシンのメモリのオーバーヘッドも VDC の使用可能な容量から取得されるため、VDC のすべての容量を使用できなくなる可能性があります。false に設定すると、メモリのオーバーヘッドは、VDC の割り当て済み容量からではなく、プロバイダ VDC から取得されます。
CPU allocation	この VDC に割り当てられている CPU の量 (MHz または GHz)。CPU 割り当てによって VDC の CPU キャパシティが定義されます。VDC で実行されるすべての仮想マシンが使用する CPU の合計が、この値を超えないようにする必要があります。
CPU limit	CPU 制限によって VDC の CPU クォータが定義されます。ほとんどの場合、CPU 制限は VDC の割り当て済み CPU キャパシティと同じです。 従量課金制モデルなどの場合は、VDC に CPU を割り当てることが許可されないこともあります。その場合は、CPU 割り当てをゼロに設定し、CPU 制限をゼロ以外の値に設定することにより、全体的な CPU 使用量に対する割り当てを設定する必要があります。 この設定を使用して、無制限の CPU 割り当てを許可することもできます。無制限に設定すると、vCenter Server の VDC のバックアップ リソース プールに CPU が無制限に与えられます。
CPU resources guaranteed	VDC 用に物理的に予約されている CPU 割り当ての割合。
vCPU speed	VDC 内の仮想マシンのデフォルト vCPU 速度。

パラメータ	説明
Memory allocation	この VDC に割り当てられているメモリの容量 (MB または GB)。このパラメータにより、VDC の合計メモリ容量が定義されます。VDC で実行されるすべての仮想マシンに割り当てられる合計メモリが、この値を超えないようにする必要があります。
Memory resources guaranteed	VDC 用に物理的に予約されているメモリ割り当ての割合。
Maximum number of VMs	VDC 内の仮想マシンの最大数。

VMware Cloud Director システム管理者は、Flex 組織 VDC の柔軟性の有効/無効を設定できます。Flex 組織仮想データセンターで柔軟性のあるプール機能が有効になっていると、組織仮想データセンターは、そのプロバイダ仮想データセンターに関連付けられているすべてのリソース プールにわたり、それらを使用します。VMware Cloud Director 9.7 で柔軟性のない組織 VDC を柔軟性のある組織 VDC に変換した場合、同じ組織 VDC を柔軟性なしに変換し直すことはできません。

Flex 割り当てモデルは、他の割り当てモデルのような制約を受けずに、仮想マシン サイジング ポリシーの機能をサポートします。Flex 割り当てモデルでは、仮想マシン コンピューティング リソースの割り当ては仮想マシン サイジング ポリシーによって決まります。組織 VDC の仮想マシン サイジング ポリシーを定義しない場合、コンピューティング リソースの割り当ては組織 VDC の割り当てモデルによって決まります。Flex 割り当てモデルと組織仮想マシン サイジング ポリシーの組み合わせを使用すると、単一の組織 VDC で、他のすべての割り当てモデルに共通の設定を使用する仮想マシンに対応することができます。詳細については、[仮想マシン サイズ変更ポリシーと仮想マシン配置ポリシー](#)についてを参照してください。

Flex 組織 VDC を作成するには、VMware Cloud Director Service Provider Admin Portal または vCloud API を使用します。vCloud API の詳細については、「VMware Cloud Director API プログラミング ガイド」を参照してください。

割り当てプール割り当てモデル

割り当てプール割り当てモデルを使用すると、プロバイダ仮想データセンター (VDC) から割り当てるリソースの割合が組織仮想データセンターにコミットされます。CPU と メモリの両方に割合を指定できます。この割合は、割合の保証率と呼ばれており、これによってリソースのオーバーコミットが可能となります。

システム管理者は、割り当てプール組織 VDC の柔軟性の有効/無効を設定できます。[弾性] は、すべての割り当てプール組織 VDC に影響するグローバル設定です。『[全般システム設定の変更](#)』を参照してください。

デフォルトでは、割り当てプール組織 VDC で柔軟性のある割り当てプールが有効になります。複数のリソース プールにまたがっている仮想マシンに割り当てプール組織の VDC がある、VMware Cloud Director 5.1 からアップグレードされたシステムでは、柔軟性のある割り当てプールがデフォルトで有効になります。

割り当てプール VDC で柔軟性のある割り当てプール機能が有効になっていると、組織 VDC は、そのプロバイダ VDC に関連付けられているすべてのリソース プールにわたり、それらを使用します。結果として、vCPU の周波数は割り当てプールの必須パラメータとなります。

CPU がボトルネック要素とならずに組織 VDC 上に十分な台数の仮想マシンをデプロイできる方法で、vCPU の周波数と割合の保証率を設定してください。

仮想マシンを作成すると、配置エンジンが、仮想マシンの要件に最適なプロバイダ VDC のリソース プール上に仮想マシンを配置します。プロバイダ VDC のリソース プールの下にこの組織 VDC のサブリソース プールが作成され、そのサブリソース プールの下に仮想マシンが配置されます。

仮想マシンをパワーオンすると、配置エンジンがプロバイダ VDC のリソース プールをチェックし、仮想マシンをパワーオンできることを確認します。十分な容量がない場合、配置エンジンはその仮想マシンを、仮想マシンの実行に十分なリソースを持つプロバイダ VDC のリソース プールに移動します。組織 VDC のサブリソース プールがない場合には、作成されます。

新規仮想マシンの実行に十分なリソースを持つよう、サブリソース プールが構成されます。サブリソース プールのメモリ予約は、仮想マシンに設定されたメモリ サイズに組織仮想データセンターの割合の保証率を掛けた値だけ上昇します。サブリソースの CPU 予約は、仮想マシンに構成されている vCPU の数に組織 VDC レベルで指定されている vCPU を掛け、さらに組織 VDC レベルで設定されている CPU の割合の保証率を掛けた値だけ上昇します。柔軟性のある割り当てプール機能が有効になっている場合、サブリソース プールのメモリ制限は仮想マシンに設定されたメモリ サイズの分だけ上昇し、サブリソース プールの CPU 制限は仮想マシンに設定されている vCPU の数に組織 VDC レベルで指定された vCPU の周波数を掛けた値だけ上昇します。仮想マシンは、メモリおよび CPU 予約がゼロになるよう再構成され、仮想マシンの配置エンジンによって、仮想マシンがプロバイダ VDC のリソース プール上に配置されます。

柔軟性のある割り当てプールの割り当てモデルでは、制限を監視および管理するのは VMware Cloud Director のみです。柔軟性機能が無効な場合は、リソース プールの制限が追加で設定されます。

割り当てプール モデルのメリットは、仮想マシンが同じサブリソース プール上にあるアイドル状態の仮想マシンのリソースを活用できるという点にあります。このモデルでは、プロバイダ VDC に追加された新しいリソースを活用できます。

まれに、作成時に割り当てられていたリソース プールからパワーオン時に別のリソース プールに仮想マシンが切り替わることがあります。これは、元のリソース プールのリソース不足によるものです。この切り替えにより、仮想マシンのディスク ファイルを新しいリソース プールに移すために、若干のコストがかかる可能性があります。

柔軟性のある割り当てプール機能が無効になっている場合、割り当てプール組織 VDC の動作は、VMware Cloud Director 1.5 の割り当てプール モデルと同様の動作になります。このモデルでは、vCPU の周波数は構成可能にはなりません。オーバーコミットは、確保されるリソースの割合を設定することによって制御されます。

デフォルトでは、割り当てプール VDC 内の仮想マシンは VDC の設定から予約、制限、および共有の設定を取得します。仮想マシンを作成するか、CPU とメモリの両方のカスタム リソース割り当て設定を使用して仮想マシンを再構成するには、vCloud API を使用します。『VMware Cloud Director API プログラミング ガイド』を参照してください。

従量課金制の割り当てモデル

従量課金制の割り当てモデルでは、リソースは、組織仮想データセンター (VDC) でユーザーが vApp を作成するときのみコミットされます。リソースが保証する割合を指定でき、これによりリソースをオーバーコミットできます。従量課金制の組織 VDC に柔軟性を持たせるには、複数のリソース プールをそのプロバイダ VDC に追加します。

組織にコミットされるリソースは、仮想マシン レベルで適用されます。

仮想マシンがパワーオンされているときに、元のリソース プールが仮想マシンに対応できない場合は、配置エンジンがリソース プールをチェックして、仮想マシンを別のリソース プールに割り当てます。リソース プールのサブリソース プールが使用できない場合は、VMware Cloud Director によって制限なし、レート ゼロのサブリソース プールが作成されます。仮想マシンのレートは、上限に、コミットされたリソースの数を掛けた値に設定されます。仮想マシンは、仮想マシンの配置エンジンによってプロバイダ VDC リソース プールに配置されます。

従量課金制モデルのメリットは、プロバイダ VDC に追加された新しいリソースを活用できるという点にあります。

まれに、作成時に割り当てられていたリソース プールからパワーオン時に別のリソース プールに仮想マシンが切り替わることがあります。これは、元のリソース プールのリソース不足によるものです。この切り替えにより、仮想マシンのディスク ファイルを新しいリソース プールに移すために、若干のコストがかかる可能性があります。

従量課金制モデルでは、事前にリソースが予約されるということはないため、十分なリソースがなければ、仮想マシンのパワーオンに失敗する可能性があります。このモデルで運用されている仮想マシンは、同じサブリソース プール上のアイドル状態の仮想マシンのリソースを活用できません。これは、リソースが仮想マシン レベルで設定されているためです。

デフォルトでは、従量課金制 VDC 内の仮想マシンは VDC の設定から予約、制限、および共有の設定を取得します。仮想マシンを作成するか、CPU とメモリの両方のカスタム リソース割り当て設定を使用して仮想マシンを再設定するには、vCloud API を使用します。『VMware Cloud Director API プログラミング ガイド』を参照してください。

予約プール割り当てモデル

予約プール割り当てモデルでは、割り当てたすべてのリソースが組織 VDC に直ちにコミットされます。組織内のユーザーは、個々の仮想マシンに予約、制限、および優先順位の設定を指定して、オーバーコミットメントを制御できます。

このモデルではリソース プールとサブリソース プールがそれぞれ1つずつしかないため、配置エンジンがパワーオン時に仮想マシンのリソース プールを再割り当てすることはありません。仮想マシンのレートおよび制限は修正されません。

予約プール モデルでは、必要な時は常にソースを使用できます。また、このモデルでは、仮想マシンのレート、制限および共有の微調整も可能です。これにより、入念な計画を行えば、予約済みリソースを最大限に活用できるようになります。予約プール仮想データセンター内の仮想マシン リソース割り当ての設定の詳細については、『vCloud Air- Virtual Private Cloud OnDemand ユーザー ガイド』を参照してください。

このモデルでは、予約は常にプライマリ クラスタで行われます。プライマリ クラスタに組織仮想データセンターを作成するための十分なリソースがない場合、組織仮想データセンターの作成は失敗します。

このモデルのその他の制限事項としては、柔軟性のなさや、組織ユーザーが仮想マシンの共有、レートおよび制限を最適に設定できない可能性があり、リソースの活用不足に繋がるといった点が挙げられます。

仮想マシン サイズ変更ポリシーと仮想マシン配置ポリシーについて

仮想マシン サイズ変更ポリシーと仮想マシン配置ポリシーを使用して、特定のクラスタまたはホスト上の仮想マシン (VM) のリソース割り当ておよび配置を制御できます。

VMware Cloud Director システム管理者は、グローバル レベルで仮想マシン サイズ変更ポリシーを作成および管理し、ポリシーを1つ以上の組織 VDC に個別に公開できます。VMware Cloud Director 10.2.1 以前では、仮想マシン配置ポリシーの範囲がプロバイダ VDC レベルで設定されるため、プロバイダ VDC ごとに仮想マシン配置ポリシーを個別に作成および管理できます。VMware Cloud Director 10.2.2 以降では、仮想マシン配置ポリシーの範囲に複数のプロバイダ VDC を含めることができます。また、バージョン 10.2.2 以降では、ユーザーが vApp を vApp テンプレートとしてカタログに保存した場合、テンプレートには、元の vApp の配置ポリシーおよびサイズ変更ポリシーも変更できないタグ付けされたポリシーとして含まれます。

組織 VDC にポリシーを公開すると、組織内のユーザーはそのポリシーを使用できるようになります。組織 VDC 内で仮想マシンを作成して管理する場合、テナントは使用可能なポリシーを仮想マシンに割り当てることができます。組織 VDC のテナントとユーザーは、仮想マシン配置ポリシーや仮想マシン サイズ変更ポリシーの具体的な設定を確認することはできません。

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使用すると、クラウド プロバイダは、CPU を多用するプロファイルやメモリ使用量の多いプロファイルなど、差別化されたサービス レベルを定義して提供することができます。組織 VDC に複数の仮想マシン位置ポリシーと仮想マシン サイズ変更ポリシーを公開した場合、テナント ユーザーは、組織 VDC で仮想マシンを作成および管理するときに、すべてのカスタム ポリシーおよびデフォルト ポリシーの中から選択できます。システムのデフォルト ポリシーは、すべての VDC に対して自動生成されます。ユーザーは VDC のシステムのデフォルト ポリシーを削除して、別のカスタム ポリシーをデフォルトとしてマークできます。デフォルト ポリシーでは値が定義されておらず、すべての仮想マシン構成が許可されます。

仮想マシン配置ポリシー

仮想マシン配置ポリシーは、ホストまたはホスト グループへの仮想マシンの配置を定義します。これは、クラウド プロバイダ管理者がプロバイダ VDC 内のホストの名前付きグループを作成するためのメカニズムです。ホストの名前付きグループは、プロバイダ VDC クラスタ内のホストのサブセットで、パフォーマンス層やライセンスなどの基準に基づいて選択される可能性があります。VMware Cloud Director 10.2.2 以降では、仮想マシン配置ポリシーの範囲を複数のプロバイダ VDC に拡張できます。

仮想マシン配置ポリシーは、テナント ワークロードの配置に直接影響する、仮想マシンとホスト間のアフィニティ ルールを定義します。管理者は、vCenter Server の仮想マシン グループを使用して名前付きホスト グループを定義または公開します。仮想マシン グループは、ホスト グループへの直接のアフィニティを持ち、アフィニティを持つホスト グループを表します。

仮想マシン配置ポリシーは、プロバイダ VDC レベルで定義します。仮想マシン配置ポリシーには、次の属性が含まれます。

- 名前（プロバイダ VDC 内で一意である必要があります）
- 説明
- プロバイダ VDC 内の基盤クラスタから選択された 1 つ以上の仮想マシン グループのセット。1 つのクラスタに 1 つの仮想マシン グループを選択できます

仮想マシン配置ポリシーは仮想マシンの作成時にはオプションであり、テナントが仮想マシンに割り当てることができる仮想マシン配置ポリシーは 1 つだけです。

テナントが組織 VDC 内に仮想マシンを作成して仮想マシン配置ポリシーを選択すると、VMware Cloud Director はそのポリシーで参照されている仮想マシン グループに仮想マシンを追加します。その結果、VMware Cloud Director は該当するホスト上に仮想マシンを作成します。

仮想マシン配置ポリシーには、各クラスタから 0 または 1 つの仮想マシン グループを含めることができます。たとえば、仮想マシン配置ポリシー `oracle_license` は、仮想マシン グループ `oracle_license1` と `oracle_license2` から構成され、仮想マシン グループ `oracle_license1` はクラスタ `oracle_cluster1` に属し、仮想マシン グループ `oracle_license2` はクラスタ `oracle_cluster2` に属することができます。

仮想マシンに仮想マシン配置ポリシーを割り当てると、配置エンジンは、この仮想マシンが配置されたクラスタの対応する仮想マシン グループに、この仮想マシンを追加します。たとえば、クラスタ *oracle_cluster1* に仮想マシンをデプロイして、この仮想マシンに仮想マシン配置ポリシー *oracle_license* を割り当てると、配置エンジンは、この仮想マシンを仮想マシン グループ *oracle_license1* に追加します。

仮想マシン サイズ変更ポリシー

仮想マシン サイズ変更ポリシーは、組織 VDC 内の仮想マシン (VM) のコンピューティング リソース割り当てを定義します。コンピューティング リソースの割り当てには、CPU とメモリの割り当て、予約、制限、およびシェアが含まれます。

仮想マシン サイズ変更ポリシーを使用することで、VMware Cloud Director システム管理者は、コンピューティング リソースの使用に関する次の項目を仮想マシン レベルで制御できます。

- vCPU の数と vCPU のクロック速度
- 仮想マシンに割り当てるメモリの量
- メモリおよび CPU の予約、制限、およびシェア
- 追加の設定。

`extraConfigs` API パラメータは、仮想マシンに追加の設定値として適用される、キーと値のペア間のマッピングを表します。追加設定を使用してポリシーを作成できるのは、vCloud API を使用する場合のみです。既存の追加設定は、Service Provider Admin Portal ユーザー インターフェイスで、詳細な仮想マシン サイズ変更ポリシー ビューの [追加設定] に表示されます。

仮想マシン サイズ変更ポリシーは、グローバル レベルで定義します。仮想マシン サイズ変更ポリシーの属性の詳細については、[仮想マシン サイズ変更ポリシーの属性](#)を参照してください。

VMware Cloud Director は、すべての VDC のデフォルトの仮想マシン サイズ変更ポリシーを生成します。デフォルトの仮想マシン サイズ変更ポリシーには名前と説明のみが含まれ、残りのすべてのポリシーの属性は空です。

組織 VDC のデフォルト ポリシーとして、別の仮想マシン サイズ変更ポリシーを定義することもできます。デフォルトの仮想マシン サイズ変更ポリシーは、テナントが組織 VDC 内に作成する仮想マシンのリソース割り当ておよびリソース使用量を制御します。ただし、テナントが別の特定の仮想マシン サイズ変更ポリシーを仮想マシンに割り当てた場合を除きます。

テナントが組織 VDC 内の個々の仮想マシンに割り当てることができるコンピューティング リソースの最大数を制限するには、クラウド プロバイダが最大仮想マシン サイズ変更ポリシーを定義します。最大仮想マシン サイズ変更ポリシーが組織 VDC に割り当てられている場合は、組織 VDC 内のすべての仮想マシンのコンピューティング リソースの設定の上限として機能します。テナント ユーザーは、仮想マシンの作成時に最大仮想マシン サイズ変更ポリシーを使用できません。仮想マシン サイズ変更ポリシーを最大ポリシーとして定義した場合、VMware Cloud Director はポリシーの内容を内部的にコピーし、コピーされた内容を最大仮想マシン サイズ変更ポリシーとして使用します。その結果、組織 VDC は最初に使用した仮想マシン サイズ変更ポリシーに依存しなくなります。

仮想マシン サイズ変更ポリシーを使用すると、クラウド プロバイダは組織 VDC 内のすべての仮想マシンのコンピューティング リソース使用量を制限できます。たとえば、*Small Size*、*Medium Size*、*Large Size* などの事前定義済みの 3 つのサイズに制限できます。ワークフローは以下のようになります。

- 1 システム管理者は、次の属性を使用して 3 つの仮想マシン サイズ変更ポリシーを作成します。

名前	属性
Small Size	<ul style="list-style-type: none"> ■ 説明：サイズが小さい仮想マシン ポリシー ■ 名前：小サイズ ■ メモリ：1024 ■ vCPU の数：1
Medium Size	<ul style="list-style-type: none"> ■ 説明：サイズが中程度の仮想マシン ポリシー ■ 名前：中サイズ ■ メモリ：2048 ■ vCPU の数：2
Large Size	<ul style="list-style-type: none"> ■ 説明：サイズが大きい仮想マシン ポリシー ■ 名前：大サイズ ■ メモリ：4096 ■ vCPU の数：4

- 2 新しい仮想マシン サイズ変更ポリシーを組織 VDC に公開します。
- 3 必要に応じて、仮想マシン サイズ変更ポリシーの 1 つを、組織 VDC のデフォルトの仮想マシン サイズ変更ポリシーとして定義します。

クラウド プロバイダが使用できるポリシーの操作を以下に示します。

- ホストまたはホスト グループへの仮想マシンの配置を定義するために、配置ポリシーを作成する。[『プロバイダ VDC 内での仮想マシン配置ポリシーの作成』](#)を参照してください。
- テナント ワークロードに対する物理コンピューティング リソースの割り当てを制御するために、サイズ変更ポリシーを作成する。[『仮想マシン サイズ変更ポリシーの作成』](#)を参照してください。
- 1 つ以上の組織 VDC に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公開する。[組織 VDC への仮想マシン配置ポリシーの追加](#)を参照してください。
- 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デフォルトとして設定する。
- 仮想マシン サイズ変更ポリシーおよび仮想マシン配置ポリシーを編集する。ポリシーの名前と説明を編集するには、VMware Cloud Director ユーザー インターフェイスを使用する必要があります。
- 組織 VDC から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の公開を解除する。
- 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削除する。[仮想マシン配置ポリシーの削除および仮想マシン サイズ変更ポリシーの削除](#)を参照してください。

ORG_VDC_MANAGE_COMPUTE_POLICIES 権限を持つユーザーは、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を作成、更新、公開できます。

次の表に、テナント ユーザーが仮想マシン サイズ変更ポリシーと仮想マシン配置ポリシーに対して実行できる操作を示します。

表 6-1. テナント ユーザーによる仮想マシンサイズ変更ポリシーおよび仮想マシン配置ポリシーの操作

操作	説明
仮想マシンの作成中に、仮想マシンにポリシーを割り当てる。	<p>組織 VDC 内に仮想マシンを作成する権限を持つテナント ユーザーは、オプションで VMware Cloud Director Tenant Portal を使用することにより、仮想マシン サイズ変更ポリシーおよび仮想マシン配置ポリシーを仮想マシンに割り当てることができます。その結果、仮想マシン サイズ変更ポリシーで定義されたパラメータによって、仮想マシンの CPU およびメモリ使用量が制御されます。仮想マシンの作成中に、テナントが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割り当てる必要はありません。仮想マシンに割り当てる仮想マシン サイズ変更ポリシーがテナントで明示的に選択されていない場合は、デフォルトの仮想マシン サイズ変更ポリシーが仮想マシンに適用されます。</p> <p>仮想マシン配置ポリシーを作成しない場合、テナントには仮想マシン配置ポリシー オプションが表示されません。テナントが選択した配置ポリシーにサイズ変更情報が含まれている場合、仮想マシン サイズ変更ポリシー オプションはテナントに表示されません。サイズ変更情報を含む仮想マシン配置ポリシーを作成できるのは、vCloud API を使用する場合のみです。</p> <p>仮想マシン サイズ変更ポリシーが 1 つのみの場合、仮想マシン サイズ変更ポリシー オプションはテナントに表示されません。</p> <p>システム管理者が仮想マシン サイズ変更ポリシーで [vCPU 数]、[ソケットあたりのコア数]、[メモリ] の各属性を設定すると、テナントがポリシーを選択したとき、これらの値が表示されますが、編集はできません。</p>
既存の仮想マシンにポリシーを割り当てる。	<p>組織 VDC 内の仮想マシンを管理する権限を持つテナント ユーザーは、VMware Cloud Director Tenant Portal を使用することにより、既存の仮想マシンの仮想マシン サイズ変更ポリシーおよび仮想マシン配置ポリシーを割り当てたり、変更したりできます。テナントが仮想マシン配置ポリシーを変更すると、仮想マシンは、新しい仮想マシン配置ポリシーで定義されている仮想マシンとホストの間のアフィニティ ルールに従って新しいホストに移動します。テナントが仮想マシン サイズ変更ポリシーを変更すると、仮想マシンは、新しい仮想マシン サイズ変更ポリシーで指定されているコンピューティング リソースを使用するようにシステムによって再構成されます。</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を操作するためのワークフローは、次のとおりです。

- 1 システム管理者が 1 つ以上の仮想マシン配置ポリシーを作成します。『[プロバイダ VDC 内での仮想マシン配置ポリシーの作成](#)』を参照してください。
- 2 システム管理者が 1 つ以上の仮想マシン サイズ変更ポリシーを作成します。『[仮想マシン サイズ変更ポリシーの作成](#)』を参照してください。

仮想マシン サイズ変更ポリシーの名前は、1 つの VMware Cloud Director サイト内で一意です。仮想マシン配置ポリシーの名前は、ポリシーのプロバイダ VDC スcope内で一意です。

- 3 システム管理者が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を 1 つ以上の組織 VDC に公開します。『[組織 VDC への仮想マシン配置ポリシーの追加](#)』を参照してください。

仮想マシン配置ポリシーを公開すると、組織 VDC 内のテナント ユーザーが仮想マシンを作成するとき、および仮想マシンを編集するときに、それを使用できるようになります。

- 4 仮想マシンを作成または更新する際、テナントは vCloud API または VMware Cloud Director Tenant Portal を使用して、仮想マシン サイズ変更ポリシーと仮想マシン配置ポリシーを仮想マシンに割り当てることができます。

プロバイダ VDC 内での仮想マシン配置ポリシーの作成

仮想マシン配置ポリシーとは、プロバイダ VDC ポリシーの参照が含まれている VDC コンピューティング ポリシーのことです。VMware Cloud Director 10.2.2 以降では、仮想マシン配置ポリシーの範囲に複数のプロバイダ

VDC を追加できます。仮想マシン配置ポリシーを使用して、特定のホスト、ホスト グループ、またはクラスタ上の仮想マシンの配置を定義できます。

VMware Cloud Director 10.2.2 以降では、仮想マシン配置ポリシーに 1 つ以上のプロバイダ VDC ポリシーの参照を含めることができます。プロバイダ VDC 内から配置ポリシーを作成すると、そのポリシーは選択したプロバイダ VDC のみを参照するようになります。仮想マシン配置ポリシーを編集して、このポリシーの範囲にプロバイダ VDC を含めることができます。また、[仮想マシン配置ポリシー] タブで配置ポリシーを作成して、その範囲に複数のプロバイダ VDC を含めることもできます。[仮想マシンの配置ポリシーの編集およびグローバルな仮想マシン配置ポリシーの作成](#)を参照してください。

前提条件

- 環境内に 1 つ以上のプロバイダ VDC があることを確認します。
- 環境内に 1 つ以上の仮想マシン グループがあることを確認します。

仮想マシン グループは、正のアフィニティを使用してホスト グループにリンクできる仮想マシンの集合です。正のアフィニティ ルールを使用すると、仮想マシンのグループが特定のホストに配置されます。仮想マシン グループを作成するには、vCenter Server ユーザー インターフェイスまたは VMware Cloud Director API を使用します。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [プロバイダ VDC] を選択します。
- 3 リストからプロバイダ VDC を選択します。
- 4 [仮想マシン配置ポリシー] タブをクリックし、[新規] をクリックします。
- 5 (オプション) ウィザードの [仮想マシン配置ポリシーについて] ページで、仮想マシン配置ポリシーの情報の表示を停止するチェックボックスをオンにします。
- 6 [次へ] をクリックします。
- 7 仮想マシン配置ポリシーの名前と、必要に応じて説明を入力します。
- 8 仮想マシンをリンクする仮想マシン グループまたは論理仮想マシン グループを選択し、[次へ] をクリックします。

複数の論理グループを選択した場合、テナントがこのポリシーを仮想マシンに適用すると、その仮想マシンは、選択した論理仮想マシン グループに含まれるすべての仮想マシン グループのメンバーになります。仮想マシンは、これらのグループ内の仮想マシンに適用されるすべてのアフィニティの組み合わせに合わせるよう調整されます。VMware Cloud Director 10.2.2 以降では、仮想マシン グループと論理グループを同時に選択できます。

1 つのクラスタに 1 つの仮想マシン グループを選択することで、インライン論理仮想マシン グループを作成できます。この論理仮想マシン グループは、名前を持たず、選択した仮想マシン配置ポリシーのみで使用できます。

- 9 仮想マシン配置ポリシーの設定を確認し、[完了] をクリックします。

次のステップ

- [仮想マシン サイズ変更ポリシーの作成](#).

- [組織 VDC への仮想マシン配置ポリシーの追加](#).
- VMware Cloud Director 10.2.2 以降では、[仮想マシンの配置ポリシーの編集](#)できます。
- [仮想マシン配置ポリシーの削除](#).

グローバルな仮想マシン配置ポリシーの作成

VMware Cloud Director 10.2.2 以降では、仮想マシン配置ポリシーに 1 つ以上のプロバイダ VDC ポリシーの参照を含めることができます。仮想マシン配置ポリシーを使用して、特定のホスト、ホスト グループ、または 1 つ以上のクラスタ上の仮想マシンの配置を定義できます。

プロバイダ VDC 内から配置ポリシーを作成すると、そのポリシーは選択したプロバイダ VDC のみを参照するようになります。[プロバイダ VDC 内での仮想マシン配置ポリシーの作成](#)を参照してください。VMware Cloud Director 10.2.2 以降で、仮想マシン配置ポリシーの範囲にプロバイダ VDC を含めるには、ポリシーを編集するか、グローバルな配置ポリシーを作成します。

前提条件

- 環境内に 1 つ以上のプロバイダ VDC があることを確認します。
- 環境内に 1 つ以上の仮想マシン グループがあることを確認します。

仮想マシン グループは、正のアフィニティを使用してホスト グループにリンクできる仮想マシンの集合です。正のアフィニティ ルールを使用すると、仮想マシンのグループが特定のホストに配置されます。仮想マシン グループを作成するには、vCenter Server ユーザー インターフェイスまたは VMware Cloud Director API を使用します。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [仮想マシン配置ポリシー] を選択し、[新規] をクリックします。
- 3 (オプション) ウィザードの [仮想マシン配置ポリシーについて] ページで、仮想マシン配置ポリシーの情報の表示を停止するチェックボックスをオンにします。
- 4 [次へ] をクリックします。
- 5 仮想マシン配置ポリシーの名前と、必要に応じて説明を入力します。
- 6 仮想マシンをリンクする仮想マシン グループおよび論理仮想マシン グループを選択し、[次へ] をクリックします。

1 つのクラスタに 1 つの仮想マシン グループを選択できます。

複数の論理グループを選択した場合、テナントがこのポリシーを仮想マシンに適用すると、その仮想マシンは、選択した論理仮想マシン グループに含まれるすべての仮想マシン グループのメンバーになります。仮想マシンは、これらのグループ内の仮想マシンに適用されるすべてのアフィニティの組み合わせに合わせるよう調整されます。VMware Cloud Director 10.2.2 以降では、仮想マシン グループと論理グループを同時に選択できます。

1 つのクラスタに 1 つの仮想マシン グループを選択することで、インライン論理仮想マシン グループを作成できます。この論理仮想マシン グループは、名前を持たず、選択した仮想マシン配置ポリシーのみで使用できます。

7 仮想マシン配置ポリシーの設定を確認し、[完了] をクリックします。

次のステップ

- [仮想マシン サイズ変更ポリシーの作成](#).
- [組織 VDC への仮想マシン配置ポリシーの追加](#).
- VMware Cloud Director 10.2.2 以降では、[仮想マシンの配置ポリシーの編集](#)できます。
- [仮想マシン配置ポリシーの削除](#).

仮想マシンの配置ポリシーの編集

VMware Cloud Director 10.2.2 以降では、仮想マシン配置ポリシーの範囲を編集して変更できます。

前提条件

[グローバルな仮想マシン配置ポリシーの作成](#)

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [仮想マシン配置ポリシー] を選択します。
- 3 仮想マシン配置ポリシーを選択して、[編集] をクリックします。
- 4 (オプション) ウィザードの [仮想マシン配置ポリシーについて] ページで、仮想マシン配置ポリシーの情報の表示を停止するチェックボックスをオンにします。
- 5 [次へ] をクリックします。
- 6 仮想マシン配置ポリシーの名前と、必要に応じて説明を編集します。
- 7 仮想マシンをリンクする仮想マシン グループおよび論理仮想マシン グループを編集して、[次へ] をクリックします。

1つのクラスタに1つの仮想マシン グループを選択できます。配置ポリシーを組織 VDC に公開する場合などに、現在使用中のクラスタを選択解除することはできません。
- 8 仮想マシン配置ポリシーの設定を確認し、[完了] をクリックします。

次のステップ

- [仮想マシン サイズ変更ポリシーの作成](#).
- [組織 VDC への仮想マシン配置ポリシーの追加](#).
- [仮想マシン配置ポリシーの削除](#).

組織 VDC への仮想マシン配置ポリシーの追加

仮想マシン配置ポリシーを作成しても、テナントには表示されません。仮想マシン配置ポリシーをテナントで使用できるようにするには、そのポリシーを組織 VDC に公開します。

仮想マシン配置ポリシーを組織 VDC に公開すると、ポリシーがテナントに表示されるようになります。VMware Cloud Director 10.2.2 以降で配置ポリシーを組織 VDC に公開するには、[グローバルな仮想マシン配置ポリシーの作成](#)するか、[仮想マシンの配置ポリシーの編集](#)して、まず仮想マシン配置ポリシーの範囲にバックアップ プロバイダ VDC を含める必要があります。テナントは、新しいスタンドアロン仮想マシンの作成またはテンプレートからの仮想マシンの作成、仮想マシンの編集、vApp への仮想マシンの追加、および vApp テンプレートからの vApp の作成を行うときに、ポリシーを選択できます。テナントで使用可能な仮想マシン配置ポリシーを削除することはできません。

前提条件

- 環境内に 1 つ以上の組織 VDC があることを確認します。[組織仮想データセンターの作成](#)を参照してください。
- 1 つ以上の仮想マシン配置ポリシーがあることを確認します。『[プロバイダ VDC 内での仮想マシン配置ポリシーの作成](#)』を参照してください。VMware Cloud Director 10.2.2 以降では、1 つ以上のプロバイダ VDC ポリシーの参照を含むグローバルな配置ポリシーを作成できます。『[グローバルな仮想マシン配置ポリシーの作成](#)』を参照してください。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [組織 VDC] をクリックします。
- 3 組織 VDC を選択し、[仮想マシン配置ポリシー] タブをクリックします。
- 4 [追加] をクリックします。
- 5 組織 VDC に追加する仮想マシン配置ポリシーを選択して、[OK] をクリックします。

次のステップ

- ポリシーを選択し、[削除] をクリックしてポリシーを公開解除します。
- 仮想マシン配置ポリシーを選択し、[デフォルトとして設定] をクリックして、仮想マシンおよび vApp の作成中や仮想マシンの編集中に、テナントのデフォルトの選択肢としてそのポリシーが表示されるようにします。組織 VDC に対して複数の仮想マシン配置ポリシーが公開されている場合、テナントはデフォルトのポリシーとは異なるポリシーを選択できます。

仮想マシン配置ポリシーの削除

仮想マシン配置ポリシーがテナントに公開されていない場合は、プロバイダ仮想データセンターから削除できます。

前提条件

- 環境内に 1 つ以上の仮想マシン配置ポリシーがあることを確認します。
- 仮想マシン配置ポリシーが組織仮想データセンターに追加されていないことを確認します。テナントで使用可能な仮想マシン配置ポリシーは削除できません。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [プロバイダ VDC] を選択します。

- 3 リストからプロバイダ VDC を選択します。
- 4 [仮想マシン配置ポリシー] タブをクリックして、仮想マシン配置ポリシーを選択します。
- 5 [削除] をクリックします。

仮想マシン サイズ変更ポリシーの属性

仮想マシン (VM) サイズ変更ポリシーを作成するときに、使用可能なすべての属性のサブセットを指定できます。必須属性は、仮想マシン サイズ変更ポリシー名のみです。

仮想マシン サイズ変更ポリシーには 2 つのタイプのパラメータがあります。

- 個々の仮想マシン サイズ変更設定 - 仮想マシンの指定した RAM、vCPU 数、およびソケットあたりのコア数を現在のポリシーで事前設定します。
- 最大リソースに対する制約 - 単一の仮想マシンによるメモリおよび CPU の使用量の制限を現在のポリシーで事前設定します。

次の表に、仮想マシン サイズ変更ポリシー内で定義できるすべての属性を示します。

表 6-2. VDC コンピューティング ポリシーの属性

VDC コンピューティング ポリシーの属性		
属性	API パラメータ	説明
Name	name	仮想マシン サイズ変更ポリシーの識別子として使用される必須のパラメータ。
Description	description	仮想マシン サイズ変更ポリシーの短い説明を表します。
vCPU Speed	cpuSpeed	コアの vCPU 速度を MHz または GHz 単位で定義します。
vCPU Count	cpuCount	仮想マシンに設定される vCPU の数を定義します。これは仮想マシンのハードウェア設定です。テナントが仮想マシン サイズ変更ポリシーを仮想マシンに割り当てると、この数は仮想マシンに設定された vCPU の数になります。
Cores Per Socket	coresPerSocket	仮想マシンのソケットあたりのコア数。これは仮想マシンのハードウェア設定です。仮想マシン サイズ変更ポリシーで定義されている vCPU の数は、ソケットあたりのコア数の整数倍にする必要があります。vCPU の数がソケットあたりのコア数で割り切れない場合、ソケットあたりのコア数は無効になります。
CPU Reservation Guarantee	cpuReservationGuarantee	仮想マシンの CPU リソースの予約量を定義します。仮想マシンに割り当てられた CPU は、vCPU の数に vCPU 速度 (MHz) を掛けた値に等しくなります。この属性の値は 0 ～ 1 の範囲になります。CPU 予約保証の値を 0 にすると、CPU 予約がないことが定義されます。値を 1 にすると、100% の CPU 予約が定義されます。
CPU Limit	cpuLimit	仮想マシンの CPU 制限を MHz または GHz 単位で定義します。VDC コンピューティング ポリシーで定義されていない場合、CPU 制限は vCPU 速度に vCPU の数を掛けた値と等しくなります。

表 6-2. VDC コンピューティング ポリシーの属性（続き）

VDC コンピューティング ポリシーの属性		
属性	API パラメータ	説明
CPU Shares	cpuShares	仮想マシンの CPU シェア数を定義します。 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。仮想マシンの CPU のシェアが別の仮想マシンの 2 倍である場合、これら 2 台の仮想マシンでリソースの獲得に競争が生じた際に、シェアが 2 倍の仮想マシンは、別の仮想マシンの 2 倍の CPU を使用できます。VDC コンピューティング ポリシーで定義されていない場合は、通常のシェア数が仮想マシンに適用されます。
Memory	memory	仮想マシンに設定されるメモリを MB または GB 単位で定義します。これは仮想マシンのハードウェア設定です。 テナントが仮想マシンに仮想マシン サイズ変更ポリシーを割り当てると、仮想マシンはこの属性で定義されるメモリの容量を受け取ります。
Memory Reservation Guarantee	memoryReservationGuarantee	仮想マシンに設定されるメモリの予約量を定義します。 この属性の値は 0 ~ 100% の範囲になります。
Memory Limit	memoryLimit	仮想マシンのメモリ制限を MB または GB 単位で定義します。 仮想マシン サイズ変更ポリシーで定義されていない場合、メモリ制限は仮想マシンに割り当てられたメモリと等しくなります。
Memory Shares	memoryShares	仮想マシンのメモリ シェア の数を定義します。 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。仮想マシンのメモリのシェアが別の仮想マシンの 2 倍である場合、これら 2 台の仮想マシンでリソースの獲得に競争が生じた際に、シェアが 2 倍の仮想マシンは、別の仮想マシンの 2 倍のメモリを使用できます。VDC コンピューティング ポリシーで定義されていない場合は、通常のシェア数が仮想マシンに適用されます。
Extra Configuration s	extraConfigs	仮想マシンに追加の設定値として適用される、キーと値ペア間のマッピングを表します。 追加設定を使用してポリシーを作成できるのは、vCloud API を使用する場合のみです。既存の追加設定は、Service Provider Admin Portal ユーザー インターフェイスで、詳細な仮想マシン サイズ変更ポリシー ビューの [追加設定] に表示されます。

仮想マシン サイズ変更ポリシーの作成

仮想マシン サイズ変更ポリシーを作成して、事前定義された CPU およびメモリの使用量の制約をテナントで使用可能にすることができます。テナントはこの制約を組織仮想データセンター内の個々の仮想マシンに適用できます。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで、[仮想マシン サイジング ポリシー] をクリックします。
- 3 [新規] をクリックします。
- 4 仮想マシン サイズ変更ポリシーの名前と、オプションで説明を入力します。
- 5 [次へ] をクリックします。
- 6 [CPU] ページで、ポリシーに適用する CPU 割り当て設定を選択し、[次へ] をクリックします。
- 7 ポリシーに適用するメモリ割り当て設定を選択し、[次へ] をクリックします。

8 仮想マシン サイズ変更ポリシーの設定を確認し、[完了] をクリックします。

次のステップ

- 仮想マシン サイズ変更ポリシーを作成した後は、仮想マシン サイズ変更ポリシーの名前と説明のみを編集できます。『[仮想マシン サイズ変更ポリシーの編集](#)』を参照してください。
- [組織 VDC への仮想マシン サイズ変更ポリシーの追加](#)。
- [プロバイダ VDC 内での仮想マシン配置ポリシーの作成](#)。

組織 VDC への仮想マシン サイズ変更ポリシーの追加

仮想マシン サイズ変更ポリシーを作成しても、テナントには表示されません。仮想マシン サイズ変更ポリシーをテナントで使用できるようにするには、そのポリシーを組織 VDC に公開します。

仮想マシン サイズ変更ポリシーを組織 VDC に公開すると、ポリシーがテナントに表示されるようになります。テナントは、新しいスタンドアローン仮想マシンの作成またはテンプレートからの仮想マシンの作成、仮想マシンの編集、vApp への仮想マシンの追加、および vApp テンプレートからの vApp の作成を行うときに、ポリシーを選択できます。テナントで使用可能な仮想マシン サイズ変更ポリシーを削除することはできません。

前提条件

- 環境内に 1 つ以上の組織 VDC があることを確認します。『[組織仮想データセンターの作成](#)』を参照してください。
- 1 つ以上の仮想マシン サイズ変更ポリシーがあることを確認します。『[仮想マシン サイズ変更ポリシーの作成](#)』を参照してください。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [組織 VDC] をクリックします。
- 3 組織 VDC を選択し、[仮想マシン サイズ変更ポリシー] タブをクリックします。
- 4 [追加] をクリックします。
- 5 組織 VDC に追加する仮想マシン サイズ変更ポリシーを選択して、[OK] をクリックします。

