

vCloud Director 管理者ガイド

2019 年 3 月 28 日

VMware Cloud Director 9.7

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 © 2010-2020 VMware, Inc. All rights reserved. 著作権および商標情報。

目次

vCloud Director 管理者ガイド 10

更新情報 11

1 vCloud Director のスタート ガイド 12

vCloud Director 管理の概要 12

Web コンソールへのログイン 16

システム管理者のホーム ページ 16

システムの準備 16

SSL 証明書の置換 17

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 17

2 vCloud Director へのリソースの追加 19

vCenter Server および NSX リソースの追加 20

vCenter Server インスタンスの関連付け 20

vCenter Server で NSX ライセンス キーを割り当てる 23

クラウド リソースの追加 23

プロバイダ仮想データセンター 24

プロバイダ仮想データセンターの作成 24

外部ネットワーク 26

外部ネットワークの追加 27

ネットワーク プール 28

SDDC および SDDC プロキシの 31

3 組織の作成およびプロビジョニング 33

リースについて 33

割り当てモデルについて 34

推奨される割り当てモデルの使用法 35

Flex 割り当てモデル 36

割り当てプール割り当てモデル 36

従量課金制の割り当てモデル 38

予約プール割り当てモデル 38

コンピューティング ポリシーについて 39

プロバイダ仮想データセンターのコンピューティング ポリシー 39

仮想データセンターのコンピューティング ポリシー 42

組織の作成 46

[新しい組織] ウィザードの起動 46

組織の名前の指定	47
組織の LDAP オプションの指定	47
組織へのローカル ユーザーの追加	48
組織のカatalog共有、公開、およびサブスクリプション ポリシーの設定	48
電子メール環境設定の構成	48
組織のリース、割り当て容量、および制限の設定の構成	49
設定の確認と組織の作成	50
組織へのリソースの割り当て	50
[リソースの割り当て] ウィザードの起動	52
プロバイダ仮想データセンターの選択	52
割り当てモデルの選択	52
割り当てモデルの構成	53
ストレージを割り当て	55
ネットワーク プールおよびサービス	55
Edge ゲートウェイの構成	56
外部ネットワークの構成	56
新規 Edge ゲートウェイ上の IP 設定の構成	57
新規 Edge ゲートウェイ上の IP プールの細分割り当て	57
新規 Edge ゲートウェイ上のレート制限の構成	58
組織仮想データセンター ネットワークの作成	58
組織仮想データセンターの名前の指定	58
設定の確認と組織仮想データセンターの作成	59

4 Catalogの操作 60

新規Catalogの追加	61
Catalogへのアクセス	63
Catalogの共有	63
外部組織へのCatalogの公開	64
Catalogの所有者の変更	65
Catalogの削除	65
Catalogのプロパティの変更	65
外部Catalog フィードのサブスクリプション	66

5 クラウド リソースの管理 68

プロバイダ仮想データセンターの管理	68
プロバイダ仮想データセンターの有効化または無効化	68
プロバイダ仮想データセンターの削除	69
プロバイダ仮想データセンターの名前および説明の変更	69
プロバイダ仮想データセンターのマーキング	69
レガシーのプロバイダ VDC での VXLAN の有効化	70
プロバイダ仮想データセンターのデータストア	70

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	71
プロバイダ仮想データセンターでの Storage I/O Control サポートの構成	72
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の編集	73
プロバイダ VDC へのリソース プールの追加	73
プロバイダ仮想データセンター リソース プールの有効化または無効化	74
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	74
プロバイダ仮想データセンター上のリソース プール間での仮想マシンの移行	75
プロバイダ仮想データセンター データストアの低ディスク容量しきい値の構成	76
プロバイダ仮想データセンター ユーザーへの電子メール通知の送信	76
組織仮想データセンターの管理	77
組織仮想データセンターの作成	77
テンプレートからの組織仮想データセンターの作成	86
組織仮想データセンターの有効化または無効化	86
組織仮想データセンターの削除	87
組織仮想データセンターのプロパティ	87
組織仮想データセンターへのストレージ ポリシーの追加	89
組織仮想データセンター テンプレートの管理	90
組織仮想データセンター テンプレートの作成	91
組織仮想データセンター テンプレートのインスタンス化	98
組織仮想データセンター テンプレートの修正	98
組織仮想データセンター テンプレートのクローン作成	105
組織仮想データセンター テンプレートの削除	105
外部ネットワークの管理	106
外部ネットワークの名前および説明の変更	106
外部ネットワーク仕様の表示と変更	106
外部ネットワーク仕様の追加	106
外部ネットワークをバックアップする vSphere ネットワークの編集	107
外部ネットワークの削除	107
Edge ゲートウェイの管理	108
Edge クラスタの操作	108
Edge ゲートウェイの追加	110
Edge ゲートウェイから詳細ゲートウェイへの変換	114
詳細ゲートウェイで分散ルーティングを有効または無効にする	114
Edge ゲートウェイ サービスの構成	115
Edge ゲートウェイのプロパティの編集	115
Edge ゲートウェイのアップグレード	118
Edge ゲートウェイの削除	118
Edge ゲートウェイの IP 使用の表示	118
Edge ゲートウェイへの Syslog サーバー設定の適用	119
組織仮想データセンター ネットワークの管理	119
組織仮想データセンターへのネットワークの追加	120

組織 VDC ネットワークのプロパティの表示または変更	125
組織仮想データセンター ネットワーク サービスの構成	126
組織仮想データセンター ネットワークのリセット	135
組織仮想データセンター ネットワークの接続、切断、移動	136
組織仮想データセンター ネットワークを使用する vApp および vApp テンプレートの表示	137
組織仮想データセンター ネットワークの削除	137
組織仮想データセンター ネットワークの IP 使用の表示	137
クロス仮想データセンター ネットワークの構成	137
ネットワーク プールの管理	141
ネットワーク プールの名前および説明の変更	141
ネットワーク プールへのポート グループの追加	142
ネットワーク プールへの VLAN ID の追加	142
ネットワーク プールの削除	142
クラウド セルの管理	143
クラウド セルの追加	143
クラウド セルの削除	144
クラウド セルのメンテナンス メッセージの表示	144
クラウド セルのメンテナンス メッセージの非表示	144
サービス オファリングの管理	145
拡張機能の登録	146
拡張機能のプロパティの表示または変更	146
サービス オファリングと組織仮想データセンターの関連付け	147
組織仮想データセンターからサービス オファリングの関連付けを解除する	147
拡張機能の登録解除	147
サービス インスタンスの作成	148
サービス インスタンス プロパティの変更	148
仮想マシンへのサービス インスタンスの追加	149
サービス インスタンスの削除	149
マルチサイト展開の設定と管理	149
オブジェクト メタデータの作成または更新	151

6 vSphere リソースの管理 154

vCenter Server の管理	154
vCenter Server への vCloud Director の登録	154
vCenter Server 設定の変更	155
vCenter Server インスタンスの再接続	156
vCenter Server インスタンスの有効化または無効化	156
vCenter Server インスタンスの削除	157
NSX Manager 設定の変更	157
仮想マシンとホスト間のアフィニティ ルールの管理	158
ホスト グループの作成または更新	160

仮想マシン グループの作成または更新	160
仮想マシンとホストのアフィニティ ルールの作成または更新	161
vApp の検出および採用	162
vSphere データストアの管理	163
データストアの有効化または無効化	163
データストアの低ディスク領域警告の構成	163
データストアでの高速プロビジョニングのために VAAI を有効化	164
取り残されたアイテムの管理	164
取り残されたアイテムの削除	164
取り残されたアイテムの強制削除	165
リソース プールのプロパティの表示	165
ストレージ ポリシーのプロパティの表示	166

7 組織の管理 167

組織の有効化または無効化	167
組織の削除	167
組織へのカタログの追加	168
組織のプロパティの編集	168
組織名の変更	169
組織の完全な名前および説明の変更	169
組織の LDAP オプションの変更	170
組織のカタログ共有、公開、およびサブスクリプション ポリシーの変更	171
組織の電子メール環境設定の変更	171
組織のリース、割り当て容量、および制限の設定の変更	172
組織リソースの管理	173
組織 vApp および仮想マシンの管理	173
vSphere 仮想マシンの vApp への追加	173
vSphere 仮想マシンに基づく vApp の作成	174
vApp のメンテナンス モードへの設定	174
実行中の vApp の強制停止	175
仮想マシンの高速プロビジョニング	176
vApp テンプレートに関連付けられているシャドウ仮想マシンの表示	176
テナント ストレージの移行	177

8 システム管理者およびロールの管理 178

システム管理者の追加	178
システム管理者のインポート	179
システム管理者の有効化または無効化	179
システム管理者の削除	180
システム管理者のプロファイルおよび連絡先情報の編集	180
ユーザーへの電子メール通知の送信	180

システムへのアクセス権限を失ったシステム管理者の削除	181
グループのインポート	181
LDAP グループの削除	182
グループ プロパティの表示	182
権限およびロールの管理	182
事前定義ロールとその権限	184
このリリースの新しい権限	192
ロールの作成、更新、削除	193
ロールのコピー	194

9 システム設定の管理 195

全般システム設定の変更	195
全般システム設定	196
システムの電子メール設定の編集	197
SMTP 設定の構成	198
システム通知設定の構成	198
ブロック タスクおよび通知の構成	198
AMQP ブローカーの構成	199
ブロック タスク設定の構成	199
ブロック タスクの有効化	200
システムの LDAP の設定	200
LDAP 接続の構成	201
ケルベロス レalmの追加	202
LDAP 設定のテスト	203
LDAP ユーザーおよびグループ属性のカスタマイズ	203
vCloud Director と LDAP サーバーの同期	203
vCloud Director クライアント UI のカスタマイズ	204
システムのデフォルトのロゴに戻す	204
システムのデフォルトのテーマに戻す	205
公開アドレスの構成	205
公開エンドポイントのカスタマイズ	205
システム制限の構成	208
アカウント ロックアウト ポリシーの構成	209
vSphere SSO SAML プロバイダを使用するための vCloud Director の設定	210

10 vCloud Director の監視 212

vCloud Director とコスト レポート	212
タスクとイベントの表示	213
処理中および完了したシステム タスクの表示	213
処理中および完了した組織タスクの表示	213
システム イベントの表示	214

組織イベントの表示	214
実行中および完了したテナントのストレージ移行の表示	215
ブロック タスクの監視および管理	215
プロバイダ仮想データセンターの使用状況情報の表示	215
組織仮想データセンターの使用状況情報の表示	216
vCloud Director の JMX サービスの使用	216
JConsole を使用した JMX サービスへのアクセス	216
vCloud Director ログの表示	217

11 セル管理ツール リファレンス 218

vCloud Director インストール環境の構成	221
セルの管理	223
セル アプリケーションの管理	224
データベース テーブルのエクスポート	226
PostgreSQL データベースへの移行	229
データベース接続プロパティを更新する	231
破損したスケジューラ データの検出および修復	234
HTTP およびコンソール プロキシ エンドポイントの自己署名証明書の生成	235
HTTP およびコンソール プロキシ エンドポイントの証明書の置き換え	237
外部サービスからの SSL 証明書のインポート	238
許可された SSL 暗号のリストの管理	239
許可された SSL プロトコルのリストの管理	241
メトリック収集の設定	242
Cassandra メトリック データベースの構成	245
システム管理者のパスワードの復元	246
タスクの失敗ステータスの更新	247
監査メッセージ処理の構成	248
電子メール テンプレートの構成	249
親なしの仮想マシンの検索	250
VMware カスタマ エクスペリエンス改善プログラムへの参加または離脱	252
アプリケーションの設定の更新	253
カタログ同期のスロットリングの設定	254
vCenterServer 仮想マシン検出のデバッグ	255
マルチサイト拡張ネットワークの MAC アドレスの再生成	256
vCloud Director セルのデータベース IP アドレスの更新	258

vCloud Director 管理者ガイド

この『vCloud Director 管理者ガイド』は、VMware vCloud Director[®] for Service Providers 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。

対象読者

本書は、vCloud Director インストール環境の設定および管理を担当する vCloud Director システム管理者を対象としています。本書の情報は、Linux、Windows、IP ネットワーク、および VMware vSphere[®] に精通した、経験の豊富なシステムの管理者向けに記載されています。

このガイドの手順には、vCloud Director Web コンソール（Flex ベース ユーザー インターフェイス）が反映されています。vCloud Director Service Provider Admin Portal の使用に関する詳細については、『vCloud Director Service Provider Admin Portal Guide』を参照してください。

更新情報

『vCloud Director 管理者ガイド』は、製品のリリースごとに、または必要に応じて更新されます。

『vCloud Director 管理者ガイド』の更新履歴については、次の表をご確認ください。

リリース	説明
2019 年 6 月 11 日	トピック: vCloud Director セルのデータベース IP アドレスの更新 を追加しました。
2019 年 4 月 18 日	<ul style="list-style-type: none">■ 「vCloud Director とコスト レポート」のトピックを削除し、10 章 vCloud Director の監視を更新しました。■ プロバイダ仮想データセンターの作成をサポートされる最新の仮想ハードウェア バージョンに関する情報で更新しました。
2019 年 4 月 05 日	割り当てモデルについておよびコンピューティング ポリシーについての章 の情報を改訂しました。
2019 年 3 月 28 日	初期リリース。

vCloud Director のスタート ガイド

1

vCloud Director Web コンソールに初めてログインするときに、[ホーム] タブを起点にインストール環境の構成手順を実行できます。

■ vCloud Director 管理の概要

VMware vCloud 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。

■ Web コンソールへのログイン

vCloud Director のユーザー インターフェイスには、Web ブラウザを使用してアクセスできます。

■ システム管理者のホーム ページ

[ホーム] タブには、共通のタスクとサポート リソースへのリンクが表示されます。

■ システムの準備

vCloud Director Web コンソールの [ホーム] タブには、システムの使用準備のために必要なタスクへのリンクが表示されます。リンクは、前提条件のタスクを完了するとアクティブになります。

■ SSL 証明書の置換

vCloud Director サーバー グループのメンバーが自己署名した SSL 証明書を使用する場合、クラウドの中でより高い信頼性を獲得するために署名された SSL 証明書にアップグレードすることができます。

■ 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。システム管理者アカウントのパスワードも変更できます。

■ 名前と説明に対する長さの制限

vCloud 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。

vCloud Director 管理の概要

VMware vCloud 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。

『vCloud Director 管理者ガイド』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

vCloud 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、vCloud 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。

vCloud 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、vCloud Director Service Provider Admin Portal Guide またはサービス プロバイダ向け vCloud API プログラミング ガイドを参照してください。

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、vCloud 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。vCloud 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。また、vCloud Director 9.7 には、vCloud Director から基盤となる vSphere 環境へのアクセスを提供するクラウド リソースとして Software-Defined Data Center (SDDC) および SDDC プロキシが導入されています。

クラウド リソースを vCloud 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。

SDDC および SDDC プロキシ

vCloud 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 が導入されています。SDDC 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 SDDC プロキシが 1 つ以上含まれています。プロバイダは、SDDC 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、SDDC およびそのプロキシをテナントに公開できます。

SDDC およびプロキシを作成して管理するには、vCloud OpenAPI を使用する必要があります。<https://code.vmware.com> にある vCloud 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。

vCloud Director ネットワーク

vCloud 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、vCloud 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、vCloud 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。

vCloud 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。

vCloud 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。

vCloud 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、『vCloud 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アップされます。vCloud 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。

vCloud 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

vCloud 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『vCloud 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。

Web コンソールへのログイン

vCloud Director のユーザー インターフェイスには、Web ブラウザを使用してアクセスできます。

サポート対象ブラウザのリストについては、『VMware vCloud Director Installation and Configuration Guide』を参照してください。

前提条件

システム セットアップ時に作成した、システム管理者のユーザー名とパスワードが必要です。

手順

- 1 Web ブラウザを開き、**`https://hostname.domain.tld/cloud`** に移動します。

hostname.domain.tld には、vCloud Director サーバ ホストのプライマリ IP アドレスに関連付けられた完全修飾ドメイン名を指定します。たとえば、**`https://cloud.example.com/cloud`** です。

- 2 システム管理者のユーザー名とパスワードを入力し、[ログイン] をクリックします。

結果

vCloud Director に、次に実行するタスクのリストが表示されます。

システム管理者のホーム ページ

[ホーム] タブには、共通のタスクとサポート リソースへのリンクが表示されます。

vCloud Director のインストール後に初めてログインすると、[ホーム] タブには、システムを起動して稼働させるためのクイック スタート タスクの一覧が表示されます。システムの構成後も、それらのタスクに引き続きアクセスできます。

[ホーム] タブには、クラウド リソース、組織、およびシステム ユーザーの管理に関連する、共通性の高いタスクの多くに移動するためのリンクも表示されます。

システムの準備

vCloud Director Web コンソールの [ホーム] タブには、システムの使用準備のために必要なタスクへのリンクが表示されます。リンクは、前提条件のタスクを完了するとアクティブになります。

それぞれのタスクの詳細については、[表 1-1. クイック スタート タスク](#) を参照してください。

表 1-1. クイック スタート タスク

タスク	詳細
vCenter の接続	vCenter Server インスタンスの関連付け
プロバイダ仮想データセンターの作成	プロバイダ仮想データセンターの作成
外部ネットワークの作成	外部ネットワークの追加
ネットワーク プールの作成	ネットワーク プール

表 1-1. クイック スタート タスク（続き）

タスク	詳細
組織の作成	組織の作成
組織へのリソースの割り当て	組織仮想データセンターの作成
組織へのネットワークの追加	組織仮想データセンターへのネットワークの追加
組織へのカタログの追加	組織へのカタログの追加

SSL 証明書の置換

vCloud Director サーバー グループのメンバーが自己署名した SSL 証明書を使用する場合、クラウドの中でより高い信頼性を獲得するために署名された SSL 証明書にアップグレードすることができます。

セル管理ツール (CMT) の証明書のサブコマンドを使用して、vCloud Director サーバ上の SSL 証明書をアップグレードできます。詳細については、[HTTP およびコンソール プロキシ エンドポイントの証明書の置き換え](#)を参照してください。

各 vCloud Director サーバーには Java キーストア ファイル内に 2 つの SSL 証明書 (IP アドレスごとに 1 つ) が必要です。vCloud Director サーバ グループのメンバーごとに CMT ユーティリティを実行する必要があります。署名付きの証明書（信頼された証明書発行機関により署名）または自己署名した証明書を使用できます。署名付き証明書は、最高レベルの信頼を提供します。

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。システム管理者アカウントのパスワードも変更できます。

手順

- 1 Web コンソールのタイトル バーで [環境設定] をクリックします。
- 2 [デフォルト] タブをクリックします。
- 3 ログインしたときに表示するページを選択します。
- 4 ランタイム リースの期限が切れる何日前または何時間前に電子メール通知を受信するかを選択します。
- 5 ストレージ リースの期限が切れる何日前または何時間前に電子メール通知を受信するかを選択します。
- 6 [パスワードを変更] タブをクリックします。
- 7 (オプション) 現在のパスワードを入力し、新しいパスワードを 2 回入力します。
- 8 [OK] をクリックします。

名前と説明に対する長さの制限

vCloud 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 1-2. 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	256
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

vCloud Director へのリソースの追加

2

vCloud 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 vCloud 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。

vCloud 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、vCloud 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 vCloud Director アカウントを使用して、vCloud 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。

vCloud 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、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、[SDDC および SDDC プロキシ](#)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 SDDC 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 SDDC を作成したり、その逆を行ったりすることはできません。vCloud API を使用すると、vCenter Server インスタンスがプロバイダ仮想データセンターと SDDC の両方をバックアップできるように、vCloud Director インストールのシステム設定を変更できます。

この章には、次のトピックが含まれています。

- [vCenter Server および NSX リソースの追加](#)
- [クラウド リソースの追加](#)

vCenter Server および NSX リソースの追加

vCloud 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、vCloud 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 vCloud 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 インスタンスの関連付け

vCenter Server インスタンスを接続して、vCenter Server のリソースが vCloud Director で使用可能になるようにします。vCenter Server を関連付けたら、そのリソース プール、データストア、ネットワークをプロバイダ仮想データセンターに割り当てることができます。

vCloud Director 9.7 以降では、vCenter Server インスタンスを接続した後に、vSphere インフラストラクチャ全体をカプセル化する Software-Defined Data Center (SDDC) を作成することもできます。SDDC には、基盤となる vSphere 環境へのアクセスポイントとして、SDDC プロキシがもう 1 つ含まれています。

注： vCloud Director Web Console では、vCenter Server インスタンスを接続するには、関連付けられている NSX Manager インスタンスと一緒に接続する必要があります。vCenter Server インスタンスのみを接続する方法と、NSX-T Manager インスタンスを登録する方法については、「vCloud Director Service Provider Admin Portal Guide」または「サービス プロバイダ向け vCloud API プログラミング ガイド」を参照してください。

前提条件

VMware NSX®のインスタンスがインストールされ、vCloud Director に合わせて構成されていること。詳細については、『VMware vCloud Director インストールおよび構成ガイド』を参照してください。

手順

1 [vCenter の新規接続] ウィザードの起動

[vCenter の新規接続] ウィザードを起動して、vCenter Server を vCloud Director に関連付けるプロセスを開始します。

2 vCenter Server 接続の提供と情報の表示

vCenter Server を vCloud Director に関連付けるには、vCenter Server の接続情報と表示名を提供する必要があります。

3 NSX Manager への接続

vCenter Server インスタンスと関連付けられた NSX Manager インスタンスを接続するときは、NSX Manager インスタンスのアクセスの詳細を入力する必要があります。クロス仮想データセンター ネットワークを有効にする場合は、分散論理ルーター (DLR) のコントロール仮想マシンについての詳細も指定する必要があります。

4 設定の確認と vCenter Server の接続

新しい vCenter Server を接続する前に、入力した設定を確認します。

[vCenter の新規接続] ウィザードの起動

[vCenter の新規接続] ウィザードを起動して、vCenter Server を vCloud Director に関連付けるプロセスを開始します。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [vCenter] をクリックします。
- 2 [vCenter の新規接続] ボタンをクリックします。
[vCenter の新規接続] ウィザードが起動します。

vCenter Server 接続の提供と情報の表示

vCenter Server を vCloud Director に関連付けるには、vCenter Server の接続情報と表示名を提供する必要があります。

手順

- 1 vCenter Server のホスト名または IP アドレスを入力します。
- 2 vCenter Server が使用するポート番号を選択します。
デフォルトのポート番号は 443 です。
- 3 vCenter Server 管理者のユーザー名およびパスワードを入力します。
ユーザー アカウントには、vCenter の管理者のロールが含まれている必要があります。
- 4 vCenter Server の名前を入力します。
入力した名前は、vCloud Director における vCenter Server の表示名となります。
- 5 (オプション) vCenter Server の説明を入力します。
- 6 [次へ] をクリックして変更内容を保存し、次のページに進みます。

NSX Manager への接続

vCenter Server インスタンスと関連付けられた NSX Manager インスタンスを接続するときは、NSX Manager インスタンスのアクセスの詳細を入力する必要があります。クロス仮想データセンター ネットワークを有効にする場合は、分散論理ルーター (DLR) のコントロール仮想マシンについての詳細も指定する必要があります。

前提条件

この vCenter Server インスタンスでバックアップされる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場合、NSX Manager インスタンスに対して DLR コントロール仮想マシンを展開する必要があります。分散論理ルーターの追加については、『NSX インストール ガイド』を参照してください。

手順

- 1 vCenter Server インスタンスに関連付けられている NSX Manager インスタンスのホスト名または IP アドレスを入力します。

2 ユーザー名とパスワードを入力し、NSX Manager インスタンスに接続します。

デフォルトのユーザー名は **admin**、デフォルトのパスワードは **default** です。これらのデフォルトは、NSX Manager のユーザー インターフェイスで変更できます。

3 この vCenter Server インスタンスでバックアップされる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場合、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 コンポーネントで 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。

オプション	説明
コントロール仮想マシンのリソース プールの vCenter Server バス	<p>クラスターから始まる 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。</p> <p>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。</p>
コントロール仮想マシンのデータストア名	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 。
コントロール仮想マシンの管理インターフェイス名 (HA 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	<p>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。</p> <p>クロス仮想データセンター グループの管理については、『vCloud Director Tenant Portal Guide』を参照してください。</p>

4 [次へ] をクリックして変更内容を保存し、次のページに進みます。

設定の確認と vCenter Server の接続

新しい vCenter Server を接続する前に、入力した設定を確認します。

手順

- 1 vCenter Server および NSX Manager の設定を確認します。
- 2 (オプション) [戻る] をクリックして設定を変更します。
- 3 [完了] をクリックして設定を受け入れ、vCenter Server を接続します。

結果

システムは新しい vCenter Server を接続し、プロバイダ仮想データセンターでできるようにそのリソースを登録します。

次のステップ

vCenter Server で NSX Manager のライセンス キーを割り当てます。

vCenter Server で NSX ライセンス キーを割り当てる

vCenter Server を vCloud Director に接続した後、vSphere Client を使用して、vCloud Director ネットワークをサポートする NSX Manager 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。

vCloud 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 で使用できます。

- 6 [OK] 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、vCloud Director 仮想マシンおよび vApps 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 vCloud 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、[組織へのリソースの割り当て](#)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、[組織仮想データセンター ネットワークの管理](#)を参照してください。

vCloud 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 が導入されています。プロバイダは、SDDC の作成と有効化、テナントへの SDDC 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 SDDC プロキシの作成と有効化を行うことができます。SDDC 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、vCloud OpenAPI を使用する必要があります。<https://code.vmware.com> にある vCloud OpenAPI のスタート ガイドを参照してください。

SDDC および SDDC プロキシの詳細については、[SDDC および SDDC プロキシ](#)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（プロバイダ 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、vCloud Director Web Console 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、vCloud API を使用します。

標準的な vCloud 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 vCloud 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を作成します。

注： この手順は、NSX Data Center for vSphere 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適用されます。NSX-T Data Center で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方法については、『サービス プロバイダ向け vCloud API プログラミング ガイド』を参照してください。

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 VDC と、これがサポートする組織 VDC の関係は、管理上の決定事項であり、サービス オファリングの範囲、vSphere インフラストラクチャの容量および地理的分散などの考慮事項に基づいて判断できます。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 VDC 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 VDC 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 プールで実装できますが、[プロバイダ VDC へのリソース プールの追加](#)で説明されているように、特別に設定された vSphere クラスタに基づいて追加のリソース プールを作成し、仮想データセンターに追加することが必要になる機能もあります。

- IOPS のサポートや、仮想マシンとホストのアフィニティ ルールなどの機能を使用するには、プロバイダ仮想データセンターをバックアップする vCenter Server インスタンスで基盤となるサポートを構成する必要があります。[プロバイダ仮想データセンターでの Storage I/O Control サポートの構成](#)および[仮想マシンとホスト間のアフィニティ ルールの管理](#)を参照してください。

- 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

- 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。1つのリソース プールは、1つのプロバイダ仮想データセンターのみが使用できます。リソース プールを作成するには、vSphere Client を使用します。

vSphere HA を使用するクラスタの一部になっているリソース プールを追加する場合は、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。

- 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 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。『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 トランスポート ゾーン用の VXLAN にバックアップされているネットワーク プールの作成](#)を参照してください。
- vCloud Director Web コンソールにシステム管理者としてログインします。

手順

- 1 [管理および監視] タブの左側のペインで、[プロバイダ VDC] をクリックします。
- 2 [新規のプロバイダ VDC] をクリックします。
- 3 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。

- 4 (オプション) 作成時にプロバイダ仮想データセンターを無効にするには、[有効] を選択解除します。
- 5 [次へ] をクリックします。
- 6 vCenter Server インスタンスと、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 プールを選択して、[次へ] をクリックします。

このページには、vCloud 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。

- 7 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、[追加] をクリックして、[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。

重要: vCloud Director は、暗号化や Storage I/O Control などの host-based データ サービスで仮想マシンのストレージ ポリシーをサポートしません。

8 このプロバイダ VDC の VXLAN ネットワーク プールを設定します。

すべてのプロバイダ VDC には VXLAN 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 トランスポート ゾーンに基づいたカスタム VXLAN プールを使用することもできます。

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 VDC 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。

9 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 VDC でバックアップされる組織 VDC 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も高い仮想ハードウェア 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。

注： プロバイダ VDC 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 Web 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。

10 選択内容を確認し、[完了] をクリックすると、プロバイダ VDC 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 VDC が提供するようにできます。[プロバイダ VDC 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

vCloud 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。外部ネットワークは、システム管理者が作成する必要があります。1 つ以上の vSphere ネットワークでバックアップできます。

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 ネットワークでバックアップできます。複数の vSphere ネットワーク (vCenter Server インスタンスごとに 1 つのネットワーク) でバックアップされる外部ネットワークを作成することもできます。この方法を使用すると、vCloud 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。

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

単一の 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

外部ネットワークが単一の vSphere ネットワークでバックアップされる場合、システム管理者は、すべての組織の外部ネットワーク利用者が使用する IP アドレスの割り当てを管理する必要があります。これを行うには、基盤となる VLAN の IP 範囲を手動で構成し、vSphere ネットワークで重複しない一連の IP アドレスを外部ネットワークの各利用者に提供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が、いくつかの制約があります。

- 外部ネットワークは、システムに登録された各 vCloud 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 (DVSwitch または標準スイッチのいずれかを使用します)。

外部ネットワークの追加

外部ネットワークを追加して、vCloud Director で vSphere ネットワーク リソースを使用できるように登録します。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

vSphere ポート グループは、VLAN トランクの有無に関わらず使用できます。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 [管理および監視] タブをクリックし、左側のペインで [外部ネットワーク] をクリックします。
- 2 [ネットワークを追加] ボタンをクリックします。
- 3 1 つ以上のバックアップ vSphere ネットワークを構成し、[次へ] をクリックします。
 - a 接続先の vSphere ネットワークが所属する vCenter Server インスタンスを選択します。
 - b vSphere ネットワークを選択します。
 - c [追加] をクリックします。
 - d (オプション) 別の vSphere ネットワークを追加するには、手順を繰り返します。

複数の vSphere ネットワークが同じ種類のスイッチ (DVSwitch または標準スイッチ) を経由して接続されている必要があります。各 vCenter Server インスタンスから選択できる vSphere ネットワークは 1 つのみです。

- 4 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、手順を繰り返します。
- 5 ネットワークの名前と、必要に応じて説明を入力して、[次へ]をクリックします。
- 6 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仮想データセンター ネットワークを作成できます。

ネットワーク プール

ネットワーク プールとは、組織仮想データセンター内で vApp ネットワークおよび特定のタイプの組織仮想データセンター 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 リソースによってバックイングされます。vCloud 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。

vCloud 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同じネットワーク 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。

プロバイダ仮想データセンターの作成時に VXLAN ネットワーク プールが作成されます。ほとんどの場合は、必要となるネットワーク プールはこれだけです。

VXLAN ネットワーク プール

すべてのプロバイダ仮想データセンターには VXLAN ネットワーク プールが含まれています。

このプールには、含まれるプロバイダ仮想データセンターの名前から派生する名前が与えられ、作成時に名付けられます。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。プロバイダ仮想データセンター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。

vCloud Director VXLAN ネットワークは、IETF VXLAN 標準に基づいており、次の利点があります。

- 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)

vCloud 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 トランスポート ゾーン用の VXLAN にバックアップされているネットワーク プールの作成

VXLAN にバックアップされているネットワーク プールを追加して、vCloud Director で使用するための NSX トランスポート ゾーンを登録できます。

前提条件

vCloud Director に登録されている任意の vCenter Server で NSX 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 [管理および監視] タブをクリックし、左側のペインで [ネットワーク プール] をクリックします。
- 2 [ネットワーク プールを追加] をクリックします。
- 3 [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。
- 4 vCenter Server と NSX トランスポート ゾーンを選択し、[次へ] をクリックします。
- 5 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。
- 6 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。

VLAN ID によってバックアップされるネットワーク プールの追加

vSphere VLAN ID を vCloud Director で使用できるように登録するために、VLAN によってバックアップされるネットワーク プールを追加することができます。VLAN によってバックアップされるネットワーク プールは、組織仮想データセンター ネットワークに最も適したセキュリティ、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 台の 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 はレイヤー 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、ネットワークで中断が起こる恐れがあります。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [ネットワーク プール] をクリックします。
- 2 [ネットワーク プールを追加] をクリックします。
- 3 [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。

- 4 VLAN ID の範囲を入力し、[追加] をクリックします。
各 VLAN ID に 1 つのネットワークを作成できます。
- 5 vCenter Server と vSphere Distributed Switch を選択し、[次へ] をクリックします。
- 6 ネットワークの名前と、オプションで説明を入力し、[次へ] をクリックします。
- 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

これで、ネットワーク プールによってバックアップされる組織仮想データセンター ネットワークを作成したり、ネットワーク プールを組織仮想データセンターと関連付けて vApp ネットワークを作成したりすることができます。

vSphere 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 プールの追加

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 プールを追加して、vSphere ポート グループを vCloud Director で使用できるように登録できます。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、サードパーティの分散スイッチ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、ネットワークの中断が発生することがあります。

前提条件

1 つ以上のポート グループが vSphere 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 ホストで使用できる必要があり、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 [管理および監視] タブをクリックし、左側のペインで [ネットワーク プール] をクリックします。
- 2 [ネットワーク プールを追加] をクリックします。
- 3 [vSphere 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。
- 4 vCenter Server を選択し、[次へ] をクリックします。
- 5 1 つ以上のポート グループを選択し、[追加] をクリックして [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。
- 6 ネットワークの名前と、必要に応じて説明を入力し、[次へ] をクリックします。
- 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

これで、ネットワーク プールがバックアップする組織仮想データセンター ネットワークを作成したり、ネットワーク プールを組織仮想データセンターと関連付けて vApp ネットワークを作成したりできます。

SDDC および SDDC プロキシの

バージョン 9.7 以降では、vCloud Director はテナントと基盤となる vSphere 環境の間の HTTP プロキシ サーバとして機能することができます。Software-Defined Data Center (SDDC) は、影響を受ける vCenter Server インスタンスのインフラストラクチャをカプセル化します。SDDC プロキシは、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)。

SDDC 機能を使用すると、すべての vSphere 環境の統合管理ポイントとして vCloud Director を使用できます。

- 対応する SDDC 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の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 SDDC にアクセスできますが、VPN は必須ではありません。
- vCloud 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。
- vCloud 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。

SDDC を作成する前に、ターゲット vCenter Server インスタンスを vCloud Director に接続する必要があります。 [vCenter Server インスタンスの関連付け](#)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 SDDC 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 SDDC を作成したり、その逆を行ったりすることはできません。vCloud API を使用すると、vCenter Server インスタンスがプロバイダ仮想データセンターと SDDC の両方をバックアップできるように、vCloud Director インストールのシステム設定を変更できます。

SDDC および SDDC プロキシを作成して、クラウド内の組織に公開することができます。ユーザーは SDDC プロキシを使用して、基盤となる vSphere 環境にアクセスできます。ユーザーは、vCloud Director アカウントを使用して、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。

vCloud Director 内に SDDC があることにより、vCenter Server を公開して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、vCloud Director で SDDC を有効または無効にします。SDDC プロキシを有効または無効にすることもできます。

SDDC および SDDC プロキシの作成と管理

SDDC およびプロキシを作成して管理するには、vCloud OpenAPI を使用する必要があります。<https://code.vmware.com> にある vCloud OpenAPI のスタート ガイドを参照してください。

重要： vCloud Director では、SDDC として使用する各 vCenter Server インスタンスへの直接ネットワーク接続が必要になります。vCenter Server インスタンスが外部 Platform Services Controller インスタンスを使用している場合は、vCloud Director に Platform Services Controller インスタンスへの直接ネットワーク接続が必要です。

プロキシされた SDDC で VMware OVF Tool を使用するには、vCloud Director を各 ESXi ホストに直接接続する必要があります。

- 1 接続された有効な vCenter Server インスタンスによってバックアップされる SDDC を作成します。

vCloud Director は、vCenter Server インスタンスにデフォルト プロキシをもつ SDDC を作成します。vCenter Server インスタンスが外部 Platform Services Controller インスタンスを使用している場合、vCloud Director は Platform Services Controller インスタンス用のプロキシも作成します。

- 2 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。
- 3 SDDC を有効にします。
- 4 1 つ以上の組織に SDDC を公開します。
- 5 ユーザーが vCloud Director Tenant Portal から SDDC および SDDC 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。を参照してください。vCloud Director Service Provider Admin Portal Guide を参照してください。

SDDC を作成して公開した後に、その SDDC プロキシを追加、編集、有効化、無効化、および削除できます。

注： SDDC 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。

組織の作成およびプロビジョニング

3

組織はユーザーのグループにリソースを提供し、ユーザーがこれらのリソースを消費する方法を決定するポリシーを設定します。独自のリソースまたはポリシー、あるいはその両方を必要とするユーザーの各グループについて組織を作成します。

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](#)
- [割り当てモデルについて](#)
- [コンピューティング ポリシーについて](#)
- [組織の作成](#)
- [組織へのリソースの割り当て](#)

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、vCloud Director は vApp を停止します。

ストレージ リースの目的は、使用されていない vApp および vApp テンプレートがストレージ リソースを消費するのを防ぐことです。vApp ストレージ リースは、ユーザーが vApp を停止したときに始まります。ストレージ リースは、実行中の vApp には影響を及ぼしません。vApp テンプレートのストレージ リースは、ユーザーが vApp テンプレートを vApp に追加したとき、vApp テンプレートをワークスペースに追加したとき、vApp テンプレートのダウンロード、コピー、移動を行ったときに始まります。

ストレージ リースの期限が切れると、vCloud Director は設定された組織ポリシーに従って、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。

リース設定の指定の詳細については、[組織のリース、割り当て容量、および制限の設定の構成](#) を参照してください。

ユーザーは電子メール通知を構成して、ランタイム リースまたはストレージ リースの期限が切れる前にメッセージを受信できます。リース期限の環境設定の詳細については、[ユーザー環境設定の設定](#)を参照してください。

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 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、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 VDC コンピューティング 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 VDC コンピューティング 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

	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
仮想マシンの RAM 制限	仮想マシンの VDC コンピューティング 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 VDC コンピューティング 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

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。vCloud 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、長期にわたってワークロードを安定させるために使用します。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 ますが、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。
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。vCloud 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

vCloud 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 VDC コンピューティング 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。

vCloud Director 9.7 で Flex 以外の組織 VDC を作成する場合、Flex 割り当てモデルを使用するように組織 VDC を再設定できます。組織 VDC がバージョン 9.7 より前の vCloud Director バージョンを使用して作成されている場合、Flex 割り当てモデルを使用するように組織データセンターを再設定することはできません。

Flex 組織 VDC を作成する場合、システム管理者は組織 VDC の次の属性を制御します。

- 柔軟性のあるプールの機能を有効または無効にします。
- メモリのオーバーヘッドを含めるか、または除外します。
- 組織 VDC のデフォルトの VDC コンピューティング ポリシーの指定。
- メモリおよび CPU の割り当てと保証
- ネットワークの割り当て容量
- ストレージ プロファイル

vCloud 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。vCloud 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、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組織 VDC のコンピューティング ポリシーによって決まります。組織 VDC の VDC コンピューティング 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 VDC コンピューティング 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、[コンピューティング 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、vCloud 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、「サービス プロバイダ向け vCloud API プログラミング ガイド」を参照してください。

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。

vCloud Director 5.1.2 以降では、システム管理者は、割り当てプール組織 VDC を柔軟性ありとなしのいずれでも構成できます。[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、vCloud 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 vCloud 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、vCloud Director 1.5 の割り当てプール モデルと似た動作になります。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設定するには、vCloud API を使用します。『サービス プロバイダ向け vCloud API プログラミング ガイド』を参照してください。

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、vCloud 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。『サービス プロバイダ向け vCloud API プログラミング ガイド』を参照してください。

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。

コンピューティング ポリシーについて

vCloud Director 9.7 以降では、コンピューティング ポリシーを使用して、リソース割り当てと仮想マシン (VM) の配置を制御できます。コンピューティング ポリシーには、範囲と機能に基づいて、プロバイダ仮想データセンター (VDC) コンピューティング ポリシーと VDC コンピューティング ポリシーの 2 つのタイプがあります。

プロバイダ VDC コンピューティング ポリシー

プロバイダ VDC コンピューティング 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。テナント ユーザーには、プロバイダ VDC コンピューティング ポリシーが表示されません。

プロバイダ VDC コンピューティング ポリシーの範囲は、プロバイダ VDC レベルです。

VDC コンピューティング ポリシー

VDC コンピューティング ポリシーは、仮想マシンのコンピューティング特性を組織 VDC レベルで制御します。テナント ユーザーには、プロバイダ VDC コンピューティング ポリシーが表示されないため、テナントが使用できるように仮想マシンとホスト間のアフィニティ ルールを公開するには、VDC コンピューティング ポリシー内のプロバイダ VDC コンピューティング ポリシーを参照します。

プロバイダ仮想データセンターのコンピューティング ポリシー

vCloud Director システム管理者はプロバイダ仮想データセンター (VDC) コンピューティング ポリシーを使用して、仮想マシン (VM) グループおよび論理仮想マシン グループをテナントに公開することができます。

プロバイダ VDC コンピューティング ポリシーには、次のコレクションが含まれている場合があります。

- 類似の仮想マシンを含む仮想マシン グループ。各仮想マシン グループは、異なるクラスタに属しています。
- さまざまな機能に適した論理仮想マシン グループ。
- 仮想マシン グループと論理仮想マシン グループの両方。

プロバイダ VDC コンピューティング ポリシーおよび論理仮想マシン グループ

システム管理者は、仮想マシン グループと論理仮想マシン グループを使用して、vSphere Distributed Resource Schedule (DRS) 仮想マシンとホストのアフィニティ ルールをテナントに公開できます。DRS 仮想マシン/ホストのアフィニティ ルールは、仮想マシン グループとして vCloud Director でプロバイダ レベルで公開されます。仮想マシンとホストのアフィニティ ルールは、特定のクラスタにバインドされます。柔軟性のあるプロバイダ VDC は複数の vSphere クラスタに分散している場合があるため、論理仮想マシン グループは、論理的に同等な仮想マシン グループにバインドされたクラスタをグループ化することで、複数のクラスタ間で機能する DRS 仮想マシン/ホストのアフィニティ ルールを抽象化します。論理仮想マシン グループを管理するには、vCloud OpenAPI を使用します。vCloud OpenAPI の詳細については、<https://code.vmware.com> の『vCloud OpenAPI スタートガイド』を参照してください。

仮想マシン/ホストのアフィニティ ルールを公開するには、仮想マシン グループと論理仮想マシン グループをプロバイダ VDC コンピューティング ポリシーに追加し、プロバイダ VDC コンピューティング ポリシーと VDC コンピューティング ポリシー間のリファレンスを作成します。

プロバイダ VDC コンピューティング ポリシーのコンテキストでは、論理仮想マシン グループには互いに AND の関係があります。

vCloud Director システム管理者はプロバイダ VDC コンピューティング ポリシーと論理仮想マシン グループを使用して、組織 VDC 内のテナント ユーザーに複数の仮想マシン グループを公開できます。たとえば、2 つのクラスター *cluster1* と *cluster2* を含む環境について考えます。*cluster1* にはホスト *SQL_host_1* が配置されていて、*cluster2* にはホスト *SQL_fast_host* および *Fast_host* が配置されています。

- 1 *cluster1* 内に *SQL_host_group1* と *VM_group1* を作成します。

VM_group1 と *SQL_host_group1* の間に正のアフィニティを作成します。

- 2 *cluster2* 内に 4 つのグループを作成します。

- *SQL_host_group2* および *VM_group2* を作成します。

VM_group2 と *SQL_host_group2* の間に正のアフィニティを作成します。

- *fast_host_group* および *VM_group3* を作成します。

VM_group3 と *fast_host_group* の間に正のアフィニティを作成します。

logical_VM_group1 と *logical_VM_group2* で構成される *PVDC_compute_policy1* を作成します。

logical_VM_group1 は *VM_group1* および *VM_group2* で構成されています。*logical_VM_group2* は *VM_group3* で構成されています。

SQL_and_fast VDC コンピューティング ポリシーを作成して組織 VDC に公開し、*PVDC_compute_policy1* へのリファレンスを追加します。*SQL_and_fast* VDC コンピューティング ポリシーと *PVDC_compute_policy1* の間にリファレンスを作成するときに、論理仮想マシン グループと仮想マシン グループの情報を組織 VDC 内のテナント ユーザーに公開します。その結果、テナントが仮想マシンに *SQL_and_fast* VDC コンピューティング ポリシーを適用すると、配置エンジンは *cluster2* 内の *SQL_fast_host* にその仮想マシンを追加します。

ワークフローは以下のようになります。

- 1 vCenter Server 管理者は、vSphere Client を使用してホスト グループを作成します。

詳細については、VMware vSphere ESXi および vCenter Server ドキュメントのトピック「ホスト DRS グループの作成 (MSCS)」を参照してください。

- 2 vCenter Server 管理者または vCloud Director システム管理者は、仮想マシン グループを作成します。

詳細については、『vCloud Director 管理者ガイド』にあるトピック「仮想マシングループの作成またはアップデート」を参照してください。

- 3 vCloud Director システム管理者は、仮想マシン グループとホスト グループの間に適切なアフィニティ ルールを作成します。

詳細については、『vCloud Director 管理者ガイド』の「仮想マシンとホストのアフィニティ ルールの管理」を参照してください。

- 4 vCloud Director システム管理者は、vCloud OpenAPI を使用して、論理的に同等な仮想マシン グループを論理仮想マシン グループにグループ化します。

- 5 vCloud Director システム管理者は、プロバイダ VDC コンピューティング ポリシーを作成し、vCloud OpenAPI を使用して論理仮想マシン グループを追加します。

- 6 vCloud Director システム管理者は、プロバイダ VDC コンピューティング ポリシーを参照する VDC コンピューティング ポリシーを作成し、vCloud OpenAPI を使用して組織 VDC に VDC コンピューティング ポリシーを公開します。

テナントが組織 VDC 内に仮想マシンを作成して、VDC コンピューティング ポリシーを選択すると、vCloud Director は VDC コンピューティング 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、vCloud Director は該当するホスト上に仮想マシンを作成します。

プロバイダ VDC コンピューティング ポリシーおよび仮想マシン グループ

プロバイダ VDC コンピューティング 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、プロバイダ VDC コンピューティング ポリシー *oracle_license* は仮想マシン グループ *oracle_license1* と *oracle_license2* で構成することができます。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* に属します。

仮想マシンにプロバイダ VDC コンピューティング 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、この仮想マシンにプロバイダ VDC コンピューティング 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。

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、vCloud OpenAPI を使用して、1 つ以上のプロバイダ VDC コンピューティング ポリシーを作成します。
- 2 システム管理者は、vCloud OpenAPI を使用して、1 つ以上の VDC コンピューティング ポリシーを作成します。

VDC コンピューティング ポリシーは、0 または 1 つのプロバイダ VDC コンピューティング ポリシーに関連付けることができます。VDC コンピューティング ポリシーには、名前およびプロバイダ VDC コンピューティング ポリシーごとに一意の名前が付けられます。

- 3 システム管理者は、vCloud OpenAPI を使用して、1 つ以上の組織 VDC に VDC コンピューティング ポリシーを公開します。

テナントには、組織 VDC に公開されている VDC コンピューティング ポリシーのみが表示されます。テナントレベルでは、プロバイダ VDC コンピューティング ポリシーは利用できません。

- 4 テナントは、仮想マシンを作成または更新するときに、vCloud API または vCloud Director テナント ポータルを使用して、組織 VDC コンピューティング ポリシーを仮想マシンに割り当てることができます。

最初は、システムにはプロバイダ VDC コンピューティング ポリシーが含まれておらず、各組織 VDC にはデフォルトのコンピューティング ポリシーのみが含まれます。デフォルトのコンピューティング ポリシーは、プロバイダ VDC コンピューティング ポリシーに関連付けられていません。

プロバイダ VDC コンピューティング ポリシーとグローバルな VDC コンピューティング ポリシーを作成して管理するには、vCloud OpenAPI を使用する必要があります。<https://code.vmware.com> で『vCloud OpenAPI スタートガイド』を参照してください。

仮想データセンターのコンピューティング ポリシー

仮想データセンター (VDC) のコンピューティング ポリシーは、テナント ワークロードの物理コンピューティング リソース割り当てを制御します。特定のワークロード要件に基づいて物理リソースを割り当てるには、テナント ユーザーがデフォルトとカスタムの VDC コンピューティング ポリシーの中から選択します。

VDC コンピューティング ポリシーでは、組織 VDC 内の仮想マシンのコンピューティング リソースの割り当てを定義する属性がグループ化されています。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。

vCloud Director システム管理者は、グローバル レベルでコンピューティング ポリシーを作成および管理し、コンピューティング ポリシーを 1 つ以上の組織 VDC に個別に公開できます。組織 VDC に VDC コンピューティング 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、テナント管理者は使用可能な VDC コンピューティング 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 のテナント管理者とユーザーは、VDC コンピューティング ポリシーの特定の設定を確認できません。

VDC コンピューティング ポリシーを使用すると、クラウド プロバイダは、テナントが組織 VDC 内の仮想マシンに関連付けることができる、名前付きの CPU プロファイルおよびメモリ使用量プロファイルを定義できます。VDC コンピューティング 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率の高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。また、VDC コンピューティング ポリシーで組織 VDC 内の仮想マシンの CPU およびメモリ使用量を制限または制約することもできます。

VDC コンピューティング ポリシーを使用することで、vCloud 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

仮想データセンターのコンピューティング ポリシーの属性

仮想データセンター (VDC) コンピューティング 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、VDC コンピューティング ポリシー名のみです。

次の表に、VDC コンピューティング ポリシー内で定義できるすべての属性を示します。

表 3-1. 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	VDC コンピューティング 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	VDC コンピューティング ポリシーの短い説明を表します。
vCPU Speed	cpuSpeed	仮想マシン (VM) の vCPU 速度を MHz 単位で定義します。

表 3-1. 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
Memory	memory	仮想マシンに設定されるメモリを MB 単位で定義します。 テナントが仮想マシンに VDC コンピューティング 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。
Number of vCPUs	cpuCount	仮想マシンに設定される vCPU の数を定義します。 テナントが仮想マシンに VDC コンピューティング 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数の vCPU を受け取ります。
Cores per Socket	coresPerSocket	仮想マシンのソケットあたりのコア数。 VDC コンピューティング 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。
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 ～ 1 の範囲になります。 メモリ予約保証率の値を 0 にすると、メモリ保証がないことが定義されます。値を 1 にすると、100% のメモリ予約が定義されます。
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 単位で定義します。 値を -1 にすると、CPU 制限が制限なしに定義されます。 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 制限は仮想マシンに割り当てられた CPU と等しくなります。
Memory Limit	memoryLimit	仮想マシンのメモリ制限を MB 単位で定義します。 値を -1 にすると、メモリ制限が制限なしに定義されます。 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、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。
CPU Shares	cpuShares	仮想マシンの CPU シェア数を定義します。 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は、通常のシェア数が仮想マシンに適用されます。
Memory Shares	memoryShares	仮想マシンのメモリ シェア数を定義します。 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。
Provider VDC Compute Policy	pvdccomputePolicy	プロバイダ VDC コンピューティング ポリシーの VDC コンピューティング ポリシーのリファレンスを定義します。

仮想データセンターのコンピューティング ポリシーの使用

vCloud Director は、すべての仮想データセンター (VDC) のデフォルトのコンピューティング ポリシーを生成します。デフォルトの VDC コンピューティング ポリシーには名前と説明のみが含まれていて、残りのすべての VDC コンピューティング ポリシーの属性は空になります。

組織 VDC のデフォルト ポリシーとして、別の VDC コンピューティング ポリシーを定義することもできます。デフォルトの VDC コンピューティング ポリシーは、テナントが組織 VDC 内に作成する仮想マシン (VM) 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 VDC コンピューティング 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 VDC コンピューティング ポリシーを定義します。最大 VDC コンピューティング 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 VDC コンピューティング ポリシーを使用できません。VDC コンピューティング ポリシーを最大 VDC コンピューティング ポリシーとして定義した場合、vCloud 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 VDC コンピューティング 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 VDC コンピューティング ポリシーに依存しなくなります。

組織 VDC に複数の VDC コンピューティング 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。

クラウド プロバイダが使用できる VDC コンピューティング ポリシーの操作を以下に示します。

- VDC コンピューティング ポリシーを作成する。
- 1 つ以上の組織 VDC に VDC コンピューティング ポリシーを公開する。
- 組織 VDC から VDC コンピューティング ポリシーの公開を解除する。
- VDC コンピューティング ポリシーを削除する。

ORG_VDC_MANAGE_COMPUTE_POLICIES 権限を持つユーザーは、VDC コンピューティング ポリシーを作成、更新、および公開できます。VDC コンピューティング ポリシーを作成するには、vCloud API を使用します。