次のステップ

- ポリシーを選択し、[削除] をクリックしてポリシーを公開解除します。
- 仮想マシン サイズ変更ポリシーを選択し、[デフォルトとして設定] をクリックして、仮想マシンおよび vApp の作成中や仮想マシンの編集に、テナントのデフォルトの選択肢としてそのポリシーが表示されるようにします。組織 VDC に対して複数の仮想マシン サイズ変更ポリシーが公開されている場合、テナントはデフォルトのポリシーとは異なるポリシーを選択できます。

仮想マシン サイズ変更ポリシーの編集

仮想マシン サイズ変更ポリシーを作成した後は、その名前と説明のみを編集できます。CPU とメモリのパラメータの編集はサポートされていません。

前提条件

- 環境内に 1 つ以上の組織 VDC があることを確認します。『[組織仮想データセンターの作成](#)』を参照してください。
- 1 つ以上の仮想マシン サイズ変更ポリシーがあることを確認します。『[仮想マシン サイズ変更ポリシーの作成](#)』を参照してください。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで、[仮想マシン サイジング ポリシー] をクリックします。
- 3 編集する仮想マシン サイズ変更ポリシーの名前をクリックします。
- 4 ポリシーの名前と説明を編集するには、[編集] をクリックします。
- 5 [保存] をクリックします。

次のステップ

[組織 VDC への仮想マシン サイズ変更ポリシーの追加](#)

仮想マシン サイズ変更ポリシーの削除

テナントに公開されていない仮想マシン サイズ変更ポリシーを削除できます。

前提条件

- 環境内に 1 つ以上の仮想マシン サイズ変更ポリシーがあることを確認します。
- 仮想マシン サイズ変更ポリシーが組織仮想データセンターに追加されていないことを確認します。テナントで使用可能な仮想マシン サイズ変更ポリシーは削除できません。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで、[仮想マシン サイジング ポリシー] をクリックします。
- 3 仮想マシン サイズ変更ポリシーを選択し、[削除] をクリックします。

VMware Cloud Director での Kubernetes の使用

VMware Cloud Director で Kubernetes を使用することにより、テナントにマルチテナントの Kubernetes サービスを提供できます。

Container Service Extension

Kubernetes Container Clusters は VMware Cloud Director 用の Container Service Extension プラグインです。サービス プロバイダおよびテナントが Kubernetes クラスタを作成するには、Kubernetes Container Clusters プラグインを使用する必要があります。VMware Cloud Director 10.2 以降では、プラグインの手動ダウンロードや、VMware Cloud Director Service Provider Admin Portal へのアップロードを行う必要はありません。VMware Cloud Director では、デフォルトでこのプラグインを使用できますが、Kubernetes クラスタを作成できるようにするには、テナントにプラグインを公開する必要があります。

ネイティブ クラスタと VMware Tanzu Kubernetes Grid Integrated Edition (TKGI) クラスタを作成するには、サービス プロバイダとテナントの両方が Container Service Extension バージョン 3.0 を使用する必要があります。Container Service Extension 3.0 サーバのセットアップを完了し、Container Service Extension ネイティブ配置ポリシーを 1 つ以上の組織 VDC に公開する必要があります。

VMware Cloud Director の vSphere with VMware Tanzu

VMware Cloud Director の vSphere with VMware Tanzu を使用すると、スーパーバイザー クラスタによってバックアップされているプロバイダ仮想データセンター (VDC) を作成できます。vSphere with VMware Tanzu が有効になっているホスト クラスタは、スーパーバイザー クラスタと呼ばれます。リソースの使用に制限を設定し、組織、ユーザー、グループあたりの Kubernetes クラスタの数など、使用可能なリソースを制限することができます。詳細については、[組織のリソース使用に対する割り当て容量の管理](#)を参照してください。

VMware Cloud Director で vSphere with VMware Tanzu を使用するには、まず vSphere 7.0 以降のクラスタで vSphere with VMware Tanzu 機能を有効にして、そのクラスタをスーパーバイザー クラスタとして構成する必要があります。vSphere ドキュメントの『vSphere with Kubernetes の構成および管理』ガイドを参照してください。使用する vCenter Server インスタンスには、ホスト クラスタとスーパーバイザー クラスタを両方含めることができます。

クラスタを作成するには、Tanzu Kubernetes プロバイダ VDC Kubernetes ポリシーを組織に公開し、作成時に組織 VDC Kubernetes ポリシーを適用する必要があります。ネイティブ クラスタおよび TKGI クラスタは、プロバイダ VDC Kubernetes ポリシーと組織 VDC Kubernetes ポリシーを使用しません。

Kubernetes クラスタ タイプ

- ネイティブ クラスタ - Kubernetes Container Clusters プラグインは、ネイティブの Kubernetes ランタイムを使用してクラスタを管理します。これらのクラスタは制御プレーン ノードが 1 台で、High Availability 機能は削減されています。また、パーシステント ボリュームの選択肢は少なく、ネットワークの自動化機能もありません。ただし、コストが低くなる場合があります。ネイティブの Kubernetes クラスタ環境では、Container Service Extension サーバをセットアップする必要があります。Container Service Extension (CSE) のドキュメントの『[CSE サーバ管理](#)』の章を参照してください。
- Tanzu Kubernetes クラスタ - vSphere with Tanzu ランタイム オプションを使用して、vSphere with VMware Tanzu で管理される Tanzu Kubernetes クラスタを作成できます。このオプションを使用すると、機能は増えますが、コストが高くなる可能性があります。詳細については、vSphere ドキュメントの『vSphere with Kubernetes の構成および管理』ガイドを参照してください。

- TKGI クラスタ - VMware Tanzu Kubernetes Grid Integrated Edition は、マルチクラウドのエンタープライズ プロバイダおよびサービス プロバイダが運用できる Kubernetes を対象とする、専用のコンテナ ソリューションです。これらの機能には、Kubernetes クラスタの高可用性、自動拡張、健全性チェック、自己修復、ローリング アップグレードなどがあります。TKGI クラスタの詳細については、VMware Tanzu Kubernetes Grid Integrated Edition のドキュメントを参照してください。

Tanzu Kubernetes クラスタ作成用のワークフロー

- 1 vSphere with VMware Tanzu 機能が有効になっている vCenter Server 7.0 以降のインスタンスを VMware Cloud Director に追加します。『[vCenter Server インスタンスを単独、または NSX Manager インスタンスと共に接続する](#)』を参照してください。
- 2 各スーパーバイザー クラスタのネットワーク設定を確認して、Kubernetes のワークロードを実行できるようにします。

重要： Ingress CIDRs および Services CIDR パラメータの IP アドレス範囲が、services および pods パラメータのデフォルトの vSphere の値である IP アドレス 10.96.0.0/12 および 192.168.0.0/192.16 と重複することはできません。『[vSphere with Kubernetes の構成および管理](#)』ガイドの Tanzu Kubernetes クラスタの構成パラメータに関する情報を参照してください。

注： VMware Cloud Director 10.2.2 以降で、初期セットアップ後にスーパーバイザー クラスタのネットワーク設定を変更した場合は、vCenter Server インスタンスを更新して、クラスタが作成された組織仮想データセンターの外部にある Tanzu Kubernetes クラスタからのアクセスをブロックする自動ファイアウォール ポリシーおよび NAT ルールを調整する必要があります。

- 3 スーパーバイザー クラスタによってバックアップされるプロバイダ VDC を作成します。『[プロバイダ仮想データセンターの作成](#)』を参照してください。

または、既存のプロバイダ VDC にスーパーバイザー クラスタを追加することもできます。vSphere 6.7 以前の環境を使用している場合は、環境をバージョン 7.0 にアップグレードして、既存のクラスタで vSphere with VMware Tanzu を有効にすることもできます。

スーパーバイザー クラスタによってバックアップされているプロバイダ VDC は、すべてのプロバイダ VDC が表示されているグリッド内に、名前の横に Kubernetes アイコンが付いた状態で表示されます。

- 4 (オプション) VMware Cloud Director によって、スーパーバイザー クラスタでバックアップされているプロバイダ VDC のデフォルトのプロバイダ VDC Kubernetes ポリシーが自動的に生成されます。Tanzu Kubernetes クラスタに対して、追加のプロバイダ VDC Kubernetes ポリシーを作成できます。『[プロバイダ VDC Kubernetes ポリシーの作成](#)』を参照してください。
- 5 [プロバイダ VDC] タブの [プロバイダ VDC Kubernetes ポリシーの組織 VDC への公開](#) または [組織 VDC] タブの [組織 VDC Kubernetes ポリシーの追加](#)。
- 6 サービス プロバイダに Kubernetes Container Clusters プラグインを公開します。『[組織からのプラグインの公開または公開解除](#)』を参照してください。テナントで Kubernetes クラスタを作成できるようにするには、これらの組織に Kubernetes Container Clusters プラグインを公開する必要があります。VMware Cloud Director プラグインの管理の詳細については、[プラグインの管理](#)を参照してください。

- 7 Tanzu Kubernetes クラスタを作成および管理する権限をテナントに付与する場合は、クラスタを使用する組織に `vmware : tkgcluster` 資格権限バンドルを公開する必要があります。権限バンドルを共有したら、Tanzu Kubernetes クラスタを作成および変更するロールに編集 : Tanzu Kubernetes ゲスト クラスタ権限を追加する必要があります。ユーザーがクラスタの削除も行う場合は、ロールに完全コントロール : Tanzu Kubernetes ゲスト クラスタ権限を追加する必要があります。さらに、組織内のすべての Tanzu Kubernetes クラスタを表示するユーザーや、サイト間でクラスタを管理するユーザーに、管理者権限を割り当てることもできます。ランタイム定義エンティティ (RDE) の権限およびアクセス レベルの詳細については、[14 章 定義済みエンティティの管理](#)を参照してください。
- 8 アクセス コントロール リスト (ACL) エントリを作成して、テナントまたはシステム管理者にアクセス権を付与します。ランタイム定義エンティティ (RDE) の共有の詳細については、[定義済みエンティティの共有](#)を参照してください。
- 9 [Tanzu Kubernetes クラスタの作成](#)

ネイティブ クラスタおよび TKGI クラスタ作成のワークフロー

- 1 サービス プロバイダに Kubernetes Container Clusters プラグインを公開します。『[組織からのプラグインの公開または公開解除](#)』を参照してください。テナントで Kubernetes クラスタを作成できるようにするには、これらの組織に Kubernetes Container Clusters プラグインを公開する必要があります。VMware Cloud Director プラグインの管理の詳細については、[プラグインの管理](#)を参照してください。
- 2 Container Service Extension サーバをセットアップし、Container Service Extension ネイティブ配置ポリシーまたは TKGI 有効化メタデータを組織 VDC に公開します。CSE サーバの設定の詳細については、Container Service Extension (CSE) のドキュメントの[CSE サーバ管理](#)の章を参照してください。
- 3 ネイティブ クラスタを作成および管理する権限をテナントに付与する場合は、ネイティブ クラスタを使用する組織に `cse : nativeCluster` 資格権限バンドルを公開する必要があります。権限バンドルを共有したら、ネイティブ クラスタを作成および変更するロールに 編集 : CSE : NATIVECLUSTER 権限を追加する必要があります。ユーザーがクラスタの削除も行う場合は、ロールに完全コントロール : CSE : NATIVECLUSTER 権限を追加する必要があります。さらに、組織内のすべての Tanzu Kubernetes クラスタを表示するユーザーや、サイト間でクラスタを管理するユーザーに、管理者権限を割り当てることもできます。ランタイム定義エンティティ (RDE) の権限およびアクセス レベルの詳細については、[14 章 定義済みエンティティの管理](#)を参照してください。
- 4 TKGI クラスタを作成および管理する権限をテナントに付与する場合は、特定の組織に `{cse} : PKS DEPLOY RIGHT` 権限を公開し、TKGI クラスタを作成および管理するロールに `{cse} : PKS DEPLOY RIGHT` 権限を追加する必要があります。`{cse} : PKS DEPLOY RIGHT` は、Container Service Extension サーバのインストール中に作成されます。
- 5 ネイティブ クラスタのアクセス コントロール リスト (ACL) エントリを作成して、テナントまたはシステム管理者にアクセス権を付与します。ランタイム定義エンティティ (RDE) の共有の詳細については、[定義済みエンティティの共有](#)を参照してください。
- 6 [ネイティブ Kubernetes クラスタの作成または VMware Tanzu Kubernetes Grid Integrated Edition クラスタの作成](#)。

組織 VDC Kubernetes ポリシーの追加

プロバイダ VDC Kubernetes ポリシーを使用して、組織 VDC Kubernetes ポリシーを追加できます。テナントは組織 VDC Kubernetes ポリシーを使用して、Tanzu Kubernetes クラスタを作成できます。

プロバイダ VDC Kubernetes ポリシーを組織 VDC に追加または公開する場合は、そのポリシーをテナントが使用できるようにします。テナントは、利用可能な組織 VDC Kubernetes ポリシーを使用して、Tanzu Kubernetes クラスタを作成するときに Kubernetes キャパシティを利用できます。Kubernetes ポリシーによって、配置、インフラストラクチャの品質、パーシステント ボリュームのストレージ クラスがカプセル化されます。Kubernetes ポリシーには、コンピューティングに関するさまざまな制限を設定できます。

1 つの組織 VDC に複数の組織 VDC Kubernetes ポリシーを追加できます。1 つのプロバイダ VDC Kubernetes ポリシーを使用して、複数の組織 VDC Kubernetes ポリシーを作成できます。組織 VDC Kubernetes ポリシーは、サービス品質のインジケータとして使用できます。たとえば、保証型マシン クラスと高速ストレージ クラスを選択できるゴールド Kubernetes ポリシー、またはベスト エフォート型マシン クラスと低速ストレージ クラスを選択できるシルバー Kubernetes ポリシーを公開できます。

前提条件

- 環境内に 1 つ以上の Flex 組織 VDC があることを確認します。[組織仮想データセンターの作成](#)を参照してください。
- 環境内に、スーパーバイザー クラスタによってバックアップされているプロバイダ VDC が 1 つ以上あることを確認します。スーパーバイザー クラスタによってバックアップされているプロバイダ VDC は、[プロバイダ VDC] タブに Kubernetes アイコン付きで表示されます。VMware Cloud Director の vSphere with VMware Tanzu の詳細については、[VMware Cloud Director での Kubernetes の使用](#)を参照してください。
- Tanzu Kubernetes クラスタの仮想マシン クラス タイプについて理解しておきます。vSphere ドキュメントの『vSphere with Kubernetes の構成および管理』ガイドを参照してください。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [組織 VDC] を選択し、Flex 組織 VDC の名前をクリックします。
- 3 [ポリシー] で [Kubernetes] を選択し、[追加] をクリックします。
[組織 VDC に公開] ウィザードが表示されます。
- 4 テナントに表示される、組織 VDC Kubernetes ポリシーの名前と説明を入力し、[次へ] をクリックします。
- 5 使用するプロバイダ VDC Kubernetes ポリシーを選択して、[次へ] をクリックします。
- 6 このポリシーで作成された Tanzu Kubernetes クラスタの CPU およびメモリの制限を選択します。

上限は、組織 VDC の CPU とメモリの割り当てによって異なります。ポリシーを追加する場合、選択した制限はテナントの最大値として機能します。

- 7 このポリシーで作成された Tanzu Kubernetes クラスタ ノードの CPU とメモリを予約するかどうかを選択して、[次へ] をクリックします。

クラス タイプごとに、保証型とベスト エフォート型の 2 つのエディションがあります。保証型クラス エディションでは構成済みリソースが完全に予約されますが、ベスト エフォート型エディションではリソースのオーバーコミットが許可されます。選択内容に応じて、ウィザードの次のページで、仮想マシンのクラス タイプを、保証型エディションまたはベスト エフォート型エディションの中から選択できます。

- CPU とメモリを完全に予約する保証型エディションの仮想マシンクラス タイプを指定するには、[はい] を選択します。
- CPU とメモリが予約されていないベスト エフォート型エディションの仮想マシン クラス タイプを指定するには、[いいえ] を選択します。

- 8 ウィザードの [マシン クラス] 画面で、このポリシーで使用可能な仮想マシン クラス タイプを 1 つ以上選択します。

組織 VDC へのポリシーの追加の際にテナントで使用可能なクラス タイプは、ここで選択したマシン クラスに限定されます。

- 9 1 つ以上のストレージ ポリシーを選択します。

- 10 選択内容を確認し、[公開] をクリックします。

結果

公開されたポリシーの情報が、Kubernetes ポリシーのリストに表示されます。公開されたポリシーによって、スーパーバイザー クラスタ上に、指定されたリソース制限を持つスーパーバイザー ネームスペースが作成されます。

テナントは、Kubernetes ポリシーを使用して、Tanzu Kubernetes クラスタを作成できます。VMware Cloud Director は、作成された各 Tanzu Kubernetes を、同じスーパーバイザー ネームスペース内のこの Kubernetes ポリシーの下に配置します。ポリシーのリソース制限が、スーパーバイザー ネームスペースのリソース制限になります。スーパーバイザー ネームスペースの、テナントで作成されたすべての Tanzu Kubernetes クラスタは、これらの制限内のリソースについて競合します。

次のステップ

[組織のリソース使用に対する割り当て容量の管理](#)

組織 VDC Kubernetes ポリシーの編集

ユーザーは組織 VDC Kubernetes ポリシーを修正して、説明および CPU とメモリに関する制限を変更できます。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [組織 VDC] を選択し、Flex 組織 VDC の名前をクリックします。
- 3 [ポリシー] で [Kubernetes] を選択し、編集するポリシーを選択して、[編集] をクリックします。

[VDC Kubernetes ポリシーの編集] ウィザードが表示されます。

- 4 組織 VDC Kubernetes ポリシーの説明を編集して、[次へ] をクリックします。

ポリシーの名前は、ポリシーの公開中に作成されたスーパーバイザー ネームスペースにリンクされているため、変更できません。

- 5 組織 VDC Kubernetes ポリシーの CPU およびメモリに関する制限を編集して、[次へ] をクリックします。

CPU およびメモリの予約を編集することはできません。

- 6 新しいポリシーの詳細を確認して、[保存] をクリックします。

Tanzu Kubernetes クラスタの作成

Kubernetes Container Clusters プラグインを使用して Tanzu Kubernetes クラスタを作成できます。

クラスタ作成に関するさまざまな Kubernetes ランタイム オプションの詳細については、[VMware Cloud Director での Kubernetes の使用](#)を参照してください。

コンテナ サービス拡張機能 CLI を使用して、Kubernetes クラスタを管理することもできます。[Container Service Extension](#) のドキュメントを参照してください。

VMware Cloud Director は、PodSecurityPolicy アドミッション コントローラが有効な状態で Tanzu Kubernetes クラスタをプロビジョニングします。ワークロードをデプロイするには、ポッドのセキュリティ ポリシーを作成する必要があります。ポッドのセキュリティ ポリシーを Kubernetes で使用する実装の詳細については、『vSphere with Kubernetes の構成および管理』ガイドの「Tanzu Kubernetes クラスタでのポッドのセキュリティ ポリシーの使用」を参照してください。

前提条件

- Tanzu Kubernetes クラスタを管理するすべての組織に Kubernetes Container Clusters プラグインを公開します。
- 組織 VDC 内に 1 つ以上の組織 VDC Kubernetes ポリシーがあることを確認します。組織 VDC Kubernetes ポリシーを追加するには、[組織 VDC Kubernetes ポリシーの追加](#)を参照してください。
- クラスタを使用する組織に、vmware : tkgcluster 資格権限バンドルを公開する必要があります。権限バンドルを共有したら、Tanzu Kubernetes クラスタを作成および変更するロールに編集 : Tanzu Kubernetes ゲスト クラスタ権限を追加する必要があります。ユーザーがクラスタの削除も行う場合は、ロールに完全コントロール : Tanzu Kubernetes ゲスト クラスタ権限を追加する必要があります。さらに、組織内のすべての Tanzu Kubernetes クラスタを表示するユーザーや、サイト間でクラスタを管理するユーザーに、管理者権限を割り当てることもできます。ランタイム定義エンティティ (RDE) の権限およびアクセス レベルの詳細については、[14 章 定義済みエンティティの管理](#)を参照してください。
- アクセス コントロール リスト (ACL) エントリを作成して、テナントまたはシステム管理者にアクセス権を付与します。ランタイム定義エンティティ (RDE) の共有の詳細については、[定義済みエンティティの共有](#)を参照してください。

手順

- 1 上部ナビゲーション バーで、[詳細] - [Kubernetes Container Clusters] の順に選択します。
- 2 (オプション) TKGI クラスタを作成する際に組織 VDC が有効になっている場合は、[Kubernetes Container Clusters] 画面で [vSphere with Tanzu およびネイティブ] タブを選択します。

- 3 [新規] をクリックします。
- 4 [vSphere with Tanzu] ランタイム オプションを選択して、[次へ] をクリックします。
- 5 新しい Kubernetes クラスタの名前を入力して、[次へ] をクリックします。
- 6 Tanzu Kubernetes クラスタをデプロイする組織 VDC を選択して、[次へ] をクリックします。
- 7 組織 VDC Kubernetes ポリシーと Kubernetes バージョンを選択して、[次へ] をクリックします。

VMware Cloud Director に、組織 VDC または Kubernetes ポリシーにも関連付けられていないデフォルトの Kubernetes バージョン セットが表示されます。これらのバージョンはグローバル設定です。使用可能なバージョンのリストを変更するには、セル管理ツールを使用して、`./cell-management-tool manage-config --name wcp.supported.kubernetes.versions -v version_numbers` コマンドにカンマ区切りのバージョン番号を指定して実行します。

- 8 新しいクラスタの制御プレーンおよびワーカー ノードの数を選択します。
- 9 制御プレーンおよびワーカー ノードのマシン クラスを選択して、[次へ] をクリックします。
- 10 制御プレーンおよびワーカー ノードの Kubernetes ポリシー ストレージ クラスを選択して、[次へ] をクリックします。
- 11 (オプション) VMware Cloud Director 10.2.2 以降の場合は、Kubernetes サービスの IP アドレスの範囲と Kubernetes ポッドの範囲を指定して、[次へ] をクリックします。

Classless Inter-Domain Routing (CIDR) は、IP ルーティングと IP アドレス割り当ての方法です。

オプション	説明
Pods CIDR	Kubernetes ポッドで使用する IP アドレスの範囲を指定します。デフォルト値は 192.168.0.0/16 です。ポッドのサブネット サイズは /24 以上にする必要があります。この値はスーパーバイザー クラスタの設定と重複することはできません。1 つの IP アドレス範囲を入力できます。
Services CIDR	Kubernetes サービスで使用する IP アドレスの範囲を指定します。デフォルト値は 10.96.0.0/12 です。この値はスーパーバイザー クラスタの設定と重複することはできません。1 つの IP アドレス範囲を入力できます。

- 12 クラスタの設定を確認し、[終了] をクリックします。

次のステップ

- ワーカー ノードの数を変更する場合は、Kubernetes クラスタのサイズを変更します。
- kubeconfig ファイルをダウンロードします。kubectl コマンドライン ツールは、kubeconfig ファイルを使用して、クラスタ、ユーザー、名前空間、および認証メカニズムに関する情報を取得します。
- Kubernetes クラスタを削除します。

ネイティブ Kubernetes クラスタの作成

Kubernetes Container Clusters プラグインを使用して、Container Service Extension 3.0 管理対象の Kubernetes クラスタを作成できます。

クラスタ作成に関するさまざまな Kubernetes ランタイム オプションの詳細については、[VMware Cloud Director での Kubernetes の使用](#)を参照してください。

コンテナ サービス拡張機能 CLI を使用して、Kubernetes クラスタを管理することもできます。[Container Service Extension](#) のドキュメントを参照してください。

前提条件

- サービス プロバイダが、Kubernetes Container Clusters プラグインを組織に公開していることを確認します。Kubernetes Container Clusters は VMware Cloud Director 用の Container Service Extension プラグインです。このプラグインは、上部ナビゲーション バーの [詳細] - [Kubernetes Container Clusters] で確認できます。
- ネイティブ Kubernetes クラスタ環境で組織 VDC を有効にするには、Container Service Extension サーバを設定します。Container Service Extension (CSE) のドキュメントの [CSE サーバ管理](#) の章を参照してください。
- CSE サーバのセットアップ中に作成された CSE ネイティブ ポリシーを組織 VDC に公開します。ユーザー インターフェイスを使用するには、[組織 VDC への仮想マシン配置ポリシーの追加](#)を参照してください。CSE 3.0 CLI を使用してポリシーを発行するには、`vcd cse ovdc enable Organization_VDC_Name --org Organization _Name --native` コマンドを実行します。
- `cse : nativeCluster` 資格権限バンドルを、ネイティブ クラスタを使用する組織に公開する必要があります。権限バンドルを共有したら、Tanzu Kubernetes クラスタを作成および変更するロールに編集 : CSE : NATIVECLUSTER 権限を追加する必要があります。ユーザーがクラスタの削除も行う場合は、ロールに完全コントロール : CSE : NATIVECLUSTER 権限を追加する必要があります。さらに、組織内のすべての Tanzu Kubernetes クラスタを表示するユーザーや、サイト間でクラスタを管理するユーザーに、管理者権限を割り当てることもできます。ランタイム定義エンティティ (RDE) の権限およびアクセス レベルの詳細については、[14 章 定義済みエンティティの管理](#)を参照してください。
- アクセス コントロール リスト (ACL) エントリを作成して、テナントまたはシステム管理者にアクセス権を付与します。ランタイム定義エンティティ (RDE) の共有の詳細については、[定義済みエンティティの共有](#)を参照してください。

手順

- 1 上部ナビゲーション バーで、[詳細] - [Kubernetes Container Clusters] の順に選択します。
- 2 (オプション) TKGI クラスタを作成する際に組織 VDC が有効になっている場合は、[Kubernetes Container Clusters] 画面で [vSphere with Tanzu およびネイティブ] タブを選択します。
- 3 [新規] をクリックします。
- 4 [ネイティブ] Kubernetes ランタイム オプションを選択します。
- 5 名前を入力し、リストから Kubernetes テンプレートを選択します。
- 6 (オプション) 新しい Kubernetes クラスタおよび SSH パブリック キーの説明を入力します。
- 7 [次へ] をクリックします。
- 8 ネイティブ クラスタをデプロイする組織 VDC を選択して、[次へ] をクリックします。

- 9 制御プレーンおよびワーカー ノードの数を選択し、必要に応じてノードのサイズ変更ポリシーを選択します。
- 10 [次へ] をクリックします。
- 11 NFS ソフトウェアを使用して追加の仮想マシンをデプロイする場合は、[NFS を有効化] をオンにします。
- 12 (オプション) 制御プレーンおよびワーカー ノードのストレージ ポリシーを選択します。
- 13 [次へ] をクリックします。
- 14 Kubernetes クラスタのネットワークを選択して、[次へ] をクリックします。
- 15 クラスタの設定を確認し、[終了] をクリックします。

次のステップ

- ワーカー ノードの数を変更する場合は、Kubernetes クラスタのサイズを変更します。
- kubeconfig ファイルをダウンロードします。kubectl コマンドライン ツールは、kubeconfig ファイルを使用して、クラスタ、ユーザー、名前空間、および認証メカニズムに関する情報を取得します。
- Kubernetes クラスタを削除します。

VMware Tanzu Kubernetes Grid Integrated Edition クラスタの作成

Container Service Extension を使用して VMware Tanzu Kubernetes Grid Integrated Edition (TKGI) クラスタを作成できます。

クラスタ作成に関するさまざまな Kubernetes ランタイム オプションの詳細については、[VMware Cloud Director での Kubernetes の使用](#)を参照してください。

コンテナ サービス拡張機能 CLI を使用して、Kubernetes クラスタを管理することもできます。[Container Service Extension](#) のドキュメントを参照してください。

TKGI の有効化メタデータを使用することで、TKGI クラスタを作成し、TKGI 対応の組織 VDC にアクセスするためのアクセス権をテナントに提供することができます。TKGI クラスタを作成するテナントの機能を制限する場合は、組織 VDC へのアクセス権のみを提供します。この場合、テナントは既存の TKGI クラスタを管理することはできませんが、新しいクラスタを作成することはできません。

前提条件

- サービス プロバイダが、Kubernetes Container Clusters プラグインを組織に公開していることを確認します。Kubernetes Container Clusters は VMware Cloud Director 用の Container Service Extension プラグインです。このプラグインは、上部ナビゲーション バーの [詳細] - [Kubernetes Container Clusters] で確認できます。
- TKGI Kubernetes クラスタ環境で組織 VDC を有効にするには、Container Service Extension サーバを設定します。CSE CLI を使用して TKGI の組織 VDC を有効にする方法については、Container Service Extension (CSE) ドキュメントの [CSE サーバ管理](#) の章を参照してください。
- TKGI の作成と管理にテナントからアクセスできるようにする場合は、特定の組織に {cse} : PKS DEPLOY RIGHT 権限を公開し、TKGI クラスタを作成および管理するロールに {cse} : PKS DEPLOY RIGHT を追加する必要があります。{cse} : PKS DEPLOY RIGHT は、Container Service Extension サーバのインストール中に作成されます。

手順

- 1 上部ナビゲーション バーで、[詳細] - [Kubernetes Container Clusters] の順に選択します。
- 2 [Kubernetes Container Clusters] 画面で [TKGI] タブを選択し、[新規] をクリックします。
[新しい TKGI クラスタの作成] ウィザードが開きます。
- 3 TKGI クラスタをデプロイする組織 VDC を選択して、[次へ] をクリックします。
VMware Cloud Director から CSE サーバ内の情報が要求されるため、リストがロードされるまで時間がかかることがあります。
- 4 新しい TKGI クラスタの名前を入力し、ワーカー ノードの数を選択します。
TKGI クラスタには、1 台以上のワーカー ノードが必要です。
- 5 [次へ] をクリックします。
- 6 クラスタの設定を確認し、[終了] をクリックします。
- 7 (オプション) 新しい TKGI クラスタをクラスタ リストに表示するには、ページの右側にある [更新] ボタンをクリックします。

次のステップ

- ワーカー ノードの数を変更する場合は、Kubernetes クラスタのサイズを変更します。
- kubeconfig ファイルをダウンロードします。kubectl コマンドライン ツールは、kubeconfig ファイルを使用して、クラスタ、ユーザー、名前空間、および認証メカニズムに関する情報を取得します。
- Kubernetes クラスタを削除します。

組織仮想データセンターの作成

組織にリソースを割り当てるには、組織仮想データセンター (VDC) を作成する必要があります。組織仮想データセンターは、プロバイダ VDC からリソースを取得します。1 つの組織で複数の組織 VDC を持つことができます。

前提条件

プロバイダ VDC を作成します。『[プロバイダ仮想データセンターの作成](#)』を参照してください。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで、[組織 VDC] をクリックし、[新規] をクリックします。
- 3 新しい組織 VDC の名前と、オプションで説明を入力します。
- 4 (オプション) 作成時に新しい組織 VDC を無効にするには、[組織 VDC の有効化] トグルをオフにします。
ユーザーは、無効化された組織 VDC に vApp をデプロイすることはできません。
- 5 [次へ] をクリックします。
- 6 この VDC を追加する組織の名前の横にあるラジオ ボタンを選択して、[次へ] をクリックします。

- 7 組織 VDC のコンピューティング リソースおよびストレージ リソースの取得元となるプロバイダ VDC の名前の横にあるラジオ ボタンを選択して、[次へ] をクリックします。

プロバイダ VDC のリストに、サイト内で有効になっているすべてのプロバイダ VDC が利用可能なリソースの情報とともに表示されます。ネットワーク リストには、選択したプロバイダ VDC で使用できるネットワークの情報が表示されます。

- 8 この組織 VDC の割り当てモデルを選択して、[次へ] をクリックします。

オプション	説明
割り当てプール	プロバイダ VDC から割り当てるリソースの割合が組織 VDC にコミットされます。CPU とメモリの両方に割合を指定できます。
従量課金制	リソースは、組織 VDC でユーザーが vApp を作成するときのみコミットされます。
予約プール	割り当てたすべてのリソースは、組織 VDC に直ちにコミットされます。
Flex	VDC と各仮想マシン レベルの両方で、リソース使用量を制御できます。Flex 割り当てモデルは、組織 VDC コンピューティング ポリシーの機能をサポートします。Flex 割り当てモデルは、他の割り当てモデルで使用可能なすべての割り当て設定をサポートします。

- 9 選択した割り当てモデルの割り当て設定を行い、[次へ] をクリックします。

オプション	説明	割り当てモデル
[弾性]	柔軟性のあるプール機能を有効または無効にします。柔軟性のある組織 VDC は、そのプロバイダ VDC に関連付けられているすべてのリソース プールを使用できます。	Flex
[仮想マシン メモリのオーバーヘッドを含める]	メモリのオーバーヘッドを含めるか、または除外します。	Flex
[CPU の割り当て]	この組織 VDC で実行されている仮想マシンに割り当てる CPU の最大量。	<ul style="list-style-type: none"> ■ 割り当てプール ■ 予約プール ■ Flex
[CPU リソースを予約値を超えて拡張できるようにします]	この組織 VDC に無制限の CPU リソースを提供するには、このトグルをオンにします。	予約プール
[CPU 割り当て]	この組織 VDC の CPU 使用量の最大値。	<ul style="list-style-type: none"> ■ 従量課金制 ■ Flex
[確保された CPU リソース]	この組織 VDC で実行されている仮想マシンに確保する CPU リソースの割合。100% 未満を確保することで、CPU リソースのオーバー コミットメントを制御できます。 割り当てプールの割り当てモデルの場合、割合の保証によってこの組織 VDC にコミットされる CPU の割り当ての割合も決定されます。	<ul style="list-style-type: none"> ■ 割り当てプール ■ 従量課金制 ■ Flex
[vCPU 速度]	vCPU 速度。組織 VDC で実行されている仮想マシンには、vCPU あたりこの GHz 単位の速度が割り当てられます。	<ul style="list-style-type: none"> ■ 従量課金制 ■ Flex
[メモリの割り当て]	この組織 VDC で実行されている仮想マシンに割り当てるメモリの最大量。	<ul style="list-style-type: none"> ■ 割り当てプール ■ 予約プール
[メモリ割り当て]	この組織 VDC のメモリ使用量の最大値。	<ul style="list-style-type: none"> ■ 従量課金制 ■ Flex

オプション	説明	割り当てモデル
[確保されたメモリ リソース]	この組織 VDC で実行されている仮想マシンに確保するメモリ リソースの割合。100 パーセント未満を確保すると、リソースをオーバーコミットできます。 割り当てプールの割り当てモデルの場合、割合の保証によってこの組織 VDC にコミットされるメモリの割り当ての割合も決定されます。	<ul style="list-style-type: none"> ■ 割り当てプール ■ 従量課金制 ■ Flex
[最大仮想マシン数]	組織 VDC に配置可能な仮想マシンの最大数。	<ul style="list-style-type: none"> ■ 割り当てプール ■ 従量課金制 ■ 予約プール ■ Flex

10 この組織 VDC のストレージ設定を行って、[次へ] をクリックします。

リストには、ソース プロバイダ VDC で有効なストレージ ポリシーが含まれています。

- a この組織 VDC に追加する 1 個以上のストレージ ポリシーのチェック ボックスを選択します。
- b (オプション) 選択したストレージ ポリシーに割り当てられたストレージ容量を制限するには、[割り当てタイプ] セルのドロップダウン メニューで [制限] を選択し、[割り当て済みストレージ] セルに最大容量を入力します。
- c (オプション) デフォルトのストレージ ポリシーを変更するには、[デフォルトのインスタンス化ポリシー] ドロップダウン メニューからターゲット デフォルト ストレージ ポリシーを選択します。

VMware Cloud Director は、ストレージ ポリシーが仮想マシンまたは vApp テンプレートのレベルで指定されていないすべての仮想マシンのプロビジョニング操作で、デフォルトのストレージ ポリシーを使用します。

- d (オプション) 組織 VDC 内の仮想マシンのシン プロビジョニングを有効にするには、[シン プロビジョニング] トグルをオンにします。
- e (オプション) 組織 VDC 内の仮想マシンの高速プロビジョニングを無効にするには、[高速プロビジョニング] トグルをオフにします。

11 この組織 VDC のネットワーク プールの設定を行って、[次へ] をクリックします。

VMware Cloud Director はネットワーク プールを使用して、vApp ネットワークおよび組織 VDC の内部ネットワークを作成します。

- この段階でネットワーク プールの追加をスキップするには、[ネットワーク プールを使用] 切り替えを無効にします。
- ネットワーク プールを設定するには、ターゲット ネットワーク プールの名前の横にあるラジオ ボタンを選択して、この組織 VDC の割り当て容量を入力します。

割り当て容量とは、このネットワーク プールによってバックアップされる組織 VDC 内でプロビジョニングされるネットワークの最大数です。選択したネットワーク プールで使用可能なネットワーク数を超えることはできません。

注： NSX-T Data Center によってバックアップされている組織 VDC は Geneve ネットワーク プールのみをサポートします。

12 [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の有効化または無効化

追加の vApp および仮想マシンに対して組織仮想データセンターのコンピューティング リソースおよびストレージ リソースの使用を禁止するには、この組織仮想データセンターを無効にします。実行中の vApp およびパワーオンされた仮想マシンは継続して実行されますが、追加の vApp または仮想マシンを作成したり開始したりすることはできません。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [組織 VDC] をクリックします。
- 3 ターゲット組織仮想データセンターの名前の横にあるラジオ ボタンを選択して、[有効化] または [無効化] をクリックします。
- 4 確認するには、[OK] をクリックします。

組織仮想データセンターの削除

組織から組織仮想データセンターのすべてのリソースを削除するには、この組織仮想データセンターを削除します。リソースは、ソース プロバイダ仮想データセンターにそのまま残ります。

重要： この操作を行うと、組織仮想データセンターと、そのすべての仮想マシン、vApp、組織仮想データセンター ネットワーク、および Edge Gateway が完全に削除されます。

前提条件

ターゲット組織仮想データセンターに属する特定の仮想マシン、vApp、vApp テンプレート、またはメディア ファイルを保持する場合は、それらを別の組織仮想データセンターに移動します。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [組織 VDC] をクリックします。
- 3 削除する組織仮想データセンター名の横にあるラジオ ボタンを選択して、[削除] をクリックします。
- 4 この組織仮想データセンターに、仮想マシン、vApp、組織仮想データセンター ネットワーク、Edge Gateway などのリソースが含まれている場合は、削除の確定のために各ソース タイプのチェックボックスを選択します。
- 5 確定するには、[削除] をクリックします。

仮想データセンター テンプレートの管理

VMware Cloud Director 10.2.2 以降では、仮想データセンター (VDC) テンプレートを作成および共有し、テナント組織と共有することで、組織管理者がこれを使用して VDC を作成できるようになりました。

VDC テンプレートを作成して組織と共有することで、プロバイダ VDC 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 VDC のセルフサービス プロビジョニングを行うことができます。

VDC テンプレートは、新しい組織 VDC の割り当てモデル、メモリ、CPU リソース構成、およびストレージ ポリシーを指定し、必要に応じて Edge Gateway および組織 VDC ネットワークを指定します。

組織仮想データセンター テンプレートの作成

VMware Cloud Director 10.2.2 以降では、HTML5 ユーザー インターフェイスを使用して、NSX Data Center for vSphere または NSX-T Data Center によってバックアップされる VDC の組織仮想データセンター (VDC) テンプレートを作成できます。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで、[組織 VDC テンプレート] をクリックし、[新規] をクリックします。
- 3 ネットワーク プロバイダ タイプを選択し、プロバイダ VDC と外部ネットワークのペアを選択して、[次へ] をクリックします。

NSX Data Center for vSphere の場合は、ユーザーがこのテンプレートから組織 VDC をインスタンス化すると、選択した Edge クラスタが VMware Cloud Director によって新しい組織 VDC に適用されます。新しい組織 VDC 内に新しくデプロイされたすべての Edge Gateway は、これらのプライマリおよびセカンダリ Edge クラスタを配置として使用します。

NSX-T Data Center の場合は、VMware Cloud Director は [サービス Edge クラスタ] を使用して、DHCP、VPN、DNS サービスなどのネットワーク サービスをデプロイします。VMware Cloud Director はゲートウェイのデプロイには [NSX-T ゲートウェイの Edge クラスタ] を使用します。

組織 VDC テンプレートをインスタンス化した後で、Edge クラスタを編集することはできません。

- 4 この組織 VDC の割り当てモデルを選択して、[次へ] をクリックします。

オプション	説明
割り当てプール	プロバイダ VDC から割り当てるリソースの割合が組織 VDC にコミットされます。CPU とメモリの両方に割合を指定できます。
従量課金制	リソースは、組織 VDC でユーザーが vApp を作成するときのみコミットされます。
予約プール	割り当てたすべてのリソースは、組織 VDC に直ちにコミットされます。
Flex	VDC と各仮想マシン レベルの両方で、リソース使用量を制御できます。Flex 割り当てモデルは、組織 VDC コンピューティング ポリシーの機能をサポートします。Flex 割り当てモデルは、他の割り当てモデルで使用可能なすべての割り当て設定をサポートします。