次の表に、テナント ユーザーが使用できる VDC コンピューティング ポリシーの操作を示します。

表 3-2. テナント ユーザー用の VDC コンピューティング ポリシー操作

操作	説明
仮想マシンの作成中に、仮想マシンに VDC コンピューティング ポリシーを割り当てる。	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 VDC コンピューティング 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、VDC コンピューティング 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 VDC コンピューティング 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 VDC コンピューティング 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 VDC ポリシーが仮想マシンに適用されます。テナント ユーザーは、vCloud Director テナント ポータルを使用して仮想マシンを作成するときに、仮想マシンに VDC コンピューティング ポリシーを割り当てることができます。
既存の仮想マシンに VDC コンピューティング ポリシーを割り当てる。	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、仮想マシンと VDC コンピューティング ポリシー間の関連付けを更新できます。その結果、新しい VDC コンピューティング ポリシーで指定されたコンピューティング リソースを使用するように、仮想マシンが再設定されます。テナント ユーザーは、vCloud Director テナント ポータルを使用して、既存の仮想マシンに VDC コンピューティング ポリシーを割り当てることができます。

VDC コンピューティング 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 VDC コンピューティング 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 VDC コンピューティング ポリシーを組織 VDC に公開します。

組織 VDC に VDC コンピューティング ポリシーを公開すると、組織 VDC 内のテナント ユーザーはそのポリシーを使用できるようになります。

- 3 必要に応じて、VDC コンピューティング ポリシーの 1 つを、組織 VDC のデフォルト VDC ポリシーとして定義します。

組織 VDC のデフォルト ポリシーを定義した場合、および仮想マシンの作成中にテナント ユーザーが別のポリシーを指定しなかった場合は、デフォルトのポリシーが仮想マシンに適用されます。

VDC コンピューティング ポリシーを表示して変更するには、vCloud API を使用する必要があります。『サービス プロバイダ向け vCloud API プログラミング ガイド』を参照してください。

組織の作成

組織を作成するには、組織の設定を指定し、組織管理者のユーザー アカウントを作成します。

手順

1 [新しい組織] ウィザードの起動

[新規の組織] ウィザードを起動して、組織を作成するプロセスを開始します。

2 組織の名前の指定

新しい組織にわかりやすい名前を指定し、必要に応じて説明を入力します。

3 組織の LDAP オプションの指定

LDAP サービスを使用して、組織のユーザーおよびグループのディレクトリを提供します。LDAP サービスを指定しない場合は、組織のユーザーごとにユーザー アカウントを作成する必要があります。LDAP オプションを設定できるのは、システム管理者のみです。組織管理者は、LDAP オプションを変更できません。

4 組織へのローカル ユーザーの追加

LDAP および SAML サービスを使用できない場合でもユーザーがログインできるように、すべての組織は少なくとも1つのローカルの組織管理者アカウントを持っている必要があります。

5 組織のカatalog共有、公開、およびサブスクリプション ポリシーの設定

Catalogは、組織ユーザーが仮想マシンでの vApp の作成とアプリケーションのインストールに使用できる、vApp テンプレートとメディアのCatalogを提供します。

6 電子メール環境設定の構成

vCloud Director には、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 サーバーが必要です。組織は、システムのメール設定を使用することも、独自のメール設定を使用することもできます。

7 組織のリース、割り当て容量、および制限の設定の構成

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消費する能力が制限されます。これらの設定により、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。

8 設定の確認と組織の作成

組織を作成する前に、入力した設定を確認します。

[新しい組織] ウィザードの起動

[新規の組織] ウィザードを起動して、組織を作成するプロセスを開始します。

手順

1 [管理および監視] タブをクリックし、左側のペインで [組織] をクリックします。

2 [新規の組織] ボタンをクリックします。

[新規の組織] ウィザードが起動します。

組織の名前の指定

新しい組織にわかりやすい名前を指定し、必要に応じて説明を入力します。

手順

- 1 組織名を入力します。

この名前は、組織のメンバーが組織へのログインで使用する URL に含まれる一意の識別子となります。

- 2 組織の表示名を入力します。

この名前は、組織のメンバーが一意の URL を使用して vCloud Director にログインするときに、ブラウザのヘッダーに表示されます。管理者または組織管理者は、後でこの名前を変更できます。

- 3 (オプション) 組織の説明を入力します。

- 4 [次へ] をクリックします。

組織の LDAP オプションの指定

LDAP サービスを使用して、組織のユーザーおよびグループのディレクトリを提供します。LDAP サービスを指定しない場合は、組織のユーザーごとにユーザー アカウントを作成する必要があります。LDAP オプションを設定できるのは、システム管理者のみです。組織管理者は、LDAP オプションを変更できません。

カスタム LDAP 設定の入力に関する詳細については、[システムの LDAP の設定](#) を参照してください。

手順

- 1 組織ユーザーのソースを選択します。

オプション	説明
LDAP を使用しない	組織管理者が組織内のユーザーごとにローカル ユーザー アカウントを作成します。このオプションを選択した場合、グループを作成できません。
VCD システム LDAP サービス	vCloud Director システムの LDAP サービスを、組織のユーザーおよびグループのソースとして使用します。
カスタム LDAP サービス	組織を、組織独自の非公開 LDAP サービスに接続します。

- 2 選択した項目で必要とされる追加情報をすべて提供します。

オプション	操作
LDAP を使用しない	[次へ] をクリックします。
VCD システム LDAP サービス	<p>(省略可能) 組織にインポートできるユーザーを制限するために使用する組織単位 (OU) の識別名を入力し、[次へ] をクリックします。何も入力しない場合は、システム LDAP サービス内のすべてのユーザーを組織にインポートできます。</p> <p>注： OU を指定しても、インポートできる LDAP グループは制限されません。システム LDAP ルートから任意の LDAP グループをインポートできます。ただし、OU およびインポートされたグループの両方に属するユーザーのみが組織にログインできます。</p>
カスタム LDAP サービス	[次へ] をクリックし、組織のカスタム LDAP 設定を入力します。

組織へのローカル ユーザーの追加

LDAP および SAML サービスを使用できない場合でもユーザーがログインできるように、すべての組織は少なくとも 1 つのローカルの組織管理者アカウントを持っている必要があります。

手順

- 1 [追加] をクリックします。
- 2 ユーザー名とパスワードを入力します。
- 3 ユーザーにロールを割り当てます。
- 4 (オプション) ユーザーの連絡先情報を入力します。
- 5 [制限なし] を選択するか、または格納済みで実行中の仮想マシンのユーザー割り当て容量を入力し、[OK] をクリックします。

これらの割り当て容量によって、ユーザーが組織内のストレージ リソースおよびコンピューティング リソースを消費する能力が制限されます。ここで組織レベルに設定された割り当て容量とは異なる割り当て容量を設定すると、この割り当て容量が優先されます。

- 6 [次へ] をクリックします。

組織のカatalog共有、公開、およびサブスクリプション ポリシーの設定

カタログは、組織ユーザーが仮想マシンでの vApp の作成とアプリケーションのインストールに使用できる、vApp テンプレートとメディアのカタログを提供します。

カタログは、vCloud Director の異なるインスタンス内の組織間、vCloud Director の同じインスタンス内の組織間で共有できるほか、アクセスをホスト組織内に限ることもできます。

手順

- 1 組織のカタログ ポリシーを設定します。

オプション	説明
[他の組織へのカタログの共有を許可する]	組織管理者がこの組織のカタログを、vCloud 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タログを共有することはできます。
[外部組織に使用されるカタログ フィードの作成を許可する]	組織管理者がこの組織のカタログを、vCloud Director のこのインスタンスの外部の組織と共有することを許可します。
[外部カタログ フィードのサブスクリプションを許可]	組織管理者が、この組織が vCloud Director のこのインスタンスの外部からのカタログ フィードをサブスクライブすることを許可します。

- 2 [次へ] をクリックします。

電子メール環境設定の構成

vCloud Director には、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 サーバーが必要です。組織は、システムのメール設定を使用することも、独自のメール設定を使用することもできます。

手順

- 1 SMTP サーバーのオプションを選択します。

オプション	説明
システム デフォルトの SMTP サーバーを使用	この組織はシステムの SMTP サーバーを使用します。
組織の SMTP サーバーを設定	この組織は独自の SMTP サーバーを使用します。SMTP サーバーの DNS ホスト名または IP アドレスとポート番号を入力します。(省略可能) [認証が必要] チェック ボックスをオンにし、ユーザー名とパスワードを入力します。

- 2 通知設定のオプションを選択します。

オプション	説明
システム デフォルトの通知設定を使用	この組織はシステムの通知設定を使用します。
組織の通知設定を設定	この組織は独自の通知設定を使用します。組織の電子メールの送信者として表示される電子メール アドレスと件名のプリフィックスとして使用するテキストを入力し、受信者を選択します。

- 3 (オプション) 宛先のメール アドレスを入力し、[電子メール設定をテスト] をクリックして、すべての SMTP サーバー設定が正常に構成されていることを確認します。
- 4 [次へ] をクリックします。

組織のリース、割り当て容量、および制限の設定の構成

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消費する能力が制限されます。これらの設定により、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。

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 vApp および vApp テンプレートのリース オプションを選択します。

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 リソースに対する制御のレベルを提供します。また、ストレージ リースの有効期限が切れた場合の vApp と vApp テンプレートの動作も指定できます。

- 2 実行中および格納された仮想マシンの割り当て容量を選択します。

割り当て容量により、組織内の各ユーザーが組織の仮想データセンターで格納およびパワーオンすることができる仮想マシンの数が決まります。指定する割り当て容量は、組織に追加されるすべての新規ユーザーにとってのデフォルト設定となります。ユーザー レベルで設定された割り当て容量は、組織レベルで設定された割り当て容量よりも優先されます。

- 3 リソースを大量に消費する操作の制限値を選択します。

コピーや移動などの特定の vCloud Director 操作では、他の操作より多くのリソースが消費されます。制限値を設定して、リソースを大量に消費する操作が組織内のすべてのユーザーに影響を与えることを防止し、サービス拒否攻撃を防御することもできます。

- 4 仮想マシンごとに、VMware Remote Console の同時接続数を選択します。

パフォーマンスやセキュリティ上の理由により、同時接続数を制限できます。

注： この設定は、Virtual Network Computing (VNC) 接続や Remote Desktop Protocol (RDP) 接続には影響しません。

- 5 (オプション) [アカウント ロックアウトの有効化] チェック ボックスをオンにし、ユーザー 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たら、ロックアウト間隔を選択します。

- 6 [次へ] をクリックします。

設定の確認と組織の作成

組織を作成する前に、入力した設定を確認します。

手順

- 1 組織の設定を確認します。
- 2 (オプション) [戻る] をクリックして設定を変更します。
- 3 [完了] をクリックして設定を受け入れ、組織を作成します。

次のステップ

リソースを組織に割り当てます。

組織へのリソースの割り当て

プロバイダ仮想データセンターからパーティション化される組織仮想データセンターを作成することで、組織にリソースを割り当てます。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。

注： Flex 組織仮想データセンターを作成するには、vCloud Director Service Provider Admin Portal または vCloud API を使用します。『vCloud Director Service Provider Admin Portal Guide』または『サービス プロバイダ向け vCloud API プログラミング ガイド』を参照してください。

前提条件

リソースを組織に割り当てるには、事前にプロバイダ仮想データセンターを持っている必要があります。

手順

- 1 [リソースの割り当て] ウィザードの起動

[リソースの割り当て] ウィザードを起動して、組織の組織仮想データセンターを作成するプロセスを開始します。

2 プロバイダ仮想データセンターの選択

組織仮想データセンターは、使用するコンピューティング リソースとストレージ リソースをプロバイダ仮想データセンターから入手します。組織仮想データセンターは、これらのリソースを、組織内の vApp と仮想マシンに提供します。

3 割り当てモデルの選択

割り当てモデルにより、管理者が割り当てるプロバイダ仮想データセンターのコンピューティング リソースとメモリ リソースが組織仮想データセンターにコミットされる方法とタイミングが決定されます。

4 割り当てモデルの構成

割り当てモデルを構成して、組織仮想データセンターに割り当てるプロバイダ仮想データセンター リソースの量を指定します。

5 ストレージを割り当て

組織仮想データセンターでは、vApp および vApp テンプレートのためのストレージ領域が必要です。プロバイダ仮想データセンターのデータストアで使用可能な領域から、ストレージを割り当てることができます。

6 ネットワーク プールおよびサービス

ネットワーク プールは、vApp ネットワークと内部の組織仮想データセンター 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。

7 Edge ゲートウェイの構成

1 つ以上の外部ネットワークに接続できるように、Edge ゲートウェイを構成します。

8 外部ネットワークの構成

Edge ゲートウェイが接続できる外部ネットワークを選択します。

9 新規 Edge ゲートウェイ上の IP 設定の構成

新規 Edge ゲートウェイ上の外部ネットワークの IP 設定を構成します。

10 新規 Edge ゲートウェイ上の IP プールの細分割り当て

Edge ゲートウェイ上の外部ネットワークが提供する IP プールを複数の固定 IP プールに細分割り当てします。

11 新規 Edge ゲートウェイ上のレート制限の構成

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します。

12 組織仮想データセンター ネットワークの作成

新しい Edge ゲートウェイに接続する組織仮想データセンター ネットワークを作成できます。

13 組織仮想データセンターの名前の指定

新しい組織仮想データセンターで使用する vSphere 機能を示すため、わかりやすい名前を指定し、必要に応じて説明も入力できます。

14 設定の確認と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を作成する前に、入力した設定を確認します。

次のステップ

ネットワークを組織に追加します。

[リソースの割り当て] ウィザードの起動

[リソースの割り当て] ウィザードを起動して、組織の組織仮想データセンターを作成するプロセスを開始します。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織] をクリックします。
- 2 組織名を右クリックし、メニューから [リソースの割り当て] を選択します。

[リソースの割り当て] ウィザードが起動します。

プロバイダ仮想データセンターの選択

組織仮想データセンターは、使用するコンピューティング リソースとストレージ リソースをプロバイダ仮想データセンターから入手します。組織仮想データセンターは、これらのリソースを、組織内の vApp と仮想マシンに提供します。

手順

- 1 プロバイダ仮想データセンターを選択します。

プロバイダ仮想データセンター リストには使用可能なリソースに関する情報が表示され、ネットワーク リストには選択したプロバイダ仮想データセンターで使用可能なネットワークに関する情報が表示されます。

- 2 [次へ] をクリックします。

割り当てモデルの選択

割り当てモデルにより、管理者が割り当てるプロバイダ仮想データセンターのコンピューティング リソースとメモリ リソースが組織仮想データセンターにコミットされる方法とタイミングが決定されます。

前提条件

どの割り当てモデルが環境に適しているかについて理解していることを確認します。[割り当てモデルについて](#)を参照してください。

手順

- 1 割り当てモデルを選択します。

オプション	説明
割り当てプール	プロバイダ仮想データセンターから割り当てるリソースの割合は、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。
従量課金制	リソースは、組織仮想データセンターでユーザーが vApp を作成するときのみコミットされます。
予約プール	割り当てるすべてのリソースは、組織仮想データセンターに直ちにコミットされます。

配置エンジンおよび仮想マシンの共有、レートおよび制限の詳細については、『vCloud Director ユーザー ガイド』を参照してください。

2 [次へ] をクリックします。

割り当てモデルの構成

割り当てモデルを構成して、組織仮想データセンターに割り当てるプロバイダ仮想データセンター リソースの量を指定します。

手順

1 割り当てモデルのオプションを選択します。

モデルによっては、一部のオプションが含まれていないものもあります。

オプション	アクション
CPU の割り当て	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 の最大使用量を GHz 単位で入力します。このオプションは、割り当てプールと予約プールの割り当てモデルの場合にのみ指定できます。予約プール モデルに含まれる [CPU リソースを予約値を超えて拡張できるようにします。] チェック ボックスでは、仮想データセンターが CPU リソースを上限なしで提供できるかどうかを選択できます。
確保された CPU 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保証する CPU リソースの割合を入力します。100% 未満を保証すると、リソースをオーバーコミットできます。このオプションは、割り当てプールと従量課金制の割り当てモデルの場合にのみ指定できます。割り当てプールのデフォルト値は 50% で、従量課金制のデフォルトは 20% です。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。
vCPU 速度	vCPU 速度を GHz 単位で入力します。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。このオプションは、割り当てプールと従量課金制の割り当てモデルの場合にのみ指定できます。
メモリの割り当て	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使用量を GB 単位で入力します。このオプションは、割り当てプールと予約プールの割り当てモデルの場合にのみ指定できます。
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保証するメモリ リソースの割合を入力します。100% 未満を保証すると、リソースをオーバーコミットできます。このオプションは、割り当てプールと従量課金制の割り当てモデルの場合にのみ指定できます。割り当てプールのデフォルトは 50% で、従量課金制のデフォルトは 20% です。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。
最大仮想マシン数	組織仮想データセンターで作成可能な仮想マシンの最大数を入力します。

2 [次へ] をクリックします。

例：割り当てモデルの構成

組織仮想データセンターを作成すると、vCloud Director は、指定される割り当てモデルの設定に基づいて vSphere リソース プールを作成します。

表 3-3. 単ークラスタの割り当てプール機能が有効になっている場合の割り当てプール設定によるリソース プール設定への影響

割り当てプール設定	割り当てプール値	リソース プール設定	リソース プール値
CPU の割り当て	25 GHz	CPU 制限	25 GHz
CPU % の保証	10%	CPU の予約	2.5GHz
メモリの割り当て	50 GB	メモリの制限	50 GB
メモリ % の保証	20%	メモリの予約	10GB

表 3-4. 単ークラスタの割り当てプール機能が無効になっている場合の割り当てプール設定によるリソース プール設定への影響

割り当てプール設定	割り当てプール値	リソース プール設定	サブリソース プール値	すべてのサブリソース プールでこの組織仮想データセンターにコミットされた値
CPU の割り当て	25 GHz	CPU 制限	vCPU の合計数に、関連付けられているすべての仮想マシンの vCPU 周波数を掛けた値	該当なし
CPU % の保証	10%	CPU の予約	関連付けられているすべての仮想マシンの vCPU の数に、vCPU 周波数、CPU の割合保証を掛けた合計値	2.5GHz
メモリの割り当て	50 GB	メモリの制限	関連付けられているすべての仮想マシンの構成済みのメモリサイズの合計	該当なし
メモリ % の保証	20%	メモリの予約	構成済みのメモリ サイズの合計に、関連付けられているすべての仮想マシンのメモリの割合の保証を掛けた値	10GB

表 3-5. 従量課金制の設定によるリソース プール設定への影響

従量課金制の設定	従量課金制の値	リソース プール設定	リソース プール値
CPU % の保証	10%	CPU の予約、CPU の制限	0.00GHz、無制限
メモリ % の保証	100%	メモリの予約、メモリの制限	0.00 GB、無制限

従量課金制の組織仮想データセンターをサポートするために作成されるリソース プールには、予約または制限がありません。従量課金制の設定は、オーバーコミットにのみ影響を与えます。100% 保証とは、オーバーコミットの可能性がないことを意味します。割合が低いほど、オーバーコミットの可能性が高くなります。

表 3-6. 予約プール設定によるリソース プール設定への影響

予約プール設定	予約プール値	リソース プール設定	リソース プール値
CPU の割り当て	25 GHz	CPU の予約、CPU の制限	25GHz、25GHz
メモリの割り当て	50 GB	メモリの予約、メモリの制限	50 GB、50 GB

ストレージを割り当て

組織仮想データセンターでは、vApp および vApp テンプレートのためのストレージ領域が必要です。プロバイダ仮想データセンターのデータストアで使用可能な領域から、ストレージを割り当てることができます。

シン プロビジョニングはストレージの過剰な割り当てを回避するために役立ちます。シン プロビジョニングされた仮想ディスクを使用する仮想マシンでは、ESXi により、ディスクの最大容量に基づいてすべてのストレージが予約されますが、初期操作にディスクが必要とするストレージのみがコミットされます。ディスクで必要になると、追加のストレージがコミットされます。

高速プロビジョニングでは、できる限りリンク クローンを使用するため、時間が節約されます。[仮想マシンの高速プロビジョニング](#)を参照してください。

手順

- 1 割り当てるストレージ ポリシーを選択して、[追加] をクリックします。
- 2 割り当てるストレージの量を入力します。
- 3 ドロップダウン メニューから [デフォルトのインスタンス化ポリシー] を選択します。
これは、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使用される、デフォルトのストレージ ポリシーです。
- 4 (オプション) [シン プロビジョニングを有効化] チェック ボックスをオンにして、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化します。
- 5 (オプション) [高速プロビジョニングを有効化] チェック ボックスをオフにして、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化します。
- 6 [次へ] をクリックします。

ネットワーク プールおよびサービス

ネットワーク プールは、vApp ネットワークと内部の組織仮想データセンター 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。

手順

- 1 ネットワーク プールを選択するか、[なし] を選択します。
[なし] を選択する場合は、後でネットワーク プールを追加できます。
- 2 (オプション) 選択したネットワーク プールを VXLAN プールに変換します。
選択したネットワーク プールが VCDNI プールの場合は、[VXLAN に移行] ボタンが表示されます。VMware ナレッジベースの記事 <https://kb.vmware.com/kb/2148381> を参照してください。
- 3 組織がネットワーク プールからプロビジョニングできるネットワークの最大数を入力します。
- 4 (オプション) 使用可能なそれぞれのサードパーティまたは Edge ゲートウェイ サービスに [有効化] を選択し、有効化します。
- 5 [次へ] をクリックします。

Edge ゲートウェイの構成

1 つ以上の外部ネットワークに接続できるように、Edge ゲートウェイを構成します。

手順

- 1 システム リソースに基づいて Edge ゲートウェイ構成を選択します。

オプション	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 [特大] 構成では、同じセキュリティ機能が提供されます。
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適しています。
超特大	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。

Edge ゲートウェイを導入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』の「NSX のシステム要件」を参照してください。

- 2 (オプション) 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するには、[高可用性を有効にする] を選択します。
- 3 (オプション) [分散ルーティングの有効化] を選択し、分散論理ルーティングを提供するように詳細ゲートウェイを設定します。

このオプションは、[詳細ゲートウェイとして作成] を選択する場合にのみ使用できます。分散ルーティングを有効にすると、はるかに多くの組織 VDC ネットワークをゲートウェイに作成できます。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。

- 4 (オプション) [FIPS モードの有効化] を選択して、Edge Gateway で NSX の FIPS モードを使用できるように設定します。

このオプションは、システム管理者が Edge Gateway での FIPS モードの有効化を許可している場合にのみ使用できます。NSX 6.3 以降が必要です。[全般システム設定](#)を参照してください。FIPS モードの詳細については、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。

- 5 (オプション) [IP 設定の構成] を選択し、外部インターフェイスの IP アドレスを手動で構成します。
- 6 (オプション) [IP プールの細分割り当て] を選択し、使用するゲートウェイ サービスの一連の IP アドレスを割り当てます。
- 7 (オプション) [レート制限の構成] を選択し、外部接続された各インターフェイスの着信および発信のレート制限を選択します。
- 8 [次へ] をクリックします。

外部ネットワークの構成

Edge ゲートウェイが接続できる外部ネットワークを選択します。

このページは、[新規の Edge ゲートウェイの作成] を選択した場合にのみ表示されます。

手順

- 1 リストから外部ネットワークを選択して [追加] をクリックします。
複数のネットワークを選択するには、Ctrl キーを押しながら操作します。
- 2 デフォルト ゲートウェイにするネットワークを選択します。
- 3 (オプション) [DNS リレーのデフォルトのゲートウェイを使用します]を選択します。
- 4 [次へ] をクリックします。

新規 Edge ゲートウェイ上の IP 設定の構成

新規 Edge ゲートウェイ上の外部ネットワークの IP 設定を構成します。

このページは、ゲートウェイの構成中に [IP 設定の構成] を選択した場合にのみ表示されます。

手順

- 1 [IP 設定の構成] ページで、[IP 割り当ての変更] をクリックします。
- 2 IP アドレスを指定するそれぞれの外部ネットワークについて、ドロップダウン メニューから [手動] を選択します。
- 3 [手動] に設定するそれぞれの外部ネットワークの IP アドレスを入力し、[次へ] をクリックします。

新規 Edge ゲートウェイ上の IP プールの細分割り当て

Edge ゲートウェイ上の外部ネットワークが提供する IP プールを複数の固定 IP プールに細分割り当てします。

このページは、ゲートウェイの構成中に [IP プールの細分割り当て] を選択した場合にのみ表示されます。

前提条件

Edge Gateway に割り当てる IP アドレスが vCloud Director の外部で使用されていないことを確認します。

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。vCloud 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 vCloud 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 外部ネットワークと細分割り当てする IP プールを選択します。
- 2 IP プールの範囲内の IP アドレスまたは IP アドレスの範囲を入力し、[追加] をクリックします。
この手順を繰り返し、細分割り当てされた複数の IP プールを追加します。
- 3 (オプション) 細分割り当てされた IP プールを選択し、[変更] をクリックして、細分割り当てされた IP プールの IP アドレスの範囲を変更します。
- 4 (オプション) 細分割り当てされた IP プールを選択し、[削除] をクリックして、細分割り当てされた IP プールを削除します。

- 5 [次へ] をクリックします。

新規 Edge ゲートウェイ上のレート制限の構成

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します。

このページは、ゲートウェイの構成中に [レート制限の構成] を選択した場合にのみ表示されます。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アップ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 レート制限を有効化するそれぞれの外部ネットワークに対して [有効化] をクリックします。
- 2 有効化されたそれぞれの外部ネットワークに対し、[着信のレート制限] を 1 秒あたりのギガビットで入力します。
- 3 有効化されたそれぞれの外部ネットワークに対し、[発信のレート制限] を 1 秒あたりのギガビットで入力し、[次へ] をクリックします。

組織仮想データセンター ネットワークの作成

新しい Edge ゲートウェイに接続する組織仮想データセンター ネットワークを作成できます。

このページは、[新規の Edge ゲートウェイの作成] を選択した場合にのみ表示されます。

手順

- 1 (オプション) [この新規 Edge ゲートウェイに接続されたこの仮想データセンターのネットワークを作成する] を選択します。
- 2 新しい組織仮想データセンター ネットワークの名前を入力し、必要に応じて説明も入力します。
- 3 (オプション) [このネットワークを組織内の他の VDC と共有する] を選択します。
- 4 組織仮想データセンター ネットワークのゲートウェイ アドレスとネットワーク マスクを入力します。
- 5 (オプション) [ゲートウェイ DNS を使用] を選択し、ゲートウェイの DNS リレーを使用します。
このオプションは、ゲートウェイで DNS リレーが有効化されている場合にのみ使用できます。
- 6 (オプション) DNS を使用する DNS 設定を入力します。
- 7 IP アドレスまたは IP アドレスの範囲を入力し、[追加] をクリックして固定 IP プールを作成します。
この手順を繰り返し、複数の固定 IP プールを追加します。
- 8 [次へ] をクリックします。

組織仮想データセンターの名前の指定

新しい組織仮想データセンターで利用できる vSphere 機能を示すため、わかりやすい名前を指定し、必要に応じて説明も入力できます。

手順

- 1 名前と、必要に応じて説明を入力します。

名前と説明の各フィールドには、特殊文字を使用しないでください。長さの制限については、[名前と説明に対する長さの制限](#)を参照してください。

- 2 (オプション) [有効] をオフにします。

組織仮想データセンターを無効にすると、新規 vApp はその仮想データセンターにデプロイされなくなります。実行中の vApp は継続して実行されますが、その他の vApp は開始できません。

- 3 [次へ] をクリックします。

設定の確認と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を作成する前に、入力した設定を確認します。

手順

- 1 組織仮想データセンターの設定を確認します。

- 2 (オプション) [戻る] をクリックして設定を変更します。

- 3 (オプション) この仮想データセンターの組織仮想データセンター ネットワークをすぐに作成するには、[このウィザードを終了後、この組織にネットワークを追加します] を選択します。

- 4 [完了] をクリックして設定を受け入れ、組織仮想データセンターを作成します。

組織仮想データセンターを作成すると、vCloud Director は、CPU とメモリのリソースを提供するために vSphere でリソース プールを作成します。

カタログの操作

4

新規作成された組織には、カタログがありません。組織管理者またはカタログ作成者がカタログを作成すると、組織のメンバーはそのカタログをアップロード先またはサブスクリプションベースのコンテンツのソースとして使用できます。

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。組織のメンバーは、カタログ項目を構成要素として使用して、独自の vApp を作成します。

カタログ コンテンツ

カタログには、vApp テンプレートとメディア イメージへの参照が含まれています。カタログは次のように構成できます。

- カatalog所有者がプライベートに使用するローカル コンテンツ、またはクラウド内の他のユーザー、グループ、および組織と共有するローカル コンテンツのリポジトリとして。
- 他のクラウドから購読できる公開済みコンテンツのソースとして。
- 他のクラウドで公開されたコンテンツのローカル リポジトリ、または VMware Content Subscription Protocol (VCSP) エンドポイントをホストする Web サイトとして。

カタログの共有設定の管理は、組織管理者またはカタログ所有者が行います。組織内のカタログの公開オプションおよびサブスクリプション オプションの管理は、カタログを公開する権限を持つ組織内の組織管理者が行います。システム管理者は、カタログと外部ソースとのバックグラウンド同期を有効にし、バックグラウンド同期スケジュールを設定して、このアクティビティによるネットワーク バンド幅の使用量を制御できます。

カタログへのアクセス

カタログは、初期状態で所有者にフル コントロール権を付与し、他のユーザーにはアクセス権を付与しません。カタログの所有者、組織管理者、またはカタログ作成者は、組織の他のメンバーにカタログへのアクセス権を個別または一括で付与できます。組織管理者とシステム管理者は、クラウド内の他の組織とカタログを共有できます。

この章には、次のトピックが含まれています。

- [新規カタログの追加](#)
- [カタログへのアクセス](#)
- [カタログの共有](#)
- [外部組織へのカタログの公開](#)

- [カタログの所有者の変更](#)
- [カタログの削除](#)
- [カタログのプロパティの変更](#)
- [外部カタログ フィードのサブスクリプション](#)

新規カタログの追加

vApp テンプレートとメディア ファイルをグループ化するには、カタログを作成します。

前提条件

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

手順

- 1 [カタログ] をクリックし、左側のペインで [マイ組織のカタログ] をクリックします。
- 2 [カタログ] タブで、[カタログを追加] をクリックします。
- 3 カatalog名と、オプションで説明を入力し、[次へ] をクリックします。
- 4 このカタログ内の vApp テンプレートおよび ISO に使用するストレージのタイプを選択し、[次へ] をクリックします。

オプション	説明
組織内で使用できるすべてのストレージを使用する	このカタログは、組織内で使用できるすべてのストレージを使用します。
特定のストレージ ポリシーに事前にプロビジョニングされたストレージ	このカタログの vApp テンプレートおよび ISO に使用する仮想データセンター ストレージ ポリシーを選択し、[追加] をクリックします。選択したストレージ ポリシーにより、vApp テンプレートのサイズがカタログ ストレージの割り当て容量を考慮したものとなります。

5 [メンバーを追加] をクリックします。

注： このオプションは、組織の設定によって無効になっていることがあります。

a 組織内で、このカタログにアクセスできるユーザーおよびグループを選択します。

- [組織の全員] を選択すると、組織内のすべてのユーザーおよびグループにカタログへのアクセスが許可されます。
- [特定のユーザーとグループ] を選択し、特定のユーザーまたはグループにカタログへのアクセスを許可し、[追加] をクリックします。

b このカタログへアクセスできるユーザーのアクセス レベルをドロップダウン メニューから選択し、[OK] をクリックします。

- [読み取り専用] を選択すると、カタログの vApp テンプレートおよび ISO への読み取りアクセス権が与えられます。
- [読み取り/書き込み] を選択すると、カタログの vApp テンプレートおよび ISO への読み取りアクセス権が与えられるほか、ユーザーが vApp テンプレートおよび ISO をカタログに追加できるようになります。
- [完全コントロール] を選択すると、カタログのコンテンツおよび設定への完全なアクセス権が与えられます。

6 [組織の追加] をクリックします。

注： このオプションは、組織の設定によって無効になっていることがあります。

a この vCloud Director インストール環境上で、このカタログにアクセスできる組織を選択します。

- [すべての組織] を選択すると、vCloud Director インストール環境内のすべての組織にカタログへのアクセス権が与えられます。
- [特定の組織] を選択し、特定の組織にカタログへのアクセス権を与え、[追加] をクリックします。

b このカタログへアクセスできるユーザーのアクセス レベルをドロップダウン メニューから選択し、[OK] をクリックします。

- [読み取り専用] を選択すると、カタログの vApp テンプレートおよび ISO への読み取りアクセス権が与えられます。
- [読み取り/書き込み] を選択すると、カタログの vApp テンプレートおよび ISO への読み取りアクセス権が与えられるほか、組織が vApp テンプレートおよび ISO をカタログに追加できるようになります。
- [完全コントロール] を選択すると、カタログのコンテンツおよび設定への完全なアクセス権が与えられます。

7 [次へ] をクリックします。

8 (オプション) [有効] を選択し、クリックして、この vCloud Director インストール環境外のカatalogが使用するCatalog フィードの作成を許可し、Catalog フィードのパスワードを入力します。

- 9 (オプション) [同期を最適化するためにカタログの早期エクスポートを有効化します] を選択します。

このオプションを選択する前に、転送サーバの場所にエクスポートしたカタログ用に利用可能なストレージがあることを確認してください。

- 10 (オプション) [ID 情報の保存] を選択して、ダウンロードされた OVF パッケージに BIOS および UUID 情報を含めます。

このオプションを有効にすると、OVF パッケージの移植性が制限されます。

- 11 カタログ設定を確認し、[完了] をクリックします。

結果

マイ組織のカタログに新しいカタログが表示されます。このページに表示されるカタログのステータスは、カタログのテンプレートおよび vApp のステータスを反映したものではありません。

カタログへのアクセス

組織内のカタログを共有しているユーザーは、そのカタログにアクセスできます。公開カタログには、組織管理者が組織内でのアクセスを許可している場合にアクセスできます。

前提条件

カタログへのアクセスは、各自のロールの権限ではなく、カタログの共有によって制御されます。

手順

- 1 [カタログ] をクリックします。
- 2 左側のペインで、カタログのオプションを 1 つクリックします。
- 3 右側のペインでカタログを選択し、右クリックして [開く] を選択します。

カタログの共有

カタログは、組織のすべてのメンバーまたは特定のメンバーと共有できます。外部組織に公開することもできます。

前提条件

- この操作には、事前定義のカタログ作成者ロールに含まれている権限、またはそれに相当する権限が必要です。
- カatalogの所有者である必要があります。

手順

- 1 [カタログ] をクリックし、左側のペインで [マイ組織のカタログ] を選択します。
- 2 [カタログ] タブでカタログ名を右クリックし、[設定の発行] を選択します。
- 3 [共有] タブで [メンバーを追加] をクリックします。

- 4 組織内で、このカタログにアクセスできるユーザーおよびグループを選択します。

オプション	説明
組織の全員	組織内のすべてのユーザーおよびグループがこのカタログにアクセスできます。
特定のユーザーとグループ	カタログへのアクセスを認めるユーザーまたはグループを選択し、[追加] をクリックします。

- 5 このカタログへアクセスできるユーザーのアクセス レベルをドロップダウン メニューから選択します。

オプション	説明
読み取り専用	このカタログへアクセスできるユーザーは、カタログの vApp テンプレートおよび ISO への読み取りアクセス権を有します。
読み取り/書き込み	このカタログへアクセスできるユーザーは、カタログの vApp テンプレートおよび ISO への読み取りアクセス権を有し、vApp テンプレートおよび ISO をカタログに追加することができます。
完全コントロール	このカタログへアクセスできるユーザーは、カタログのコンテンツおよび設定を完全にコントロールすることができます。

- 6 (オプション) 外部公開のオプションを指定するには、[外部公開] をクリックします。

このオプションは、システム管理者が外部に公開する権限を組織に付与している場合にのみ使用できます。

- a このカタログをシステムのすべての組織に公開するには、[公開を有効化] を選択します。

必要な場合は、組織内でのこのカタログへのアクセスを有効にする際に、パスワードを使用するように組織管理者に要求できます。

- b 公開済みの vApp テンプレートに BIOS UUID と MAC アドレスを含めるには、[ID 情報の保存] を選択します。

ID 情報は、他のすべての組織で使用可能ではない場合があります。

- 7 [OK] をクリックして、変更内容を保存します。

外部組織へのカタログの公開

システム管理者からカタログへのアクセスを許可された場合、カタログを外部に公開し、そのカタログの vApp テンプレートとメディア ファイルを、vCloud Director インストール環境外の組織の購読で使用できます。

前提条件

システム管理者によって組織に対するカタログ公開が有効化されており、カタログへのアクセス権が与えられていることを確認します。

手順

- 1 [カタログ] をクリックし、左側のペインで [マイ組織のカタログ] を選択します。
- 2 [カタログ] タブでカタログ名を右クリックし、[設定の発行] を選択します。
- 3 [外部公開] タブで、[有効] を選択し、カタログ フィールドのパスワードを入力します。
- 4 [OK] をクリックします。

次のステップ

[外部公開] タブに一覧表示されているサブスクリプション URL とパスワードを入力し、カタログへのアクセスを許可します。カタログのコンテンツにアクセスするには、組織でそのカタログをサブスクライブする必要があります。

カタログの所有者の変更

管理者は、カタログの所有者を変更できます。

カタログを所有するユーザーを削除する前に、所有者の変更またはカタログの削除を行う必要があります。

前提条件

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

手順

- 1 [カタログ] - [マイ組織のカタログ] を選択します。
- 2 [カタログ] タブをクリックし、カタログを右クリックして、[所有者の変更] を選択します。
- 3 リストからユーザーを選択するか、または検索します。
ユーザーは、完全な名前またはユーザー名を条件にして検索できます。
- 4 [OK] をクリックします。

カタログの削除

組織からカタログを削除できます。

前提条件

この操作には、事前定義の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。

カタログには、vApp テンプレートやメディア ファイルが含まれていないようにする必要があります。これらの項目は、別のカタログに移動するか、削除することができます。

手順

- 1 [カタログ] をクリックします。
- 2 左側のペインで、[マイ組織のカタログ] をクリックします。
- 3 カatalogを選択して右クリックし、[削除] を選択します。
- 4 [はい] をクリックして確認します。

結果

空のカタログは、組織から削除されます。

カタログのプロパティの変更

カタログのプロパティを確認および変更できます。

前提条件

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

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

Catalogの所有者である必要があります。

手順

- 1 [Catalog] をクリックします。
- 2 左側のペインで、[マイ組織のCatalog] をクリックします。
- 3 Catalogを選択して右クリックし、[プロパティ] を選択します。
- 4 [全般] タブ、[共有] タブ、および [外部公開] タブのプロパティを確認します。
- 5 関連するプロパティを変更し、[OK] をクリックします。

結果

Catalogのプロパティが更新されます。

外部Catalog フィードのサブスクリプション

外部Catalog フィードにサブスクライブすると、組織は外部ソースからCatalogにアクセスできます。

外部Catalogは、自分の組織と同じ vCloud Director のインストール環境にない組織のソースによって提供されるCatalogです。

前提条件

- この操作には、事前定義の組織管理者ロールに含まれている権限、またはそれに相当する権限が必要です。
- システム管理者は、外部Catalogにサブスクライブする権限を組織に付与する必要があります。

手順

- 1 [Catalog] をクリックし、左側のペインで [マイ組織のCatalog] をクリックします。
- 2 [Catalogを追加] をクリックし、Catalog フィードの名前と、オプションで説明を入力します。
- 3 [外部Catalogにサブスクライブする] を選択し、[次へ] をクリックします。
- 4 このCatalogに使用するストレージのタイプを選択し、[次へ] をクリックします。

オプション	説明
組織内で使用できるすべてのストレージを使用する	このCatalog フィードは、組織内で使用できるすべてのストレージを使用します。
特定のストレージ ポリシーに事前にプロビジョニングされたストレージ	このCatalog フィードに使用する仮想データセンター ストレージ ポリシーを選択し、[追加] をクリックします。

- 5 [メンバーを追加] をクリックします。

- 6 組織内で、このカタログ フィードにアクセスできるユーザーおよびグループを選択し、[OK] をクリックします。

オプション	説明
組織の全員	組織内のすべてのユーザーおよびグループがこのカタログ フィードにアクセスできます。
特定のユーザーとグループ	カタログ フィードへのアクセスを認めるユーザーまたはグループを選択し、[追加] をクリックします。

- 7 [組織の追加] をクリックします。

- 8 この vCloud Director インストール 環境で、このカタログ フィードにアクセスできる組織を選択し、[OK] をクリックします。

オプション	説明
すべての組織	vCloud Director インストール環境内のすべての組織がこのカタログ フィードにアクセスできます。
特定の組織	カタログ フィードへのアクセスを認める組織を選択し、[追加] をクリックします。

- 9 [次へ] をクリックします。

- 10 カタログ フィード設定を確認し、[完了] をクリックします。

クラウド リソースの管理

5

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、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、およびネットワーク プールは、すべてクラウド リソースとみなされます。クラウド リソースを vCloud Director に追加したら、クラウド リソースを変更したり、クラウド リソースの相互関係に関する情報を表示したりできます。

この章には、次のトピックが含まれています。

- [プロバイダ仮想データセンターの管理](#)
- [組織仮想データセンターの管理](#)
- [組織仮想データセンター テンプレートの管理](#)
- [外部ネットワークの管理](#)
- [Edge ゲートウェイの管理](#)
- [組織仮想データセンター ネットワークの管理](#)
- [ネットワーク プールの管理](#)
- [クラウド セルの管理](#)
- [サービス オファリングの管理](#)
- [マルチサイト展開の設定と管理](#)
- [オブジェクト メタデータの作成または更新](#)

プロバイダ仮想データセンターの管理

作成したプロバイダ仮想データセンターについては、プロパティの変更、無効化や削除、ESXi ホストとデータストアの管理を実行できます。

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を無効化して、そ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組織仮想データセンターが作成されないようにすることができます。

プロバイダ仮想データセンターを無効にすると、vCloud Director はそのリソースを使用する組織仮想データセンターも無効にします。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 [管理および監視] タブをクリックし、左側のペインで [プロバイダ vDC] をクリックします。
- 2 プロバイダ仮想データセンター名を右クリックし、[有効化] または [無効化] を選択します。

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を削除し、そ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 vCloud Director から削除することができます。リソースは、影響を受けずに vSphere に残されます。

前提条件

- プロバイダ仮想データセンターを無効化します。
- プロバイダ仮想データセンターを使用する組織仮想データセンターをすべて無効化して削除します。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [プロバイダ vDC] をクリックします。
- 2 プロバイダ仮想データセンター名を右クリックし、[削除] を選択します。
- 3 [はい] をクリックします。

プロバイダ仮想データセンターの名前および説明の変更

vCloud Director のインストール環境の規模が大きくなるにつれて、既存のプロバイダ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 [管理および監視] タブをクリックし、左側のペインで [プロバイダ vDC] をクリックします。
- 2 プロバイダ仮想データセンター名を右クリックし、[プロパティ] を選択します。
- 3 新しい名前または説明を入力し、[OK] をクリックします。

名前フィールドと説明フィールドを使用して、プロバイダ仮想データセンターで利用できる vSphere HA などの vSphere 機能を示すことができます。

プロバイダ仮想データセンターのマージ

2 つ以上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、マージされたすべてのプロバイダ仮想データセンターのリソースを統合できます。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [プロバイダ vDC] をクリックします。
- 2 他のプロバイダ仮想データセンターとマージするプロバイダ仮想データセンターを右クリックし、[次とマージ] を選択します。

- 3 このプロバイダ仮想データセンターとマージする 1 つ以上のプロバイダ仮想データセンターを選択し、[追加] をクリックします。

複数のプロバイダ仮想データセンターを選択するには、Ctrl キーを押しながら操作します。

- 4 (オプション) プロバイダ仮想データセンターの新しい名前と説明を入力します。
- 5 [OK] をクリックします。

結果

選択したプロバイダ仮想データセンターが、このプロバイダ仮想データセンターにマージされます。

レガシーのプロバイダ VDC での VXLAN の有効化

vSphere VXLAN は、新しいプロバイダ VDC に対してデフォルトで有効化されています。システム管理者は、vCloud Director の以前のリリースで作成されたプロバイダ VDC では、VXLAN を手動で有効にする必要があります。

前提条件

この操作は、システム管理者に制限されます。

お使いの vCloud Director 環境用に VXLAN を構成します。『NSX 管理ガイド』を参照してください。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [プロバイダ vDC] をクリックします。
- 2 プロバイダ VDC 名を右クリックし、[VXLAN を有効化] を選択します。

結果

プロバイダ VDC 用の VXLAN ネットワーク プールが作成されます。[VXLAN ネットワーク プール](#)を参照してください。

プロバイダ仮想データセンターのデータストア

プロバイダ仮想データセンターのデータストアは、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します。

プロバイダ仮想データセンターのデータストア メトリック

各プロバイダ仮想データセンターのデータストアに関する次の情報が、プロバイダ仮想データセンターの [データストア] タブに表示されます。

表 5-1. データストア メトリック

タイトル	説明
名前	プロバイダ仮想データセンターのデータストアの名前。
有効	プロバイダ仮想データセンターのデータストアが有効にされている場合、チェックマークが表示されます。

表 5-1. データストア メトリック（続き）

タイトル	説明
タイプ	仮想マシン ファイル システム (VMFS) か、ネットワーク ファイル システム (NFS) か、データストアが使用するファイル システムのタイプ。
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容量。仮想マシンをパワーオンすると、使用済みストレージ容量にログ ファイルも含まれます。
プロビジョニング済み	仮想マシンに確保されているデータストア容量。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。
要求済み	<p>データストア上で vCloud Director が管理する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"> ■ vCloud Director 仮想マシンのプロビジョニング ■ カタログ アイテム（テンプレートとメディア） ■ NSX Edge ■ 仮想マシンのメモリ スワップ要件（未使用の場合も含む） <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	データストアに関連付けられた vCenter Server。

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

プロバイダ仮想データセンターへ仮想マシン ストレージ ポリシーを追加すると、ストレージ ポリシーは、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サポートします。

仮想マシン ストレージ ポリシーは、vSphere において作成され、管理されます。ストレージ ポリシー ベース管理 (SPBM) の詳細については、『vSphere のストレージ』ドキュメントを参照するか、vSphere 管理者にお問い合わせください。

重要： vCloud Director は、暗号化や Storage I/O Control などの host-based データ サービスで仮想マシンのストレージ ポリシーをサポートしません。

前提条件

vCloud Director Web Console にシステム管理者としてログインします。

手順

- 1 [管理および監視] タブの左側のペインで、[プロバイダ VDC] をクリックします。
- 2 プロバイダ仮想データセンター名を右クリックし、[開く] をクリックします。
- 3 [ストレージ ポリシー] タブで、[ストレージ ポリシーの追加] をクリックします。

4 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、vCloud Director は、データソースがプロバイダ仮想データセンターのデータソース クラスタに追加、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。

5 [OK] をクリックします。

結果

ストレージ ポリシーのサポートが、プロバイダ仮想データセンターに追加されます。

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での Storage I/O Control サポートの構成

組織のメンバーごとにハード ディスクの読み取り/書き込みパフォーマンスの指定を有効にするには、その組織をサポートするプロバイダ仮想データセンターに、適切に構成された vSphere データストアによってバックアップされているストレージ プロファイルが含まれている必要があります。

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。組織仮想データセンターのストレージ プロファイルが、IOPS の割り当てに対応したストレージ デバイスを含むプロバイダ仮想データセンターのストレージ プロファイルによってバックアップされている場合は、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 対応ディスクを構成できます。IOPS をサポートするようにストレージ プロファイルが構成されている場合は、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め、IOPS をサポートするすべてのディスクにデフォルトの IOPS 値が割り当てられます。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 プロファイル、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 プロファイルを使用できません。

適切に構成されたプロバイダ仮想データセンター ストレージ プロファイルによってバックアップされている場合は、それらのプロファイルを使用するディスクに対して指定されたレベルの I/O パフォーマンスを提供するように組織仮想データセンターのストレージ プロファイルを構成できます。組織仮想データセンターで Storage I/O Control サポートを構成する方法については、『サービス プロバイダ向け vCloud API プログラミング ガイド』を参照してください。

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 適切に構成された vSphere ストレージ ポリシーを選択するか、新規に作成します。

vCloud Director でプロバイダ仮想データセンター ストレージ プロファイルの IOPS を有効にするには、IOPS に対応した vSphere ストレージ ポリシーが、vCloud Director に登録済みの vCenter サーバ上にある必要があります。

- また、基盤となる vSphere データストアをバックアップするストレージ デバイスで IOPS がサポートされている必要があります。

注： VMware Virtual SAN データストアでは、IOPS のサポートを有効にすることはできません。

- vSphere 管理者は VMware ナレッジベースの記事 <http://kb.vmware.com/kb/2148300> で説明されているとおりに特定の vSphere カスタム フィールドと値を使用してデータストアを構成する必要があります。
 - vSphere 管理者は IOPS 対応のデータストアを含む vSphere ストレージ ポリシーを作成する必要があります。
- 2 プロバイダ仮想データセンターに IOPS 対応の vSphere ストレージ プロファイルを追加します。

プロバイダ仮想データセンターを作成する際に使用する VMWProviderVdcParams 要求の本文の ProviderVdcStorageProfile 要素、またはプロバイダ仮想データセンター ストレージ プロファイルを更新する際に使用する updateStorageProfiles 要求の本文の UpdateProviderVdcStorageProfiles 要素で、IOPS 対応 vSphere ストレージ プロファイルを名前で参照します。

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の編集

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編集できます。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [プロバイダ vDC] をクリックします。
- 2 プロバイダ仮想データセンター名を右クリックし、[開く] を選択します。
- 3 [ストレージ ポリシー] タブをクリックします。
- 4 ストレージ ポリシーを右クリックし、[プロパティ] を選択します。
- 5 適宜メタデータを編集し、[OK] をクリックします。

プロバイダ VDC 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が提供する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るように、プロバイダ仮想データセンターにセカンダリ リソース プールを 1 つ以上追加できます。

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。

前提条件

- プロバイダ組織仮想データセンターのプライマリ リソース プールを提供する 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を確認します。
- vCloud Director Web コンソールにシステム管理者としてログインします。

手順

- 1 [管理および監視] タブの左側のペインで、[プロバイダ VDC] をクリックします。
- 2 プロバイダ仮想データセンター名を右クリックし、[開く] をクリックします。
- 3 [リソース プール] タブで [リソース プールの添付] をクリックします。
- 4 追加するリソース プールを選択し、[完了] をクリックします。

結果

vCloud 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用できるよう追加し、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すべての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に柔軟性を持たせます。

vCloud 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 リソース プールの有効化または無効化

リソース プールを無効化すると、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。

プロバイダ仮想データセンター上には、少なくとも 1 つの有効化されたリソース プールが必要です。リソース プールを無効化しても、すでに進行中のプロセスによるリソースの使用は妨げられません。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [プロバイダ vDC] をクリックします。
- 2 プロバイダ仮想データセンター名を右クリックし、[開く] を選択します。
- 3 [リソース プール] タブをクリックします。
- 4 リソース プールを右クリックし、[有効化] または [無効化] を選択します。

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リソース プールを分離することができます。

前提条件

- 1 プロバイダ仮想データセンターでリソース プールを無効化します。

- 2 そのリソース プールから仮想マシンを有効化されたリソース プールへ移行します。
- 3 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。
- 4 無効化されたリソース プールの影響を受ける Edge ゲートウェイを再デプロイします。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [プロバイダ vDC] をクリックします。
- 2 プロバイダ仮想データセンター名を右クリックし、[開く] を選択します。
- 3 [リソース プール] タブをクリックします。
- 4 リソース プールを右クリックし、[分離] をクリックします。

プロバイダ仮想データセンター上のリソース プール間での仮想マシンの移行

仮想マシンを、同じプロバイダ仮想データセンター上の 1 つのリソース プールから別のリソース プールへ移行することができます。仮想マシンを移行することにより、最近追加されたリソース プールに仮想マシンを追加したり、コミッション解除する予定のリソース プールから仮想マシンを削除したり、手動でプロバイダ仮想データセンター リソースのバランスをとったりすることができます。

予約プール組織仮想データセンターの一部である仮想マシンは、移行することができません。テンプレートとメディアは、データストアの移行を使用して別々に移行してください。

前提条件

プロバイダ仮想データセンターに、仮想マシンが存在するリソース プール以外のリソース プールが少なくとも 1 つ存在することを確認してください。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [プロバイダ vDC] をクリックします。
- 2 プロバイダ仮想データセンター名を右クリックし、[開く] を選択します。
- 3 [リソース プール] タブをクリックします。
- 4 リソース プール名を右クリックして [開く] を選択します。
- 5 仮想マシン名を右クリックして、[次に移行] を選択します。

複数の仮想マシンを選択するには、Ctrl キーを押しながらクリックします。

- 6 仮想マシンのターゲット リソース プールを選択する方法を選択します。

オプション	説明
自動的にリソース プールを選択	vCloud Director は、存在するすべてのリソース プールの現在のリソース バランスに基づいて、仮想マシンのターゲット リソース プールを選択します。
手動でリソース プールを選択	使用可能なリソース プールのリストから、仮想マシンの移行先にするリソース プールを選択します。