5 選択した割り当てモデルの割り当て設定を行い、[次へ] をクリックします。

オプション	説明	割り当てモデル
[弾性]	柔軟性のあるプール機能を有効または無効にします。柔軟性のある組織 VDC は、そのプロバイダ VDC に関連付けられているすべてのリソース プールを使用できます。	Flex
[仮想マシン メモリのオーバーヘッドを含める]	メモリのオーバーヘッドを含めるか、または除外します。	Flex
[CPU の割り当て]	この組織仮想データセンターで実行されている仮想マシンに割り当てる CPU の最大量。	<input type="checkbox"/> 割り当てプール <input type="checkbox"/> 予約プール <input type="checkbox"/> Flex
[CPU リソースを予約値を超えて拡張できるようにします]	この組織仮想データセンターに無制限の CPU リソースを提供するには、この切り替えを有効にします。	予約プール
[CPU 割り当て]	この組織仮想データセンターの CPU 使用量の最大値。	<input type="checkbox"/> 従量課金制 <input type="checkbox"/> Flex
[確保された CPU リソース]	この組織仮想データセンターで実行されている仮想マシンに確保する CPU リソースの割合。100% 未満を確保することで、CPU リソースのオーバーコミットメントを制御できます。 割り当てプールの割り当てモデルの場合、割合の確保によってこの組織仮想データセンターにコミットされる CPU の割り当ての割合も決定されます。	<input type="checkbox"/> 割り当てプール <input type="checkbox"/> 従量課金制 <input type="checkbox"/> Flex
[vCPU 速度]	vCPU の速度。組織仮想データセンターで実行されている仮想マシンには、vCPU あたりこの GHz 単位の速度が割り当てられます。	<input type="checkbox"/> 従量課金制 <input type="checkbox"/> Flex
[メモリの割り当て]	この組織仮想データセンターで実行されている仮想マシンに割り当てるメモリの最大容量。	<input type="checkbox"/> 割り当てプール <input type="checkbox"/> 予約プール
[メモリ制限]	この組織仮想データセンターのメモリ使用量の最大値。	<input type="checkbox"/> 従量課金制 <input type="checkbox"/> Flex
[確保されたメモリ リソース]	組織仮想データセンターで実行されている仮想マシンに確保するメモリ リソースの割合。100 パーセント未満を確保すると、リソースをオーバーコミットできます。 割り当てプールの割り当てモデルの場合、割合の確保によってこの組織仮想データセンターにコミットされるメモリの割り当ての割合も決定されます。	<input type="checkbox"/> 割り当てプール <input type="checkbox"/> 従量課金制 <input type="checkbox"/> Flex
[最大仮想マシン数]	組織仮想データセンターに配置できる仮想マシンの最大数。	<input type="checkbox"/> 割り当てプール <input type="checkbox"/> 従量課金制 <input type="checkbox"/> 予約プール <input type="checkbox"/> Flex

6 この組織仮想データセンターのストレージ設定を行って、[次へ] をクリックします。

リストには、ソース プロバイダ VDC で有効なストレージ ポリシーが含まれています。

- a 追加する 1 個以上のストレージ ポリシーを選択し、この組織 VDC に追加します。
- b (オプション) 選択したストレージ ポリシーに割り当てられたストレージ容量を制限するには、[割り当てタイプ] セルのドロップダウン メニューで [制限] を選択し、[割り当て済みストレージ] セルに最大容量を入力します。

- c (オプション) デフォルトのストレージ ポリシーを変更するには、[デフォルトのインスタンス化ポリシー] ドロップダウン メニューからターゲット デフォルト ストレージ ポリシーを選択します。

VMware Cloud Director は、ストレージ ポリシーが仮想マシンまたは vApp テンプレートのレベルで指定されていないすべての仮想マシンのプロビジョニング操作で、デフォルトのストレージ ポリシーを使用します。

- d (オプション) 組織 VDC 内の仮想マシンのシン プロビジョニングを有効にするには、[シン プロビジョニング] トグルをオンにします。
- e (オプション) 組織 VDC 内の仮想マシンの高速プロビジョニングを無効にするには、[高速プロビジョニング] トグルをオフにします。

7 (オプション) Edge Gateway を作成します。

- a 新しい Edge Gateway の名前と、オプションで説明を入力します。
- b NSX Data Center for vSphere でバックアップされる VDC のテンプレートを作成する場合は、一般的な Edge Gateway の設定をカスタマイズして、[次へ] をクリックします。

全般設定	説明
分散ルーティング	分散論理ルーティングを指定するように詳細ゲートウェイを構成します。
FIPS モード	NSX FIPS モードを使用するよう Edge ゲートウェイを構成します。
高可用性	バックアップ Edge ゲートウェイへの自動フェイルオーバーを有効にします。

- c NSX Data Center for vSphere によってバックアップされる VDC のテンプレートを作成する場合は、システム リソースの Edge Gateway 構成を変更します。

構成	説明
コンパクト	必要なメモリとコンピューティング リソースが少なく済みます。
大	[コンパクト] 設定よりも大きな容量と高いパフォーマンスを提供します。[大] 構成と [超特大] 構成では、同じセキュリティ機能が提供されます。
超特大	多数の同時セッションが実行される、ロード バランサを含む環境に使用します。
特大	スループットが多量である環境に使用します。高速な接続速度が必要です。

- d (オプション) ゲートウェイ サービスを使用するために割り当てる IP アドレスの数を指定します。

8 組織 VDC ネットワークを構成して、[次へ] をクリックします。

- 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 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。

- c 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] トグルをオンに切り替えます。

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、従量課金モデルのセカンダリ組織 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。

9 使用可能な固定 IP プールの範囲から IP アドレス範囲を追加して、[次へ] をクリックします。**10 (オプション) 組織 VDC のネットワーク プールの設定を行って、[次へ] をクリックします。**

割り当て容量とは、このネットワーク プールによってバックアップされる組織 VDC 内でプロビジョニングされるネットワークの最大数です。割り当て容量は、選択したネットワーク プールで使用可能なネットワーク数を超えることはできません。

11 このテンプレートから VDC を表示およびインスタンス化する組織を選択して、[次へ] をクリックします。

システム管理者は任意の組織 VDC テンプレートから VDC をインスタンス化できます。組織管理者は VMware Cloud Director Tenant Portal を使用することで、組織がテンプレートのアクセス リストに含まれている場合に VDC をインスタンス化できます。

12 テンプレートのシステム名とテナント側の名前を入力して、[次へ] をクリックします。**13 組織 VDC テンプレートの構成を確認し、[完了] をクリックします。****次のステップ**

- [テンプレートからの仮想データセンターのインスタンス化](#).
- [組織 VDC テンプレートの編集](#). ネットワーク プロバイダ タイプを除く、既存の VDC テンプレートのすべてのプロパティを編集できます。
- 必要に応じてカスタマイズできる組織 VDC テンプレートのコピーを作成するには、テンプレートのクローンを作成します。クローン作成の手順は、テンプレートを編集する手順と同様です。
- 組織 VDC テンプレートを削除します。

テンプレートからの仮想データセンターのインスタンス化

仮想データセンター (VDC) テンプレートから組織 VDC を作成するには、VDC をインスタンス化します。

システム管理者は任意の組織 VDC テンプレートから VDC をインスタンス化できます。組織管理者は VMware Cloud Director Tenant Portal を使用することで、組織がテンプレートのアクセス リストに含まれている場合に VDC をインスタンス化できます。

前提条件

組織仮想データセンター テンプレートの作成

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルにある [組織 VDC テンプレート] を選択します。
- 3 組織 VDC テンプレートを選択して、[VDC のインスタンス化] をクリックします。
- 4 新しい組織仮想データセンターの名前と、必要に応じて説明を入力します。
- 5 組織 VDC の組織を選択し、[作成] をクリックします。

組織 VDC テンプレートの編集

ネットワーク プロバイダ タイプを除く、既存の仮想データセンター (VDC) テンプレートのすべてのプロパティを変更できます。

前提条件

組織仮想データセンター テンプレートの作成

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで、[組織 VDC テンプレート] をクリックし、[編集] をクリックします。
- 3 プロバイダ VDC と外部ネットワークのペアを選択して、[次へ] をクリックします。

NSX Data Center for vSphere の場合は、ユーザーがこのテンプレートから組織 VDC をインスタンス化すると、選択した Edge クラスタが VMware Cloud Director によって新しい組織 VDC に適用されます。新しい組織 VDC 内に新しくデプロイされたすべての Edge Gateway は、これらのプライマリおよびセカンダリ Edge クラスタを配置として使用します。

NSX-T Data Center の場合は、VMware Cloud Director は [サービス Edge クラスタ] を使用して、DHCP、VPN、DNS サービスなどのネットワーク サービスをデプロイします。VMware Cloud Director はゲートウェイのデプロイには [NSX-T ゲートウェイの Edge クラスタ] を使用します。

組織 VDC テンプレートをインスタンス化した後で、Edge クラスタを編集することはできません。

- 4 この組織 VDC の割り当てモデルを選択して、[次へ] をクリックします。

オプション	説明
割り当てプール	プロバイダ VDC から割り当てるリソースの割合が組織 VDC にコミットされます。CPU とメモリの両方に割合を指定できます。
従量課金制	リソースは、組織 VDC でユーザーが vApp を作成するときのみコミットされます。

オプション	説明
予約プール	割り当てたすべてのリソースは、組織 VDC に直ちにコミットされます。
Flex	VDC と各仮想マシン レベルの両方で、リソース使用量を制御できます。Flex 割り当てモデルは、組織 VDC コンピューティング ポリシーの機能をサポートします。Flex 割り当てモデルは、他の割り当てモデルで使用可能なすべての割り当て設定をサポートします。

5 選択した割り当てモデルの割り当て設定を行い、[次へ] をクリックします。

オプション	説明	割り当てモデル
[弾性]	柔軟性のあるプール機能を有効または無効にします。柔軟性のある組織 VDC は、そのプロバイダ VDC に関連付けられているすべてのリソース プールを使用できます。	Flex
[仮想マシン メモリのオーバーヘッドを含める]	メモリのオーバーヘッドを含めるか、または除外します。	Flex
[CPU の割り当て]	この組織仮想データセンターで実行されている仮想マシンに割り当てる CPU の最大量。	<ul style="list-style-type: none"> ■ 割り当てプール ■ 予約プール ■ Flex
[CPU リソースを予約値を超えて拡張できるようにします]	この組織仮想データセンターに無制限の CPU リソースを提供するには、この切り替えを有効にします。	予約プール
[CPU 割り当て]	この組織仮想データセンターの CPU 使用量の最大値。	<ul style="list-style-type: none"> ■ 従量課金制 ■ Flex
[確保された CPU リソース]	この組織仮想データセンターで実行されている仮想マシンに確保する CPU リソースの割合。100% 未満を確保することで、CPU リソースのオーバーコミットメントを制御できます。 割り当てプールの割り当てモデルの場合、割合の確保によってこの組織仮想データセンターにコミットされる CPU の割り当ての割合も決定されます。	<ul style="list-style-type: none"> ■ 割り当てプール ■ 従量課金制 ■ Flex
[vCPU 速度]	vCPU 速度。組織仮想データセンターで実行されている仮想マシンには、vCPU あたりこの GHz 単位の速度が割り当てられます。	<ul style="list-style-type: none"> ■ 従量課金制 ■ Flex
[メモリの割り当て]	この組織仮想データセンターで実行されている仮想マシンに割り当てるメモリの最大容量。	<ul style="list-style-type: none"> ■ 割り当てプール ■ 予約プール
[メモリ制限]	この組織仮想データセンターのメモリ使用量の最大値。	<ul style="list-style-type: none"> ■ 従量課金制 ■ Flex
[確保されたメモリ リソース]	組織仮想データセンターで実行されている仮想マシンに確保するメモリ リソースの割合。100 パーセント未満を確保すると、リソースをオーバーコミットできます。 割り当てプールの割り当てモデルの場合、割合の確保によってこの組織仮想データセンターにコミットされるメモリの割り当ての割合も決定されます。	<ul style="list-style-type: none"> ■ 割り当てプール ■ 従量課金制 ■ Flex
[最大仮想マシン数]	組織仮想データセンターに配置できる仮想マシンの最大数。	<ul style="list-style-type: none"> ■ 割り当てプール ■ 従量課金制 ■ 予約プール ■ Flex

6 この組織仮想データセンターのストレージ設定を行って、[次へ] をクリックします。

リストには、ソース プロバイダ VDC で有効なストレージ ポリシーが含まれています。

- a 追加する 1 個以上のストレージ ポリシーを選択し、この組織 VDC に追加します。
- b (オプション) 選択したストレージ ポリシーに割り当てられたストレージ容量を制限するには、[割り当てタイプ] セルのドロップダウン メニューで [制限] を選択し、[割り当て済みストレージ] セルに最大容量を入力します。
- c (オプション) デフォルトのストレージ ポリシーを変更するには、[デフォルトのインスタンス化ポリシー] ドロップダウン メニューからターゲット デフォルト ストレージ ポリシーを選択します。

VMware Cloud Director は、ストレージ ポリシーが仮想マシンまたは vApp テンプレートのレベルで指定されていないすべての仮想マシンのプロビジョニング操作で、デフォルトのストレージ ポリシーを使用します。

- d (オプション) 組織 VDC 内の仮想マシンのシン プロビジョニングを有効にするには、[シン プロビジョニング] トグルをオンにします。
- e (オプション) 組織 VDC 内の仮想マシンの高速プロビジョニングを無効にするには、[高速プロビジョニング] トグルをオフにします。

7 (オプション) Edge Gateway を作成します。

- a 新しい Edge Gateway の名前と、オプションで説明を入力します。
- b NSX Data Center for vSphere でバックアップされる VDC のテンプレートを編集する場合は、一般的な Edge Gateway の設定をカスタマイズして、[次へ] をクリックします。

全般設定	説明
分散ルーティング	分散論理ルーティングを指定するように詳細ゲートウェイを構成します。
FIPS モード	NSX FIPS モードを使用するよう Edge ゲートウェイを構成します。
高可用性	バックアップ Edge ゲートウェイへの自動フェイルオーバーを有効にします。

- c NSX Data Center for vSphere によってバックアップされる VDC のテンプレートを編集する場合は、システム リソースの Edge Gateway 構成を変更します。

構成	説明
コンパクト	必要なメモリとコンピューティング リソースが少なく済みます。
大	[コンパクト] 設定よりも大きな容量と高いパフォーマンスを提供します。[大] 構成と [超特大] 構成では、同じセキュリティ機能が提供されます。
超特大	多数の同時セッションが実行される、ロード バランサを含む環境に使用します。
特大	スループットが多量である環境に使用します。高速な接続速度が必要です。

- d (オプション) ゲートウェイ サービスを使用するために割り当てる IP アドレスの数を指定します。

8 組織 VDC ネットワークを構成して、[次へ] をクリックします。

- 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 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。

- c 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] トグルをオンに切り替えます。

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、従量課金モデルのセカンダリ組織 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。

9 使用可能な固定 IP プールの範囲から IP アドレス範囲を追加して、[次へ] をクリックします。**10 (オプション) 組織 VDC のネットワーク プールの設定を行って、[次へ] をクリックします。**

割り当て容量とは、このネットワーク プールによってバックアップされる組織 VDC 内でプロビジョニングされるネットワークの最大数です。割り当て容量は、選択したネットワーク プールで使用可能なネットワーク数を超えることはできません。

11 このテンプレートから VDC を表示およびインスタンス化する組織を選択して、[次へ] をクリックします。**12 テンプレートのシステム名とテナント側の名前を入力して、[次へ] をクリックします。****13 組織 VDC テンプレートの構成を確認し、[完了] をクリックします。**

組織仮想データセンターの名前および説明の変更

VMware Cloud Director のインストール環境が拡大するにつれて、既存の組織仮想データセンターによりわかりやすい名前または説明を割り当てることが必要になる場合があります。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [組織 VDC] をクリックし、ターゲット組織仮想データセンターの名前をクリックします。
- 3 [全般] タブで、右上隅にある [編集] をクリックします。
- 4 新しい名前および説明を入力して、[保存] をクリックします。

組織仮想データセンターの割り当てモデルの設定の変更

組織仮想データセンターの割り当てモデルは変更できませんが、組織仮想データセンターの作成時に指定した割り当てモデルの割り当て設定は変更できます。

組織仮想データセンターの作成時に設定した割り当てモデルの割り当て設定は、変更が可能です。[手順 9](#) を参照してください。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [組織 VDC] をクリックし、ターゲット組織仮想データセンターの名前をクリックします。
- 3 [割り当て] タブで、右上隅にある [編集] をクリックします。
- 4 割り当てモデルの設定を編集し、[保存] をクリックします。

組織仮想データセンターのストレージ設定の変更

組織仮想データセンターの作成時に設定したストレージ設定は、変更が可能です。

組織仮想データセンターのストレージ ポリシーでの仮想マシン暗号化の有効化

暗号化が有効なストレージ ポリシーを組織 VDC に追加できます。仮想マシンおよびディスクを暗号化するには、仮想マシンの暗号化機能を備えたストレージ ポリシーに関連付けます。

VMware Cloud Director 10.1 以降では、仮想マシンの暗号化を使用してデータのセキュリティを強化できます。暗号化により、仮想マシンだけでなく仮想マシンのディスクやファイルも保護することができます。API およびユーザー インターフェイスで、ストレージ ポリシーの機能や、仮想マシンとディスクの暗号化ステータスを表示できます。それぞれの vCenter Server バージョンでサポートされている暗号化された仮想マシンとディスクには、すべての操作を実行できます。

仮想マシンの暗号化が有効になっているストレージ ポリシーがプロバイダ VDC に設定されている場合は、暗号化が有効なポリシーを組織 VDC に追加できます。[プロバイダ仮想データセンターのストレージ ポリシーでの仮想マシン暗号化の有効化](#)および[組織仮想データセンターへの仮想マシン ストレージ ポリシーの追加](#)を参照してください。その後、テナントは VMware Cloud Director Tenant Portal を使用して、仮想マシンの暗号化が有効になっているストレージ ポリシーを仮想マシンまたはディスクに関連付けることができます。

仮想マシンの暗号化に関する制限事項

VMware Cloud Director 10.1 では、次のアクションはサポートされていません。

- パワーオン状態の仮想マシンまたはそのディスクを暗号化または復号化します。
- 暗号化された仮想マシンの OVF をエクスポートします。
- 仮想マシンのディスクがスナップショットに含まれている場合に、このスナップショットを使用してディスクを暗号化および復号します。
- 仮想マシンのディスクが暗号化されたポリシーに含まれている場合に、仮想マシンを復号します。
- 暗号化されたディスクを暗号化されていない仮想マシンに追加します。
- 暗号化されていない仮想マシン上の既存のディスクを暗号化します。
- 暗号化された名前付きディスクを暗号化されていない仮想マシンに追加します。
- 暗号化されたリンク クローンを作成します。

- リンク クローン仮想マシンまたはそのディスクを暗号化します。
- ソース仮想マシンが暗号化されている場合に、vCenter Server インスタンス間で仮想マシンのインスタンス化、移動、またはクローン作成を行います。

注： 高速プロビジョニング済みの組織 VDC でソースまたはターゲット仮想マシンが暗号化されている場合に、クローンを作成すると、VMware Cloud Director は常にフル クローンを作成します。

仮想マシンの暗号化ストレージ機能の識別

システム管理者と組織管理者には、デフォルトで、組織 VDC のストレージ機能を表示し、仮想マシンとディスクが暗号化されているかどうかを参照するために必要な権限が設定されています。vApp 作成者は、仮想マシンとディスクの暗号化ステータスを参照できます。ロールおよび権限の詳細については、[事前定義ロールとその権限](#)を参照してください。

すべてのストレージ機能は、[リソース] - [vSphere リソース] - [ストレージ ポリシー] の [機能] 列で確認できます。この列には、仮想マシンの暗号化、タグベースの関連付け、vSAN、IOPS 制限ストレージ機能が表示されます。ストレージ機能の完全なリストを表示するには、ストレージ ポリシー名の左側にある矢印をクリックして行を展開します。

組織 VDC の [ストレージ] タブで、ストレージ機能の情報を表示することもできます。

組織仮想データセンターの仮想マシン プロビジョニング設定の変更

組織仮想データセンターを作成するときに設定した仮想マシンのシン プロビジョニングおよび高速プロビジョニングの設定を変更できます。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [組織 VDC] をクリックし、ターゲット組織仮想データセンターの名前をクリックします。
- 3 [ポリシー] で [ストレージ] を選択し、[編集] をクリックします。
- 4 (オプション) シン プロビジョニングの設定を変更します。
 - 組織仮想データセンター内の仮想マシンのシン プロビジョニングを無効にするには、[シン プロビジョニング] トグルをオフにします。
 - 組織仮想データセンター内の仮想マシンのシン プロビジョニングを有効にするには、[シン プロビジョニング] トグルをオンにします。
- 5 (オプション) 高速プロビジョニングの設定を変更します。
 - 組織仮想データセンター内の仮想マシンの高速プロビジョニングを有効にするには、[高速プロビジョニング] トグルをオンにします。
 - 組織仮想データセンター内の仮想マシンの高速プロビジョニングを無効にするには、[高速プロビジョニング] トグルをオフにします。
- 6 [[編集]]をクリックします。

組織仮想データセンターへの仮想マシン ストレージ ポリシーの追加

組織仮想データセンターを構成して、バックアップ プロバイダ仮想データセンターに以前追加した仮想マシン ストレージ ポリシーをサポートできます。

前提条件

ターゲットの仮想マシン ストレージ ポリシーをソース プロバイダ仮想データセンターに追加していること。[プロバイダ仮想データセンターへの仮想マシン ストレージ ポリシーの追加](#)を参照してください。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [組織 VDC] をクリックし、ターゲット組織仮想データセンターの名前をクリックします。
- 3 [ポリシー] で [ストレージ] を選択し、[追加] をクリックします。
ソース プロバイダ仮想データセンター内の、使用可能な追加ストレージ ポリシーのリストが表示されます。
- 4 追加する 1 個以上のストレージ ポリシーのチェック ボックスを選択して、[追加] をクリックします。

組織仮想データセンターのデフォルト ストレージ ポリシーの変更

組織仮想データセンターの作成時に設定したデフォルト ストレージ ポリシーを変更できます。

VMware Cloud Director は、ストレージ ポリシーが仮想マシンまたは vApp テンプレートのレベルで指定されていないすべての仮想マシンのプロビジョニング操作で、デフォルトのストレージ ポリシーを使用します。

前提条件

- ターゲット デフォルト ストレージ ポリシーが、組織仮想データセンターに追加されています。[組織仮想データセンターへの仮想マシン ストレージ ポリシーの追加](#)を参照してください。
- ターゲット デフォルト ストレージ ポリシーが、組織仮想データセンターで有効になっています。[組織仮想データセンター上のストレージ ポリシーの有効化または無効化](#)を参照してください。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [組織 VDC] をクリックし、ターゲット組織仮想データセンターの名前をクリックします。
- 3 [ポリシー] で [ストレージ] を選択します。
- 4 ターゲット デフォルト ストレージ ポリシーの名前の横にあるラジオ ボタンをクリックし、[デフォルトとして設定] をクリックします。
- 5 確認するには、[OK] をクリックします。

組織仮想データセンターのストレージ ポリシーの制限の編集

組織仮想データセンターの作成時にストレージ ポリシーに対して設定した、割り当て済みストレージ容量の制限を変更できます。

割り当て済みストレージ容量を無制限に設定するか、組織仮想データセンターのストレージ ポリシーに割り当てられるストレージ容量の最大値を設定することができます。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [組織 VDC] をクリックし、ターゲット組織仮想データセンターの名前をクリックします。
- 3 [ポリシー] で [ストレージ] を選択します。
- 4 対象のストレージ ポリシーの名前の横にあるラジオ ボタンをクリックして、[制限の編集] をクリックします。
- 5 このストレージ ポリシーの制限を構成します。
 - 制限を設定するには、上部のラジオ ボタンを選択し、この組織仮想データセンターのこのストレージ ポリシーに対するストレージ リソースの最大量を入力します。
 - 制限を設定しない場合は、[制限なし] ラジオ ボタンを選択します。
- 6 [[編集]] をクリックします。

組織仮想データセンター上の仮想マシン ストレージ ポリシーのメタデータの変更

組織仮想データセンター上のストレージ ポリシーのメタデータを追加、編集、または削除できます。

オブジェクト メタデータを使用すると、ユーザー定義の *name=value* ペアに、組織仮想データセンターのストレージ ポリシーを関連付けることができます。vCloud API クエリのフィルタ式内でオブジェクト メタデータを使用できます。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [組織 VDC] をクリックし、ターゲット組織仮想データセンターの名前をクリックします。
- 3 [ポリシー] で [ストレージ] を選択します。
- 4 対象のストレージ ポリシー名の横にあるラジオ ボタンをクリックして、[メタデータ] をクリックします。
- 5 [[編集]] をクリックします。
- 6 (オプション) キーと値のペアを追加するには、[追加] をクリックして、名前と値を入力し、新しいキーと値のペアのタイプを選択します。
- 7 (オプション) キーと値のペアを編集するには、新しい名前と値を入力し、キーと値のペアに新しいタイプを選択します。
- 8 (オプション) キーと値のペアを削除するには、行の右端にある [削除] アイコンをクリックします。
- 9 [保存] をクリックし、[OK] をクリックします。

組織仮想データセンター上のストレージ ポリシーの有効化または無効化

追加の vApp および仮想マシンに対して組織仮想データセンターのストレージ ポリシーの使用を禁止するには、組織仮想データセンターでこのストレージ ポリシーを無効にします。実行中の vApp およびパワーオンされた仮想マシンは継続して実行されますが、このストレージ ポリシーに関して追加の vApp または仮想マシンを作成したり開始したりすることはできません。

デフォルトのストレージ ポリシーを無効にすることはできません。

前提条件

デフォルトのストレージ ポリシーを無効にする場合は、[組織仮想データセンターのデフォルト ストレージ ポリシーの変更](#)。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [組織 VDC] をクリックし、ターゲット組織仮想データセンターの名前をクリックします。
- 3 [ポリシー] で [ストレージ] を選択します。
- 4 ターゲット ストレージ ポリシーの名前の横にあるラジオ ボタンをクリックして、[有効化] または [無効化] をクリックします。
- 5 確認するには、[OK] をクリックします。

組織仮想データセンターからの仮想マシン ストレージ ポリシーの削除

組織仮想データセンターがストレージ ポリシーを使用しないようにするには、このストレージ ポリシーを組織仮想データセンターから削除します。実行中の vApp およびパワーオンされた仮想マシンは継続して実行されますが、このストレージ ポリシーに関して追加の vApp または仮想マシンを作成したり開始したりすることはできません。

前提条件

削除するストレージ ポリシーを無効にします。[組織仮想データセンター上のストレージ ポリシーの有効化または無効化](#)を参照してください。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [組織 VDC] をクリックし、ターゲット組織仮想データセンターの名前をクリックします。
- 3 [ポリシー] で [ストレージ] を選択します。
- 4 対象のストレージ ポリシー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。
- 5 確認するには、[削除] をクリックします。

組織 VDC ストレージ ポリシーの設定の編集

組織 VDC ストレージ ポリシーの 1 秒あたりの I/O 処理数 (IOPS) の設定を変更できます。デフォルトでは、組織 VDC ストレージ ポリシーは、プロバイダ VDC ストレージ ポリシーの設定を継承します。組織 VDC ストレージ ポリシーごとに設定をカスタマイズできます。

前提条件**組織仮想データセンターへの仮想マシン ストレージ ポリシーの追加****手順**

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [組織 VDC] を選択し、ターゲット組織仮想データセンターの名前をクリックします。
- 3 [ポリシー] で [ストレージ] を選択します。
- 4 ターゲット ストレージ ポリシーの横にあるラジオ ボタンをクリックして、[設定の編集] をクリックします。
- 5 組織 VDC ストレージ ポリシーの IOPS 設定をプロバイダ VDC ストレージ ポリシーと異なる設定にするには、[プロバイダ VDC から継承] トグルをオフにします。
- 6 1 秒あたりの I/O 処理数を制限する場合は、[IOPS 制限が有効] トグルをオンにします。
- 7 配置中に IOPS が考慮されるようにする場合は、[影響のある配置] トグルをオンにします。

[影響のある配置] トグルがオンになっている場合、VMware Cloud Director はデータストア間で IOPS のロード バランシングを行います。ディスクの IOPS 設定を行うときに、VMware Cloud Director は選択したディスクに必要な IOPS キャパシティを持つデータストアを考慮します。[影響のある配置] トグルがオフになっている場合は、データストアごとに IOPS キャパシティを設定する必要はありません。Storage DRS クラスタを使用することができます。

- 8 (オプション) 最大およびデフォルトの IOPS 設定を行います。
- 9 [保存] をクリックします。

組織仮想データセンターのネットワーク設定の編集

組織仮想データセンターで新しいネットワークをプロビジョニングする場合のプロビジョニング元になるネットワーク プールを変更できます。組織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することもできます。

ネットワーク プールは、vApp ネットワーク、経路指定された組織 VDC ネットワーク、および内部の組織 VDC ネットワークを作成するための、区別されていないネットワークのグループです。新しいネットワークのネットワーク プールを変更できます。既存のネットワークでは、引き続き古いネットワーク プールが使用されます。

クロス仮想データセンター ネットワークが有効な組織仮想データセンターを使用すると、関連する権限を持つ組織ユーザーは、データセンター グループを作成し、これらのグループに拡張レイヤー 2 ネットワークを作成することができます。

前提条件

組織仮想データセンターでクロス VDC ネットワークを有効にする場合は、バックアップ プロバイダ仮想データセンターに対して Cross-vCenter NSX が構成されていることを確認します。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。

- 2 左側のパネルで [組織 VDC] をクリックし、ターゲット組織仮想データセンターの名前をクリックします。
- 3 [ネットワーク プール] タブで、右上隅にある [編集] をクリックします。

この組織仮想データセンターによって使用されているネットワークの数が表示されます。

- 4 (オプション) この組織仮想データセンターのネットワーク プールを構成します。

注: NSX-T Data Center によってバックアップされている組織 VDC は Geneve ネットワーク プールのみをサポートします。

- この組織仮想データセンターのネットワーク プールを使用しない場合は、[ネットワーク プールを使用] 切り替えを無効にします。
- この組織仮想データセンターにネットワーク プールを構成する場合は、次の手順を実行します。
 - a [ネットワーク プールを使用] 切り替えを有効にします。
 使用可能なネットワーク プールのリストが、これらの使用状況、使用可能なネットワーク、および容量に関する情報と共に表示されます。
 - b ターゲット リソース プールの名前の横にあるラジオ ボタンを選択します。
 - c この組織仮想データセンター内のこのネットワーク プールの割り当てを構成します。
 割り当てとは、プロビジョニングされたネットワークの最大数のことです。選択したネットワーク プールで使用可能なネットワーク数を超えることはできません。

- 5 この組織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するには、[クロス VDC ネットワーク] をオンにします。
- 6 [保存] をクリックします。

結果

VMware Cloud Director テナント ポータルのデータセンターのリストに、クロス仮想データセンター ネットワークが有効な仮想データセンターが表示され、データセンター グループを作成することができます。データセンター グループの作成の詳細については、『VMware Cloud Director Tenant Portal Guide』を参照してください。

クロス仮想データセンター ネットワークの構成

クロス仮想データセンター ネットワーク機能を利用すると、複数の vCenter Server インスタンスによってバックアップされた仮想データセンターを持つ組織は、レイヤー 2 ネットワークを最大で 4 つの仮想データセンターにまたがって拡張することが可能になります。クロス仮想データセンター ネットワークは、Cross-vCenter NSX を使用し、複数の VMware Cloud Director サイトにまたがることができます。

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。

クロス仮想データセンター ネットワークを使用すると、組織は最大で 4 つの仮想データセンターをグループ化し、各グループに出力方向とレイヤ 2 拡張ネットワークを設定できます。

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

組織はクロス仮想データセンター ネットワークを使用して、高可用性ソリューションまたは分散システム アーキテクチャを実装することが可能となり、複数の仮想データセンターまたはサイト間でアプリケーションを配布することができます。

システム管理者は、基盤となる Cross-vCenter NSX 環境と VMware Cloud Director サーバを構成して、各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する必要があります。

- 1 NSX Manager インスタンスの 1 つをプライマリ NSX Manager インスタンスとして設定します。『Cross-vCenter NSX インストール ガイド』を参照してください。
 - a プライマリ NSX Manager インスタンスに NSX クラスタをデプロイします。
 - b プライマリ NSX Manager インスタンスに ESXi ホストを準備します。
 - c プライマリ NSX Manager インスタンスからの VXLAN を構成します。
 - d NSX Manager インスタンスにプライマリ ロールを割り当てます。
 - e ユニバーサル トランスポート ゾーン用のセグメント IP アドレスのプールを作成します。
 - f ユニバーサル トランスポート ゾーンを追加します。
- 2 他の NSX Manager インスタンスをセカンダリ NSX Manager として設定します。『Cross-vCenter NSX インストール ガイド』を参照してください。
 - a 各セカンダリ NSX Manager インスタンスに ESXi ホストを準備します。
 - b 各セカンダリ NSX Manager インスタンスからの VXLAN を構成します。
 - c 各 NSX Manager インスタンスにセカンダリ ロールを割り当てます。
 - d ESXi クラスタをユニバーサル トランスポート ゾーンに接続します。
- 3 各 NSX Manager インスタンスのコントロール仮想マシンのプロパティを構成します。『[NSX Manager 設定の変更](#)』を参照してください。
- 4 任意の vCenter Server インスタンスからユニバーサル タイプのトランスポート ゾーンを使用して VXLAN でバックアップされたネットワーク プールを作成します。[NSX Data Center for vSphere トランスポート ゾーンによってバックアップされるネットワーク プールの作成](#)を参照してください。

注： マルチサイト展開では、VMware Cloud Director サイトごとに VXLAN でバックアップされたネットワーク プールを作成する必要があります。

- 5 各組織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ます。『[組織仮想データセンターのネットワーク設定の編集](#)』を参照してください。
- 6 組織にマルチサイトの仮想データセンターがある場合、各 VMware Cloud Director サイトのインストール ID が異なっていることを確認します。同じインストール ID が設定された VMware Cloud Director サイトがある場合は、VMware Cloud Director インストール、構成、およびアップグレード ガイドの「[マルチサイト拡張ネットワークの MAC アドレスの再生成](#)」を参照してください。

これにより、組織管理者はデータセンター グループ、出力方向、拡張ネットワークの作成と構成ができるようになります。クロス仮想データセンター ネットワークの管理については、『VMware Cloud Director Tenant Portal Guide』を参照してください。

組織仮想データセンターのメタデータの変更

組織仮想データセンターのメタデータを追加、編集、または削除できます。

オブジェクト メタデータを使用すると、ユーザー定義の *name=value* ペアに、組織仮想データセンターを関連付けることができます。vCloud API クエリのフィルタ式内でオブジェクト メタデータを使用できます。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [組織 VDC] をクリックし、ターゲット組織仮想データセンターの名前をクリックします。
- 3 [メタデータ] タブをクリックします。
- 4 [[編集]] をクリックします。
- 5 (オプション) キーと値のペアを追加するには、[追加] をクリックして、名前と値を入力し、新しいキーと値のペアのタイプを選択します。
- 6 (オプション) キーと値のペアを編集するには、新しい名前と値を入力し、キーと値のペアに新しいタイプを選択します。
- 7 (オプション) キーと値のペアを削除するには、行の右端にある [削除] アイコンをクリックします。
- 8 [保存] をクリックし、[OK] をクリックします。

組織仮想データセンターのリソース プールの表示

組織仮想データセンターで使用する vCenter Server リソース プールのリストを表示できます。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [組織 VDC] をクリックし、ターゲット組織仮想データセンターの名前をクリックします。
- 3 [リソース プール] タブをクリックします。

結果

組織仮想データセンターで使用されているリソース プール、および各リソース プールが属する vCenter Server インスタンスが示されたテーブルが表示されます。

組織仮想データセンターの分散ファイアウォールの管理

組織仮想データセンターでレイヤー 3 およびレイヤー 2 ネットワーク セキュリティを提供するには、この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して、そのルールを作成します。分散ファイアウォール ルールが有効な場合は、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を保護できます。

VMware Cloud 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。

分散ファイアウォール ルールを作成する場合は、さまざまなグループ オブジェクトとセキュリティ グループを使用できます。[オブジェクトのグループ分け（カスタム）](#) および [セキュリティ グループの操作](#) を参照してください。

Edge Gateway との間で送受信されるトラフィックの保護については、[NSX Data Center for vSphere Edge Gateway ファイアウォールの管理](#)を参照してください。

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設定を管理するには、この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しておく必要があります。

VMware Cloud 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。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [組織 VDC] をクリックします。
- 3 ターゲット組織仮想データセンターの横にあるラジオ ボタンをクリックして、[ファイアウォールの管理] をクリックします。
- 4 [分散ファイアウォール] - [全般] タブで [分散ファイアウォールの有効化] 切り替えを有効にします。

結果

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た、デフォルトのファイアウォール ルールが表示されます。

- [分散ファイアウォール] - [全般] タブに、レイヤー 3 トラフィックのデフォルトの分散ファイアウォール ルール（名前付きのデフォルトの許可ルール）が表示されます。
- [分散ファイアウォール] - [イーサネット] タブに、レイヤー 2 トラフィックのデフォルトの分散ファイアウォール ルール（名前付きのデフォルトの許可ルール）が表示されます。

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

- [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 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [組織 VDC] をクリックします。
- 3 ターゲット組織仮想データセンターの横にあるラジオ ボタンをクリックして、[ファイアウォールの管理] をクリックします。
- 4 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。

- 5 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。

- 6 [名前] セルをクリックし、名前を入力します。
- 7 [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>

8 [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>

9 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> <ol style="list-style-type: none"> サービス プロトコルを選択します。 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> <ol style="list-style-type: none"> 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。 [保持] をクリックします。

10 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。

11 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。

12 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。

13 [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。

14 [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

VMware Cloud 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 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [組織 VDC] をクリックします。
- 3 ターゲット組織仮想データセンターの横にあるラジオ ボタンをクリックして、[ファイアウォールの管理] をクリックします。
- 4 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。
- 5 [変更を保存] をクリックします。

オブジェクトのグループ分け（カスタム）

NSX 環境の VMware Cloud 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、[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。このページを開くには、組織 VDC の分散ファイアウォール設定に移動するか、組織 VDC に属する Edge ゲートウェイのサービス設定に移動する必要があります。


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
組織 VDC の分散ファイアウォール設定から	<ol style="list-style-type: none"> a 上部ナビゲーション バーの [リソース] で [クラウド リソース] を選択します。 b 左側のパネルで [組織 VDC] をクリックします。 c ターゲット組織仮想データセンターの名前の横にあるラジオ ボタンを選択して、[ファイアウォールの管理] をクリックします。 d [オブジェクトのグループ分け] タブをクリックします。
組織 VDC の Edge Gateway のサービス設定から	<ol style="list-style-type: none"> a 上部ナビゲーション バーの [リソース] で [クラウド リソース] を選択します。 b 左側のパネルで [Edge Gateway] をクリックします。 c ターゲット組織仮想データセンターに属する Edge Gateway の名前の横にあるラジオ ボタンを選択して、[サービス] をクリックします。 d [オブジェクトのグループ分け] タブをクリックします。

- 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 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 セットを作成するには、[オブジェクトのグループ分け] 画面を使用します。この画面を開くには、組織 VDC の分散ファイアウォール設定に移動するか、組織 VDC に属する Edge Gateway のサービス設定に移動する必要があります。


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
組織 VDC の分散ファイアウォール設定から	<ol style="list-style-type: none"> a 上部ナビゲーション バーの [リソース] で [クラウド リソース] を選択します。 b 左側のパネルで [組織 VDC] をクリックします。 c ターゲット組織仮想データセンターの名前の横にあるラジオ ボタンを選択して、[ファイアウォールの管理] をクリックします。 d [オブジェクトのグループ分け] タブをクリックします。
組織 VDC の Edge Gateway のサービス設定から	<ol style="list-style-type: none"> a 上部ナビゲーション バーの [リソース] で [クラウド リソース] を選択します。 b 左側のパネルで [Edge Gateway] をクリックします。 c ターゲット組織仮想データセンターに属する Edge Gateway の名前の横にあるラジオ ボタンを選択して、[サービス] をクリックします。 d [オブジェクトのグループ分け] タブをクリックします。

- 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 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 ルールで使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。

使用可能なサービスを表示するには、[オブジェクトのグループ分け] 画面を使用します。この画面を開くには、組織 VDC の分散ファイアウォール設定に移動するか、組織 VDC に属する Edge Gateway のサービス設定に移動する必要があります。

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
組織 VDC の分散ファイアウォール設定から	<ol style="list-style-type: none"> 上部ナビゲーション バーの [リソース] で [クラウド リソース] を選択します。 左側のパネルで [組織 VDC] をクリックします。 ターゲット組織仮想データセンターの名前の横にあるラジオ ボタンを選択して、[ファイアウォールの管理] をクリックします。 [オブジェクトのグループ分け] タブをクリックします。
組織 VDC の Edge Gateway のサービス設定から	<ol style="list-style-type: none"> 上部ナビゲーション バーの [リソース] で [クラウド リソース] を選択します。 左側のパネルで [Edge Gateway] をクリックします。 ターゲット組織仮想データセンターに属する Edge Gateway の名前の横にあるラジオ ボタンを選択して、[サービス] をクリックします。 [オブジェクトのグループ分け] タブをクリックします。

- 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。

使用可能なサービス グループを表示するには、[オブジェクトのグループ分け] 画面を使用します。この画面を開くには、組織 VDC の分散ファイアウォール設定に移動するか、組織 VDC に属する Edge Gateway のサービス設定に移動する必要があります。

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
組織 VDC の分散ファイアウォール設定から	<ol style="list-style-type: none"> 上部ナビゲーション バーの [リソース] で [クラウド リソース] を選択します。 左側のパネルで [組織 VDC] をクリックします。 ターゲット組織仮想データセンターの名前の横にあるラジオ ボタンを選択して、[ファイアウォールの管理] をクリックします。 [オブジェクトのグループ分け] タブをクリックします。
組織 VDC の Edge Gateway のサービス設定から	<ol style="list-style-type: none"> 上部ナビゲーション バーの [リソース] で [クラウド リソース] を選択します。 左側のパネルで [Edge Gateway] をクリックします。 ターゲット組織仮想データセンターに属する Edge Gateway の名前の横にあるラジオ ボタンを選択して、[サービス] をクリックします。 [オブジェクトのグループ分け] タブをクリックします。