- 7 [OK] をクリックします。

プロバイダ仮想データセンター データストアの低ディスク容量しきい値の構成

データストアで使用可能な容量として指定したしきい値に到達したら vCloud Director から電子メールを受信するように、データストアの低ディスク領域しきい値を構成できます。これらの警告により、問題が発生する前に、ディスク領域が少ないことが通知されます。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [プロバイダ vDC] をクリックします。
- 2 プロバイダ仮想データセンター名を右クリックし、[開く] を選択します。
- 3 [データストア] タブをクリックします。
- 4 データストア名を右クリックし、[プロパティ] を選択します。
- 5 データストアのディスク領域しきい値を選択します。

黄色と赤の 2 つのしきい値を設定できます。スタンドアロン データストア上でしきい値を設定すると、しきい値はそのデータストアにのみ適用されます。ストレージ POD 上でしきい値を設定すると、しきい値はストレージ POD のすべてのデータストアに適用されます。デフォルトでは、vCloud Director は赤色のしきい値は 15% に、黄色のしきい値はスタンドアロンのデータストアまたは POD の合計容量の 25% に設定します。

ストレージ POD 上のデフォルトのしきい値は POD の合計容量に基づいているため、しきい値は POD 内の個々のデータストアの容量を超える場合があります。ストレージ POD 上のしきい値を設定する場合は、POD 内の各データストアの容量を考慮し、デフォルトのしきい値設定を使用するのではなく、手動でしきい値を設定してください。

- 6 [OK] をクリックします。

結果

vCloud Director は、データストアを使用するすべてのプロバイダ仮想データセンターのしきい値を設定します。vCloud Director は、データストアがしきい値を超えるとメール アラートを送信します。データストアがその赤色のしきい値に到達すると、仮想マシン配置エンジンは、すでに配置済みのインポートされた仮想マシンを除き、そのデータストアに対する新しい仮想マシンの配置を停止します。

プロバイダ仮想データセンター ユーザーへの電子メール通知の送信

プロバイダ仮想データセンター内のオブジェクト (vApp やメディア ファイルなど) を所有するすべてのユーザーに、電子メール通知を送信できます。たとえば、電子メール通知を送信して、ユーザーに今後のシステム メンテナンスなどを知らせることができます。

前提条件

SMTP サーバに対する有効な接続があることを確認します。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [プロバイダ vDC] をクリックします。
- 2 プロバイダ仮想データセンター名を右クリックし、[通知] を選択します。
- 3 電子メールの件名および本文を入力し、[電子メールを送信] をクリックします。

組織仮想データセンターの管理

組織仮想データセンターを作成したら、組織仮想データセンターのプロパティを変更したり、組織仮想データセンター自体を無効化/削除したり、組織仮想データセンターの割り当てモデル、ストレージ、ネットワーク設定を管理したりできます。

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を作成して、組織にリソースを割り当てます。組織仮想データセンターは、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。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。

前提条件

リソースを組織に割り当てるには、事前にプロバイダ仮想データセンターを持っている必要があります。

注： Flex 組織仮想データセンターを作成するには、vCloud Director Service Provider Admin Portal または vCloud API を使用します。『vCloud Director Service Provider Admin Portal Guide』または『サービス プロバイダ向け vCloud API プログラミング ガイド』を参照してください。

手順

1 [新しい組織仮想データセンター] ウィザードの起動

[新規の組織仮想データセンター] ウィザードを起動して、組織仮想データセンターを作成するプロセスを開始します。

2 組織仮想データセンターの組織の選択

組織仮想データセンターを作成すると、vCloud Director システムのどの組織にでもリソースを提供できます。1つの組織に対して、複数の組織仮想データセンターを作成できます。

3 プロバイダ仮想データセンターの選択

組織仮想データセンターは、使用するコンピューティング リソースとストレージ リソースをプロバイダ仮想データセンターから入手します。組織仮想データセンターは、これらのリソースを、組織内の vApp と仮想マシンに提供します。

4 割り当てモデルの選択

割り当てモデルにより、管理者が割り当てるプロバイダ仮想データセンターのコンピューティング リソースとメモリ リソースが組織仮想データセンターにコミットされる方法とタイミングが決定されます。

5 割り当てモデルの構成

割り当てモデルを構成して、組織仮想データセンターに割り当てるプロバイダ仮想データセンター リソースの量を指定します。

6 ストレージを割り当て

組織仮想データセンターでは、vApp および vApp テンプレートのためのストレージ領域が必要です。プロバイダ仮想データセンターのデータストアで使用可能な領域から、ストレージを割り当てることができます。

7 ネットワーク プールおよびサービス

ネットワーク プールは、vApp ネットワークと内部の組織仮想データセンター 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。

8 Edge ゲートウェイの構成

1つ以上の外部ネットワークに接続できるように、Edge ゲートウェイを構成します。

9 外部ネットワークの構成

Edge ゲートウェイが接続できる外部ネットワークを選択します。

10 新規 Edge ゲートウェイ上の IP 設定の構成

新規 Edge ゲートウェイ上の外部ネットワークの IP 設定を構成します。

11 新規 Edge ゲートウェイ上の IP プールの細分割り当て

Edge ゲートウェイ上の外部ネットワークが提供する IP プールを複数の固定 IP プールに細分割り当てします。

12 新規 Edge ゲートウェイ上のレート制限の構成

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します。

13 組織仮想データセンター ネットワークの作成

新しい Edge ゲートウェイに接続する組織仮想データセンター ネットワークを作成できます。

14 組織仮想データセンターの名前の指定

新しい組織仮想データセンターで使用できる vSphere 機能を示すため、わかりやすい名前を指定し、必要に応じて説明も入力できます。

15 設定の確認と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を作成する前に、入力した設定を確認します。

[新しい組織仮想データセンター] ウィザードの起動

[新規の組織仮想データセンター] ウィザードを起動して、組織仮想データセンターを作成するプロセスを開始します。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織 VDC] をクリックします。
- 2 追加ボタンをクリックします。

組織仮想データセンターの組織の選択

組織仮想データセンターを作成すると、vCloud Director システムのどの組織にでもリソースを提供できます。1つの組織に対して、複数の組織仮想データセンターを作成できます。

手順

- 1 組織を選択します。
- 2 [次へ] をクリックします。

プロバイダ仮想データセンターの選択

組織仮想データセンターは、使用するコンピューティング リソースとストレージ リソースをプロバイダ仮想データセンターから入手します。組織仮想データセンターは、これらのリソースを、組織内の vApp と仮想マシンに提供します。

手順

- 1 プロバイダ仮想データセンターを選択します。

プロバイダ仮想データセンター リストには使用可能なリソースに関する情報が表示され、ネットワーク リストには選択したプロバイダ仮想データセンターで使用可能なネットワークに関する情報が表示されます。

- 2 [次へ] をクリックします。

割り当てモデルの選択

割り当てモデルにより、管理者が割り当てるプロバイダ仮想データセンターのコンピューティング リソースとメモリ リソースが組織仮想データセンターにコミットされる方法とタイミングが決定されます。

前提条件

どの割り当てモデルが環境に適しているかについて理解していることを確認します。[割り当てモデルについて](#)を参照してください。

手順

- 1 割り当てモデルを選択します。

オプション	説明
割り当てプール	プロバイダ仮想データセンターから割り当てるリソースの割合は、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。
従量課金制	リソースは、組織仮想データセンターでユーザーが vApp を作成するときのみコミットされます。
予約プール	割り当てるすべてのリソースは、組織仮想データセンターに直ちにコミットされます。

配置エンジンおよび仮想マシンの共有、レートおよび制限の詳細については、『vCloud Director ユーザー ガイド』を参照してください。

- 2 [次へ] をクリックします。

割り当てモデルの構成

割り当てモデルを構成して、組織仮想データセンターに割り当てるプロバイダ仮想データセンター リソースの量を指定します。

手順

1 割り当てモデルのオプションを選択します。

モデルによっては、一部のオプションが含まれていないものもあります。

オプション	アクション
CPU の割り当て	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 の最大使用量を GHz 単位で入力します。このオプションは、割り当てプールと予約プールの割り当てモデルの場合にのみ指定できます。予約プール モデルに含まれる [CPU リソースを予約値を超えて拡張できるようにします。] チェック ボックスでは、仮想データセンターが CPU リソースを上限なしで提供できるかどうかを選択できます。
確保された CPU 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保証する CPU リソースの割合を入力します。100% 未満を保証すると、リソースをオーバーコミットできます。このオプションは、割り当てプールと従量課金制の割り当てモデルの場合にのみ指定できます。割り当てプールのデフォルト値は 50% で、従量課金制のデフォルトは 20% です。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。
vCPU 速度	vCPU 速度を GHz 単位で入力します。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。このオプションは、割り当てプールと従量課金制の割り当てモデルの場合にのみ指定できます。
メモリの割り当て	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使用量を GB 単位で入力します。このオプションは、割り当てプールと予約プールの割り当てモデルの場合にのみ指定できます。
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保証するメモリ リソースの割合を入力します。100% 未満を保証すると、リソースをオーバーコミットできます。このオプションは、割り当てプールと従量課金制の割り当てモデルの場合にのみ指定できます。割り当てプールのデフォルトは 50% で、従量課金制のデフォルトは 20% です。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。
最大仮想マシン数	組織仮想データセンターで作成可能な仮想マシンの最大数を入力します。

2 [次へ] をクリックします。

例：割り当てモデルの構成

組織仮想データセンターを作成すると、vCloud Director は、指定される割り当てモデルの設定に基づいて vSphere リソース プールを作成します。

表 5-2. 単一クラスタの割り当てプール機能が有効になっている場合の割り当てプール設定によるリソース プール設定への影響

割り当てプール設定	割り当てプール値	リソース プール設定	リソース プール値
CPU の割り当て	25 GHz	CPU 制限	25 GHz
CPU % の保証	10%	CPU の予約	2.5GHz
メモリの割り当て	50 GB	メモリの制限	50 GB
メモリ % の保証	20%	メモリの予約	10GB

表 5-3. 単ークラスタの割り当てプール機能が無効になっている場合の割り当てプール設定によるリソース プール設定への影響

割り当てプール設定	割り当てプール値	リソース プール設定	サブリソース プール値	すべてのサブリソース プールでこの組織仮想データセンターにコミットされた値
CPU の割り当て	25 GHz	CPU 制限	vCPU の合計数に、関連付けられているすべての仮想マシンの vCPU 周波数を掛けた値	該当なし
CPU % の保証	10%	CPU の予約	関連付けられているすべての仮想マシンの vCPU の数に、vCPU 周波数、CPU の割合保証を掛けた合計値	2.5GHz
メモリの割り当て	50 GB	メモリの制限	関連付けられているすべての仮想マシンの構成済みのメモリ サイズの合計	該当なし
メモリ % の保証	20%	メモリの予約	構成済みのメモリ サイズの合計に、関連付けられているすべての仮想マシンのメモリの割合の保証を掛けた値	10GB

表 5-4. 従量課金制の設定によるリソース プール設定への影響

従量課金制の設定	従量課金制の値	リソース プール設定	リソース プール値
CPU % の保証	10%	CPU の予約、CPU の制限	0.00GHz、無制限
メモリ % の保証	100%	メモリの予約、メモリの制限	0.00 GB、無制限

従量課金制の組織仮想データセンターをサポートするために作成されるリソース プールには、予約または制限がありません。従量課金制の設定は、オーバーコミットにのみ影響を与えます。100% 保証とは、オーバーコミットの可能性があることを意味します。割合が低いほど、オーバーコミットの可能性が高くなります。

表 5-5. 予約プール設定によるリソース プール設定への影響

予約プール設定	予約プール値	リソース プール設定	リソース プール値
CPU の割り当て	25 GHz	CPU の予約、CPU の制限	25GHz、25GHz
メモリの割り当て	50 GB	メモリの予約、メモリの制限	50 GB、50 GB

ストレージを割り当て

組織仮想データセンターでは、vApp および vApp テンプレートのためのストレージ領域が必要です。プロバイダ仮想データセンターのデータストアで使用可能な領域から、ストレージを割り当てることができます。

シン プロビジョニングはストレージの過剰な割り当てを回避するために役立ちます。シン プロビジョニングされた仮想ディスクを使用する仮想マシンでは、ESXi により、ディスクの最大容量に基づいてすべてのストレージが予約されますが、初期操作にディスクが必要とするストレージのみがコミットされます。ディスクで必要になると、追加のストレージがコミットされます。

高速プロビジョニングでは、できる限りリンク クローンを使用するため、時間が節約されます。[仮想マシンの高速プロビジョニング](#)を参照してください。

手順

- 1 割り当てるストレージ ポリシーを選択して、[追加] をクリックします。
- 2 割り当てるストレージの量を入力します。
- 3 ドロップダウン メニューから [デフォルトのインスタンス化ポリシー] を選択します。
これは、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使用する、デフォルトのストレージ ポリシーです。
- 4 (オプション) [シン プロビジョニングを有効化] チェック ボックスをオンにして、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化します。
- 5 (オプション) [高速プロビジョニングを有効化] チェック ボックスをオフにして、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化します。
- 6 [次へ] をクリックします。

ネットワーク プールおよびサービス

ネットワーク プールは、vApp ネットワークと内部の組織仮想データセンター 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。

手順

- 1 ネットワーク プールを選択するか、[なし] を選択します。
[なし] を選択する場合は、後でネットワーク プールを追加できます。
- 2 (オプション) 選択したネットワーク プールを VXLAN プールに変換します。
選択したネットワーク プールが VCDNI プールの場合は、[VXLAN に移行] ボタンが表示されます。VMware ナレッジベースの記事 <https://kb.vmware.com/kb/2148381> を参照してください。
- 3 組織がネットワーク プールからプロビジョニングできるネットワークの最大数を入力します。
- 4 (オプション) 使用可能なそれぞれのサードパーティまたは Edge ゲートウェイ サービスに [有効化] を選択し、有効化します。
- 5 [次へ] をクリックします。

Edge ゲートウェイの構成

1 つ以上の外部ネットワークに接続できるように、Edge ゲートウェイを構成します。

手順

- 1 システム リソースに基づいて Edge ゲートウェイ構成を選択します。

オプション	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 [特大] 構成では、同じセキュリティ機能が提供されます。
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適しています。
超特大	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。

Edge ゲートウェイを導入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』の「NSX のシステム要件」を参照してください。

- 2 (オプション) 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するには、[高可用性を有効にする] を選択します。
- 3 (オプション) [分散ルーティングの有効化] を選択し、分散論理ルーティングを提供するように詳細ゲートウェイを設定します。

このオプションは、[詳細ゲートウェイとして作成] を選択する場合にのみ使用できます。分散ルーティングを有効にすると、はるかに多くの組織 VDC ネットワークをゲートウェイに作成できます。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。

- 4 (オプション) [FIPS モードの有効化] を選択して、Edge Gateway で NSX の FIPS モードを使用できるように設定します。

このオプションは、システム管理者が Edge Gateway での FIPS モードの有効化を許可している場合にのみ使用できます。NSX 6.3 以降が必要です。[全般システム設定](#)を参照してください。FIPS モードの詳細については、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。

- 5 (オプション) [IP 設定の構成] を選択し、外部インターフェイスの IP アドレスを手動で構成します。
- 6 (オプション) [IP プールの細分割り当て] を選択し、使用するゲートウェイ サービスの一連の IP アドレスを割り当てます。
- 7 (オプション) [レート制限の構成] を選択し、外部接続された各インターフェイスの着信および発信のレート制限を選択します。
- 8 [次へ] をクリックします。

外部ネットワークの構成

Edge ゲートウェイが接続できる外部ネットワークを選択します。

このページは、[新規の Edge ゲートウェイの作成] を選択した場合にのみ表示されます。

手順

- 1 リストから外部ネットワークを選択して [追加] をクリックします。

複数のネットワークを選択するには、Ctrl キーを押しながら操作します。

- 2 デフォルト ゲートウェイにするネットワークを選択します。
- 3 (オプション) [DNS リレーのデフォルトのゲートウェイを使用します]を選択します。
- 4 [次へ] をクリックします。

新規 Edge ゲートウェイ上の IP 設定の構成

新規 Edge ゲートウェイ上の外部ネットワークの IP 設定を構成します。

このページは、ゲートウェイの構成中に [IP 設定の構成] を選択した場合にのみ表示されます。

手順

- 1 [IP 設定の構成] ページで、[IP 割り当ての変更] をクリックします。
- 2 IP アドレスを指定するそれぞれの外部ネットワークについて、ドロップダウン メニューから [手動] を選択します。
- 3 [手動] に設定するそれぞれの外部ネットワークの IP アドレスを入力し、[次へ] をクリックします。

新規 Edge ゲートウェイ上の IP プールの細分割り当て

Edge ゲートウェイ上の外部ネットワークが提供する IP プールを複数の固定 IP プールに細分割り当てします。

このページは、ゲートウェイの構成中に [IP プールの細分割り当て] を選択した場合にのみ表示されます。

前提条件

Edge Gateway に割り当てる IP アドレスが vCloud Director の外部で使用されていないことを確認します。

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。vCloud 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 vCloud 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 外部ネットワークと細分割り当てする IP プールを選択します。
- 2 IP プールの範囲内の IP アドレスまたは IP アドレスの範囲を入力し、[追加] をクリックします。
この手順を繰り返し、細分割り当てされた複数の IP プールを追加します。
- 3 (オプション) 細分割り当てされた IP プールを選択し、[変更] をクリックして、細分割り当てされた IP プールの IP アドレスの範囲を変更します。
- 4 (オプション) 細分割り当てされた IP プールを選択し、[削除] をクリックして、細分割り当てされた IP プールを削除します。
- 5 [次へ] をクリックします。

新規 Edge ゲートウェイ上のレート制限の構成

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します。

このページは、ゲートウェイの構成中に [レート制限の構成] を選択した場合にのみ表示されます。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 レート制限を有効化するそれぞれの外部ネットワークに対して [有効化] をクリックします。
- 2 有効化されたそれぞれの外部ネットワークに対し、[着信のレート制限] を 1 秒あたりのギガビットで入力します。
- 3 有効化されたそれぞれの外部ネットワークに対し、[発信のレート制限] を 1 秒あたりのギガビットで入力し、[次へ] をクリックします。

組織仮想データセンター ネットワークの作成

新しい Edge ゲートウェイに接続する組織仮想データセンター ネットワークを作成できます。

このページは、[新規の Edge ゲートウェイの作成] を選択した場合にのみ表示されます。

手順

- 1 (オプション) [この新規 Edge ゲートウェイに接続されたこの仮想データセンターのネットワークを作成する] を選択します。
- 2 新しい組織仮想データセンター ネットワークの名前を入力し、必要に応じて説明も入力します。
- 3 (オプション) [このネットワークを組織内の他の VDC と共有する] を選択します。
- 4 組織仮想データセンター ネットワークのゲートウェイ アドレスとネットワーク マスクを入力します。
- 5 (オプション) [ゲートウェイ DNS を使用] を選択し、ゲートウェイの DNS リレーを使用します。
このオプションは、ゲートウェイで DNS リレーが有効化されている場合にのみ使用できます。
- 6 (オプション) DNS を使用する DNS 設定を入力します。
- 7 IP アドレスまたは IP アドレスの範囲を入力し、[追加] をクリックして固定 IP プールを作成します。
この手順を繰り返し、複数の固定 IP プールを追加します。
- 8 [次へ] をクリックします。

組織仮想データセンターの名前の指定

新しい組織仮想データセンターで利用できる vSphere 機能を示すため、わかりやすい名前を指定し、必要に応じて説明も入力できます。

手順

- 1 名前と、必要に応じて説明を入力します。

名前と説明の各フィールドには、特殊文字を使用しないでください。長さの制限については、[名前と説明に対する長さの制限](#)を参照してください。

- 2 (オプション) [有効] をオフにします。

組織仮想データセンターを無効にすると、新規 vApp はその仮想データセンターにデプロイされなくなります。実行中の vApp は継続して実行されますが、その他の vApp は開始できません。

- 3 [次へ] をクリックします。

設定の確認と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を作成する前に、入力した設定を確認します。

手順

- 1 組織仮想データセンターの設定を確認します。
- 2 (オプション) [戻る] をクリックして設定を変更します。
- 3 (オプション) この仮想データセンターの組織仮想データセンター ネットワークをすぐに作成するには、[このウィザードを終了後、この組織にネットワークを追加します] を選択します。
- 4 [完了] をクリックして設定を受け入れ、組織仮想データセンターを作成します。

組織仮想データセンターを作成すると、vCloud Director は、CPU とメモリのリソースを提供するために vSphere でリソース プールを作成します。

テンプレートからの組織仮想データセンターの作成

組織がアクセスできる仮想データセンター テンプレートから、新しい組織仮想データセンターを作成することができます。

前提条件

組織仮想データセンターの作成対象となる組織が仮想データセンター テンプレートのアクセス リストに存在することを確認します。

手順

- 1 新しい組織仮想データセンターの作成対象となる組織で、[マイ クラウド] をクリックし、左側のペインで [組織 VDC テンプレート] をクリックします。
- 2 インスタンス化する仮想データセンター テンプレートを右クリックして、[インスタンス化] を選択します。
- 3 新しい組織仮想データセンターの[名前]と、任意で[説明]を入力し、[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

組織仮想データセンターを無効化すると、その他の vApp と仮想マシンでコンピューティング リソースとストレージ リソースが使用できなくなります。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 [管理および監視] タブをクリックし、左側のペインで [組織 VDC] をクリックします。
- 2 組織仮想データセンター名を右クリックし、[有効化] または [無効化] を選択します。

組織仮想データセンターの削除

組織仮想データセンターを削除し、そ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 リソースを組織から削除することができます。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。

前提条件

組織仮想データセンターを無効化し、その vApp、vApp テンプレート、およびメディアをすべて移動または削除します。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織 VDC] をクリックします。
- 2 組織仮想データセンター名を右クリックし、[削除] を選択します。
- 3 [はい] をクリックします。

組織仮想データセンターのプロパティ

仮想データセンターの名前と説明、割り当てモデルの設定、ストレージ設定およびネットワーク設定など、既存の組織仮想データセンターのプロパティを編集できます。組織仮想データセンターで使用されるいずれかの VCDNI ネットワーク プールを VXLAN プールに変換することもできます。

VXLAN 変換の詳細については、[ネットワーク プールおよびサービス](#)を参照してください。

■ 組織仮想データセンターの名前および説明の変更

vCloud Director のインストール環境の規模が大きくなるにつれて、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。

■ 組織仮想データセンターの割り当てモデルの設定の編集

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設定の一部は変更できます。

■ 組織仮想データセンター ストレージの設定の編集

組織仮想データセンターを作成して使用した後で、プロバイダ仮想データセンターからストレージ リソースをさらに追加できます。また、その組織仮想データセンターのシン プロビジョニングと高速プロビジョニングを有効化または無効化することもできます。

■ 組織仮想データセンター ネットワークの設定の編集

組織仮想データセンターでプロビジョニングされるネットワークの最大数と、ネットワークのプロビジョニング元となるネットワーク プールを変更できます。

組織仮想データセンターの名前および説明の変更

vCloud Director のインストール環境の規模が大きくなるにつれて、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 [管理および監視] タブをクリックし、左側のペインで [組織 VDC] をクリックします。

- 2 組織仮想データセンター名を右クリックし、[プロパティ] を選択します。
- 3 [全般] タブで新しい名前と説明を入力し、[OK] をクリックします。

名前フィールドと説明フィールドを使用して、組織仮想データセンターで利用できる vSphere HA などの vSphere 機能を示すことができます。

組織仮想データセンターの割り当てモデルの設定の編集

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設定の一部は変更できます。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織 VDC] をクリックします。
- 2 組織仮想データセンター名を右クリックし、[プロパティ] を選択します。
- 3 [割り当て] タブで新しい割り当てモデルの設定を入力し、[OK] をクリックします。

オプション	操作
CPU の割り当て	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 の最大使用量を GHz 単位で入力します。このオプションは、割り当てプールと予約プールの割り当てモデルの場合にのみ指定できます。
確保された CPU 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保証する CPU リソースの割合を入力します。100% 未満を保証すると、リソースをオーバーコミットできます。このオプションは、割り当てプールと従量課金制の割り当てモデルの場合にのみ指定できます。
vCPU 速度	vCPU 速度を GHz 単位で入力します。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。このオプションは、従量課金制割り当てモデルの場合にのみ指定できます。
メモリの割り当て	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使用量を GB 単位で入力します。このオプションは、割り当てプールと予約プールの割り当てモデルの場合にのみ指定できます。
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保証するメモリ リソースの割合を入力します。100% 未満を保証すると、リソースをオーバーコミットできます。このオプションは、割り当てプールと従量課金制の割り当てモデルの場合にのみ指定できます。
最大仮想マシン数	組織仮想データセンターで作成可能な仮想マシンの最大数を入力します。

これらの設定は、この時点以後に起動する vApp にのみ影響します。すでに実行されている vApp は影響を受けません。vCloud Director がこの組織仮想データセンターについて報告する使用状況情報は、実行されているすべての vApp を停止して再起動するまで新しい設定に反映されません。

組織仮想データセンター ストレージの設定の編集

組織仮想データセンターを作成して使用した後で、プロバイダ仮想データセンターからストレージ リソースをさらに追加できます。また、その組織仮想データセンターのシン プロビジョニングと高速プロビジョニングを有効化または無効化することもできます。

高速プロビジョニングには、VMware vSphere ® 5.0 以降でバックアップされたプロバイダ仮想データセンターが必要です。高速プロビジョニングの詳細については、[仮想マシンの高速プロビジョニング](#)を参照してください。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織 VDC] をクリックします。
- 2 組織仮想データセンター名を右クリックし、[プロパティ] を選択します。
- 3 [ストレージ] タブをクリックします。
- 4 (オプション) [シン プロビジョニングを有効化] を選択して、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化します。
- 5 (オプション) [高速プロビジョニングを有効化] を選択して、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化します。
- 6 [OK] をクリックします。

組織仮想データセンター ネットワークの設定の編集

組織仮想データセンターでプロビジョニングされるネットワークの最大数と、ネットワークのプロビジョニング元となるネットワーク プールを変更できます。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織 VDC] をクリックします。
- 2 組織仮想データセンター名を右クリックし、[プロパティ] を選択します。
- 3 [ネットワーク プール] タブをクリックします。
- 4 (オプション) ドロップダウン メニューからネットワーク プールを選択するか、[なし] を選択します。
[なし] を選択する場合は、後でネットワーク プールを追加できます。
- 5 (オプション) 組織がネットワーク プールからプロビジョニングできるネットワークの最大数を入力します。
- 6 [OK] をクリックします。

組織仮想データセンターへのストレージ ポリシーの追加

組織仮想データセンターにストレージ ポリシーを追加し、プロバイダ仮想データセンターで仮想マシンのストレージ ポリシーをサポートします。

前提条件

1 つ以上のストレージ ポリシーを、組織仮想データセンターをバックアップするプロバイダ仮想データセンターに関連付ける必要があります。[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。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織 VDC] をクリックします。
- 2 組織仮想データセンター名をダブルクリックし、組織仮想データセンターを開きます。
- 3 [ストレージ ポリシー] タブをクリックし、[追加] をクリックします。
- 4 ストレージ ポリシーを選択し、[追加] をクリックして、[OK] をクリックします。

結果

ストレージ ポリシーのサポートが、組織仮想データセンターに追加されます。

組織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 テンプレートは、組織仮想データセンターと、オプションで Edge ゲートウェイと組織仮想データセンター ネットワークの構成を指定します。組織管理者が、組織内でシステム管理者がこれらのリソースを作成できるようにしたい場合、組織仮想データセンター テンプレートを作成して、リソースを組織と共有することができます。

仮想データセンター テンプレートを作成して共有することで、システム管理者は、プロバイダ仮想データセンターや外部ネットワークなど、システム リソースの割り当てにおける管理制御を保持しながら、組織仮想データセンターのセルフサービス プロビジョニングを可能にできます。組織の管理者、または仮想データセンター テンプレートの表示やインスタンス化の権限を持ついずれかのロールは、インスタンス化を利用して、テンプレートから組織仮想データセンターを作成します。

関連するビデオ



VDC テンプレートの作成と使用

(https://vmwaretv.vmware.com/media/t/1_pxn53bw4)

■ 組織仮想データセンター テンプレートの作成

組織仮想データセンター テンプレートを作成して、プロバイダ仮想データセンターや外部ネットワークなど、システム リソースの割り当てにおける管理制御を保持しながら、組織仮想データセンターのセルフサービス プロビジョニングを可能にできます。

■ 組織仮想データセンター テンプレートのインスタンス化

仮想データセンター テンプレートから新しい組織仮想データセンターを作成するには、仮想データセンター テンプレートをインスタンス化します。

■ 組織仮想データセンター テンプレートの修正

名前と説明、割り当てモデルの設定、ストレージ設定およびネットワーク設定など、既存の仮想データセンター テンプレートのプロパティを編集できます。

■ 組織仮想データセンター テンプレートのクローン作成

仮想データセンター テンプレートをクローン作成すると、既存の仮想データセンター テンプレートに基づいて新しい仮想データセンター テンプレートを作成することができます。

■ 組織仮想データセンター テンプレートの削除

仮想データセンター テンプレートをシステムから削除することができます。仮想データセンター テンプレートの削除は、テンプレートからすでに作成されている仮想データセンターには影響を与えません。

組織仮想データセンター テンプレートの作成

組織仮想データセンター テンプレートを作成して、プロバイダ仮想データセンターや外部ネットワークなど、システム リソースの割り当てにおける管理制御を保持しながら、組織仮想データセンターのセルフサービス プロビジョニングを可能にできます。

注： vCloud Director は、NSX Data Center for vSphere によってバックアップされる仮想データセンターの組織仮想データセンター テンプレートをサポートしています。

前提条件

vCloud Director に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。

手順

1 新規仮想データセンター テンプレート ウィザードを開く

組織仮想データセンター テンプレートを作成するプロセスを開始するには、新規仮想データセンター テンプレート ウィザードを開きます。

2 プロバイダ仮想データセンターと外部ネットワークの選択

組織仮想データセンターは、使用するコンピューティング リソースとストレージ リソースをプロバイダ仮想データセンターから取得します。組織仮想データセンターは、これらのリソースを、組織内の vApp と仮想マシンに提供します。

3 割り当てモデルの選択

割り当てモデルにより、管理者が割り当てるプロバイダ仮想データセンターのコンピューティング リソースとメモリ リソースが組織仮想データセンターにコミットされる方法とタイミングが決定されます。

4 割り当てモデルの構成

割り当てモデルを構成して、組織仮想データセンターに割り当てるプロバイダ仮想データセンター リソースの量を指定します。

5 ストレージ プロファイルの構成

組織仮想データセンターでは、vApp および vApp テンプレートのためのストレージ領域が必要です。プロバイダ仮想データセンターのデータストアで使用可能な領域から、ストレージを割り当てることができます。

6 ネットワーク プールの構成

ネットワーク プールは、vApp ネットワークと内部の組織仮想データセンター 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。仮想データセンター テンプレートを構成して、インストール環境中のネットワーク プールに自動的に接続できます。また、ネットワーク プールに接続しないことも可能です。

7 Edge ゲートウェイの構成

テンプレートから作成された組織仮想データセンター内でルーティングされたネットワーク通信が有効になるように Edge ゲートウェイを構成します。

8 新規 Edge ゲートウェイ上のネットワーク設定の構成

新規 Edge ゲートウェイ上の外部ネットワークの IP 設定を構成します。

9 アクセス リストの構成

組織を仮想データセンター テンプレートのアクセス リストに追加すると、これらの組織がテンプレートから仮想データセンターをインスタンス化できるようになります。

10 組織仮想データセンター テンプレートの命名

システムや、テンプレートにアクセスする各組織で使用する仮想データセンターの記述名とオプションの説明を提供します。

11 組織仮想データセンター テンプレート設定の確認

仮想データセンター テンプレートに対して入力した設定をレビューして確認します。

新規仮想データセンター テンプレート ウィザードを開く

組織仮想データセンター テンプレートを作成するプロセスを開始するには、新規仮想データセンター テンプレート ウィザードを開きます。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織 VDC テンプレート] をクリックします。
- 2 追加ボタンをクリックします。

プロバイダ仮想データセンターと外部ネットワークの選択

組織仮想データセンターは、使用するコンピューティング リソースとストレージ リソースをプロバイダ仮想データセンターから取得します。組織仮想データセンターは、これらのリソースを、組織内の vApp と仮想マシンに提供します。

手順

- 1 プロバイダ仮想データセンターと外部ネットワークを仮想データセンター テンプレートに追加するには、上部のリストからプロバイダ仮想データセンターと外部ネットワークのペアを選択し、[追加] をクリックします。

このテンプレートに基づく組織仮想データセンターは、選択されたプロバイダ仮想データセンターと外部ネットワークを使用します。各プロバイダ仮想データセンターに対して、外部ネットワークは1つしか構成できません。

注： vCloud Director は、NSX Data Center for vSphere によってバックアップされる仮想データセンターの組織仮想データセンター テンプレートをサポートしています。

- 2 [次へ] をクリックします。

割り当てモデルの選択

割り当てモデルにより、管理者が割り当てるプロバイダ仮想データセンターのコンピューティング リソースとメモリ リソースが組織仮想データセンターにコミットされる方法とタイミングが決定されます。

前提条件

どの割り当てモデルが環境に適しているかについて理解していることを確認します。[割り当てモデルについて](#)を参照してください。

手順

- 1 割り当てモデルを選択します。

オプション	説明
割り当てプール	プロバイダ仮想データセンターから割り当てるリソースの割合は、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。
従量課金制	リソースは、組織仮想データセンターでユーザーが vApp を作成するときのみコミットされます。
予約プール	割り当てるすべてのリソースは、組織仮想データセンターに直ちにコミットされます。

配置エンジンおよび仮想マシンの共有、レートおよび制限の詳細については、『vCloud Director ユーザー ガイド』を参照してください。

- 2 [次へ] をクリックします。

割り当てモデルの構成

割り当てモデルを構成して、組織仮想データセンターに割り当てるプロバイダ仮想データセンター リソースの量を指定します。

手順

- 1 割り当てモデルのオプションを選択します。

モデルによっては、一部のオプションが含まれていないものもあります。

オプション	アクション
CPU の割り当て	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 の最大使用量を GHz 単位で入力します。このオプションは、割り当てプールと予約プールの割り当てモデルの場合にのみ指定できます。予約プール モデルに含まれる [CPU リソースを予約値を超えて拡張できるようにします。] チェック ボックスでは、仮想データセンターが CPU リソースを上限なしで提供できるかどうかを選択できます。
確保された CPU 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保証する CPU リソースの割合を入力します。100% 未満を保証すると、リソースをオーバーコミットできます。このオプションは、割り当てプールと従量課金制の割り当てモデルの場合にのみ指定できます。割り当てプールのデフォルト値は 50% で、従量課金制のデフォルトは 20% です。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。
vCPU 速度	vCPU 速度を GHz 単位で入力します。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。このオプションは、割り当てプールと従量課金制の割り当てモデルの場合にのみ指定できます。
メモリの割り当て	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使用量を GB 単位で入力します。このオプションは、割り当てプールと予約プールの割り当てモデルの場合にのみ指定できます。

オプション	アクション
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保証するメモリ リソースの割合を入力します。100% 未満を保証すると、リソースをオーバーコミットできます。このオプションは、割り当てプールと従量課金制の割り当てモデルの場合にのみ指定できます。割り当てプールのデフォルトは 50% で、従量課金制のデフォルトは 20% です。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。
最大仮想マシン数	組織仮想データセンターで作成可能な仮想マシンの最大数を入力します。

2 [次へ] をクリックします。

例：割り当てモデルの構成

組織仮想データセンターを作成すると、vCloud Director は、指定される割り当てモデルの設定に基づいて vSphere リソース プールを作成します。

表 5-6. 単ークラスタの割り当てプール機能が有効になっている場合の割り当てプール設定によるリソース プール設定への影響

割り当てプール設定	割り当てプール値	リソース プール設定	リソース プール値
CPU の割り当て	25 GHz	CPU 制限	25 GHz
CPU % の保証	10%	CPU の予約	2.5GHz
メモリの割り当て	50 GB	メモリの制限	50 GB
メモリ % の保証	20%	メモリの予約	10GB

表 5-7. 単ークラスタの割り当てプール機能が無効になっている場合の割り当てプール設定によるリソース プール設定への影響

割り当てプール設定	割り当てプール値	リソース プール設定	サブリソース プール値	すべてのサブリソース プールでこの組織仮想データセンターにコミットされた値
CPU の割り当て	25 GHz	CPU 制限	vCPU の合計数に、関連付けられているすべての仮想マシンの vCPU 周波数を掛けた値	該当なし
CPU % の保証	10%	CPU の予約	関連付けられているすべての仮想マシンの vCPU の数に、vCPU 周波数、CPU の割合保証を掛けた合計値	2.5GHz
メモリの割り当て	50 GB	メモリの制限	関連付けられているすべての仮想マシンの構成済みのメモリ サイズの合計	該当なし
メモリ % の保証	20%	メモリの予約	構成済みのメモリ サイズの合計に、関連付けられているすべての仮想マシンのメモリの割合の保証を掛けた値	10GB

表 5-8. 従量課金制の設定によるリソース プール設定への影響

従量課金制の設定	従量課金制の値	リソース プール設定	リソース プール値
CPU % の保証	10%	CPU の予約、CPU の制限	0.00GHz、無制限
メモリ % の保証	100%	メモリの予約、メモリの制限	0.00 GB、無制限

従量課金制の組織仮想データセンターをサポートするために作成されるリソース プールには、予約または制限がありません。従量課金制の設定は、オーバーコミットにのみ影響を与えます。100% 保証とは、オーバーコミットの可能性がないことを意味します。割合が低いほど、オーバーコミットの可能性が高くなります。

表 5-9. 予約プール設定によるリソース プール設定への影響

予約プール設定	予約プール値	リソース プール設定	リソース プール値
CPU の割り当て	25 GHz	CPU の予約、CPU の制限	25GHz、25GHz
メモリの割り当て	50 GB	メモリの予約、メモリの制限	50 GB、50 GB

ストレージ プロファイルの構成

組織仮想データセンターでは、vApp および vApp テンプレートのためのストレージ領域が必要です。プロバイダ仮想データセンターのデータストアで使用可能な領域から、ストレージを割り当てることができます。

手順

- （オプション）[利用可能なストレージ プロファイル] リストからストレージ プロファイルを選択し、[追加] をクリックして、仮想データセンター テンプレートに追加します。
複数のストレージ プロファイルを追加するには、この手順を繰り返します。
- （オプション）[選択されているストレージ プロファイル] リストからストレージ プロファイルを選択し、[削除] をクリックして、仮想データセンター テンプレートから削除します。
複数のストレージ プロファイルを削除するには、この手順を繰り返します。
- [選択されているストレージ プロファイル] リストに少なくとも 1 つストレージ プロファイルがあることを確認し、[次へ] をクリックします。

ネットワーク プールの構成

ネットワーク プールは、vApp ネットワークと内部の組織仮想データセンター 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。仮想データセンター テンプレートを構成して、インストール環境中のネットワーク プールに自動的に接続できます。また、ネットワーク プールに接続しないことも可能です。

注： vCloud Director は、NSX Data Center for vSphere によってバックアップされる仮想データセンターの組織仮想データセンター テンプレートをサポートしています。

手順

- 1 仮想データセンターをどのようにネットワーク プールに接続するか選択します。

オプション	説明
自動 (推奨)	vCloud Director は、テンプレートをインスタンス化する時に、自動的に仮想データセンターをネットワーク プールに接続します。
なし	テンプレートをインスタンス化する時に、仮想データセンターはネットワーク プールに接続されません。

- 2 [次へ] をクリックします。

Edge ゲートウェイの構成

テンプレートから作成された組織仮想データセンター内でルーティングされたネットワーク通信が有効になるように Edge ゲートウェイを構成します。

手順

- 1 (オプション) [新規の Edge ゲートウェイの作成] を選択し、テンプレート内で Edge ゲートウェイを作成および構成します。
- 2 新しい Edge ゲートウェイの名前を入力し、必要に応じて説明も入力します。
- 3 Edge ゲートウェイの構成を選択します。

オプション	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] オプション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 [特大] 構成では、同じセキュリティ機能が提供されます。
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適しています。
超特大	高いスループットと高い接続速度を必要とする環境に適しています。

このオプションは、新規の Edge ゲートウェイの作成を選択した場合にのみ表示されます。Edge ゲートウェイを導入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』の「NSX のシステム要件」を参照してください。

- 4 バックアップ ゲートウェイへの自動フェイルオーバーを有効化するには、[高可用性を有効にする] を選択します。
- 5 DNS リレーに選択されたデフォルト ゲートウェイを使用するには、[DNS リレーにデフォルト ゲートウェイを使用] を選択します。
- 6 [次へ] をクリックします。

新規 Edge ゲートウェイ上のネットワーク設定の構成

新規 Edge ゲートウェイ上の外部ネットワークの IP 設定を構成します。

このページは、ゲートウェイの構成時に、[新規の Edge ゲートウェイの作成] を選択した場合にのみ表示されます。

手順

- 1 [IP 設定の構成] ページで、[IP 割り当ての変更] をクリックします。
- 2 IP アドレスを指定するそれぞれの外部ネットワークについて、ドロップダウン メニューから [手動] を選択します。
- 3 [手動] に設定するそれぞれの外部ネットワークの IP アドレスを入力し、[次へ] をクリックします。

アクセス リストの構成

組織を仮想データセンター テンプレートのアクセス リストに追加すると、これらの組織がテンプレートから仮想データセンターをインスタンス化できるようになります。

手順

- 1 [利用可能な組織] リストから組織を選択し、[追加] をクリックして、組織を仮想データセンター テンプレートのアクセス リストに追加します。

複数の組織をアクセス リストに追加する場合は、この手順を繰り返します。

- 2 [選択されている組織] リストから組織を選択し、[削除] をクリックして、組織を仮想データセンター アクセス リストから削除します。

複数の組織をアクセス リストから削除する場合は、この手順を繰り返します。

- 3 [次へ] をクリックします。

組織仮想データセンター テンプレートの命名

システムや、テンプレートにアクセスする各組織で使用する仮想データセンターの記述名とオプションの説明を提供します。

手順

- 1 仮想データセンター テンプレートの [システム名] を入力します。

これは、システムの仮想データセンター テンプレート リストに表示される名前です。

- 2 (オプション) 仮想データセンター テンプレートの [システムの説明] を入力します。

これは、システムの仮想データセンター テンプレートのリストに表示される説明です。

- 3 仮想データセンター テンプレートの [テナント名] を入力します。

- 4 (オプション) その仮想データセンター テンプレートにアクセスできる組織に、システムの説明と異なる説明を表示させたい場合は、仮想データセンターの [テナントの説明] を入力します。

- 5 [次へ] をクリックします。

組織仮想データセンター テンプレート設定の確認

仮想データセンター テンプレートに対して入力した設定をレビューして確認します。

手順

- 1 仮想データセンター テンプレートの設定を確認します。

- 2 (オプション) [戻る] をクリックして設定を変更します。
- 3 [完了] をクリックします。

組織仮想データセンター テンプレートのインスタンス化

仮想データセンター テンプレートから新しい組織仮想データセンターを作成するには、仮想データセンター テンプレートをインスタンス化します。

前提条件

新しい組織仮想データセンターの作成対象となる組織が仮想データセンター テンプレートにアクセスできることを確認します。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織 VDC テンプレート] をクリックします。
- 2 インスタンス化する仮想データセンター テンプレートを右クリックして、[インスタンス化] を選択します。
- 3 新しい組織仮想データセンターの[名前]と、任意で[説明]を入力し、[完了] をクリックします。

組織仮想データセンター テンプレートの修正

名前と説明、割り当てモデルの設定、ストレージ設定およびネットワーク設定など、既存の仮想データセンター テンプレートのプロパティを編集できます。

手順

- 1 **新規仮想データセンター テンプレート編集ウィザードを開く**
仮想データセンター テンプレートを修正するプロセスを開始するには、仮想データセンター テンプレート編集ウィザードを開きます。
- 2 **プロバイダ仮想データセンターと外部ネットワークの選択**
組織仮想データセンターは、使用するコンピューティング リソースとストレージ リソースをプロバイダ仮想データセンターから取得します。組織仮想データセンターは、これらのリソースを、組織内の vApp と仮想マシンに提供します。
- 3 **割り当てモデルの選択**
割り当てモデルにより、管理者が割り当てるプロバイダ仮想データセンターのコンピューティング リソースとメモリ リソースが組織仮想データセンターにコミットされる方法とタイミングが決定されます。
- 4 **割り当てモデルの構成**
割り当てモデルを構成して、組織仮想データセンターに割り当てるプロバイダ仮想データセンター リソースの量を指定します。
- 5 **ストレージ プロファイルの構成**
組織仮想データセンターでは、vApp および vApp テンプレートのためのストレージ領域が必要です。プロバイダ仮想データセンターのデータストアで使用可能な領域から、ストレージを割り当てることができます。

6 ネットワーク プールの構成

ネットワーク プールは、vApp ネットワークと内部の組織仮想データセンター 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。仮想データセンター テンプレートを構成して、インストール環境中のネットワーク プールに自動的に接続できます。また、ネットワーク プールに接続しないことも可能です。

7 Edge ゲートウェイの構成

テンプレートから作成された組織仮想データセンター内でルーティングされたネットワーク通信が有効になるように Edge ゲートウェイを構成します。

8 新規 Edge ゲートウェイ上のネットワーク設定の構成

新規 Edge ゲートウェイ上の外部ネットワークの IP 設定を構成します。

9 アクセス リストの構成

組織を仮想データセンター テンプレートのアクセス リストに追加すると、これらの組織がテンプレートから仮想データセンターをインスタンス化できるようになります。

10 組織仮想データセンター テンプレートの命名

システムや、テンプレートにアクセスする各組織で使用する仮想データセンターの記述名とオプションの説明を提供します。

11 組織仮想データセンター テンプレート設定の確認

仮想データセンター テンプレートに対して入力した設定をレビューして確認します。

新規仮想データセンター テンプレート編集ウィザードを開く

仮想データセンター テンプレートを修正するプロセスを開始するには、仮想データセンター テンプレート編集ウィザードを開きます。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織 VDC テンプレート] をクリックします。
- 2 修正する仮想データセンター テンプレートを右クリックして、[プロパティ] を選択します。

プロバイダ仮想データセンターと外部ネットワークの選択

組織仮想データセンターは、使用するコンピューティング リソースとストレージ リソースをプロバイダ仮想データセンターから取得します。組織仮想データセンターは、これらのリソースを、組織内の vApp と仮想マシンに提供します。

手順

- 1 プロバイダ仮想データセンターと外部ネットワークを仮想データセンター テンプレートに追加するには、上部のリストからプロバイダ仮想データセンターと外部ネットワークのペアを選択し、[追加] をクリックします。

このテンプレートに基づく組織仮想データセンターは、選択されたプロバイダ仮想データセンターと外部ネットワークを使用します。各プロバイダ仮想データセンターに対して、外部ネットワークは1つしか構成できません。

注： vCloud Director は、NSX Data Center for vSphere によってバックアップされる仮想データセンターの組織仮想データセンター テンプレートをサポートしています。

- 2 [次へ] をクリックします。

割り当てモデルの選択

割り当てモデルにより、管理者が割り当てるプロバイダ仮想データセンターのコンピューティング リソースとメモリ リソースが組織仮想データセンターにコミットされる方法とタイミングが決定されます。

前提条件

どの割り当てモデルが環境に適しているかについて理解していることを確認します。[割り当てモデルについて](#)を参照してください。

手順

- 1 割り当てモデルを選択します。

オプション	説明
割り当てプール	プロバイダ仮想データセンターから割り当てるリソースの割合は、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。
従量課金制	リソースは、組織仮想データセンターでユーザーが vApp を作成するときのみコミットされます。
予約プール	割り当てるすべてのリソースは、組織仮想データセンターに直ちにコミットされます。

配置エンジンおよび仮想マシンの共有、レートおよび制限の詳細については、『vCloud Director ユーザー ガイド』を参照してください。

- 2 [次へ] をクリックします。

割り当てモデルの構成

割り当てモデルを構成して、組織仮想データセンターに割り当てるプロバイダ仮想データセンター リソースの量を指定します。

手順

1 割り当てモデルのオプションを選択します。

モデルによっては、一部のオプションが含まれていないものもあります。

オプション	アクション
CPU の割り当て	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 の最大使用量を GHz 単位で入力します。このオプションは、割り当てプールと予約プールの割り当てモデルの場合にのみ指定できます。予約プール モデルに含まれる [CPU リソースを予約値を超えて拡張できるようにします。] チェック ボックスでは、仮想データセンターが CPU リソースを上限なしで提供できるかどうかを選択できます。
確保された CPU 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保証する CPU リソースの割合を入力します。100% 未満を保証すると、リソースをオーバーコミットできます。このオプションは、割り当てプールと従量課金制の割り当てモデルの場合にのみ指定できます。割り当てプールのデフォルト値は 50% で、従量課金制のデフォルトは 20% です。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。
vCPU 速度	vCPU 速度を GHz 単位で入力します。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。このオプションは、割り当てプールと従量課金制の割り当てモデルの場合にのみ指定できます。
メモリの割り当て	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使用量を GB 単位で入力します。このオプションは、割り当てプールと予約プールの割り当てモデルの場合にのみ指定できます。
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保証するメモリ リソースの割合を入力します。100% 未満を保証すると、リソースをオーバーコミットできます。このオプションは、割り当てプールと従量課金制の割り当てモデルの場合にのみ指定できます。割り当てプールのデフォルトは 50% で、従量課金制のデフォルトは 20% です。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。
最大仮想マシン数	組織仮想データセンターで作成可能な仮想マシンの最大数を入力します。

2 [次へ] をクリックします。

例：割り当てモデルの構成

組織仮想データセンターを作成すると、vCloud Director は、指定される割り当てモデルの設定に基づいて vSphere リソース プールを作成します。

表 5-10. 単ークラスターの割り当てプール機能が有効になっている場合の割り当てプール設定によるリソース プール設定への影響

割り当てプール設定	割り当てプール値	リソース プール設定	リソース プール値
CPU の割り当て	25 GHz	CPU 制限	25 GHz
CPU % の保証	10%	CPU の予約	2.5GHz
メモリの割り当て	50 GB	メモリの制限	50 GB
メモリ % の保証	20%	メモリの予約	10GB

表 5-11. 単ークラスタの割り当てプール機能が無効になっている場合の割り当てプール設定によるリソース プール設定への影響

割り当てプール設定	割り当てプール値	リソース プール設定	サブリソース プール値	すべてのサブリソース プールでこの組織仮想データセンターにコミットされた値
CPU の割り当て	25 GHz	CPU 制限	vCPU の合計数に、関連付けられているすべての仮想マシンの vCPU 周波数を掛けた値	該当なし
CPU % の保証	10%	CPU の予約	関連付けられているすべての仮想マシンの vCPU の数に、vCPU 周波数、CPU の割合保証を掛けた合計値	2.5GHz
メモリの割り当て	50 GB	メモリの制限	関連付けられているすべての仮想マシンの構成済みのメモリ サイズの合計	該当なし
メモリ % の保証	20%	メモリの予約	構成済みのメモリ サイズの合計に、関連付けられているすべての仮想マシンのメモリの割合の保証を掛けた値	10GB

表 5-12. 従量課金制の設定によるリソース プール設定への影響

従量課金制の設定	従量課金制の値	リソース プール設定	リソース プール値
CPU % の保証	10%	CPU の予約、CPU の制限	0.00GHz、無制限
メモリ % の保証	100%	メモリの予約、メモリの制限	0.00 GB、無制限

従量課金制の組織仮想データセンターをサポートするために作成されるリソース プールには、予約または制限がありません。従量課金制の設定は、オーバーコミットにのみ影響を与えます。100% 保証とは、オーバーコミットの可能性があることを意味します。割合が低いほど、オーバーコミットの可能性が高くなります。

表 5-13. 予約プール設定によるリソース プール設定への影響

予約プール設定	予約プール値	リソース プール設定	リソース プール値
CPU の割り当て	25 GHz	CPU の予約、CPU の制限	25GHz、25GHz
メモリの割り当て	50 GB	メモリの予約、メモリの制限	50 GB、50 GB

ストレージ プロファイルの構成

組織仮想データセンターでは、vApp および vApp テンプレートのためのストレージ領域が必要です。プロバイダ仮想データセンターのデータストアで使用可能な領域から、ストレージを割り当てることができます。

手順

- 1 (オプション) [利用可能なストレージ プロファイル] リストからストレージ プロファイルを選択し、[追加] をクリックして、仮想データセンター テンプレートに追加します。

複数のストレージ プロファイルを追加するには、この手順を繰り返します。

- 2 (オプション) [選択されているストレージ プロファイル] リストからストレージ プロファイルを選択し、[削除] をクリックして、仮想データセンター テンプレートから削除します。

複数のストレージ プロファイルを削除するには、この手順を繰り返します。

- 3 [選択されているストレージ プロファイル] リストに少なくとも 1 つストレージ プロファイルがあることを確認し、[次へ] をクリックします。

ネットワーク プールの構成

ネットワーク プールは、vApp ネットワークと内部の組織仮想データセンター 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。仮想データセンター テンプレートを構成して、インストール環境中のネットワーク プールに自動的に接続できます。また、ネットワーク プールに接続しないことも可能です。

注： vCloud Director は、NSX Data Center for vSphere によってバックアップされる仮想データセンターの組織仮想データセンター テンプレートをサポートしています。

手順

- 1 仮想データセンターをどのようにネットワーク プールに接続するか選択します。

オプション	説明
自動 (推奨)	vCloud Director は、テンプレートをインスタンス化する時に、自動的に仮想データセンターをネットワーク プールに接続します。
なし	テンプレートをインスタンス化する時に、仮想データセンターはネットワーク プールに接続されません。

- 2 [次へ] をクリックします。

Edge ゲートウェイの構成

テンプレートから作成された組織仮想データセンター内でルーティングされたネットワーク通信が有効になるように Edge ゲートウェイを構成します。

手順

- 1 (オプション) [新規の Edge ゲートウェイの作成] を選択し、テンプレート内で Edge ゲートウェイを作成および構成します。
- 2 新しい Edge ゲートウェイの名前を入力し、必要に応じて説明も入力します。
- 3 Edge ゲートウェイの構成を選択します。

オプション	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] オプション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 [特大] 構成では、同じセキュリティ機能が提供されます。
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適しています。
超特大	高いスループットと高い接続速度を必要とする環境に適しています。

このオプションは、新規の Edge ゲートウェイの作成を選択した場合にのみ表示されます。Edge ゲートウェイを導入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』の「NSX のシステム要件」を参照してください。

- 4 バックアップ ゲートウェイへの自動フェイルオーバーを有効化するには、[高可用性を有効にする] を選択します。
- 5 DNS リレーに選択されたデフォルト ゲートウェイを使用するには、[DNS リレーにデフォルト ゲートウェイを使用] を選択します。
- 6 [次へ] をクリックします。

新規 Edge ゲートウェイ上のネットワーク設定の構成

新規 Edge ゲートウェイ上の外部ネットワークの IP 設定を構成します。

このページは、ゲートウェイの構成時に、[新規の Edge ゲートウェイの作成] を選択した場合にのみ表示されます。

手順

- 1 [IP 設定の構成] ページで、[IP 割り当ての変更] をクリックします。
- 2 IP アドレスを指定するそれぞれの外部ネットワークについて、ドロップダウン メニューから [手動] を選択します。
- 3 [手動] に設定するそれぞれの外部ネットワークの IP アドレスを入力し、[次へ] をクリックします。

アクセス リストの構成

組織を仮想データセンター テンプレートのアクセス リストに追加すると、これらの組織がテンプレートから仮想データセンターをインスタンス化できるようになります。

手順

- 1 [利用可能な組織] リストから組織を選択し、[追加] をクリックして、組織を仮想データセンター テンプレートのアクセス リストに追加します。

複数の組織をアクセス リストに追加する場合は、この手順を繰り返します。

- 2 [選択されている組織] リストから組織を選択し、[削除] をクリックして、組織を仮想データセンター アクセス リストから削除します。

複数の組織をアクセス リストから削除する場合は、この手順を繰り返します。

- 3 [次へ] をクリックします。

組織仮想データセンター テンプレートの命名

システムや、テンプレートにアクセスする各組織で使用する仮想データセンターの記述名とオプションの説明を提供します。

手順

- 1 仮想データセンター テンプレートの [システム名] を入力します。

これは、システムの仮想データセンター テンプレート リストに表示される名前です。

- 2 (オプション) 仮想データセンター テンプレートの [システムの説明] を入力します。

これは、システムの仮想データセンター テンプレートのリストに表示される説明です。

- 3 仮想データセンター テンプレートの [テナント名] を入力します。
- 4 (オプション) その仮想データセンター テンプレートにアクセスできる組織に、システムの説明と異なる説明を表示させたい場合は、仮想データセンターの [テナントの説明] を入力します。
- 5 [次へ] をクリックします。

組織仮想データセンター テンプレート設定の確認

仮想データセンター テンプレートに対して入力した設定をレビューして確認します。

手順

- 1 仮想データセンター テンプレートの設定を確認します。
- 2 (オプション) [戻る] をクリックして設定を変更します。
- 3 [完了] をクリックします。

組織仮想データセンター テンプレートのクローン作成

仮想データセンター テンプレートをクローン作成すると、既存の仮想データセンター テンプレートに基づいて新しい仮想データセンター テンプレートを作成することができます。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織 VDC テンプレート] をクリックします。
- 2 インスタンス化する仮想データセンターを右クリックして、[クローン作成] を選択します。
- 3 左側のペインで [この VDC テンプレートの名前前の設定] をクリックし、新しい仮想データセンター テンプレートの [システム名] を入力します。
- 4 (オプション) 左側のペインの設定のいずれかをクリックすると、その設定を修正することができます。

新しい仮想データセンター テンプレートでは、修正されていない設定が元の仮想データセンター テンプレートから保持されます。

- 5 [完了] をクリックします。

組織仮想データセンター テンプレートの削除

仮想データセンター テンプレートをシステムから削除することができます。仮想データセンター テンプレートの削除は、テンプレートからすでに作成されている仮想データセンターには影響を与えません。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織 VDC テンプレート] をクリックします。
- 2 削除する仮想データセンターを右クリックして、[削除] をクリックします。

外部ネットワークの管理

外部ネットワークを作成すると、ネットワーク仕様の追加と削除、バックリング vSphere ネットワークの追加と削除、およびその他の大部分のネットワーク プロパティの変更が可能になります。

vCloud Director は、IPv4 および IPv6 の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。

外部ネットワークの名前および説明の変更

vCloud Director のインストール環境の規模が大きくなるにつれて、既存の外部ネットワークによりわかりやすい名前または説明を割り当てる必要がある場合があります。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [外部ネットワーク] をクリックします。
- 2 外部ネットワーク名を右クリックし、[プロパティ] を選択します。
- 3 [名前と説明] タブで新しい名前と説明を入力し、[OK] をクリックします。

外部ネットワーク仕様の表示と変更

外部ネットワークの既存のサブネット仕様を表示および変更できます。たとえば、IP アドレス範囲と IP アドレスを IP アドレス プールに追加できます。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [外部ネットワーク] をクリックします。
- 2 外部ネットワーク名を右クリックし、[プロパティ] を選択します。
- 3 [ネットワーク仕様] タブをクリックします。

Classless Inter-Domain Routing (CIDR) 設定、DNS 設定、および IP アドレス プールを使用して現在のサブネットを表示できます。

ネットワーク CIDR の形式は *network_gateway_IP_address/subnet_prefix_length* で、たとえば **192.167.1.1/24** のようになります。

- 4 サブネットの仕様を変更するには、ターゲット サブネットの行を選択し、[変更] をクリックします。
- 5 設定と IP アドレス プールを変更し、[OK] をクリックします。
- 6 [OK] をクリックします。

外部ネットワーク仕様の追加

外部ネットワークにサブネット仕様を追加できます。

外部ネットワークのタイプに関係なく、IPv4 または IPv6 サブネットを追加することができます。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [外部ネットワーク] をクリックします。
- 2 外部ネットワーク名を右クリックし、[プロパティ] を選択します。
- 3 [ネットワークの仕様] タブで [追加] をクリックします。
- 4 使用する外部ネットワーク仕様の [ネットワーク CIDR] 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。
- 5 (オプション) 使用する外部ネットワーク仕様の [プライマリ DNS]、[セカンダリ DNS]、および [DNS サフィックス] を入力します。
- 6 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。
複数の IP アドレス範囲または IP アドレスはキャリッジ リターンで区切ります。
- 7 [OK] をクリックします。

外部ネットワークをバックアップする vSphere ネットワークの編集

システムに複数の vCenter サーバと vSphere ネットワークが含まれている場合は、外部ネットワークをバックアップする vSphere ネットワークの指定を変更できます。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [外部ネットワーク] をクリックします。
- 2 外部ネットワークを右クリックし、[プロパティ] を選択します。
- 3 [vSphere ネットワーク] タブをクリックします。
- 4 この外部ネットワークをバックアップする vSphere ネットワークの設定を変更するには、[編集] をクリックします。
- 5 複数の vCenter サーバが一覧表示されている場合は、vCenter サーバと vSphere ネットワークを選択して、[追加] または [削除] をクリックします。
外部ネットワークをバックアップするすべての vSphere ネットワークが同じ種類のスイッチ (DVSwitch または 標準スイッチ) を経由して接続されている必要があります。各 vCenter サーバから選択できる vSphere ネットワークは 1 つのみです。現在使用中のバックアップ ネットワークを削除することはできません。
- 6 vCenter サーバと、この外部ネットワークをバックアップする vSphere ネットワークの編集が完了したら、[OK] をクリックします。

外部ネットワークの削除

外部ネットワークを削除して vCloud Director から削除します。

前提条件

外部ネットワークを削除するには、事前にそのネットワークに依存する Edge ゲートウェイと組織仮想データセンター ネットワークをすべて削除する必要があります。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [外部ネットワーク] をクリックします。
- 2 外部ネットワーク名を右クリックし、[ネットワークを削除] を選択します。

Edge ゲートウェイの管理

Edge ゲートウェイは、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、ロードバランス化、ネットワーク アドレス変換およびファイアウォールなどのサービスを提供できます。vCloud Director は、IPv4 および IPv6 の Edge ゲートウェイをサポートします。

Edge ゲートウェイを使用するには、NSX Data Center for vSphere が必要です。詳細については、『NSX 管理ガイド』を参照してください。

vCloud 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。 [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。を参照してください。

重要： バージョン 9.7 以降では、vCloud 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。

Edge クラスタの操作

vCloud Director 9.7 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 オブジェクトが導入されています。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。

バージョン vCloud Director 9.7 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 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 vCloud 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、vCloud OpenAPI `EdgeClusters` メソッドを使用する必要があります。<https://code.vmware.com> にある vCloud 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とは、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、vCloud OpenAPI `VdcNetworkProfile` メソッドを使用する必要があります。<https://code.vmware.com> にある vCloud 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 ゲートウェイの追加

Edge Gateway は、経路指定された組織仮想データセンター ネットワークに経路指定およびその他のサービスを提供します。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、スタティック ルーティングをサポートします。

前提条件

- 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。 [Edge クラスタの操作](#)を参照してください。

手順**1 新規 Edge ゲートウェイ ウィザードの起動**

新規 Edge ゲートウェイ ウィザードを起動して、組織仮想データセンターに Edge ゲートウェイを追加するプロセスを開始します。

2 新規 Edge ゲートウェイのゲートウェイおよび IP 構成オプションの選択

1 つ以上の物理ネットワークに接続できるように、Edge ゲートウェイを構成します。

3 新規 Edge ゲートウェイの外部ネットワークの選択

Edge ゲートウェイが接続できる外部ネットワークを選択します。

4 新規 Edge ゲートウェイ上の IP 設定の構成

新規 Edge ゲートウェイ上の外部ネットワークの IP 設定を構成します。

5 新規 Edge ゲートウェイ上の IP プールの細分割り当て

Edge ゲートウェイ上の外部ネットワークが提供する IP プールを複数の固定 IP プールに細分割り当てします。

6 新規 Edge ゲートウェイ上のレート制限の構成

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します。

7 新規 Edge ゲートウェイの名前と説明の構成

Edge ゲートウェイの名前と、必要に応じて説明を入力します。

8 新規 Edge ゲートウェイの構成の確認

追加プロセスを完了する前に、Edge ゲートウェイの構成を確認します。

新規 Edge ゲートウェイ ウィザードの起動

新規 Edge ゲートウェイ ウィザードを起動して、組織仮想データセンターに Edge ゲートウェイを追加するプロセスを開始します。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織 VDC] をクリックします。
- 2 組織仮想データセンター名をダブルクリックし、組織仮想データセンターを開きます。
- 3 [Edge ゲートウェイ] タブをクリックし、追加ボタンをクリックします。

結果

新規 Edge ゲートウェイ ウィザードが起動します。

新規 Edge ゲートウェイのゲートウェイおよび IP 構成オプションの選択

1 つ以上の物理ネットワークに接続できるように、Edge ゲートウェイを構成します。

前提条件

IP プールを細分割り当てする場合は、Edge Gateway に割り当てる IP アドレスが vCloud Director の外部で使用されていないことを確認します。

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。vCloud 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 vCloud 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 システム リソースに基づいて Edge ゲートウェイ構成を選択します。

オプション	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 [特大] 構成では、同じセキュリティ機能が提供されます。
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適しています。
超特大	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。

Edge ゲートウェイを導入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』の「NSX のシステム要件」を参照してください。

- 2 (オプション) 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するには、[高可用性を有効にする] を選択します。

- 3 (オプション) [分散ルーティングの有効化] を選択し、分散論理ルーティングを提供するように詳細ゲートウェイを設定します。

このオプションは、[詳細ゲートウェイとして作成] を選択する場合にのみ使用できます。分散ルーティングを有効にすると、はるかに多くの組織 VDC ネットワークをゲートウェイに作成できます。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。

- 4 (オプション) [FIPS モードの有効化] を選択して、Edge Gateway で NSX の FIPS モードを使用できるように設定します。

このオプションは、システム管理者が Edge Gateway での FIPS モードの有効化を許可している場合にのみ使用できます。NSX 6.3 以降が必要です。[全般システム設定](#)を参照してください。FIPS モードの詳細については、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。

- 5 (オプション) [IP 設定の構成] を選択し、外部インターフェイスの IP アドレスを手動で構成します。
- 6 (オプション) [IP プールの細分割り当て] を選択し、使用するゲートウェイ サービスの一連の IP アドレスを割り当てます。
- 7 (オプション) [レート制限の構成] を選択し、外部接続された各インターフェイスの着信および発信のレート制限を選択します。
- 8 [次へ] をクリックします。

新規 Edge ゲートウェイの外部ネットワークの選択

Edge ゲートウェイが接続できる外部ネットワークを選択します。

Edge クラスタを組織 VDC に割り当てた場合は、ここにアクセスできる外部ネットワークを選択する必要があります。[Edge クラスタの操作](#)を参照してください。

手順

- 1 リストから外部ネットワークを選択して [追加] をクリックします。
複数のネットワークを選択するには、Ctrl キーを押しながら操作します。
- 2 [デフォルト ゲートウェイ] にするネットワークを選択します。
- 3 (オプション) [DNS リレーのデフォルトのゲートウェイを使用します]を選択します。
- 4 [次へ] をクリックします。

新規 Edge ゲートウェイ上の IP 設定の構成

新規 Edge ゲートウェイ上の外部ネットワークの IP 設定を構成します。

このページは、ゲートウェイの構成中に [IP 設定の構成] を選択した場合にのみ表示されます。

手順

- 1 [IP 設定の構成] ページで、[IP 割り当ての変更] をクリックします。

- 2 IP アドレスを指定するそれぞれの外部ネットワークについて、ドロップダウン メニューから [手動] を選択します。
- 3 [手動] に設定するそれぞれの外部ネットワークの IP アドレスを入力し、[次へ] をクリックします。

新規 Edge ゲートウェイ上の IP プールの細分割り当て

Edge ゲートウェイ上の外部ネットワークが提供する IP プールを複数の固定 IP プールに細分割り当てします。

このページは、ゲートウェイの構成中に [IP プールの細分割り当て] を選択した場合にのみ表示されます。

前提条件

Edge Gateway に割り当てる IP アドレスが vCloud Director の外部で使用されていないことを確認します。

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。vCloud 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 vCloud 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 外部ネットワークと細分割り当てする IP プールを選択します。
- 2 IP プールの範囲内の IP アドレスまたは IP アドレスの範囲を入力し、[追加] をクリックします。
この手順を繰り返し、細分割り当てされた複数の IP プールを追加します。
- 3 (オプション) 細分割り当てされた IP プールを選択し、[変更] をクリックして、細分割り当てされた IP プールの IP アドレスの範囲を変更します。
- 4 (オプション) 細分割り当てされた IP プールを選択し、[削除] をクリックして、細分割り当てされた IP プールを削除します。
- 5 [次へ] をクリックします。

新規 Edge ゲートウェイ上のレート制限の構成

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します。

このページは、ゲートウェイの構成中に [レート制限の構成] を選択した場合にのみ表示されます。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 レート制限を有効化するそれぞれの外部ネットワークに対して [有効化] をクリックします。
- 2 有効化されたそれぞれの外部ネットワークに対し、[着信のレート制限] を 1 秒あたりのギガビットで入力します。
- 3 有効化されたそれぞれの外部ネットワークに対し、[発信のレート制限] を 1 秒あたりのギガビットで入力し、[次へ] をクリックします。

新規 Edge ゲートウェイの名前と説明の構成

Edge ゲートウェイの名前と、必要に応じて説明を入力します。

手順

- 1 Edge ゲートウェイの [名前] を入力します。
- 2 (オプション) Edge ゲートウェイの [説明] を入力します。
- 3 [次へ] をクリックします。

新規 Edge ゲートウェイの構成の確認

追加プロセスを完了する前に、Edge ゲートウェイの構成を確認します。

手順

- 1 新規 Edge ゲートウェイの設定を確認し、それらが正しいことを確認します。
- 2 (オプション) [戻る] をクリックして変更します。
- 3 [完了] をクリックします。

Edge ゲートウェイから詳細ゲートウェイへの変換

Edge ゲートウェイを詳細ゲートウェイに変換した後は、vCloud Director テナント ポータルを使用してゲートウェイ上の NSX services を構成できます。

前提条件

Edge ゲートウェイを詳細ゲートウェイに変換できるのは、システム管理者または組織管理者のみです。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [Edge ゲートウェイ] をクリックします。
- 2 [Edge ゲートウェイ] タブで Edge ゲートウェイ名を右クリックし、[詳細ゲートウェイに変換] を選択します。
選択の確認を求めるプロンプトが表示された後、ゲートウェイの変換が実行されます。

重要： Edge ゲートウェイの変換後、既存の vCloud API クライアントは Edge ゲートウェイで一部の操作を完了できなくなる場合があります。<http://kb.vmware.com/kb/2147625> を参照してください。

詳細ゲートウェイで分散ルーティングを有効または無効にする

Edge ゲートウェイを詳細ゲートウェイに変換した後、このゲートウェイで vCloud Director 分散ルーティングの実行を有効にできます。

Edge ゲートウェイで vCloud Director 分散ルーティングを有効にすると、はるかに多くの組織 VDC ネットワークをゲートウェイに作成できます。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に最適化されます。

前提条件

- vCloud Director によって使用される NSX インストール環境は、1 台以上の NSX Controller ノードで構成される必要があります。『vCloud 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。
- システム管理者、または [組織 VDC ゲートウェイ: 分散ルーティングの有効化] の権限が含まれたロールのユーザーであることが必要です。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [Edge ゲートウェイ] をクリックします。
- 2 [Edge ゲートウェイ] タブで、Edge ゲートウェイ名を右クリックし、[分散ルーティングの有効化] を選択します。

分散ルーティングがすでに有効である場合は、[分散ルーティングの有効化] オプションの代わりに、[分散ルーティングの無効化] オプションが表示されます。

選択を確認するプロンプトが表示され、この機能が有効または無効になります。

Edge ゲートウェイ 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。

Edge Gateway の名前を右クリックして [Edge ゲートウェイ サービス] を選択すると、vCloud Director テナント ポータル内の [NSX Edge ゲートウェイ サービスの構成] ページにリダイレクトされます。vCloud Director テナントの高度なネットワーク機能の管理の詳細については、vCloud Director Tenant Portal Guide を参照してください。

Edge ゲートウェイのプロパティの編集

高可用性、外部ネットワーク設定、IP プールおよびレート制限など、既存の Edge ゲートウェイの設定を変更できます。

- [Edge ゲートウェイの高可用性の有効化](#)
高可用性について Edge ゲートウェイを構成できます。
- [Edge ゲートウェイ上の外部ネットワークの構成](#)
Edge ゲートウェイに接続されている外部ネットワークを追加または削除します。
- [Edge ゲートウェイ上の外部ネットワーク IP 設定の構成](#)
Edge ゲートウェイ上の外部インターフェイスの IP アドレスを変更します。
- [Edge ゲートウェイ上の IP プールの細分割り当て](#)
Edge ゲートウェイ上の外部ネットワークが提供する IP プールを複数の固定 IP プールに細分割り当てします。
- [Edge ゲートウェイ上のレート制限の構成](#)
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します。

Edge ゲートウェイの高可用性の有効化

高可用性について Edge ゲートウェイを構成できます。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織 VDC] をクリックします。
- 2 組織仮想データセンター名をダブルクリックし、組織仮想データセンターを開きます。
- 3 [Edge ゲートウェイ] タブをクリックし、Edge ゲートウェイ名を右クリックし、[プロパティ] を選択します。
- 4 [全般] タブをクリックし、[HA の有効化] を選択します。

Edge ゲートウェイ上の外部ネットワークの構成

Edge ゲートウェイに接続されている外部ネットワークを追加または削除します。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織 VDC] をクリックします。
- 2 組織仮想データセンター名をダブルクリックし、組織仮想データセンターを開きます。
- 3 [Edge ゲートウェイ] タブをクリックし、Edge ゲートウェイ名を右クリックし、[プロパティ] を選択します。
- 4 [外部ネットワーク] タブをクリックします。
- 5 (オプション) トップのリストから外部ネットワークを選択し、[追加] をクリックして外部ネットワークを Edge ゲートウェイに追加します。
複数のネットワークを選択するには、Ctrl キーを押しながら操作します。
- 6 (オプション) トップのリストから外部ネットワークを選択し、[削除] をクリックして外部ネットワークを Edge ゲートウェイから削除します。
複数のネットワークを選択するには、Ctrl キーを押しながら操作します。
- 7 [デフォルト ゲートウェイ] にするネットワークを選択します。
- 8 (オプション) [DNS リレーのデフォルトのゲートウェイを使用します]を選択します。
- 9 [OK] をクリックします。

Edge ゲートウェイ上の外部ネットワーク IP 設定の構成

Edge ゲートウェイ上の外部インターフェイスの IP アドレスを変更します。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織 VDC] をクリックします。
- 2 組織仮想データセンター名をダブルクリックし、組織仮想データセンターを開きます。
- 3 [Edge ゲートウェイ] タブをクリックし、Edge ゲートウェイ名を右クリックし、[プロパティ] を選択します。
- 4 [IP 設定の構成] タブをクリックし、[IP 割り当ての変更] をクリックします。

- 5 IP アドレスを指定するそれぞれの外部ネットワークについて、ドロップダウン メニューから [手動] を選択します。
- 6 [手動] に設定されたそれぞれの外部ネットワークの新しい IP アドレスを入力し、[OK] をクリックします。

Edge ゲートウェイ上の IP プールの細分割り当て

Edge ゲートウェイ上の外部ネットワークが提供する IP プールを複数の固定 IP プールに細分割り当てします。

前提条件

Edge Gateway に割り当てる IP アドレスが vCloud Director の外部で使用されていないことを確認します。

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。vCloud 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 vCloud 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 [管理および監視] タブをクリックし、左側のペインで [組織 VDC] をクリックします。
- 2 組織仮想データセンター名をダブルクリックし、組織仮想データセンターを開きます。
- 3 [Edge ゲートウェイ] タブをクリックし、Edge ゲートウェイ名を右クリックし、[プロパティ] を選択します。
- 4 [IP プールの細分割り当て] タブをクリックします。
- 5 外部ネットワークと細分割り当てする IP プールを選択します。
- 6 (オプション) IP プールの範囲内の IP アドレスまたは IP アドレスの範囲を入力し、[追加] をクリックして細分割り当てされた IP プールを追加します。
- 7 (オプション) 細分割り当てされた IP プールを選択し、[変更] をクリックして、細分割り当てされた IP プールの IP アドレスの範囲を変更します。
- 8 (オプション) 細分割り当てされた IP プールを選択し、[削除] をクリックして、細分割り当てされた IP プールを削除します。
- 9 [OK] をクリックします。

Edge ゲートウェイ上のレート制限の構成

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します。

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アップ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 [管理および監視] タブをクリックし、左側のペインで [組織 VDC] をクリックします。
- 2 組織仮想データセンター名をダブルクリックし、組織仮想データセンターを開きます。
- 3 [Edge ゲートウェイ] タブをクリックし、Edge ゲートウェイ名を右クリックし、[プロパティ] を選択します。
- 4 [レート制限の構成] タブをクリックします。

- 5 レート制限を有効化するそれぞれの外部ネットワークに対して [有効化] をクリックします。
- 6 有効化されたそれぞれの外部ネットワークに対し、[着信のレート制限] を 1 秒あたりのギガビットで入力します。
- 7 有効化されたそれぞれの外部ネットワークに対し、[発信のレート制限] を 1 秒あたりのギガビットで入力し、[OK] をクリックします。

Edge ゲートウェイのアップグレード

既存の Edge ゲートウェイをアップグレードしてゲートウェイの容量およびパフォーマンスを改善します。

前提条件

完全構成および高可用性を有効化して Edge ゲートウェイを完全-4 構成にアップグレードする場合には、ESXi に CPU が 8 個以上あることを確認してください。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織 VDC] をクリックします。
- 2 組織仮想データセンター名をダブルクリックし、組織仮想データセンターを開きます。
- 3 [Edge ゲートウェイ] タブをクリックし、Edge ゲートウェイ名を右クリックし、[アップグレード] を選択します。

結果

コンパクト構成の Edge ゲートウェイは完全構成にアップグレードされ、完全構成の Edge ゲートウェイは完全-4 構成にアップグレードされます。

次のステップ

コンパクト ゲートウェイを完全構成にアップグレードした場合には、アップグレード手順を繰り返して 完全-4 構成のゲートウェイにアップグレードします。

Edge ゲートウェイの削除

Edge ゲートウェイを削除することで、組織仮想データセンターからそれを削除できます。

前提条件

Edge ゲートウェイがバックアップしている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 [管理および監視] タブをクリックし、左側のペインで [組織 VDC] をクリックします。
- 2 組織仮想データセンター名をダブルクリックし、組織仮想データセンターを開きます。
- 3 [Edge ゲートウェイ] タブをクリックし、Edge ゲートウェイ名を右クリックし、[削除] を選択します。

Edge ゲートウェイの IP 使用の表示

Edge ゲートウェイ上の外部インターフェイスが現在使用している IP アドレスの一覧を表示できます。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織 VDC] をクリックします。
- 2 組織仮想データセンター名をダブルクリックし、組織仮想データセンターを開きます。
- 3 [Edge ゲートウェイ] タブをクリックし、Edge ゲートウェイ名を右クリックし、[外部 IP の割り当て] を選択します。

Edge ゲートウェイへの Syslog サーバー設定の適用

Edge ゲートウェイに Syslog サーバー設定を適用すると、ファイアウォール ルールのログ記録機能を有効化できます。

Syslog サーバー設定は、初回指定時以前に作成されたすべての Edge ゲートウェイに適用する必要があります。

Syslog サーバー設定は、設定変更が行われるたびに Edge ゲートウェイに適用してください。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織 VDC] をクリックします。
- 2 組織仮想データセンター名をダブルクリックし、組織仮想データセンターを開きます。
- 3 [Edge ゲートウェイ] タブをクリックし、Edge ゲートウェイ名を右クリックし、[Syslog サーバー設定の同期] を選択します。
- 4 [はい] をクリックします。

組織仮想データセンター ネットワークの管理

システム管理者および組織管理者は、経路指定された組織仮想データセンター ネットワークおよび隔離された組織仮想データセンター ネットワークの追加、削除、変更を行うことができます。直接ネットワークおよびクロス仮想データセンター組織の仮想データセンター ネットワークを追加、削除、変更できるのは、システム管理者のみです。

■ 組織仮想データセンターへのネットワークの追加

ネットワークを組織仮想データセンターに追加して、その仮想マシン間の相互通信やインターネットへのアクセスを可能にします。1つの組織仮想データセンターに複数のネットワークを追加できます。

■ 組織 VDC ネットワークのプロパティの表示または変更

組織 VDC ネットワークを作成した後は、その名前、説明、DNS 設定、共有、および固定 IP プールを変更できます。

■ 組織仮想データセンター ネットワーク サービスの構成

DHCP、ファイアウォール、ネットワーク アドレス変換 (NAT)、VPN などのサービスを、特定の組織仮想データセンター ネットワークに対して構成できます。組織管理者は、自分の組織仮想データセンター ネットワークに対していくつかのネットワーク サービスを構成することもできます。

■ 組織仮想データセンター ネットワークのリセット

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

■ 組織仮想データセンター ネットワークの接続、切断、移動

組織仮想データセンター ネットワークは、接続、切断、または移動することができます。

■ 組織仮想データセンター ネットワークを使用する vApp および vApp テンプレートの表示

組織仮想データセンター ネットワークに接続する NIC を持つ仮想マシンが含まれる、すべての vApp および vApp テンプレートのリストを表示することができます。vApp または vApp テンプレートが接続されている組織仮想データセンター ネットワークを削除することはできません。

■ 組織仮想データセンター ネットワークの削除

組織仮想データセンター ネットワークを削除し、組織仮想データセンターからそれを削除することができます。

■ 組織仮想データセンター ネットワークの IP 使用の表示

組織仮想データセンター ネットワーク IP プールで現在使用中の IP アドレスのリストを表示できます。

■ 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 vCloud Director サイトにまたがることができます。

組織仮想データセンターへのネットワークの追加

ネットワークを組織仮想データセンターに追加して、その仮想マシン間の相互通信やインターネットへのアクセスを可能にします。1 つの組織仮想データセンターに複数のネットワークを追加できます。

表 5-14. 組織仮想データセンター ネットワークのタイプとその要件

組織仮想データセンター ネットワークのタイプ	説明	要件
外部ネットワークへの直接接続	<p>複数の組織によってアクセス可能。異なる組織に属する仮想マシンからこのネットワークのトラフィックに接続し、確認できます。</p> <p>このネットワークは、組織外のマシンに対して直接レイヤ 2 接続を提供します。この組織外の仮想マシンは、組織内の仮想マシンに直接接続できます。</p> <p>IPv4 または IPv6 を選択します。</p>	外部ネットワークは、組織からアクセスできる必要があります。
経路指定された組織仮想データセンター ネットワーク	<p>この組織によってのみアクセス可能。この組織内の仮想マシンのみがこのネットワークに接続できます。</p> <p>このネットワークは、外部ネットワークに対する制限されたアクセスを提供します。システム管理者および組織管理者はネットワークアドレス変換 (NAT) およびファイアウォールの設定を構成して、特定の仮想マシンを外部ネットワークからアクセスできるようにできます。</p> <p>IPv4 または IPv6 を選択します。</p>	組織 VDC に Edge ゲートウェイが設定されている必要があります。

表 5-14. 組織仮想データセンター ネットワークのタイプとその要件（続き）

組織仮想データセンター ネットワークのタイプ	説明	要件
隔離された組織仮想データセンター ネットワーク	<p>この組織によってのみアクセス可能。この組織内の仮想マシンのみがこのネットワークのトラフィックに接続して確認できます。</p> <p>このネットワークは、複数の vApp が接続できる隔離された非公開ネットワークを、組織に対して提供します。このネットワークは、この組織外の仮想マシンまたは組織内の他のネットワークの仮想マシンへの接続は提供しません。</p> <p>ネットワーク プールまたは NSX-T 論理スイッチのいずれかによってバックアップできます。NSX-T 組織仮想データセンター ネットワークの管理については、『vCloud Director Service Provider Admin Portal Guide』を参照してください。</p> <p>IPv4 のみを選択できます。</p>	組織 VDC にネットワーク プールまたは NSX-T 論理スイッチが設定されている必要があります。
クロス仮想データセンター ネットワーク	<p>このネットワークは、データセンター グループにまたがる拡張ネットワークの一部です。単一またはマルチサイトの vCloud Director 展開では、データセンター グループに 2 ～ 4 つの組織仮想データセンターを含めることができます。</p> <p>このネットワークに接続された仮想マシンは、基盤となる拡張ネットワークに接続されます。</p> <p>IPv4 のみを選択できます。</p> <p>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、『vCloud Director Tenant Portal Guide』を参照してください。</p>	組織 VDC にデータセンター グループが設定されている必要があります。

直接接続による組織 VDC ネットワークの作成

システム管理者は、IPv4 または IPv6 外部ネットワークに直接接続する組織仮想データセンター ネットワークを作成できます。組織の仮想マシンは、外部ネットワークを使用してインターネットを含む他のネットワークに接続できます。

前提条件

- この操作は、システム管理者に制限されます。
- 外部ネットワークが必要です。[外部ネットワークの追加](#)を参照してください。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織 VDC] をクリックします。
- 2 組織 VDC 名をダブルクリックして VDC を開きます。
- 3 [組織 VDC ネットワーク] タブをクリックし、[ネットワークを追加] をクリックします。
- 4 [外部ネットワークに直接接続します] を選択します。
- 5 外部ネットワークを選択し、[次へ] をクリックします。
- 6 名前と、必要に応じて説明を入力します。
- 7 (オプション) [このネットワークを組織内の他の VDC と共有する] を選択し、組織内の他の VDC がネットワークを使用できるようにします。

8 [次へ] をクリックします。

9 ネットワーク設定を確認します。

[完了] をクリックして設定を受け入れてネットワークを作成するか、または [戻る] をクリックして設定を変更します。

経路指定された接続による組織 VDC ネットワークの作成

経路指定された接続による組織 VDC ネットワークでは、組織 VDC の外部のマシンとネットワークへのアクセスを制御できます。システム管理者および組織管理者は、ネットワークの Edge ゲートウェイにネットワーク アドレス変換 (NAT) およびファイアウォールを設定して、VDC 内の特定の仮想マシンに対して外部ネットワークからのアクセスを可能にすることができます。

IPv4 または IPv6 経路指定ネットワークを作成できます。

前提条件

- この操作には、事前定義の組織管理者ロールに含まれている権限、またはそれに相当する権限が必要です。
- 組織 VDC には、Edge ゲートウェイを含める必要があります。[Edge ゲートウェイの追加](#)を参照してください。

手順

- 1 [管理] タブで、左側のペインの [仮想データセンター] をクリックします。
- 2 組織 VDC 名をダブルクリックし、組織 VDC を開きます。
- 3 [組織 VDC ネットワーク] タブをクリックし、[ネットワークを追加] をクリックします。
- 4 [既存のエッジ ゲートウェイに接続して経路指定ネットワークを作成します] を選択します。

- a (オプション) このネットワークの接続先である Edge ゲートウェイを選択します。

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

- b (オプション) 新しいネットワークの接続の詳細を指定します。

[外部ネットワークに直接接続します] を選択した場合、他のネットワーク プロパティは設定できません。外部ネットワークに直接接続されない、経路指定されたネットワークでは、NSX ネットワーク機能を利用できるように、ネットワークの他のオプションを指定できます。これらの機能の詳細については、『NSX 管理ガイド』を参照してください。

オプション	説明
ゲスト VLAN の許可	このネットワークでゲスト VLAN のタギングを有効にするには、このオプションを選択します。
サブインターフェイスとして作成	サブインターフェイスとしてネットワークを作成するには、このオプションを選択します。
分散インターフェイスとして作成	この Edge ゲートウェイに接続されている分散論理ルーター上にネットワークを作成するには、このオプションを選択します。

- 5 [ネットワークの構成] 画面で、新しいネットワークの [ネットワーク CIDR] を入力します。

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

- 6 (オプション) ネットワークの DNS を設定します。

このネットワークに接続する仮想マシンが DNS サービスを使用できるようにする場合は、ここで設定できます。必要な場合は、後でこのネットワークのプロパティを編集して、これらの設定を更新できます。

オプション	説明
ゲートウェイ DNS を使用	このオプションは、Edge ゲートウェイと同じ DNS 設定を使用するようにネットワークを設定するものです。ゲートウェイの [DNS リレーにデフォルト ゲートウェイを使用] プロパティが有効な場合にのみ利用可能です。
プライマリ DNS、セカンダリ DNS、DNS サフィックス	[ゲートウェイ DNS を使用] を選択しない場合は、独自の DNS の設定値を入力できます。

- 7 (オプション) このネットワークの固定 IP アドレスを設定します。

このネットワークで固定 IP アドレスを必要とする仮想マシンに割り当てる 1 つ以上のアドレスを予約する場合は、アドレスまたはアドレス範囲を入力して [追加] をクリックします。この手順を繰り返し、複数の固定 IP プールを追加します。

- 8 [次へ] をクリックします。

- 9 ネットワークの名前と、オプションで説明を入力します。

- 10 (オプション) 組織の他の VDC が組織 VDC ネットワークを使用できるようにするには、[このネットワークを組織内の他の VDC と共有する] を選択します。

- 11 (オプション) このオブジェクトのメタデータを作成または更新します。

[オブジェクト メタデータの作成または更新](#)を参照してください。

- 12 [OK] をクリックして、変更内容を保存します。

- 13 [次へ] をクリックします。

- 14 ネットワーク設定を確認します。

[完了] をクリックして設定を受け入れてネットワークを作成するか、または [戻る] をクリックして設定を変更します。

隔離された組織 VDC ネットワークの作成

隔離された組織 VDC ネットワークは、組織 VDC の仮想マシンが接続できるプライベート ネットワークを提供します。このネットワークは、この組織 VDC の外部にあるマシンへの接続は提供しません。

vCloud Director Web Console では、ネットワーク プールによってバックアップされている隔離された VDC ネットワークを作成できます。NSX-T 論理スイッチによってバックアップされている隔離された VDC ネットワークを作成するには、Service Provider Admin Portal を使用する必要があります。NSX-T 組織仮想データセンター ネットワークの管理については、『vCloud Director Service Provider Admin Portal Guide』を参照してください。

IPv4 の隔離された組織 VDC ネットワークのみを作成できます。

前提条件

- この操作には、事前定義の組織管理者ロールに含まれている権限、またはそれに相当する権限が必要です。
- 組織 VDC には、ネットワーク プールを含める必要があります。デフォルトでは、すべての組織 VDC が VXLAN ネットワーク プールを使用して作成されます。

手順

- 1 [管理] タブで、左側のペインの [仮想データセンター] をクリックします。
- 2 組織 VDC 名をダブルクリックし、組織 VDC を開きます。
- 3 [組織 VDC ネットワーク] タブをクリックし、[ネットワークを追加] をクリックします。
- 4 [この仮想データセンター内で隔離されたネットワークを作成します] を選択し、[次へ] をクリックします。
- 5 [ネットワークの構成] 画面で、新しいネットワークの [ネットワーク CIDR] を入力します。

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

- 6 (オプション) ネットワークの DNS を設定します。

このネットワークに接続する仮想マシンが DNS サービスを使用できるようにする場合は、ここで設定できます。必要な場合は、後でこのネットワークのプロパティを編集して、これらの設定を更新できます。

オプション	説明
ゲートウェイ DNS を使用	このオプションは、Edge ゲートウェイと同じ DNS 設定を使用するようにネットワークを設定するものです。ゲートウェイの [DNS リレーにデフォルト ゲートウェイを使用] プロパティが有効な場合にのみ利用可能です。
プライマリ DNS、セカンダリ DNS、DNS サフィックス	[ゲートウェイ DNS を使用] を選択しない場合は、独自の DNS の設定値を入力できます。

- 7 (オプション) このネットワークの固定 IP アドレスを設定します。

このネットワークで固定 IP アドレスを必要とする仮想マシンに割り当てる 1 つ以上のアドレスを予約する場合は、アドレスまたはアドレス範囲を入力して [追加] をクリックします。この手順を繰り返し、複数の固定 IP プールを追加します。

- 8 [次へ] をクリックします。
- 9 ネットワークの名前と、オプションで説明を入力します。
- 10 (オプション) 組織の他の VDC が組織 VDC ネットワークを使用できるようにするには、[このネットワークを組織内の他の VDC と共有する] を選択します。
- 11 (オプション) このオブジェクトのメタデータを作成または更新します。

[オブジェクト メタデータの作成または更新](#)を参照してください。

- 12 [OK] をクリックして、変更内容を保存します。
- 13 [次へ] をクリックします。

14 ネットワーク設定を確認します。

[完了] をクリックして設定を受け入れてネットワークを作成するか、または [戻る] をクリックして設定を変更します。

組織 VDC ネットワークのプロパティの表示または変更

組織 VDC ネットワークを作成した後は、その名前、説明、DNS 設定、共有、および固定 IP プールを変更できます。

前提条件

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

手順

- 1 [管理] タブで、左側のペインの [仮想データセンター] をクリックします。
- 2 組織 VDC 名をダブルクリックして VDC を開きます。
- 3 [組織 VDC ネットワーク] タブで、ネットワーク名を右クリックし、[プロパティ] をクリックして [ネットワークのプロパティ] ページを開きます。
- 4 (オプション) ネットワークの [全般] プロパティを変更します。
 - a ネットワークの名前と、オプションで説明を入力します。
 - b [このネットワークを組織内の他の VDC と共有する] を選択し、組織内の他の VDC でネットワークを使用できるようにします。
- 5 (オプション) [ネットワークの仕様] を変更します。
 - a ネットワークの DNS 設定を変更します。

オプション	説明
ゲートウェイ DNS を使用	このオプションは、Edge ゲートウェイと同じ DNS 設定を使用するようにネットワークを設定するものです。ゲートウェイの [DNS リレーにデフォルト ゲートウェイを使用] プロパティが有効な場合にのみ利用可能です。
プライマリ DNS、セカンダリ DNS、DNS サフィックス	[ゲートウェイ DNS を使用] を選択しない場合は、独自の DNS の設定値を入力できます。システム管理者は、組織内のネットワークに対して適切な値を提案できます。

- b このネットワークの [固定 IP プール] を変更します。

このネットワークで固定 IP アドレスを必要とする仮想マシンに割り当てる 1 つ以上のアドレスを予約する場合は、アドレスまたはアドレス範囲を入力して [追加] をクリックします。この手順を繰り返し、複数の固定 IP プールを追加します。

- 6 (オプション) このオブジェクトのメタデータを作成または更新します。

[オブジェクト メタデータの作成または更新](#)を参照してください。

- 7 [OK] をクリックして、変更内容を保存します。

組織仮想データセンター ネットワーク サービスの構成

DHCP、ファイアウォール、ネットワーク アドレス変換 (NAT)、VPN などのサービスを、特定の組織仮想データセンター ネットワークに対して構成できます。組織管理者は、自分の組織仮想データセンター ネットワークに対していくつかのネットワーク サービスを構成することもできます。

表 5-15. ネットワーク タイプ別の使用可能なネットワーク サービス に、vCloud Director から各タイプの組織仮想データセンター ネットワークに提供されるネットワーク サービスのリストを表示します。

表 5-15. ネットワーク タイプ別の使用可能なネットワーク サービス

ネットワーク タイプ	DHCP	ファイアウォール	NAT	VPN
外部組織仮想データセンター ネットワーク - 直接接続				
外部組織仮想データセンター ネットワーク - 経路指定接続	X	X	X	X
内部組織仮想データセンター ネットワーク	X			

組織仮想データセンター ネットワークの DHCP の構成

組織内の仮想マシンに DHCP サービスを提供するために、特定の組織仮想データセンター ネットワークを構成できます。

仮想マシンをパワーオンし次のタスクを実行すると、vCloud Director は DHCP IP アドレスを仮想マシンに割り当てます。

- 組織仮想データセンター ネットワークに対する DHCP の有効化
- 組織内の仮想マシン上の NIC のネットワークへの接続
- NIC の IP モードとして [DHCP] を選択

システム管理者と組織管理者が DHCP を構成できます。

前提条件

経路指定された組織仮想データセンター ネットワークまたは内部組織仮想データセンター ネットワークが存在することを確認します。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織 VDC] をクリックします。
- 2 組織仮想データセンター名をダブルクリックし、組織仮想データセンターを開きます。
- 3 [組織 VDC ネットワーク] タブをクリックし、組織仮想データセンター ネットワーク名を右クリックし、[サービスの構成] を選択します。
- 4 [DHCP] タブをクリックし、[DHCP を有効化] を選択します。

- 5 IP アドレスの範囲を入力するか、デフォルトの範囲を使用します。

vCloud Director は、これらのアドレスを使用して DHCP 要求に応えます。DHCP IP アドレスの範囲は、組織仮想データセンター ネットワークの固定 IP プールと重複できません。

- 6 デフォルトのリース期間および最大のリース期間を設定するか、デフォルト値を使用します。
- 7 [OK] をクリックします。

結果

vCloud Director は、DHCP サービスを提供するためにネットワークを更新します。

組織仮想データセンター ネットワークのファイアウォールの有効化

ファイアウォール サービスが提供されるように、特定の組織仮想データセンター ネットワークを構成できます。組織仮想データセンター ネットワークでファイアウォールを有効化すると、受信トラフィック、送信トラフィック、または両方でファイアウォール ルールを施行できます。

すべての受信トラフィック、すべての送信トラフィック、またはその両方を拒否できます。また、特定のファイアウォール ルールを追加し、そのルールに合致するトラフィックがファイアウォールを通過するのを許可または拒否するように設定することもできます。このようなルールは、すべての受信トラフィックまたは送信トラフィックを拒否する一般ルールよりも優先されます。[組織仮想データセンター ネットワークのファイアウォール ルールの追加](#)を参照してください。

システム管理者と組織管理者は、ファイアウォールを有効化できます。

前提条件

外部の経路指定された組織仮想データセンター ネットワークが存在することを確認します。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織 VDC] をクリックします。
- 2 組織仮想データセンター名をダブルクリックし、組織仮想データセンターを開きます。
- 3 [組織 VDC ネットワーク] タブをクリックし、組織仮想データセンター ネットワーク名を右クリックし、[サービスの構成] を選択します。
- 4 [ファイアウォール] タブをクリックし、[ファイアウォールを有効化] を選択します。
- 5 デフォルトのファイアウォールのアクションを選択します。
- 6 (オプション) デフォルトのファイアウォールのアクションに関連するイベントをログに記録するには、[ログ] チェック ボックスをオンにします。
- 7 [OK] をクリックします。

組織仮想データセンター ネットワークのファイアウォール ルールの追加

ファイアウォール ルールは、ファイアウォールをサポートする組織仮想データセンター ネットワークに追加できます。ルールを作成することにより、そのルールに合致するトラフィックがファイアウォールを通過することを許可または拒否するように設定できます。

ファイアウォール ルールが施行されるようにするには、組織仮想データセンター ネットワークのファイアウォールを有効化する必要があります。[組織仮想データセンター ネットワークのファイアウォールの有効化](#)を参照してください。

新しいファイアウォール ルールを組織仮想データセンター ネットワークに追加すると、ファイアウォール ルール リストの一番下に表示されます。施行するファイアウォール ルールの優先順位の設定方法については、[組織仮想データセンター ネットワークのファイアウォール ルールの順序変更](#)を参照してください

システム管理者と組織管理者は、ファイアウォール ルールを追加できます。

前提条件

外部の NAT 経由の組織仮想データセンター ネットワークが存在することを確認します。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織 VDC] をクリックします。
- 2 組織仮想データセンター名をダブルクリックし、組織仮想データセンターを開きます。
- 3 [組織 VDC ネットワーク] タブをクリックし、組織仮想データセンター ネットワーク名を右クリックし、[サービスの構成] を選択します。
- 4 [ファイアウォール] タブをクリックし、[追加] をクリックします。
- 5 ルールの名前を入力します。
- 6 トラフィックの方向を選択します。
- 7 ソース IP アドレスを入力し、ソース ポートを選択します。
受信トラフィックの場合、ソースは外部ネットワークです。送信トラフィックの場合、ソースは組織仮想データセンター ネットワークです。
- 8 ターゲット IP アドレスを入力し、ターゲット ポートを選択します。
受信トラフィックの場合、ターゲットは組織仮想データセンター ネットワークです。送信トラフィックの場合、ターゲットは外部ネットワークです。
- 9 プロトコルおよびアクションを選択します。
ファイアウォール ルールでは、そのルールに合致するトラフィックを許可または拒否するように設定できます。
- 10 [有効] チェック ボックスをオンにします。
- 11 (オプション) [ファイアウォール ルールのネットワーク トラフィックをログに記録する] チェック ボックスをオンにします。
このオプションを有効化した場合、vCloud Director では、このルールによって影響を受ける接続についてのログ イベントを Syslog サーバー に送信します。それぞれの Syslog メッセージは、論理的ネットワークと組織 UUID を含みます。
- 12 [OK] をクリックし、もう一度 [OK] をクリックします。

組織仮想データセンター ネットワークのファイアウォール ルールの順序変更

ファイアウォール ルールはファイアウォール リストに表示された順に施行されます。リストのルールの表示順次は変更できます。

新しいファイアウォール ルールを組織仮想データセンター ネットワークに追加すると、ファイアウォール ルール リストの一番下に表示されます。既存のルールよりも先に新しいルールが施行されるようにするには、ルールの順序を変更します。

前提条件

2 つ以上のファイアウォール ルールのある、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ます。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織 VDC] をクリックします。
- 2 組織仮想データセンター名をダブルクリックし、組織仮想データセンターを開きます。
- 3 [組織 VDC ネットワーク] タブをクリックし、組織仮想データセンター ネットワーク名を右クリックし、[サービスの構成] を選択します。
- 4 [ファイアウォール] タブをクリックします。
- 5 ファイアウォール ルールをドラッグして、ルールが適用される順に表示順序を変更します。
- 6 [OK] をクリックします。

組織仮想データセンター ネットワークの VPN の有効化

組織仮想データセンター ネットワークの VPN を有効化し、別のネットワークへのセキュアなトンネルを作成できます。

vCloud Director では、同じ組織にある組織仮想データセンター ネットワーク間、異なる組織にある組織仮想データセンター ネットワーク間 (vCloud Director の異なるインスタンスにおける組織仮想データセンター ネットワークを含む)、およびリモート ネットワーク間における VPN をサポートします。

システム管理者と組織管理者は、VPN を有効化できます。

前提条件

外部の経路指定された組織仮想データセンター ネットワークが存在することを確認します。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織 VDC] をクリックします。
- 2 組織仮想データセンター名をダブルクリックし、組織仮想データセンターを開きます。
- 3 [組織 VDC ネットワーク] タブをクリックし、組織仮想データセンター ネットワーク名を右クリックし、[サービスの構成] を選択します。
- 4 [VPN] タブをクリックし、[VPN の有効化] を選択します。
- 5 (オプション) [公開 IP の構成] をクリックし、公開 IP アドレスを入力し、[OK] をクリックします。

6 [OK] をクリックします。

次のステップ

別のネットワークへの VPN トンネルを作成します。

組織内での VPN トンネルの作成

同じ組織における 2 つの組織仮想データセンター ネットワーク間に VPN トンネルを作成できます。

システム管理者と組織管理者は、どちらも VPN トンネルを作成できます。

トンネル エンドポイント間にファイアウォールがある場合、次の IP プロトコルおよび UDP ポートを許可するように構成する必要があります。

- 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

前提条件

両方のネットワーク上で IP サブネットが重複しておらず、VPN が有効化されている、2 つ以上の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ます。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織 VDC] をクリックします。
- 2 組織仮想データセンター名をダブルクリックし、組織仮想データセンターを開きます。
- 3 [組織 VDC ネットワーク] タブをクリックし、組織仮想データセンター ネットワーク名を右クリックし、[サービスの構成] を選択します。
- 4 [VPN] タブをクリックし、[追加] をクリックします。
- 5 名前と、必要に応じて説明を入力します。
- 6 ドロップダウン メニューから [この組織のネットワーク] を選択し、ピア ネットワークを選択します。
- 7 トンネル設定を確認し、[OK] をクリックします。

結果

vCloud Director によって、ピア ネットワークのエンドポイントが両方とも構成されます。

リモート ネットワークへの VPN トンネルの作成

組織仮想データセンター ネットワークとリモート ネットワーク間に VPN トンネルを作成できます。

システム管理者と組織管理者が VPN トンネルを作成できます。

トンネル エンドポイント間にファイアウォールがある場合、次の IP プロトコルおよび UDP ポートを許可するように構成する必要があります。

- 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

前提条件

経路指定されている組織仮想データセンター ネットワークと、IPSec を使用する経路指定されているリモート ネットワークがあることを確認します。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織 VDC] をクリックします。
- 2 組織仮想データセンター名をダブルクリックし、組織仮想データセンターを開きます。
- 3 [組織 VDC ネットワーク] タブをクリックし、組織仮想データセンター ネットワーク名を右クリックし、[サービスの構成] を選択します。
- 4 [VPN] タブをクリックし、[追加] をクリックします。
- 5 名前と、必要に応じて説明を入力します。
- 6 ドロップダウン メニューから [リモート ネットワーク] を選択します。
- 7 ピア設定を入力します。

VMware ナレッジベースの記事 <https://kb.vmware.com/kb/2051370> を参照してください。

- 8 トンネル設定を確認し、[OK] をクリックします。

結果

vCloud Director によって、組織のピア ネットワークのエンドポイントが構成されます。

次のステップ

リモートのピア ネットワークのエンドポイントを手動で構成します。

組織仮想データセンター ネットワークの固定ルーティングの設定

特定の組織仮想データセンター ネットワークを設定して、固定ルートを追加し、異なる vApp ネットワーク間のトラフィックを組織仮想データセンター ネットワークに経路指定できます。

作成するすべての固定ルートは自動的に有効になります。固定ルートを無効にするには、これを削除する必要があります。

前提条件

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。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織 VDC] をクリックします。
- 2 組織仮想データセンター名をダブルクリックし、組織仮想データセンターを開きます。
- 3 [組織 VDC ネットワーク] タブをクリックし、組織仮想データセンター ネットワーク名を右クリックし、[サービスの構成] を選択します。

次のステップ

固定ルートを作成します。同じ組織仮想データセンター ネットワークに経路指定されている vApp ネットワーク間での固定ルートの追加 および 異なる組織仮想データセンター ネットワークに経路指定されている vApp ネットワーク間での固定ルートの追加 を参照してください。