- 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。

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 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [組織 VDC] をクリックします。
- 3 ターゲット組織仮想データセンターの横にあるラジオ ボタンをクリックして、[ファイアウォールの管理] をクリックします。
- 4 [オブジェクトのグループ分け] - [セキュリティ グループ] タブをクリックします。

- 5 [作成] () ボタンをクリックします。

- 6 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。

- 7 (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。

8 (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。

9 (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。

10 変更内容を保持するには、[保持] をクリックします。

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 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。

2 左側のパネルで [組織 VDC] をクリックします。

3 ターゲット組織仮想データセンターの横にあるラジオ ボタンをクリックして、[ファイアウォールの管理] をクリックします。

4 [オブジェクトのグループ分け] - [セキュリティ グループ] タブをクリックします。

5 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。

6 (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。

7 (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。
- 8 (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。
- 9 (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。
- 10 (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。
- 11 (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。
- 12 [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 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [組織 VDC] をクリックします。
- 3 ターゲット組織仮想データセンターの横にあるラジオ ボタンをクリックして、[ファイアウォールの管理] をクリックします。
- 4 [オブジェクトのグループ分け] - [セキュリティ グループ] タブをクリックします。
- 5 削除するセキュリティ グループを選択します。
- 6 [削除] () ボタンをクリックします。
- 7 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。

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 ルールで使用できるセキュリティ 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 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [組織 VDC] をクリックします。
- 3 ターゲット組織仮想データセンターの横にあるラジオ ボタンをクリックして、[ファイアウォールの管理] をクリックします。
- 4 [セキュリティ タグ] タブをクリックします。

5 [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。

6 (オプション) セキュリティ タグの説明を入力します。

7 (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。

8 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 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。

2 左側のパネルで [組織 VDC] をクリックします。

3 ターゲット組織仮想データセンターの横にあるラジオ ボタンをクリックして、[ファイアウォールの管理] をクリックします。

4 [セキュリティ タグ] タブをクリックします。

5 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。

6 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。

7 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。

8 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 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [組織 VDC] をクリックします。
- 3 ターゲット組織仮想データセンターの横にあるラジオ ボタンをクリックして、[ファイアウォールの管理] をクリックします。
- 4 [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。
- 5 [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、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 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [組織 VDC] をクリックします。
- 3 ターゲット組織仮想データセンターの横にあるラジオ ボタンをクリックして、[ファイアウォールの管理] をクリックします。
- 4 [セキュリティ タグ] タブをクリックします。
- 5 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。
- 6 [編集] () ボタンをクリックします。
- 7 セキュリティ タグの名前と説明を編集します。
- 8 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。
- 9 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 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [組織 VDC] をクリックします。
- 3 ターゲット組織仮想データセンターの横にあるラジオ ボタンをクリックして、[ファイアウォールの管理] をクリックします。
- 4 [セキュリティ タグ] タブをクリックします。

5 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。

6 [削除] () ボタンをクリックします。

7 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。

NSX Data Center for vSphere Edge Gateway の管理

7

NSX Data Center for vSphere Edge Gateway は、経路指定された組織仮想データセンター ネットワークに対し、外部ネットワークへの接続を提供し、ロード バランシング、ネットワーク アドレス変換、ファイアウォールなどのサービスを提供できます。VMware Cloud Director は、IPv4 および IPv6 の Edge ゲートウェイをサポートします。

VMware Cloud Director 9.7 以降では、さまざまな vSphere リソース プールおよびストレージ ポリシーを使用して、コンピューティング ワークロードとネットワーク ワークロードが隔離されます。Edge Gateway が配置される Edge クラスタは、以前は作成が必須でした。NSX Data Center for vSphere Edge クラスタの操作を参照してください。

これらの Edge Gateway を再デプロイすることで、レガシーの Edge Gateway を対応する Edge クラスタに移行できます。Edge Gateway の再デプロイを参照してください。

重要： バージョン 9.7 以降では、VMware Cloud Director でサポートされるのは詳細 Edge Gateway のみです。詳細以外のレガシー Edge Gateway を詳細 Edge Gateway に変換する必要があります。<https://kb.vmware.com/kb/66767> 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。

- NSX Data Center for vSphere Edge クラスタの操作
- NSX Data Center for vSphere Edge Gateway の追加
- NSX Data Center for vSphere Edge Gateway サービスの構成
- Edge Gateway のネットワーク使用と IP 割り当ての表示
- Edge ゲートウェイのプロパティの編集
- Edge Gateway の再デプロイ
- Edge ゲートウェイの削除
- 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

NSX Data Center for vSphere Edge クラスタの操作

VMware Cloud Director では、コンピューティング ワークロードをネットワーク ワークロードから隔離するために Edge クラスタ オブジェクトがサポートされています。Edge クラスタは、vSphere リソースプールと、組織仮

想データセンターの Edge Gateway 専用のストレージ ポリシーで構成されます。プロバイダ仮想データセンターは、Edge クラスタ専用のリソースを使用できず、Edge クラスタはプロバイダ仮想データセンター専用のリソースを使用できません。

Edge クラスタには専用の L2 ブロードキャスト ドメインが用意されていて、これにより VLAN のスプロールを抑え、ネットワークのセキュリティおよび隔離を確実に実現できます。たとえば、Edge クラスタに物理ルーターとのピアリング用の追加の VLAN を含めることができます。

作成できる Edge クラスタ数に制限はありません。Edge クラスタを組織仮想データセンターに割り当てる場合は、プライマリ Edge クラスタまたはセカンダリ Edge クラスタとして割り当てることができます。

- 組織仮想データセンターのプライマリ Edge クラスタは、組織 VDC Edge Gateway のメインの Edge アプライアンスとして使用されます。
- Edge Gateway が HA モードになっている場合は、組織仮想データセンターのセカンダリ Edge クラスタがスタンバイ Edge アプライアンスとして使用されます。

複数の組織仮想データセンターで Edge クラスタを共有することも、独自の専用 Edge クラスタを設定することもできます。

vCloud Director 9.7 以降では、メタデータを使用して Edge Gateway の配置を制御する以前のプロセスは廃止されています。<https://kb.vmware.com/kb/2151398> を参照してください。

これらの Edge Gateway を再デプロイすることで、レガシーの Edge Gateway を新しく作成された Edge クラスタに移行できます。[Edge Gateway の再デプロイ](#)を参照してください。

Edge クラスタの環境の準備

- 1 vSphere で、ターゲット Edge クラスタのリソース プールを作成します。

組織仮想データセンターで VLAN ネットワーク プールが使用されている場合は、この組織仮想データセンターの VLAN ネットワーク プールおよび Edge クラスタが同じ vSphere Distributed Switch に配置されている必要があります。

- 2 組織仮想データセンターで VXLAN ネットワーク プールが使用されている場合は、NSX で、VXLAN トランスポート ゾーンに Edge クラスタを追加し、その後で VMware Cloud Director の VXLAN ネットワーク プールを同期します。

- 3 vSphere で、Edge クラスタ ストレージ プロファイルを作成します。

Edge クラスタの作成と管理

環境の準備を行った後に、Edge クラスタを作成および管理するには、VMware Cloud Director OpenAPI の `EdgeClusters` メソッドを使用する必要があります。<https://code.vmware.com> にある VMware Cloud Director OpenAPI のスタート ガイドを参照してください。

Edge クラスタを表示するには、Edge クラスタの表示権限が必要です。Edge クラスタの作成、更新、および削除には、Edge クラスタの管理権限が必要です。

Edge クラスタを作成するときに、名前、vSphere リソース プール、およびストレージ プロファイル名を指定します。

Edge クラスタを作成した後で、名前と説明を変更できます。含まれている Edge ゲートウェイを削除または移動した後で、Edge クラスタを削除できます。

組織仮想データセンターへの Edge クラスタの割り当て

Edge クラスタを作成した後で、組織仮想データセンター ネットワーク プロファイルを更新して、この Edge クラスタを組織仮想データセンターに割り当てることができます。Edge クラスタを組織仮想データセンターに割り当てる場合は、プライマリ Edge クラスタまたはセカンダリ Edge クラスタとして割り当てることができます。

セカンダリ Edge クラスタを割り当てない場合は、HA モードの Edge Gateway のスタンバイ Edge アプライアンスがプライマリ Edge クラスタにデプロイされますが、プライマリ Edge アプライアンスを実行しているホストとは異なるホストに配置されます。

組織仮想データセンター ネットワーク プロファイルを更新、表示、および削除するには、VMware Cloud Director OpenAPI の `VdcNetworkProfile` メソッドを使用する必要があります。<https://code.vmware.com> にある VMware Cloud Director OpenAPI のスタート ガイドを参照してください。

考慮事項：

- プライマリおよびセカンダリ Edge クラスタは、同じ vSphere Distributed Switch に配置する必要があります。
- 組織仮想データセンターで VXLAN ネットワーク プールが使用されている場合、NSX トランスポート ゾーンはコンピューティング クラスタと Edge クラスタにまたがって配置されている必要があります。
- 組織仮想データセンターで VLAN ネットワーク プールが使用されている場合、Edge クラスタおよびコンピューティング クラスタは同じ vSphere Distributed Switch に配置されている必要があります。

組織仮想データセンターのプライマリ Edge クラスタまたはセカンダリ Edge クラスタを再度更新して既存の Edge Gateway を新しいクラスタに移動する場合、この Edge Gateway を再デプロイする必要があります。[Edge Gateway の再デプロイ](#)を参照してください。

NSX Data Center for vSphere Edge Gateway の追加

NSX Data Center for vSphere Edge Gateway は、経路指定の組織 VDC ネットワークに対し、外部ネットワークへの接続を提供し、ロードバランシング、ネットワーク アドレス変換、ファイアウォールなどのサービスを提供できます。

VMware Cloud Director 9.7 以降、NSX Data Center for vSphere Edge Gateway は、事前に作成されて組織 VDC に割り当てられた Edge クラスタにデプロイされます。

1 つ以上の外部ネットワークに接続する IPv4 または IPv6 Edge ゲートウェイを追加できます。

注： IPv6 Edge ゲートウェイ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、固定ルーティングをサポートします。

前提条件

- NSX Data Center for vSphere Edge Gateway をデプロイするためのシステム要件の詳細については、『NSX 管理ガイド』を参照してください。

- 専用の Edge クラスタに Edge Gateway をデプロイする場合は、Edge クラスタを作成して、組織仮想データセンターに割り当てます。 [NSX Data Center for vSphere Edge クラスタの操作](#) を参照してください。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のペインで、[Edge ゲートウェイ] をクリックし、[新規] をクリックします。
- 3 Edge Gateway を作成する、NSX-V によってバックアップされる組織仮想データセンターを選択し、[次へ] をクリックします。
- 4 新しい Edge Gateway の名前と、オプションで説明を入力します。
- 5 全般的な Edge ゲートウェイの設定をそれぞれ有効にするか、無効のままにします。

全般設定	説明
分散ルーティング	分散論理ルーティングを指定するよう Edge ゲートウェイを構成します。
FIPS モード	NSX FIPS モードを使用するよう Edge ゲートウェイを構成します。
高可用性	バックアップ Edge ゲートウェイへの自動フェイルオーバーを有効にします。

- 6 システム リソースの Edge ゲートウェイ構成を選択して、[次へ] をクリックします。

構成	説明
コンパクト	必要なメモリとコンピューティング リソースが少なく済みます。
大	[コンパクト] 設定よりも大きな容量と高いパフォーマンスを提供します。[大] 構成と [超特大] 構成では、同じセキュリティ機能が提供されます。
超特大	多数の同時セッションが実行される、ロード バランサを含む環境に使用します。
特大	スループットが多量である環境に使用します。高速な接続速度が必要です。

- 7 Edge ゲートウェイが接続できる外部ネットワークから 1 つ以上のサブネットを選択し、[次へ] をクリックします。

Edge クラスタが組織仮想データセンターに割り当てられていると、表示されるリストには、この Edge クラスタからアクセス可能な外部ネットワークが含まれます。

- 8 (オプション) ネットワークをデフォルト ゲートウェイとして構成します。
 - a [デフォルト ゲートウェイの構成] 切り替えを有効にします。
 - b ターゲット外部ネットワークの名前の横にあるラジオ ボタンをクリックし、ターゲット IP アドレスの横にあるラジオ ボタンをクリックします。
 - c (オプション) [DNS リレーにデフォルト ゲートウェイを使用] 切り替えを有効にします。
- 9 [次へ] をクリックします。

- 10 詳細 Edge ゲートウェイの設定をそれぞれ有効にするか、無効のままにして、[次へ] をクリックします。

詳細設定	説明
IP アドレス設定	Edge Gateway の各サブネットの IP アドレスを手動で入力できます。
IP プールの細分割り当て	Edge ゲートウェイ上の各外部ネットワークの使用可能な IP アドレス プールを複数の固定 IP アドレス プールに細分割り当てすることができます。
レート制限	Edge ゲートウェイのそれぞれの外部ネットワークについて着信および発信のレート制限を設定できます。

- 11 (オプション) 手順 手順 10 で 1 つ以上の詳細設定を有効にした場合は、有効にした各設定を適用します。

詳細設定	ステップ
[IP アドレス設定]	Edge Gateway のネットワークごとに、[IP アドレス] セルに IP アドレスを入力し、[次へ] をクリックします。 ネットワークの IP アドレスを入力しない場合は、このネットワークに任意の IP アドレスが割り当てられます。
[IP プールの細分割り当て]	<ol style="list-style-type: none"> 外部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。 この外部ネットワークに使用可能な IP アドレス プールと、現在細分割り当てされている IP アドレス プール（設定されている場合）が表示されます。 この外部ネットワークに細分割り当てされている IP アドレス プールを編集し、[保存] をクリックします。 使用可能な IP アドレス プールの範囲から IP アドレスと IP アドレス範囲を追加できます。 [保存] をクリックします。 システムは重複する IP アドレス範囲を結合します。 [次へ] をクリックします。 <p>注: Edge Gateway への IP アドレスの割り当ては、プロバイダが IP アドレスの所有権をゲートウェイに割り当てるプロセスです。VMware Cloud Director の割り当てプロセス中に、該当するゲートウェイ インターフェイスにセカンダリ アドレスが自動的に設定されます。IP アドレスのいずれかが VMware Cloud Director の外部で使用されている場合は、IP アドレスが競合する可能性があります。</p>
[レート制限]	Edge Gateway 上の外部ネットワークごとに、[有効化] 切り替えを有効にし、[着信レート] セルおよび [発信レート] セルに制限を入力して、[次へ] をクリックします。

- 12 [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。

NSX Data Center for vSphere Edge Gateway 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)、VPN などのサービスを、Edge Gateway に構成できます。

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、[組織仮想データセンターの分散ファイアウォールの管理](#)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] トグルを使用して、Edge Gateway ファイアウォールを無効または有効にします。

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

- 1 Edge Gateway サービスを開きます。
 - a 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] タブをクリックします。
 - b 左側のパネルで [Edge Gateway] をクリックします。
 - c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[サービス] をクリックします。
- 2 [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。
- 3 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。
- 4 [名前] セルをクリックし、名前を入力します。

- 5 [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

1 Edge Gateway サービスを開きます。

- a 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] タブをクリックします。
- b 左側のパネルで [Edge Gateway] をクリックします。
- c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[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。

NSX Data Center for vSphere Edge Gateway への Syslog サーバ設定の適用

1 つ以上の Edge Gateway ファイアウォール ルールのログを有効にした場合、Edge Gateway は Syslog サーバに接続されます。Syslog サーバの初期構成の前に Edge Gateway を作成した場合、または Syslog サーバの設定を変更した場合は、この Edge Gateway の Syslog サーバ設定を同期する必要があります。

手順

1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。

- 2 左側のパネルで [Edge Gateway] をクリックします。
- 3 ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[Syslog の同期] をクリックします。
- 4 確認するには、[OK] をクリックします。

NSX Data Center for vSphere 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 を構成します。

[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 が有効な Edge Gateway 上の DNS 設定を変更すると、Edge Gateway は DHCP サービスの提供を停止します。この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] トグルを使用して、その Edge Gateway 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 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] タブをクリックします。
 - b 左側のパネルで [Edge Gateway] をクリックします。
 - c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[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

VMware Cloud 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

- Edge Gateway サービスを開きます。
 - 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] タブをクリックします。
 - 左側のパネルで [Edge Gateway] をクリックします。
 - ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[サービス] をクリックします。
- [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。

オプション	説明
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

VMware Cloud 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、VMware Cloud 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 のサブネットに 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

VMware Cloud Director 環境内の NSX ソフトウェアにより、Edge Gateway は VMware Cloud 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

- Edge Gateway サービスを開きます。
 - 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] タブをクリックします。
 - 左側のパネルで [Edge Gateway] をクリックします。
 - ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[サービス] をクリックします。
- [DHCP] - [リレー] の順に移動します。
- 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。

- 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。

- [変更を保存] をクリックします。

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

VMware Cloud 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 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] タブをクリックします。
 - b 左側のパネルで [Edge Gateway] をクリックします。
 - c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[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）を構成します。

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 アドレスを入力するか、リストから割り当てられた IP アドレスを選択します。 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。

オプション	説明
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。
ソース IP アドレス	ルールを特定のドメインのトラフィックにのみ適用する場合、このドメインの IP アドレスまたは IP アドレス範囲を CIDR 形式で入力します。このテキスト ボックスを空白のままにすると、DNAT ルールはローカル サブネット内のすべての IP アドレスに適用されます。
ソース ポート	(オプション) ソースのポート番号を入力します。
説明	(オプション) DNAT ルールのわかりやすい説明を入力します。
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）を構成します。

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 アドレスの範囲を入力するか、割り当てられた IP アドレスをリストから選択します。 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。
ターゲット IP アドレス	(オプション) ルールを特定のドメインへのトラフィックにのみ適用する場合、このドメインの IP アドレスまたは IP アドレス範囲を CIDR 形式で入力します。このテキスト ボックスを空白のままにすると、SNAT ルールはローカル サブネット外のすべてのターゲットに適用されます。
ターゲット ポート	(オプション) ターゲットのポート番号を入力します。
説明	(オプション) SNAT ルールのわかりやすい説明を入力します。
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 NSX Data Center for vSphere 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 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] タブをクリックします。
 - b 左側のパネルで [Edge Gateway] をクリックします。
 - c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[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している必要があります。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 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] タブをクリックします。
 - b 左側のパネルで [Edge Gateway] をクリックします。
 - c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[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している必要があります。 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 ルートを経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。VMware Cloud Director 環境に置かれた Edge

ゲートウェイの OSPF は、一般に、VMware Cloud 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 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] タブをクリックします。
 - b 左側のパネルで [Edge Gateway] をクリックします。
 - c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[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 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] タブをクリックします。
 - b 左側のパネルで [Edge Gateway] をクリックします。
 - c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[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。

オプション	説明
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思なして、このネイバーからルートを削除します。</p>
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

- 1 Edge Gateway サービスを開きます。
 - a 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] タブをクリックします。
 - b 左側のパネルで [Edge Gateway] をクリックします。
 - c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[サービス] をクリックします。
- 2 [ルーティング] - [ルートの再分散] に移動します。
- 3 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、リソース使用の最適化、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。

NSX ロード バランサは、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、高速バ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、バックエンド 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。

NSX Data Center for vSphere 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 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] タブをクリックします。
 - b 左側のパネルで [Edge Gateway] をクリックします。
 - c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[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。

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 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] タブをクリックします。
- b 左側のパネルで [Edge Gateway] をクリックします。
- c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[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 バススルーの有効化	クリックすると、仮想サーバに対し、SSL 認証のバ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。
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ったとそのクライアントを同じプール メンバーに返します。</p> <ul style="list-style-type: none"> ■ [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ことです。</p> <ul style="list-style-type: none"> ■ [SSL セッション ID] <p>SSL バ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	(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。

オプション	説明
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=0I24B9ASD7BSSD</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。
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 パ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>

オプション	説明
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	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。 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。

7 変更内容を保持するには、[保持] をクリックします。


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。
 - 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] タブをクリックします。
 - 左側のパネルで [Edge Gateway] をクリックします。
 - ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[サービス] をクリックします。
- [ロード バランサー] > [サービス監視] の順に移動します。
- [作成] () ボタンをクリックします。
- サービス監視の名前を入力します。
- (オプション) サービス監視に関する次のオプションを構成します。

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）。

オプション	説明
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 変更内容を保持するには、[保持] をクリックします。

例：各プロトコルでサポートされる拡張機能

表 7-1. 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= <i>SECONDS</i>	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= <i>STRING</i>	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= <i>STRING</i> または ereg= <i>STRING</i>	正規表現の STRING をページで検索します。
eregi= <i>STRING</i>	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= <i>AUTH_PAIR</i>	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= <i>STRING</i>	HTTP ヘッダーの文字列を User Agent として送信します。
header= <i>STRING</i>	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。

表 7-1. HTTP/HTTPS プロトコルの拡張機能（続き）

監視の拡張機能	説明
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= <i>INTEGER:INTEGER</i>	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 7-2. 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=[<i>INTEGER</i>]	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 7-3. 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= <i>STRING</i>	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 criti 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= <i>INTEGER</i>	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= <i>INTEGER</i>	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= <i>INTEGER</i> [, <i>INTEGER</i>]	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。

表 7-3. TCP プロトコルの拡張機能（続き）

監視の拡張機能	説明
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。
 - 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] タブをクリックします。
 - 左側のパネルで [Edge Gateway] をクリックします。
 - ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[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。
- [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、サーバ上の既存の接続数に基づいて複数のサーバに分散させます。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が指定されます。このオプションにより、サーバが停止しない限り、URI は必ず同じサーバに転送されます。

オプション	説明
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 headerName=<name> 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 urlParam=<url> 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 変更内容を保持するには、[保持] をクリックします。


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 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] タブをクリックします。
 - b 左側のパネルで [Edge Gateway] をクリックします。
 - c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[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/2.2/configuration.html> を参照してください。
- 6 変更内容を保持するには、[保持] をクリックします。

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 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] タブをクリックします。
 - b 左側のパネルで [Edge Gateway] をクリックします。
 - c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[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	仮想サーバー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 変更内容を保持するには、[保持] をクリックします。

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

NSX Data Center for vSphere 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。

VMware Cloud 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： VMware Cloud 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

VMware Cloud Director 環境の NSX Data Center for vSphere 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。

VMware Cloud 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。NSX Data Center for vSphere 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 [NSX Data Center for vSphere 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 [NSX Data Center for vSphere 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 [NSX Data Center for vSphere 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、NSX Data Center for vSphere 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 NSX Data Center for vSphere Edge Gateway での SSL VPN-Plus の全般設定のカスタマイズ

VMware Cloud 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。VMware Cloud 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 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] タブをクリックします。
 - b 左側のパネルで [Edge Gateway] をクリックします。
 - c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[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。[NSX Data Center for vSphere 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。NSX Data Center for vSphere 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 ポリシーを構成します。

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、[サーバ証明書を変更] 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。[NSX Data Center for vSphere 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。

NSX Data Center for vSphere 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 で構成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 プールを構成します。

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。[NSX Data Center for vSphere 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。

NSX Data Center for vSphere 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](#)。
- [NSX Data Center for vSphere 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。

オプション	アクション
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> <ul style="list-style-type: none"> ■ [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>
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	<p>プライベート ネットワークを有効または無効にします。</p>

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。 [NSX Data Center for vSphere 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。

NSX Data Center for vSphere 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](#)。
- [NSX Data Center for vSphere 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、NSX Data Center for vSphere 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、「[NSX Data Center for vSphere 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

- [SSL VPN-Plus] タブで、[ユーザー] をクリックします。
- [作成] () ボタンをクリックします。
- ユーザーの次のオプションを構成します。

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。

- [保持] をクリックします。
- 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、NSX Data Center for vSphere 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 パッケージを構成します。

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。

- 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。

- (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。

- (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。

このオプションはデフォルトで無効です。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。

- [変更を保存] をクリックします。

NSX Data Center for vSphere Edge Gateway での SSL VPN-Plus の全般設定のカスタマイズ

VMware Cloud 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。VMware Cloud 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

- [SSL VPN-Plus] タブで、[全般設定] をクリックします。
- 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使用す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。
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。

オプション	説明
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

VMware Cloud 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に、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 NSX Data Center for vSphere Edge Gateway 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、VMware Cloud Director テナント ポータルで [IPsec VPN サイト] 画面を使用します。

3 NSX Data Center for vSphere Edge Gateway 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 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] タブをクリックします。
- b 左側のパネルで [Edge Gateway] をクリックします。
- c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[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。[NSX Data Center for vSphere Edge Gateway の IPsec VPN サイト接続の設定](#)を参照してください。

NSX Data Center for vSphere Edge Gateway 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、VMware Cloud 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、VMware Cloud Director 環境のコンテキスト内での接続の概念について理解している必要があります。

- 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 [IPsec VPN] タブで、[IPsec VPN サイト] をクリックします。

2 [追加] () ボタンをクリックします。

3 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。</p> <p>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>
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>

オプション	アクション
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>
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。

4 [保持] をクリックします。

5 [変更を保存] をクリックします。

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。[NSX Data Center for vSphere Edge Gateway での IPsec VPN サービスの有効化](#) を参照してください。

NSX Data Center for vSphere Edge Gateway 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せん。

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。[NSX Data Center for vSphere Edge Gateway 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 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] タブをクリックします。
 - b 左側のパネルで [Edge Gateway] をクリックします。
 - c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[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

VMware Cloud Director 環境の NSX Data Center for vSphere 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。

手順

1 [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。

2 L2 VPN サーバとしての NSX Data Center for vSphere 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。

3 L2 VPN クライアントとしての NSX Data Center for vSphere 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。

4 NSX Data Center for vSphere 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。

[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 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] タブをクリックします。
 - b 左側のパネルで [Edge Gateway] をクリックします。
 - c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[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 NSX Data Center for vSphere Edge Gateway の構成](#)を参照してください。

L2 VPN サーバとしての NSX Data Center for vSphere 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。

次のステップ

この Edge Gateway で L2 VPN サービスを有効にします。 [NSX Data Center for vSphere 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 NSX Data Center for vSphere 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。
- 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。

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。[NSX Data Center for vSphere Edge Gateway](#) での [L2 VPN サービスの有効化](#) を参照してください。

NSX Data Center for vSphere 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 NSX Data Center for vSphere 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 NSX Data Center for vSphere 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。

NSX Data Center for vSphere Edge Gateway 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 Gateway 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 Gateway から削除されます。

SSL 証明書の管理

VMware Cloud 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。

VMware Cloud 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

VMware Cloud 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 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] タブをクリックします。
 - b 左側のパネルで [Edge Gateway] をクリックします。
 - c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[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構成します。

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 VMware Cloud 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。FIPS モードがオンの場合、RSA キー サイズは 2048 ビット以上にする必要があります。 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

- 1 Edge Gateway サービスを開きます。
 - a 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] タブをクリックします。
 - b 左側のパネルで [Edge Gateway] をクリックします。
 - c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[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 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。
- 4 署名付き証明書をインポートします。
 - a [CSR 用に生成された署名付き証明書] をクリックします。
 - b 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。
 - c (オプション) 説明を入力します。
 - d [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 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] タブをクリックします。
 - b 左側のパネルで [Edge Gateway] をクリックします。
 - c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[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 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] タブをクリックします。
 - b 左側のパネルで [Edge Gateway] をクリックします。
 - c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[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 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] タブをクリックします。
 - b 左側のパネルで [Edge Gateway] をクリックします。
 - c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[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 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] タブをクリックします。
 - b 左側のパネルで [Edge Gateway] をクリックします。
 - c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[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。
 FIPS モードがオンの場合、RSA キー サイズは 2048 ビット以上にする必要があります。
 - 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 VMware Cloud 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、[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。このページを開くには、組織 VDC の分散ファイアウォール設定に移動するか、組織 VDC に属する Edge ゲートウェイのサービス設定に移動する必要があります。

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
組織 VDC の分散ファイアウォール設定から	<ol style="list-style-type: none"> a 上部ナビゲーション バーの [リソース] で [クラウド リソース] を選択します。 b 左側のパネルで [組織 VDC] をクリックします。 c ターゲット組織仮想データセンターの名前の横にあるラジオ ボタンを選択して、[ファイアウォールの管理] をクリックします。 d [オブジェクトのグループ分け] タブをクリックします。
組織 VDC の Edge Gateway のサービス設定から	<ol style="list-style-type: none"> a 上部ナビゲーション バーの [リソース] で [クラウド リソース] を選択します。 b 左側のパネルで [Edge Gateway] をクリックします。 c ターゲット組織仮想データセンターに属する Edge Gateway の名前の横にあるラジオ ボタンを選択して、[サービス] をクリックします。 d [オブジェクトのグループ分け] タブをクリックします。

- 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 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 セットを作成するには、[オブジェクトのグループ分け] 画面を使用します。この画面を開くには、組織 VDC の分散ファイアウォール設定に移動するか、組織 VDC に属する Edge Gateway のサービス設定に移動する必要があります。


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
組織 VDC の分散ファイアウォール設定から	<ol style="list-style-type: none"> a 上部ナビゲーション バーの [リソース] で [クラウド リソース] を選択します。 b 左側のパネルで [組織 VDC] をクリックします。 c ターゲット組織仮想データセンターの名前の横にあるラジオ ボタンを選択して、[ファイアウォールの管理] をクリックします。 d [オブジェクトのグループ分け] タブをクリックします。
組織 VDC の Edge Gateway のサービス設定から	<ol style="list-style-type: none"> a 上部ナビゲーション バーの [リソース] で [クラウド リソース] を選択します。 b 左側のパネルで [Edge Gateway] をクリックします。 c ターゲット組織仮想データセンターに属する Edge Gateway の名前の横にあるラジオ ボタンを選択して、[サービス] をクリックします。 d [オブジェクトのグループ分け] タブをクリックします。

- 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 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 ルールで使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。

使用可能なサービスを表示するには、[オブジェクトのグループ分け] 画面を使用します。この画面を開くには、組織 VDC の分散ファイアウォール設定に移動するか、組織 VDC に属する Edge Gateway のサービス設定に移動する必要があります。

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
組織 VDC の分散ファイアウォール設定から	<ol style="list-style-type: none"> 上部ナビゲーション バーの [リソース] で [クラウド リソース] を選択します。 左側のパネルで [組織 VDC] をクリックします。 ターゲット組織仮想データセンターの名前の横にあるラジオ ボタンを選択して、[ファイアウォールの管理] をクリックします。 [オブジェクトのグループ分け] タブをクリックします。
組織 VDC の Edge Gateway のサービス設定から	<ol style="list-style-type: none"> 上部ナビゲーション バーの [リソース] で [クラウド リソース] を選択します。 左側のパネルで [Edge Gateway] をクリックします。 ターゲット組織仮想データセンターに属する Edge Gateway の名前の横にあるラジオ ボタンを選択して、[サービス] をクリックします。 [オブジェクトのグループ分け] タブをクリックします。

- 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。

使用可能なサービス グループを表示するには、[オブジェクトのグループ分け] 画面を使用します。この画面を開くには、組織 VDC の分散ファイアウォール設定に移動するか、組織 VDC に属する Edge Gateway のサービス設定に移動する必要があります。

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
組織 VDC の分散ファイアウォール設定から	<ol style="list-style-type: none"> 上部ナビゲーション バーの [リソース] で [クラウド リソース] を選択します。 左側のパネルで [組織 VDC] をクリックします。 ターゲット組織仮想データセンターの名前の横にあるラジオ ボタンを選択して、[ファイアウォールの管理] をクリックします。 [オブジェクトのグループ分け] タブをクリックします。
組織 VDC の Edge Gateway のサービス設定から	<ol style="list-style-type: none"> 上部ナビゲーション バーの [リソース] で [クラウド リソース] を選択します。 左側のパネルで [Edge Gateway] をクリックします。 ターゲット組織仮想データセンターに属する Edge Gateway の名前の横にあるラジオ ボタンを選択して、[サービス] をクリックします。 [オブジェクトのグループ分け] タブをクリックします。

- 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 のネットワーク使用と IP 割り当ての表示

Edge Gateway のネットワーク、および IP アドレス プールの使用とサブネットに関する情報を表示できます。各ネットワークに割り当てられた IP アドレスを表示することもできます。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [Edge Gateway] をクリックし、ターゲット Edge Gateway の名前をクリックします。
- 3 外部ネットワーク、および IP アドレス プールの使用とサブネットに関する情報を表示するには、[外部ネットワーク] - [ネットワークおよびサブネット] タブをクリックします。
- 4 外部ネットワーク、および IP アドレスとカテゴリに関する情報を表示するには、[外部ネットワーク] - [IP の割り当て] タブをクリックします。

Edge ゲートウェイのプロパティの編集

Edge Gateway での分散ルーティングの有効化または無効化

Edge Gateway で VMware Cloud Director 分散ルーティングを有効にすると、組織管理者は、この Edge Gateway に接続された分散インターフェイスを持つ経路指定された組織仮想データセンター ネットワークを多数作成できるようになります。これらのネットワーク上のトラフィックは、仮想マシン間の通信用に最適化されます。

前提条件

バックアップ NSX Manager インスタンスには、NSX Controller クラスタが構成されています。『NSX 管理ガイド』を参照してください。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [Edge Gateway] をクリックします。
- 3 ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[分散ルーティングの有効化] または [分散ルーティングの無効化] をクリックします。
- 4 確認するには、[OK] をクリックします。

外部ネットワークと Edge Gateway 設定の変更

外部ネットワークと Edge Gateway の設定を変更するには、Edge Gateway の作成に使用したウィザードと同じページが含まれている [Edge ゲートウェイの編集] ウィザードを使用します。

Edge Gateway を追加したときの設定を変更できます。[NSX Data Center for vSphere Edge Gateway の追加](#) を参照してください。

分散ルーティングの設定を変更するには、[Edge Gateway での分散ルーティングの有効化または無効化](#)を参照してください。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [Edge Gateway] をクリックします。
- 3 変更する Edge Gateway 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。
- 4 Edge Gateway の設定を変更するには、[次へ] をクリックして [Edge ゲートウェイの編集] ウィザードのページに移動し、[設定内容の確認] ページで [完了] をクリックします。

Edge Gateway の全般設定の編集

Edge Gateway の名前と説明の変更、FIPS モードや高可用性の有効/無効の切り替え、Edge Gateway のサイズ設定の変更を実行できます。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [Edge Gateway] をクリックし、ターゲット Edge Gateway の名前をクリックします。
- 3 [全般] タブで、右上隅にある [編集] をクリックします。
- 4 (オプション) Edge Gateway の名前と説明を編集します。
- 5 (オプション) Edge Gateway の全般設定をそれぞれ有効または無効にします。

全般設定	説明
FIPS モード	NSX FIPS モードを使用するよう Edge ゲートウェイを構成します。
高可用性	バックアップ Edge ゲートウェイへの自動フェイルオーバーを有効にします。

- 6 (オプション) システム リソースの Edge Gateway 構成を変更します。

構成	説明
コンパクト	必要なメモリとコンピューティング リソースが少なく済みます。
大	[コンパクト] 設定よりも大きな容量と高いパフォーマンスを提供します。[大] 構成と [超特大] 構成では、同じセキュリティ機能が提供されます。
超特大	多数の同時セッションが実行される、ロード バランサを含む環境に使用します。
特大	スループットが多量である環境に使用します。高速な接続速度が必要です。

- 7 変更を確定するには、[保存] をクリックします。

Edge Gateway のデフォルト ゲートウェイの編集

Edge Gateway がデフォルト ゲートウェイとして使用するネットワークを変更できます。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [Edge Gateway] をクリックし、ターゲット Edge Gateway の名前をクリックします。
- 3 [外部ネットワーク] - [デフォルト ゲートウェイ] タブで、右上隅にある [編集] をクリックします。
- 4 (オプション) ネットワークをデフォルト ゲートウェイとして構成します。
 - a [デフォルト ゲートウェイの構成] 切り替えを有効にします。
 - b ターゲット外部ネットワークの名前の横にあるラジオ ボタンを選択し、宛先 IP アドレスの横にあるラジオ ボタンを選択します。
 - c (オプション) [DNS リレーにデフォルト ゲートウェイを使用] 切り替えを有効にします。
- 5 変更を確定するには、[保存] をクリックします。

Edge Gateway の IP アドレスの設定の編集

Edge Gateway の外部ネットワークの IP アドレス設定を変更できます。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [Edge Gateway] をクリックし、ターゲット Edge Gateway の名前をクリックします。
- 3 [外部ネットワーク] - [IP アドレス設定] タブで [編集] をクリックします。
- 4 Edge Gateway のネットワークごとに、[IP アドレス] セルに IP アドレスを入力するか、セルを空白のままにします。

ネットワークの IP アドレスを入力しない場合は、このネットワークに任意の IP アドレスが割り当てられます。
- 5 変更を確定するには、[保存] をクリックします。

Edge ゲートウェイ上の細分割り当てされた IP アドレス プールの編集

Edge ゲートウェイ上の外部ネットワークの使用可能な IP アドレス プールを複数の固定 IP アドレス プールに細分割り当てすることができます。

注： 細分割り当てによる Edge Gateway への IP アドレスの割り当ては、プロバイダが IP アドレスの所有権をゲートウェイに割り当てるプロセスです。VMware Cloud Director では、細分割り当てプロセスで適切なゲートウェイ インターフェイスにセカンダリ アドレスを自動的に設定します。このため、いずれかの IP アドレスが VMware Cloud Director の外部で使用されている場合は、IP アドレスの競合が発生する可能性があります。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。

- 2 左側のパネルで [Edge Gateway] をクリックし、ターゲット Edge Gateway の名前をクリックします。
- 3 [外部ネットワーク] - [細分割り当て済み IP プール] タブの順にクリックします。

この Edge ゲートウェイ上のそれぞれの外部ネットワークについて現在の細分割り当て済み IP アドレス プールが表示されます。

- 4 外部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。

この外部ネットワークに使用可能な IP アドレス プールと、現在細分割り当てされている IP アドレス プール（設定されている場合）が表示されます。

- 5 この外部ネットワークに細分割り当てされている IP アドレス プールを編集し、[保存] をクリックします。

使用可能な IP アドレス プールの範囲から IP アドレスと IP アドレス範囲を追加、変更、および削除できます。

結果

システムは重複する IP アドレス範囲を結合します。

Edge ゲートウェイ上のレート制限の編集

Edge ゲートウェイのそれぞれの外部ネットワークについて着信および発信のレート制限を設定できます。

レート制限は、静的結合の分散ポート グループによりバックキングされている外部ネットワークにのみ適用されます。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [Edge Gateway] をクリックし、ターゲット Edge Gateway の名前をクリックします。
- 3 [外部ネットワーク] - [レート制限] タブで、右上隅にある [編集] をクリックします。

この Edge ゲートウェイ上のそれぞれの外部ネットワークについて現在のレート制限が表示されます。

- 4 レート制限を編集して、[保存] をクリックします。

Edge Gateway 上のそれぞれの外部ネットワークについて、レート制限を有効または無効にしたり、着信および発信レートを変更することができます。

Edge Gateway の再デプロイ

新しい Edge Gateway アプライアンスを削除し、最新の構成を使用してデプロイすることができます。

Edge サービスが予期されたとおりに動作しない場合は、Edge Gateway アプライアンスを再デプロイできます。

Edge Gateway を再デプロイすると、VMware Cloud Director は Edge Gateway を削除した後、最新の構成で再作成します。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [Edge Gateway] をクリックします。
- 3 対象の Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[再デプロイ] 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

Edge Gateway 仮想マシンが新しい仮想マシンに置き換えられ、すべてのサービスがリストアされます。

Edge ゲートウェイの削除

組織仮想データセンターから Edge Gateway を削除できます。

前提条件

対象の Edge Gateway を使用するすべての組織仮想データセンター ネットワークを削除します。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [Edge Gateway] をクリックします。
- 3 対象の Edge Gateway 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 確定するには、[削除] をクリックします。

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 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] タブをクリックします。
 - b 左側のパネルで [Edge Gateway] をクリックします。
 - c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[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。

- 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] タブをクリックします。
- 左側のパネルで [Edge Gateway] をクリックします。
- ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[サービス] をクリックします。

2 [Edge 設定] タブで [Syslog サーバーの編集] 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。

VMware Cloud Director システム管理者が VMware Cloud 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 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] タブをクリックします。
 - b 左側のパネルで [Edge Gateway] をクリックします。
 - c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[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。

NSX-T Data Center Edge Gateway の管理

8

NSX-T Data Center Edge Gateway は経路指定された組織 VDC ネットワークまたはデータセンター グループ 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)、IPsec VPN、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。

- 専用外部ネットワーク
- NSX-T Data Center Edge Gateway の追加
- NSX-T Data Center Edge Gateway への IP セットの追加
- NSX-T Data Center 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
- NSX-T Edge Gateway の IP アドレスの割り当ての編集
- 迅速な IP アドレスの割り当て
- 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 Data Center Edge Gateway のポリシーベースの IPsec VPN
- 専用の外部ネットワーク サービスの設定
- NSX-T Data Center Edge Gateway での NSX Advanced ロード バランシングの管理

専用外部ネットワーク

仮想データセンターに完全に経路指定されたネットワーク トポロジを提供するために、外部ネットワークを特定の NSX-T Data Center Edge Gateway 専用にすることができます。

この設定では、外部ネットワークと NSX-T Data Center Edge Gateway との間に 1 対 1 の関係があり、他の Edge Gateway を外部ネットワークに接続することはできません。

専用の外部ネットワークに関連付けられている Tier-0 論理ルーターまたは VRF-Lite ゲートウェイは、テナント ネットワーク スタックに含まれています。外部ネットワークは、VMware Cloud Director ネットワーク ルーティング ドメインの一部と見なされます。

外部ネットワークを Edge Gateway 専用にすると、ルートのアドバタイズ管理や境界ゲートウェイ プロトコル (BGP) 設定などの追加の Edge Gateway サービスがテナントに提供されます。