同じ組織仮想データセンター ネットワークに経路指定されている vApp ネットワーク間での固定ルートの追加

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

固定ルートは、重複しているネットワーク間やフェンスされた vApp 間に追加することはできません。固定ルートを組織仮想データセンター ネットワークに追加したら、固定ルートでトラフィックが許可されるようにネットワークファイアウォール ルールを構成します。

固定ルートは、これらのルートに含まれる vApp が実行されている場合にのみ機能します。固定ルートが含まれている vApp で次の操作を実行した場合、その固定ルートは機能なくなり、手動で削除しなければなりません。

- vApp の親ネットワークを変更
- vApp を削除
- vApp ネットワークを削除

前提条件

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

ネットワークが以下の構成を持っていることを確認してください。

- 組織仮想データセンター ネットワークが経路指定されていること。
- 固定ルーティングは、組織仮想データセンター ネットワークで有効化されています。
- 2 つの vApp ネットワークは、組織仮想データセンター ネットワークに経路指定されています。
- vApp ネットワークは、少なくとも 1 回は開始された vApp にあります。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織 VDC] をクリックします。
- 2 組織仮想データセンター名をダブルクリックし、組織仮想データセンターを開きます。
- 3 [組織 VDC ネットワーク] タブをクリックし、組織仮想データセンター ネットワーク名を右クリックし、[サービスの構成] を選択します。

- 4 [固定ルーティング] タブで、[追加] をクリックします。
- 5 名前、ネットワーク アドレス、および次ホップ IP を入力します。
ネットワーク アドレスは、固定ルートを追加する最初の vApp ネットワークに対するものです。次ホップ IP は、その vApp ネットワークのルーターの外部 IP アドレスです。
- 6 [このネットワーク内] を選択し、[OK] をクリックします。
- 7 [OK] をクリックします。
- 8 2 つ目の vApp ネットワークにルートを追加するために、[手順 4](#) から [手順 7](#) までを繰り返します。

例：固定ルーティング例

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

表 5-16. ネットワーク情報

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

Org VDC Network Shared で、vApp Network 1 への固定ルートと vApp Network 2 への別の固定ルートを作成します。

表 5-17. 固定ルーティング設定

ネットワークへの固定ルート	ルート名	ネットワーク	次ホップ IP アドレス	ルート
vApp Network 1	tovapp1	192.168.1.0/24	192.168.0.100	このネットワーク内
vApp Network 2	tovapp2	192.168.2.0/24	192.168.0.101	このネットワーク内

次のステップ

固定ルートのトラフィックが許可されるように、ファイアウォール ルールを作成します。[組織仮想データセンター ネットワークのファイアウォール ルールの追加](#)を参照してください。

異なる組織仮想データセンター ネットワークに経路指定されている vApp ネットワーク間での固定ルートの追加

組織管理者は、異なる組織仮想データセンター ネットワークに経路指定されている 2 つの vApp ネットワーク間に固定ルートを追加できます。固定ルートにより、ネットワーク間のトラフィックが許可されます。

固定ルートは、重複しているネットワーク間やフェンスされた vApp 間に追加することはできません。固定ルートを組織仮想データセンター ネットワークに追加したら、固定ルートでトラフィックが許可されるようにネットワーク ファイアウォール ルールを構成します。固定ルートを持つ vApp に対しては、[この vApp または関連付けられているネットワークが削除されるまで常に割り当てられた IP アドレスを使用します] チェック ボックスをオンにします。

固定ルートは、これらのルートに含まれる vApp が実行されている場合にのみ機能します。vApp に固定ルートが含まれていて、次の操作を実行した場合、その固定ルートは機能することができず、手動で削除しなければなりません。

- vApp の親ネットワークを変更
- vApp を削除
- vApp ネットワークを削除

前提条件

vCloud Director が以下の構成を持っていることを確認してください。

- 同じ外部ネットワークに経路指定されている 2 つの組織仮想データセンター ネットワーク。
- 固定ルーティングは、両方の組織仮想データセンター ネットワークで有効化されています。
- vApp ネットワークは、それぞれの組織仮想データセンター ネットワークに経路指定されています。
- vApp ネットワークは、少なくとも 1 回は開始された vApp にあります。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織 VDC] をクリックします。
- 2 組織仮想データセンター名をダブルクリックし、組織仮想データセンターを開きます。
- 3 [組織 VDC ネットワーク] タブをクリックし、組織仮想データセンター ネットワーク名を右クリックし、[サービスの構成] を選択します。
- 4 [固定ルーティング] タブで、[追加] をクリックします。
- 5 名前、ネットワーク アドレス、および次ホップ IP アドレスを入力します。

ネットワーク アドレスは、固定ルートを追加する対象の vApp ネットワークに対するものです。次ホップ IP アドレスは、その vApp ネットワークが経路指定されている対象の組織仮想データセンター ネットワークのルーターの外部 IP アドレスです。

- 6 [外部ネットワークへ] を選択し、[OK] をクリックします。
- 7 [追加] をクリックします。
- 8 名前、ネットワーク アドレス、および次ホップ IP アドレスを入力します。

ネットワーク アドレスは、この組織仮想データセンター ネットワークに経路指定されている vApp ネットワークに対するものです。次ホップ IP アドレスは、その vApp ネットワークのルーターの外部 IP アドレスです。

- 9 [このネットワーク内] を選択し、[OK] をクリックします。

- 10 2つ目の組織仮想データセンター ネットワークに固定ルートを追加するには、「手順 4」から「手順 9」までの手順を繰り返します。

例：固定ルーティング例

vApp Network 1 は Org VDC Network 1 に経路指定されています。vApp Network 2 は Org VDC Network 2 に経路指定されています。組織仮想データセンター ネットワークで固定ルートを作成し、vApp ネットワーク間のトラフィックを可能にします。固定ルートを作成するには、vApp ネットワークと組織仮想データセンター ネットワークに関する情報を使用できます。

表 5-18. ネットワーク情報

ネットワーク名	ネットワーク仕様	ルーターの外部 IP アドレス
vApp Network 1	192.168.1.0/24	192.168.0.100
vApp Network 2	192.168.11.0/24	192.168.10.100
Org VDC Network 1	192.168.0.0/24	10.112.205.101
Org VDC Network 2	192.168.10.0/24	10.112.205.100

Org VDC Network 1 で、vApp Network 2 への固定ルートと vApp Network 1 への別の固定ルートを作成します。Org VDC Network 2 で、vApp Network 1 への固定ルートと vApp Network 2 への別の固定ルートを作成します。

表 5-19. Org VDC Network 1 に対する固定ルーティング設定

ネットワークへの固定ルート	ルート名	ネットワーク	次ホップ IP アドレス	ルート
vApp Network 2	tovapp2	192.168.11.0/24	10.112.205.100	外部ネットワークへ
vApp Network 1	tovapp1	192.168.1.0/24	192.168.0.100	このネットワーク内

表 5-20. Org VDC Network 2 に対する固定ルーティング設定

ネットワークへの固定ルート	ルート名	ネットワーク	次ホップ IP アドレス	ルート
vApp Network 1	tovapp1	192.168.1.0/24	10.112.205.101	外部ネットワークへ
vApp Network 2	tovapp2	192.168.11.0/24	192.168.10.100	このネットワーク内

次のステップ

固定ルートのトラフィックが許可されるように、ファイアウォール ルールを作成します。[組織仮想データセンター ネットワークのファイアウォール ルールの追加](#) を参照してください。

組織仮想データセンター ネットワークのリセット

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

プロバイダ仮想データセンターを削除する前に、その仮想データセンターに依存する組織仮想データセンター ネットワークをリセットします。

組織仮想データセンター ネットワークのリセット中は、ネットワーク サービスを使用できません。

前提条件

経路指定された組織仮想データセンター ネットワークまたは内部組織仮想データセンター ネットワークが存在することを確認します。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織 VDC] をクリックします。
- 2 組織仮想データセンター名をダブルクリックし、組織仮想データセンターを開きます。
- 3 [組織 VDC ネットワーク] タブをクリックし、組織仮想データセンター ネットワーク名を右クリックして、[ネットワークをリセット] を選択します。
- 4 [はい] をクリックします。

組織仮想データセンター ネットワークの接続、切断、移動

組織仮想データセンター ネットワークは、接続、切断、または移動することができます。

組織仮想データセンター ネットワークを別の Edge Gateway に移動しているときは、ネットワーク サービスは一切利用できません。

前提条件

- この操作には、事前定義の組織管理者ロールに含まれている権限、またはそれに相当する権限が必要です。
- 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ます。
- 組織管理者権限を持っていることを確認します。

手順

- 1 [管理] をクリックし、組織仮想データセンターを選択します。
- 2 組織仮想データセンター ネットワークを右クリックし、オプションを選択します。

隔離されたネットワークを Edge Gateway に接続すると、経路指定されたネットワークに変換されます。経路指定されたネットワークは、Edge Gateway から別の Edge Gateway に移動することができます。

オプション	説明
ゲートウェイに接続	ネットワークの接続先の Edge Gateway を選択し、[OK] をクリックします。
ネットワークの切断	[はい] をクリックして、ネットワークを切断することを確認します。
ネットワークの移動	(経路指定のネットワークのみ。) ネットワークの移動先の Edge Gateway を選択し、[OK] をクリックします。

組織仮想データセンター ネットワークを使用する vApp および vApp テンプレートの表示

組織仮想データセンター ネットワークに接続する NIC を持つ仮想マシンが含まれる、すべての vApp および vApp テンプレートのリストを表示することができます。vApp または vApp テンプレートが接続されている組織仮想データセンター ネットワークを削除することはできません。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織 VDC] をクリックします。
- 2 組織仮想データセンター名をダブルクリックし、組織仮想データセンターを開きます。
- 3 [組織 VDC ネットワーク] タブをクリックし、組織仮想データセンター ネットワーク名を右クリックして、[接続されている vApp] を選択します。
- 4 [OK] をクリックします。

組織仮想データセンター ネットワークの削除

組織仮想データセンター ネットワークを削除し、組織仮想データセンターからそれを削除することができます。

前提条件

組織仮想データセンター ネットワークに接続されている仮想マシンが存在しないことを確認します。[組織仮想データセンター ネットワークを使用する vApp および vApp テンプレートの表示](#) を参照してください。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織 VDC] をクリックします。
- 2 組織仮想データセンター名をダブルクリックし、組織仮想データセンターを開きます。
- 3 [組織 VDC ネットワーク] タブをクリックし、組織仮想データセンター ネットワーク名を右クリックして、[削除] を選択します。

組織仮想データセンター ネットワークの IP 使用の表示

組織仮想データセンター ネットワーク IP プールで現在使用中の IP アドレスのリストを表示できます。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織 VDC] をクリックします。
- 2 組織仮想データセンター名をダブルクリックし、組織仮想データセンターを開きます。
- 3 [組織 VDC ネットワーク] タブをクリックし、組織仮想データセンター ネットワーク名を右クリックして、[IP の割り当て] を選択します。

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 vCloud Director サイトにまたがることができます。

vCloud Director 9.5 ではクロス仮想データセンター ネットワークを導入しました。これにより、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ー 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 vCloud Director サイトに属することができます。[マルチサイト展開の設定と管理](#)を参照してください。

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 vCloud 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 Controller クラスタを展開します。
 - 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設定します。 [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 トランスポート ゾーン用の VXLAN にバックアップされているネットワーク 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、vCloud 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。 [クロス仮想データセンター ネットワークの有効化](#)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 vCloud 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。同一のインストール ID で設定された vCloud Director サイトがある場合は、「[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、『vCloud 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 ネットワークの有効化

組織仮想データセンターに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ができます。該当する権限を持つ組織ユーザーは、有効な仮想データセンターを使用して、データセンター グループおよびレイヤー 2 拡張ネットワークを作成することができます。

手順

- 1 [管理および監視] タブの [クラウド リソース] で、[組織 VDC] をクリックします。
- 2 ターゲットの組織仮想データセンターを右クリックして、[プロパティ] をクリックします。
- 3 [ネットワーク プールとサービス] タブで、[クロス VDC ネットワークを有効にする] を選択します。

結果

vCloud Director テナント ポータルでは、データセンターのリストに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、『vCloud Director Tenant Portal Guide』を参照してください。

マルチサイト拡張ネットワークの MAC アドレスの再生成

同じインストール ID で構成されている 2 つの vCloud Director サイトを関連付けると、これらのサイト間の拡張ネットワークで MAC アドレスの競合が発生する可能性があります。このような競合を回避するには、インストール ID とは異なるカスタム シードに基づいて、いずれかのサイトで MAC アドレスを再生成する必要があります。

vCloud Director の初期セットアップ中に、インストール ID を設定します。vCloud Director はインストール ID を使用して、仮想マシン ネットワーク インターフェイスの MAC アドレスを生成します。同じインストール ID で構成されている 2 つの vCloud Director インストールでは、同じ MAC アドレスが生成されることがあります。MAC アドレスが重複すると、関連付けられた 2 つのサイト間の拡張ネットワークで競合が発生する可能性があります。

同じインストール ID で構成されている、関連付けられたサイト間で拡張ネットワークを作成する前に、セル管理ツールの `mac-address-management` サブコマンドを使用して、いずれかのサイトで MAC アドレスを再生成する必要があります。

```
cell-management-tool
mac-address-management
options
```

新しい MAC アドレスを生成するには、インストール ID とは異なるカスタム シードを設定します。シードはインストール ID を上書きしませんが、データベースには 2 番目の構成パラメータとして最新のシードが保存され、インストール ID がオーバーライドされます。

mac-address-management サブコマンドは、サーバ グループの任意の vCloud Director メンバーから実行します。このコマンドは vCloud Director データベースに対して実行されるため、1 つのサーバ グループに対して 1 回コマンドを実行します。

重要： MAC アドレスの再生成には、vCloud Director の一定のダウンタイムが必要です。再生成を開始する前に、サーバ グループ内のすべてのセルのアクティビティを休止する必要があります。

表 5-21. セル管理ツールのオプションと引数、mac-address-management サブコマンド

オプション	引数	説明
--help (-h)	なし	このカテゴリで使用可能なコマンドの概要を示します。
--regenerate	なし	<p>使用されていないすべての MAC アドレスを削除し、現在のシードに基づいて新しい MAC アドレスを生成します。これまでシードを設定したことがない場合は、MAC アドレスはインストール ID に基づいて再生成されます。使用中の MAC アドレスは保持されます。</p> <p>注： サーバ グループ内のすべてのセルは非アクティブである必要があります。セル上のアクティビティを休止する方法については、セルの管理を参照してください。</p>
--regenerate-with-seed	0 ～ 63 のシード番号	<p>データベースに新しいカスタム シードを設定し、使用されていないすべての MAC アドレスを削除して、新しく設定したシードに基づいて新しい MAC アドレスを生成します。使用中の MAC アドレスは保持されます。</p> <p>注： サーバ グループ内のすべてのセルは非アクティブである必要があります。セル上のアクティビティを休止する方法については、セルの管理を参照してください。</p>
--show-seed	なし	現在のシードと各シードに使用されている MAC アドレスの数を返します。

重要： 使用中の MAC アドレスは保持されます。使用中の MAC アドレスを再生成された MAC アドレスに変更するには、ネットワーク インターフェイスの MAC アドレスをリセットする必要があります。仮想マシンのプロパティの編集については、『vCloud Director Tenant Portal Guide』を参照してください。

例：新しいカスタム シードに基づく MAC アドレスの再生成

次のコマンドを実行すると、現在のシードを 9 に設定し、新しく設定したシードに基づいて、使用されていないすべての MAC アドレスを再生成します。

```
[root@cell11 /opt/vmware/vcloud-director/
bin]#./cell-management-tool --regenerate-with-seed 9Successfully removed 65,535 unused MAC
addresses. Successfully generated new MAC addresses.
```

例：現在のシードと各シードに使用されている MAC アドレスの数の表示

次のコマンドを実行すると、現在のシードと各シードの MAC アドレスの数に関する情報を返します。

```
[root@cell11 /opt/vmware/vcloud-director/bin]#./cell-management-tool --show-seedCurrent MAC
address seed is '9' and based on MacAddressSeed config. MAC address seed 9 is in use by 12
MAC addresses MAC address seed 1 is in use by 1 MAC addresses
```

この例では、現在のシードが 9 であり、12 個の MAC アドレスで使用されていることがシステム出力に示されています。また、1 つ前のシードまたはインストール ID に基づく MAC アドレスが 1 つあることも示されています。

ネットワーク プールの管理

ネットワーク プールを作成したら、その名前や説明を変更したり、ネットワーク プール自体を削除したりできます。ネットワーク プールのタイプによっては、ポート グループや VLAN ID を追加することもできます。VXLAN ネットワーク プールの変更または削除はできません。

- **ネットワーク プールの名前および説明の変更**

vCloud Director のインストール環境の規模が大きくなるにつれて、既存のネットワーク プールによりわかりやすい名前または説明を割り当てる必要がある場合があります。

- **ネットワーク プールへのポート グループの追加**

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 プールに、ポート グループを追加できます。

- **ネットワーク プールへの VLAN ID の追加**

VLAN によってバックアップされるネットワーク プールに、VLAN ID を追加できます。

- **ネットワーク プールの削除**

ネットワーク プールを削除して vCloud Director から削除します。VXLAN ネットワーク プールは削除できません。

ネットワーク プールの名前および説明の変更

vCloud Director のインストール環境の規模が大きくなるにつれて、既存のネットワーク プールによりわかりやすい名前または説明を割り当てる必要がある場合があります。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [ネットワーク プール] をクリックします。
- 2 ネットワーク プール名を右クリックし、[プロパティ] を選択します。

3 [全般] タブで新しい名前または説明を入力し、[OK] をクリックします。

ネットワーク プールへのポート グループの追加

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 プールに、ポート グループを追加できます。

前提条件

- 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 プールが存在することを確認します。
- vSphere で使用可能なポート グループが存在することを確認します。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [ネットワーク プール] をクリックします。
- 2 ネットワーク プール名を右クリックし、[プロパティ] を選択します。
- 3 [ネットワーク プールの設定] タブでポート グループを選択し、[追加] をクリックして、[OK] をクリックします。

ネットワーク プールへの VLAN ID の追加

VLAN によってバックアップされるネットワーク プールに、VLAN ID を追加できます。

前提条件

以下の項目がシステムに含まれていることを確認します。

- VLAN によってバックアップされるネットワーク プール
- vSphere で使用可能な VLAN ID

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [ネットワーク プール] をクリックします。
- 2 ネットワーク プール名を右クリックし、[プロパティ] を選択します。
- 3 [ネットワーク プールの設定] タブで VLAN ID の範囲を入力し、[追加] をクリックします。
- 4 vSphere Distributed Switch を選択し、[OK] をクリックします。

ネットワーク プールの削除

ネットワーク プールを削除して vCloud Director から削除します。VXLAN ネットワーク プールは削除できません。

前提条件

以下の条件を満たしていることを確認します。

- いずれの組織仮想データセンターもネットワーク プールに関連付けられていない。
- いずれの vApp もネットワーク プールを使用しない。
- いずれの組織仮想データセンターもネットワーク プールを使用しない。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [ネットワーク プール] をクリックします。
- 2 ネットワーク プール名を右クリックし、[削除] を選択します。
- 3 [はい] をクリックします。

クラウド セルの管理

ほとんどの場合、クラウド セルの管理は、そのセルが存在する vCloud Director サーバー ホストから行いますが、vCloud Director Web コンソールからクラウド セルを削除することもできます。

表 5-22. クラウド セルのコマンド に、クラウド セルを制御するための基本的なコマンドのリストを示します。

表 5-22. クラウド セルのコマンド

コマンド	説明
<code>service vmware-vcd start</code>	セルを開始する
<code>service vmware-vcd restart</code>	セルを再起動する
<code>service vmware-vcd stop</code>	セルを停止する

セルを停止した場合は、ブラウザまたは vCloud API を使用して、そのセルにアクセスしようとするユーザーにメンテナンス メッセージを表示できます。[クラウド セルのメンテナンス メッセージの表示](#)を参照してください。

■ クラウド セルの追加

vCloud Director インストール環境にクラウド セルを追加するには、同じ vCloud Director クラスタの追加の Cloud Director サーバー ホストに vCloud Director ソフトウェアをインストールします。

■ クラウド セルの削除

ソフトウェアを再インストールするため、またはその他の理由により、クラウド セルは vCloud Director インストール環境から削除することができます。

■ クラウド セルのメンテナンス メッセージの表示

セルを停止してメンテナンスを実行していることをユーザーに知らせるために、メンテナンス メッセージを表示できます。

■ クラウド セルのメンテナンス メッセージの非表示

メンテナンスの実行がセルで終了し、このセルを再起動する準備ができた場合、メンテナンス メッセージを非表示にすることができます。

クラウド セルの追加

vCloud Director インストール環境にクラウド セルを追加するには、同じ vCloud Director クラスタの追加の Cloud Director サーバー ホストに vCloud Director ソフトウェアをインストールします。

詳細については、『VMware vCloud Director インストールおよび構成ガイド』を参照してください。

クラウド セルの削除

ソフトウェアを再インストールするため、またはその他の理由により、クラウド セルは vCloud Director インストール環境から削除することができます。

到達不可能になったセルを削除することもできます。

前提条件

`service vmware-vcd stop` コマンドを使用して、セルを停止する必要があります。

手順

- 1 [管理および監視] タブをクリックし、左側のペインの [クラウド セル] をクリックします。
- 2 セル名を右クリックし、[削除] を選択します。

結果

vCloud Director によって、そのセルに関する情報がデータベースから削除されます。

クラウド セルのメンテナンス メッセージの表示

セルを停止してメンテナンスを実行していることをユーザーに知らせるために、メンテナンス メッセージを表示できます。

メンテナンス メッセージをオンにすると、ブラウザからセルにログインしようとするユーザーにメッセージが表示され、このセルはメンテナンスのために使用できないということが示されます。vCloud API を使用してセルに到達しようとするユーザーも、同様のメッセージを受け取ります。

手順

- 1 `service vmware-vcd stop` コマンドを使用して、セルを停止します。
- 2 `/opt/vmware/vcloud-director/bin/vmware-vcd-cell maintenance` コマンドを実行します。

結果

これで、ユーザーはブラウザまたは vCloud API を使用してセルにアクセスできません。

クラウド セルのメンテナンス メッセージの非表示

メンテナンスの実行がセルで終了し、このセルを再起動する準備ができた場合、メンテナンス メッセージを非表示にすることができます。

手順

- ◆ セルで次のコマンドを実行して、メンテナンス メッセージをオフにします。

```
[root@cell11 /opt/vmware/vcloud-director/bin]# service vmware-vcd restart
```


結果

これで、ユーザーはブラウザまたは vCloud API を使用してセルにアクセスできます。

サービス オファリングの管理

サービス オファリングによって、製品とプラットフォームを仮想データセンターのサービスとして提供することができます。

vCloud Director と他の VMware 製品との互換性に関する最新情報については、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、英語) を参照してください。

サービス オファリングの統合を有効にするには、[vCloud API を使用して vCloud Director サービス オファリングの統合を有効にする](#) を参照してください。

■ 拡張機能の登録

拡張機能を登録し、vCloud Director 内で vFabric Data Director または Cloud Foundry サービスを提供します。

■ 拡張機能のプロパティの表示または変更

拡張機能のタイプおよび関連するサービス オファリングを表示し、名前、ネームスペース、ユーザー名、パスワードなど、拡張機能のプロパティを変更することができます。

■ サービス オファリングと組織仮想データセンターの関連付け

拡張サービスを組織仮想データセンターに関連付けて、それらのサービスを仮想データセンターの仮想マシンで使用可能にすることができます。

■ 組織仮想データセンターからサービス オファリングの関連付けを解除する

組織仮想データセンターからサービス オファリングの関連付けを解除し、組織仮想データセンターの仮想マシンからサービスへのアクセスを削除することができます。

■ 拡張機能の登録解除

拡張機能を登録解除し、vCloud Director からサービスへのアクセスを削除することができます。

■ サービス インスタンスの作成

組織仮想データセンターの仮想マシンによって使用できるサービス インスタンスを作成します。

■ サービス インスタンス プロパティの変更

名前、説明、パラメータなど、サービス インスタンスのプロパティを変更することができます。

■ 仮想マシンへのサービス インスタンスの追加

組織仮想データセンターの仮想マシンに、組織仮想データセンターの任意のサービス インスタンスを追加することができます。

■ サービス インスタンスの削除

組織仮想データセンターからサービス インスタンスを削除できます。

拡張機能の登録

拡張機能を登録し、vCloud Director 内で vFabric Data Director または Cloud Foundry サービスを提供します。

前提条件

- vCloud Director でのサービス オファリングの統合を有効化します。[vCloud API を使用して vCloud Director サービス オファリングの統合を有効にする](#) を参照してください。
- vFabric Data Director または Cloud Foundry のバージョンがサポートされていることを確認します。[サービス オファリングの管理](#) を参照してください。
- vFabric Data Director または Cloud Foundry インストールの URL または IP アドレスにアクセス可能であることを確認します。

手順

- 1 [管理および監視] タブをクリックし、[拡張機能] をクリックします。
- 2 [追加] をクリックします。
- 3 ドロップダウン メニューから拡張機能のタイプを選択します。

オプション	説明
Data Director	VMware vFabric Data Director 拡張機能を登録します。vCloud Director は VMware vFabric Data Director バージョン 2.7 サービスをサポートします。
Cloud Foundry	Cloud Foundry 拡張機能を登録します。vCloud Director は Cloud Foundry プラットフォーム バージョン 1.0 サービスをサポートします。

- 4 拡張機能のネームスペースを入力します。
- 5 拡張機能の名前と、必要に応じて説明を入力します。
- 6 拡張機能に使用する vFabric Data Director または Cloud Foundry インストールの URL または IP アドレスを入力します。
- 7 拡張機能のユーザー名とパスワードを入力し、[OK] をクリックします。

次のステップ

仮想データセンターに拡張機能のサービス オファリングを関連付けます。[サービス オファリングと組織仮想データセンターの関連付け](#) を参照してください。

拡張機能のプロパティの表示または変更

拡張機能のタイプおよび関連するサービス オファリングを表示し、名前、ネームスペース、ユーザー名、パスワードなど、拡張機能のプロパティを変更することができます。

手順

- 1 [管理および監視] タブをクリックし、[拡張機能] をクリックします。
- 2 拡張機能を右クリックし、[プロパティ] を選択します。

- 3 (オプション) [全般] タブをクリックし、拡張機能の新しい設定を入力します。
- 4 (オプション) [サービス オファリング] タブをクリックし、拡張機能に関連付けられたサービス オファリングを表示します。
- 5 [OK] をクリックします。

サービス オファリングと組織仮想データセンターの関連付け

拡張サービスを組織仮想データセンターに関連付けて、それらのサービスを仮想データセンターの仮想マシンで使用可能にすることができます。

前提条件

vCloud Director を使用して拡張機能を登録します。 [拡張機能の登録](#) を参照してください。

手順

- 1 [管理および監視] タブをクリックし、[拡張機能] をクリックします。
- 2 サービス オファリングに関連付ける拡張機能を右クリックし、[サービス オファリングの関連付け] を選択します。
- 3 関連付けるサービス オファリングを選択して、[次へ] をクリックします。
- 4 サービス オファリングに関連付け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 サービス オファリングの関連付けを確認し、[完了] 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の仮想マシンによって使用するサービス インスタンスを作成します。 [サービス インスタンスの作成](#) を参照してください。

組織仮想データセンターからサービス オファリングの関連付けを解除する

組織仮想データセンターからサービス オファリングの関連付けを解除し、組織仮想データセンターの仮想マシンからサービスへのアクセスを削除することができます。

手順

- 1 [管理および監視] タブをクリックし、[拡張機能] をクリックします。
- 2 サービス オファリングに関連させる拡張機能を右クリックし、[サービス オファリングの関連付け解除] を選択します。
- 3 関連付けを解除するサービス オファリングを選択し、[次へ] をクリックします。
- 4 サービス オファリングの関連付けを解除す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 サービス オファリングの関連付けの解除を確認し、[完了] をクリックします。

拡張機能の登録解除

拡張機能を登録解除し、vCloud Director からサービスへのアクセスを削除することができます。

手順

- 1 [管理および監視] タブをクリックし、[拡張機能] をクリックします。
- 2 拡張機能を右クリックし、[登録解除] を選択します。
- 3 [はい] をクリックします。

サービス インスタンスの作成

組織仮想データセンターの仮想マシンによって使用できるサービス インスタンスを作成します。

前提条件

組織仮想データセンターへのサービス オファリングの関連付け[サービス オファリングと組織仮想データセンターの関連付け](#) を参照してください。

手順

- 1 [管理および監視] タブをクリックし、[組織 VDC] をクリックします。
- 2 組織仮想データセンター名を右クリックし、[開く] を選択します。
- 3 [マイ クラウド] をクリックし、左側のペインで [サービス] をクリックします。
- 4 [追加] をクリックします。
- 5 このインスタンスに使用するサービス オファリングを選択し、[次へ] をクリックします。
- 6 必要なサービス オファリング パラメータの値をそれぞれ入力して[次へ] をクリックします。
- 7 サービス インスタンスの名前と、必要に応じて説明を入力し、[次へ] をクリックします。
- 8 サービス オファリングの構成を確認し、[完了] をクリックします。

次のステップ

サービス インスタンスを仮想マシンに追加します。[仮想マシンへのサービス インスタンスの追加](#) を参照してください。

サービス インスタンス プロパティの変更

名前、説明、パラメータなど、サービス インスタンスのプロパティを変更することができます。

手順

- 1 [管理および監視] タブをクリックし、[組織 VDC] をクリックします。
- 2 組織仮想データセンター名を右クリックし、[開く] を選択します。
- 3 [マイ クラウド] をクリックし、左側のペインで [サービス] をクリックします。
- 4 削除するサービス インスタンスを右クリックし、[プロパティ] を選択します。
- 5 (オプション) [全般] をクリックして、サービス インスタンスの新しい名前および説明を入力します。
- 6 (オプション) [パラメータ] をクリックして、サービス インスタンス パラメータの新しい値を入力します。

7 [OK] をクリックします。

仮想マシンへのサービス インスタンスの追加

組織仮想データセンターの仮想マシンに、組織仮想データセンターの任意のサービス インスタンスを追加することができます。

前提条件

組織仮想データセンターにサービス インスタンスを作成します。[サービス インスタンスの作成](#) を参照してください。

手順

- 1 [管理および監視] タブをクリックし、[組織 VDC] をクリックします。
- 2 組織仮想データセンター名を右クリックし、[開く] を選択します。
- 3 [マイ クラウド] をクリックし、左側のペインで [仮想マシン] をクリックします。
- 4 仮想マシンを右クリックし、[プロパティ] を選択します。
- 5 [サービス] タブをクリックします。
- 6 追加するサービス インスタンスを選択して、[追加] をクリックします。

サービス インスタンスを選択すると、そのパラメータがダイアログ ボックスの下部に表示されます。

7 OK をクリックします。

サービス インスタンスの削除

組織仮想データセンターからサービス インスタンスを削除できます。

手順

- 1 [管理および監視] タブをクリックし、[組織 VDC] をクリックします。
- 2 組織仮想データセンター名を右クリックし、[開く] を選択します。
- 3 [マイ クラウド] をクリックし、左側のペインで [サービス] をクリックします。
- 4 削除するサービス インスタンスを右クリックし、[削除] を選択します。
- 5 [はい] をクリックします。

マルチサイト展開の設定と管理

vCloud Director マルチサイト機能を使用すると、サービス プロバイダ、または地理的に分散した複数の vCloud Director インストール（サーバ グループ）のテナントが、これらのインストールおよびその組織を単一エンティティとして管理および監視できます。

2 つの vCloud 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 vCloud Director テナント ポータルを使用して、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。リモートの関連付けメンバーが所有するリソースにアクセスするために、vCloud Director Web コンソールは使用できません。

重要： サイトを関連付けるには、vCloud API を使用する必要があります。2 つのサイトが関連付けられた後、vCloud API または vCloud Director のテナント ポータルを使用して、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。サービス プロバイダ向け vCloud API プログラミング ガイド および vCloud Director Tenant Portal Guide 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、vCloud Director サーバ グループ (vCloud 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 vCloud 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 vCloud Director サーバ グループで管理権限を持つシステム管理者は、vCloud 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 vCloud 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 アクセス制御

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) に届く要求を、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。サイトのセルが1つのみである場合を除いて、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。

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より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 vCloud 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 vCloud 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 vCloud 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 vCloud API 要求を行うことができます。

オブジェクト メタデータの作成または更新

vCloud Director には、ユーザー定義メタデータをオブジェクトに関連付けるための汎用機能があります。管理者またはオブジェクトの所有者は、オブジェクトのプロパティ ページにある [メタデータ] タブを使用して、オブジェクトのメタデータにアクセスできます。

オブジェクトのメタデータにより、サービス プロバイダおよびテナントはユーザー定義プロパティ (*name=value* のペア) をオブジェクトに柔軟に関連付けることができます。オブジェクト メタデータは、オブジェクトがコピーされても保持されます。また、vCloud API クエリ フィルタ式に含めることができます。

オブジェクトの所有者は、次のタイプのオブジェクトのメタデータを作成または更新できます。

- カタログ
- カタログ項目
- 独立したディスク
- メディア
- 組織 VDC ネットワーク
- vApp
- vApp テンプレート
- 仮想マシン

次のタイプのオブジェクトのメタデータを作成または更新できるのは、システム管理者のみです。

- プロバイダ VDC
- プロバイダ VDC ストレージ プロファイル
- 組織 VDC
- VdcStorageProfile

手順

1 オブジェクトの [プロパティ] ページを開きます。

2 [メタデータ] タブをクリックします。

このタブには、既存のすべてのメタデータが表示されます。また、メタデータの新規作成や既存のメタデータの更新が可能です。

3 (オプション) メタデータを新規作成します。

a ドロップダウン メニューからメタデータの [タイプ] を選択します。

b メタデータの [名前] と [値] を入力します。

名前は、このオブジェクトに関連付けられているメタデータ名の領域内で一意にする必要があります。

c 新しいメタデータ アイテムにアクセス レベルを指定します。

システム管理者は、このタブを使用して、作成したメタデータ アイテムへのユーザー アクセスを制限できます。システム管理者以外の任意のユーザーに対して、メタデータ アイテムを非表示にすることもできます。

d [追加] をクリックして、新しいメタデータ アイテムをオブジェクトに関連付けます。

4 (オプション) 既存のメタデータを更新します。

- a [既存のメタデータ] アイテムをダブルクリックします。
- b アイテムを変更または削除します。

オプション	説明
更新	アイテムの値を更新します。メタデータ アイテムの名前を変更することはできませんが、既存のアイテムを削除して、別の名前で新規作成することができます。
削除	アイテムを削除します。
リセット	編集中のアイテムを前の値に戻します。

vSphere リソースの管理

6

vSphere のリソースを vCloud Director システムに追加した後は、vCloud Director からいくつかの管理機能を実行できます。また、vSphere Client を使用してこれらのリソースを管理できます。

vSphere のリソースには、vCenter Server、リソース プール、ESXi ホスト、データストア、ネットワーク スイッチとポートなどがあります。

この章には、次のトピックが含まれています。

- vCenter Server の管理
- 仮想マシンとホスト間のアフィニティ ルールの管理
- vApp の検出および採用
- vSphere データストアの管理
- 取り残されたアイテムの管理
- リソース プールのプロパティの表示
- ストレージ ポリシーのプロパティの表示

vCenter Server の管理

vCenter Server インスタンスを vCloud Director インストールに接続した後で、設定を変更し、インスタンスを再接続して、有効または無効にすることができます。

重要： vCloud Director Web Console でサポートされるのは、NSX Manager インスタンスに関連付けられた vCenter Server インスタンスのみです。NSX Manager インスタンスに関連付けられていない vCenter Server インスタンスを取得および管理するには、vCloud API を使用する必要があります。

vCenter Server への vCloud Director の登録

vCloud Director インストールを使用先の vCenter Server システムに登録します。

vCloud Director を接続先の vCenter Server インスタンスに登録すると、vSphere Client Solutions Manager タブに拡張機能として表示されます。さらに、vCloud Director が管理する仮想マシンの [管理者] プロパティが vSphere Client によって設定され、それらの仮想マシンが vSphere Client を使用して変更されないように保護します。

重要： この手順は、NSX Manager インスタンスに関連付けられている接続された vCenter Server インスタンスにのみ適用されます。NSX Manager インスタンスに関連付けられていない vCenter Server インスタンスを取得および管理するには、vCloud API を使用する必要があります。

手順

- 1 [管理および監視] タブの左側のペインで、[vCenter] をクリックします。
- 2 vCenter Server の名前を右クリックし、[更新] をクリックします。
- 3 [はい] をクリックします。

vCenter Server 設定の変更

vCenter Server インスタンスの接続情報が変更された場合や、vCloud Director での名前または説明の表示方法を変更する場合は、設定を変更できます。

重要： この手順は、NSX Manager インスタンスに関連付けられている接続された vCenter Server インスタンスにのみ適用されます。NSX Manager インスタンスに関連付けられていない vCenter Server インスタンスを取得および管理するには、vCloud API を使用する必要があります。

手順

- 1 [管理および監視] タブの左側のペインで、[vCenter] をクリックします。
- 2 ターゲット vCenter Server の名前を右クリックし、[プロパティ] をクリックします。
- 3 [全般] タブで設定を編集し、[OK] をクリックします。

オプション	説明
[ホスト名または IP アドレス]	vCenter Server インスタンスの FQDN または IP アドレス
[ポート番号]	vCenter Server インスタンスの HTTPS ポート
[ユーザー名]	管理者の vCenter Single Sign-On アカウントのユーザー名
[パスワード]	vCenter Single Sign-On 管理者ユーザーのパスワード
[vCenter 名]	vCloud Director の vCenter Server インスタンスの名前

オプション	説明
[説明]	vCloud Director の vCenter Server インスタンスのオプションの説明
[vSphere Web Client の URL]	<p>vCenter Server vSphere Web Client のオプションの URL です。</p> <ul style="list-style-type: none"> ■ vSphere Lookup Service を使用するように vCloud Director インストールを設定した場合は、[vSphere サービスを利用してこの URL を提供] を選択します。 ■ vSphere Lookup Service を使用するように vCloud Director インストールが設定されていない場合は、[次の URL を使用] を選択して、URL を手動で入力します。

次のステップ

vCenter Server インスタンスの接続情報を変更した場合は、[vCenter Server インスタンスの再接続](#) を実行できます。

vCenter Server インスタンスの再接続

vCloud Director と vCenter Server インスタンスとの接続が切断された場合、または接続設定を変更する場合は、再接続を試みることができます。

重要： この手順は、NSX Manager インスタンスに関連付けられている接続された vCenter Server インスタンスにのみ適用されます。NSX Manager インスタンスに関連付けられていない vCenter Server インスタンスを取得および管理するには、vCloud API を使用する必要があります。

手順

- 1 [管理および監視] タブの左側のペインで、[vCenter] をクリックします。
- 2 ターゲット vCenter Server の名前を右クリックし、[vCenter の再接続] をクリックします。
- 3 情報メッセージを確認し、[はい] をクリックします。

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には、vCenter Server インスタンスを無効にします。

重要： この手順は、NSX Manager インスタンスに関連付けられている接続された vCenter Server インスタンスにのみ適用されます。NSX Manager インスタンスに関連付けられていない vCenter Server インスタンスを取得および管理するには、vCloud API を使用する必要があります。

手順

- 1 [管理および監視] タブの左側のペインで、[vCenter] をクリックします。
- 2 ターゲット vCenter Server の名前を右クリックし、[無効化] または [有効化] をクリックします。
- 3 [はい] をクリックします。

vCenter Server インスタンスの削除

vCenter Server インスタンスのリソースの使用を停止するには、vCloud 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。

重要： この手順は、NSX Manager インスタンスに関連付けられている接続された vCenter Server インスタンスにのみ適用されます。NSX Manager インスタンスに関連付けられていない vCenter Server インスタンスを取得および管理するには、vCloud API を使用する必要があります。

前提条件

vCenter Server インスタンスを無効にし、このリソース 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。

手順

- 1 [管理および監視] タブの左側のペインで、[vCenter] をクリックします。
- 2 ターゲット vCenter Server の名前を右クリックし、[分離] をクリックします。
- 3 [はい] をクリックします。

NSX Manager 設定の変更

NSX Manager 設定を変更するか、別の NSX Manager インスタンスを接続する場合は、NSX Manager 接続の設定を変更できます。クロス仮想データセンター ネットワークを有効にする場合は、NSX Manager インスタンスを DLR コントロール仮想マシンの詳細で設定する必要があります。

重要： この手順は、vCenter Server に関連付けられている NSX Manager インスタンスにのみ適用されます。vCenter Server に関連付けられていない NSX Manager インスタンスを取得および管理するには、vCloud API を使用する必要があります。

手順

- 1 [管理および監視] タブの左側のペインで、[vCenter] をクリックします。
- 2 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 システムを右クリックして、[プロパティ] をクリックします。
- 3 [NSX Manager] タブで新しい設定を入力し、[OK] をクリックします。

NSX Manager のホスト名および管理者の認証情報を変更できます。この vCenter Server インスタンスでバックアップされる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場合、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 コンポーネントで 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。

オプション	説明
コントロール仮想マシンのリソース プールの vCenter Server 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 。
コントロール仮想マシンのデータストア名	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 。
コントロール仮想マシンの管理インターフェイス名 (HA 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、『vCloud Director Tenant Portal Guide』を参照してください。

仮想マシンとホスト間のアフィニティ ルールの管理

vCloud Director システム管理者は、リソース プール内に仮想マシン グループを作成した後、仮想マシンとホストのアフィニティ ルールを使用して、仮想マシン グループのメンバーを vSphere ホスト DRS グループのメンバーにデプロイする必要があるかどうかを指定できます。

vCloud Director システム管理者は、vCloud Director 仮想マシンとホストのアフィニティ ルールを使用して、vSphere Distributed Resource Scheduler (DRS) でリソース プール内のホストに仮想マシンをどのように配置するかを指定できます。仮想マシンとホストのアフィニティ ルールは、ホストベールのライセンスに基づき、特定のアプリケーションを実行している仮想マシンを、それらのアプリケーションを実行するためのライセンスが割り当てられているホスト上に配置する必要がある場合に便利です。また、ワークロード固有の設定を含む仮想マシンを、特定の特性を持つホスト上に配置する必要がある場合にも便利です。テクニカル ホワイト ペーパー『Best Practices for Performance Tuning of Telco and NFV Workloads in vSphere』(<http://www.vmware.com/files/pdf/techpaper/vmware-tuning-telco-nfv-workloads-vsphere.pdf>) に、特定のプロパティを持つホストを必要とする仮想マシン構成の例がいくつか記載されています。

vCloud Director 9.5 以降、サービス プロバイダは VDC コンピューティング ポリシーを使用して、テナントに仮想マシン グループを公開できます。

ホスト グループと仮想マシン グループ

vSphere 仮想マシンとホストのアフィニティ ルールは [仮想マシンからホストへ] タイプのルールであり、ホスト グループと仮想マシン グループを指定する必要があります。vCloud Director システム管理者が仮想マシンとホストのアフィニティ ルールを作成するには、事前に vSphere 管理者が vCloud Director プロバイダ仮想データセンターにマッピングされたリソース プール内に少なくとも 1 つのホスト DRS グループを作成し、vSphere 管理者または vCloud Director システム管理者が同じリソース プール内に仮想マシン グループを作成する必要があります。仮想マシンとホストのアフィニティ ルールは、ホスト DRS グループ内のすべてのホストに対する、仮想マシン グループに含まれるすべてのメンバーのアフィニティを表すため、仮想マシンによってホストに要求される可能性が

ある特性がグループ内のすべてのホストで共有されている必要があります。たとえば、適用されているアプリケーション ライセンスに基づいてホストをグループ化し、必要なアプリケーション ライセンスに基づいて仮想マシンをグループ化することができます。そうすることで、必要なライセンスが適用されているホストに仮想マシンが配置されるように、仮想マシンとホストのアフィニティ ルールを作成できるようになります。

仮想マシンとホストのアフィニティ ルールはリソース プールのプロパティであるため、ルールの適用対象となるグループに含まれるメンバーはすべて同じリソース プールにデプロイされる必要があります。仮想マシンまたはホストがリソース プールから削除された場合、メンバーであった仮想マシン グループまたはホスト グループからも自動的に削除されます。ただし、ホストまたは仮想マシンがリソース プールに戻された場合、グループは自動的に更新されません。

アフィニティ ルールの相互作用と競合

リソース プールに仮想マシンとホストのアフィニティ ルールが複数ある場合は、すべてのルールに同じ優先順位が割り当てられます。そのため、ルール間の相互作用に関して考慮すべき点がいくつかあります。たとえば、2 つの仮想マシン グループに所属する仮想マシンがあり、それぞれのグループが異なる必須の仮想マシンとホストのアフィニティ ルールで指定されている場合、その仮想マシンは両方のホスト グループに所属するホスト上でのみ実行できます。仮想マシンとホストのアフィニティ ルールの作成時に、システムはこのような相互作用の可能性を確認しません。

ただし、複数の必須ルールが適用された場合に発生する可能性がある競合については確認されます。たとえば、異なる必須アフィニティ ルールの適用対象となる別々のグループに所属する仮想マシンおよびホストに適用される必須の非アフィニティ ルールを作成できるように仮想マシンとホストをグループ化した場合、システムはいずれのルールも適用できません。2 つ以上の仮想マシンとホストのアフィニティ ルールがこのように競合する場合、システムは最も古いルールを適用し、その他のルールを無効にします。この問題を解決するには、ルールを必須ではなくオプションにするか、このような必須ルールの競合の可能性が極力少なくなるように仮想マシンとホストをグループ化します。

アフィニティ ルールと vSphere リソース管理

DRS、vSphere HA、vSphere DPM などの vSphere リソース管理機能は、必須に設定された仮想マシンとホストのアフィニティ ルールに違反する可能性があるアクションを実行しません。

- DRS は、ホストをメンテナンス モードにするために仮想マシンを退避させません。
- DRS は、仮想マシンのパワーオンや仮想マシンのロード バランシングを行いません。
- vSphere HA は、フェイルオーバーを実行しません。
- vSphere DPM は、ホストをスタンバイ モードにして電源管理を最適化することをしません。

このような状況を回避するため、特定の仮想マシンとホストのペアに影響する必須のアフィニティ ルールを複数作成する場合は注意が必要です。ホストが失われたことによりルールの適用対象となる仮想マシンを実行できるホストが 1 台も存在しなくなることがないように、十分な数のホストがリソース プールに含まれていることを確認してください。必須でないルールは、DRS、vSphere HA、および vSphere DPM を正しく機能させるために無視される場合があります。

ホスト グループの作成または更新

ホスト グループは、vSphere ホストの DRS グループです。vSphere 管理者は、vCloud Director 仮想マシンとホストのアフィニティ ルールでホスト DRS グループを使用する前に、vCloud Director プロバイダ仮想データセンターにマッピングされたリソース プール内にホスト DRS グループ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にマッピングされているリソース プール内に作成された vSphere ホスト DRS グループはそれらのリソース プール内に表示され、仮想マシンとホストのアフィニティ ルールで指定することができます。ホスト DRS グループの詳細については、VMware vSphere ESXi および vCenter Server のドキュメントを参照してください。

手順

- ◆ ホスト グループはリソース プールのプロパティです。[vSphere のプロパティ] にある [リソース プール] リストからリソース プールを選択します。

リソース プール内のホスト DRS グループが、そのリソース プールの [ホスト グループ] タブに表示されます。

仮想マシン グループの作成または更新

仮想マシン グループは、類似するホスト要件を持つ仮想マシンの集合です。仮想マシンはすべて同じリソース プールに属している必要があります。

前提条件

仮想マシン グループを作成または更新できるのはシステム管理者のみです。

手順

- 1 仮想マシン グループはリソース プールのプロパティです。[vSphere のプロパティ] にある [リソース プール] リストからリソース プールを選択します。

リソース プール内の仮想マシン グループが、そのリソース プールの [仮想マシン グループ] タブに表示されます。すべてのリソース プール内にあるすべての仮想マシン グループのリストを表示するには、[vSphere のプロパティ] にある [仮想マシン グループ] をクリックします。

- 2 リソース プール内に仮想マシン グループを作成するには、[仮想マシン グループ] タブにあるプラス記号のアイコンをクリックして [仮想マシン グループの作成] ウィンドウを開きます。

グループに名前を付け、[OK] をクリックします。

グループが作成され、仮想マシンを追加できるようになります。

- 3 仮想マシン グループを編集して仮想マシンを追加または削除するには、[vSphere のプロパティ] にある [仮想マシン グループ] をクリックし、[仮想マシン グループ] リスト内のグループ名を右クリックして、[編集] を選択します。

オプション	アクション
グループに仮想マシンを追加	上部のテーブルから 1 つ以上の仮想マシンを選択し、[追加] をクリックします。
グループから仮想マシンを削除	下部のテーブルから 1 つ以上の仮想マシンを選択し、[削除] をクリックします。

仮想マシンとホストのアフィニティ ルールの作成または更新

仮想マシンとホストのアフィニティ ルールは、同じリソース プール内のホスト グループと仮想マシン グループの関係を定義します。システム管理者は、仮想マシンとホストのアフィニティ ルールを作成したり、削除したり、有効または無効にしたりすることができます。

仮想マシンとホストのアフィニティ ルールを作成した後は、次のようにルールを更新できます。

- ルールを有効にする。
- ルールを無効にする。
- ルールを削除する。

その他の変更を加えるには（たとえば、仮想マシン グループまたはホスト グループを変更するには）、新しいルール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にマッピングされているリソース プール内に作成された vSphere 仮想マシンとホストのアフィニティ ルールは、[vSphere のプロパティ] にある [リソース プール] リストに表示される各プール内に表示されます。ホスト DRS の仮想マシンとホストのアフィニティの詳細については、VMware vSphere ESXi および vCenter Server のドキュメントを参照してください。

前提条件

- この操作は、システム管理者に制限されます。
- ホスト グループと仮想マシン グループが含まれていないリソース プールでは、仮想マシンとホストのアフィニティ ルールを作成できません。

手順

- 1 ルールを追加するリソース プールを選択します。

[vSphere のプロパティ] にある [リソース プール] リストからリソース プールを選択します。リソース プール内の仮想マシンとホストのアフィニティ ルールが、そのリソース プールの [アフィニティ ルール] タブに表示されます。

- 2 リソース プール内に仮想マシンとホストのアフィニティ ルールを作成するには、[アフィニティ ルール] タブにあるプラス記号のアイコンをクリックして [新しい仮想マシンとホストのアフィニティ ルール] ウィンドウを開きます。

ルールの名前、仮想マシン グループ、およびホスト グループを指定する必要があります。

- a [ルール名] フィールドに、ルールの名前を入力します。
- b ルールを適用する [仮想マシン グループ] と [ホスト グループ] を選択します。

ドロップダウン メニューを使用して、選択したリソース プール内にあるすべての仮想マシン グループとホスト グループを一覧表示します。少なくとも 1 つの仮想マシン グループとホスト グループがリソース プールに含まれていない場合は、ルールを作成できません。

- c ルールの極性を指定します。アフィニティ ルールを作成するには、[ホスト上で実行する必要があります] をクリックします。非アフィニティ ルールを作成するには、[ホスト上では実行できません] をクリックします。

- d ルールを有効または無効にします。
- e ルールに必須にするかどうかを指定します。

ルールを必須にすると、システムの動作に影響する競合が発生する可能性が高くなります（特に、複数の必須ルールが仮想マシンに適用されている場合）。[アフィニティ ルールの相互作用と競合](#)を参照してください。

- 3 既存の仮想マシンとホストのアフィニティ ルールを有効または無効にする、または削除するには、[アフィニティ ルール] タブでルール名を右クリックし、いずれかのアクションを選択します。

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 つの仮想マシンが含まれており、vCloud 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、プロバイダ VDC にある指定されたリソース プールを採用する組織 VDC を vCloud API で作成できます。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 Server 仮想マシンが vCloud Director で検出されない場合、[vCenterServer 仮想マシン検出のデバッグ](#)により、潜在的な原因を調査できます。

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] チェック ボックスをオフにする必要があります。組織管理者は、vCloud API を使用して、個々の仮想データセンターで仮想マシンの検出を無効にすることも、組織内のすべての仮想データセンター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のと同様の方法で、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、vCloud 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 vCloud 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 で設定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。

vSphere データストアの管理

vCloud Director システムの vSphere データストアを有効または無効にしたり、データストアのディスク領域低残量の警告を構成したり、vCloud Director システムからデータストアを削除。

データストアの有効化または無効化

プロバイダ仮想データセンターに追加されたデータストアを有効化または無効化することができます。vCloud Director からデータストアを削除するには、事前にそのデータストアを無効化する必要があります。

データストアを無効化すると、そのデータストアに関連付けられている vApp を開始したり、そのデータストアで vApp を作成したりすることはできなくなります。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [データストア] をクリックします。
- 2 データストア名を右クリックし、[有効化] または [無効化] を選択します。

結果

vCloud Director は、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のデータストアを有効化または無効化します。