テナントは、Edge Gateway に接続されているテナント ネットワークの中から、外部ネットワークにアドバタイズするものを決定できます。これにより、NAT 経由の組織仮想データセンター ネットワークと、完全に経路指定された組織仮想データセンター ネットワークが混在する可能性があります。

NSX-T Data Center Edge Gateway の全般設定を編集することで、Edge Gateway の作成中に、または作成した後に、外部ネットワークを Edge Gateway 専用にすることができます。

NSX-T Data Center Edge Gateway の追加

NSX-T Data Center Edge Gateway は、経路指定の組織 VDC ネットワークに対し、外部ネットワークへの接続を提供し、ロード バランシング、ネットワーク アドレス変換、ファイアウォールなどのサービスを提供できます。

前提条件

NSX-T Data Center Edge Gateway をデプロイするためのシステム要件の詳細については、『NSX-T Data Center 管理ガイド』を参照してください。

バージョン 10.1 以降の VMware Cloud Director では、専用の外部ネットワーク設定がサポートされています。外部ネットワークを Edge Gateway 専用にすると、ルートのアドバタイズ管理や境界ゲートウェイ プロトコル (BGP) 設定などの追加の Edge Gateway サービスがテナントに提供されます。詳細については、[専用外部ネットワーク](#)を参照してください。

VMware Cloud Director では、基本的な NSX-T Data Center Edge クラスタ設定がサポートされています。NSX Edge クラスタの詳細については、『NSX-T Data Center インストール ガイド』を参照してください。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [Edge Gateway] をクリックします。
- 3 [新規] をクリックします。
- 4 Edge Gateway を作成する、NSX-T Data Center によってバックアップされる組織仮想データセンターを選択し、[次へ] をクリックします。
- 5 新しい Edge Gateway の名前と、オプションで説明を入力します。
- 6 Edge Gateway の BGP およびルート アドバタイズを有効にするには、[専用の外部ネットワーク] オプションをオンにして、[次へ] をクリックします。
- 7 新しい Edge Gateway を接続する外部ネットワークを選択して、[次へ] をクリックします。

[専用の外部ネットワーク] オプションをオンに切り替えると、他の Edge Gateway がこの外部ネットワークにアクセスできなくなります。

- 8 Edge Gateway をデプロイする Edge クラスタを選択し、[次へ] をクリックします。

外部ネットワークに関連付けられているものとは異なる Edge クラスタ上で Edge Gateway サービスを実行する場合は、別の Edge クラスタを使用するように Edge Gateway を設定できます。

- Edge Gateway が接続されている外部ネットワークの Edge クラスタを使用します。
- Edge Gateway をデプロイする組織仮想データセンターで利用できる Edge クラスタのリストから選択します。

- 9 (オプション) Edge Gateway に割り当てられている IP アドレスまたは IP アドレス範囲を編集し、[次へ] をクリックします。

- 10 [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。

NSX-T Data Center Edge Gateway への IP セットの追加

ファイアウォール ルールを作成して NSX-T Data Center Edge Gateway に追加するには、まず IP セットを作成する必要があります。IP セットは、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 IP セットにまとめると、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 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [Edge Gateway] をクリックします。
- 3 NSX-T Edge Gateway をクリックします。
- 4 [セキュリティ] で [IP アドレス セット] タブをクリックし、[新規] をクリックします。
- 5 IP セットの名前と、必要に応じて説明を入力します。
- 6 IP セット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。
- 7 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

IP セットが作成され、NSX-T Edge Gateway に追加されました。

次のステップ

[NSX-T Data Center Edge Gateway ファイアウォール ルールの追加](#)

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

NSX-T Data Center 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 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。

- 2 左側のパネルで [Edge Gateway] をクリックします。
- 3 Edge Gateway をクリックします。
- 4 [サービス] セクションに [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。
- 5 [ルールの編集] をクリックします。
- 6 [最上部に新規作成] ボタンをクリックします。
新しいルールの行が、選択したルールの上に追加されます。
- 7 ファイアウォール ルールを構成します。

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。
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] を有効にします。 ■ 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] を有効にします。 ■ 特定のファイアウォール グループへ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。 ■ ブロックされたクライアントに通知せずに指定されたソース、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、[ドロップ] 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して、ブロックされたクライアントにトラフィックが拒否されたことを通知するには、[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	<p>ルールを適用するトラフィックの方向を選択します。</p> <p>注： VMware Cloud Director 10.2.1 以降のバージョンでは、このオプションは使用できなくなりました。</p>
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。

- 8 [保存] をクリックします。
- 9 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。

VMware Cloud 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。

NO SNAT ルールでは、組織仮想データセンターから送信されたパケットの内部ソース 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せん。

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。

NO 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仮想データセンターが受信したパケットの外部 IP アドレスを変換しません。

NSX-T Data Center Edge Gateway で NAT サービスを使用する場合、VMware Cloud Director はルートの自動再分散をサポートします。

重要： Tanzu Kubernetes クラスタを使用している場合に、矛盾するルールが作成されないようにするには、Edge Gateway に作成されたシステム SNAT ルールを書き留めます。

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 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [Edge Gateway] をクリックします。
- 3 Edge Gateway をクリックし、[サービス] で [NAT] をクリックします。
- 4 ルールを追加するには、[新規] をクリックします。
- 5 SNAT ルールまたは NO SNAT ルールを構成します（内側から外側へ）。

オプション	説明
名前	ルールに意味のある名前を入力します。
説明	（オプション） ルールの説明を入力します。

オプション	説明
インターフェイス タイプ	ドロップダウン メニューから、[SNAT] または [NO SNAT] を選択します。
外部 IP	<p>作成するルールのタイプに応じて、いずれかのオプションを選択します。</p> <ul style="list-style-type: none"> ■ SNAT ルールを作成している場合、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。 ■ NO SNAT ルールを作成している場合、テキスト ボックスは空白のままにします。
内部 IP	SNAT を設定する仮想マシンの IP アドレスまたは IP アドレスのリストを入力し、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。
ターゲット IP アドレス	(オプション) ルールを特定のドメインへのトラフィックにのみ適用する場合、このドメインの IP アドレスまたは IP アドレスのリストを入力します。このテキスト ボックスを空白のままにすると、SNAT ルールはローカル サブネット外のすべてのターゲットに適用されます。
詳細設定 (オプション)	<p>追加設定を行うには、[詳細設定] タブをクリックします。</p> <p>状態</p> <p>作成時にルールを有効にするには、[状態] オプションを有効にします。</p> <p>ログ記録</p> <p>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、[ログ記録] オプションを有効にします。</p> <p>優先度</p> <p>アドレスに複数の NAT ルールが設定されている場合は、これらのルールにさまざまな優先順位を割り当てて、適用される順序を決定できます。値が小さいほど、このルールの優先順位は高くなります。</p> <p>ファイアウォールによる一致</p> <p>ファイアウォール一致ルールを設定すると、NAT 中にファイアウォールを適用する方法を決定できます。ドロップダウン メニューから、次のいずれかのオプションを選択します。</p> <ul style="list-style-type: none"> ■ NAT ルールの内部アドレスにファイアウォール ルールを適用するには、[内部アドレスとの一致] を選択します。 ■ NAT ルールの外部アドレスにファイアウォール ルールを適用するには、[外部アドレスとの一致] を選択します。 ■ ファイアウォール ルールの適用をスキップするには、[バイパス] を選択します。

6 DNAT ルールまたは NO DNAT ルールを構成します (外側から内側へ)。

オプション	説明
名前	ルールに意味のある名前を入力します。
説明	(オプション) ルールの説明を入力します。
インターフェイス タイプ	ドロップダウン メニューから、[DNAT] または [NO DNAT] を選択します。
外部 IP	<p>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。</p> <p>入力する IP アドレスは、Edge Gateway にサブ割り当てされている必要があります。</p>
外部ポート	(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を入力します。

オプション	説明
内部 IP	<p>作成するルールのタイプに応じて、いずれかのオプションを選択します。</p> <ul style="list-style-type: none"> ■ DNAT ルールを作成している場合、DNAT を設定する仮想マシンの IP アドレスまたは IP アドレスのリストを入力し、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。 ■ NO DNAT ルールを作成している場合、テキスト ボックスは空白のままにします。
アプリケーション	<p>(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。</p>
詳細設定 (オプション)	<p>追加設定を行うには、[詳細設定] タブをクリックします。</p> <p>状態</p> <p>作成時にルールを有効にするには、[状態] オプションを有効にします。</p> <p>ログ記録</p> <p>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、[ログ記録] オプションを有効にします。</p> <p>優先度</p> <p>アドレスに複数の NAT ルールが設定されている場合は、これらのルールにさまざまな優先順位を割り当てて、適用される順序を決定できます。値が小さいほど、このルールの優先順位は高くなります。</p> <p>ファイアウォールによる一致</p> <p>ファイアウォール一致ルールを設定すると、NAT 中にファイアウォールを適用する方法を決定できます。ドロップダウン メニューから、次のいずれかのオプションを選択します。</p> <ul style="list-style-type: none"> ■ NAT ルールの内部アドレスにファイアウォール ルールを適用するには、[内部アドレスとの一致] を選択します。 ■ NAT ルールの外部アドレスにファイアウォール ルールを適用するには、[外部アドレスとの一致] を選択します。 ■ ファイアウォール ルールの適用をスキップするには、[バイパス] を選択します。

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。

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 フォワーダを構成します。

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 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。

2 左側のパネルで [Edge Gateway] をクリックします。

- 3 Edge Gateway をクリックし、[IP アドレス管理] で [DNS] をクリックします。
- 4 [DNS フォワーダ] セクションで [編集] をクリックします。
- 5 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。
- 6 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。
- 7 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。
- 8 [保存] をクリックします。
- 9 (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。

NSX-T Edge Gateway の IP アドレスの割り当ての編集

外部ネットワークの複数の IP アドレスを Edge Gateway に割り当てることができます。

手順

- 1 Edge Gateway サービスを開きます。
 - a 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] タブをクリックします。
 - b 左側のパネルで [Edge Gateway] をクリックします。
 - c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[サービス] をクリックします。
- 2 Edge Gateway をクリックし、[IP の割り当て] をクリックします。

IP アドレス管理グリッドには、Edge Gateway に割り当てられている IP アドレスと、現在 Edge Gateway で使用されている IP アドレスが表示されます。
- 3 [割り当てられた IP アドレス] セクションで [IP アドレス管理] をクリックします。

[IP アドレス管理] グリッドに、Edge Gateway で使用可能な外部ネットワーク別に IP アドレスの使用状況が表示されます。
- 4 IP アドレス範囲を入力し、[追加] をクリックします。
- 5 [保存] をクリックします。

結果

IP アドレスが Edge Gateway に割り当てられます。

次のステップ

Edge Gateway に割り当てられている IP アドレスを確認し、必要に応じて IP アドレスの追加または削除を行います。

迅速な IP アドレスの割り当て

迅速な IP アドレスの割り当てを使用すると、特定の IP アドレスまたは IP アドレス範囲を入力せずに、外部ネットワークのサブネットから Edge Gateway に IP アドレスを割り当てることができます。

手順

- 1 Edge Gateway サービスを開きます。

- a 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] タブをクリックします。
- b 左側のパネルで [Edge Gateway] をクリックします。
- c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[サービス] をクリックします。

- 2 Edge Gateway をクリックし、[IP の割り当て] をクリックします。

IP アドレス管理グリッドには、Edge Gateway に割り当てられている IP アドレスと、現在 Edge Gateway で使用されている IP アドレスが表示されます。

- 3 [割り当てられた IP アドレス] セクションで [迅速な IP アドレスの割り当て] をクリックします。

- 4 ドロップダウン メニューから、IP アドレスを割り当てるサブネットを選択します。

複数のサブネットを使用できる場合に [任意] を選択すると、1 つ以上のサブネットから IP アドレスが割り当てられます。

- 5 Edge Gateway に割り当てる IP アドレスの数を入力して、[保存] をクリックします。

この数は、選択したサブネット内の使用可能な IP アドレスの数未満にする必要があります。

結果

IP アドレスが Edge Gateway に割り当てられます。

次のステップ

Edge Gateway に割り当てられている IP アドレスを確認し、必要に応じて IP アドレスの追加または削除を行います。

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 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [Edge Gateway] をクリックします。
- 3 Edge Gateway をクリックします。
- 4 [セキュリティ] で [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。
- 5 [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。
- 6 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。
- 7 ドロップダウン メニューからプロトコルを選択します。
- 8 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 Data Center 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。

NSX-T Data Center Edge Gateway のポリシーベースの IPsec VPN

バージョン 10.1 以降では、VMware Cloud Director は、NSX-T Data Center Edge Gateway インスタンスとリモート サイト間のサイトツーサイトのポリシーベースの IPsec VPN をサポートしています。

IPsec VPN は、Edge Gateway と、同じく NSX-T Data Center を使用しているか、IPSec をサポートするサードパーティのハードウェア ルーターまたは VPN ゲートウェイを備えているリモート サイトとの間のサイトツーサイトの接続を提供します。

ポリシーベースの IPsec VPN では、VPN ポリシーをパケットに適用して、VPN トンネルを通過する前に IPsec で保護するトラフィックを決定する必要があります。このタイプの VPN は、ローカル ネットワーク トポロジや構成が変更されると、その変更に合わせて VPN ポリシー設定も更新する必要があるため、静的と見なされます。

NSX-T Data Center Edge Gateway は、IPsec トラフィックがルーティングを優先する、分割トンネル構成をサポートします。

NSX-T Edge Gateway で IPsec VPN を使用する場合、VMware Cloud Director はルートの自動再分散をサポートします。

NSX-T ポリシーベースの IPsec VPN の設定

NSX-T Data Center Edge Gateway とリモート サイトの間でサイト間接続を構成できます。リモート サイトは、NSX-T Data Center を使用し、サードパーティ製ハードウェア ルーター、または IPsec をサポートする VPN ゲートウェイを使用する必要があります。

NSX-T Data Center Edge Gateway で IPsec VPN を構成する場合、VMware Cloud Director はルートの自動再分散をサポートします。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [Edge Gateway] をクリックし、ターゲット Edge Gateway の名前をクリックします。
- 3 [サービス] で [IPsec VPN] をクリックします。
- 4 IPsec VPN トンネルを設定するには、[新規] をクリックします。
- 5 IPsec VPN トンネルの名前と、オプションで説明を入力します。
- 6 作成時にトンネルを有効にするには、[有効] オプションをオンにします。
- 7 入力する事前共有キーを選択します。

注： 事前共有キーは、IPSec VPN トンネルの相手側でも同じにする必要があります。

- 8 ローカル エンドポイントの Edge Gateway で使用できる IP アドレスのいずれかを入力します。

注： IP アドレスは、Edge Gateway のプライマリ IP アドレス、または外部ネットワークから Edge Gateway に個別に割り当てられる IP アドレスのいずれかにする必要があります。

- 9 IPsec VPN トンネルに使用する 1 つ以上のローカル IP サブネット アドレスを CIDR 表記で入力します。
- 10 リモート サイトの IP アドレスを入力します。
- 11 IPsec VPN トンネルに使用する 1 つ以上のリモート IP サブネット アドレスを CIDR 表記で入力します。
- 12 (オプション) ログ記録を有効にするには、[ログ記録] オプションをオンにします。
- 13 [保存] をクリックします。
- 14 トンネルが機能していることを確認するには、そのトンネルを選択して [統計情報の表示] をクリックします。

トンネルが機能している場合は、[トンネルのステータス] と [IKE サービス ステータス] の両方に 到達可能 と表示されます。

結果

新しく作成された IPSec VPN トンネルは、[IPsec VPN] ビューに表示されます。IPsec VPN トンネルは、デフォルトのセキュリティ プロファイルを使用して作成されます。

次のステップ

必要に応じて IPsec VPN トンネル設定を編集し、そのセキュリティ プロファイルをカスタマイズすることができます。

IPsec VPN トンネルのセキュリティ プロファイルのカスタマイズ

作成時に IPsec VPN トンネルに割り当てられたシステム生成のセキュリティ プロファイルをそのまま使用しない場合は、カスタマイズして使用できます。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [Edge Gateway] をクリックし、ターゲット Edge Gateway の名前をクリックします。
- 3 [サービス] で [IPsec VPN] をクリックします。
- 4 IPsec VPN トンネルを選択し、[セキュリティ プロファイルのカスタマイズ] をクリックします。
- 5 IKE プロファイルを構成します。

Internet Key Exchange (IKE) プロファイルは、IKE トンネルの確立時にネットワーク サイト間の共有シークレット キーの認証、暗号化、および確立に使用されるアルゴリズムに関する情報を提供します。

- a IPsec プロトコルスイートで Security Association (SA) を設定する IKE プロトコルのバージョンを選択します。

オプション	説明
IKEv1	このオプションを選択すると、IPsec VPN は IKEv1 プロトコルのみを開始し、応答します。
IKEv2	デフォルトのオプション。このバージョンを選択すると、IPsec VPN は IKEv2 プロトコルのみを開始し、応答します。
IKE-Flex	このオプションを選択すると、IKEv2 プロトコルでトンネルの確立が失敗した場合、ソース サイトはフォールバックせず、IKEv1 プロトコルで接続を開始します。また、リモート サイトが IKEv1 プロトコルで接続を開始した場合には、接続を受け入れます。

- b Internet Key Exchange (IKE) ネゴシエーション中に使用する、サポートされている暗号化アルゴリズムを選択します。
- c [ダイジェスト] ドロップダウン メニューから、IKE ネゴシエーション中に使用するセキュア ハッシュ アルゴリズムを選択します。
- d [Diffie-Hellman グループ] ドロップダウン メニューから、ピア サイトと Edge Gateway が安全でない通信チャネルを介して共有シークレット キーを確立できるように、いずれかの暗号化スキームを選択します。
- e (オプション) [関連付けの有効時間] テキスト ボックスで、IPsec トンネルの再確立が必要になるまでのデフォルトの秒数を変更します。

6 IPsec VPN トンネルを構成します。

- a Perfect Forward Secrecy を有効にするには、オプションをオンにします。
- b 最適化ポリシーを選択します。

最適化ポリシーは、内部パケットにある最適化ビットを処理するのに役立ちます。

オプション	説明
コピー	内部 IP パケットから外部パケットに最適化ビットをコピーします。
クリア	内部パケットにある最適化ビットを無視します。

- c Internet Key Exchange (IKE) ネゴシエーション中に使用する、サポートされている暗号化アルゴリズムを選択します。
- d [ダイジェスト] ドロップダウン メニューから、IKE ネゴシエーション中に使用するセキュア ハッシュ アルゴリズムを選択します。
- e [Diffie-Hellman グループ] ドロップダウン メニューから、ピア サイトと Edge Gateway が安全でない通信チャネルを介して共有シークレット キーを確立できるように、いずれかの暗号化スキームを選択します。
- f (オプション) [関連付けの有効時間] テキスト ボックスで、IPsec トンネルの再確立が必要になるまでのデフォルトの秒数を変更します。

7 (オプション) [プローブ間隔] テキスト ボックスで、Dead ピア検出のデフォルトの秒数を変更します。

8 [保存] をクリックします。

結果

IPsec VPN ビューで、IPsec VPN トンネルのセキュリティ プロファイルが [ユーザー定義] として表示されます。

専用の外部ネットワーク サービスの設定

仮想データセンターに完全に経路指定されたネットワーク トポロジを提供するために、システム管理者は外部ネットワークを特定の NSX-T Data Center Edge Gateway 専用にすることができます。

専用の外部ネットワークを使用すると、ルート アドバタイズ管理や Border Gateway Protocol (BGP) の設定など、追加のルーティング サービスの設定を実行できます。

ルート アドバタイズの管理

ルート アドバタイズを使用して、完全にルーティングされたネットワーク環境を組織の仮想データセンター (VDC) 内に作成できます。

NSX-T Data Center Edge Gateway に接続されているネットワーク サブネットの中から、専用の外部ネットワークにアドバタイズするものを決定できます。

サブネットがアドバタイズ フィルタに追加されていない場合、そのサブネットへのルートは外部ネットワークにアドバタイズされず、プライベートのままになります。

注： VMware Cloud Director は、アドバタイズされるルート内にあるすべての組織仮想データセンター ネットワークをアドバタイズします。そのため、アドバタイズされるネットワークの一部である各サブネット用にフィルタを作成する必要はありません。

ルート アドバタイズは、NSX-T Data Center Edge Gateway 上で自動的に構成されます。

NSX-T Edge Gateway でルート アドバタイズを使用する場合、VMware Cloud Director はルートの自動再分散をサポートします。ルートの再分散は、専用の外部ネットワークに接続される Tier-0 論理ルーター上で自動的に構成されます。

前提条件

- 外部ネットワークを組織内の NSX-T Data Center Edge Gateway 専用に行っていることを確認します。[専用外部ネットワーク](#)を参照してください。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [Edge Gateway] をクリックし、ターゲット Edge Gateway の名前をクリックします。
- 3 [ルーティング] で [ルート アドバタイズ] をクリックし、[編集] をクリックします。
- 4 アドバタイズするサブネットを追加するには、[追加] をクリックします。
- 5 IPv4 または IPv6 のサブネットを追加します。

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

BGP の全般設定

専用の外部ネットワークを持つ NSX-T Data Center Edge Gateway と物理インフラストラクチャ内のルーター間に、外部または内部 Border Gateway Protocol (eBGP または iBGP) 接続を設定できます。

BGP は、自律システム (AS) 間の複数のルートを指定する IP アドレス 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、コア ルーティングを決定します。

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。

注： VRF ゲートウェイによってバックアップされる外部ネットワークに接続されている Edge Gateway では、ローカル AS 番号とグレースフル リスタートの設定は読み取り専用です。これらの設定は、NSX-T Data Center の親 Tier-0 ゲートウェイで編集できます。

前提条件

- 外部ネットワークを組織内の NSX-T Data Center Edge Gateway 専用に行っていることを確認します。[専用外部ネットワーク](#)を参照してください。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [Edge Gateway] をクリックし、ターゲット Edge Gateway の名前をクリックします。
- 3 [ルーティング] で [BGP] をクリックし、[構成] で [編集] をクリックします。
- 4 [ステータス] オプションをオンにして、BGP を有効にします。
- 5 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 番号を入力します。

VMware Cloud Director は、ローカル AS 番号を Edge Gateway に割り当てます。Edge Gateway が他の自律システム内の BGP ネイバーと接続する場合は、この ID を通知します。

- 6 ドロップダウン メニューから、[グレースフル リスタート モード] オプションを選択します。

オプション	説明
ヘルパーとグレースフル リスタート	<p>すべてのゲートウェイからの BGP ピアリングは常にアクティブであるため、Edge Gateway でグレースフル リスタート機能を有効にすることはベスト プラクティスではありません。</p> <p>フェイルオーバー時には、グレースフル リスタート機能により、リモート ネイバーが代替の Tier-0 ゲートウェイを選択するのにかかる時間が長くなります。このため、BFD ベースの統合が遅延します。</p> <p>注： Edge Gateway 構成は、ネイバー固有の設定でオーバーライドされない限り、すべての BGP ネイバーに適用されます。</p>
ヘルパーのみ	<p>グレースフル リスタートが可能なネイバーから学習したルートに関連付けられているトラフィックの中断を軽減または排除するのに便利です。再起動の実行中、ネイバーはフォワーディング テーブルを保持している必要があります。</p>
無効化	<p>Edge Gateway でグレースフル リスタート モードを無効にします。</p>

- 7 (オプション) グレースフル リスタート タイマーのデフォルト値を変更します。
- 8 (オプション) 古いルート タイマーのデフォルト値を変更します。
- 9 [ECMP] オプションをオンにして、ECMP を有効にします。
- 10 [保存] をクリックします。

次のステップ

- [IP アドレス プリフィックス リストの作成](#)
- [BGP ネイバーの追加](#)

IP アドレス プリフィックス リストの作成

1 つまたは複数の IP アドレスを含む IP アドレス プリフィックス リストを作成できます。IP アドレス プリフィックス リストを使用して、ルートのアドバタイズのアクセス権限を BGP ネイバーに割り当てます。

IP アドレス プリフィックス リストは BGP ネイバー フィルタを介して参照され、BGP ピア間で交換される BGP 更新の数が制限されます。ルート フィルタリングを使用すると、BGP の更新に必要なシステム リソースの量を削減できます。

たとえば、IP アドレス プリフィックス リストに IP アドレス 192.168.100.3/27 を追加し、Edge Gateway へのルートの再配分を拒否することができます。

また、IP アドレスに `less than or equal to (le)` および `greater than or equal to (ge)` 修飾子を追加して、ルートの再配分を許可または制限することができます。たとえば、192.168.100.3/27 ge 26 le 32 修飾子は、長さが 26 ビット以上 32 ビット以下のサブネット マスクに一致します。

前提条件

- 外部ネットワークを組織内の NSX-T Data Center Edge Gateway 専用に行っていることを確認します。[専用外部ネットワーク](#)を参照してください。
- [BGP の全般設定](#)。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [Edge Gateway] をクリックし、ターゲット Edge Gateway の名前をクリックします。
- 3 [ルーティング] で、[BGP] および [IP アドレス プリフィックス リスト] をクリックします。
- 4 IP アドレス プリフィックス リストを追加するには、[新規] をクリックします。
- 5 プリフィックス リストの名前と、オプションで説明を入力します。
- 6 [新規] をクリックして、プリフィックスの CIDR 表記を追加します。
- 7 ドロップダウン メニューから、プリフィックスに適用するアクションを選択します。
- 8 (オプション) `greater than or equal to` および `less than or equal to` 修飾子を入力して、ルートの再配分を許可または制限します。

次のステップ

- 必要に応じて、IP アドレス プリフィックス リストを編集または削除できます。
- ルート フィルタリングを構成します。[BGP ネイバーの追加](#)を参照してください。

BGP ネイバーの追加

BGP ルーティング ネイバーを追加するときに、個々の設定を行うことができます。

前提条件

- 外部ネットワークを組織内の NSX-T Data Center Edge Gateway 専用に行っていることを確認します。[専用外部ネットワーク](#)を参照してください。
- Edge Gateway にグローバル BGP を設定してあることを確認します。[BGP の全般設定](#)を参照してください。

- ルート フィルタリングを使用する場合は、IP プリフィックス リストを作成していることを確認します。 [IP アドレス プリフィックス リストの作成](#)を参照してください。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [Edge Gateway] をクリックし、ターゲット Edge Gateway の名前をクリックします。
- 3 [ルーティング] で、[BGP] および [ネイバー] をクリックします。
- 4 新しい BGP ネイバーを追加するには、[新規] をクリックします。
- 5 新しい BGP ネイバーの全般設定を入力します。
 - a 新しい BGP ネイバーの IPv4 または IPv6 アドレスを入力します。
 - b リモート自律システム (AS) 番号を ASPLAIN 形式で入力します。
 - c BGP ピアにキープアライブ メッセージを送信する時間間隔を入力します。
 - d BGP ピアの Dead を宣言するまでの時間間隔を入力します。
 - e ドロップダウン メニューから、このネイバーの [グレースフル リスタート モード] オプションを選択します。

オプション	説明
無効化	グローバル Edge Gateway の設定をオーバーライドし、このネイバーのグレースフル リスタート モードを無効にします。
ヘルパーのみ	グローバル Edge Gateway の設定をオーバーライドし、このネイバーのグレースフル リスタート モードを [ヘルパーのみ] に設定します。
グレースフル リスタートとヘルパー	グローバル Edge Gateway の設定をオーバーライドし、このネイバーのグレースフル リスタート モードを [グレースフル リスタートとヘルパー] に設定します。

- f [AllowAS-in] トグルをオンにして、同じ AS でルートを受信できるようにします。
 - g BGP ネイバーが認証を必要とする場合は、BGP ネイバーのパスワードを入力します。
- 6 新しい BGP ネイバーの Bidirectional Forwarding Detection (BFD) を構成します。
 - a (オプション) 障害検出のために BFD を有効にするには、[BFD] オプションをオンにします。
 - b [BFD 間隔] テキスト ボックスに、ハートビート パケットを送信する時間間隔を定義します。
 - c [複数回 Dead] テキスト ボックスに、BFD が BGP ネイバーの停止を宣言するまで許容されるハートビート パケット送信の失敗回数を入力します。
 - 7 (オプション) ルート フィルタリングを構成します。
 - a [IP アドレス ファミリ] ドロップダウン メニューから、IP アドレス ファミリを選択します。
 - b 受信フィルタを設定するには、IP アドレス プリフィックス リストを選択します。
 - c 送信フィルタを設定するには、IP アドレス プリフィックス リストを選択します。
 - 8 [保存] をクリックします。

次のステップ

各 BGP ネイバーのステータスを表示し、必要に応じて BGP ネイバーを編集または削除できます。

NSX-T Data Center Edge Gateway での NSX Advanced ロード バランシングの管理

システム管理者として、NSX-T Data Center ゲートウェイでロード バランシングを有効にし、サービス エンジン グループを Edge Gateway に割り当てることができます。

組織管理者は、ロード バランサ サーバ プールと仮想サービスを作成します。

NSX-T Data Center Edge Gateway でのロード バランサの有効化

[組織管理者]がロード バランシング サービスを構成する前に、[システム管理者]が NSX-T Data Center Edge Gateway でロード バランサを有効にしておく必要があります。

前提条件

- [システム管理者]であることを確認します。
- VMware NSX Advanced Load Balancer がクラウド インフラストラクチャに統合されていることを確認します。NSX Advanced Load Balancer の管理の詳細については、「VMware Cloud Director Service Provider Admin Portal Guide」を参照してください。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [Edge Gateway] をクリックします。
- 3 ロード バランシングを有効にする NSX-T Data Center Edge Gateway をクリックします。
- 4 ロード バランサで [全般設定] をクリックします。
- 5 [編集] をクリックして、[ロード バランサの状態] オプションをオンにします。
- 6 仮想サービスの作成に使用する IP アドレスの取得元となるサービス ネットワーク サブネットのネットワーク CIDR を入力します。

デフォルトのサービス ネットワーク サブネットを使用するには、[デフォルトを使用] チェック ボックスを選択します。

- 7 [保存] をクリックします。

次のステップ

[NSX-T Data Center Edge Gateway へのサービス エンジン グループの割り当て](#)。

NSX-T Data Center Edge Gateway へのサービス エンジン グループの割り当て

組織管理者が NSX-T Data Center Edge Gateway でロード バランシング サービスを構成するには、システム管理者がサービス エンジン グループを Edge Gateway に割り当てておく必要があります。

NSX Advanced Load Balancer によって提供されるロード バランシング コンピューティング インフラストラクチャは、サービス エンジン グループに含まれています。システム管理者は、1 つ以上のサービス エンジン グループを NSX-T Data Center Edge Gateway に割り当てることができます。

単一の Edge Gateway に割り当てられているすべてのサービス エンジン グループは、同じサービス ネットワークを使用します。

前提条件

- [システム管理者] であることを確認します。
- [NSX-T Data Center Edge Gateway でのロード バランサの有効化](#)。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [Edge Gateway] をクリックします。
- 3 サービス エンジン グループの割り当て先となる NSX-T Data Center Edge Gateway をクリックします。
- 4 ロード バランサで、[サービス エンジン グループ] をクリックします。
- 5 [追加] をクリックします。
- 6 リストから使用可能なサービス エンジン グループを選択します。
- 7 Edge Gateway に配置できる仮想サービスの最大数を入力します。
- 8 Edge Gateway で確保されている使用可能な仮想サービスの数を入力します。
- 9 設定を確定するには、[保存] をクリックします。

サービス エンジン グループの設定の編集

システム管理者は、サポートされている仮想サービスの最大数と、サービス エンジン グループに対して予約されている仮想サービスの数を編集できます。

サービス エンジン グループを同期した後に、サポートされている仮想サービスの新しい最大数の方が予約されている仮想サービスの数よりも少ない場合、サービス エンジン グループは割り当て超過としてマークされます。

サービス エンジン グループが過剰に割り当てられている場合は、仮想サービスを作成する Edge Gateway で十分に容量が予約されている場合でも、新しい仮想サービスの作成は失敗することがあります。

仮想サービスの作成の失敗を回避するには、サービス エンジン グループの設定を編集するときに、サポートされる仮想サービスの最大数が最初に予約された仮想サービスの数を下回らないようにします。

前提条件

- [システム管理者] であることを確認します。
- [NSX-T Data Center Edge Gateway でのロード バランサの有効化](#)。
- [NSX-T Data Center Edge Gateway へのサービス エンジン グループの割り当て](#)

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [Edge Gateway] をクリックします。
- 3 サービス エンジン グループが割り当てられている NSX-T Data Center Edge Gateway をクリックします。
- 4 ロード バランサで、[サービス エンジン グループ] をクリックします。
- 5 [編集] をクリックします。
- 6 Edge Gateway で使用できる仮想サービスの最大許容数を編集します。
 値を小さくすることが必須でない場合は、小さくしないでください。値を小さくすると、仮想サービスの作成時に障害が発生する可能性があります。
- 7 Edge Gateway で確保されている使用可能な仮想サービスの数を編集します。
- 8 [保存] をクリックします。

ロード バランサ サーバ プールの追加

サーバ プールは、同じアプリケーションを実行して高可用性を実現するために構成された 1 台以上のサーバのグループです。

前提条件

- NSX-T Data Center Edge Gateway でのロード バランサの有効化。
- NSX-T Data Center Edge Gateway へのサービス エンジン グループの割り当て。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [Edge Gateway] をクリックします。
- 3 ロード バランサ プールを構成する NSX-T Data Center Edge Gateway をクリックします。
- 4 ロード バランサで [プール] をクリックし、[追加] をクリックします。

5 ロード バランサ プールの全般設定を行います。

- a サーバ プールのわかりやすい名前と、必要に応じて説明を入力します。
- b アルゴリズム バランシング メソッドを選択します。

ロード バランシング アルゴリズムは、サーバ プールのメンバー間での受信接続の分散方法を定義します。

オプション	説明
リスト コネクション	新しい接続は、現在の接続数が最も少ないサーバに送信されます。
ラウンド ロビン	新しい接続は、プール内の順序で次の適格なサーバに送信されます。
最速応答	新しい接続は、新しい接続または要求に対する応答が最速のサーバに送信されます。
コンシステント ハッシュ	新しい接続は、クライアントの IP アドレスを使用して IP ハッシュ キーを生成することによって、サーバ間で分散されます。
最小負荷	新しい接続は、サーバの接続数に関係なく、負荷が最小のサーバに送信されます。
最小数のサーバ	すべてのサーバですべての接続または要求を分散せずに、ロード バランサが現在のクライアントの負荷への対応に必要なサーバの最小数を決定します。
ランダム	ロード バランサはサーバをランダムに選択します。
最小数のタスク	負荷はサーバのフィードバックに基づいて適宜分散されます。
コア アフィニティ	各 CPU コアはサーバのサブセットを使用し、各サーバはコアのサブセットで使用されます。基本的に、サーバとコアは多対多でマッピングされています。

- c 作成時にサーバ プールを有効にするには、[状態] オプションをオンにします。
- d プール メンバーへのトラフィックに使用されるデフォルトのターゲット サーバ ポートを入力します。
- e (オプション) [グレースフル無効化のタイムアウト] テキストボックスに、プール メンバーを正常に無効にする最大時間を分単位で入力します。
仮想サービスは、無効にされたメンバーへの既存の接続を終了するまで、指定した時間待機します。
- f (オプション) パッシブ健全性監視を有効にするには、[パッシブ健全性監視] オプションをオンにします。
- g (オプション) アクティブ健全性監視を選択します。

オプション	説明
HTTP	健全性を検証する場合に、HTTP 要求と応答が使用されます。
HTTPS	健全性を検証する場合に、HTTPS によって暗号化された Web サーバに対して使用されます。
TCP	健全性を検証する場合に、TCP 接続が使用されます。
UDP	健全性を検証する場合に、UDP データグラムが使用されます。
PING	健全性を検証する場合に、ICMP ping が使用されます。

6 サーバ プールにメンバーを追加します。

- a [メンバー] タブをクリックし、[追加] をクリックします。
- b プール メンバーの IP アドレスを入力します。

- c [状態] オプションをオンにして、プール メンバーを有効にします。
 - d (オプション) サーバ プール メンバー用のカスタム ポートを追加します。
デフォルトのポート番号は、プールに対して入力されたターゲット ポートです。
 - e プール メンバーの比率を入力します。
各プール メンバーの比率は、各サーバ プール メンバーに送信されるトラフィックを表します。比率が 2 のサーバは、比率が 1 のサーバの 2 倍のトラフィックを受信します。デフォルト値は 1 です。
- 7 [SSL 設定] タブで、ロード バランサ プールのメンバーによって提示される証明書を検証するための SSL 設定を行います。
- a SSL を有効にするには、[SSL が有効] オプションをオンにします。
 - b プライベート キーを使用する証明書を非表示にし、CA 証明書のリストのみを表示するには、[サービス証明書を非表示] チェック ボックスをオンにします。
- 8 サーバ証明書のコモン ネーム チェックを有効にするには、[コモン ネーム チェック] オプションをオンにして、プールに最大 10 個のドメイン名を入力します。
- 9 [保存] をクリックします。

次のステップ

[仮想サービスの作成](#)。

仮想サービスの作成

仮想サービスは IP アドレスへのトラフィックを待機し、クライアント要求を処理し、有効な要求をロード バランサ サーバ プールのメンバーに転送します。

仮想サービスは、単一ネットワーク プロトコルを使用する IP アドレスとポートの組み合わせです。仮想サービスは外部ネットワークに通知され、クライアント要求を待機しています。クライアントが仮想サービスに接続すると、ロード バランサは構成されたロード バランサ サーバ プールのメンバーに要求を転送します。

仮想サービスの SSL 終端を保護するには、証明書ライブラリ内の証明書を使用します。詳細については、[証明書ライブラリへの証明書のインポート](#)を参照してください。

前提条件

- [NSX-T Data Center Edge Gateway](#) でのロード バランサの有効化。
- [NSX-T Data Center Edge Gateway](#) へのサービス エンジン グループの割り当て。
- [ロード バランサ サーバ プールの追加](#)。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [Edge Gateway] をクリックします。
- 3 仮想サービスを作成する [NSX-T Data Center Edge Gateway](#) をクリックします。
- 4 ロード バランサで [仮想サービス] をクリックし、[追加] をクリックします。

- 5 仮想サービスのわかりやすい名前と、必要に応じて説明を入力します。
- 6 作成時に仮想サービスを有効にするには、[有効] オプションをオンにします。
- 7 仮想サービスのサービス エンジン グループを選択します。
- 8 仮想サービスのロード バランサ プールを選択します。
- 9 仮想サービスの IP アドレスを入力します。
- 10 仮想サービスのタイプを選択します。

オプション	説明
HTTP	仮想サービスは、非セキュアなレイヤー 7 HTTP 要求を待機します。 このサービス タイプを選択すると、サービス ポート テキスト ボックスに 80 が自動入力されます。この番号は、別の有効なポート番号に置き換えることができます。
HTTPS	仮想サービスは、セキュアなレイヤー 7 HTTPS 要求を待機します。 このサービス タイプを選択すると、サービス ポート テキスト ボックスにポート 443 が自動入力されます。この番号は、別の有効なポート番号に置き換えることができます。SSL 終端に使用する SSL 証明書を選択します。
L4	仮想サービスは、レイヤー 4 要求を待機します。 このサービス タイプを選択すると、サービス ポート テキスト ボックスに 80 が自動入力されます。この番号は、別の有効なポート番号に置き換えることができます。
L4 TLS	仮想サービスは、セキュアなレイヤー 4 TLS 要求を待機します。 このサービス タイプを選択すると、サービス ポート テキスト ボックスに TCP ポート 443 が自動入力されます。この番号は、別の有効なポート番号に置き換えることができます。SSL 終端に使用する SSL 証明書を選択します。

- 11 [保存] をクリックします。

専用 vCenter Server インスタンスの管理

9

専用 vCenter Server インスタンスを使用すると、vSphere 環境の統合管理ポイント (CPOM) として VMware Cloud Director を使用できます。

vCenter Server インスタンスを VMware Cloud Director に追加するときに、インスタンスの目的を指定できます。

専用 vCenter Server

接続された vCenter Server インスタンスのインフラストラクチャは、Software-Defined Data Center (SDDC) としてカプセル化され、単一テナントの専用インスタンスになります。専用 vCenter Server インスタンスを作成するには、そのインスタンスに対するテナント アクセスを有効にします。テナント アクセスを有効にすると、専用 vCenter Server インスタンスをテナントに公開できるようになります。

共有 vCenter Server

プロバイダは、複数のプロバイダ VDC にまたがる vCenter Server インスタンスのさまざまなリソース プールを使用して、それらのリソース プールを複数のテナントに割り当てることができます。共有 vCenter Server インスタンスをテナントに公開することはできません。

なし

vCenter Server インスタンスには特定の目的がありません。

VMware Cloud Director は、専用 vCenter Server インスタンスおよび目的が設定されていない vCenter Server インスタンスの HTTP プロキシ サーバとして機能できます。

専用 vCenter Server インスタンスを使用すると、すべての vSphere 環境の統合管理ポイントとして VMware Cloud Director を使用できます。

- 対応する専用 vCenter Server をその組織にのみ公開することで、vCenter Server インスタンスのリソースを単一テナントの専用リソースにすることができます。テナントは、これらのリソースを他のテナントと共有しません。テナントはユーザー インターフェイスまたは API プロキシを使用してこの専用 vCenter Server インスタンスにアクセスできます。VPN は必須ではありません。
- VMware Cloud Director を軽量のディレクトリとして使用して、すべての vCenter Server インスタンスを登録することができます。
- VMware Cloud Director は、すべての vCenter Server インスタンスの API エンドポイントとして使用できます。

ターゲット vCenter Server インスタンスを VMware Cloud Director に接続している間、または接続した後に、テナント アクセスを有効にして、vCenter Server インスタンスを専用としてマークすることができます。

vCenter Server インスタンスを単独、または NSX Manager インスタンスと共に接続するを参照してください。

接続された vCenter Server インスタンスを使用すると、共有 vCenter Server または専用 vCenter Server のいずれかを作成できます。共有 vCenter Server インスタンスを作成した場合、この vCenter Server インスタンスを使用して専用 vCenter Server を作成したり、その逆を行ったりすることはできません。

テナントが基盤となる vSphere 環境にアクセスする際に使用できるエンドポイントを作成できます。ユーザーは VMware Cloud Director アカウントを使用することで、プロキシの有無に関係なく、コンポーネントのユーザーインターフェイスまたは API にログインできます。

VMware Cloud Director 内に専用 vCenter Server インスタンスがあることにより、vCenter Server を一般にアクセス可能にする必要がなくなります。アクセスを制御するには、VMware Cloud Director で SDDC へのテナント アクセスを有効または無効にします。

エンドポイントは、SDDC からコンポーネントへのアクセス ポイントです (vCenter Server インスタンス、ESXi ホスト、または NSX Manager インスタンスなど)。エンドポイントはプロキシに接続できます。プロキシを有効または無効にすると、そのプロキシを介したテナント アクセスを許可または停止できます。

VMware Cloud Director 10.2 以降では、テナント構成でマルチサイトの関連付けがサポートされている場合に、API を使用して専用の vCenter Server エンティティおよびプロキシ エンティティにクエリを実行すると、VMware Cloud Director はマルチサイト応答を返します。結果は、使用可能なすべての関連付けから取得されます。

専用 vCenter Server インスタンスの作成と管理

専用 vCenter Server インスタンスおよびプロキシを作成および管理するには、Service Provider Admin Portal または VMware Cloud Director OpenAPI を使用します。VMware Cloud Director OpenAPI については、『VMware Cloud Director OpenAPI のスタート ガイド』(<https://code.vmware.com>) を参照してください。

重要： VMware Cloud Director を使用するには、各専用 vCenter Server インスタンスに直接ネットワーク接続する必要があります。vCenter Server インスタンスが外部 Platform Services Controller を使用している場合は、VMware Cloud Director には Platform Services Controller インスタンスへの直接ネットワーク接続も必要になります。

プロキシが設定された専用 vCenter Server で VMware OVF Tool を使用するには、VMware Cloud Director を各 ESXi ホストに直接接続する必要があります。

1 専用 vCenter Server インスタンスを作成します。

VMware Cloud Director 環境に vCenter Server インスタンスを追加すると、[vCenter Server の追加] ウィザードでテナント アクセスを有効にして、専用の vCenter Server インスタンスを作成できるようになります。『**vCenter Server インスタンスの追加**』を参照してください。

専用の vCenter Server インスタンスを作成すると、そのインスタンスのデフォルト エンドポイントも作成されます。vCenter Server インスタンスの接続中に、プロキシを作成することもできます。ただし、デフォルトでは、デフォルト エンドポイントはどのプロキシにも接続されていません。プロキシに接続するには、デフォルトのエンドポイントを編集するか、新しいエンドポイントを作成する必要があります。『[エンドポイントの作成](#)』を参照してください。

VMware Cloud Director にすでに追加されていて、用途が指定されていない vCenter Server インスタンスのテナント アクセスを有効にすることができます。『[接続された vCenter Server のテナント アクセスの有効化](#)』を参照してください。テナント アクセスを有効にすると、vCenter Server インスタンスをテナントに公開できるようになります。

2 プロキシを追加します。

プロキシは vCenter Server インスタンスを VMware Cloud Director に接続するときに作成するか、後で作成することができます。vCenter Server インスタンスが外部 Platform Services Controller を使用している場合、VMware Cloud Director は Platform Services Controller のプロキシも作成します。親と子のプロキシを使用すると、テナントから特定のプロキシを非表示にしたり、親プロキシを使用して子プロキシのグループを有効または無効にしたりできます。vCenter Server インスタンスを VMware Cloud Director に追加した後にプロキシを作成する方法については、[基盤となる vCenter Server リソースにアクセスするためのプロキシの追加](#)を参照してください。

[vSphere リソース] の [プロキシ] タブでプロキシの編集、有効化、無効化、および削除ができます。

注： 専用 vCenter Server インスタンスにプロキシを追加するときは、証明書とサムプリントをアップロードする必要があります。これにより、プロキシが設定されたコンポーネントが自己署名証明書を使用する場合に、テナントが証明書とサムプリントを取得できるようになります。

証明書および証明書失効リスト (CRL) を表示および管理するには、[プロキシ証明書および CRL の管理](#)を参照してください。

3 作成されたプロキシの証明書およびサムプリントを取得し、証明書とサムプリントがあること、およびこれらが正しいことを確認します。『[プロキシ証明書および CRL の管理](#)』を参照してください。

4 1つ以上の組織に専用 vCenter Server インスタンスを公開します。

専用 vCenter Server インスタンスをテナントに公開し、VMware Cloud Director Tenant Portal に表示することができます。通常は、1つの vCenter Server インスタンスを1つのテナントにのみ公開する必要があります。『[専用 vCenter Server の公開](#)』を参照してください。

5 テナントが VMware Cloud Director Tenant Portal から専用 vCenter Server インスタンスおよびプロキシにアクセスできるようにするには、[CPOM 拡張機能] プラグインを組織に公開する必要があります。[組織からのプラグインの公開または公開解除](#)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。

- [接続された vCenter Server のテナント アクセスの有効化](#)
- [専用 vCenter Server の公開](#)

接続された vCenter Server のテナント アクセスの有効化

VMware Cloud Director にすでに追加されていて、用途が指定されていない vCenter Server インスタンスのテナント アクセスを有効にすることができます。テナント アクセスを有効にすると、専用 vCenter Server インスタンスが作成され、テナントに公開できるようになります。

接続された vCenter Server インスタンスを使用すると、共有 vCenter Server または専用 vCenter Server のいずれかを作成できます。共有 vCenter Server インスタンスを作成した後で、それを専用 vCenter Server として使用する場合は、まず vCenter Server インスタンスのリソースを使用しているすべてのプロバイダ仮想データセンター (VDC) を削除する必要があります。共有 vCenter Server インスタンスにリンクされているすべてのプロバイダ VDC を削除すると、ステータスが [なし] に変更されます。

前提条件

接続された、専用でも共有でもない vCenter Server が環境内に 1 つ以上あることを確認します。

手順

- 1 上部ナビゲーション バーの [リソース] で [インフラストラクチャ リソース] をクリックします。
- 2 左側のパネルで [vCenter Server インスタンス] を選択します。
- 3 [使用率] 列で目的が指定されていない vCenter Server を選択します。
- 4 [テナント アクセスの有効化] をクリックします。

次のステップ

[専用 vCenter Server の公開](#)を参照してください。

専用 vCenter Server の公開

専用 vCenter Server をテナントに公開し、VMware Cloud Director Tenant Portal を使用して表示することができます。デフォルトでは、1 つの vCenter Server を 1 つのテナントにのみ公開する必要があります。

デフォルトでは、SDDC は、対応する専用 vCenter Server インスタンスをその組織のみに公開することによって単一テナント専用処理する vCenter Server インスタンスです。テナントは、専用 vCenter Server インスタンスのリソースを他のテナントと共有しません。専用 vCenter Server インスタンスを複数のテナントに公開すると、テナントの境界違反になります。ただし、テナントが複数の専用 vCenter Server インスタンスにアクセスしなければならない場合もあります。このような場合は、専用 vCenter Server インスタンスを複数のテナントに公開できます。

前提条件

- VMware Cloud Director 環境で、テナント アクセスが有効になっている vCenter Server インスタンスが 1 つ以上あることを確認します。『[9 章 専用 vCenter Server インスタンスの管理](#)』を参照してください。

手順

- 1 上部ナビゲーション バーの [リソース] で [インフラストラクチャ リソース] をクリックします。
- 2 左側のパネルで [vCenter Server インスタンス] を選択します。

3 テナント アクセスが有効な vCenter Server を選択します。

テナント アクセスが有効な vCenter Server インスタンスは、[使用率] 列に [専用] 値が設定されています。

4 [テナントの管理] をクリックします。

5 vCenter Server インスタンスを公開するテナントを選択します。

リストからテナントの選択を解除すると、vCenter Server が公開解除されます。

6 [保存] をクリックします。

次のステップ

ユーザーが VMware Cloud Director Tenant Portal から専用 vCenter Server インスタンスおよびプロキシにアクセスできるようにするには、[CPOM 拡張機能] プラグインを組織に公開する必要があります。[組織からのプラグインの公開または公開解除](#)を参照してください。

システム管理者およびロールの管理

10

VMware Cloud Director Service Provider Admin Portal を使用すると、システム管理者を VMware Cloud Director に対して個別に、または LDAP グループの一部として追加することができます。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。

注： VMware Cloud Director 9.5 以降では、サービス プロバイダは VMware Cloud Director Service Provider Admin Portal または vCloud OpenAPI を使用してプロバイダ ロールを作成し、プロバイダ ユーザーおよびグループを管理できます。プロバイダのロール、ユーザー、およびグループの管理の詳細については、『VMware Cloud Director Service Provider Admin Portal Guide』を参照してください。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。

この章には、次のトピックが含まれています。

- 権限およびロールの管理
- プロバイダ ユーザーおよびグループの管理

権限およびロールの管理

権限は、VMware Cloud Director のアクセス コントロールの基本単位です。ロールとは、ロール名に一連の権限が関連付けられたものです。組織ごとに異なる権限およびロールを設定できます。

VMware Cloud Director は、ロールとそれに関連付けられた権限を使用して、ユーザーまたはグループが操作の実行を許可されているかどうかを判断します。VMware Cloud Director のガイドに記載されている手順の多くには、前提条件ロールが含まれています。これらの前提条件では、指定されたロールが、未変更の事前定義ロール、または対応する一連の権限を含むロールであることを想定しています。

システム管理者は権限バンドルおよびグローバル テナント ロールを使用して、各組織で使用可能な権限およびロールを管理することができます。

VMware Cloud Director をインストールしたシステムには、システム権限バンドルのみが含まれており、このバンドルにはシステムで使用可能なすべての権限が含まれています。システム権限バンドルは、どの組織にも公開されません。システムには、すべての組織に公開される組み込みのグローバル テナント ロールも含まれます。事前定義済みロールの詳細については、「[事前定義ロールとその権限](#)」を参照してください。

VMware Cloud Director バージョン 9.1 以前からアップグレードしたシステムには、システム権限バンドルの他に、既存の各組織のレガシー権限バンドルも含まれています。各レガシー権限バンドルにはアップグレード時点で関連付けられた組織で使用可能な権限で、この組織でのみ公開されているものが含まれています。

注： 既存の組織の権限バンドル モデルを使用するには、対応するレガシー権限バンドルを削除する必要があります。

VMware Cloud Director バージョン 9.1 以前からアップグレードした場合、既存のロール テンプレートは、グローバル テナント ロールとしてすべての組織に公開され、ロール テンプレートからリンク解除された既存のロールは、組織がテナント固有のロールとして使用できます。

権限に関する用語

権限

各権限は、VMware Cloud Director で特定のオブジェクト タイプへのアクセスを管理および表示します。権限は、関連するオブジェクトに応じて、vApp、カタログ、組織などのさまざまなカテゴリに属しています。プロバイダ組織には、システムで使用可能なすべての権限が含まれています。システム管理者は、各組織が使用できる権限を定義します。VMware Cloud Director に含まれる権限を作成または変更することはできません。

権限バンドル

システム管理者は権限バンドルを使用して、各組織が使用できる権限を管理できます。権限バンドルとは、システム管理者が1つ以上の組織に公開できる権限のセットを指します。システム管理者は、サービスの階層、個別の収益化可能な機能、またはその他の任意の権限グループ分けに応じて権限バンドルを作成して、公開できます。権限バンドルを表示および管理できるのは、システム管理者のみです。複数のバンドルを同じ組織に公開できません。

組織の権限

組織の権限とは、組織が使用できる権限の完全なセットを指します。組織の権限は複数の権限バンドルで構成されますが、組織管理者およびユーザーにはフラットな権限セットが表示され、テナント固有のロールを作成および変更する際に使用できるようになります。

ロールに関する用語

ロール

ロールとは、1つまたは複数のユーザーおよびグループに割り当てることができる権限セットを指します。ユーザーまたはグループを作成またはインポートするときは、ロールを割り当てる必要があります。

プロバイダ ロール

プロバイダ ロールとは、プロバイダ組織のみが使用できるロール セットを指します。プロバイダ ロールは、プロバイダ ユーザーにのみ割り当てることができます。システム管理者は、カスタム プロバイダ ロールを作成できます。

テナント ロール

テナント ロールとは、組織が使用できるロール セットのことです。

システム管理者は、グローバル テナント ロールを作成および編集し、1 つ以上の組織に公開することができます。グローバル テナント ロールは、公開先の組織内のテナント ユーザーに割り当てることができます。組織管理者は、グローバル テナント ロールを編集できません。

注： テナント ユーザーは、組織に公開されているロール内の権限のみを使用できます。

テナント固有のロール

組織管理者は、組織に対してローカルなテナント固有のロールを作成および編集できます。テナント固有のロールは、所属先の組織内のテナント ユーザーにのみ割り当てることができます。テナント固有のロールには、組織の権限のサブセットのみを含めることができます。

テナント固有のロールの管理の詳細については、『VMware Cloud Director Tenant Portal Guide』を参照してください。

事前定義ロールとその権限

VMware Cloud 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、プロバイダ組織のみに設定されています。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、[システム管理者の権限](#)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 Cloud Director OpenAPI 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る場合、ユーザーには、そのユーザーの OAuth トークンの `roles` アレイで指定される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る場合、ユーザーには、組織の `OrgFederationSettings` にある `SamlAttributeMapping` 要素内の `RoleAttributeName` 要素に名前が表示される 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

システム管理者は、Service Provider Admin Portal を使用して、ロールに含まれる権限のリストを表示できます。

- 1 上部ナビゲーション バーで [管理] をクリックします。

2 左側のパネルの [プロバイダ アクセス コントロール] で、[ロール] を選択します。

3 表示するロールの名前をクリックします。

組織管理者は、Service Provider Admin Portal または Cloud Director OpenAPI を使用して、ロールの権限を表示できます。また、組織にローカルなロールを作成することもできます。

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 ロール内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。

システム管理者の権限

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、デフォルトで VMware Cloud Director に関するすべての権限が含まれています。

システム管理者ロールには、VMware Cloud Director に関するすべての権限が含まれています。このリストは、システム管理者のみが使用できる権限で構成されています。システム管理者ロールには [事前定義グローバル テナント ロールの権限](#)も含まれています。

表 10-1. システム管理者のみがデフォルトで使用可能な権限

このリリースの新機能	権限名
	すべての組織 VDC へのアクセス
	アクセス コントロール リスト：管理
	アクセス コントロール リスト：表示
	追加サービス：ワークフローの実行
	追加サービス：実行中のワークフローを表示
	追加サービス：ワークフローの表示
	リソース プールの選択：表示
✓	アドバイザリの定義：作成と削除
✓	アドバイザリの定義：読み取り
	代替管理者エンティティ：表示
	AMQP 設定：管理
	AMQP 設定：表示
	API Explorer：表示
	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：カタログを作成/削除
	カタログ：プロパティの編集

表 10-1. システム管理者のみがデフォルトで使用可能な権限（続き）

このリリースの新機能	権限名
	カタログ：vSphere からのメディアをインポート
	カタログ：公開
	カタログ：シャドウ仮想マシン ビュー
	カタログ：共有
	カタログ：VCSP 公開サブスクリプション
	カタログ：VCSP 公開サブスクリプションのキャッシング
	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
	セル構成：表示
	証明書ライブラリ：管理
	証明書ライブラリ：表示
	クラウド トンネル サーバ：管理
	クラウド トンネル サーバ：表示
	コンテンツ ライブラリのシステム設定：管理
	コンテンツ ライブラリのシステム設定：表示
	カスタム エンティティ：カスタム エンティティ定義の作成
	カスタム エンティティ：カスタム エンティティ定義の削除
	カスタム エンティティ：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：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 エンティティ定義の表示
	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
	データストア：削除
	データストア：編集
	データストア：有効化または無効化
	データストア：vSphere で開く
	データストア：表示
	直接的な組織 VDC ネットワーク：管理

表 10-1. システム管理者のみがデフォルトで使用可能な権限（続き）

このリリースの新機能	権限名
	分散仮想スイッチ：vSphere で開く
	Edge クラスタ：管理
	Edge クラスタ：表示
	拡張機能サービス API の定義：管理
	拡張機能サービス API の定義：表示
	拡張機能サービス：表示
	拡張機能：表示
	外部サービス：管理
	外部サービス：表示
✓	全般 ACL：管理
✓	全般 ACL：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
	全般：エラー詳細の表示
	グローバル ロール：編集
	グローバル ロール：表示
	グループ/ユーザー：表示
	ホスト：有効化または無効化
	ホスト：管理
	ホスト：vSphere で開く
	ホスト：準備または準備解除
	ホスト：修復
	ホスト：アップグレード
	ホスト：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

表 10-1. システム管理者のみがデフォルトで使用可能な権限（続き）

このリリースの新機能	権限名
	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
	Kerberos 設定：管理
	Kerberos 設定：表示
	LDAP 設定：管理
	LDAP 設定：表示
	ライセンス レポート：表示
✓	ロード バランサ コントローラ：編集
✓	ロード バランサ コントローラ：表示
✓	ロード バランサ サービス エンジン グループの割り当て：編集
✓	ロード バランサ サービス エンジン グループの割り当て：表示
✓	ロード バランサ サービス エンジン グループ：編集
✓	ロード バランサ サービス エンジン グループ：表示
	ローカライズ リソース：管理
	ネットワーク ブール：作成または削除
	ネットワーク ブール：編集
	ネットワーク ブール：vSphere で開く
	ネットワーク ブール：修復
	ネットワーク ブール：表示
	NSX-T：編集
	NSX-T：表示
	オブジェクト エクステンション：管理
	オブジェクト エクステンション：表示

表 10-1. システム管理者のみがデフォルトで使用可能な権限（続き）

このリリースの新機能	権限名
	組織ネットワーク：作成または削除
	組織ネットワーク：プロパティの編集
	組織ネットワーク：vSphere で開く
	組織ネットワーク：表示
✓	組織の割り当て容量：管理
	組織 VDC コンピューティング ポリシー：管理者ビュー
	組織 VDC コンピューティング ポリシー：管理
	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：有効化/無効化
	組織 VDC 分散ファイアウォール：ルールの表示
	組織 VDC ゲートウェイ：BGP ルーティングの構成
	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構成
	組織 VDC ゲートウェイ：IPsec VPN の構成
	組織 VDC ゲートウェイ：L2 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：OSPF ルーティングの構成
	組織 VDC ゲートウェイ：リモート アクセスの構成
	組織 VDC ゲートウェイ：ルート アドバタイズの設定
✓	組織 VDC ゲートウェイ：SLAAC プロファイルの構成
	組織 VDC ゲートウェイ：SSL VPN 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：システム ログの構成

表 10-1. システム管理者のみがデフォルトで使用可能な権限（続き）

このリリースの新機能	権限名
	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：作成
	組織 VDC ゲートウェイ：削除
	組織 VDC ゲートウェイ：分散ルーティング
	組織 VDC ゲートウェイ：インポート
	組織 VDC ゲートウェイ：フォーム ファクタの修正
	組織 VDC ゲートウェイ：更新
	組織 VDC ゲートウェイ：プロパティの更新
	組織 VDC ゲートウェイ：アップグレード
	組織 VDC ゲートウェイ：表示
	組織 VDC ゲートウェイ：BGP ルーティングの表示
	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：L2 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：OSPF ルーティングの表示
	組織 VDC ゲートウェイ：リモート アクセスの表示
	組織 VDC ゲートウェイ：ルート アドバタイズの表示
✓	組織 VDC ゲートウェイ：SLAAC プロファイルの表示
	組織 VDC ゲートウェイ：SSL VPN 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 Kubernetes ポリシー：編集
	組織 VDC 名前付きディスク：所有者の変更
	組織 VDC 名前付きディスク：作成
	組織 VDC 名前付きディスク：削除

表 10-1. システム管理者のみがデフォルトで使用可能な権限（続き）

このリリースの新機能	権限名
	組織 VDC 名前付きディスク：プロパティの編集
	組織 VDC 名前付きディスク：暗号化ステータスの表示
	組織 VDC 名前付きディスク：プロパティの表示
	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：インポート
	組織 VDC ネットワーク：表示
	組織 VDC リソース プール：vSphere で開く
	組織 VDC リソース プール：表示
✓	組織 VDC 共有名前付きディスク：作成
	組織 VDC ストレージ ポリシー：編集
	組織 VDC ストレージ ポリシー：有効化または無効化
	組織 VDC ストレージ ポリシー：vSphere で開く
	組織 VDC ストレージ ポリシー：削除
	組織 VDC ストレージ ポリシー：機能の表示
	組織 VDC ストレージ プロファイル：デフォルトの設定
	組織 VDC：作成
	組織 VDC：削除
	組織 VDC：ACL の編集
	組織 VDC：有効化または無効化
	組織 VDC：拡張編集
	組織 VDC：拡張表示
	組織 VDC：ファイアウォールの管理
	組織 VDC：簡易編集
	組織 VDC：ユーザー表示
	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：有効化または無効化

表 10-1. システム管理者のみがデフォルトで使用可能な権限（続き）

このリリースの新機能	権限名
	組織：作成または削除
	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：制限の編集
	組織：名前の編集
	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 の編集中に IdP からユーザー/グループを暗黙的にインポート
	組織：テナント ストレージの移行
	組織：管理者クエリを実行
	組織：プロバイダ LDAP をテナントとして使用
	組織：表示
	組織：メトリックの表示
	ポート グループ：vSphere で開く
	環境設定：環境設定の定義の管理
	プロバイダ ネットワーク：作成または削除
	プロバイダ ネットワーク：編集
	プロバイダ ネットワーク：vSphere で開く
	プロバイダ ネットワーク：表示
	プロバイダ VDC コンピューティング ポリシー：管理
	プロバイダ VDC コンピューティング ポリシー：表示
	プロバイダ VDC リソース プール：仮想マシンの移行
	プロバイダ VDC リソース プール：vSphere で開く

表 10-1. システム管理者のみがデフォルトで使用可能な権限（続き）

このリリースの新機能	権限名
	プロバイダ VDC リソース プール：表示
	プロバイダ VDC ストレージ ポリシー：編集
	プロバイダ VDC ストレージ ポリシー：有効化または無効化
	プロバイダ VDC ストレージ ポリシー：vSphere で開く
	プロバイダ VDC ストレージ ポリシー：削除
	プロバイダ VDC ストレージ ポリシー：表示
	プロバイダ VDC：リソース プールの追加
	プロバイダ VDC：作成または削除
	プロバイダ VDC：リソース プールの削除
	プロバイダ VDC：編集
	プロバイダ VDC：有効化または無効化
	プロバイダ VDC：リソース プールの有効化または無効化
	プロバイダ VDC：vSphere VXLAN の有効化
	プロバイダ VDC：マージ
	プロバイダ VDC：表示
✓	割り当てポリシー機能：表示
✓	割り当てポリシー：管理
✓	割り当てポリシー：表示
	仮想マシンの再ロード：管理
	リソース クラス アクション：管理
	リソース クラス アクション：表示
	リソース プール：開く
	リソース プール：vSphere で開く
	リソース プール：表示
	権限：管理
	権限：表示
	権限バンドル：編集
	権限バンドル：表示

表 10-1. システム管理者のみがデフォルトで使用可能な権限（続き）

このリリースの新機能	権限名
	ロール：作成、編集、削除、またはコピー
	SDDC：管理
	SDDC：プロキシの管理
	SDDC：表示
	セクタ エクステンション：管理
	セクタ エクステンション：表示
	サービス アプリケーション：管理
	サービス アプリケーション：表示
	サービス認証：管理
	サービス構成：管理
	サービス構成：表示
	サービス ライブラリ：サービス ライブラリの作成
	サービス ライブラリ：サービス ライブラリからサービスを削除
	サービス ライブラリ：サービス メタデータの編集
	サービス ライブラリ：サービスのコンテンツの編集
	サービス ライブラリ：サービス ライブラリの表示
	サービス リンク：管理
	サービス リンク：表示
	サービス リソース タイプ：管理
	サービス リソース タイプ：表示
	サービス リソース：管理
	サービス リソース：表示
	共有組織 VDC ネットワーク：管理
	サイト：編集
	サイト：表示
	SSL 設定：表示
✓（バージョン 10.2.2 以降で使用可能）	SSL 設定：管理
✓	SSL：接続のテスト

表 10-1. システム管理者のみがデフォルトで使用可能な権限（続き）

このリリースの新機能	権限名
	取り残されたアイテム：管理
	取り残されたアイテム：表示
✓（バージョン 10.2.2 以降で使用可能）	サポートされているストレージ エンティティ タイプ：管理
	システム操作：システム操作を実行
	システム組織：管理
	システム組織：表示
	システム設定：管理
	システム設定：表示
✓	Tanzu Kubernetes ゲスト クラスタ：管理者の完全コントロール
✓	Tanzu Kubernetes ゲスト クラスタ：管理者の表示
✓	Tanzu Kubernetes ゲスト クラスタ：編集
✓	Tanzu Kubernetes ゲスト クラスタ：完全コントロール
✓	Tanzu Kubernetes ゲスト クラスタ：表示
	タスク：再開、中止、または失敗
	タスク：更新
	タスク：タスクの表示
	トークン：管理
	トークン：すべての管理
	トラストストア：管理
	トラストストア：表示
	ユーザー インターフェイス プラグイン：定義、アップロード、変更、削除、関連付け、または関連付け解除
	ユーザー インターフェイス プラグイン：表示
	ユーザー インターフェイス ポータルのブランド：管理
	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
	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：マイ クラウドへの追加

表 10-1. システム管理者のみがデフォルトで使用可能な権限（続き）

このリリースの新機能	権限名
	vApp テンプレート：所有者の変更
	vApp テンプレート ダウンロード
	vApp テンプレート：ストレージ リース期限の強制
	vApp テンプレート：インポート
	vApp テンプレート：vSphere で開く
	vApp：すべての追加構成を許可
	vApp：イーサネット一体化の追加構成を許可
	vApp：遅延の追加構成を許可
	vApp：一致する追加構成を許可
	vApp：NUMA ノード アフィニティの追加構成を許可
	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：すべての VDC タイプの仮想マシン CPU およびメモリ予約の編集
	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：メンテナンス モードの開始/終了
	vApp：ランタイム リース期限の強制
	vApp：ストレージ リース期限の強制
	vApp：インポート オプション
	vApp：メンテナンス管理

表 10-1. システム管理者のみがデフォルトで使用可能な権限（続き）

このリリースの新機能	権限名
	vApp : 仮想マシンのパスワード設定を管理
	vApp : vSphere で開く
	vApp : パワー操作
	vApp : シャドウ仮想マシン ビュー
	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 : 仮想マシンおよび仮想マシンのディスクの暗号化ステータスを表示
	vApp : 仮想マシンのメトリックを表示
	vApp : 仮想マシンのブート オプション
	vApp : 仮想マシンのコンプライアンス チェック
	vApp : 仮想マシンの移行、強制的な展開解除、再配置、統合
	VAPP_VM_METADATA_TO_VCENTER
	vCD の拡張機能 : 登録、登録解除、更新、関連付け、または関連付け解除
	vCD の拡張機能 : 表示
	vCenter Server : 接続または接続解除
	vCenter Server : 有効化または無効化
	vCenter Server : vSphere で開く
	vCenter Server : 更新
	vCenter Server : 表示
	VDC グループ : 構成
✓	VDC グループ : ログ記録の構成
	VDC グループ : 表示
	VDC テンプレート : ACL 管理
	VDC テンプレート : 拡張表示
	VDC テンプレート : インスタンス化

表 10-1. システム管理者のみがデフォルトで使用可能な権限（続き）

このリリースの新機能	権限名
	VDC テンプレート：管理
	VDC テンプレート：表示
	VMC：SDDC の登録
✓	VMWARE：NATIVECLUSTER：管理者の完全コントロール
✓	VMWARE：NATIVECLUSTER：管理者の表示
✓	VMWARE：NATIVECLUSTER：編集
✓	VMWARE：NATIVECLUSTER：完全コントロール
✓	VMWARE：NATIVECLUSTER：表示
	vRealize Orchestrator：テナントへのワークフローの公開および公開解除
	vRealize Orchestrator：vRealize Orchestrator サーバの登録および登録解除
	vRealize Orchestrator：登録済み vRealize Orchestrator サーバを表示
	vSphere Server：管理
	vSphere Server：プロキシの管理
	vSphere Server：プロキシ構成の管理
	vSphere Server：表示

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。

VMware Cloud 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：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	✓	✓			

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
	カタログ：共有	✓	✓			
	カタログ：VCSP 公開サブスクリプション	✓	✓			
	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	✓				
	証明書ライブラリ：管理	✓				
	証明書ライブラリ：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	✓				
	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	✓				

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
	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	✓				
	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構成	✓				
	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	✓				

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：固定ルーティン グの表示	✓				
	組織 VDC 名前付きディスク：所有者の変 更	✓	✓			
	組織 VDC 名前付きディスク：作成	✓	✓	✓		
	組織 VDC 名前付きディスク：削除	✓	✓	✓		
	組織 VDC 名前付きディスク：プロパティ の編集	✓	✓	✓		
	組織 VDC 名前付きディスク：暗号化ステ ータスの表示	✓		✓		
	組織 VDC 名前付きディスク：プロパティ 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：表示	✓		✓		
	組織 VDC ストレージ ポリシー：機能の 表示	✓				
	組織 VDC ストレージ プロファイル：デ フォルトの設定	✓				
	組織 VDC：ACL の編集	✓				
	組織 VDC：ファイアウォールの管理	✓				
	組織 VDC：簡易編集	✓				
	組織 VDC：ユーザー表示	✓	✓			
	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：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	✓				

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：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 の編集中に 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	✓				
✓	割り当てポリシー機能：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	✓				
✓	SSL：接続のテスト	✓	✓			
	ユーザー インターフェイス プラグイン：表示	✓	✓	✓	✓	
✓ (バージョン 10.2.1 以降で使用可能)	トラストストア：管理	✓				
✓ (バージョン 10.2.1 以降で使用可能)	トラストストア：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	✓	✓			
	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：マイ クラウドへの追加	✓	✓	✓	✓	
	vApp テンプレート：所有者の変更	✓	✓			
	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	✓	✓	✓		

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 : 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 : 仮想マシンおよび仮想マシンのデ ィスクの暗号化ステータスを表示	✓		✓		
	vApp : 仮想マシンのメトリックを表示	✓		✓	✓	
	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 メタデータ	✓	✓	✓		
✓	VDC グループ : 構成	✓				
✓	VDC グループ : ログ記録の構成	✓				
✓	VDC グループ : 表示	✓				
	VDC テンプレート : インスタンス化	✓				
	VDC テンプレート : 表示	✓				

権限バンドルの管理

システム管理者は権限バンドルを作成し、クラウド内の 1 つ以上の組織に公開できます。既存の権限バンドルを編集および削除できます。クラウド内の組織から権限バンドルの公開を解除することができます。

権限バンドルの作成

権限のセットを権限バンドルとしてグループ化し、システム内の 1 つ以上の組織に公開できます。

手順

- 1 上部ナビゲーション バーで [管理] を選択します。
- 2 左側のパネルの [テナント アクセス コントロール] で、[権限バンドル] を選択します。
- 3 [追加] をクリックします。
- 4 新しい権限バンドルの名前と、オプションで説明を入力します。
- 5 このバンドルに関連付ける権限を選択します。

権限は、関連するオブジェクトへのアクセス権を表示および管理するために、カテゴリとサブカテゴリにグループ化されています。

権限はサブカテゴリ別に表示または管理するか、グローバルに表示または管理して、個別に選択することができます。

カテゴリ	説明
アクセス コントロール	組織、権限、ロール、およびユーザーを表示して管理するための権限が含まれています。
管理	一般的な設定やマルチサイトの設定を表示して管理するための権限が含まれています。
コンピュート	組織およびプロバイダの仮想データセンター、vApp、組織仮想データセンター テンプレート、および仮想マシンの監視を表示して管理するための権限が含まれています。
拡張機能	VMware Cloud Director プラグインおよび拡張機能を表示して管理するための権限が含まれています。
インフラストラクチャ	vSphere リソースを表示して管理するための権限が含まれています。
ライブラリ	カタログおよびカタログ項目を表示して管理するための権限が含まれています。
ネットワーク	ネットワーク リソースを表示して管理するための権限が含まれています。

- 6 [保存] をクリックします。

次のステップ

新しく作成した権限バンドルは、システム内の 1 つ以上の組織に公開できます。[権限バンドルの公開または公開の解除](#)を参照してください。

権限バンドルのクローン作成

既存の権限バンドルをテンプレートとして新規バンドルの作成に使用できます。

前提条件

VMware Cloud Director に新規ロールを追加する権限があることを確認します。

手順

- 1 上部ナビゲーション バーで [管理] を選択します。
- 2 左側のパネルの [テナント アクセス コントロール] で、[権限バンドル] を選択します。
- 3 クローン作成する権限バンドルを選択して、[クローン作成] をクリックします。
- 4 [権限バンドルのクローン作成] ウィンドウで、クローン作成されたバンドルの名前と説明を入力します。
- 5 (オプション) クローン作成された権限を編集するには、[選択した権限の変更] をオンに切り替え、クローン作成されたロールに対し変更する権限を選択または選択解除します。
- 6 [保存] をクリックします。

権限バンドルの公開または公開の解除

権限バンドルをシステム内の 1 つ以上の組織に公開できます。権限バンドルを組織に公開すると、このバンドル内の権限は組織の権限セットの一部となります。

組織の権限は複数の権限バンドルで構成されますが、組織管理者およびユーザーにはフラットな権限セットが表示され、これらを使用してロールを作成および変更できるようになります。

手順

- 1 上部ナビゲーション バーで [管理] を選択します。
- 2 左側のパネルの [テナント アクセス コントロール] で、[権限バンドル] を選択します。
- 3 ターゲット バンドルの横にあるラジオ ボタンを選択して、[公開] をクリックします。
- 4 バンドルを公開するには：
 - a [テナントに公開] を選択します。
 - b ロールを公開する組織を選択します。
 - バンドルをシステム内のすべての既存の組織および新規に作成された組織に公開する場合は、[すべてのテナントに公開] を選択します。
 - システム内の特定の組織にバンドルを公開する場合は、組織を個別に選択します。
- 5 バンドルの公開を解除するには：
 - システム内のすべての組織からバンドルの公開を解除する場合は、[テナントに公開] を選択解除します。
 - システム内の特定の組織からバンドルを公開解除する場合は、[すべてのテナントに公開] を選択解除して、組織を個別に選択解除します。
- 6 [保存] をクリックします。

結果

公開されたバンドル内の権限は選択した組織内で使用することができ、これらの組織内のロールで使用することができます。

公開解除されたロール内の権限は選択した組織から削除され、これらの組織内のロールで使用できなくなります。

権限バンドルの表示および編集

権限バンドルに含まれている権限を表示できます。バンドルの名前、説明、および権限を変更できます。

手順

- 1 上部ナビゲーション バーで [管理] を選択します。
- 2 左側のパネルの [テナント アクセス コントロール] で、[権限バンドル] を選択します。
- 3 ターゲット バンドルの名前をクリックします。

権限カテゴリを展開して、バンドルに関連付けられている権限を表示できます。

- 4 バンドルを編集して、[保持] をクリックします。

結果

バンドルの権限を変更した場合、新しい権限セットが権限バンドルの公開先となるすべての組織に適用されます。

権限バンドルの削除

組織で使用しなくなった権限バンドルは削除することができます。

手順

- 1 上部ナビゲーション バーで [管理] を選択します。
- 2 左側のパネルの [テナント アクセス コントロール] で、[権限バンドル] を選択します。
- 3 対象のバンドルの横にあるラジオ ボタンを選択し、[削除] をクリックします。
- 4 確認するには、[OK] をクリックします。

グローバル テナント ロールの管理

システム管理者はグローバル テナント ロールを作成し、作成したロールをクラウド内の 1 つ以上の組織に公開できます。既存のグローバル テナント ロールを編集および削除できます。クラウド内の個別の組織でグローバル テナント ロールの公開を解除できます。

VMware Cloud Director の初回インストールおよびセットアップを行うと、システムには、すべての組織に公開されている事前定義済みのグローバル テナントのセットが含まれます。[事前定義ロールとその権限](#)を参照してください。

グローバル テナント ロールの作成

システム内の 1 つ以上の組織に公開できるグローバル テナント ロールを作成できます。

VMware Cloud Director の初回インストールおよびセットアップ後、システムには、すべての組織に公開される事前定義済みグローバル テナント ロールが含まれています。事前定義済みロールの詳細については、「[事前定義ロールとその権限](#)」を参照してください。

システムにカスタム グローバル ロールを追加することもできます。

手順

- 1 上部ナビゲーション バーで [管理] を選択します。
- 2 左側のパネルの [テナント アクセス コントロール] で、[グローバル ロール] を選択します。
- 3 [追加] をクリックします。
- 4 新しいロールの名前と、オプションで説明を入力します。
- 5 ロールに関連付ける権限を選択します。

権限は、関連するオブジェクトへのアクセス権を表示および管理するために、カテゴリとサブカテゴリにグループ化されています。

権限はサブカテゴリ別に表示または管理するか、グローバルに表示または管理して、個別に選択することができます。

カテゴリ	説明
アクセス コントロール	組織、権限、ロール、およびユーザーを表示して管理するための権限が含まれています。
管理	一般的な設定やマルチサイトの設定を表示して管理するための権限が含まれています。
コンピュート	組織およびプロバイダの仮想データセンター、vApp、組織仮想データセンター テンプレート、および仮想マシンの監視を表示して管理するための権限が含まれています。
拡張機能	VMware Cloud Director プラグインおよび拡張機能を表示して管理するための権限が含まれています。
インフラストラクチャ	vSphere リソースを表示して管理するための権限が含まれています。
ライブラリ	カタログおよびカタログ項目を表示して管理するための権限が含まれています。
ネットワーク	ネットワーク リソースを表示して管理するための権限が含まれています。

- 6 [保持] をクリックします。

結果

作成時、新しいグローバル テナント権限は、VMware Cloud Director プロバイダの組織のみが利用できます。

次のステップ

新しく作成したロールは、システム内の 1 つ以上の組織に公開できます。[グローバル テナント ロールの公開または公開の解除](#)を参照してください。

グローバル テナント ロールのクローン作成

既存のグローバル テナント ロールをテンプレートとして新規ロールの作成に使用できます。

前提条件

VMware Cloud Director に新規ロールを追加する権限があることを確認します。

手順

- 1 上部ナビゲーション バーで [管理] を選択します。
- 2 左側のパネルの [テナント アクセス コントロール] で、[グローバル ロール] を選択します。
- 3 クローン作成するロールを選択して、[クローン作成] をクリックします。
- 4 [グローバル ロールのクローン作成] ウィンドウで、クローン作成したロールの名前と説明を入力します。
- 5 (オプション) クローン作成された権限を編集するには、[選択した権限の変更] をオンに切り替え、クローン作成されたロールに対し変更する権限を選択または選択解除します。
- 6 [保存] をクリックします。

グローバル テナント ロールの公開または公開の解除

グローバル テナント ロールをシステム内の 1 つ以上の組織に公開できます。ロールを組織に公開すると、このロールはテナント ロールの組織セットの一部となります。

前提条件

組織からグローバル テナント ロールの公開を解除する場合は、このロールに割り当てられたユーザーが組織内にいないことを確認します。

手順

- 1 上部ナビゲーション バーで [管理] を選択します。
- 2 左側のパネルの [テナント アクセス コントロール] で、[グローバル ロール] を選択します。
- 3 ターゲット ロールの横にあるラジオ ボタンを選択して、[公開] をクリックします。
- 4 ロールを公開するには：
 - a [テナントに公開] を選択します。
 - b ロールを公開する組織を選択します。
 - ロールをシステム内のすべての既存の組織および新規に作成された組織に公開する場合は、[すべてのテナントに公開] を選択します。
 - システム内の特定の組織にロールを公開する場合は、組織を個別に選択します。
- 5 ロールの公開を解除するには：
 - システム内のすべての組織でロールの公開を解除する場合は、[テナントに公開] を選択解除します。
 - システム内の特定の組織でロールの公開を解除する場合は、[すべてのテナントに公開] を選択解除して、組織を個別に選択解除します。

6 [保存] をクリックします。

結果

公開されたロールは、選択した組織内で使用することができ、組織内のユーザーに割り当てることができます。組織管理者は、組織に公開されたグローバル テナント ロールを編集できません。

公開解除されたロールは選択した組織から削除されるため、これらの組織内のユーザーに割り当ててはできません。

グローバル テナント ロールの表示および編集

グローバル テナント ロールに含まれている権限を表示できます。グローバル テナント ロールの名前、説明、および権限を変更できます。

手順

- 1 上部ナビゲーション バーで [管理] を選択します。
- 2 左側のパネルの [テナント アクセス コントロール] で、[グローバル ロール] を選択します。
- 3 ターゲット ロールの名前をクリックします。

ロールに関連付けられた権限は、権限カテゴリを展開して表示することができます。

- 4 ロールの名前、説明、または権限を変更するには、[編集] をクリックします。
- 5 ロールを編集して、[保持] をクリックします。

結果

ロールの権限を変更した場合は、このロールに割り当てられているすべての組織のユーザーに新しい権限セットが適用されます。

グローバル テナント ロールの削除

組織で使用しなくなったグローバル テナント ロールは削除することができます。

前提条件

削除するグローバル テナント ロールがすべての組織において、いずれのユーザーにも割り当てられていないこと。

手順

- 1 上部ナビゲーション バーで [管理] を選択します。
- 2 左側のパネルの [テナント アクセス コントロール] で、[グローバル ロール] を選択します。
- 3 ターゲット ロールの横にあるラジオ ボタンを選択して、[削除] をクリックします。
- 4 確認するには、[OK] をクリックします。