データストアの低ディスク領域警告の構成

データストアで使用可能な容量として指定したしきい値に到達したら vCloud Director から電子メールを受信するように、データストアの低ディスク領域警告を構成できます。これらの警告により、問題が発生する前に、ディスク領域が少ないことが通知されます。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [データストア] をクリックします。
- 2 データストア名を右クリックし、[プロパティ] を選択します。
- 3 [全般] タブで、データストアのディスク領域のしきい値を選択します。

黄色と赤の 2 つのしきい値を設定できます。vCloud Director が電子メール アラートを送信するとき、メッセージには、どちらのしきい値を超えたのかが示されます。

- 4 [OK] をクリックします。

結果

vCloud Director は、データストアがしきい値を超えると電子メール警告を送信します。

データストアでの高速プロビジョニングのために VAAI を有効化

高速プロビジョニングのために VAAI を有効化すると、互換性のある複数の NFS アレイでクローン操作の負荷を分散できます。

重要: ネイティブ スナップショットを使用するストレージ コンテナでは、高速プロビジョニングされた仮想マシンのインプレース統合はサポートされていません。VVOL および VAAI 対応のデータストアではネイティブ スナップショットが使用されるので、これらのストレージ コンテナの 1 つにデプロイされた、高速プロビジョニングされた仮想マシンは統合できません。VVOL または VAAI 対応のデータストアにデプロイされた、高速プロビジョニングされた仮想マシンを統合する必要がある場合は、仮想マシンを別のストレージ コンテナに再配置する必要があります。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [データストア] をクリックします。
- 2 データストア名を右クリックし、[プロパティ] を選択します。
- 3 [全般] タブで、[高速プロビジョニングのために VAAI を有効化] を選択します。
- 4 [OK] をクリックします。

取り残されたアイテムの管理

vCloud Director のオブジェクトを削除するときに、そのオブジェクトが vSphere にも存在すると、vCloud Director は、vSphere にあるそのオブジェクトを削除しようとします。状況によっては、vCloud Director が vSphere にあるオブジェクトを削除できず、その場合にはオブジェクトが取り残されます。

取り残されたアイテムの一覧を表示してもう一度削除を試みるか、vSphere Client を使用して vSphere に取り残されたオブジェクトを削除できます。

取り残されたアイテムの削除

vCloud Director からすでに削除されているオブジェクトを vSphere から削除するためには、取り残されたアイテムを削除できます。

手順

- 1 [管理および監視] タブをクリックし、左側のペインの [取り残されたアイテム] をクリックします。
- 2 取り残されたアイテムを右クリックし、[削除] を選択します。
- 3 [はい] をクリックします。

vCloud Director が、vSphere から取り残されたアイテムの削除を試みます。

- 4 ページの表示を更新します。

削除操作が正常に行われると、vCloud Director により、取り残されたアイテムの一覧からそのアイテムが削除されます。

次のステップ

削除操作に失敗した場合は、そのアイテムを強制的に削除できます。[取り残されたアイテムの強制削除](#)を参照してください。

取り残されたアイテムの強制削除

vCloud Director で取り残されたアイテムを削除できない場合は、強制削除を実行して、取り残されたアイテムのリストから削除できます。取り残されたアイテムは、vSphere 内に存在し続けます。

取り残されたアイテムを強制的に削除する前に、通常の削除を試みてください。[取り残されたアイテムの削除](#)を参照してください。

手順

- 1 [管理および監視] タブをクリックし、左側のペインの [取り残されたアイテム] をクリックします。
- 2 取り残されたアイテムを右クリックし、[強制削除] を選択します。
- 3 [はい] をクリックします。

結果

vCloud Director により、取り残されたアイテムの一覧からそのアイテムが削除されます。

リソース プールのプロパティの表示

メモリ予約やリソース プールで使用可能なデータストアなどのリソース プールのプロパティを表示できます。

手順

- 1 [管理および監視] タブで、[リソース プール] をクリックします。
- 2 リソース プールを右クリックし、[プロパティ] をクリックします。

結果

vCloud Director にリソース プールの以下のプロパティが表示されます。

表 6-1. リソース プールのプロパティ

プロパティ	説明
[名前]	リソース プールの名前。
[メモリ予約 (使用済み/合計)]	リソース プールの合計および使用済みメモリ予約 (MB 単位)。
[CPU 予約 (使用済み/合計)]	リソース プールの合計および使用済みメモリ予約 (MHz 単位)。
[データストア]	リソース プールで使用可能な各データストアの名前。
[タイプ]	リソース プールで使用可能な各データストアのタイプ。
[接続中]	リソース プールで使用可能なデータストアのうち接続されているもの。緑のチェックマークはデータストアが接続されていることを示します。赤い X はデータストアが切断されていることを示します。
[容量 (使用済み/合計)]	リソース プールで使用可能な各データストアの使用済みおよび合計容量。
[% 使用済み]	現在使用中の各データストアの割合。

ストレージ ポリシーのプロパティの表示

ストレージ ポリシーのデータストアおよびデータストアのクラスタを表示できます。

手順

- 1 [管理および監視] タブで、[ストレージ ポリシー] をクリックします。
- 2 ストレージ ポリシーを右クリックし、[プロパティ] をクリックします。

結果

vCloud Director にストレージ ポリシーのデータストアとデータストア クラスタのリストが表示されます。

組織の管理

7

組織を作成したら、組織のプロパティを変更したり、組織を有効化/無効化したり、削除したり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。

- 組織の有効化または無効化
- 組織の削除
- 組織へのカタログの追加
- 組織のプロパティの編集
- 組織リソースの管理
- 組織 vApp および仮想マシンの管理
- テナント ストレージの移行

組織の有効化または無効化

組織を無効化すると、ユーザーは組織にログインできなくなり、また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、組織が無効化されていても、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 [管理および監視] タブをクリックし、左側のペインで [組織] をクリックします。
- 2 組織名を右クリックし、[有効化] または [無効化] を選択します。

組織の削除

組織を削除して、vCloud Director から永続的に削除します。

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 [管理および監視] タブをクリックし、左側のペインで [組織] をクリックします。
- 2 組織名を右クリックし、[削除] を選択します。
- 3 [はい] をクリックします。

組織へのカタログの追加

アップロードおよびインポートされた vApp テンプレートとメディア ファイルを含めるために、組織にカタログを追加することができます。組織に複数のカタログを追加して、各カタログへのアクセスを個々に制御できます。

前提条件

カタログを作成する対象の組織が存在することを確認します。

手順

- 1 [ホーム] タブをクリックし、[組織へのカタログの追加] をクリックします。
- 2 組織名を選択し、[次へ] をクリックします。
- 3 カatalog名と、必要に応じて説明を入力し、[次へ] をクリックします。
- 4 発行オプションを選択し、[次へ] をクリックします。

オプション	説明
その他の組織にこのカタログを発行しない	カタログに追加した項目は、組織内のみで使用できます。
すべての組織に発行	カタログに追加した項目は、vCloud Director インストール環境のすべての組織で使用できます。各組織の管理者は、ユーザーに提供するカタログ項目を選択できます。

- 5 カatalog設定を確認し、[完了] をクリックします。

組織のプロパティの編集

組織の名前と説明、LDAP オプション、カタログ発行ポリシー、電子メール環境設定、およびストレージおよび処理の制限など、既存の組織のプロパティを編集できます。

■ 組織名の変更

vCloud Director のインストール環境の規模が大きくなるにつれて、既存の組織によりわかりやすい名前を割り当てることが必要になる場合があります。

■ 組織の完全な名前および説明の変更

vCloud Director のインストール環境の規模が大きくなるにつれて、既存の組織によりわかりやすい完全な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。

■ 組織の LDAP オプションの変更

LDAP サービスを使用して、組織にインポートするユーザーとグループのディレクトリを指定できます。LDAP サービスを指定しない場合は、組織のユーザーごとにユーザー アカウントを作成する必要があります。LDAP オプションは、システム管理者のみが設定でき、組織管理者が変更することはできません。

■ 組織のカatalog共有、公開、およびサブスクリプション ポリシーの変更

Catalogは、組織ユーザーが仮想マシンでの vApp の作成とアプリケーションのインストールに使用できる、vApp テンプレートとメディアのCatalogを提供します。Catalogは、vCloud Director の異なるインスタンス内の組織間、vCloud Director の同じインスタンス内の組織間で共有できるほか、アクセスをホスト組織内に限ることもできます。

■ 組織の電子メール環境設定の変更

vCloud Director には、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 サーバーが必要です。組織を作成したときに指定した設定を変更できます。

■ 組織のリース、割り当て容量、および制限の設定の変更

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消費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。

組織名の変更

vCloud Director のインストール環境の規模が大きくなるにつれて、既存の組織によりわかりやすい名前を割り当てるが必要になる場合があります。

前提条件

組織の名前を変更するには、事前に組織を無効にする必要があります。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織] をクリックします。
- 2 組織名を右クリックし、[プロパティ] を選択します。
- 3 [全般] タブで新しい組織名を入力し、[OK] をクリックします。

結果

新しい名前を反映して、内部の組織 URL が変更されます。

組織の完全な名前および説明の変更

vCloud Director のインストール環境の規模が大きくなるにつれて、既存の組織によりわかりやすい完全な名前または説明を割り当てるが必要になる場合があります。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織] をクリックします。
- 2 組織名を右クリックし、[プロパティ] を選択します。

- 3 [全般] タブで新しい完全な名前または説明を入力し、[OK] をクリックします。

組織の LDAP オプションの変更

LDAP サービスを使用して、組織にインポートするユーザーとグループのディレクトリを指定できます。LDAP サービスを指定しない場合は、組織のユーザーごとにユーザー アカウントを作成する必要があります。LDAP オプションは、システム管理者のみが設定でき、組織管理者が変更することはできません。

カスタム LDAP 設定の入力に関する詳細については、[システムの LDAP の設定](#) を参照してください。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織] をクリックします。
- 2 組織名を右クリックし、[プロパティ] を選択します。
- 3 [LDAP オプション] タブをクリックします。
- 4 組織ユーザーの新しいインポート元を選択します。

オプション	説明
LDAP を使用しない	組織管理者が組織内のユーザーごとにローカル ユーザー アカウントを作成します。このオプションを選択した場合、グループを作成できません。
VCD システム LDAP サービス	vCloud Director システムの LDAP サービスを、組織のユーザーおよびグループのインポート元として使用します。
カスタム LDAP サービス	組織を、組織独自の非公開 LDAP サービスに接続します。

- 5 選択した項目で必要とされる追加情報をすべて提供します。

オプション	操作
LDAP を使用しない	[OK] をクリックします。
VCD システム LDAP サービス	<p>(省略可能) 組織にインポートできるユーザーを制限するために使用する組織単位 (OU) の識別名を入力し、[OK] をクリックします。何も入力しない場合は、システム LDAP サービス内のすべてのユーザーを組織にインポートできます。</p> <p>注： OU を指定しても、インポートできる LDAP グループは制限されません。システム LDAP ルートから任意の LDAP グループをインポートできます。ただし、OU およびインポートされたグループの両方に属するユーザーのみが組織にログインできます。</p>
カスタム LDAP サービス	[カスタム LDAP] タブをクリックし、組織のカスタム LDAP 設定を入力して、[OK] をクリックします。

結果

現在ログインしているシステム管理者と組織管理者の場合、現在のセッションのキャッシュの期限が切れるか、ログアウトして再びログインするまで、変更した LDAP オプションを使用してユーザーとグループをインポートすることはできません。

組織のカatalog共有、公開、およびサブスクリプション ポリシーの変更

カタログは、組織ユーザーが仮想マシンでの vApp の作成とアプリケーションのインストールに使用できる、vApp テンプレートとメディアのカタログを提供します。カタログは、vCloud Director の異なるインスタンス内の組織間、vCloud Director の同じインスタンス内の組織間で共有できるほか、アクセスをホスト組織内に限ることもできます。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織] をクリックします。
- 2 組織名を右クリックし、[プロパティ] を選択します。
- 3 [カタログ] タブをクリックします。
- 4 カatalog公開オプションを選択し、[OK] をクリックします。

オプション	説明
カatalogを公開できません	組織管理者は、組織外のユーザーにはカatalogを公開できません。
すべての組織へのカatalogの公開を許可する	組織管理者は、すべての組織のユーザーにカatalogを公開できます。

- 5 組織のカatalog ポリシーを設定します。

オプション	説明
[他の組織へのカatalogの共有を許可する]	組織管理者がこの組織のカatalogを、vCloud 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。
[外部組織に使用されるカatalog フィードの作成を許可する]	組織管理者がこの組織のカatalogを、vCloud Director のこのインスタンスの外部の組織と共有することを許可します。
[外部カatalog フィードのサブスクリプションを許可]	組織管理者が、この組織が vCloud Director のこのインスタンスの外部からのカatalog フィードをサブスクライブすることを許可します。

- 6 [OK] をクリックします。

次のステップ

カatalogの同期中に、システムが過負荷になるのを回避するには、セル管理ツールを使用して同時に同期できるライブラリ アイテムの数を制限できます。[カatalog同期のスロットリングの設定](#)を参照してください。

組織の電子メール環境設定の変更

vCloud Director には、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 サーバーが必要です。組織を作成したときに指定した設定を変更できます。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織] をクリックします。
- 2 組織名を右クリックし、[プロパティ] を選択します。
- 3 [電子メールの環境設定] タブをクリックします。

4 SMTP サーバーのオプションを選択します。

オプション	説明
システム デフォルトの SMTP サーバーを使用	組織はシステムの SMTP サーバを使用します。
組織の SMTP サーバーを設定	組織は独自の SMTP サーバを使用します。このオプションを選択した場合、SMTP サーバの DNS ホスト名または IP アドレスとポート番号を入力します。(省略可能) [認証が必要] チェック ボックスをオンにし、ユーザー名とパスワードを入力します。

5 通知設定のオプションを選択します。

オプション	説明
システム デフォルトの通知設定を使用	組織はシステムの通知設定を使用します。
組織の通知設定を設定	組織は独自の通知設定を使用します。このオプションを選択した場合、組織の電子メールの送信者として表示される電子メール アドレスと件名のプリフィックスとして使用するテキストを入力し、受信者を選択します。

6 (オプション) 宛先のメール アドレスを入力し、[電子メール設定をテスト] をクリックして、すべての SMTP サーバー設定が正常に構成されていることを確認します。

7 [OK] をクリックします。

組織のリース、割り当て容量、および制限の設定の変更

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消費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。

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。

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。また、ストレージ リースの有効期限が切れた場合の vApp と vApp テンプレートの動作も指定できます。

割り当て容量により、組織内の各ユーザーが組織の仮想データセンターで格納およびパワーオンすることができる仮想マシンの数が決まります。指定した割り当て容量は、組織に追加されるすべての新しいユーザーのデフォルトとして機能します。

コピーや移動などの特定の vCloud Director 操作では、他の操作より多くのリソースが消費されます。制限値を設定して、リソースを大量に消費する操作が組織内のすべてのユーザーに影響を与えることを防止し、サービス拒否攻撃を防御することもできます。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織] をクリックします。
- 2 組織名を右クリックし、[プロパティ] を選択します。
- 3 [ポリシー] タブをクリックします。
- 4 vApp および vApp テンプレートのリース オプションを選択します。

5 実行中および格納された仮想マシンの割り当て容量を選択します。

ユーザー レベルで設定された割り当て容量は、組織レベルで設定された割り当て容量よりも優先されます。

6 リソースを大量に使用する操作、仮想マシンに対するコンソール接続数、および組織ごとのデータセンター数のシステム上限値を選択します。

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。
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。

これらの制限により、サービス拒否攻撃からの保護が可能になります。

7 [OK] をクリックします。

組織リソースの管理

vCloud Director 組織は、1 つ以上の組織仮想データセンターのためにリソースを取得します。組織でさらにリソースが必要な場合は、新しい組織仮想データセンターを追加するか、既存の組織仮想データセンターを変更できます。組織仮想データセンターを削除または変更して、組織からリソースを削除できます。

組織仮想データセンターの追加に関する詳細は、[組織仮想データセンターの作成](#)を参照してください。

組織仮想データセンターの削除に関する詳細は、[組織仮想データセンターの削除](#)を参照してください。

既存の組織仮想データセンターが使用できるリソースの変更にに関する詳細は、[組織仮想データセンターの割り当てモデルの設定の編集](#)および[組織仮想データセンター ストレージの設定の編集](#)を参照してください。

組織 vApp および仮想マシンの管理

システム管理者のみが実行できる、組織 vApp および仮想マシンの管理に関連するタスクがいくつかあります。たとえば、システム管理者は既存の vApp に vSphere 仮想マシンを追加したり、vSphere 仮想マシンに基いて vApp を作成したり、vApp をメンテナンス モードに設定したりすることができます。

組織の vApp の操作の詳細については、『VMware vCloud Director ユーザー ガイド』を参照してください。

vSphere 仮想マシンの vApp への追加

システム管理者は、vSphere 仮想マシンを既存の vCloud Director vApp にインポートできます。

前提条件

vCloud Director にシステム管理者としてログインしており、vApp が含まれている組織に利用できる組織仮想データセンターが存在する必要があります。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織] をクリックします。
- 2 組織名を右クリックし、[開く] を選択します。
- 3 [マイ クラウド] タブをクリックし、左側のペインで [vApp] をクリックします。
- 4 vApp 名を右クリックし、[開く] を選択します。
- 5 [仮想マシン] タブで、アクション ボタンをクリックし、[vSphere からのインポート] を選択します。
- 6 vCenter Server と仮想マシンを選択します。
- 7 仮想マシンの名前と、必要に応じて説明を入力します。
- 8 インポート元の仮想マシンをコピーするか、移動するかを選択します。
- 9 [OK] をクリックします。

vSphere 仮想マシンに基く vApp の作成

システム管理者は、vSphere 仮想マシンを vCloud Director vApp として組織にインポートできます。

前提条件

vCloud Director にシステム管理者としてログインしており、使用可能な組織仮想データセンターが組織に存在することを確認します。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織] をクリックします。
- 2 組織名を右クリックし、[開く] を選択します。
- 3 [マイ クラウド] タブをクリックし、左側のペインで [vApp] をクリックします。
- 4 [vSphere からのインポート] をクリックします。
- 5 vCenter Server と仮想マシンを選択します。
- 6 vApp の名前と、必要に応じて説明を入力し、インポート先となる組織仮想データセンターを選択します。
- 7 インポート元の仮想マシンをコピーするか、移動するかを選択します。
- 8 [OK] をクリックします。

vApp のメンテナンス モードへの設定

システム管理者は、vApp をメンテナンス モードにして、非管理者ユーザーが vApp の状態を変更できないようにすることができます。これは、サードパーティのバックアップ ソリューションを使用して vApp をバックアップする場合などに便利です。

vApp がメンテナンス モードになっているときには、システム管理者以外のユーザーは vApp やその仮想マシンの状態を変更するようなアクションは実行できません。vApp とその仮想マシンについての情報を表示したり、仮想マシン コンソールにアクセスしたりすることは可能です。

vApp をメンテナンス モードにしても、vApp が関与する実行中のタスクには影響はありません。

前提条件

vCloud Director にシステム管理者としてログインする必要があります。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織] をクリックします。
- 2 組織名を右クリックし、[開く] を選択します。
- 3 [マイ クラウド] タブをクリックし、左側のペインで [vApp] をクリックします。
- 4 vApp 名を右クリックし、[メンテナンス モードに切り替え] を選択します。
- 5 [はい] をクリックします。

結果

vApp のステータスが [メンテナンス モード] に変わります。[メンテナンス モードを終了] を選択するまで、vApp はメンテナンス モードのままです。

実行中の vApp の強制停止

組織ユーザーは、実行中の vApp を強制停止できませんが、システム管理者はできます。

ユーザーが、実行中の vApp を停止できない場合があります。従来の vApp 停止方法が失敗した場合、vApp を強制停止して、ユーザーに料金が請求されるのを防止できます。

vApp を強制停止しても、vApp が vSphere のリソースを消費することを防ぐわけではありません。vCloud Director で vApp を強制停止したら、vSphere Client を使用して vSphere の vApp のステータスを確認し、必要な操作を実行します。

前提条件

vCloud Director にシステム管理者としてログインする必要があります。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織] をクリックします。
- 2 組織名を右クリックし、[開く] を選択します。
- 3 [マイ クラウド] タブをクリックし、左側のペインで [vApp] をクリックします。
- 4 実行中の vApp を右クリックし、[強制停止] を選択します。
- 5 [はい] をクリックします。

仮想マシンの高速プロビジョニング

高速プロビジョニングでは、仮想マシンのプロビジョニング操作に対してリンク クローンを使用することにより時間を節約します。高速プロビジョニングは、組織 VDC ではデフォルトで有効化されます。

リンク クローンは、元の仮想マシンと同じベース ディスクを使用する仮想マシンの複製で、一連の差分ディスクを使用して元の仮想マシンとクローンの差分を追跡します。高速プロビジョニングを無効化すると、すべてのプロビジョニング操作はフル クローンになります。

リンク クローンは、元の仮想マシンとは異なる vCenter データセンターまたはデータストアに存在することはできません。vApp テンプレートに関連付けられた仮想マシンに対するリンク クローン作成を vCenter データセンターとデータストア全体でサポートするために、vCloud Director ではシャドウ仮想マシンを作成します。シャドウ仮想マシンは、元の仮想マシンの完全なコピーです。シャドウ仮想マシンは、リンク クローンが作成されるデータセンターとデータストアに作成されます。テンプレート仮想マシンに関連付けられているシャドウ仮想マシンのリストは、表示することができます。[vApp テンプレートに関連付けられているシャドウ仮想マシンの表示](#) を参照してください。

重要： ネイティブ スナップショットを使用するストレージ コンテナでは、高速プロビジョニングされた仮想マシンのインプレース統合はサポートされていません。VVOL および VAAI 対応のデータストアではネイティブ スナップショットが使用されるので、これらのストレージ コンテナの 1 つにデプロイされた、高速プロビジョニングされた仮想マシンは統合できません。VVOL または VAAI 対応のデータストアにデプロイされた、高速プロビジョニングされた仮想マシンを統合する必要がある場合は、仮想マシンを別のストレージ コンテナに再配置する必要があります。

vApp テンプレートに関連付けられているシャドウ仮想マシンの表示

シャドウ仮想マシンでは、vCenter データセンターとデータストア全体で vApp テンプレートに関連付けられている仮想マシンのリンク クローンをサポートします。

シャドウ仮想マシンは、リンク クローンが作成される対象のデータセンターとデータストアで vCloud Director によって作成された元の仮想マシンの完全なコピーです。[仮想マシンの高速プロビジョニング](#) を参照してください。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織] をクリックします。
- 2 組織名を右クリックし、[開く] を選択します。
- 3 [カタログ] をクリックします。
- 4 [vApp テンプレート] タブで vApp テンプレートをダブル クリックして開きます。
- 5 [シャドウ仮想マシン] タブをクリックします。

結果

vCloud Director では、vApp テンプレートに関連付けられているシャドウ仮想マシンのリストを表示します。このリストには、各シャドウ仮想マシンの vCenter における名前、各シャドウ仮想マシンが存在する対象のデータストア、およびシャドウ仮想マシンが属する vCenter Server が含まれます。

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。
- ターゲット組織が使用するストレージ ポリシー内のデータストアを判別します。[ストレージ ポリシーのプロパティの表示](#)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。
- vCloud Director Web Console 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。

手順

- 1 [管理および監視] タブの左側のペインで、[データストアとデータストア クラスター] をクリックします。
- 2 データストアまたはクラスター名を右クリックし、[テナント ストレージの移行] をクリックして、[OK] をクリックします。
- 3 移行する組織を1つ以上選択し、[追加] をクリックして [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、[追加] をクリックして [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 ターゲット データストアを1つ以上選択し、[追加] をクリックして [次へ] をクリックします。
- 6 [サマリ] 画面を確認し、[完了] をクリックして、移行を開始します。

次のステップ

[実行中および完了したテナントのストレージ移行の表示](#)

システム管理者およびロールの管理

8

vCloud Director Web コンソールを使用すると、システム管理者を vCloud Director に個別に追加したり、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： vCloud Director 9.5 以降では、サービス プロバイダは vCloud 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、『vCloud 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。

- システム管理者の追加
- システム管理者のインポート
- システム管理者の有効化または無効化
- システム管理者の削除
- システム管理者のプロファイルおよび連絡先情報の編集
- ユーザーへの電子メール通知の送信
- システムへのアクセス権限を失ったシステム管理者の削除
- グループのインポート
- LDAP グループの削除
- グループ プロパティの表示
- 権限およびロールの管理

システム管理者の追加

システム管理者アカウントを作成すると、システム管理者を vCloud Director に追加できるようになります。システム管理者は、vCloud Director およびそのすべての組織に対して完全な権限を所有します。

手順

- 1 [管理] タブをクリックし、左側のペインで [ユーザー] をクリックします。

- 2 [新規] をクリックします。
- 3 新規ユーザーのアカウント情報を入力し、[OK] をクリックします。

システム管理者のインポート

システム管理者権限を所有するユーザーを追加するために、LDAP ユーザーまたは vCenter Single Sign On ユーザーをシステム管理者としてインポートできます。システム管理者は、vCloud Director およびそのすべての組織に対して完全な権限を所有します。

前提条件

LDAP サーバに対する有効な接続があること、あるいは vCenter Single Sign On が有効であることを確認します。vSphere SSO SAML プロバイダを使用するための vCloud Director の設定 を参照してください。

手順

- 1 [管理] タブをクリックし、左側のペインで [ユーザー] をクリックします。
- 2 [ユーザーのインポート] をクリックします。
- 3 ユーザーのインポートの [ソース] を選択します。

LDAP サーバが1つしかない場合、あるいは vCenter Single Sign On が構成されている場合、ソースは読み取り専用となります。

オプション	説明
LDAP	LDAP サーバからユーザーをインポートします。 a テキスト ボックスに名前の全部または一部を入力し、[ユーザーを検索] をクリックします。 b インポートするユーザーを選択し、[追加] をクリックします。
vSphere SSO	vCenter Single Sign On からユーザーをインポートします。インポートするユーザーのユーザー名を入力し、[追加] をクリックします。インポートするユーザー名にはドメイン名が含まれる必要があります (例: user@domain.com)。複数のユーザーは、キャリッジ リターンで区切ります。

- 4 [OK] をクリックします。

システム管理者の有効化または無効化

システム管理者ユーザーを無効にして、そのユーザーが vCloud Director にログインできないようにすることができます。システム管理者を削除するには、事前にそのアカウントを無効にする必要があります。

手順

- 1 [管理] タブをクリックし、左側のペインで [ユーザー] をクリックします。
- 2 ユーザー名を右クリックし、[アカウントを有効化] または [アカウントを無効化] を選択します。

システム管理者の削除

アカウントを削除すると、システム管理者を vCloud Director システムから削除できるようになります。

前提条件

システム管理者のアカウントを無効にします。

手順

- 1 [管理] タブをクリックし、左側のペインで [ユーザー] をクリックします。
- 2 ユーザー名を右クリックし、[削除] を選択します。
- 3 [はい] をクリックします。

システム管理者のプロファイルおよび連絡先情報の編集

システム管理者アカウントのパスワードと連絡先情報を変更できます。

アカウント情報を編集できるのは、ローカル ユーザーのみです。

手順

- 1 [管理] タブをクリックし、左側のペインで [ユーザー] をクリックします。
- 2 ユーザー名を右クリックし、[プロパティ] を選択します。
- 3 ユーザー アカウントの新しい情報を入力し、[OK] をクリックします。

ユーザーへの電子メール通知の送信

インストール環境全体におけるすべてのユーザー、すべてのシステム管理者、またはすべての組織管理者に、電子メール通知を送信できます。たとえば、次のシステム メンテナンスについてユーザーに通知するために、電子メール通知を送信することができます。

前提条件

SMTP サーバに対する有効な接続があることを確認します。

手順

- 1 [管理] タブをクリックし、左側のペインで [ユーザー] をクリックします。
- 2 [通知] をクリックします。
- 3 受信者を選択します。
- 4 電子メールの件名および本文を入力し、[電子メールを送信] をクリックします。

システムへのアクセス権限を失ったシステム管理者の削除

LDAP グループが vCloud Director から削除されたときにシステムに対するアクセス権限を失った、ユーザー アカウントのリストを表示できます。ユーザーをシステムに再度追加してそのユーザーを [未分類] から削除するかどうかを決定できます。

LDAP グループが削除されたときに誤ってシステムから削除されたユーザーを追加するには、[システム管理者の追加](#) および [システム管理者のインポート](#) を参照してください。

手順

- 1 [管理] タブをクリックし、左側のペインで [未分類] をクリックします。
- 2 ユーザー名を右クリックし、[ユーザーを削除] を選択します。

グループのインポート

システム管理者権限を所有するユーザーのグループを追加するために、LDAP グループまたは vCenter Single Sign On グループをシステム管理者としてインポートできます。システム管理者は、vCloud Director およびそのすべての組織に対して完全な権限を所有します。

前提条件

LDAP サーバに対する有効な接続があること、あるいは vCenter Single Sign On が有効であることを確認します。 [vSphere SSO SAML プロバイダを使用するための vCloud Director の設定](#) を参照してください。

手順

- 1 [管理] タブをクリックし、左側のペインで [グループ] をクリックします。
- 2 [グループのインポート] をクリックします。
- 3 インポートの [ソース] を選択します。

LDAP サーバが 1 つしかない場合、あるいは vCenter Single Sign On が構成されている場合、ソースは読み取り専用となります。

オプション	説明
LDAP	LDAP サーバーからグループをインポートします。 a テキスト ボックスに名前の全部または一部を入力し、[グループの検索] をクリックします。 b インポートするグループを選択し、[追加] をクリックします。
vSphere SSO	vCenter Single Sign On からグループをインポートします。グループ名を入力し、[追加] をクリックします。複数のグループは、キャリッジ リターンで区切ります。

- 4 [OK] をクリックします。

LDAP グループの削除

LDAP グループを削除すると、システム管理者のグループを vCloud Director システムから削除できるようになります。

LDAP グループを削除すると、vCloud Director アカウントを所有しているユーザーは、そのグループのメンバーシップのみに基づいて取り残され、ログインできなくなります。[システムへのアクセス権限を失ったシステム管理者の削除](#) を参照してください。

手順

- 1 [管理] タブをクリックし、左側のペインで [グループ] をクリックします。
- 2 グループ名を右クリックし、[削除] を選択します。
- 3 [はい] をクリックし、削除することを確認します。

グループ プロパティの表示

グループの名前、ロールおよび組織など、グループ プロパティを表示できます。

手順

- 1 [管理] タブをクリックし、左側のペインで [グループ] をクリックします。
- 2 グループ名を右クリックし、[プロパティ] を選択します。

結果

グループのプロパティが表示されます。

権限およびロールの管理

権限は、vCloud 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。

vCloud 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。vCloud 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。

vCloud Director 9.5 には、権限バンドルおよびグローバル テナント ロールが導入されています。システム管理者はこれを使用して、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。

vCloud 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。

vCloud 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。

vCloud 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、vCloud 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。vCloud 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す。

権限バンドルの管理の詳細については、『vCloud Director Service Provider Admin Portal Guide』を参照してください。

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。

プロバイダ ロールの管理については、『vCloud Director Service Provider Admin Portal Guide』を参照してください。

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。

グローバル テナント ロールの管理の詳細については、『vCloud Director Service Provider Admin Portal Guide』を参照してください。

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、『vCloud 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

vCloud Director の各事前定義ロールには、共通ワークフロー内の操作の実行に必要な一連のデフォルト権限が含まれています。デフォルトで、事前定義済みのすべてのグローバル テナント ロールは、システムのすべての組織に公開されます。

■ このリリースの新しい権限

vCloud Director 9.7 で導入された新しい権限で、テナントに公開した既存のグローバル ロールにこの権限を追加することができます。

■ ロールの作成、更新、削除

■ ロールのコピー

事前定義ロールとその権限

vCloud Director の各事前定義ロールには、共通ワークフロー内の操作の実行に必要な一連のデフォルト権限が含まれています。デフォルトで、事前定義済みのすべてのグローバル テナント ロールは、システムのすべての組織に公開されます。

事前定義済みのプロバイダ ロール

デフォルトでは、プロバイダ組織のみにローカルなプロバイダ ロールは、システム管理者ロールとマルチサイト システムロールです。システム管理者は、追加のカスタム プロバイダ ロールを作成できます。

システム管理者

システム管理者ロールは、プロバイダ組織にのみ設定されています。システム管理者ロールには、システムのすべての権限が含まれています。システム管理者の認証情報は、インストールおよび構成時に確立されます。システム管理者は、プロバイダ組織に追加のシステム管理者およびユーザー アカウントを作成できます。

マルチサイト システム

マルチサイト展開のためのハートビート プロセスを実行する場合に使用します。このロールには、マルチサイトシステムの操作 という権限のみが付与されています。これにより、サイト関連付けのリモート メンバーのステータスを取得する vCloud API 要求を行うことができます。

事前定義済みのグローバル テナント ロール

デフォルトでは、事前定義済みのグローバル テナント ロールおよびそこに含まれている権限がすべての組織に公開されます。システム管理者は、個別の組織で権限およびグローバル テナント ロールの公開を解除することができます。システム管理者は、事前定義済みのグローバル テナント ロールを編集または削除できます。システム管理者は、追加のグローバル テナント ロールを作成および公開できます。

組織管理者

組織の作成後、システム管理者は、組織管理者ロールを組織内のどのユーザーにでも割り当てることができます。事前定義された組織管理者ロールを持つユーザーは、vCloud Director Web コンソール、テナント ポータル、または vCloud OpenAPI を使用して、組織内のユーザーとグループを管理し、（事前定義の組織管理者ロールを含む）ロールを割り当てることができます。組織管理者によって作成または変更されたロールは、他の組織には表示されません。

カタログ作成者

事前定義済みのカタログ作成者ロールに関連付けられた権限を持つユーザーは、カタログを作成および公開できます。

vApp 作成者

事前定義の vApp 作成者ロールに関連付けられた権限を持つユーザーは、カタログを使用し、vApp を作成できます。

vApp ユーザー

事前定義の vApp ユーザーロールに関連付けられた権限を持つユーザーは、既存の vApp を使用できます。

コンソールのアクセスのみ

事前定義のコンソールのアクセスのみロールに関連付けられた権限を持つユーザーは、仮想マシンの状態およびプロパティを表示し、ゲスト OS を使用できます。

ID プロバイダに従う

事前定義の ID プロバイダに従うロールに関連付けられた権限は、ユーザーの OAuth または SAML ID プロバイダから受信した情報に基づいて決定されます。ユーザーまたはグループに ID プロバイダに従うロールが割り当てられているときに包含の資格を得るには、ID プロバイダによって提供されたロールまたはグループ名が、組織内で定義されたロールまたはグループ名と大文字小文字も含めて完全に一致する必要があります。

- ユーザーが OAuth ID プロバイダによって定義されている場合、ユーザーには、ユーザーの OAuth トークンの `roles` アレイで指定されたロールが割り当てられます。
- ユーザーが SAML ID プロバイダによって定義されている場合、ユーザーには、名前が組織の `OrgFederationSettings` にある `SamlAttributeMapping` 要素内の `RoleAttributeName` 要素に表示される SAML 属性で指定されたロールが割り当てられます。

ユーザーに ID プロバイダに従うロールが割り当てられているが、一致するロールまたはグループ名が組織内で利用できない場合、ユーザーは組織にログインすることができますが、権限はありません。ID プロバイダがユーザーをシステム管理者などのシステムレベルのロールに関連付けている場合、ユーザーは組織にログインすることができますが、権限はありません。このようなユーザーにはロールを手動で割り当てる必要があります。

ID プロバイダに従うロールは例外として、事前定義ロールにはすべてデフォルトの権限セットが含まれています。システム管理者のみが、事前定義ロールの権限を変更できます。システム管理者が事前定義ロールを変更すると、変更内容がシステム内のロールのすべてのインスタンスに反映されます。

事前定義グローバル テナント ロールの権限

システム管理者は、vCloud Director Web コンソールを使用して、ロールに含まれる権限のリストを表示できます。

- 1 [管理] タブをクリックします。
- 2 左側のペインで、[ロール] をクリックします。
- 3 ロールを右クリックし、[プロパティ] を選択します。

組織管理者は、Service Provider Admin Portal または vCloud 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。

表 8-1. vCloud Director のグローバル テナント ロールに含まれる権限

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：マイ クラウドからの vApp を追加	X	X	X		
カタログ：カタログの外部公開/サブスクリプションを許可	X	X			
カタログ：所有者を変更	X				
カタログ：カタログを作成/削除	X	X			
カタログ：カタログのプロパティを編集	X	X			

表 8-1. vCloud Director のグローバル テナント ロールに含まれる権限（続き）

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：他の組織とカタログを共有	X	X			
カタログ：現在の組織内のユーザー/グループとカタログを共有	X	X			
カタログ：現在の組織内のプライベートおよび共有のカタログを表示	X	X	X		
カタログ：他の組織から共有されたカタログを表示	X				
カタログ項目：マイ クラウドへの追加	X	X	X	X	
カタログ項目：vApp テンプレート/メディアのコピー/移動	X	X	X		
カタログ項目：vApp テンプレート/メディアの作成/アップロード	X	X			
カタログ項目：vApp テンプレート/メディアの編集	X	X			
カタログ項目：vApp テンプレート/メディア ダウンロードを有効化	X	X			
カタログ項目：vApp テンプレート/メディアの表示	X	X	X	X	
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	X				
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	X				
ディスク：所有者を変更	X	X			
ディスク：ディスクの作成	X	X	X		
ディスク：ディスクの削除	X	X	X		
ディスク：ディスク プロパティの編集	X	X	X		
ディスク：ディスク プロパティの表示	X	X	X	X	
分散ファイアウォール：分散ファイアウォール ルールの構成	X				
分散ファイアウォール：分散ファイアウォールの有効化/無効化	X				
分散ファイアウォール：分散ファイアウォール ルールの表示	X				
Edge クラスタ：Edge クラスタの表示	X				
Edge クラスタ：Edge クラスタの管理	X				
ゲートウェイ：Syslog サーバの構成	X				

表 8-1. vCloud Director のグローバル テナント ロールに含まれる権限 (続き)

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
ゲートウェイ：システム ログの構成	X				
ゲートウェイ：詳細ゲートウェイに変換	X				
ゲートウェイ：ゲートウェイの表示	X				
ゲートウェイ：分散ルーティングの有効化	X				
ゲートウェイ：Edge Gateway のインポート	X				
ゲートウェイ サービス：BGP ルーティングの設定					
ゲートウェイ サービス：DHCP の設定	X				
ゲートウェイ サービス：ファイアウォールの設定	X				
ゲートウェイ サービス：IPsec VPN の設定	X				
ゲートウェイ サービス：L2 VPN の設定					
ゲートウェイ サービス：ロード バランサーの設定	X				
ゲートウェイ サービス：NAT の設定	X				
ゲートウェイ サービス：OSPF ルーティングの設定	X				
ゲートウェイ サービス：リモート アクセスの設定	X				
ゲートウェイ サービス：SSL VPN の設定	X				
ゲートウェイ サービス：スタティック ルーティングの設定	X				
ゲートウェイ サービス：BGP ルーティング ビューのみ	X				
ゲートウェイ サービス：DHCP ビューのみ	X				
ゲートウェイ サービス：ファイアウォール ビューのみ	X				
ゲートウェイ サービス：IPSEC VPN ビューのみ	X				
ゲートウェイ サービス：L2 VPN ビューのみ	X				
ゲートウェイ サービス：ロード バランサ ビューのみ	X				
ゲートウェイ サービス：NAT ビューのみ	X				
ゲートウェイ サービス：OSPF ルーティング ビューのみ	X				
ゲートウェイ サービス：リモート アクセス ビューのみ	X				

表 8-1. vCloud Director のグローバル テナント ロールに含まれる権限（続き）

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
ゲートウェイ サービス：SSL VPN ビューのみ	X				
ゲートウェイ サービス：スタティック ルーティング ビューのみ	X				
全般：管理者のコントロール	X				
全般：管理者の表示	X				
全般：通知の送信	X				
ハイブリッド トンネル：コントロール チケットを取得	X				
ハイブリッド トンネル：クラウドからのトンネル チケットを取得	X				
ハイブリッド トンネル：クラウドへのトンネル チケットを取得	X				
ハイブリッド トンネル：クラウドからのトンネルを作成	X				
ハイブリッド トンネル：クラウドへのトンネルを作成	X				
ハイブリッド トンネル：クラウドからのトンネルを削除	X				
ハイブリッド トンネル：クラウドへのトンネルを削除	X				
ハイブリッド トンネル：クラウドからのトンネルのエンドポイント タグを更新	X				
ハイブリッド トンネル：クラウド トンネル サーバの設定を表示	X				
ハイブリッド トンネル：クラウドからのトンネルを表示	X				
ハイブリッド トンネル：クラウドへのトンネルを表示	X				
組織：すべての組織 VDC へのアクセスの許可	X				
組織：組織 VDC のアクセス制御リストの編集	X				
組織：連携設定の編集	X				
組織：リース ポリシーの編集	X				
組織：組織の関連付けの編集	X				

表 8-1. vCloud Director のグローバル テナント ロールに含まれる権限（続き）

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：組織のネットワーク プロパティの編集	X				
組織：組織の OAuth 設定の編集	X				
組織：組織のプロパティの編集	X				
組織：パスワード ポリシーの編集	X				
組織：割り当て容量ポリシーの編集	X				
組織：SMTP 設定の編集	X				
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	X				
組織：組織 VDC のアクセス制御リストの表示	X				
組織：カタログ ACL を表示	X	X			
組織：組織のネットワークの表示	X				
組織：組織の表示	X	X	X		
組織：vApp ACL を表示	X	X	X	X	
組織 VDC：組織 VDC の名前と説明の編集	X				
組織 VDC：仮想マシン - 仮想マシン アフィニティ ルールの編集	X	X	X		
組織 VDC：組織 VDC の拡張プロパティを編集	X				
組織 VDC：ファイアウォールの管理	X				
組織 VDC：デフォルトのストレージ ポリシーの設定	X				
組織 VDC：組織 VDC の コンピューティング ポリシーを表示	X	X	X	X	
組織 VDC：組織 VDC の拡張プロパティを表示	X				
組織 VDC ネットワーク：プロパティの表示	X				
組織 VDC ネットワーク：プロパティの編集	X				
組織 VDC ネットワーク：ネットワークのインポート	X				
組織 VDC：組織 VDC の表示	X				
組織 VDC テンプレート：組織 VDC テンプレートをインスタンス化	X				
組織 VDC テンプレート：VDC テンプレートの表示	X				

表 8-1. vCloud Director のグローバル テナント ロールに含まれる権限 (続き)

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
プロバイダ ネットワーク：プロバイダ ネットワークを表示	X				
プロバイダ ネットワーク：プロバイダ ネットワークを作成/削除	X				
ロール：ロールを作成/更新/削除	X				
サービス ライブラリ：サービス ライブラリを構成するサービスを表示	X				
ユーザー：グループ/ユーザーの表示	X				
VCD の拡張機能：テナント ポータル プラグイン情報を表示	X	X	X	X	
VDC グループ：VDC グループの表示	X				
VDC グループ：VDC グループの設定	X				
仮想マシンの監視：組織の履歴メトリックを表示	X				
仮想マシンの監視：組織 VDC の履歴メトリックを表示	X				
vApp：仮想マシン コンソールへのアクセス	X	X	X	X	X
vApp：vCenter Server へのメタデータ マッピング ドメインを許可	X	X	X		
vApp：所有者を変更	X				
vApp：vApp テンプレート所有者の変更	X	X			
vApp：vApp をコピー	X	X	X	X	
vApp：vApp の作成/再構成	X	X	X		
vApp：スナップショットを作成/元に戻す/削除	X	X	X	X	
vApp：vApp を削除	X	X	X	X	
vApp：vApp のダウンロード	X	X	X		
vApp：仮想マシンのブート オプションを編集/表示	X	X	X		
vApp：仮想マシンの CPU を編集	X	X	X		
vApp：仮想マシンのハード ディスクを編集	X	X	X		
vApp：仮想マシンのメモリを編集	X	X	X		
vApp：仮想マシンのネットワークを編集	X	X	X	X	
vApp：仮想マシンのプロパティを編集	X	X	X	X	

表 8-1. vCloud Director のグローバル テナント ロールに含まれる権限（続き）

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 : vApp のプロパティを編集	X	X	X	X	
vApp : 仮想マシンのコンピューティング ポリシーを編集	X	X	X		
vApp : 仮想マシンのパスワード設定を管理	X	X	X	X	X
vApp : vApp を共有	X	X	X	X	
vApp : vApp を開始/停止/サスペンド/リセット	X	X	X	X	
vApp : vApp のアップロード	X	X	X		
vApp : 仮想マシンのメトリックを表示	X		X	X	

vCloud Director 9.7 で導入される新しい権限の詳細については、[このリリースの新しい権限](#)を参照してください。

このリリースの新しい権限

vCloud Director 9.7 で導入された新しい権限で、テナントに公開した既存のグローバル ロールにこの権限を追加することができます。

権限	説明	デフォルトのロール
SDDC : SDDC の表示	組織に公開されているすべての SDDC を表示できます。 システム管理者は、すべての SDDC を表示できます。	システム管理者および組織管理者
SDDC : SDDC の管理	SDDC を追加、削除、および編集できます。	システム管理者
SDDC : SDDC プロキシの管理	SDDC プロキシを追加、削除、有効化、および無効化できます。	システム管理者
サービス アプリケーション : サービス アプリケーションの表示	登録されているサービス アプリケーションのリストを表示できます。 VMC アカウントに使用されます。	システム管理者
サービス アプリケーション : VMC の SDDC を登録	サービス アプリケーションを作成、表示、編集、および削除できます。 VMC アカウントに使用されます。	システム管理者
サービス アプリケーション : サービス アプリケーションの管理	サービス アプリケーションを登録できます。 VMC アカウントに使用されます。	システム管理者
Edge クラスタ : Edge クラスタの表示	Edge クラスタのリストを表示し、個々の Edge クラスタを取得できます。	システム管理者および組織管理者
Edge クラスタ : Edge クラスタの管理	Edge クラスタを作成、編集、および削除できます。	システム管理者および組織管理者

権限	説明	デフォルトのロール
vApp: 仮想マシンのコンピューティング ポリシーを編集	仮想マシンのコンピューティング ポリシーを変更できます。	システム管理者、組織管理者、カタログ作成者、および vApp 作成者
ゲートウェイ: Edge Gateway のインポート	Tier-1 ルーターを Edge Gateway としてインポートできます。	システム管理者および組織管理者

権限およびロールの管理の詳細については、『vCloud Director Service Provider Admin Portal Guide』を参照してください。

ロールの作成、更新、削除

システム管理者は、vCloud Director Web Console または vCloud API を使用して、システム内のすべての組織のロール オブジェクトを作成したり、更新したりできます。組織管理者は、vCloud API を使用して、管理対象の組織のロール オブジェクトを作成または更新できます。

vCD 9.5 以降では、サービス プロバイダは Service Provider Admin Portal を使用して権限、ロール、ユーザー、グループを管理することができます。『vCloud Director Service Provider Admin Portal Guide』を参照してください。

前提条件

vCloud Director Web Console を使用してロール オブジェクトを作成または更新できるのは、システム管理者に限られます。

手順

- ◆ [管理] タブをクリックし、左側のペインで [ロール] をクリックします。

すべてのロールとそれらが含まれる組織のリストが表示されます。

- ◆ ロールを作成するには、[新規] をクリックします。

- a ロールを作成する組織を選択します。
- b ロールの名前と、オプションで説明を入力します。
- c ロールの権限を選択します。

権限カテゴリを展開すると、それに含まれる個々の権限が表示されます。デフォルトでは、すべての権限カテゴリが表示されます。ロールに追加する権限を 1 つ以上選択した権限カテゴリのみが表示されるように権限カテゴリのリストを制限するには、[選択した権限のみを表示] を選択します。

- d [OK] をクリックして、変更内容を保存します。

- ◆ ロールを更新するには、リスト内のエントリ（ロールと組織）を右クリックし、[プロパティ] を選択します。

- a ロールの権限を選択します。

権限カテゴリを展開すると、それに含まれる個々の権限が表示されます。デフォルトでは、すべての権限カテゴリが表示されます。ロールに追加する権限を 1 つ以上選択した権限カテゴリのみが表示されるように権限カテゴリのリストを制限するには、[選択した権限のみを表示] を選択します。

- b [OK] をクリックして、変更内容を保存します。

- ◆ ロールを削除するには、リスト内のエントリ（ロールと組織）を右クリックし、[削除] を選択します。
[はい] をクリックし、削除することを確認します。

ロールのコピー

システム管理者は、vCloud Director Web コンソールを使用して、組織内のロール オブジェクトをコピーできます。

前提条件

vCloud Director Web Console を使用してロール オブジェクトを作成または更新できるのは、システム管理者に限られます。

手順

- 1 [管理] タブをクリックし、左側のペインで [ロール] をクリックします。
すべてのロールとそれらが含まれる組織のリストが表示されます。
- 2 リスト内のエントリを右クリックし、[コピー] を選択します。

重要： [ロールのコピー] ダイアログで選択した組織にかかわらず、常にソース組織にコピーが作成されます。

- 3 コピーするロールの名前と、必要に応じて説明を入力します。
- 4 ロールの権限を選択し、[OK] をクリックします。

権限カテゴリを展開すると、それに含まれる個々の権限が表示されます。デフォルトでは、すべての権限カテゴリが表示されます。ロールに追加する権限を 1 つ以上選択した権限カテゴリのみが表示されるように権限カテゴリのリストを制限するには、[選択した権限のみを表示] を選択します。

結果

組織内でロールのコピーが作成されます。

システム設定の管理

9

vCloud Director システム管理者は、LDAP、電子メール通知、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
- システムの電子メール設定の編集
- ブロック タスクおよび通知の構成
- システムの LDAP の設定
- vCloud Director クライアント UI のカスタマイズ
- 公開アドレスの構成
- システム制限の構成
- アカウント ロックアウト ポリシーの構成
- vSphere SSO SAML プロバイダを使用するための vCloud Director の設定

全般システム設定の変更

vCloud Director には、ログイン ポリシー、セッション タイムアウトなどに関連する全般システム設定があります。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： vCloud 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 [管理] タブをクリックし、左側のペインで [全般] をクリックします。
- 2 設定を変更して [適用] をクリックします。

全般システム設定

vCloud 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 9-1. 全般システム設定

名前	カテゴリ	説明
同期の開始時刻	LDAP 同期	LDAP 同期を開始する時刻。
同期の間隔	LDAP 同期	LDAP 同期の間隔（時間単位）。
保持するアクティビティ ログ履歴	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。 ログを削除しない場合は、 0 を入力します。
アクティビティ ログ履歴の表示	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場合は、 0 を入力します。
デバッグ情報の表示	アクティビティ ログ	vCloud 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 アドレス リリース タイムアウト	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。
外部ネットワークの重複を許可	ネットワーク	同じネットワーク セグメントで実行される外部ネットワークを追加するには、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。
FIPS モードを許可	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。
ネットワークのデフォルトの Syslog サーバ設定	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 サーバには適用されません。
プロバイダ ロケール	ローカライズ	ログ エントリ、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。
アイドル セッション タイムアウト	タイムアウト	vCloud 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。
最大セッション タイムアウト	タイムアウト	vCloud 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。
ホスト更新間隔	タイムアウト	ESXi ホストがアクセス可能かどうかを vCloud Director が確認する頻度。
ホスト ハングアップ タイムアウト	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。
転送セッション タイムアウト	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。
__ 秒のタイムアウトのアップロード検疫を有効化	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。

表 9-1. 全般システム設定（続き）

名前	カテゴリ	説明
vCenter Server と vSphere SSO 証明書の検証	証明書	vCloud Director が信頼されている vCenter Server のみと通信できるようにするには、このチェック ボックスをオンにします。[参照] をクリックして JCEKS キーストアを探し、キーストアのパスワードを入力します。
NSX Manager 証明書の検証	証明書	vCloud Director が信頼されている NSX Manager のインスタンスのみと通信できるようにするには、このチェック ボックスをオンにします。[参照] をクリックして JCEKS キーストアを探し、キーストアのパスワードを入力します。
組織ごとの仮想データセンターの最大数	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。
ユーザーごとのリソースを大量に消費する操作実行数	操作の制限	ユーザー 1 人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、[制限なし] 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	操作の制限	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、[制限なし] 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	操作の制限	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、[制限なし] を選択します。
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	操作の制限	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、[制限なし] を選択します。
デフォルトの vApp 名の指定	その他	新しい vApp のデフォルト名を提供するように vCloud 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。
割り当てプールの組織 VDC を拡張性ありにする	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 ボックスをオンにします。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。
仮想マシンの検出を有効化	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仮想データセンターについて、この設定が無効になります。

システムの電子メール設定の編集

SMTP および通知設定など、システムの電子メール設定を編集できます。

■ SMTP 設定の構成

vCloud 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警告のメールを送信するために SMTP サーバが必要です。組織では、システムの SMTP 設定またはカスタム SMTP 設定を使用できます。

■ システム通知設定の構成

vCloud Director では、重要な情報を報告するときにシステム警告の電子メールを送信します。たとえば、vCloud Director は、データストアの領域が不足するような場合に警告を送信します。すべてのシステム管理者または指定した電子メール アドレス リスト宛てに電子メール警告を送信するように、vCloud Director を構成できます。