プロバイダ ロールの管理

VMware Cloud Director プロバイダ組織でロールを作成して管理することができます。

テナント ロールの管理の詳細については、『VMware Cloud Director Tenant Portal Guide』を参照してください。

プロバイダ ロールの作成

VMware Cloud Director プロバイダの組織内にロールを作成することができます。

VMware Cloud Director の初回インストールとセットアップ後、システムには、プロバイダ組織のローカルな事前定義済みロールと、すべての組織に対するグローバルな事前定義済みロールが含まれています。事前定義済みロールの詳細については、「[事前定義ロールとその権限](#)」を参照してください。

プロバイダ組織には、カスタムのプロバイダ ロールを追加できます。

手順

- 1 上部ナビゲーション バーで [管理] を選択します。
- 2 左側のパネルの [プロバイダ アクセス コントロール] で、[ロール] を選択します。
- 3 [新規] をクリックします。
- 4 新しいロールの名前と、オプションで説明を入力します。
- 5 ロールに関連付ける権限を選択します。

権限は、関連するオブジェクトへのアクセス権を表示および管理するために、カテゴリとサブカテゴリにグループ化されています。

権限はサブカテゴリ別に表示または管理するか、グローバルに表示または管理して、個別に選択することができます。

カテゴリ	説明
アクセス コントロール	組織、権限、ロール、およびユーザーを表示して管理するための権限が含まれています。
管理	一般的な設定やマルチサイトの設定を表示して管理するための権限が含まれています。
コンピュート	組織およびプロバイダの仮想データセンター、vApp、組織仮想データセンター テンプレート、および仮想マシンの監視を表示して管理するための権限が含まれています。
拡張機能	VMware Cloud Director プラグインおよび拡張機能を表示して管理するための権限が含まれています。
インフラストラクチャ	vSphere リソースを表示して管理するための権限が含まれています。
ライブラリ	カタログおよびカタログ項目を表示して管理するための権限が含まれています。
ネットワーク	ネットワーク リソースを表示して管理するための権限が含まれています。

- 6 [保存] をクリックします。

結果

新しく作成したロールは、プロバイダ組織のユーザーに割り当てることができます。

プロバイダ ロールのクローン作成

既存のプロバイダ ロールをテンプレートとして新規ロールの作成に使用できます。

前提条件

VMware Cloud Director に新規ロールを追加する権限があることを確認します。

手順

- 1 上部ナビゲーション バーで [管理] を選択します。
- 2 左側のパネルの [プロバイダ アクセス コントロール] で、[ロール] を選択します。
- 3 クローン作成するロールを選択して、[クローン作成] をクリックします。
- 4 [ロールのクローン作成] ウィンドウで、クローン作成されたロールの名前と説明を入力します。
- 5 (オプション) クローン作成された権限を編集するには、[選択した権限の変更] をオンに切り替え、クローン作成されたロールに対し変更する権限を選択または選択解除します。
- 6 [保存] をクリックします。

プロバイダ ロールの表示または編集

VMware Cloud Director プロバイダ組織のローカル ロールに含まれている権限を表示できます。ロールの名前、説明、および権限を変更できます。

手順

- 1 上部ナビゲーション バーで [管理] を選択します。
- 2 左側のパネルの [プロバイダ アクセス コントロール] で、[ロール] を選択します。
- 3 ターゲット ロールの名前をクリックします。
ロールに関連付けられた権限は、権限カテゴリを展開して表示することができます。
- 4 ロールの名前、説明、または権限を変更するには、[編集] をクリックします。
- 5 ロールを編集して、[保存] をクリックします。

結果

ロールの権限を変更した場合は、このロールに割り当てられているユーザーに新しい権限セットが適用されます。

プロバイダ ロールの削除

VMware Cloud Director プロバイダの組織で使えなくなったロールは削除することができます。

前提条件

削除するロールがいずれのユーザーにも割り当てられていないこと。

手順

- 1 上部ナビゲーション バーで [管理] を選択します。
- 2 左側のパネルの [プロバイダ アクセス コントロール] で、[ロール] を選択します。
- 3 ターゲット ロールの横にあるラジオ ボタンを選択して、[削除] をクリックします。
- 4 確認するには、[OK] をクリックします。

プロバイダ ユーザーおよびグループの管理

ユーザーおよびグループを VMware Cloud Director プロバイダ組織に追加およびインポートできます。

組織ユーザーおよびグループの管理の詳細については、『VMware Cloud Director Tenant Portal Guide』を参照してください。

プロバイダ ユーザーの管理

プロバイダ組織内のユーザーを管理するには、Service Provider Admin Portal を使用します。

組織内のテナント ユーザーの管理の詳細については、『VMware Cloud Director Tenant Portal Guide』を参照してください。

プロバイダ ユーザーの作成

VMware Cloud Director プロバイダの組織内にユーザーを作成することができます。

VMware Cloud Director のインストールおよびセットアップ時に、システム管理者アカウントを作成します。初期セットアップ後、追加の管理者およびユーザーをプロバイダの組織に作成できます。

手順

- 1 上部ナビゲーション バーで [管理] を選択します。
- 2 左側のパネルの [プロバイダ アクセス コントロール] で、[ユーザー] を選択します。
- 3 [新規] をクリックします。
- 4 新規ユーザーのユーザー名とパスワードを入力します。
パスワードには 6 文字以上を含める必要があります。
- 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 [使用可能なロール] ドロップダウン メニューから、ユーザーのロールを選択します。
使用可能なロールのリストには、グローバル ロールと、システム組織のローカル ロールが構成されています。
- 7 (オプション) ユーザーの連絡先情報を入力します。
フル ネーム、メール アドレス、電話番号、インスタント メッセージ ID が入力可能です。
- 8 (オプション) ユーザーの割り当てを設定します。
 - a ユーザーによって所有される仮想マシンの制限を設定するか、または [制限なし] を選択できます。
 - b ユーザーが所有する実行中の仮想マシンの制限を設定するか、または [制限なし] を選択できます。

プロバイダ ユーザーのインポート

以前に設定された LDAP または SAML ID プロバイダから VMware Cloud Director プロバイダ組織にユーザーをインポートできます。

前提条件

「システムの LDAP 接続の構成」または「システムでの SAML ID プロバイダの使用を有効化」。

手順

- 1 上部ナビゲーション バーで [管理] を選択します。
- 2 左側のパネルの [プロバイダ アクセス コントロール] で、[ユーザー] を選択します。
- 3 [ユーザーのインポート] をクリックします。
- 4 [ソース] ドロップダウン メニューで、ID プロバイダのタイプを選択します。

[LDAP] または [SAML] を選択できます。

設定した ID プロバイダが1つのみの場合は、このオプションはハードコードされます。

- 5 ユーザーを指定します。

オプション	説明
LDAP	<ol style="list-style-type: none"> a ユーザーの完全な名前または名前の一部を入力し、[検索] をクリックします。 b 検索結果でインポートするユーザーを選択します。 c [ロールの割り当て] ドロップダウン メニューでインポートされたユーザーのロールを選択します。
SAML	<ol style="list-style-type: none"> a SAML ID プロバイダでサポートされている名前識別子の形式でインポートするユーザーの名前を入力します。 ユーザー名ごとに新しい行を使用します。 b [ロールの割り当て] ドロップダウン メニューでインポートされたユーザーのロールを選択します。

- 6 [保存] をクリックします。

結果

ユーザーのリストでインポートされたユーザーを確認できます。

プロバイダ ユーザーの編集

プロバイダ組織内のユーザーのパスワード、ロール、連絡先情報、および割り当て容量を変更できます。ユーザー名は変更できません。

手順

- 1 上部ナビゲーション バーで [管理] を選択します。
- 2 左側のパネルの [プロバイダ アクセス コントロール] で、[ユーザー] を選択します。
- 3 ターゲット ユーザー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 ユーザーの詳細を編集して、[保存] をクリックします。

プロバイダ ユーザーの有効化または無効化

ユーザーを無効にすると、そのユーザーは VMware Cloud Director にログインできなくなります。

手順

- 1 上部ナビゲーション バーで [管理] を選択します。
- 2 左側のパネルの [プロバイダ アクセス コントロール] で、[ユーザー] を選択します。
- 3 ターゲット 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、[無効化] または [有効化] をクリックします。
- 4 ユーザーを無効にする場合は、[OK] をクリックして確認します。

プロバイダ ユーザーの削除

VMware Cloud Director プロバイダの組織からユーザーを削除するには、そのユーザー アカウントを削除します。

LDAP グループが削除されたために、システムに対するアクセス権限を失った取り残されたユーザーを削除するには、VMware Cloud Director API を使用します。

前提条件

削除するユーザーを無効にします。 [プロバイダ ユーザーの有効化または無効化](#) を参照してください。

手順

- 1 上部ナビゲーション バーで [管理] を選択します。
- 2 左側のパネルの [プロバイダ アクセス コントロール] で、[ユーザー] を選択します。
- 3 対象のユーザー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。
- 4 確認するには、[OK] をクリックします。

プロバイダ ユーザーのロック解除

パスワード ポリシー システム設定でアカウントのロックアウトを有効にした場合に、ユーザーが無効なログインを特定の回数だけ試行すると、アカウントがロックされる可能性があります。ロックアウトにアカウントのロックアウト間隔が設定されている場合でも、ロックが期限切れになるのを待たずに、ユーザー アカウントのロックを解除できます。

アカウント ロックアウト ポリシーの設定の詳細については、 [パスワード ポリシーの設定](#) を参照してください。

手順

- 1 上部ナビゲーション バーで [管理] を選択します。
- 2 左側のパネルの [プロバイダ アクセス コントロール] で、[ユーザー] を選択します。
- 3 ターゲット 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、[ロック解除] をクリックします。

プロバイダ グループの管理

Service Provider Admin Portal を使用して、プロバイダ組織からグループをインポート、編集、および削除できます。

組織内のグループの管理の詳細については、『VMware Cloud Director Tenant Portal Guide』を参照してください。

プロバイダ グループのインポート

以前に設定された LDAP または SAML ID プロバイダから VMware Cloud Director プロバイダ組織にグループをインポートできます。

前提条件

「システムの LDAP 接続の構成」または「システムでの SAML ID プロバイダの使用を有効化」。

手順

- 1 上部ナビゲーション バーで [管理] を選択します。
- 2 左側のパネルの [プロバイダ アクセス コントロール] で、[グループ] を選択します。
- 3 [グループのインポート] をクリックします。
- 4 [ソース] ドロップダウン メニューで、ID プロバイダのタイプを選択します。

[LDAP] または [SAML] を選択できます。

設定した ID プロバイダが1つのみの場合は、このオプションはハードコードされます。

- 5 ユーザーを指定します。

オプション	説明
LDAP	<ol style="list-style-type: none"> a グループの完全な名前または名前の一部を入力し、[検索] をクリックします。 b 検索結果でインポートするグループを選択します。 c [ロールの割り当て] ドロップダウン メニューから、インポートされたグループ内のユーザーにロールを選択します。
SAML	<ol style="list-style-type: none"> a SAML ID プロバイダでサポートされている名前識別子の形式で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。 b [ロールの割り当て] ドロップダウン メニューから、インポートされたグループ内のユーザーにロールを選択します。

- 6 [保存] をクリックします。

プロバイダ グループの編集

VMware Cloud Director プロバイダ組織に以前にインポートしたグループの説明を編集したり、グループのメンバーのロールを変更することができます。

手順

- 1 上部ナビゲーション バーで [管理] を選択します。
- 2 左側のパネルの [プロバイダ アクセス コントロール] で、[グループ] を選択します。
- 3 ターゲット 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 グループの詳細を編集して、[保存] をクリックします。

プロバイダ グループの削除

VMware Cloud Director プロバイダの組織からグループを削除することができます。

手順

- 1 上部ナビゲーション バーで [管理] を選択します。
- 2 左側のパネルの [プロバイダ アクセス コントロール] で、[グループ] を選択します。
- 3 対象のグループ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。
- 4 確認するには、[OK] をクリックします。

システム設定の管理

11

VMware Cloud Director システム管理者は、LDAP、E メール通知、ライセンス、および全般システムの環境設定に関連するシステム全体の設定を管理できます。

この章には、次のトピックが含まれています。

- [全般システム設定の変更](#)
- [全般システム設定](#)
- [サーバ グループのセルに対する FIPS モードの有効化](#)
- [システム メールの設定](#)
- [VMware Cloud Director ライセンスの変更](#)
- [カタログ同期の設定](#)
- [アドバイザリ ダッシュボードの作成](#)
- [ブロック タスクおよび通知の構成と監視](#)
- [公開アドレスの構成](#)
- [ID プロバイダの管理](#)
- [証明書の管理](#)
- [プラグインの管理](#)
- [VMware Cloud Director ポータルのカスタマイズ](#)
- [パスワード ポリシーの設定](#)
- [vSphere サービスの構成](#)

全般システム設定の変更

VMware Cloud Director には、アクティビティ ログ、ネットワーク、セッション タイムアウト、証明書、組織の制限、操作の制限などに関連する一般的なシステム設定が含まれています。デフォルトの設定は多くの環境に適していますが、ニーズに合わせて設定を変更できます。

変更できるプロパティのリストについては、[全般システム設定](#)を参照してください。

注： VMware Cloud Director アプライアンスの日付、時刻、またはタイム ゾーンを変更する方法については、<https://kb.vmware.com/kb/59674> を参照してください。

手順

- 1 上部ナビゲーション バーで [管理] を選択します。
- 2 左側のパネルの [設定] で、[全般] をクリックします。
- 3 変更するセクションの [編集] をクリックし、プロパティを編集して、[保存] をクリックします。

全般システム設定

VMware Cloud Director には全般システム設定が含まれており、ニーズに合わせて変更できます。

表 11-1. 全般システム設定

名前	カテゴリ	説明
Activity log history to keep	アクティビティ ログ	ログ履歴を削除せずに保持する日数。 0 と入力すると、ログが一切削除されなくなります。
Activity log history shown	アクティビティ ログ	ログ履歴を表示する日数。 すべてのアクティビティを表示するには、0 と入力します。
Display debug information	アクティビティ ログ	VMware Cloud Director タスク ログのデバッグ情報を表示するには、この設定を有効にします。
IP address release timeout	ネットワーク	解放された IP アドレスを再び割り当てられるようにするまで保持する時間を秒単位で指定します。デフォルト設定は 2 時間 (7200 秒) で、古いエントリがクライアント ARP テーブルから失効できるようにします。
Allow Overlapping External Networks	ネットワーク	同じネットワーク セグメントで実行されている外部ネットワークを追加する場合に、このチェック ボックスをオンにします。 VLAN を使用せずに外部ネットワークを隔離している場合のみ、この設定を有効にします。
Allow FIPS mode	ネットワーク	Edge Gateway 上で FIPS モードの有効化を許可します。NSX 6.3 以降が必要です。VMware NSX for vSphere のドキュメントで、 FIPS モード を参照してください。
Default syslog server settings for networks	ネットワーク	ネットワークが使用する IP アドレスを、最大 2 台の Syslog サーバに対して入力します。この設定は、クラウド セルにより使用される Syslog サーバーには適用されません。
Provider Locale	ローカライズ	ログ エントリ、電子メール アラートなどのプロバイダ アクティビティのロケールを選択します。
Idle session timeout	タイムアウト	VMware Cloud Director アプリケーションが、ユーザーの操作なしでアクティブな状態を維持する時間。
Maximum session timeout	タイムアウト	VMware Cloud Director アプリケーションが、アクティブな状態を維持する最大時間。
Host refresh frequency	タイムアウト	ESXi ホストがアクセス可能かどうかを VMware Cloud Director が確認する頻度。

表 11-1. 全般システム設定（続き）

名前	カテゴリ	説明
Host hung timeout	タイムアウト	ホストをハングアップしているとマークされるまでの待機時間を選択します。
Transfer session timeout	タイムアウト	一時停止またはキャンセルされたアップロード タスク (メディアのアップロードや vApp テンプレートのアップロードなど) が失敗するまで待機する時間を指定します。このタイムアウトは、進行中のアップロード タスクには適用されません。
Enable upload quarantine with a timeout of __ seconds	タイムアウト	アップロードしたファイルを隔離するには、このチェック ボックスをオンにし、時間を表すタイムアウト値を入力します。
Verify vCenter and vSphere SSO certificates	証明書	VMware Cloud Director は、常に証明書を検証します。有効にすると、vCenter Server 証明書内のホスト名が検証されます。
Verify NSX Manager certificates	証明書	VMware Cloud Director は、常に証明書を検証します。有効にすると、VMware Cloud Director によって NSX Manager 証明書内のホスト名が検証されます。
Edit Organization Limits	組織 VDC の制限	組織あたりの仮想データセンターの最大数を入力するか、[制限なし]を選択します。
Number of resource intensive operations running per user	操作の制限	ユーザーあたりの、リソースを大量に使用する操作の同時実行最大数を入力するか、[制限なし]を選択します。
Number of resource intensive operations to be queued per user (in addition to running)	操作の制限	ユーザーあたりの、リソースを大量に使用する操作のキュー登録最大数を入力するか、[制限なし]を選択します。
Number of resource intensive operations running per organization	操作の制限	組織あたりの、リソースを大量に使用する操作の同時実行最大数を入力するか、[制限なし]を選択します。
Number of resource intensive operations to be queued per organization	操作の制限	組織あたりの、リソースを大量に使用する操作のをキュー登録最大数を入力するか、[制限なし]を選択します。
Provide default vApp names	その他	新しい vApp のデフォルト名を提供するように VMware Cloud Director を設定するには、このチェック ボックスをオンにします。
Make Allocation pool Org VDCs elastic	その他	柔軟性のある割り当てプールを有効にして、割り当てプールのすべての組織仮想データセンターに柔軟性を持たせるには、このチェック ボックスを選択します。このオプションを選択解除する前に、組織の各仮想データセンターのすべての仮想マシンが単一のクラスタに移行されていることを確認します。
VM discovery enabled	その他	デフォルトでは、それぞれの組織仮想データセンターは、仮想データセンターをバックアップするいずれかのリソース プールで作成された vCenter Server 仮想マシンを自動的に検出します。オフにすると、システム内のすべての VDC について、この設定が無効になります。

サーバ グループのセルに対する FIPS モードの有効化

Linux で、FIPS 140-2 認定の暗号化モジュールを使用して FIPS 対応モードで実行するように VMware Cloud Director 10.2.2 以降を構成することができます。

FIPS (Federal Information Processing Standard) 140-2 は、暗号化モジュールのセキュリティ要件を指定する、米国およびカナダの政府規格です。NIST Cryptographic Module Validation Program (CMVP) は、FIPS 140-2 規格に準拠した暗号化モジュールを検証します。

VMware Cloud Director FIPS サポートは、規制の厳しいさまざまな環境でのコンプライアンスとセキュリティのアクティビティを容易にすることを目的としています。VMware 製品における FIPS 140-2 のサポートの詳細については、<https://www.vmware.com/security/certifications/fips.html> を参照してください。

VMware Cloud Director では、FIPS 認定の暗号化はデフォルトで無効になっています。FIPS モードを有効にすることで、FIPS 140-2 認定の暗号化モジュールを使用し、FIPS 準拠モードで実行するように VMware Cloud Director が構成されます。

注： FIPS モードを有効にすると、ホスト名の逆引きも有効になります。

重要： FIPS モードを有効にした場合、vRealize Orchestrator との統合は動作しません。

VMware Cloud Director 10.2.2 で FIPS モードを有効にした場合は、SAML アサーションを暗号化できません。FIPS モードでない場合は、アサーション暗号化に制限はありません。

VMware Cloud Director は、次の FIPS 140-2 認定の暗号化モジュールを使用します。

- VMware の BC-FJA (Bouncy Castle FIPS Java API)、バージョン 1.0.2.1： [Certificate #3673](#)
- VMware の OpenSSL FIPS オブジェクト モジュール、バージョン 2.0.20-vmw： [Certificate #3857](#)。

VMware Cloud Director はセル管理ツール (CMT) に付属のバンドルに含まれています。ただし、セル管理ツールは FIPS に準拠していません。

VMware Cloud Director アプライアンスで FIPS モードを有効にする方法については、[VMware Cloud Director アプライアンスでの FIPS モードの有効化または無効化](#)を参照してください。

前提条件

- 証明書に OpenSSL を使用して KeyCertSign ビットがアサートされていることを確認します。FIPS モードが機能できるのは、VMware Cloud Director SSL 証明書に KeyCertSign がアサートされている場合に限られます。

```
openssl crl2pkcs7 -nocrl -certfile certificates.pem | openssl pkcs7 -print_certs -text -noout
```

証明書に拡張機能が含まれていない場合は、SSL 証明書キーストアを作成するときに KeyCertSign ビットを指定します。

- ユーティリティの rng-tools セットをインストールして、有効にします。<https://wiki.archlinux.org/index.php/Rng-tools> を参照してください。
- メトリックの収集が有効になっている場合は、Cassandra 証明書が X.509 v3 証明書の標準に従っていて、必要なすべての拡張機能が含まれていることを確認します。Cassandra は、VMware Cloud Director が使用するのと同じ暗号化スイートを使用して構成する必要があります。許可された SSL 暗号の詳細については、[許可された SSL 暗号のリストの管理](#)を参照してください。

- VMware Cloud Director を vCenter Lookup Service から登録解除します。[vSphere サービスの構成](#)を参照してください。

手順

- 1 上部ナビゲーション バーで [管理] を選択します。
- 2 左側のパネルの [設定] で、[SSL] を選択します。
- 3 [有効化] をクリックします。
- 4 使用環境が FIPS モードを有効にするためのすべての前提条件を満たしていることを確認します。
FIPS モード構成を開始する前に使用環境がすべての前提条件を満たしていない場合は、VMware Cloud Director にアクセスできなくなることがあります。
- 5 プロセスの開始を確定するには、[有効化] をクリックします。
構成が完了すると、VMware Cloud Director にセルを再起動するよう求めるメッセージが表示されます。
- 6 VMware Cloud Director にクラウド セルを再起動するよう求めるメッセージが表示されたら、VMware Cloud Director サーバ グループ内のすべてのセルを再起動します。

次のステップ

- [無効化] をクリックして FIPS モードを無効にします。構成の準備が完了したことが VMware Cloud Director に示されたら、セルを再起動します。
- `fips-mode CMT` コマンドを使用して、アクティブな VMware Cloud Director セルの FIPS ステータスを表示します。VMware Cloud Director インストール、構成、およびアップグレード ガイドの「[すべてのアクティブ セルの FIPS ステータスの表示](#)」を参照してください。

システム メールの設定

SMTP サーバの設定や VMware Cloud Director の通知設定など、システム メールの設定を編集できます。

VMware Cloud Director では、システム ユーザーにユーザー通知およびシステム アラート メールを送信するために SMTP サーバが必要です。

VMware Cloud Director では、重要な情報を報告するときにシステム アラート メールを送信します。たとえば、VMware Cloud Director は、データストアの容量が不足しそうな場合にアラートを送信します。すべてのシステム管理者または指定したメール アドレス リスト宛てにメール アラートを送信するように、VMware Cloud Director を構成できます。

手順

- 1 上部ナビゲーション バーで [管理] を選択します。
- 2 左側のパネルの [設定] で、[E メール] を選択し、[編集] をクリックします。
- 3 SMTP メール サーバの DNS ホスト名または IP アドレスを入力します。
- 4 SMTP サーバのポート番号を入力します。

- 5 (オプション) SMTP サーバがユーザー名を要求する場合は、[認証が必要] オプションをオンにして、SMTP アカウントのユーザー名およびパスワードを入力します。
- 6 [通知設定] タブを選択します。
- 7 VMware Cloud Director の E メールで送信者として表示するメール アドレスを入力します。
VMware Cloud Director では、送信者のメール アドレスを使用して、ランタイム リースおよびストレージ リースの有効期限のアラートを送信します。
- 8 (オプション) サブジェクトのプリフィックスのテキストを入力します。
- 9 通知の受信者を選択します。
デフォルトでは、組織管理者のみが SMTP 通知を受信します。
- 10 [保存] をクリックします。
- 11 (オプション) SMTP 設定をテストします。
 - a [テスト] をクリックします。
 - b [認証が必要] オプションを有効にしている場合は、SMTP サーバのパスワードを入力します。
 - c 送信先のメール アドレスを入力し、[テスト] をクリックします。

VMware Cloud Director ライセンスの変更

VMware Cloud Director を実行するには、シリアル番号として指定される有効なライセンスが必要です。最初の VMware Cloud Director 構成時に入力したライセンス情報は変更できます。

VMware Cloud Director 製品シリアル番号は、vCenter Server のライセンス キーとは異なります。VMware Cloud Director のシリアル番号は、VMware ライセンス ポータルから取得できます。

手順

- 1 上部ナビゲーション バーで [管理] を選択します。
- 2 左側のパネルで、[ライセンス] を選択し、[編集] をクリックします。
- 3 新しいシリアル番号を入力して [保存] をクリックします。

カタログ同期の設定

カタログ サブスクリプションの更新率など、すべての組織およびカタログのカタログ同期の設定を編集できます。

手順

- 1 上部ナビゲーション バーで [管理] を選択します。
- 2 左側のパネルの [設定] で、[カタログ] を選択します。
- 3 [[編集]] をクリックします。
- 4 カタログ同期を有効にします。
- 5 同期の開始時刻と終了時刻を設定します。

6 同期間隔を設定します。

同期間隔は、カタログ サブスクリプションの更新率です。

7 [保存] をクリックします。

次のステップ

カタログ同期のスロットリングの設定については、VMware Cloud Director インストール、構成、およびアップグレード ガイドを参照してください。

アドバイザリ ダッシュボードの作成

VMware Cloud Director Service Provider Admin Portal および Tenant Portal のユーザー インターフェイス画面の上部に表示される通知を作成できます。メッセージは、システム管理者、組織内のユーザー、またはすべての組織のユーザーに表示できます。

作成したアドバイザリを編集することはできません。

手順

1 上部ナビゲーション バーで [管理] を選択します。

2 左側のパネルの [設定] で [アドバイザリ] を選択し、[新規] をクリックします。

3 説明ボックスに、通知のテキストを追加します。

基本的な Markdown を使用して、通知へのリンクを追加できます。

4 メッセージの優先度を選択します。

メッセージは優先度ごとに異なる色で表示されます。通知は、優先度の順番で表示されます。必須のアドバイザリを破棄または停止することはできません。

5 ユーザー インターフェイスに通知を表示する期間を選択します。

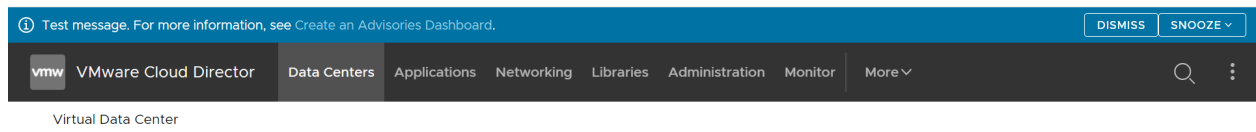
[アドバイザリ] タブにすべてのアドバイザリが表示されますが、選択したユーザー グループにアドバイザリが表示されるのは、選択した期間のみです。

6 通知をシステム管理者にのみ表示するのか、それとも特定の組織または複数の組織内のすべてのユーザーに表示するのかを選択します。

7 [OK] をクリックします。

結果

通知は、選択したポータルの上部ナビゲーション バーの上に表示されます。



次のステップ

通知の横にあるラジオ ボタンを選択し、[削除]をクリックして、通知を削除します。期限が切れた後も、アドバイザーは [アドバイザー] タブに表示されます。リストからアドバイザーを削除するには、削除する必要があります。

ブロック タスクおよび通知の構成と監視

ブロック タスクおよび通知を使用して、特定のイベントによってトリガされた AMQP メッセージを送信するように VMware Cloud Director を構成できます。

これらのメッセージの一部は、単にイベントが発生したことを通知します。他のメッセージは、要求されたアクションが、指定の AMQP エンドポイントに関連付けられているクライアント アプリケーションによってブロックされ、アクションが保留中であることを示す情報をそのエンドポイントに発行します。これらのメッセージはブロック タスクと呼ばれます。

システム管理者は、AMQP クライアントによるプログラム上のアクションの対象となるブロック タスクのシステム全体のセットを構成できます。

AMQP ブローカーの構成

VMware Cloud Director が特定のイベントによってトリガされた AMQP メッセージを送信するようにするには、AMQP ブローカーを構成する必要があります。AMQP メッセージを使用して、基盤となるユーザー要求の処理を自動化できます。

手順

- 1 上部ナビゲーション バーで [管理] を選択します。
- 2 [設定] で、[拡張性] を選択します。
[AMQP ブローカー] タブが開きます。
- 3 [AMQP ブローカー] セクションの [編集] ボタンをクリックします。
- 4 AMQP ホストの DNS ホスト名または IP アドレスを入力します。
RabbitMQ サーバ ホストの完全修飾ドメイン名 (例: *amqp.example.com*)。
- 5 AMQP ポートを入力します。
ブローカーがメッセージをリスンするデフォルトのポートは 5672 です。
- 6 Exchange を入力します。
- 7 vHost を入力します。
デフォルトは、/ です。
- 8 プリフィックスを入力します。

- 9 (オプション) SSL を使用するには、[SSL を使用] トグルを有効にして、証明書オプションを 1 つ選択します。

デフォルトでは、VMware Cloud Director AMQP サービスは暗号化されていないメッセージを送信します。SSL を使用してこれらのメッセージを暗号化するように AMQP サービスを構成できます。VMware Cloud Director セルで Java ランタイム環境のデフォルトの JCEKS トラスト ストアを使用して、ブローカー証明書 (通常は \$VCLLOUD_HOME/jre/lib/security/cacerts) を検証するようにサービスを構成することもできます。

オプション	説明
[すべての証明書を承認]	証明書オーナー フィールドからの CN レコードは、AMQP ブローカー ホスト名に一致する必要があります。ブローカー ホスト名に一致しない証明書を使用するには、[すべての証明書を承認] トグルを有効にします。
[SSL 証明書]	SSL 証明書をアップロードします。
[SSL キー ストア (JCEKS)]	SSL キー ストアをアップロードして、キー ストアのパスワードを入力します。

- 10 ユーザー名およびパスワードを入力して AMQP ホストに接続します。

- 11 [保存] をクリックします。

- 12 (オプション) 設定をテストするには、[AMQP ブローカー] セクションの下の [テスト] ボタンをクリックして、パスワードを入力します。

- 13 (オプション) 監査イベントを AMQP ブローカーに公開するには、[非ブロック AMQP 通知] セクションの下の [編集] ボタンをクリックして、[通知の有効化] トグルを有効にします。

ブロック タスク設定の構成

ブロック タスクとして特定の操作を構成できます。これらの操作は、システム管理者によって実行されるか、タイマーに事前構成された時間が経過するまでサスペンド状態になります。タイムアウト設定およびデフォルトのアクションをブロック タスクに対して指定できます。これらの設定は、インストール環境内のすべての組織に適用されます。

手順

- 1 上部ナビゲーション バーで [管理] を選択します。
- 2 [設定] で、[拡張性] を選択します。
- 3 [ブロック タスク] タブを選択します。
- 4 デフォルトの拡張機能タイムアウトおよびデフォルトのタイムアウト アクションを編集するには、[全般] セクションの下の [編集] ボタンをクリックします。
 - a [デフォルトのブロック タスクのタイムアウト] を編集します。
 - b [デフォルトのタイムアウトのアクション] を編集します。
 [デフォルトのタイムアウトのアクション] は、[デフォルトのブロック タスクのタイムアウト] の時間が経過した後のアクションです。
 - c [保存] をクリックします。

- 5 ブロック タスクと見なされる操作のリストを編集するには、[操作] セクションの下の [編集] ボタンをクリックします。
 - a ブロック タスクのリストから操作を選択または選択解除します。
 - b [保存] をクリックします。

ブロックされているタスクの監視

現在ブロックされているタスクを監視したり、タイマーに事前構成された時間が経過する前に、手動でタスクをキャンセル、失敗、または再開したりできます。

前提条件

ブロック タスク設定の構成

手順

- 1 上部ナビゲーション バーの [監視] で [ブロック タスク] を選択します。

タブには、現在ブロックされているタスクのリストが表示されます。
- 2 手動で編集するタスクを選択します。
- 3 タスクのキャンセル、失敗、または再開を決定し、対応するボタンをクリックします。
- 4 メッセージを入力し、[保存] をクリックします。

タスクの詳細にメッセージが表示されます。

公開アドレスの構成

ロード バランサまたはプロキシの要件を満たすには、VMware Cloud Director Web ポータル、VMware Cloud Director API、およびコンソール プロキシのデフォルトのエンドポイント Web アドレスを変更します。

公開アドレスとは、VMware Cloud Director のクライアントに公開される Web アドレスです。これらのアドレスのデフォルト値はインストール時に指定されます。必要な場合は、アドレスを更新できます。

VMware Cloud Director が単一のセルで構成されている場合、インストーラは、通常 API および Web クライアントに対して十分なアクセスを提供するパブリック エンドポイントを作成します。複数のセルを含むインストールおよびデプロイでは、通常、セルとクライアントの間にロード バランサが配置されます。クライアントは、ロード バランサのアドレスでシステムにアクセスします。ロード バランサは、使用可能なセル全体にクライアント要求を分散させます。そのほか、プロキシが配置されたネットワーク構成や、セルが DMZ に配置されるネットワーク構成の場合も、カスタマイズされたエンドポイントが必要になります。エンドポイント URL の詳細は、ネットワーク構成ごとに異なります。

VMware Cloud Director Tenant Portal および VMware Cloud Director Web コンソールのエンドポイントでは、（可能であれば署名付きの）SSL 証明書が必要です。VMware Cloud Director をインストールまたはデプロイするときにこれらの証明書へのパスを指定する必要があります。これらのエンドポイントのいずれかをインストールまたはデプロイ後にカスタマイズする場合は、hostname や subject alternative name などのエンドポイントの詳細に一致する新しい証明書をインストールする必要があります。

VMware Cloud Director アプライアンスはコンソール プロキシ サービスに単一の IP アドレスとカスタム ポート 8443 を使用するため、VMware Cloud Director 公開コンソールのプロキシ アドレスを設定する必要があります。手順 6 を参照してください。

前提条件

システム管理者としてログインしていることを確認します。システム管理者のみが公開エンドポイントをカスタマイズできます。

手順

- 1 上部ナビゲーション バーで [管理] を選択します。
- 2 左側のパネルの [設定] で、[公開アドレス] をクリックします。
- 3 公開エンドポイントをカスタマイズするには、[編集] をクリックします。
- 4 VMware Cloud Director URL をカスタマイズするには、[Web ポータル] エンドポイントを編集します。

- a HTTP（非セキュア）接続用のカスタムの VMware Cloud Director パブリック URL を入力します。
- b HTTPS（セキュア）接続用のカスタムの VMware Cloud Director パブリック URL を入力し、[アップロード] をクリックして、そのエンドポイントの信頼チェーンを確立する証明書をアップロードします。

証明書チェーンはサービス エンドポイントで使用する証明書と一致する必要があります。この証明書は、エイリアス `consoleproxy` を使用して VMware Cloud Director セルの各キーストアにアップロードされた証明書です。ロード バランサでコンソール プロキシ接続の SSL 終端はサポートされていません。証明書チェーンには、プライベート キーを含まない PEM 形式のエンドポイント証明書、中間証明書、およびルート証明書が含まれている必要があります。

- 5（オプション）Cloud Director REST API と OpenAPI URL をカスタマイズするには、[Web ポータル設定の使用] トグルを無効にします。

- a カスタムの HTTP ベース URL を入力します。

たとえば、HTTP ベース URL を `http://vcloud.example.com` に設定した場合は、`http://vcloud.example.com/api` から VMware Cloud Director API に、`http://vcloud.example.com/cloudapi` から VMware Cloud Director OpenAPI にアクセスできます。

- b カスタムの HTTPS REST API ベース URL を入力し、[アップロード] をクリックして、そのエンドポイントの信頼チェーンを確立する証明書をアップロードします。

たとえば、HTTPS REST API ベース URL を `https://vcloud.example.com` に設定した場合は、`https://vcloud.example.com/api` から VMware Cloud Director API に、`https://vcloud.example.com/cloudapi` から VMware Cloud Director OpenAPI にアクセスできます。

証明書チェーンはサービス エンドポイントで使用する証明書と一致する必要があります。この証明書は、エイリアス `http` を使用して VMware Cloud Director セルの各キーストアにアップロードされた証明書、またはロード バランサの VIP 証明書（SSL 終端が使用されている場合）のいずれかになります。証明書チェーンには、プライベート キーを含まない PEM 形式のエンドポイント証明書、中間証明書、およびルート証明書が含まれている必要があります。

6 カスタムの VMware Cloud Director 公開コンソール プロキシ アドレスを入力します。

- VMware Cloud Director アプライアンスの公開コンソール プロキシ アドレスをカスタマイズします。

このアドレスは、コンソール プロキシ サービスにカスタム ポート 8443 を使用して、FQDN または IP アドレスで指定された VMware Cloud Director アプライアンス `eth0` NIC の完全修飾ドメイン名 (FQDN) です。

- Linux 上の VMware Cloud Director の公開コンソール プロキシ アドレスをカスタマイズします。

このアドレスは、ポート番号が指定された、VMware Cloud Director サーバまたはロード バランサの完全修飾ドメイン名 (FQDN) です。デフォルト ポートは 443 です。

たとえば、VMware Cloud Director アプライアンスのインスタンスの FQDN が `vcloud.example.com` の場合は、「**`vcloud.example.com:8443`**」と入力します。

VMware Cloud Director は、仮想マシン上でリモート コンソール ウィンドウを開くときにコンソール プロキシ アドレスを使用します。

7 [保存] をクリックします。

ID プロバイダの管理

クラウドを外部 ID プロバイダと連携させて、ユーザーおよびグループを組織にインポートすることができます。LDAP サーバ接続はシステム レベルまたは組織レベルで設定できます。SAML 連携は組織レベルで設定できます。

LDAP 接続の管理

システム管理者は、ユーザーおよびグループの送信元として LDAP サーバを使用するよう、VMware Cloud Director システムの組織およびシステム内の別の任意の組織を設定できます。組織はシステムの LDAP 接続またはプライベート LDAP 接続のいずれかを使用できます。

バージョン 10.1 以降の VMware Cloud Director は、証明書を管理するために、一元化されたテナント対応のストレージ エリアに移動しています。そうすることで、VMware Cloud Director はすべての証明書を 1 か所に統合し、システム内のさまざまなコンポーネントで使用されているすべての証明書をシステム管理者および組織管理者が表示、監査、および管理できるようにします。VMware Cloud Director API を使用して、新しいテナント対応のストレージ エリアの証明書を追加、更新、または削除できます。VMware Cloud Director API スキーマ リファレンスを参照してください。

新しい LDAP サーバ エンドポイントを追加または編集すると、VMware Cloud Director ユーザー インターフェイスによって、エンドポイントが提示する証明書が調査されます。VMware Cloud Director は、信頼される証明書を中央の証明書ストレージ エリアに追加します。

システムの LDAP 接続の構成

VMware Cloud Director および組織に、ユーザーおよびグループへの共有アクセスを提供するには、LDAP 接続をシステム レベルで構成できます。

手順

- 1 上部ナビゲーション バーで [管理] を選択します。

- 2 左側のパネルの [ID プロバイダ] で、[LDAP] をクリックします。

現在の LDAP の設定が表示されます。

次のステップ

[LDAP 接続の構成、テスト、および同期](#)。

組織 LDAP 接続の設定

組織で、ユーザーおよびグループの共有ソースとしてシステムの LDAP 接続が使用されるように設定できます。組織で、ユーザーおよびグループのプライベート ソースとして個別の LDAP 接続が使用されるように設定できます。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [組織] を選択します。
- 3 ターゲット組織の名前をクリックします。
組織の VMware Cloud Director テナント ポータルにリダイレクトされます。
- 4 上部ナビゲーション バーで [管理] を選択します。
- 5 左側のパネルの [ID プロバイダ] で、[LDAP] をクリックします。
現在の LDAP の設定が表示されます。
- 6 [LDAP オプション] タブで、[編集] をクリックします。
- 7 この組織のユーザーおよびグループの LDAP ソースを設定し、[保存] をクリックします。

オプション	説明
[LDAP を使用しない]	組織は、組織のユーザーおよびグループのソースとして LDAP サーバを使用しません。
[VCD システム LDAP サービス]	組織は、設定済みの VMware Cloud Director システムの LDAP 接続を使用します。 システムの LDAP 接続の構成 を参照してください。
[カスタム LDAP サービス]	組織は、組織のユーザーおよびグループのソースとしてプライベート LDAP サーバを使用します。 [カスタム LDAP] タブをクリックし、 [LDAP 接続の構成、テスト、および同期] を実行します。

LDAP 接続の構成、テスト、および同期

LDAP 接続を構成するには、LDAP サーバの詳細を設定します。接続をテストすることで、設定が適切に入力されていることと、ユーザーおよびグループ属性が適切にマッピングされていることを確認できます。LDAP 接続が正常に完了すると、ユーザーおよびグループの情報を LDAP サーバといつでも同期できます。

前提条件

SSL (LDAPS) 経由で LDAP サーバに接続する場合は、LDAP サーバの証明書が Java 8 Update 181 で導入されたエンドポイント ID に準拠していることを確認します。証明書のコモン ネーム (CN) または Subject Alternative Name (SAN) は、LDAP サーバの FQDN と一致する必要があります。詳細については、<https://www.java.com> の「Java 8 Release Changes」を参照してください。

手順

- 1 [接続] タブで、LDAP 接続に必要な情報を入力します。

必要な情報	説明
[サーバ]	LDAP サーバのホスト名または IP アドレス。
[ポート]	LDAP サーバが待機するポート番号。 LDAP のデフォルト ポート番号は 389 です。LDAPS のデフォルト ポート番号は 636 です。
[ベースの識別名]	ベース識別名 (DN) は、VMware Cloud Director が接続する LDAP ディレクトリ内の場所です。 root レベルで接続するには、 DC=example,DC=com のようにドメイン コンポーネントのみを入力します。 ドメイン ツリー構造内のノードに接続するには、 OU=ServiceDirector,DC=example,DC=com のようにノードの識別名を入力します。 ノードに接続すると、VMware Cloud Director が使用できるディレクトリの範囲が制限されます。
[コネクタ タイプ]	LDAP サーバのタイプ。[Active Directory] または [OpenLDAP] を使用できます。
[SSL を使用]	サーバが LDAPS の場合は、このチェック ボックスを選択します。
[すべての証明書を承認]	サーバが LDAPS の場合は、このチェック ボックスを選択するか、または LDAP の SSL 証明書をアップロードします。
[カスタム トラストストア]	サーバが LDAPS の場合は、[アップロード] ボタンをクリックして LDAP の SSL 証明書をインポートするか、[すべての証明書を承認] を選択します。
[認証方法]	シンプルな認証では、ユーザーの DN とパスワードを LDAP サーバに送信します。 LDAP を使用している場合、LDAP パスワードはネットワーク上で平文として送信されます。 Kerberos を使用する場合は、vCloud API を使用して LDAP 接続を構成する必要があります。
[ユーザー名]	ドメイン管理者権限を持つサービス アカウントの完全な LDAP 識別名 (DN) を入力します。VMware Cloud Director は、このアカウントを使用して LDAP ディレクトリにクエリを実行し、ユーザー情報を取得します。 LDAP サーバで匿名読み取り対応が有効になっている場合は、これらのテキスト ボックスを空白にしておくことができます。
[パスワード]	LDAP サーバに接続するサービス アカウントのパスワード。 LDAP サーバで匿名読み取り対応が有効になっている場合は、これらのテキスト ボックスを空白にしておくことができます。

- 2 [ユーザー属性] タブをクリックして、ユーザー属性のデフォルト値を確認します。LDAP ディレクトリで別のスキーマが使用されている場合には、値を変更します。
- 3 [グループ属性] タブをクリックして、グループ属性のデフォルト値を確認します。LDAP ディレクトリで別のスキーマが使用されている場合には、値を変更します。
- 4 [保存] をクリックします。
- 5 [SSL を使用] チェック ボックスをオンにした場合に、LDAPS サーバの証明書がまだ信頼されていないときは、[信頼証明書] ウィンドウで、サーバ エンドポイントによって提示された証明書を信頼するかどうかを確認します。
- 6 LDAP 接続の設定と LDAP 属性のマッピングをテストするには、以下の手順を実行します。
 - a [テスト] をクリックします。
 - b 設定した LDAP サーバ ユーザーのパスワードを入力し、[テスト] をクリックします。

正常に接続されている場合は、緑色のチェック マークが表示されます。

取得したユーザーおよびグループ属性の値がテーブルに表示されます。LDAP 属性に正常にマッピングされた値には、緑色のチェック マークが付けられます。マッピングされた LDAP 属性以外の値は空白になり、赤色の感嘆符が付けられます。
 - c 終了するには [キャンセル] をクリックします。
- 7 VMware Cloud Director を設定した LDAP サーバと同期するには、[同期] をクリックします。

VMware Cloud Director は、システムの全般設定で指定された同期間隔に基づき、ユーザーおよびグループ情報を LDAP サーバと定期的に同期します。

同期が完了するまで数分間待機します。

結果

ユーザーとグループは、新たに設定した LDAP サーバからインポートできます。

システムでの SAML ID プロバイダの使用を有効化

SAML ID プロバイダからユーザーおよびグループをシステム組織にインポートする場合は、その SAML の ID プロバイダで、システム組織を構成する必要があります。インポートされたユーザーは、SAML ID プロバイダで確立した認証情報を使用してシステム組織にログインできます。

VMware Cloud Director を SAML の ID プロバイダで構成するには、SAML サービス プロバイダと ID プロバイダのメタデータを交換して相互信頼を確立します。

インポートされたユーザーがログインすると、システムは SAML トークンから以下の属性を抽出し（使用可能な場合）、それらをユーザーに関する情報の対応する要素の解釈に使用します。

- email address = "EmailAddress"
- user name = "UserName"
- full name = "FullName"
- user's groups = "Groups"

- `user's roles = "Roles"` (この属性は設定可能です)

ユーザーが直接インポートされない場合、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する際には、グループ情報が使用されます。ユーザーは複数のグループに所属することができます。したがって、1人のユーザーがセッション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 を使用して設定可能です。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与えられません。

ヒント: ローカル ユーザーとしてログインする必要がある場合は、`https://vcloud.example.com/tenant/tenant_name/login` などの構成したベース URL を使用できます。

前提条件

- 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 プロバイダからの次のメタデータを含む XML ファイルを取得します。
 - 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 プロバイダのドキュメントを参照してください。

手順

- 1 上部ナビゲーション バーで [管理] を選択します。
- 2 左側のパネルで、ID プロバイダの下で、[SAML] をクリックし、[編集] をクリックします。

現在の SAML 設定が表示されます。

- 3 [サービス プロバイダ] タブから、VMware Cloud Director SAML サービス プロバイダのメタデータをダウンロードします。

- a システム組織のエントリ ID を入力します。

エントリ ID は、ID プロバイダがシステム組織を識別するためのものです。

- b 証明書の有効期限を確認し、期限切れが近い場合、[再生成] をクリックして、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、これらのいずれかまたは両方が必要になることがあります。

- c [メタデータ] リンクをクリックします。

リンクは、`https://VCD_host_name/cloud/org/System/saml/metadata/alias/vcd` のようになります。

ブラウザで、ID プロバイダに提供する必要のある SAML サービス プロバイダのメタデータが、XML ファイル形式でダウンロードされます。

- 4 [ID プロバイダ] タブで、ID プロバイダから以前に受信した SAML メタデータをアップロードします。

- a [SAML の ID プロバイダを使用する] を選択します。

- b [参照] アイコンをクリックしてファイルをアップロードするか、またはファイルのコンテンツをコピーして [メタデータ XML] テキスト ボックスに貼り付けます。

- 5 [保存] をクリックします。

証明書の管理

VMware Cloud Director から証明書をインポート、ダウンロード、編集、および削除できます。証明書の PEM データをクリップボードにコピーできます。

信頼されている証明書のインポート

vCenter Server、NSX Manager など、VMware Cloud Director が通信するサーバの証明書をインポートできます。

FIPS モードで VMware Cloud Director を使用する場合は、FIPS と互換性のあるプライベート キーを使用する必要があります。pyOpenSSL を使用すると、FIPS と互換性のある PKCS#8 形式でプライベート キーを生成できます。OpenSSL を使用して PKCS#8 プライベート キーを生成した場合、プライベート キーに FIPS との互換性はありません。FIPS モードの詳細については、[サーバ グループのセルでの FIPS モードの有効化または VMware Cloud Director アプライアンスでの FIPS モードの有効化または無効化](#)を参照してください。

手順

- 1 上部ナビゲーション バーで [管理] を選択します。
- 2 左側のパネルの [証明書の管理] で [信頼されている証明書] を選択し、[インポート] をクリックします。
- 3 インポートする証明書を含む PEM ファイルをアップロードして、[インポート] をクリックします。
- 4 (オプション) 証明書名を編集します。

5 [インポート] をクリックします。

次のステップ

- 証明書をダウンロードします。
- 証明書名を編集します。
- 証明書を削除します。
- PEM データをクリップボードにコピーします。

証明書ライブラリへの証明書のインポート

VMware Cloud Director の証明書ライブラリでは、サーバや Edge Gateway など、保護が必要なエンティティを作成する場合に使用する証明書をインポートできます。

証明書ライブラリには、1つの証明書、証明書チェーン、プライベート キー、証明書の有効期限、証明書で保護されているエンティティなどの情報が含まれています。

証明書ライブラリはサイトごとに個別に管理する必要があります。

FIPS モードで VMware Cloud Director を使用する場合は、FIPS と互換性のある自己署名証明書とプライベート キーを使用する必要があります。pyOpenSSL を使用して、自己署名付きの暗号化されていない証明書とプライベート キーを生成できます。OpenSSL を使用して自己署名証明書とプライベート キーを生成した場合、証明書とプライベート キーに FIPS との互換性はありません。FIPS モードの詳細については、[サーバ グループのセルでの FIPS モードの有効化または VMware Cloud Director アプライアンスでの FIPS モードの有効化または無効化](#)を参照してください。

手順

- 1 上部ナビゲーション バーで [管理] を選択します。
- 2 左側のパネルの [証明書の管理] で [証明書ライブラリ] を選択し、[インポート] をクリックします。
- 3 証明書ライブラリ内のこの証明書の名前と、必要に応じて説明を入力して、[次へ] をクリックします。
- 4 インポートする証明書チェーンを含む PEM ファイルをアップロードして、[次へ] をクリックします。
- 5 (オプション) プライベート キー ファイルをアップロードします。

プライベート キー ファイルはパスフレーズで保護されない可能性があります。

- 6 [インポート] をクリックします。

結果

インポートされた証明書は、保護が必要なエンティティを作成するときに使用可能な証明書のリストに表示されます。

次のステップ

- 証明書をダウンロードします。
- 証明書の名前と説明を編集します。
- 証明書を削除します。削除できるのは、エンティティを保護していない証明書のみです。

- 証明書の PEM データをクリップボードにコピーします。

プラグインの管理

VMware Cloud Director プラグインは、Service Provider Admin Portal および VMware Cloud Director Tenant Portal の機能を拡張します。Service Provider Admin Portal からプラグインのアップロード、無効化、および削除ができます。また、サービス プロバイダや個々の組織にプラグインを公開できます。

一部のプラグインは、VMware Cloud Director の一部としてインストールされます。

CPOM 拡張機能

VMware Cloud Director Tenant Portal を使用して専用 vCenter Server インスタンスおよびプロキシを表示および管理する機能を提供します。

ポータルのカスタマイズ

VMware Cloud Director Service Provider Admin Portal および VMware Cloud Director Tenant Portal をカスタマイズする機能を提供します。

vCloud Availability

VMware vCloud[®] Availability[™] プラグインには、VMware Cloud Director のユーザー インターフェイスから vCloud Availability Portal に直接アクセスできる機能があります。詳細については、[vCloud Availability のドキュメント](#)を参照してください。

プラグインのアップロード

サービス プロバイダやクラウド内の組織が使用できるように、追加のプラグインを VMware Cloud Director Service Provider Admin Portal にアップロードすることができます。

前提条件

プラグインのインストール ファイルをダウンロードします。

手順

- 1 上部ナビゲーション バーで、[詳細] - [ポータルのカスタマイズ] の順に選択します。
- 2 [アップロード] をクリックします。
- 3 [プラグイン ファイルの選択] をクリックして、ターゲット インストール ファイルを参照し、[開く] をクリックします。
- 4 [次へ] をクリックします。

- 5 このプラグインの範囲を選択します。

オプション	説明
サービス プロバイダ	プラグイン機能は、VMware Cloud Director Service Provider Admin Portal で使用可能になります。
テナント	プラグイン機能は、選択した組織の VMware Cloud Director Service Provider Admin Portal で使用可能になります。

- 6 プラグインの範囲をテナントに設定した場合は、このプラグインを公開する組織を選択します。

- 7 [確認して完了] 画面を確認し、[完了] をクリックします。

プラグインの有効化または無効化

すべての組織がプラグインを使用できないようにするには、プラグインを無効にします。

手順

- 1 上部ナビゲーション バーで、[詳細] - [ポータルのカスタマイズ] の順に選択します。
- 2 対象のプラグインの名前の横にあるチェック ボックスを選択し、[有効化] または [無効化] をクリックします。

プラグインの削除

1 つ以上のプラグインを VMware Cloud Director Service Provider Admin Portal から削除できます。

手順

- 1 上部ナビゲーション バーで、[詳細] - [ポータルのカスタマイズ] の順に選択します。
- 2 削除するプラグインの名前の横にあるチェック ボックスを選択して、[削除] をクリックします。
- 3 確認するには、[保存] をクリックします。

組織からのプラグインの公開または公開解除

プラグインが提供する機能を使用できる組織の組み合わせは、変更することができます。

組織の組み合わせは、複数のプラグインに対して変更できます。

手順

- 1 上部ナビゲーション バーで、[詳細] - [ポータルのカスタマイズ] の順に選択します。
- 2 ターゲット プラグインの名前の横にあるチェック ボックスを選択し、[公開] をクリックします。
- 3 このプラグインの範囲を選択します。

オプション	説明
サービス プロバイダ	プラグイン機能は、VMware Cloud Director Service Provider Admin Portal で使用可能になります。
テナント	プラグイン機能は、選択した組織の VMware Cloud Director Service Provider Admin Portal で使用可能になります。

- 4 プラグインの範囲をテナントに設定した場合は、このプラグインを公開する組織を選択します。
- 5 [保存] をクリックします。

VMware Cloud Director ポータルのカスタマイズ

企業のブランディング基準を満たし、完全に独自のクラウド エクスペリエンスを実現するには、VMware Cloud Director Service Provider Admin Portal および各組織の VMware Cloud Director Tenant Portal にロゴとテーマを設定します。また、VMware Cloud Director ポータルの右上にある 2 つのメニューを変更して、カスタム リンクを追加することもできます。

注： ブランディングの属性およびリンクをカスタマイズするには、branding vCloud OpenAPI メソッドを使用する必要があります。<https://code.vmware.com>にある VMware Cloud Director OpenAPI のスタート ガイドを参照してください。

ポータル ブランディング

VMware Cloud Director には、インストールの一部として、2 つのテーマ（デフォルト テーマとダーク テーマ）が含まれています。ユーザーはカスタム テーマを作成、管理、および適用できます。ポータル名、ロゴ、およびブラウザ アイコンも変更できます。また、ブラウザのタイトルには設定したポータル名が使用されます。

ブランディングの属性をシステム レベルで設定すると、VMware Cloud Director Service Provider Admin Portal をカスタマイズできます。特定のテナントにブランディング属性を設定した場合以外は、各組織の VMware Cloud Director Tenant Portal にはシステム ブランディング属性が使用されます。

特定のテナントに、ポータル名、背景色、ロゴ、アイコン、テーマ、およびカスタム リンクの任意の組み合わせを選択して、オーバーライドすることができます。設定しなかった値には、対応するシステムのデフォルト値が使用されます。

注： デフォルトでは、ログインしたセッション以外の場所に個々のテナント ブランディングは表示されません。テナント間で他のテナントの存在を認識できないように、ログインおよびログアウト画面には各テナントのブランディングは表示されません。ログインしたセッション以外の場所でブランディングを有効にするには、次のセル管理ツールを使用します。

```
manage-config -n backend.branding.requireAuthForBranding -v false
```

セル管理ツールの使用については、『VMware Cloud Director インストール、構成、およびアップグレード ガイド』を参照してください。

カスタム リンク

カスタム リンクは、ポータル ブランディングのコンポーネントです。カスタム リンクには、次の 2 種類があります。

- `override` メニュー項目は、[ヘルプ]、[バージョン情報]、および [VMRC のダウンロード] のメニュー項目の既存のリンクを置き換えます。デフォルトでは、ユーザーは [VMRC のダウンロード] から <https://my.vmware.com> にリダイレクトされ、VMRC をダウンロードできます。ユーザーが VMRC をダウンロードするには、アカウントを登録する必要があります。このリンクをオーバーライドすることで、VMRC インストーラを独自のサーバに再配置できます。
- `link` メニュー項目は、ポータルの右上隅にある [ログアウト] メニュー項目に追加される新しいリンクです。新しいカスタム リンクは、API 呼び出し内で指定した順序で表示されます。

これらのカスタム リンクを整理するには、`section` および `separator` のメニュー項目を使用します。
`section` メニュー項目はメニューにヘッダーを追加し、`separator` メニュー項目はメニューに行を追加します。

カスタム リンクはカスタム変数をサポートします。カスタム変数は、識別情報をクエリ パラメータの形式で他のアプリケーションに渡す場合に使用できます。

VMware Cloud Director では、カスタム リンクの `url` 値に次のカスタム変数を使用できます。

表 11-2. カスタム リンクのカスタム変数

変数	説明
<code>\${TENANT_NAME}</code>	組織名
<code>\${TENANT_ID}</code>	組織 ID
<code>\${SESSION_TOKEN}</code>	x-vcloud-authorization トークン

たとえば、次のようになります。

```
url: https://host:port/tenant/${TENANT_NAME}/vdc
```

組織 `myorg` の VMware Cloud Director Tenant Portal であれば、次のようになります。

```
url: https://host:port/tenant/myorg/vdc
```

パスワード ポリシーの設定

ユーザーが一定の回数のログインに失敗したら VMware Cloud Director にログインできなくなるようにするには、アカウント ロックアウトを有効にします。

システム アカウント ロックアウト ポリシーの変更は、すべての新しい組織に適用されます。アカウント ロックアウト ポリシーの変更前に作成された組織は、組織レベルで変更する必要があります。

手順

- 1 上部ナビゲーション バーで [管理] を選択します。

- 2 左側のパネルの [設定] で、[パスワード ポリシー] をクリックします。
- 3 [編集] をクリックします。
- 4 アカウント ロックアウトを有効にするには、[アカウント ロックアウト] トグルをオンにします。
- 5 アカウントのロック前に許可される無効なログイン回数を選択します。
- 6 ロックアウト間隔を選択します。
- 7 システム管理者 アカウントのロックアウトを有効にするには、[システム管理者アカウントはロックアウトできます] トグルをオンにします。
- 8 [保存] をクリックします。

vSphere サービスの構成

vSphere ID プロバイダがシステム管理者を認証できるように、VMware Cloud Director を構成して vCenter Single Sign-On の使用を有効にすることができます。

vCenter Lookup Service には vSphere インフラストラクチャに関するトポロジ情報が含まれており、vSphere コンポーネントが安全に相互接続できます。

手順

- 1 上部ナビゲーション バーで [管理] を選択します。
- 2 左側のパネルの [設定] で、[vSphere サービス] を選択します。
- 3 vSphere サービスを構成します。
 - VMware Cloud Director を vCenter Lookup Service に登録するには、[登録] をクリックします。
 - VMware Cloud Director を vCenter Lookup Service から登録解除するには、[登録解除] をクリックします。
- 4 vCenter Lookup Service の URL (たとえば、`https://hostname:443/lookupservice/sdk`) を入力します。
- 5 管理者権限を持つ vCenter Single Sign-On ユーザー (たとえば、`administrator@your_domain_name` ユーザー) のユーザー名とパスワードを入力します。

結果

VMware Cloud Director を vCenter Lookup Service に登録した場合、システム管理者は、vCenter Single Sign-On 認証情報を使用して VMware Cloud Director にログインする必要があります。

VMware Cloud Director の監視

12

システム管理者は、完了した操作と処理中の操作を監視し、プロバイダ仮想データセンター、組織仮想データセンター、およびデータストア レベルでリソース使用状況に関する情報を表示できます。

バージョン 9.1 以降の VMware Cloud Director は VMware vCenter Chargeback Manager をサポートしていません。VMware 製品の相互運用性マトリックス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。

- VMware Cloud Director およびコスト レポート作成
- プロバイダ仮想データセンターの使用情報の表示

VMware Cloud Director およびコスト レポート作成

VMware Cloud Director に VMware vRealize Operations Tenant App を使用して、VMware Cloud Director のコスト レポート作成システムを設定できます。

VMware vRealize Operations Tenant App には、サービス プロバイダがユーザー ベースにチャージバック サービスを提供するための測定機能があります。

VMware vRealize Operations Tenant App は、テナント管理者に使用環境および請求データの表示機能を提供するテナント用アプリケーションでもあります。

VMware Cloud Director と VMware vRealize Operations Tenant App の互換性の詳細については、VMware 製品の相互運用性マトリックス (http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php) を参照してください。

VMware vRealize Operations Tenant App は <https://marketplace.vmware.com/vsx/solutions/management-pack-for-vcloud-director> からダウンロードできます。

VMware vRealize Operations Tenant App の使用方法については、『サービス プロバイダとしての VMware Cloud Director 向け vRealize Operations テナント アプリの使用』および『テナントとしての VMware Cloud Director 向け vRealize Operations テナント アプリの使用』を参照してください。

プロバイダ仮想データセンターの使用情報の表示

プロバイダ仮想データセンターは、コンピューティング リソース、メモリ リソース、およびストレージ リソースを組織仮想データセンターに提供します。プロバイダ仮想データセンター リソースの使用を監視して、リソースを追加するかどうかを決定できます。

手順

- 1 上部ナビゲーション バーで [リソース] を選択し、[クラウド リソース] をクリックします。
- 2 左側のパネルで [プロバイダ VDC] を選択し、ターゲット プロバイダ仮想データセンターの名前をクリックします。
- 3 [設定] - [メトリック] タブの順にクリックします。
- 4 各パラメータの詳細については、各情報アイコンをクリックします。

VMware Cloud Director Service Provider Admin Portal の [コンテンツ ライブラリ] ビューには、vRealize Orchestrator と統合するためのインターフェイスが用意されています。vRealize Orchestrator ワークフローは、サービス プロバイダの管理者がテナントまたはその他のサービス プロバイダに公開できるサービスのカタログとして使用することができます。この方法で、サービスプロバイダが提供する一連の機能および管理機能を拡張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。

- [vRealize Orchestrator と VMware Cloud Director の統合](#)
- [サービス カテゴリの作成](#)
- [サービス カテゴリの編集](#)
- [サービスのインポート](#)
- [サービスの検索](#)
- [サービスの実行](#)
- [サービス カテゴリの変更](#)
- [サービスの登録解除](#)
- [サービスの公開](#)

vRealize Orchestrator と VMware Cloud Director の統合

vRealize Orchestrator と VMware Cloud Director を統合するには、VMware Cloud Director Service Provider Admin Portal を使用します。

vRealize Orchestrator と VMware Cloud Director を統合すると、VMware Cloud Director の基本機能が拡張され、サービス プロバイダの管理者がワークフローのオーケストレーションおよびサードパーティ プラグインを利用して複雑な自動化タスクを開発できるようになります。

サービス プロバイダの管理者は VMware Cloud Director Service Provider Admin Portal を使用して、登録された vRealize Orchestrator サーバ インスタンスからワークフローを表示、インポート、および実行できます。

VMware Cloud Director Service Provider Admin Portal で vRealize Orchestrator ワークフローをサービス プロバイダまたはテナントに公開することにより、クイック アクセス制御を許可し、カスタム サービスと組み込みサービスを両方とも実行できるようになります。

vRealize Orchestrator の詳細なワークフロー ライブラリには、特定の課題を解決し、一般的な管理者タスクを実行するために設計された事前作成済みのタスクが含まれています。サードパーティ プラグインは [VMware Solution Exchange](#) で入手することもできます。

VMware Cloud Director への vRealize Orchestrator インスタンスの登録

VMware Cloud Director で vRealize Orchestrator を使用してワークフローのオーケストレーションとタスクの自動化を利用するには、VMware Cloud Director Service Provider Admin Portal に vRealize Orchestrator インスタンスを登録します。

前提条件

- vRealize Orchestrator サーバ インスタンスを展開して、設定します。詳細については、vRealize Orchestrator ドキュメントの『VMware vRealize Orchestrator のインストールと構成』を参照してください。
- 認証プロバイダとして vSphere を使用するように vRealize Orchestrator を構成します。
- VMware Cloud Director に、vRealize Orchestrator で認証に使用される vCenter Single Sign-On と同じ Platform Services Controller の Lookup Service が登録されていることを確認します。

手順

- 1 上部ナビゲーション バーで [ライブラリ] を選択します。
 - a 左側のパネルで [サービス管理] を選択します。

登録されている vRealize Orchestrator サーバのリストが表示されます。
 - 2 新しい vRealize Orchestrator サーバを登録するには、[追加] をクリックします。
- [vRealize Orchestrator の登録] ダイアログが表示されます。
- 3 以下の値を入力します。

オプション	説明
名前	登録されている vRealize Orchestrator インスタンスの名前。
説明	登録されている vRealize Orchestrator サーバ インスタンスの説明。
ホスト名	vRealize Orchestrator サーバの完全修飾ドメイン名およびサーバ ポート。デフォルト HTTPS ポートの値は 443 です。
	注： VMware Cloud Director は vRealize Orchestrator の API インターフェイスに接続されます。
ユーザー名	vRealize Orchestrator 管理者グループのメンバーであるユーザー アカウント。
パスワード	vRealize Orchestrator 管理者アカウントのパスワード。
トラスト アンカー	PEM 形式の vRealize Orchestrator サーバの SSL 証明書。 アップロード アイコンをクリックして、.pem ファイルを検索して選択します。

- 4 [OK] をクリックして、登録を完了します。

vRealize Orchestrator サーバが VMware Cloud Director に登録されました。

サービス カテゴリの作成

サービスをサービス カテゴリで分類できます。

手順

- 1 上部ナビゲーション バーで [ライブラリ] を選択します。
 - a 左側のパネルで [サービス管理] を選択します。
 - b [サービス カテゴリ] タブに移動します。

既存のサーバ カテゴリのリストが表示されます。
- 2 新しいサービス カテゴリを作成するには、[追加] をクリックします。
[サービス カテゴリの新規作成] ダイアログが表示されます。
- 3 以下の値を入力します。


オプション	説明
名前	サービス カテゴリの名前。
アイコン	サービス カテゴリ用に表示されているアイコンをインポートします。
説明	サービス カテゴリの短い説明。

サービス カテゴリの編集

既存のサービス カテゴリを編集できます。

手順

- 1 上部ナビゲーション バーで [ライブラリ] を選択します。
 - a 左側のパネルで [サービス管理] を選択します。
 - b [サービス カテゴリ] タブに移動します。

既存のサーバ カテゴリのリストが表示されます。
- 2 選択したサービス カテゴリの左側にあるリスト バー () を使用して、[編集] をクリックします。
- 3 次の値を編集します。

オプション	説明
名前	サービス カテゴリの名前。
アイコン	サービス カテゴリ用に表示されているアイコンをインポートします。
説明	サービス カテゴリの短い説明。

サービスのインポート

VMware Cloud Director に登録されている vRealize Orchestrator インスタンスのワークフロー ライブラリから、サービスをインポートできます。

前提条件

- vRealize Orchestrator インスタンスを登録します。[VMware Cloud Director への vRealize Orchestrator インスタンスの登録](#) を参照してください。
- サービス カテゴリを作成します。[サービス カテゴリの作成](#) を参照してください。

手順

- 1 上部ナビゲーション バーで [ライブラリ] を選択します。
 - a 左側のパネルで [サービス ライブラリ] を選択します。使用可能なサービスがカード 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 個の項目が表示され、名前を基準としてアルファベット順にソートされます。各カードは項目が vRealize Orchestrator ワークフローであることを示していて、このワークフローがインポートされるサービスの名前およびサービス カテゴリに対応するタグが表示されます。
- 2 新しいサービスをインポートするには、[インポート] ボタンをクリックします。
- 3 [インポート] ウィザードの手順に沿って処理を進めます。

オプション	説明
ターゲット ライブラリにインポート	サービスをインポートするサービス カテゴリを選択します。
ソースを選択	ワークフローのインポート元の vRealize Orchestrator インスタンスを選択します。
ワークフローを選択	階層ツリー ビューを展開して、インポートする 1 つまたは複数のワークフローを選択します。
確認	詳細を確認し、[完了] をクリックしてインポートを完了します。

インポートされたワークフローが、[サービス ライブラリ] カード ビューに表示されます。

サービスの検索

サービスは、名前またはサービスが属しているサービス カテゴリで検索できます。

手順

- 1 上部ナビゲーション バーで [ライブラリ] を選択します。
 - a 左側のパネルで [サービス ライブラリ] を選択します。使用可能なサービスがカード 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 個の項目が表示され、名前を基準としてアルファベット順にソートされます。各カードは項目が vRealize Orchestrator ワークフローであることを示していて、このワークフローがインポートされるサービスの名前およびサービス 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、検索するサービスまたはサービス カテゴリの名前を表す語句または文字を入力します。

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 個の項目が表示され、名前を基準としてアルファベット順にソートされます。

サービスの実行

vRealize Orchestrator ワークフローをインポートされたサービスとして実行できます。

手順

- 1 上部ナビゲーション バーで [ライブラリ] を選択します。

a 左側のパネルで [サービス ライブラリ] を選択します。

使用可能なサービスがカード 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 個の項目が表示され、名前を基準としてアルファベット順にソートされます。各カードは項目が vRealize Orchestrator ワークフローであることを示していて、このワークフローがインポートされるサービスの名前およびサービス カテゴリに対応するタグが表示されます。

- 2 サービスを実行するには、選択したサービスのカードで [実行] をクリックします。

[サービスの実行] ウィザードが表示されます。

- 3 サービスの必須の入力パラメータを入力し、[完了] をクリックします。

結果

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。

注： vRealize Orchestrator ワークフローを VMware Cloud Director サービスとして開始すると、VMware Cloud Director はワークフローの実行コンテキストにカスタム パラメータをいくつか追加します。

カスタム プロパティ	説明
_vcd_orgName	サービスを実行するユーザーが属している組織の名前。
_vcd_orgId	サービスを実行するユーザーが属している組織の ID。
_vcd_username	サービスを実行するユーザーの名前。
_vcd_isAdmin	サービスを実行するユーザーが管理者である場合は、値が True になります。
_vdc_isAdmin	廃止されました。サービスを実行するユーザーが管理者である場合は、値が True になります。
_vdc_username	廃止されました。サービスを実行するユーザーの名前。
_vcd_sessionToken	VMware Cloud Director に対する認証の成功後に受信した認証トークン
_vcd_apiEndpoint	VMware Cloud Director REST API エンドポイント

サービス カテゴリの変更

サービスが属しているカテゴリを変更できます。

手順

- 1 上部ナビゲーション バーで [ライブラリ] を選択します。
 - a 左側のパネルで [サービス ライブラリ] を選択します。

使用可能なサービスがカード 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 個の項目が表示され、名前を基準としてアルファベット順にソートされます。各カードは項目が vRealize Orchestrator ワークフローであることを示していて、このワークフローがインポートされるサービスの名前およびサービス カテゴリに対応するタグが表示されます。
- 2 選択したサービスのカードで、[管理] - [カテゴリの変更] の順に選択します。

[カテゴリの変更] ダイアログが開きます。
- 3 サービスを配置するカテゴリを選択して、[保存] をクリックします。

サービスの登録解除

サービス プロバイダとテナントの両方のサービスへのアクセス権を削除するには、サービスを登録解除します。

手順

- 1 上部ナビゲーション バーで [ライブラリ] を選択します。
 - a 左側のパネルで [サービス ライブラリ] を選択します。

使用可能なサービスがカード 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 個の項目が表示され、名前を基準としてアルファベット順にソートされます。各カードは項目が vRealize Orchestrator ワークフローであることを示していて、このワークフローがインポートされるサービスの名前およびサービス カテゴリに対応するタグが表示されます。
- 2 選択したサービスのカードで、[管理] - [ワークフローの登録解除] の順に選択します。

[ワークフローの登録解除] ダイアログが開きます。
- 3 サービス ライブラリからサービスを削除するには、[削除] をクリックします。

サービスの公開

サービスを公開することにより、サービス プロバイダおよびテナントからサービスへのアクセスを制御できます。

手順

- 1 上部ナビゲーション バーで [ライブラリ] を選択します。
 - a 左側のパネルで [サービス ライブラリ] を選択します。

使用可能なサービスがカード 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 個の項目が表示され、名前を基準としてアルファベット順にソートされます。各カードは項目が vRealize Orchestrator ワークフローであることを示していて、このワークフローがインポートされるサービスの名前およびサービス カテゴリに対応するタグが表示されます。

- 2 選択したサービスのカードで、[管理] - [ワークフローの公開] の順に選択します。

[ワークフローの公開] ダイアログが表示されます。

- 3 サービス プロバイダに公開するには、[サービス プロバイダに公開] を選択して、[保存] をクリックします。

- 4 特定のテナント組織に公開するには、[テナントに公開] ボタンを選択します。

- a 使用可能なテナント組織のリストが表示されます。ワークフローを公開するテナント組織を選択して、[保存] をクリックします。

- 5 すべてのテナント組織に公開するには、[すべてのテナントに公開] を選択して、[保存] をクリックします。

定義済みエンティティの管理

14

VMware Cloud Director 10.2 以降では、サービス プロバイダは VMware Cloud Director API を使用して、テナントに追加の VMware Cloud Director 機能を提供する拡張機能を作成できます。

サービス プロバイダは、ランタイム定義エンティティ (RDE) を作成し、拡張機能を有効にして、VMware Cloud Director で拡張機能固有の情報を保存および操作することができます。たとえば、Kubernetes 拡張機能は、管理している Kubernetes クラスタに関する情報を RDE に保存できます。この拡張機能は、RDE の情報を使用して、これらのクラスタを管理するための拡張 API を提供できます。

定義済みエンティティへのアクセス

RDE へのアクセスは 2 つの補完的なメカニズムで制御されます。

- 権限 - RDE タイプを作成した場合は、そのタイプの権限バンドルを作成します。特定の操作に対するアクセス権を提供するには、このバンドルから他のロールに権限を割り当てる必要があります。各バンドルには、表示 : TYPE、編集 : TYPE、完全コントロール : TYPE、管理者の表示 : TYPE、管理者の完全コントロール : TYPE という 5 つのタイプ固有の権限があります。

表示 : TYPE、編集 : TYPE、および 完全コントロール : TYPE 権限は、ACL エントリと組み合わせた場合のみ機能します。

- アクセス コントロール リスト (ACL) - ACL テーブルには、システム内の特定のエンティティに対してユーザーが保持しているアクセス権を定義するエントリが含まれています。これによりエンティティの制御レベルを強化することができます。たとえば、編集 : TYPE 権限は、ユーザーがアクセス権を持つエンティティは、そのユーザーが変更できることを示します。一方、ACL テーブルは、そのユーザーがアクセスできるエンティティを定義します。

全般 ACL の表示権限を持つシステム管理者は、`accessControls` API を使用して特定の定義済みエンティティに割り当てられた ACL を表示できます。VMware Cloud Director API リファレンスについては、code.vmware.com を参照してください。

全般 ACL の管理 権限を持つシステム管理者は、`accessControls` API を使用して特定の ACL を作成、変更、および削除することができます。

表 14-1. RDE 操作に関する権限および ACL エントリ

エンティティの操作	オプション	説明
読み取り	管理者の表示 : TYPE 権限	この権限を持つユーザーは、組織内にあるこのタイプのすべての RDE を表示できます。
	表示 : TYPE 権限および表示以上の ACL エントリ	この権限および読み取りレベルの ACL を持つユーザーは、このタイプの RDE を表示できます。
変更	管理者の完全コントロール : TYPE 権限	この権限を持つユーザーは、すべての組織内にあるこのタイプの RDE を作成、表示、変更、および削除できます。
	編集 : TYPE 権限および変更以上の ACL エントリ	この権限および変更レベルの ACL を持つユーザーは、このタイプの RDE を作成、表示、および変更できます。
削除	管理者の完全コントロール : TYPE 権限	この権限を持つユーザーは、すべての組織内にあるこのタイプの RDE を作成、表示、変更、および削除できます。
	完全コントロール : TYPE 権限および完全コントロールの ACL エントリ	この権限および完全コントロールレベルの ACL を持つユーザーは、このタイプの RDE を作成、表示、変更、および削除できます。

VMware Cloud Director API またはユーザー インターフェイスを使用して、このタイプのエンティティを管理する組織に権限バンドルを公開できます。権限バンドルを公開した後に、バンドルから組織内のロールに権限を割り当てることができます。

VMware Cloud Director API を使用して、ACL テーブルを編集できます。

この章には、次のトピックが含まれています。

- [定義済みエンティティの共有](#)
- [カスタム エンティティの管理](#)

定義済みエンティティの共有

ランタイム定義エンティティ (RDE) は、他のシステム管理者またはテナントと RDE を共有することでアクセス権を付与することができます。

別のユーザーとの定義済みエンティティの共有

- 1 定義されたエンティティへのアクセス権をテナントに付与する場合は、定義済みエンティティ タイプの権限バンドルをテナントの組織に公開します。たとえば、Tanzu Kubernetes クラスタの作成と管理を行うには、`vmware : tkgcluster` 資格権限バンドルを公開する必要があります。『[権限バンドルの公開または公開の解除](#)』を参照してください。

定義済みエンティティをシステム管理者と共有する場合、この手順はスキップします。

- 2 バンドルから、定義したエンティティに対する特定のレベルのアクセス権を保持するユーザー ロールに、表示 : TYPE、編集 : TYPE、または 完全コントロール : TYPE 権限を割り当てます。

たとえば、tkg_viewer ロールを持つユーザーが組織内の Tanzu Kubernetes クラスタを表示できるようにする場合は、このロールに 表示 : Tanzu Kubernetes ゲスト クラスタ権限を追加する必要があります。

tkg_author ロールを持つユーザーが組織内の Tanzu Kubernetes クラスタを作成、表示、および変更できるようにする場合は、このロールに 編集 : Tanzu Kubernetes ゲスト クラスタ権限を追加します。tkg_admin ロールを持つユーザーがこの組織内の Tanzu Kubernetes クラスタを作成、表示、変更、および削除できるようにする場合は、このロールに 完全コントロール : Tanzu Kubernetes ゲスト クラスタ権限を追加します。

- 3 次の REST API 呼び出しを行って、特定のユーザーにアクセス コントロール リスト (ACL) を付与します。

```
POST https://[address]/cloudapi/1.0.0/entities/urn:vcloud:entity:[vendor]:[type name]:
[version]:[UUID]/accessControls
{
  "grantType" : "MembershipAccessControlGrant",
  "accessLevelId" : "urn:vcloud:accessLevel:[Access_level]",
  "memberId" : "urn:vcloud:user:[User_ID]"
}
```

Access_level には ReadOnly、ReadWrite、または FullControl を指定する必要があります。*User_ID* には、定義されたエンティティへのアクセス権を付与するユーザーの ID を指定する必要があります。

この例で示した、tkg_viewer ロールを持つユーザーには、ACL アクセス権を付与できません。tkg_author または tkg_admin ロールを持つユーザーは、API 要求を使用して、tkg_viewer、tkg_author、または tkg_admin ロールを持つユーザーに VMWARE:TKGCLUSTER エンティティへの ACL アクセスを付与することでアクセス権の共有が可能になります。

また、REST API 呼び出しを使用してアクセス権を取り消したり、エンティティへのアクセス権を持つユーザーを表示したりすることもできます。code.vmware.com の VMware Cloud Director REST API のドキュメントを参照してください。

定義済みエンティティに対する管理者権限の共有

- 1 定義されたエンティティへのアクセス権をテナントに付与する場合は、定義済みエンティティ タイプの権限バンドルをテナントの組織に公開します。たとえば、Tanzu Kubernetes クラスタの作成と管理を行うには、vmware : tkgcluster 資格権限バンドルを公開する必要があります。『[権限バンドルの公開または公開の解除](#)』を参照してください。

定義済みエンティティをシステム管理者と共有する場合、この手順はスキップします。

- 2 バンドルから、定義したエンティティへの特定のレベルのアクセス権を保持するユーザー ロールに、管理者の表示 : TYPE または管理者の完全コントロール : TYPE 権限を割り当てます。

たとえば、このロールを持つユーザーが組織内のすべての Tanzu Kubernetes クラスタを表示できるようにする場合は、このロールに管理者の表示 : Tanzu Kubernetes ゲスト クラスタ権限を追加する必要があります。このロールを持つユーザーがすべての組織内の Tanzu Kubernetes クラスタを作成、表示、変更、および削除できるようにする場合は、このロールに 管理者の完全コントロール : Tanzu Kubernetes ゲスト クラスタ権限を追加します。

管理者の完全コントロール: Tanzu Kubernetes ゲスト クラスタ権限を持つユーザーは、任意の VMWARE: TKGCLUSTER エンティティに対する ACL アクセス権を付与することができます。

定義済みエンティティの所有者の変更

定義済みエンティティの所有者、または管理者の完全コントロール: TYPE 権限を持つユーザーは、定義済みエンティティ モデルを更新し、所有者フィールドを新しい所有者の ID で変更することによって、所有権を別のユーザーに転送できます。

カスタム エンティティの管理

VMware Cloud 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。サービス プロバイダがカスタム エンティティ定義を別のサービス プロバイダに公開しているか、または 1 つ以上のテナントに公開している場合、VMware Cloud Director ユーザーは必要に応じてこれらのタイプを所有、管理、および変更することができます。サービス プロバイダのユーザーおよび組織のユーザーは、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。

カスタム エンティティの検索

カスタム エンティティを名前で検索できます。

手順

- 1 上部ナビゲーション バーで [ライブラリ] を選択します。

- a 左側のパネルで [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 個の項目が表示され、名前を基準としてアルファベット順にソートされます。

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のバインド先の vRealize Orchestrator オブジェクト タイプは変更できません。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。

手順

- 1 上部ナビゲーション バーで [ライブラリ] を選択します。

- a 左側のパネルで [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。

手順

- 1 上部ナビゲーション バーで [ライブラリ] を選択します。

- a 左側のパネルで [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 新しいカスタム エンティティを追加するには、[新規] をクリックします。

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。 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

VMware Cloud 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。

手順

- 1 上部ナビゲーション バーで [ライブラリ] を選択します。

- a 左側のパネルで [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。

手順

- 1 上部ナビゲーション バーで [ライブラリ] を選択します。

- a 左側のパネルで [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。

手順

- 1 上部ナビゲーション バーで [ライブラリ] を選択します。

- a 左側のパネルで [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。

手順

- 1 上部ナビゲーション バーで [ライブラリ] を選択します。

- a 左側のパネルで [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。

手順

- 1 上部ナビゲーション バーで [ライブラリ] を選択します。

- a 左側のパネルで [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。