SMTP 設定の構成

vCloud 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警告のメールを送信するために SMTP サーバが必要です。組織では、システムの SMTP 設定またはカスタム SMTP 設定を使用できます。

手順

- 1 [管理] タブをクリックし、左側のペインで [電子メール] をクリックします。
- 2 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。
- 3 SMTP サーバのポート番号を入力します。
- 4 (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] チェック ボックスを選択して、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。
- 5 vCloud Director の電子メールで送信者として表示する電子メール アドレスを入力します。
vCloud Director では、送信者の電子メール 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警告を送信します。
- 6 vCloud Director の電子メールで件名のプリフィックスとして使用するテキストを入力します。
- 7 (オプション) SMTP 設定をテストするには、宛先の電子メール アドレスを入力して、[SMTP 設定をテスト] をクリックします。
- 8 [適用] をクリックします。

システム通知設定の構成

vCloud Director では、重要な情報を報告するときにシステム警告の電子メールを送信します。たとえば、vCloud Director は、データストアの領域が不足しそうな場合に警告を送信します。すべてのシステム管理者または指定した電子メール アドレス リスト宛てに電子メール警告を送信するように、vCloud Director を構成できます。

組織では、システムの通知設定またはカスタム通知設定を使用できます。

前提条件

SMTP サーバーへの有効な接続。

手順

- 1 [管理] タブをクリックし、左側のペインで [電子メール] をクリックします。
- 2 システム警告電子メールの受信者を選択し、[適用] をクリックします。

ブロック タスクおよび通知の構成

ブロック タスクと通知により、システム管理者は、特定のイベントによってトリガーされた AMQP メッセージを vCloud Director が送信するように構成できるようになります。

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。これらは「通知」と呼ばれます。他には、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 プログラムによってアクションの保留中にブロックされたことを示す情報をそのエンドポイントに発行するものがあり、これらは「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

特定のイベントによってトリガーされた AMQP メッセージを vCloud Director が送信するようにする場合は、AMQP ブローカーを構成する必要があります。

手順

- 1 [管理] タブをクリックし、左側のペインで [ブロック タスク] をクリックします。
- 2 [設定] タブをクリックします。
- 3 AMQP ホストの DNS ホスト名または IP アドレスを入力します。
AMQP ポートを入力します。
デフォルト ポートは **5672** です。
- 4 Exchange を入力します。
- 5 vHost を入力します。
- 6 SSL を使用するには、[SSL] チェック ボックスをオンにし、証明書オプションを 1 つ選択します。

オプション	アクション
すべての証明書を承認	チェック ボックスをオンにします。
SSL 証明書	[参照] をクリックして SSL 証明書を探します。
SSL キーストア	[参照] をクリックして SSL キーストアを探します。キーストア パスワードを入力します。

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] を選択します。

- 7 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。
- 8 [AMQP 接続のテスト] をクリックし、設定をテストします。
- 9 [適用] をクリックします。
- 10 (オプション) 監査イベントを AMQP ブローカーに発行するには、ページの上部にある [通知を有効化] チェック ボックスをオンにします。

ブロック タスク設定の構成

ステータス テキスト、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することができます。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 [管理] タブを選択し、左側のパネルで [拡張性] を選択します。
- 2 [設定] タブで、デフォルトの拡張機能タイムアウトを選択します。
- 3 デフォルトのタイムアウトのアクションを選択します。
[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自動アクションです。
- 4 [適用] をクリックします。

ブロック タスクの有効化

ブロック タスクに対して有効化される特定のタスクを構成できます。

手順

- 1 [管理] タブをクリックし、左側のペインで [ブロック タスク] をクリックします。
- 2 [ブロック タスク] タブをクリックします。
- 3 ブロック拡張機能に対して有効化するタスクを選択します。
- 4 [適用] をクリックします。

システムの LDAP の設定

vCloud Director を設定して、サポートされている LDAP サービスからユーザーとグループの情報をインポートできます。システムの LDAP 設定は、vCloud Director が LDAP サービスに接続する方法、サービスと同期する頻度、およびユーザー名とグループ名を LDAP 属性にマッピングする方法を制御します。

vCloud Director を LDAP サーバに接続したら、LDAP ディレクトリのグループとユーザーからシステム管理者をインポートできます。また、システムの LDAP 設定を使用してユーザーとグループを組織にインポートしたり、組織ごとに個別の LDAP 設定を指定したりすることもできます。LDAP ユーザーは、システムまたは組織にインポートされるまで vCloud Director にログインできません。

インポートされた LDAP ユーザーがログインすると、vCloud Director は、入力された認証情報を LDAP サービスに対して検証し、認証情報が有効な場合はログインを許可します。vCloud Director が LDAP アカウント情報を作成または変更することはできません。LDAP アカウントを管理するにはネイティブの LDAP ツールを使用する必要があります。

注： vCloud Director では、LDAP 認証に対して階層化されたドメインはサポートされません。

サポートされている LDAP サービス

今回のリリースの vCloud Director によってサポートされている LDAP サービスの一覧については、『vCloud Director リリース ノート』を参照してください。

LDAP 接続の構成

LDAP 接続を構成して、vCloud Director およびその組織に対して LDAP サーバのユーザーおよびグループへのアクセスを提供できます。

前提条件

- LDAPS サーバに接続する場合は、Java 8 Update 181 での LDAP サポートの向上に合わせて、証明書が適切に作成されていることを確認します。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。
- 認証方法としてケルベロスを使用する場合は、[ケルベロス レルムの追加](#) する必要があります。

手順

- 1 [管理] タブをクリックし、左側のペインで [LDAP] をクリックします。

- 2 LDAP サーバのホスト名または IP アドレスを入力します。

ケルベロス認証では、完全修飾ドメイン名 (FQDN) を使用します。

- 3 ポート番号を入力します。

LDAP のデフォルト ポート番号は 389 です。LDAP over SSL (LDAPS) のデフォルト ポート番号は 636 です。

- 4 ベースとなる識別名 (Base DN) を入力します。

Base DN は、LDAP ディレクトリ内で vCloud Director が接続する場所です。VMware は、ルートでの接続を推奨します。ドメイン コンポーネントのみを入力します。たとえば **DC=example, DC=com** のようになります。

ツリー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、vCloud Director が使用できるディレクトリの範囲が制限されます。

- 5 LDAPS を使用するための SSL チェック ボックスを選択し、承認オプションのいずれかを選択します。

オプション	アクション
すべての証明書を承認	チェック ボックスをオンにします。
SSL 証明書	[参照] をクリックして SSL 証明書を探します。
SSL キーストア	[参照] をクリックして SSL キーストアを探します。キーストア パスワードを入力し、確認のためもう一度パスワードを入力します。

- 6 認証方式を選択します。

オプション	説明
シンプル	シンプル認証では、LDAP サーバにユーザーの DN とパスワードを送信します。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。
ケルベロス	ケルベロスは、認証チケットを発行してユーザーの ID を証明します。ケルベロスを選択した場合、レルムを選択する必要があります。

- 7 ユーザー名およびパスワードを入力して LDAP サーバに接続します。

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。

認証方式	ユーザー名の説明
シンプル	完全な LDAP DN を入力します。
ケルベロス	名前を <i>user@REALM.com</i> という形式で入力します。

- 8 [適用] をクリックします。

次のステップ

これで、LDAP ユーザーとグループを、システムおよびシステムの LDAP 設定を使用する組織に追加できます。

ケルベロス レルムの追加

vCloud Director で LDAP 接続にケルベロス認証を使用するには、レルムが必要です。システムとその組織に使用するレルムを 1 つ以上追加できます。システムと各組織で指定できるレルムは 1 つのみです。

前提条件

レルムを追加するには、事前に認証方式としてケルベロスを選択する必要があります。

手順

- 1 [管理] タブをクリックし、左側のペインで [LDAP] をクリックします。
- 2 [すべてのレルムを編集] をクリックします。
- 3 (オプション) [レルム] タブで [小文字のレルムを許可] を選択し、小文字を含むレルム名が許可されるようにします。
- 4 [レルム] タブで [追加] をクリックします。
- 5 レルムとその鍵配布センター (KDC) を入力し、[OK] をクリックします。
小文字のレルムを許可することを選択しなかった場合、レルム名はすべて大文字で入力する必要があります。たとえば、**REALM** のように入力します。
- 6 [DNS] タブで [追加] をクリックします。
- 7 DNS を入力し、レルムを選択して、[OK] をクリックします。
DNS のワイルドカード文字としてピリオド (.) を使用できます。たとえば、**.example.com** のように入力します。
- 8 [閉じる] をクリックし、[適用] をクリックします。

次のステップ

これで、システムの LDAP 設定または組織の LDAP 設定のレルムを選択できます。

LDAP 設定のテスト

LDAP 接続を構成したら、その設定をテストして、ユーザー属性とグループ属性が正しくマッピングされていることを確認できます。

前提条件

テストするには、事前に LDAP 接続を構成する必要があります。

手順

- 1 [管理] タブをクリックし、左側のペインで [LDAP] をクリックします。
- 2 [LDAP 設定をテスト] をクリックします。
- 3 LDAP ディレクトリ内のユーザーの名前を入力し、[テスト] をクリックします。
- 4 属性のマッピングを確認し、[OK] をクリックします。

次のステップ

テストの結果に基づいて、LDAP のユーザー属性およびグループ属性をカスタマイズできます。

LDAP ユーザーおよびグループ属性のカスタマイズ

LDAP 属性は、LDAP ディレクトリでのユーザー情報およびグループ情報の定義方法の詳細を vCloud Director に提供します。vCloud Director は、これらの情報を独自のデータベースにマッピングします。自分の LDAP ディレクトリに一致するように、ユーザー属性およびグループ属性の構文を変更します。

前提条件

LDAP 接続があることを確認します。

手順

- 1 [管理] タブをクリックし、左側のペインで [LDAP] をクリックします。
- 2 ユーザー属性およびグループ属性を変更し、[適用] をクリックします。

vCloud Director と LDAP サーバーの同期

vCloud Director は、そのユーザーおよびグループの情報を、定期的に LDAP サーバと自動で同期します。LDAP サーバとの同期は、手動でいつでも行うこともできます。

自動的な同期については、同期の頻度とタイミングを指定できます。[全般システム設定の変更](#)を参照してください。

前提条件

有効な LDAP 接続があることを確認します。

手順

- 1 [管理] タブをクリックし、左側のペインで [LDAP] をクリックします。
- 2 [LDAP を同期] をクリックします。

vCloud Director クライアント UI のカスタマイズ

vCloud Director クライアント UI、および vCloud Director Home ログイン画面に表示される一部のリンクのブランド設定をカスタマイズできます。

カスタム テーマとして vCloud Director がサポートするスタイルに関する情報を示す .css テンプレートのサンプルについては、<http://kb.vmware.com/kb/1026050> を参照してください。

vCloud Director では、ログイン画面、ヘッダー、およびフッターで、デフォルトのロゴまたは自分でアップロードしたロゴが使用されます。ログイン画面では、最小で 48x48 ピクセル、最大で 60x150 ピクセルの範囲の領域にロゴを表示します。48x48 ピクセル未満、または 60x150 ピクセル超のロゴをアップロードすることもできます。この場合、vCloud Director では、アップロードされたイメージの縦横比を維持しながら、表示領域にサイズを適合させます。アップロードするイメージのファイル サイズは、16384 バイト以下にする必要があります。ヘッダーおよびフッターでは、元のロゴの縦横比を維持しながら、ロゴが適切なサイズに変更されます。

ファイル形式は、PNG、JPEG、または GIF にする必要があります。

手順

- 1 [管理] タブをクリックし、左側のペインで [ブランド] をクリックします。

- 2 会社名を入力します。

この名前は、システム管理者のタイトル バーおよびすべてのユーザーのフッターに表示されます。

- 3 カスタム ロゴを選択するには、[参照] をクリックしてファイルを選択し、[開く] をクリックします。

- 4 カスタム テーマを選択するには、[参照] をクリックして .css ファイルを選択し、[開く] をクリックします。

- 5 自分の vCloud Director インストール環境に関する情報を提供する Web サイトにリンクしている URL を入力します。

たとえば、<http://www.example.com> のように入力します。ユーザーは、クライアント UI のフッターに表示される会社名をクリックしてリンクをたどることができます。

- 6 この vCloud Director インストール環境にサポートを提供する Web サイトにリンクしている URL を入力します。

すべての vCloud Director 組織の [ホーム] タブにある [サポート] リンクから、この URL が開きます。

- 7 ユーザーが vCloud Director アカウントにサインアップできる Web サイトにリンクされている URL を入力します。

このリンクは vCloud Director ログイン ページに表示されます。

- 8 ユーザーがパスワードを忘れた場合に復元できる Web サイトにリンクされている URL を入力します。

このリンクは vCloud Director ログイン ページに表示されます。

- 9 [適用] をクリックします。

システムのデフォルトのロゴに戻す

vCloud Director のカスタム ロゴをアップロードした後、システムのデフォルトのロゴに戻すことができます。

前提条件

カスタム ロゴがアップロードされていることを確認します。

手順

- 1 [管理] タブをクリックし、左側のペインで [ブランド] をクリックします。
- 2 [システムのデフォルトのロゴに戻す] を選択して [適用] をクリックします。

システムのデフォルトのテーマに戻す

vCloud Director のカスタム テーマを適用している場合、いつでもシステムのデフォルトのテーマに戻すことができます。

前提条件

カスタム テーマが以前に適用されていることを確認します。

手順

- 1 [管理] タブをクリックし、左側のペインで [ブランド] をクリックします。
- 2 [システムのデフォルトのテーマに戻す] を選択して [適用] をクリックします。

公開アドレスの構成

公開アドレスとは、vCloud 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。システム管理者は、必要に応じてこれらのアドレスを更新できます。

1 つのセルで構成される vCloud Director では、通常、インストーラによって作成される公開エンドポイントは、API および Web クライアントにアクセスを提供するのに適しています。複数のセルを含むインストールでは、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。

カスタマイズされたエンドポイントの SSL 証明書

vCloud Director テナント ポータルおよび vCloud 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。vCloud Director をインストール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後にカスタマイズする場合は、ホスト名や Subject Alternative Names (SAN) 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。

公開エンドポイントのカスタマイズ

ロード バランサまたはプロキシの要件を満たすには、vCloud Director Web コンソール、vCloud API、テナント ポータル、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。

vCloud 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、このアプライアンスをデプロイした場合は、vCloud 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 5](#) を参照してください。

前提条件

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 [管理] タブをクリックし、左のペインで [公開アドレス] をクリックします。

- 2 [公開エンドポイントのカスタマイズ] を選択します。

このチェックボックスの選択を解除すると、すべてのエンドポイントがデフォルト値に戻ります。これらのデフォルト値は、画面には表示されません。

- 3 vCloud REST API と OpenAPI の URL をカスタマイズするには、[API] エンドポイントを編集します。

- 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 vCloud API に、`http://vcloud.example.com/cloudapi` から vCloud 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、[参照] 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 vCloud API に、`https://vcloud.example.com/cloudapi` から vCloud 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され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 vCloud 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。

- 4 vCloud Director テナント ポータルの URL をカスタマイズするには、[テナント ポータル] エンドポイントを編集します。

- [手順 3](#) で指定したエンドポイントおよび証明書チェーンと同じものを使用するよう vCloud Director テナント ポータルを設定するには、[API URL 設定のコピー] を選択します。
- 異なるエンドポイントおよび証明書チェーンを使用するよう vCloud Director テナント ポータルを設定するには、次の手順を実行します。

- a [API URL 設定のコピー] の選択を解除します。

- b 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/tenant/org_name` からテナント ポータルにアクセスできます。

- c カスタムの HTTPS REST API ベース URL を入力し、[参照] 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/tenant/org_name** からテナント ポータル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され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 vCloud 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。

- 5 vCloud Director Web Console の URL およびコンソール プロキシのアドレスをカスタマイズするには、[Web コンソール] エンドポイントを編集します。

- a HTTP 接続用のカスタムの vCloud Director パブリック URL を入力します。

URL には /cloud を含める必要があります。

たとえば、vCloud Director パブリック URL を **http://vcloud.example.com/cloud** に設定した場合は、**http://vcloud.example.com/cloud** から vCloud Director Web Console にアクセスできます。

- b HTTPS 接続用のカスタムの REST API URL を入力し、[参照] 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。

URL には /cloud を含める必要があります。

たとえば、ベース URL を **https://vcloud.example.com** に設定した場合は、**https://vcloud.example.com/cloud** から vCloud Director Web Console 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され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 vCloud 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。

- c カスタムの vCloud Director 公開コンソール プロキシ アドレスを入力します。

このアドレスは、ポート番号が指定された、vCloud 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。

重要： vCloud Director アプライアンスは、コンソール プロキシ サービスに eth0 NIC とカスタム ポート 8443 を使用します。

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。コンソール プロキシ証明書は、エイリアス **consoleproxy** を使用して vCloud Director セルの各キーストアにアップロードされます。

たとえば、vCloud 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。

vCloud Director Web コンソールは、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。

- 6 変更内容を保存するには、[適用] をクリックします。

システム制限の構成

リソースを大量に使用する操作の数に上限を設定できます。これらの操作には、コピー、移動、[マイ クラウドへの追加]、[マイ カタログへの追加] などがあり、仮想マシンに対するコンソール接続の最大数、および組織ごとのデータセンターの最大数を制限します。これらの制限により、サービス拒否攻撃からの保護が可能になります。

手順

- 1 [管理] タブをクリックし、左側のペインで [ポリシー] をクリックします。
- 2 リソースを大量に使用する操作、仮想マシンに対するコンソール接続数、および組織ごとのデータセンター数のシステム上限値を選択します。

オプション	説明
ユーザーごとのリソースを大量に使用する操作数	ユーザーごとのリソースを大量に使用する、同時に実行可能な操作の最大数を入力するか、[制限なし] 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使用する操作数	ユーザーごと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、[制限なし] を選択します。
組織ごとのリソースを大量に使用する操作数	組織ごとのリソースを大量に使用する、同時に実行可能な操作の最大数を入力するか、[制限なし] を選択します。
組織ごとのキューに入れられるリソースを大量に使用する操作数	組織ごと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、[制限なし] 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、[制限なし] 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、[制限なし] を選択します。

リソースを大量に使用する操作は、vCenter Server の長時間実行される操作です。これらの操作はすべて、vCenter Server コンソールの [タスク] ユーザー インターフェイス パネルで報告される vCenter Server の操作です。通常、リソースを大量に使用する操作は、プロビジョニング、プロビジョニング解除、および状態または設定の変更に関連しています。

- 3 (オプション) すべての制限値をシステム制限のデフォルト値に戻すには、[元に戻す] をクリックします。
- 4 [適用] をクリックして新規のシステム制限値を保存します。

アカウント ロックアウト ポリシーの構成

アカウント ロックアウトを有効化すると、特定回数の試行が失敗した場合にユーザーが Web コンソールにログインできないようにすることができます。

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 [管理] タブをクリックし、左側のペインで [ポリシー] をクリックします。
- 2 [アカウント ロックアウトの有効化] チェック ボックス、[システム管理者アカウントはロックアウトできます。] チェック ボックス、または両方のチェック ボックスをオンにします。
- 3 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。
- 4 ロックアウト間隔を選択します。
- 5 [適用] をクリックします。

vSphere SSO SAML プロバイダを使用するための vCloud Director の設定

vSphere SAML プロバイダを使用するようにシステム組織を設定すると、vSphere からシステム管理者をインポートできます。

vSphere SSO サービスを vCloud Director システム組織の SAML ID プロバイダとして使用することは、LDAP またはローカル アカウントを使用するよりも安全な方法です。vSphere SAML プロバイダを使用するには、vCloud Director および vSphere に管理者としてログインし、各プラットフォームの SAML メタデータをクライアントのローカル ファイルにエクスポートし、最後にそのメタデータを別のプラットフォームの SAML クライアントにインポートするための認証情報が必要です。

前提条件

この操作は、システム管理者に制限されます。

また、SSO 管理者として vSphere にログインするための認証情報も必要です。

手順

1 [管理] タブをクリックし、左側のペインで [システム設定] - [連携] の順にクリックします。

2 vCloud 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 [連携] タブの [サービス プロバイダ] 領域で、証明書の有効期限を確認します。

[再生成] をクリックすると、証明書を再生成して有効期限をリセットできます。

注： 独自のキーおよび証明書チェーンを指定する必要がある場合は、vCloud API を使用できます。

b 証明書の有効期限がニーズを満たしている場合は、[メタデータ] リンクをクリックします。

vCloud Director SAML サービス プロバイダのメタデータ (XML ファイル) が、ブラウザのダウンロード保存用フォルダにダウンロードされます。

3 vCloud Director SAML メタデータを vSphere にインポートします。

a vSphere SSO 管理者として vSphere Web Client にログインします。

b [ホーム] - [管理] の順にクリックして [管理] メニューを開き、[Single Sign-On] - [構成] の順にクリックして [SSO 設定] ページを表示します。

c [SAML v2.0 ID プロバイダ] で、[SAML サービス プロバイダのメタデータ] の右側にある [インポート] ボタンをクリックします。

d [サービス プロバイダ SAML メタデータのインポート] ページで、[ファイルからインポート] をクリックし、[手順 2](#) でダウンロードした vCloud Director SAML メタデータを参照します。

4 vSphere から VMware ID プロバイダのメタデータをダウンロードします。

vSphere 管理者として vSphere Web Client にログインしている間に、[SSO 設定] ページを開き、[SAML サービス プロバイダのメタデータ] の右側にある [ダウンロード] ボタンをクリックします。vSphere SAML メタデータ (XML ファイル) が、ブラウザのダウンロード保存用フォルダにダウンロードされます。

5 vSphere ID プロバイダのメタデータを vCloud Director にアップロードします。

[連携] タブの [ID プロバイダ] 領域で、[SAML ID プロバイダを使用する] を選択し、[手順 4](#) でダウンロードした vSphere SAML メタデータをアップロードします。これにより、vSphere と vCloud Director の間の SAML メタデータの交換が完了します。

結果

これで、[ユーザーのインポート] ダイアログ ボックスで [SAML] を選択して、vSphere からユーザーをインポートできるようになります。また、[vSphere Web Client で開く] オプションを使用して、同じ SSO ドメイン内の vCenter Server の vSphere リソースにアクセスすることもできます。

vCloud Director の監視

10

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 vCloud 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。

- vCloud Director とコスト レポート
- タスクとイベントの表示
- ブロック タスクの監視および管理
- プロバイダ仮想データセンターの使用状況情報の表示
- 組織仮想データセンターの使用状況情報の表示
- vCloud Director の JMX サービスの使用
- vCloud Director ログの表示

vCloud Director とコスト レポート

vCloud Director に VMware vRealize Operations Tenant App を使用して、vCloud 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。

vCloud 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 vRealize Operations Tenant App for vCloud Director の使用』および『テナントとしての vRealize Operations Tenant App for vCloud Director の使用』を参照してください。

タスクとイベントの表示

システムのタスクとイベントおよび組織のタスクとイベントを表示し、vCloud Director アクティビティの監視と監査を行うことができます。

vCloud Director タスクは、長時間の操作とその状態の変化をタスクの進行状況として表します。たとえば、タスクの開始時のステータスは通常 **Running** です。タスクが終了すると、ステータスは **Successful** または **Error** に変化します。

vCloud Director イベントは単独の発生事象を表し、通常は操作の重要な部分、または vCloud Director オブジェクトの重要な状態の変化を示します。たとえば、vCloud Director では、ユーザーが組織仮想データセンターの作成を開始すると、イベントをログに記録し、プロセスが完了したときに別のイベントをログに記録します。また、vCloud Director では、ユーザーがログインするたびにイベントをログに記録し、ログインが成功したかどうかを記録します。

処理中および完了したシステム タスクの表示

システム ログを表示して、処理中のシステム レベルのタスク監視、失敗したタスクの検索とトラブルシューティング、および所有者別のタスク表示を行うことができます。

組織レベルのタスクに関する情報を確認するには、[処理中および完了した組織タスクの表示](#) を参照してください。

ログには、システム設定に応じてデバッグ情報を含めることもできます。[全般システム設定](#)を参照してください。

手順

- 1 vCloud Director にシステム管理者としてログインします。
- 2 [管理および監視] タブをクリックし、左側のペインで [ログ] をクリックします。
- 3 [タスク] タブをクリックします。

タスクのステータスやタスクを所有するユーザーの名前など、システム レベルのタスクに関する情報が表示されます。

- 4 詳細を表示するには、タスクをダブルクリックします。

処理中および完了した組織タスクの表示

組織のログを表示して、処理中の組織レベルのタスク監視、失敗したタスクの検索とトラブルシューティング、および所有者別のタスク表示を行うことができます。

システム レベルのタスクに関する情報を確認するには、[処理中および完了したシステム タスクの表示](#) を参照してください。

ログには、システム設定に応じてデバッグ情報を含めることもできます。[全般システム設定](#)を参照してください。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織] をクリックします。
- 2 組織名を右クリックし、[開く] を選択します。
- 3 [マイ クラウド] タブをクリックし、左側のペインで [ログ] をクリックします。
- 4 [タスク] タブをクリックします。

タスクのステータスやタスクを開始したユーザーの名前など、この組織が所有するタスクに関する情報が表示されます。

- 5 詳細を表示するには、タスクをダブルクリックします。

システム管理者のみが、ほぼすべてのタスクの詳細を表示できます。

システム イベントの表示

システム レベルのイベントを表示するには、システム ログを表示します。失敗したイベントの検索とトラブルシューティング、およびユーザー別のイベントの表示を行うことができます。

組織レベルのイベントに関する情報を確認するには、[組織イベントの表示](#) を参照してください。

手順

- 1 vCloud Director システムにシステム管理者としてログインします。
- 2 [管理および監視] タブをクリックし、左側のペインで [ログ] をクリックします。
- 3 [イベント] タブをクリックします。

vCloud Director には、システム レベルの各イベントに関する情報が表示されます。

- 4 詳細を表示するには、イベントをダブルクリックします。

組織イベントの表示

組織のログを表示して組織レベルのイベントを監視できます。失敗したイベントの検索とトラブルシューティング、およびユーザー別のイベントの表示を行うことができます。

システム レベルのイベントに関する情報を確認するには、[システム イベントの表示](#) を参照してください。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織] をクリックします。
- 2 組織名を右クリックし、[開く] を選択します。
- 3 [マイ クラウド] タブをクリックし、左側のペインで [ログ] をクリックします。
- 4 [イベント] タブをクリックします。

vCloud Director に、組織レベルの各イベントに関する情報が表示されます。

- 5 (オプション) 詳細を表示するには、イベントをダブルクリックします。

システム管理者のみが、ほぼすべてのイベントの詳細を表示できます。

実行中および完了したテナントのストレージ移行の表示

[ログ] ページの [テナント移行] タブを使用して、テナントのストレージ移行の監視やキャンセルを実行できます。

システム管理者、または [組織: テナント ストレージの移行] 権限が含まれるロールを持つユーザーは、テナント組織の vApp、独立型ディスク、カタログ アイテムのすべてを別のデータストアに移行できます。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、特に多数の資産を所有する組織の場合は、長時間にわたって実行される可能性があります。そのため、移行の進行状況を確認し、移行をキャンセルする方法が用意されています。[テナント ストレージの移行](#) を参照してください。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [ログ] をクリックします。
- 2 [テナントの移行] タブをクリックします。

vCloud Director には、キューにある、または進行中の各テナントのストレージ移行に関する情報が表示されます。

ブロック タスクの監視および管理

ブロックの結果として保留中の状態になっているタスクは、監視および管理することができます。

vCloud Director Web コンソールを使用してブロック タスクを監視および管理することは可能ですが、通常は vCloud API を使用して、コードの外部の一部が AMQP 通知を監視し、プログラムによって応答します。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [ブロック タスク] をクリックします。
- 2 タスクを右クリックし、アクションを選択します。

オプション	説明
レジューム	タスクを再開します。
中止	タスクをキャンセルし、タスクの一部として作成されたオブジェクトを削除します。
失敗	タスクを失敗させますが、タスクの一部として作成されたオブジェクトはクリーンアップしません。タスクとそのオブジェクトのステータスは、 <i>Error</i> に設定されます。

- 3 理由を入力し、[OK] をクリックします。

プロバイダ仮想データセンターの使用状況情報の表示

プロバイダ仮想データセンターは、組織仮想データセンターに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 リソースを提供します。プロバイダ仮想データセンターのリソースは、監視することも、必要に応じてさらに追加することもできます。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [プロバイダ vDC] をクリックします。
- 2 [監視] タブをクリックします。

結果

vCloud Director は 各プロバイダ仮想データセンターの CPU、メモリ、ストレージに関する情報を表示します。

組織仮想データセンターの使用状況情報の表示

組織仮想データセンターは、組織に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 リソースを提供します。組織仮想データセンターのリソースは、監視することも、必要に応じてさらに追加することもできます。

手順

- 1 [管理および監視] タブをクリックし、左側のペインで [組織 VDC] をクリックします。
- 2 [監視] タブをクリックします。

結果

vCloud Director は、各組織仮想データセンターの CPU、メモリ、ストレージに関する情報を表示します。

vCloud Director の JMX サービスの使用

各 vCloud Director サーバ ホストは、JMX を介して多くの MBean を公開することでサーバの運用管理を可能にして、内部統計情報へのアクセスを提供します。

JConsole を使用した JMX サービスへのアクセス

JMX クライアントを使用して vCloud Director JMX サービスにアクセスできます。JConsole は、JMX クライアントの 1 つです。

vCloud Director によって公開される MBean の詳細については、<http://kb.vmware.com/kb/1026065> を参照してください。

前提条件

接続先となる vCloud Director ホストのホスト名は、完全修飾ドメイン名または非修飾ホスト名の正引き参照と逆引き参照を使用して、DNS によって解決できる必要があります。

手順

- 1 JConsole を開始します。
- 2 [接続] メニューで [新規接続] を選択します。
- 3 [リモート プロセス] をクリックし、JMX サービスの URL を入力します。
URL には、vCloud Director サーバーのホスト名または IP アドレスの後にポート番号を付けます。たとえば、**example.com:8999** のように入力します。デフォルト ポートは 8999 です。
- 4 vCloud Director システム管理者のユーザー名とパスワードを入力し、[接続] をクリックします。
- 5 [MBean] タブをクリックします。

vCloud Director ログの表示

vCloud Director では、システムのクラウド セルごとにログ情報を提供します。ログを表示して、セルの監視や問題のトラブルシューティングを行うことができます。

セルのログは `/opt/vmware/vcloud-director/logs` にあります。表 10-1. vCloud Director のログでは、使用可能なログを一覧表示しています。

表 10-1. vCloud Director のログ

ログ名	説明
cell.log	vCloud Director セルからのコンソール出力。
cell-management-tool	セルからのセル管理ツール ログ メッセージ。
cell-runtime	セルからのランタイム ログ メッセージ。
cloud-proxy	セルからのクラウド プロキシ ログ メッセージ。
console-proxy	セルからのリモート コンソール プロキシ ログ メッセージ。
server-group-communications	セルからのサーバ グループ通信。
statsfeeder	vCenter Server からの仮想マシン メトリックの取得、およびストレージ情報とエラー メッセージ。
vcloud-container-debug.log	セルからのデバッグ レベルのログ メッセージ。
vcloud-container-info.log	セルからの情報ログ メッセージ。このログには、セルで発生した警告とエラーも表示されます。
vmware-vcd-watchdog.log	セル ウォッチドッグからの情報ログ メッセージ。セルがいつクラッシュしたか、再起動したかなどが記録されます。
diagnostics.log	セル診断ログ。このファイルは、ローカル ログ構成で診断ログが有効になっていない場合は空です。
YYYY_MM_DD.request.log	Apache 共通ログ形式の HTTP 要求ログ。

ログは、任意のテキスト エディタ/ビューアまたはサードパーティ ツールを使用して表示できます。

セル管理ツール リファレンス

11

セル管理ツールは、vCloud Director セルまたはデータベースの管理に使用するコマンド ライン ユーティリティです。大半の操作には、スーパーユーザーまたはシステム管理者の認証情報が必要です。

セル管理ツールは、`/opt/vmware/vcloud-director/bin/` にインストールされます。これは、単一のコマンドの実行またはインタラクティブ シェルとして実行する場合に使用できます。

使用可能なコマンドの一覧表示

使用可能なセル管理ツールのコマンドを一覧表示するには、次のコマンドラインを使用します。

```
./cell-management-tool -h
```

シェル モードの使用

セル管理ツールは、ここに示されているように引数なしで呼び出すことによって、インタラクティブ シェルとして実行できます。

```
[root@cell11 /opt/vmware/vcloud-director/bin]#./cell-management-tool
セル管理ツール v8.14.0.4146350。利用可能なサブコマンドについては、「help」と入力してください。cmt>
```

シェル モードでは、次の例に示されているように、`cmt>` プロンプトでセル管理ツールの任意のコマンドを入力できます。

```
cmt>cell -h
usage: cell [options] -a,--application-states display the state of each application on the
cell [DEPRECATED - use the cell-application command instead] -h,--help print this message
-i,--pid <arg> the process id of the cell [REQUIRED if username is not specified] -m,--
maintenance <arg> gracefully enter maintenance mode on the cell -p,--password <arg>
administrator password [OPTIONAL] -q,--quiesce <arg> quiesce activity on the cell -s,--
shutdown gracefully shutdown the cell -t,--status display activity on the cell -tt,--status-
verbose display a verbose description of activity on the cell -u,--username <arg>
administrator username [REQUIRED if pid is not specified] Note: You will be prompted for
administrator password if not entered in command line. cmt>
```

実行が終了すると、コマンドは `cmt>` プロンプトに戻ります。シェル モードを終了するには、`cmt>` プロンプトで **exit** と入力します。

例：セル管理ツールの使用法のヘルプ

この例では、使用可能なシェル管理ツールのコマンドをリストする単一の非インタラクティブ コマンドを実行しています。

```
[root@cell11 /opt/vmware/vcloud-director/bin]# ./cell-management-tool -h
usage: cell-management-tool -h,--help print this message Available commands: cell -
Manipulates the Cell and core components certificates - Reconfigures the SSL certificates for
the cell . . . For command specific help: cell-management-tool <commandName> -h
```

■ vCloud Director インストール環境の構成

サーバ グループのデータベースをシステム管理者のアカウントと関連情報で初期化するには、セル管理ツールの `system-setup` コマンドを使用します。

■ セルの管理

セル管理ツールの `cell` サブコマンドを使用すると、タスク スケジューラをサスペンドして新しいタスクを開始できないようにしたり、アクティブなタスクのステータスを表示したり、セルのメンテナンス モードをコントロールしたり、セルを正常にシャットダウンしたりすることができます。

■ セル アプリケーションの管理

セルの起動時に実行される一連のアプリケーションを管理するには、セル管理ツールの `cell-application` コマンドを使用します。

■ データベース テーブルのエクスポート

セル管理ツールの `dbextract` コマンドを使用すると、vCloud Director データベースからデータをエクスポートできます。

■ PostgreSQL データベースへの移行

セル管理ツールの `dbmigrate` サブコマンドを使用すると、既存の vCloud Director データベースを Oracle または Microsoft SQL Server から PostgreSQL に移行できます。

■ データベース接続プロパティを更新する

セル管理ツールの `reconfigure-database` サブコマンドを使用すると、vCloud Director データベースの接続プロパティを更新できます。

■ 破損したスケジューラ データの検出および修復

vCloud Director は、クォーツ ジョブ スケジューラを使用して、システムで実行されている非同期操作（ジョブ）を連携します。クォーツ スケジューラ データベースが破損すると、システムを正常に静止できない場合があります。スケジューラ データの破損の有無を確認するには、セル管理ツールの `fix-scheduler-data` コマンドを使用して、データベースをスキャンします。データが破損していた場合は、必要に応じて修復します。

■ HTTP およびコンソール プロキシ エンドポイントの自己署名証明書の生成

セル管理ツールの `generate-certs` コマンドを使用して、HTTP およびコンソール プロキシ エンドポイントの自己署名付き SSL 証明書を生成します。

■ HTTP およびコンソール プロキシ エンドポイントの証明書の置き換え

セル管理ツールの `certificates` コマンドを使用して、HTTP およびコンソール プロキシ エンドポイントの SSL 証明書を置き換えます。

■ 外部サービスからの SSL 証明書のインポート

セル管理ツールの `import-trusted-certificates` コマンドを使用して、AMQP や vCloud Director データベースなどの外部サービスへのセキュアな接続の確立に使用する証明書をインポートします。

■ 許可された SSL 暗号のリストの管理

SSL ハンドシェイク プロセス中に使用するためにセルが提供する暗号化スイートのセットを構成するには、セル管理ツールの `ciphers` コマンドを使用します。

■ 許可された SSL プロトコルのリストの管理

SSL ハンドシェイク プロセス中にセルが使用を提案する SSL プロトコルのセットを構成するには、セル管理ツールの `ssl-protocols` コマンドを使用します。

■ メトリック収集の設定

セル管理ツールの `configure-metrics` コマンドを使用して、収集するメトリックのセットを設定します。

■ Cassandra メトリック データベースの構成

セルをオプションのメトリック データベースに接続するには、セル管理ツールの `cassandra` コマンドを使用します。

■ システム管理者のパスワードの復元

vCloud Director データベースのユーザー名とパスワードが分かっている場合は、セル管理ツールの `recover-password` コマンドを使用して、vCloud Director システム管理者のパスワードを復元できます。

■ タスクの失敗ステータスの更新

セルが意図的にシャットダウンされたときに実行していたタスクに関連する完了ステータスを更新するには、セル管理ツールの `fail-tasks` コマンドを使用します。すべてのセルをシャットダウンしない限り、`fail-tasks` コマンドを使用することはできません。

■ 監査メッセージ処理の構成

システムが監査メッセージをログに記録する方法を構成するには、セル管理ツールの `configure-audit-syslog` コマンドを使用します。

■ 電子メール テンプレートの構成

電子メール アラートを作成する際にシステムが使用するテンプレートを管理するには、セル管理ツールの `manage-email` コマンドを使用します。

■ 親なしの仮想マシンの検索

セル管理ツールの `find-orphan-vms` コマンドを使用すると、vCenter データベースには存在するが vCloud Director データベースには存在しない仮想マシンへの参照を検索できます。

■ VMware カスタム エクスペリエンス改善プログラムへの参加または離脱

VMware カスタム エクスペリエンス改善プログラムに参加または離脱するには、セル管理ツールの `configure-ceip` サブコマンドを使用します。

■ アプリケーションの設定の更新

セル管理ツールの `manage-config` サブコマンドを使用すると、カタログ スロットリング アクティビティなどのさまざまなアプリケーションの構成を更新できます。

■ カタログ同期のスロットリングの設定

他の組織に公開された、または他の組織からサブスクライブされたカタログ項目が多数ある場合、カタログの同期中にシステムが過負荷にならないように、カタログ同期のスロットリングを設定できます。セル管理ツールの `manage-config` サブコマンドを使用すると、同時に同期できるライブラリ項目の数を制限することで、カタログ同期のスロットリングを設定できます。

■ vCenterServer 仮想マシン検出のデバッグ

セル管理ツールの `debug-auto-import` サブコマンドを使用すると、vApp の検出メカニズムが vCenter Server 仮想マシンを 1 台以上スキップする原因を調査できます。

■ マルチサイト拡張ネットワークの MAC アドレスの再生成

同じインストール ID で構成されている 2 つの vCloud Director サイトを関連付けると、これらのサイト間の拡張ネットワークで MAC アドレスの競合が発生する可能性があります。このような競合を回避するには、インストール ID とは異なるカスタム シードに基づいて、いずれかのサイトで MAC アドレスを再生成する必要があります。

■ vCloud Director セルのデータベース IP アドレスの更新

セル管理ツールを使用して、データベース高可用性クラスタ内の vCloud Director セルの IP アドレスを更新できます。

vCloud Director インストール環境の構成

サーバ グループのデータベースをシステム管理者のアカウントと関連情報で初期化するには、セル管理ツールの `system-setup` コマンドを使用します。

`system-setup` コマンドは、『vCloud Director インストール、構成、およびアップグレード ガイド』に記載されている vCloud Director セットアップ ウィザードの処理をコマンド ラインで実行するために用意されたコマンドです。vCloud Director サーバ グループに属するすべてのサーバを構成し、データベースに接続したら、最初のシステム管理者アカウントを作成し、次の形式のコマンド ラインを使用して vCloud Director データベースを関連情報で初期化できます。

```
cell-management-tools system-setup options
```

このコマンドを、セットアップ済みのシステムで実行することはできません。 `--unattended` と `--password` を除くすべてのオプションを指定する必要があります。

表 11-1. セル管理ツールのオプションと引数、`system-setup` サブコマンド

オプション	引数	説明
<code>--help (-h)</code>	なし	このカテゴリで使用可能なコマンドの概要を示します。
<code>--email</code>	作成するシステム管理者のメール アドレス。	システム管理者のメール アドレスは、vCloud Director データベースに格納されます。
<code>--full-name</code>	作成するシステム管理者のフル ネーム。	システム管理者のフル ネームは、vCloud Director データベースに格納されます。

表 11-1. セル管理ツールのオプションと引数、system-setup サブコマンド（続き）

オプション	引数	説明
--installation-id	1～63 の整数	この vCloud Director インストール環境のインストール ID。このインストール ID は、仮想 NIC の MAC アドレスを生成する際に使用されます。 注： マルチサイト展開の vCloud Director インストール間で拡張ネットワークを作成する予定がある場合は、各 vCloud Director インストールに一意的インストール ID を設定することを検討してください。
--password	作成するシステム管理者のパスワード。 --unattended オプションを使用する場合は必須です。--unattended オプションを使用していない場合に、コマンドラインにこのオプションを指定しないと、パスワードを尋ねるプロンプトが表示されます。	システム管理者は、vCloud Director の認証を受ける際に、このパスワードを入力します。
--serial-number	このインストールのシリアル番号（ライセンス キー）。	任意。指定する場合は、vCloud Director の有効なシリアル番号であることが必要です。
--system-name	vCloud Director vCenter Server フォルダの名前。	この vCloud Director インストール環境は、登録先の各 vCenter Server で、この名前のフォルダによって表されます。
--unattended	なし	任意。このオプションを指定してコマンドを起動すると、入力を求めるプロンプトが表示されなくなります。
--user	作成するシステム管理者のユーザー名。	システム管理者は、vCloud Director の認証を受ける際に、このユーザー名を入力します。

例： vCloud Director システム設定を指定する

この例のコマンドでは、vCloud Director インストール環境に必要なすべてのシステム設定を指定しています。--unattended および --password オプションが指定されていないため、システム管理者を作成する際にパスワードを入力および確認するよう要求されます。

```
[root@cell11 /opt/vmware/vcloud-director/
bin]#./cell-management-tool system-setup \ --user admin --full-name "VCD System
Administrator" --email vcd-admin@example.com --system-name VCD --installation-id 2
Please enter the new password for user admin (password must have more than 6 characters):

Re-enter the password to confirm:
```

```

Username: admin
Full name: VCD System Administrator
Email: vcd-admin@example.com
System name: VCD
Installation ID: 2
Are you sure you want to use these parameters? [Y/n]:y
Creating admin user.
Setting system details.
Completing system setup.
System setup is complete.

```

セルの管理

セル管理ツールの `cell` サブコマンドを使用すると、タスク スケジューラをサスペンドして新しいタスクを開始できないようにしたり、アクティブなタスクのステータスを表示したり、セルのメンテナンス モードをコントロールしたり、セルを正常にシャットダウンしたりすることができます。

セルを管理するには、次の形式でコマンドラインを使用します。

```
cell-management-tool cell -u sysadmin-username -p sysadmin-password option
```

ここで、*sysadmin-username* および *sysadmin-password* は、システム管理者のユーザー名およびパスワードです。

注： セキュリティ上の理由により、パスワードは省略できます。この場合、パスワードは画面に表示されず、パスワードの入力を求めるプロンプトが表示されます。

システム管理者の認証情報を入力する代わりに、`--pid` オプションを使用して、セル プロセスのプロセス ID を入力することもできます。セルのプロセス ID を検索するには、次のようなコマンドを使用します。

```
cat /var/run/vmware-vcd-cell.pid
```

表 11-2. セル管理ツールのオプションと引数、`cell` サブコマンド

オプション	引数	説明
<code>--help</code> (-h)	なし	このカテゴリで使用可能なコマンドの概要を示します。
<code>--pid</code> (-i)	セル プロセスのプロセス ID	このオプションは <code>-username</code> の代わりに使用できます。
<code>--maintenance</code> (-m)	true または false	セルをメンテナンス モードに設定します。 引数 true を指定すると、セルのアクティビティは静止し、セルがメンテナンス モードになります。 引数 false により、セルのメンテナンス モードが解除されます。

表 11-2. セル管理ツールのオプションと引数、cell サブコマンド（続き）

オプション	引数	説明
--password (-p)	vCloud Director システム管理者 のパスワード	-username オプションが使用されている場合は、オプションです。 このオプションを省略した場合、パスワードは画面に表示されず、パスワードの入力を求めるプロンプトが表示されます。
--quiesce (-q)	true または false	セル上のアクティビティを静止します。 引数 true はスケジューラを中断します。 引数 false はスケジューラを再開します。
--shutdown (-s)	なし	サーバ上の vCloud Director サービスを正常にシャットダウンします。
--status (-t)	なし	セル上で実行されているタスクの数とセルのステータスに関する情報を表示します。
--status-verbose (-tt)	なし	セル上で実行されているタスクとセルのステータスに関する詳細情報を表示します。
--username (-u)	vCloud Director システム管理者 のユーザー名	このオプションは -pid の代わりに使用できます。

セル アプリケーションの管理

セルの起動時に実行される一連のアプリケーションを管理するには、セル管理ツールの cell-application コマンドを使用します。

vCloud Director は vCloud Director クライアントが必要とするサービスを提供するさまざまなアプリケーションを実行します。セルはこれらのアプリケーションのサブセットをデフォルトで実行します。通常、vCloud Director のインストールをサポートするには、このサブセットに含まれるすべてのアプリケーションが必要になります。

セルの起動時に実行されるアプリケーションのリストを表示または変更するには、次の形式のコマンドラインを使用します。

```
cell-management-tool -u sysadmin-username -p sysadmin-password cell-application command
```

sysadmin-username

vCloud Director システム管理者のユーザー名。

sysadmin-password

vCloud Director システム管理者のパスワード。パスワードに特殊文字が含まれている場合はパスワードを引用符で囲む必要があります。

注： cell-management-tool コマンドラインに vCloud Director システム管理者のパスワードを入力することもできますが、パスワードを省略するほうが安全です。これにより、cell-management-tool でパスワードが要求されるようになりますが、入力内容は画面には表示されません。

システム管理者の認証情報を入力する代わりに、--pid オプションを使用して、セル プロセスのプロセス ID を入力することもできます。セルのプロセス ID を検索するには、次のようなコマンドを使用します。

```
cat /var/run/vmware-vcd-cell.pid
```

command

cell-application サブコマンド。

表 11-3. セル管理ツールのオプションと引数、cell-application サブコマンド

コマンド	引数	説明
--help (-h)	なし	このカテゴリで使用可能なコマンドの概要を示します。
--application-states	なし	セル アプリケーションと各アプリケーションの現在の状態を一覧表示します。
--disable	アプリケーション ID	セルの起動時にこのセル アプリケーションが実行されないようになります。
--enable	アプリケーション ID	セルの起動時にこのセル アプリケーションが実行されるようになります。
--pid (-i)	セル プロセスのプロセス ID	このオプションは -u または -u および -p の代わりに使用できます。
--list	なし	すべてのセル アプリケーションを一覧表示し、セルの起動時に実行するように設定されているかどうかを示します。
--password (-p)	vCloud Director 管理者パスワード	任意。コマンドラインでパスワードが入力されていない場合、コマンドの実行時にパスワードの入力を求めるプロンプトが表示されます。
--set	セミコロンで区切られたアプリケーション ID のリスト。	セルの起動時に実行するセル アプリケーションのセットを指定します。次のコマンドを使用すると、セルの起動時に起動するように設定されたセル アプリケーションの既存のセットが上書きされます。1 つのアプリケーションの起動状態を変更するには、--enable または --disable を使用します。
--username (-u)	vCloud Director 管理者ユーザー名。	--pid を指定しない場合は必須

例：セル アプリケーションとその起動状態の一覧表示

次の cell-management-tool コマンドラインを実行すると、セル アプリケーションとその起動状態のリストが返されます。コマンドの実行にはシステム管理者の認証情報が必要です。

```
[root@cell11 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool -u administrator cell-application --list
Please enter the administrator password:

name                id                enabled
```

description			
Networking	com.vmware.vc...	true	Exposes NSX api endpoints directly from vCD.
Console Proxy connection...	com.vmware.vc...	true	Proxies VM console data
Cloud Proxy site.	com.vmware.vc...	true	Proxies TCP connections from a tenant
Compute Service Broker control...	com.vmware.vc...	true	Allows registering with a service
Maintenance Application undergo ...	com.vmware.vc...	false	Indicates to users the cell is
Core Cell Application	com.vmware.vc...	true	Main cell application, Flex UI and REST API.

データベース テーブルのエクスポート

セル管理ツールの `dbextract` コマンドを使用すると、vCloud Director データベースからデータをエクスポートできます。

データベース テーブルをエクスポートするには、次の形式でコマンドラインを使用します。

```
cell-management-tool dbextract options
```

表 11-4. セル管理ツールのオプションと引数、dbextract サブコマンド

オプション	引数	説明
<code>--help (-h)</code>	なし	このカテゴリで使用可能なコマンドの概要を示します。
<code>-categories</code>	エクスポートするテーブル カテゴリのカンマ区切りリスト。	任意。NETWORKING が唯一サポートされているカテゴリです。
<code>-dataFile</code>	エクスポートするデータを記述したファイルへの絶対パス。	任意。指定しない場合、このコマンドでは <code>\$VCLLOUD_HOME/etc/data_to_export.properties</code> が使用されます。 エクスポートするテーブルと列の指定 を参照してください。
<code>-dumpFolder</code>	ダンプを作成するフォルダの絶対パス。フォルダは存在していて、vCloud から書き込み可能である必要があります。	すべてのデータはこのフォルダ内のファイルにエクスポートされます。
<code>-exportSettingsFile</code>	データ エクスポート設定プロパティ ファイルへの絶対パス。	任意。指定しない場合、このコマンドでは <code>\$VCLLOUD_HOME/etc/data_export_settings.ini</code> が使用されます。 エクスポートする行の制限と順序 を参照してください。

表 11-4. セル管理ツールのオプションと引数、dbextract サブコマンド（続き）

オプション	引数	説明
-properties	データベース接続プロパティ ファイルへの絶対パス。	任意。指定しない場合、このコマンドでは、\$VCLLOUD_HOME/etc/global.properties のデータベース接続プロパティが使用されます。 プロパティ ファイルの指定 を参照してください。
-tables	テーブルのカンマ区切りリスト。	任意。個々のテーブル名がわかるようにしてすべてのテーブルをエクスポートします。

プロパティ ファイルの指定

デフォルトで dbextract コマンドは、現在のセルの \$VCLLOUD_HOME/etc/global.properties ファイルにあるデータベース接続情報を使用して vCloud Director データベースからデータを抽出します。別の vCloud Director データベースからデータを抽出するには、ファイルでデータベース接続プロパティを指定し、コマンドラインで -properties オプションを使用してそのファイルへのパス名を指定します。プロパティ ファイルは、次の形式に従う UTF-8 ファイルです。

```
username=username
password=password
servicename=db_service_name
port=db_connection_port
database-ip=db_server_ip_address
db-type=db_type
```

username

vCloud Director データベースのユーザー名。

password

vCloud Director データベースのパスワード。

db_service_name

データベース サービス名。たとえば、orcl.example.com。

db_connection_port

データベース ポート。

db_server_ip_address

データベース サーバの IP アドレス。

db_type

データベース タイプ。Oracle または MS_SQL する必要があります。

エクスポートするテーブルと列の指定

エクスポートするデータ セットを制限するには、`-exportSettingsFile` オプションを使用し、エクスポートする個々のテーブルと、任意で各列を指定する `data_to_export.properties` ファイルを作成します。このファイルは、行を何も含まないか、`TABLE_NAME: COLUMN_NAME` 形式の行を含んだ UTF-8 ファイルです。

TABLE_NAME

データベース内のテーブルの名前。テーブル名の一覧を表示するには、すべてのテーブルをエクスポートします。

COLUMN_NAME

指定した `TABLE_NAME` 内の列の名前。

このサンプルの `data_to_export.properties` ファイルでは、ACL テーブルと ADDRESS_TRANSLATION テーブルから列をエクスポートします。

```
ACL:ORG_MEMBER_ID
ACL:SHARABLE_ID
ACL:SHARABLE_TYPE
ACL:SHARING_ROLE_ID
ADDRESS_TRANSLATION:EXTERNAL_ADDRESS
ADDRESS_TRANSLATION:EXTERNAL_PORTS
ADDRESS_TRANSLATION:ID
ADDRESS_TRANSLATION:INTERNAL_PORTS
ADDRESS_TRANSLATION:NIC_ID
```

このコマンドでは、このファイルが `$VCLLOUD_HOME/etc/data_to_export.properties` に存在すると想定していますが、別のパスを指定することもできます。

エクスポートする行の制限と順序

どのテーブルの場合でも、エクスポートする行数とエクスポートされる行の順序を指定できます。-

`exportSettingsFile` オプションを使用し、個々のテーブルを指定する `data_export_settings.ini` ファイルを作成します。このファイルは、エントリが何もないか、次の形式のエントリを含んだ UTF-8 ファイルです。

```
[TABLE_NAME]
rowlimit=int
orderby=COLUMN_NAME
```

TABLE_NAME

データベース内のテーブルの名前。テーブル名の一覧を表示するには、すべてのテーブルをエクスポートします。

COLUMN_NAME

指定した `TABLE_NAME` 内の列の名前。

このサンプルの `data_export_settings.ini` では、`AUDIT_EVENT` テーブルからエクスポートされるデータを先頭の 10000 行に制限し、`event_time` 列の値を基準に行の順序を指定しています。

```
[AUDIT_EVENT]
rowlimit=100000
orderby=event_time
```

このコマンドでは、このファイルが `$VCLLOUD_HOME/etc/data_export_settings.ini` に存在すると想定していますが、別のパスを指定することもできます。

例：現在の vCloud Director データベースからのすべてのテーブルのエクスポート

この例では、現在の vCloud Director データベースから `/tmp/dbdump` ファイルにすべてのテーブルをエクスポートします。

```
[root@cell11 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool dbextract -dumpFolder /tmp/dbdump
This utility outputs data from your vCloud Director system
that may contain sensitive data.
Do you want to continue and output the data (y/n)?
y
Exporting data now. Please wait for the process to finish
Exported 144 of 145 tables.
```

PostgreSQL データベースへの移行

セル管理ツールの `dbmigrate` サブコマンドを使用すると、既存の vCloud Director データベースを Oracle または Microsoft SQL Server から PostgreSQL に移行できます。

重要： vCloud Director 9.5 では、Oracle データベースはサポートされません。Oracle データベースを使用する vCloud Director のインストールをアップグレードする場合は、データベースをアップグレードする前に既存の Oracle データベースを PostgreSQL に移行する必要があります。

```
cell-management-tool
dbmigrate
options
```

重要： ホット移行はサポートされていません。データベースの移行を開始する前に、vCloud Director サービスを停止する必要があります。セル プラットフォームでコンソール、シェル、またはターミナル ウィンドウを開き、Linux コマンド `service vmware-vcd stop` を実行します。vCloud Director サービスの開始と停止については、『vCloud 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。

表 11-5. セル管理ツールのオプションと引数、dbmigrate サブコマンド

オプション	引数	説明
--help (-h)	なし	このカテゴリで使用可能なコマンドの概要を示します。
--database-host (-dbhost)	IP アドレスまたは完全修飾ドメイン名。	ターゲット PostgreSQL データベースホストの IP アドレスまたは完全修飾ドメイン名。
--database-name (-dbname)	PostgreSQL データベースの名前。	ターゲット PostgreSQL データベースを作成した際に選択した名前。通常は、vcloud です。
--database-password (-dbpassword)	PostgreSQL データベース ユーザーのパスワード。	ターゲット PostgreSQL データベースのデータベース ユーザー パスワード。
--database-port (-dbport)	データベース ホスト上で動作する PostgreSQL データベース サービスによって使用されるポート番号。	データベース ホスト上で動作する PostgreSQL データベース サービスによって使用されるポート番号。
--database-ssl	true または false	vCloud Director からの SSL 接続を要求するように、ターゲット PostgreSQL データベースを構成します。
--database-user (-dbuser)	PostgreSQL データベース ユーザーの名前。	ターゲット PostgreSQL データベースのデータベース ユーザー名。
--private-key-path	パブリック キーがサーバーグループ内の他のセルの <code>authorized_keys</code> に追加された、プライベート キーの絶対パス。	移行が完了した後、ターゲット PostgreSQL データベースを使用するように、サーバーグループ内のすべてのセルを再構成します。 重要： すべてのセルは、パスワードを要求せずにスーパー ユーザーからの SSH 接続を許可する必要があります。
--verbose	なし	すべてのログ出力をコンソールとログ ファイルに送信します。各テーブルの移行ステータスと、操作全体の進行状況を報告する情報が含まれます。

--private-key-path オプションを使用する場合、パスワードを要求せずにスーパー ユーザーからの SSH 接続を許可するように、すべてのセルを構成する必要があります。たとえば、検証を実行するには、次の Linux コマンドを実行します。

```
sudo -u vcloud ssh -i private-key-path root@cell-ip
```

この例では、ID が `vcloud` に設定され、`cell-ip` にあるセルへの SSH 接続が `root` として確立されますが、`root` パスワードの指定はありません。ローカル セルの `private-key-path` にあるプライベート キーがユーザー `vcloud.vcloud` から読み取り可能で、対応するパブリック キーが `cell-ip` の `root` ユーザーの `authorized-keys` ファイルにあれば、コマンドが成功します。

注： vCloud Director プロセスを実行する ID として使用するため、vCloud Director インストーラにより、`vcloud` ユーザー、`vcloud` グループ、および `vcloud.vcloud` アカウントが作成されます。`vcloud` ユーザーにはパスワードがありません。

例：vCloud Director データベースを PostgreSQL に移行し、すべてのセルのデータベース接続プロパティを更新する

次のコマンドは、現在の vCloud Director データベースをホスト `psql.example.com` にインストールされているターゲット PostgreSQL データベースに移行します。`--private-key-path` オプションが含まれているため、移行が正常に完了すると、サーバ グループ内のすべてのセルがターゲット データベースに接続するように再構成されます。

```
[root@cell11 /opt/vmware/vcloud-director/
bin]#cell-management-tool dbmigrate \ -dbhost psql.example.com -dbport 5432 -dbuser vcd-dba
-dbname vcloud -dbpassword P@55w0rd \ --private-key-path /vcloud/.ssh/id_rsa
configuring the target database...
```

`--private-key-path` オプションが含まれていない場合は、移行が完了した後、サーバ グループ内の各セルで `reconfigure-database` サブコマンドを実行することによって、セルをターゲット データベースに接続することができます。[vCloud Director データベースを PostgreSQL に移行した後、セルを再構成する](#)を参照してください。

データベース接続プロパティを更新する

セル管理ツールの `reconfigure-database` サブコマンドを使用すると、vCloud Director データベースの接続プロパティを更新できます。

vCloud Director のインストール プロセスまたは vCloud Director アプライアンスのデプロイ プロセスで、データベース タイプとデータベース接続のプロパティを設定します。『vCloud 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。

vCloud Director データベースを設定した後に、`reconfigure-database` サブコマンドを使用してデータベース接続を更新できます。既存の vCloud Director データベースの新しいホストへの移動、データベースのユーザー名またはパスワードの変更、PostgreSQL データベースの SSL 接続の有効化を行うことができます。

グループ内のセルを再構成せずに vCloud Director データベースを PostgreSQL に移行した場合は、reconfigure-database サブコマンドを使用して、セルを新しい PostgreSQL データベースに接続することができます。PostgreSQL への移行については、[PostgreSQL データベースへの移行](#)を参照してください。

```
cell-management-tool
reconfigure-database
options
```

重要： reconfigure-database コマンドを実行して加えられた変更は、セルのグローバル構成ファイル global.properties および応答ファイル responses.properties に書き込まれます。コマンドを実行する前に、応答ファイルが /opt/vmware/vcloud-director/etc/responses.properties にあり、書き込み可能であることを確認してください。応答ファイルの保護と再利用の詳細については、「vCloud 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。

--pid オプションを使用しない場合、変更を適用するには、セルを再起動する必要があります。

表 11-6. セル管理ツールのオプションと引数、reconfigure-database サブコマンド

オプション	引数	説明
--help (-h)	なし	このカテゴリで使用可能なオプションの概要を示します。
--database-host (-dbhost)	vCloud Director データベース ホストの IP アドレスまたは完全修飾ドメイン名	database.jdbcUrl プロパティの値を更新します。 重要： このコマンドは、値の形式のみを検証します。
--database-instance (-dbinstance)	SQL Server データベース インスタンス	オプション。データベース タイプが sqlserver の場合に使用します。 重要： このオプションを指定する場合は、最初にデータベースを設定したときと同じ値を指定する必要があります。
--database-name (-dbname)	データベース サービス名。	database.jdbcUrl プロパティの値を更新します。
--database-password (-dbpassword)	データベース ユーザーのパスワード。	database.password プロパティの値を更新します。指定したパスワードは暗号化されてからプロパティ値として格納されます。
--database-port (-dbport)	データベース ホスト上で動作するデータベース サービスによって使用されるポート番号。	database.jdbcUrl プロパティの値を更新します。 重要： このコマンドは、値の形式のみを検証します。

表 11-6. セル管理ツールのオプションと引数、reconfigure-database サブコマンド（続き）

オプション	引数	説明
--database-type (-dbtype)	データベース タイプ。次のいずれか： ■ sqlserver ■ postgres	database.jdbcUrl プロパティの値を更新します。
--database-user (-dbuser)	データベース ユーザーのユーザー名	database.user プロパティの値を更新します。
--database-ssl	true または false	データベース タイプが postgres の場合に使用します。vCloud Director からの SSL 接続を要求するように、PostgreSQL データベースを設定します。
--pid (-i)	セルのプロセス ID。	オプション。実行中の vCloud Director セルにホット再構成を実行します。セルを再起動する必要はありません。 --private-key-path と一緒に使用した場合は、ローカルおよびリモートのセルにコマンドを直ちに実行できます。
--private-key-path	セルのプライベート キーへのパス名。	オプション。サーバ グループ内のすべてのセルが正常にシャットダウンされ、そのデータベース プロパティが更新され、再起動されます。 重要： すべてのセルは、パスワードを要求せずにスーパー ユーザーからの SSH 接続を許可する必要があります。
--remote-sudo-user	sudo 権限を持つユーザーの名前。	リモート ユーザーが root と異なる場合に、--private-key-path オプションと一緒に使用します。 アプライアンスの場合は、postgres ユーザーにこのオプションを使用できます（--remote-sudo-user=postgres など）。

オプション --database-host および --database-port を使用した場合、コマンドでは引数の形式は検証されますが、ホストとポートの組み合わせでネットワークにアクセスできるかどうか、または指定したタイプで実行中のデータベースがあるかどうかは確認されません。

--private-key-path オプションを使用する場合、パスワードを要求せずにスーパー ユーザーからの SSH 接続を許可するように、すべてのセルを構成する必要があります。たとえば、検証を実行するには、次の Linux コマンドを実行します。

```
sudo -u vcloud ssh -i private-key-path root@cell-ip
```

この例では、ID が `vcloud` に設定され、`cell-ip` にあるセルへの SSH 接続が `root` として確立されますが、`root` パスワードの指定はありません。ローカル セルの `private-key-path` にあるプライベート キーがユーザー `vcloud.vcloud` から読み取り可能で、対応するパブリック キーが `cell-ip` の `root` ユーザーの `authorized-keys` ファイルにあれば、コマンドが成功します。

注： vCloud Director プロセスを実行する ID として使用するため、vCloud Director インストーラにより、`vcloud` ユーザー、`vcloud` グループ、および `vcloud.vcloud` アカウントが作成されます。`vcloud` ユーザーにはパスワードがありません。

例：vCloud Director データベースのユーザー名とパスワードを変更する

vCloud Director データベースのユーザー名とパスワードを変更し、他のすべての接続プロパティを最初に設定したままにしておくには、次のコマンドを実行します。

```
[root@cell11 /opt/vmware/vcloud-director/
bin]#cell-management-tool reconfigure-database \ -dbuser vcd-dba -dbpassword P@55w0rd
```

例：すべてのセルのホット再構成による vCloud Director データベースの IP アドレスの更新

`sudo` 権限を持つ非 `root` ユーザーがすべてのセルの vCloud Director データベースの IP アドレスを直ちに変更するには、次のコマンドを実行します。

```
[sudo@cell11 /opt/vmware/vcloud-director/
bin]#cell-management-tool reconfigure-database \ --dbhost db_ip_address -i $(service vmware-
vcd pid cell) --private-key-path=path_to_private-key \ --remote-sudo-user=non-root-user
```

例：vCloud Director データベースを PostgreSQL に移行した後、セルを再構成する

サーバ グループ内のセルを再構成せずに、vCloud Director データベースを Oracle または Microsoft SQL Server から PostgreSQL に移行した場合、各セルを新しい PostgreSQL データベースに接続するには、次のコマンドを実行します。

```
[root@cell11 /opt/vmware/vcloud-director/
bin]#cell-management-tool reconfigure-database \ -dbhost psql.example.com -dbport 5432
-dbuser vcd-dba -dbname vcloud -dbpassword P@55w0rd \ -dbtype postgres
```

破損したスケジューラ データの検出および修復

vCloud Director は、クォーツ ジョブ スケジューラを使用して、システムで実行されている非同期操作（ジョブ）を連携します。クォーツ スケジューラ データベースが破損すると、システムを正常に静止できない場合があります。スケジューラ データの破損の有無を確認するには、セル管理ツールの `fix-scheduler-data` コマンドを使用して、データベースをスキャンします。データが破損していた場合は、必要に応じて修復します。

データベース内で破損したスケジューラ データをスキャンするには、次の形式のコマンド ラインを使用します。

```
cell-management-tool fix-scheduler-data options
```

表 11-7. セル管理ツールのオプションと引数、fix-scheduler-data サブコマンド

オプション	引数	説明
--help (-h)	なし	このカテゴリで使用可能なコマンドの概要を示します。
--dbuser	vCloud Director データベース ユーザーのユーザー名。	コマンドラインで指定する必要があります。
--dbpassword	vCloud Director データベース ユーザーのパスワード。	指定しない場合に入力が求められます。

HTTP およびコンソール プロキシ エンドポイントの自己署名証明書の生成

セル管理ツールの `generate-certs` コマンドを使用して、HTTP およびコンソール プロキシ エンドポイントの自己署名付き SSL 証明書を生成します。

各 vCloud Director サーバ グループは 2 台の SSL エンドポイントをサポートする必要があります。1 台は HTTP サービスのエンドポイント、もう 1 台はコンソール プロキシ サービスのエンドポイントです。HTTP サービスのエンドポイントでは、vCloud Director Web コンソールおよび vCloud API をサポートします。リモート コンソール プロキシのエンドポイントでは、vApp および仮想マシンへの VMRC 接続をサポートします。

セル管理ツールの `generate-certs` コマンドは、『vCloud Director インストール、構成、およびアップグレードガイド』に示した「自己署名付き SSL 証明書の作成」手順を自動化します。

新しい自己署名付き SSL 証明書を生成して新規または既存のキーストアに追加するには、次の形式でコマンドラインを使用します。

```
cell-management-toolgenerate-certsoptions
```

表 11-8. セル管理ツールのオプションと引数、generate-certs サブコマンド

オプション	引数	説明
--help (-h)	なし	このカテゴリで使用可能なコマンドの概要を示します。
--expiration (-x)	<i>days-until-expiration</i>	証明書の有効期限が切れるまでの日数です。デフォルトでは 365 です。
--issuer (-i)	<i>name= value [, name= value, ...]</i>	証明書発行者の X.509 識別名。デフォルトでは <i>CN=FQDN</i> です。 <i>FQDN</i> はセルの完全修飾ドメイン名です。完全修飾ドメイン名が使用できない場合は、その IP アドレスです。複数の属性と値のペアを指定する場合は、各ペアをカンマで区切り、引数全体を引用符で囲んでください。
--httpcert (-j)	なし	HTTP エンドポイントの証明書を生成します。

表 11-8. セル管理ツールのオプションと引数、generate-certs サブコマンド（続き）

オプション	引数	説明
--key-size (-s)	<i>key-size</i>	整数ビットとして表されるキー ペアのサイズです。デフォルトでは 2048 です。NIST Special Publication 800-131A に従い、1024 未満のキー サイズはサポートされなくなりました。
--keystore-pwd (-w)	<i>keystore-password</i>	このホスト上のキーストアのパスワードです。
--out (-o)	<i>keystore-pathname</i>	このホスト上のキーストアへのフル パス名です。
--consoleproxycert (-p)	なし	コンソール プロキシ エンドポイントの証明書を作成します。

注： このサブコマンドの以前のリリースとの互換性を維持するために、-j と -p の両方を省略すると、-j と -p を両方指定した場合と同じ結果となります。

例： 自己署名付き証明書の作成

これらの両方の例では、キーストアが /tmp/cell.ks に存在し、パスワードが kspwであることを想定しています。このキーストアは、まだ存在しない場合には作成されます。

この例では、デフォルト値を使用して新しい証明書を作成します。発行者名は CN=Unknown に設定されています。証明書はキー長にデフォルトの 2048 ビットを使用し、作成後 1 年で期限切れになります。

```
[root@cell11 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool generate-certs -j -p -o /tmp/cell.ks -w kspw
New keystore created and written to /tmp/cell.ks.
```

この例では HTTP エンドポイント専用の新しい証明書を作成します。また、キー サイズおよび発行者名を示すカスタム値を指定します。発行者名は CN=Test, L=London, C=GB に設定されています。HTTP 接続の新しい証明書のキー長は 4096 ビットで、作成後 90 日で期限が切れます。コンソール プロキシ エンドポイントの既存の証明書は影響を受けません。

```
[root@cell11 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool generate-certs -j -o /tmp/cell.ks -w kspw -i "CN=Test, L=London,
C=GB" -s 4096 -x 90
New keystore created and written to /tmp/cell.ks.
```

重要： キーストア ファイルおよびキーストア ファイルが格納されているディレクトリは、ユーザー vcloud.vcloud から読み取り可能である必要があります。vCloud Director インストーラにより、このユーザーとグループが作成されます。

HTTP およびコンソール プロキシ エンドポイントの証明書の置き換え

セル管理ツールの `certificates` コマンドを使用して、HTTP およびコンソール プロキシ エンドポイントの SSL 証明書を置き換えます。

セル管理ツールの `certificates` コマンドにより、JCEKS キーストアに保存されている新しい証明書で既存の証明書を置き換えるプロセスが自動化されます。`certificates` コマンドを使用して、自己署名証明書を署名付き証明書に、または有効期限が切れる証明書を新しい証明書に置き換えます。署名付き証明書が格納された JCEKS キーストアを作成する方法については、『vCloud Director インストール、構成、およびアップグレード ガイド』の「自己署名付き SSL 証明書の作成」を参照してください。

エンドポイントのいずれかまたは両方の SSL 証明書を置き換えるには、次の形式でコマンドを使用します。

```
cell-management-toolcertificatesoptions
```

表 11-9. セル管理ツールのオプションと引数、`certificates` サブコマンド

オプション	引数	説明
<code>--help (-h)</code>	なし	このカテゴリで使用可能なコマンドの概要を示します。
<code>--config (-c)</code>	セルの <code>global.properties</code> ファイルへのフル パス名	デフォルト値は、 <code>\$VCLLOUD_HOME/etc/global.properties</code> です。
<code>--https (-j)</code>	なし	http エンドポイントによって使用される <code>certificates</code> という名前のキーストア ファイルを置換します。
<code>--consoleproxyks (-p)</code>	なし	コンソール プロキシ エンドポイントによって使用される <code>proxycertificates</code> という名前のキーストア ファイルを置換します。
<code>--responses (-r)</code>	セルの <code>responses.properties</code> ファイルへのフル パス名	デフォルトで <code>\$VCLLOUD_HOME/etc/responses.properties</code> です。
<code>--keystore (-k)</code>	<i>keystore-pathname</i>	署名付き証明書が保存されている JCEKS キーストアへのフル パス名です。 <code>-k</code> に置き換えられる非推奨の <code>-s</code> 短縮形
<code>--keystore-password (-w)</code>	<i>keystore-password</i>	<code>--keystore</code> オプションによって参照される JCEKS キーストアのパスワードです。非推奨の <code>-kspassword</code> および <code>--keystorepwd</code> オプションを置き換えます。

例：証明書の置換

--config オプションと --responses オプションは、そのデフォルトの場所から移動されていない限り、省略できます。この例では、キーストアが /tmp/my-new-certs.ks に存在し、パスワードは kspw となっています。この例では、セルの既存の HTTP エンドポイント証明書を /tmp/my-new-certs.ks 内の証明書で置き換えます。

```
[root@cell11 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool certificates -j -k /tmp/my-new-certs.ks -w kspw
Certificate replaced by user specified keystore at /tmp/new.ks.
You will need to restart the cell for changes to take effect.
```

注： 証明書を置換した後は、セルを再起動する必要があります。

外部サービスからの SSL 証明書のインポート

セル管理ツールの import-trusted-certificates コマンドを使用して、AMQP や vCloud Director データベースなどの外部サービスへのセキュアな接続の確立に使用する証明書をインポートします。

外部サービスへのセキュアな接続を作成するには、vCloud Director で、外部サービスの証明書を固有のトラストストアにインポートして、そのサービスの有効な信頼チェーンを確立する必要があります。信頼されている証明書をセルのトラストストアにインポートするには、次の形式でコマンドを使用します。

```
cell-management-tool import-trusted-certificates options
```

表 11-10. セル管理ツールのオプションと引数、import-trusted-certificates サブコマンド

オプション	引数	説明
--help(-h)	なし	このカテゴリで使用可能なコマンドの概要を示します。
--destination	パス名	ターゲットのトラストストアへのフルパス名。コマンドラインで指定されていない場合は、デフォルトで /opt/vmware/vcloud-director/etc/certificates が使用されます。
--destination-password	文字列	ターゲットのトラストストアのパスワード。コマンドラインで指定されていない場合、デフォルトは vcloud.ssl.truststore.password の値で設定されます。
--destination-type	キーストアのタイプ	ターゲットのトラストストアのキーストアタイプ。JKS または JCEKS のいずれかにできます。デフォルトでは JCEKS です。
--force	なし	ターゲットのトラストストア内の既存の証明書を上書きします。
--source	パス名	ソース PEM ファイルへのフルパス名。

例：信頼されている証明書のインポート

この例では、証明書を「/tmp/demo.pem」から「/opt/vmware/vcloud-director/etc/certificates」の vCloud Director ローカル キーストアにインポートします。vCloud Director はキーストアのパスワードを import-trusted-certificates コマンドで復号される暗号化形式で格納します。

```
[root@cell11 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool import-trusted-certificates --source /tmp/demo.pem
```

許可された SSL 暗号のリストの管理

SSL ハンドシェイク プロセス中に使用するためにセルが提供する暗号化スイートのセットを構成するには、セル管理ツールの ciphers コマンドを使用します。

クライアントが vCloud Director セルとの SSL 接続を確立すると、セルはデフォルトの許可暗号リスト上で構成された暗号のみを使用するよう提案します。接続を保護する十分な強度がないか、あるいは SSL 接続障害の原因となることがわかっているために、このリストに含まれていない暗号があります。vCloud Director をインストールまたはアップグレードすると、インストールまたはアップグレードのスクリプトがセルの証明書を調べます。いずれかの証明書が許可暗号リストに含まれていない暗号を使用して暗号化されている場合、スクリプトはセルの構成を変更してこの暗号の使用を許可し、警告を表示します。これらの暗号を利用しながら既存の証明書を引き続き使用することも、次の手順を実行して証明書を置き換え、許可暗号リストを再構成することもできます。

- 1 禁止されたどの暗号も使用しない新しい証明書を作成します。[許可されているすべての暗号の一覧表示](#)に示された cell-management-tool ciphers -a を使用して、デフォルト構成で許可されている暗号をすべて一覧表示することができます。
- 2 cell-management-tool certificates コマンドを使用すると、セルの既存の証明書が新しい証明書で置き換えられます。
- 3 cell-management-tool ciphers コマンドを使用すると、許可暗号リストを再構成して、新しい証明書で使用されない暗号を除外することができます。これらの暗号を除外すると、ハンドシェイク中に提供される暗号数が実用的な最小数まで減るため、セルとの SSL 接続を確立するまでの時間が短縮されます。

重要： VMRC コンソールでは AES256-SHA および AES128-SHA 暗号を使用する必要があるため、vCloud Director クライアントで VMRC コンソールを使用する場合は、これらを禁止できません。

許可されている SSL 暗号のリストを管理するには、次の形式のコマンド ラインを使用します。

```
cell-management-tool ciphers options
```

表 11-11. セル管理ツールのオプションと引数、ciphers サブコマンド

オプション	引数	説明
--help (-h)	なし	このカテゴリで使用可能なコマンドの概要を示します。
--all-allowed (-a)	なし	許可されているすべての暗号を一覧表示します。

表 11-11. セル管理ツールのオプションと引数、ciphers サブコマンド（続き）

オプション	引数	説明
<code>--compatible-reset (-c)</code>	なし	デフォルトの許可暗号リストにリセットし、さらにこのセルの証明書で使用する暗号を許可します。
<code>--disallow (-d)</code>	http://www.openssl.org/docs/apps/ciphers.html で公開されている、暗号名のカンマ区切りリスト	指定されたカンマ区切りリストで暗号を禁止します。
<code>--list (-l)</code>	なし	現在構成されている暗号を一覧表示します。
<code>--reset (-r)</code>	なし	デフォルトの許可暗号リストにリセットします。このセルの証明書で禁止された暗号が使用されている場合は、許可された暗号を使用する新しい証明書をインストールするまで、このセルとの SSL 接続は確立できません。

例：許可されているすべての暗号の一覧表示

`--all-allowed (-a)` オプションを使用すると、このセルが SSL ハンドシェイク中に提供することが許可されている暗号がすべて一覧表示されます。

```
[root@cell11 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ciphers -a
* TLS_DHE_DSS_WITH_AES_256_CBC_SHA
* TLS_DHE_DSS_WITH_AES_128_CBC_SHA
* TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
* TLS_DHE_RSA_WITH_AES_256_CBC_SHA
* TLS_DHE_RSA_WITH_AES_128_CBC_SHA
* TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
* TLS_RSA_WITH_AES_256_CBC_SHA
* TLS_RSA_WITH_AES_128_CBC_SHA
* TLS_RSA_WITH_3DES_EDE_CBC_SHA
* TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
* TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
* TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
* TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
* TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
* TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
* TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
* TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
* TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
* TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
* TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
* TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
* SSL_RSA_WITH_3DES_EDE_CBC_SHA
* SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
```


例：2つの暗号の禁止

許可暗号リストから1つ以上の暗号を削除するには、`--disallow (-d)` オプションを使用します。このオプションには1つ以上の暗号名を指定する必要があります。カンマ区切りリストでは、複数の暗号名を指定できます。`ciphers -a` の出力からこのリストの名前を取得できます。次の例では、前の例で一覧表示された2つの暗号を削除します。

```
[root@cell11 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool ciphers -d
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA,SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
```

許可された SSL プロトコルのリストの管理

SSL ハンドシェイク プロセス中にセルが使用を提案する SSL プロトコルのセットを構成するには、セル管理ツールの `ssl-protocols` コマンドを使用します。

クライアントが vCloud Director セルとの SSL 接続を確立すると、セルは許可された SSL プロトコルのリスト上で構成されたプロトコルのみを使用するよう提案します。TLSv1、SSLv3、SSLv2Hello などのプロトコルには重大なセキュリティ上の脆弱性があることがわかっているため、デフォルトのリストには含まれていません。

許可されている SSL プロトコルのリストを管理するには、次の形式のコマンド ラインを使用します。

```
cell-management-tool ssl-protocols options
```

表 11-12. セル管理ツールのオプションと引数、`ssl-protocols` サブコマンド

オプション	引数	説明
<code>--help (-h)</code>	なし	このカテゴリで使用可能なコマンドの概要を示します。
<code>--all-allowed (-a)</code>	なし	vCloud Director がサポートできるすべての SSL プロトコルをリストします。
<code>--disallow (-d)</code>	SSL プロトコル名のカンマ区切りのリスト	許可されない SSL プロトコルのリストを、リスト内で指定されたプロトコルに再構成します。
<code>--list (-l)</code>	なし	vCloud Director が現在サポートするように構成されている、許可された SSL プロトコルのセットをリストします。
<code>--reset (-r)</code>	なし	構成された SSL プロトコルのリストを出荷時のデフォルトにリセットします。

重要： `ssl-protocols --disallow` または `ssl-protocols reset` を実行した後は、セルを再起動する必要があります。

例：許可され構成された SSL プロトコルの一覧表示

--all-allowed (-a) オプションを使用すると、このセルが SSL ハンドシェイク中に提供することが許可されている SSL プロトコルがすべて一覧表示されます。

```
[root@cell11 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ssl-protocols -a
Product default SSL protocols:

* TLSv1.2
* TLSv1.1
* TLSv1
* SSLv3
* SSLv2Hello
```

このリストは通常、セルがサポートするように構成された SSL プロトコルのスーパーセットです。これらの SSL プロトコルを一覧表示するには、--list (-l) オプションを使用します。

```
[root@cell11 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ssl-protocols -l
Allowed SSL protocols:

* TLSv1.2
* TLSv1.1
```

例：許可されない SSL プロトコルのリストの再構成

--disallow (-d) オプションを使用すると、許可されない SSL プロトコルのリストが再構成されます。このオプションを使用するには、ssl-protocols -a によって生成された許可されるプロトコルのサブセットのコンマ区切りのリストが必要です。

この例では、許可される SSL プロトコルのリストを更新し、TLSv1 が含まれるようにしています。5.5 Update 3e より前の VMware® vCenter™ リリースには TLSv1 が必要です。

```
[root@cell11 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool ssl-protocols -d SSLv3,SSLv2Hello
```

このコマンドを実行した後は、セルを再起動する必要があります。

メトリック収集の設定

セル管理ツールの configure-metrics コマンドを使用して、収集するメトリックのセットを設定します。

vCloud Director は、仮想マシンのパフォーマンスおよびリソース消費に関する現在および過去の情報を提供するメトリックを収集できます。このサブコマンドを使用して、vCloud Director によって収集されるメトリックを設定します。cell-management-tool cassandra サブコマンドを使用して、vCloud Director メトリック リポジトリとして使用するための Apache Cassandra データベースを設定します。[Cassandra メトリック データベースの構成](#) を参照してください。

vCloud Director によって収集されるメトリックを設定するには、次の形式でコマンド ラインを使用します。

```
cell-management-tool configure-metrics --metrics-config pathname
```

表 11-13. セル管理ツールのオプションと引数、configure-metrics サブコマンド

コマンド	引数	説明
--help (-h)	なし	このカテゴリで使用可能なコマンドの概要を示します。
--repository-host (廃止されました)	KairosDB ホストのホスト名または IP アドレス	廃止されました。cell-management-tool cassandra サブコマンドの --cluster-nodes オプションを使用して、vCloud Director メトリック リポジトリとして使用するための Apache Cassandra データベースを設定します。
--repository-port (廃止されました)	使用する KairosDB ポート。	廃止されました。cell-management-tool cassandra サブコマンドの --port オプションを使用して、vCloud Director メトリック リポジトリとして使用するための Apache Cassandra データベースを設定します。
--metrics-config	パス名	メトリック設定ファイルへのパス

例：メトリック データベース接続の構成

この例では、/tmp/metrics.groovy ファイルで指定されているように、メトリック収集を設定します。

```
[root@cell1 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool configure-metrics --metrics-config /tmp/metrics.groovy
```

vCloud Director メトリック収集サービスでは、vSphere Performance Manager で収集されたメトリックのサブセットを実装します。メトリック名と収集パラメータの詳細については、vSphere Performance Manager のドキュメントを参照してください。metrics-config ファイルでは、1 つ以上のメトリック名を列挙し、列挙した各メトリックの収集パラメータを提供します。以下にその例を挙げます。

```
configuration {
  metric("cpu.usage.average")
  metric("cpu.usagemhz.average")
  metric("cpu.usage.maximum")
  metric("disk.used.latest") {
    currentInterval=300
    historicInterval=300
    entity="VM"
    instance=""
    minReportingInterval=1800
    aggregator="AVERAGE"
  }
}
```

次のメトリック名がサポートされています。

表 11-14. メトリック名

メトリック名	説明
cpu.usage.average	この仮想マシンでアクティブに使用される平均 CPU（使用可能な合計 CPU を占める割合）のホストのビュー。すべてのソケットのすべてのコアが含まれます。
cpu.usagemhz.average	この仮想マシンでアクティブに使用される平均 CPU（実際の測定値）のホストのビュー。すべてのソケットのすべてのコアが含まれます。
cpu.usage.maximum	この仮想マシンでアクティブに使用される最大 CPU（使用可能な合計 CPU を占める割合）のホストのビュー。すべてのソケットのすべてのコアが含まれます。
mem.usage.average	この仮想マシンによって使用されるメモリ（構成済みの合計メモリを占める割合）。
disk.provisioned.latest	含まれる組織仮想データセンターで、この仮想ハード ディスクに割り当てられたストレージ容量。
disk.used.latest	すべての仮想ハード ディスクによって使用されるストレージ。
disk.read.average	すべての仮想ハード ディスクの平均読み取り比率。
disk.write.average	すべての仮想ハード ディスクの平均書き込み比率。

注： 仮想マシンに複数のディスクが含まれる場合、メトリックはすべてのディスクの集計として報告されます。CPU メトリックは、すべてのコアおよびソケットの集計です。

名前付きの各メトリックについては、次の収集パラメータを指定できます。

表 11-15. メトリック収集パラメータ

パラメータ名	値	説明
currentInterval	秒を示す整数。	現在のメトリックのクエリで、最新の使用可能なメトリック値のクエリ時に使用する間隔（秒）。指定しない場合は、デフォルトで 20 が使用されます。20 を超える値がサポートされるのは、vSphere Performance Manager で定義されている、レベル 1 のメトリックに対してのみです。
historicInterval	秒を示す整数。	履歴のメトリック値のクエリ時に使用する間隔（秒）です。指定しない場合は、デフォルトで 20 が使用されます。20 を超える値がサポートされるのは、vSphere Performance Manager で定義されている、レベル 1 のメトリックに対してのみです。
entity	HOST、VM のいずれか	メトリックを使用できる vCenter Server オブジェクトのタイプ。指定しない場合は、デフォルトで VM が使用されます。エンティティによっては、使用できないメトリックもあります。
instance	vSphere Performance Manager の PerfMetricId インスタンス識別子。	メトリックの個々のインスタンス（たとえば、個々の CPU コア）、すべてのインスタンスの集計、またはその両方のデータを取得するかを指定します。 "*" の値を指定すると、すべてのメトリック、インスタンス、および集計のデータが収集されます。空の文字列 "" を指定すると、集計データのみが収集されます。"DISKFILE" のような固有の文字列では、そのインスタンスのみのデータが収集されます。省略した場合のデフォルト値は、 "*" です。

表 11-15. メトリック収集パラメータ（続き）

パラメータ名	値	説明
minReportingInterval	秒を示す整数。	時系列データのレポートに使用する、デフォルトの集計間隔（秒）を指定します。収集間隔の頻度が不十分である場合に、レポートの頻度を調整できます。デフォルトは 0 です（レポート用の間隔は指定しない）。
aggregator	AVERAGE、MINIMUM、MAXIMUM、SUMMATION のいずれか	minReportingInterval の間に実行される集計のタイプです。省略した場合のデフォルト値は、AVERAGE です。

Cassandra メトリック データベースの構成

セルをオプションのメトリック データベースに接続するには、セル管理ツールの `cassandra` コマンドを使用します。

vCloud Director は、仮想マシンのパフォーマンスおよびリソース消費に関する現在および過去の情報を提供するメトリックを収集できます。このサブコマンドを使用して、vCloud Director メトリック リポジトリとして使用するための Apache Cassandra データベースを設定します。 `cell-management-tool configure-metrics` サブコマンドを使用して、収集するメトリックのセットを設定します。 [メトリック収集の設定](#)を参照してください。

履歴メトリックのデータは、Apache Cassandra データベースに格納されます。オプションのデータベース ソフトウェアを設定して、パフォーマンス メトリックを格納および取得する方法の詳細については、『vCloud 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。

vCloud Director と Apache Cassandra データベース間の接続を作成するには、次の形式でコマンド ラインを使用します。

```
cell-management-tool cassandra options
```

表 11-16. セル管理ツールのオプションと引数、cassandra サブコマンド

コマンド	引数	説明
<code>--help (-h)</code>	なし	このコマンドで使用可能なオプションの概要を示します。
<code>--add-rollup</code>	なし	メトリック スキーマを更新し、集計メトリックを含めます。『vCloud Director インストール、構成、およびアップグレード ガイド』の「過去の仮想マシン パフォーマンス メトリックを格納および取得するためのオプション データベース ソフトウェアのインストールと構成」を参照してください。
<code>--cluster-nodes</code>	<i>address</i> [, <i>address</i> ...]	vCloud Director メトリックで使用する Cassandra クラスター ノードのカンマ区切りのリストです。
<code>--clean</code>	なし	Cassandra 設定を vCloud Director データベースから削除します。

表 11-16. セル管理ツールのオプションと引数、cassandra サブコマンド（続き）

コマンド	引数	説明
--configure	なし	既存の Cassandra クラスタで使用する vCloud Director を構成します。
--dump	なし	現在の接続の設定をダンプします。
--keyspace	文字列	Cassandra の vCloud Director キースペース名を <i>string</i> に設定します。デフォルトでは <code>vcloud_metrics</code> です。
--offline	なし	vCloud Director で使用するために Cassandra を設定しますが、vCloud Director に接続して設定をテストすることはありません。
--password	文字列	Cassandra データベース ユーザーのパスワード
--port	整数	各クラスタ ノードに接続するためのポート。デフォルトでは 9042 です。
--ttl	整数	<i>integer</i> 日間、メトリック データを保持します。メトリック データを永続的に保持するには、 <i>integer</i> を 0 に設定します。
--update-schema	なし	vCloud Director メトリック データを保持するため、Cassandra スキーマを初期化します。
--username	文字列	Cassandra データベース ユーザーのユーザー名。

例：Cassandra データベース接続の設定

次のようなコマンドを使用します。ここで、*node1-ip*、*node2-ip*、*node3-ip* および *node4-ip* は Cassandra クラスタのメンバーの IP アドレスです。デフォルトのポート (9042) が使用されます。メトリック データは 15 日間保持されます。

```
[root@cell11 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool cassandra --configure --create-schema \ --cluster-nodes node1-
ip,node2-ip,node3-ip, node4-ip \ --username admin --password 'P@55w0rd' --ttl 15
```

このコマンドが完了した後、セルを再起動する必要があります。

システム管理者のパスワードの復元

vCloud Director データベースのユーザー名とパスワードが分かっている場合は、セル管理ツールの `recover-password` コマンドを使用して、vCloud Director システム管理者のパスワードを復元できます。

セル管理ツールの `recover-password` コマンドでは、vCloud Director データベースのユーザー名とパスワードを知っているユーザーが、vCloud Director システム管理者のパスワードを復元できます。

システム管理者のパスワードを復元するには、次の形式でコマンドラインを使用します。

```
cell-management-tool recover-password options
```

表 11-17. セル管理ツールのオプションと引数、recover-password サブコマンド

オプション	引数	説明
--help (-h)	なし	このカテゴリで使用可能なコマンドの概要を示します。
--dbuser	vCloud Director データベース ユーザーのユーザー名。	コマンドラインで指定する必要があります。
--dbpassword	vCloud Director データベース ユーザーのパスワード。	指定しない場合に入力が求められます。

タスクの失敗ステータスの更新

セルが意図的にシャットダウンされたときに実行していたタスクに関連する完了ステータスを更新するには、セル管理ツールの `fail-tasks` コマンドを使用します。すべてのセルをシャットダウンしない限り、`fail-tasks` コマンドを使用することはできません。

`cell-management-tool -q` コマンドを使用してセルを静止すると、実行中のタスクは数分以内に安全に終了します。休止したセルでタスクが実行し続ける場合、スーパーユーザーはセルをシャットダウンすることができ、その結果実行しているタスクは失敗します。シャットダウンにより実行中のタスクが失敗した後、スーパーユーザーは `cell-management-tool fail-tasks` を実行してそれらのタスクの完了ステータスを更新することができます。これはタスクの完了ステータスを更新するオプションの方法ですが、管理アクションによって発生した失敗を明確に特定できるため、システムの整合性を維持するのに役立ちます。

休止したセルで実行し続けるタスクのリストを生成するには、次の形式でコマンドラインを使用します。

```
cell-management-tool -u sysadmin-username cell --status-verbose
```

表 11-18. セル管理ツールのオプションと引数、fail-tasks サブコマンド

コマンド	引数	説明
--help (-h)	なし	このカテゴリで使用可能なコマンドの概要を示します。
--message (-m)	メッセージ テキスト。	タスク完了ステータスに含めるメッセージ テキスト。

例：セルで実行中のタスクの終了

この例では、セルがシャットダウンされた時に実行していたタスクに関連するタスク完了ステータスを更新します。

```
[root@cell11 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool fail-tasks -m "administrative shutdown"
Operation: IMPORT_SINGLETON_VAPP, Start time: 12/16/13 6:41 PM, Username: system,
Organization: org1
Would you like to fail the tasks listed above?
```

「y」を入力すると、タスクが更新され、**管理シャットダウン**のステータスが完了になります。「n」と入力すると、タスクの実行を継続できます。

注： 応答内で複数のタスクが返された場合は、すべてのタスクを終了させるのか、それとも何も行わないのかを決定する必要があります。タスクの一部を選択して終了させることはできません。

監査メッセージ処理の構成

システムが監査メッセージをログに記録する方法を構成するには、セル管理ツールの `configure-audit-syslog` コマンドを使用します。

各 vCloud Director セル内のサービスは、監査メッセージを vCloud Director データベースにログとして記録し、メッセージは 90 日間保存されます。監査メッセージの保存期間を長くするには、監査メッセージを vCloud Director データベースだけでなく Linux syslog ユーティリティに送信するように vCloud Director サービスを構成します。

システム構成スクリプトでは、監査メッセージの処理方法を指定できます。『vCloud Director インストールおよびアップグレード ガイド』の「ネットワークおよびデータベース接続の構成」を参照してください。システム構成時に指定したログ記録のオプションは、2 つのファイル `global.properties` および `responses.properties` に保存されます。この 2 つのファイルに保存された監査メッセージのログ記録構成を変更するには、次の形式のセル管理ツールコマンド ラインを使用します。

```
cell-management-toolconfigure-audit-syslog options
```

このセル管理ツール サブコマンドで実行した変更はすべて、セルの `global.properties` ファイルおよび `responses.properties` ファイルに保存されます。変更内容はセルの再起動後に有効になります。

表 11-19. セル管理ツールのオプションと引数、`configure-audit-syslog` サブコマンド

オプション	引数	説明
<code>--help (-h)</code>	なし	このカテゴリで使用可能なコマンドの概要を示します。
<code>--disable (-d)</code>	なし	syslog に対する監査イベントのログ記録を無効にします。監査イベントを vCloud Director データベースにのみログ記録します。このオプションを指定すると、 <code>global.properties</code> および <code>responses.properties</code> の <code>audit.syslog.host</code> および <code>audit.syslog.port</code> プロパティの値が設定解除されます。
<code>--syslog-host (-loghost)</code>	syslog サーバ ホストの IP アドレスまたは完全修飾ドメイン名	このオプションを指定すると、 <code>audit.syslog.host</code> プロパティの値が、指定したアドレスまたは完全修飾ドメイン名に設定されます。
<code>--syslog-port (-logport)</code>	0~65535 の整数	このオプションを指定すると、 <code>audit.syslog.port</code> プロパティの値が、指定した整数に設定されます。

--syslog-host、--syslog-port、またはその両方の値を指定した場合、コマンドでは指定した値の形式が正しいかどうかは検証されますが、指定したホストとポートの組み合わせでネットワークにアクセスできるかどうか、または実行中の syslog サービスが存在するかどうかは確認されません。

例：syslog サーバのホスト名を変更する

重要： このコマンドを使用して実行した変更は、グローバル構成ファイルと応答ファイルに書き込まれます。このコマンドを使用する前に、応答ファイルが所定の場所 (/opt/vmware/vcloud-director/etc/responses.properties) にあって書き込み可能であることを確認してください。『vCloud Director インストールおよびアップグレード ガイド』の「応答ファイルの保護と再使用」を参照してください。

syslog メッセージの送信先ホストを変更するには、次のようなコマンドを使用します。

```
[root@cell11 /opt/vmware/vcloud-director/bin]#
cell-management-tool configure-audit-syslog -loghost syslog.example.com
Using default port 514
```

この例では、新しいホストがデフォルトのポートで syslog メッセージを待機しているものと仮定しています。

このコマンドを実行すると、global.properties および responses.properties が更新されますが、変更内容はセルの再起動後に有効になります。

電子メール テンプレートの構成

電子メール アラートを作成する際にシステムが使用するテンプレートを管理するには、セル管理ツールの manage-email コマンドを使用します。

システムは、システム管理者の介入を必要とする可能性が高いイベントや条件をシステム管理者に通知する電子メール アラートを送信するようにデフォルトで構成されています。電子メールの受信者リストは、vCloud API または Web コンソールを使用して更新できます。次の形式のセル管理ツール コマンド ラインを使用して、各種アラートのデフォルトの電子メールの内容をオーバーライドできます。

```
cell-management-tool manage-email options
```

表 11-20. セル管理ツールのオプションと引数、manage-email サブコマンド

オプション	引数	説明
--help	なし	このカテゴリで使用可能なコマンドの概要を示します。
--delete	テンプレート名	削除するテンプレートの名前。
--lookup	テンプレート名	この引数は省略可能です。この引数を省略すると、すべてのテンプレート名の一覧が返されます。

表 11-20. セル管理ツールのオプションと引数、manage-email サブコマンド（続き）

オプション	引数	説明
--locale	テンプレート ロケール	デフォルトでは、en-US ロケールのテンプレートが操作対象になります。en-US 以外のロケールを指定する場合は、このオプションを使用します。
--set-template	更新された電子メール テンプレートの格納先ファイルのパス名	このファイルは、ローカル ホストでアクセス可能であり、なおかつユーザー vcloud.vcloud によって読み取り可能である必要があります。例：/tmp/my-email-template.txt

例： メール テンプレートを更新する

次のコマンドでは、DISK_STORAGE_ALERT_VDCS 電子メール テンプレートの現在の内容を、/tmp/DISK_STORAGE_ALERT_VDCS-new.txt という名前のファイルに作成した内容で置き換えています。

```
[root@cell11 /opt/vmware/vcloud-director/
bin]#./cell-management-tool manage-email --set-template DISK_STORAGE_ALERT_VDCS /tmp/
DISK_STORAGE_ALERT_VDCS-new.txt

New property being stored: Property "email.template.DISK_STORAGE_ALERT_VDCS.en-US" has value
"This is an alert from $productName The $datastore is used by the following PVDC(s):
$pvdcList
"
Property "email.template.DISK_STORAGE_ALERT_VDCS.en-US" has value "This is an alert from
$productName The $datastore is used by the followingProvider VDC(s): $pvdcList
"

VCD Email notification details:
name                : DISK_STORAGE_ALERT_VDCS
description         : Alert when used disk storage exceeds threshold
config key          : email.template.DISK_STORAGE_ALERT_VDCS.en-US
template placeholders : [productName, storageContainerType, datastore, percentage,
currentFreeSpaceMB, diskSizeBytes, pvdcList]
template content    : This is an alert from $productName The $datastore is used by the
followingProvider VDC(s): $pvdcList
```

親なしの仮想マシンの検索

セル管理ツールの find-orphan-vmns コマンドを使用すると、vCenter データベースには存在するが vCloud Director データベースには存在しない仮想マシンへの参照を検索できます。

vCenter データベースでは参照されているが、vCloud Director データベースでは参照されていない仮想マシンは、コンピューティング リソースおよびストレージ リソースを使用するものの vCloud Director からアクセスできないため、親なしの仮想マシンと見なされます。このような参照の不一致は、高負荷のワークロード、多数のデータベース エラーや管理アクションなど、さまざまな原因で発生します。find-orphan-vmns コマンドを使用すると、

こうした親なしの仮想マシンを一覧表示して、vCloud Director から削除したり、vCloud Director に再インポートしたりできます。このコマンドには、別のトラスト ストアを指定するためのオプションが用意されています。このオプションは、自己署名証明書を使用している vCloud Director または vCenter インストール環境で作業する場合に必要なことがあります。

コマンドの形式は次のとおりです。

```
cell-management-tool find-orphan-vmsoptions
```

表 11-21. セル管理ツールのオプションと引数、find-orphan-vmsoptions サブコマンド

オプション	引数	説明
--help (-h)	なし	このカテゴリで使用可能なコマンドの概要を示します。
--enableVerifyHostname	なし	SSL ハンドシェイクのホスト名検証部分を有効にします。
--host	必須	親なしの仮想マシンの検索対象となる vCloud Director インストール先の IP アドレスまたは完全修飾ドメイン名。
--output-file	パス名または -	親なしの仮想マシンのリストの出力先となるファイルのフル パス名。リストを標準出力に書き込む場合は、パス名に - を指定します。
--password (-p)	必須	vCloud Director システム管理者のパスワード。
--port	vCloud Director の HTTPS ポート。	このオプションは、デフォルトの vCloud Director HTTPS ポートを使用しない場合のみ指定します。
--trustStore	Java トラスト ストア ファイルへのフル パス名。	このオプションは、デフォルトの vCloud Director トラスト ストア ファイルを使用しない場合のみ指定します。
--trustStorePassword	指定した --trustStore のパスワード	--trustStore を使用して別のトラスト ストア ファイルを指定した場合のみ必要です。
--trustStoreType	指定した --trustStore のタイプ (PKCS12、JCEKS など)	--trustStore を使用して別のトラスト ストア ファイルを指定した場合のみ必要です。
--user (-u)	必須	vCloud Director システム管理者のユーザー名。
--vc-name	必須	親なしの仮想マシンの検索対象 vCenter の名前。
--vc-password	必須	vCenter 管理者のパスワード。
--vc-user	必須	vCenter 管理者のユーザー名。

例：親なしの仮想マシンの検索

この例では、単一の vCenter Server にクエリを発行しています。--output-file オプションに - が指定されているため、クエリ結果は標準出力に返されます。

```
[root@cell11 /opt/vmware/vcloud-director/bin]# ./cell-management-tool find-orphan-vm \
--host 10.20.30.40 -u vcadmin -vc-name vcenter1 -vc-password P@55w0rd --vc-user admin --
output-file -
Querying for VC by name 10.20.30.40
Querying all vdc's associated with VC: 10.20.30.40 (https://10.20.30.40:443)
Querying all vdc<->resource pool mappings associated with VC: 10.20.30.40 (https://
10.20.30.40:443)
Querying all vdc<->VM Moref mappings associated with VC: 10.20.30.40 (https://10.20.30.40:443)
Processing 956 VM's on 5 VDC's across 20 resource pools
Analysis complete.
VDC: "ExampleOrgVDC [urn:vcloud:vdc:1a97...]" (org: "ExampleOrg") ResPool: primary (1a97...)
[moref: "resgroup-30515"]
The following 22 orphan VMs were discovered:
Orphan VM: "indDisk100-0-95411 (cbc358a0-e199-4024-8fff-2e5cfce20953)" (parent name: "Test
VMs", parent moref : "group-v30533")
...
Orphan VM: "indDisk12-0-51259 (0bbb4115-673e-4c84-ba26-6875159655e0)" (parent name: "Test
VMs", parent moref : "group-v30533")
```

VMware カスタマ エクスペリエンス改善プログラムへの参加または離脱

VMware カスタマ エクスペリエンス改善プログラムに参加または離脱するには、セル管理ツールの `configure-ceip` サブコマンドを使用します。

この製品は、VMware のカスタマ エクスペリエンス改善プログラム（「CEIP」）に参加しています。CEIP を通じて収集されるデータについての詳細と、VMware がこの情報を使用する目的は、Trust & Assurance Center (<http://www.vmware.com/trustvmware/ceip.html>) で説明されています。セル管理ツールを使用して、この製品の VMware CEIP への参加または離脱をいつでも実行できます。

```
cell-management-tool
configure-ceip
options
```

この製品の CEIP に参加しない場合は、--disable オプションを指定してこのコマンドを実行します。

表 11-22. セル管理ツールのオプションと引数、configure-ceip サブコマンド

オプション	引数	説明
--help (-h)	なし	このカテゴリで使用可能なコマンドの概要を示します。
--disable	なし	VMware カスタマ エクスペリエンス改善プログラムから離脱します。
--enable	なし	VMware カスタマ エクスペリエンス改善プログラムに参加します。
--status	なし	VMware カスタマ エクスペリエンス改善プログラムに対する現在の参加ステータスを表示します。

例： VMware カスタマ エクスペリエンス改善プログラムから離脱します。

VMware カスタマ エクスペリエンス改善プログラムから離脱するには、次のようなコマンドを使用します。

```
[root@cell11 /opt/vmware/vcloud-director/
bin]#cell-management-tool configure-ceip --disableParticipation disabled
```

このコマンドを実行すると、VMware カスタマ エクスペリエンス改善プログラムに対して情報が送信されなくなります。

VMware カスタマ エクスペリエンス改善プログラムに対する現在の参加ステータスを確認するには、次のようなコマンドを使用します。

```
[root@cell11 /opt/vmware/vcloud-director/
bin]#cell-management-tool configure-ceip --statusParticipation disabled
```

アプリケーションの設定の更新

セル管理ツールの manage-config サブコマンドを使用すると、カタログ スロットリング アクティビティなどのさまざまなアプリケーションの構成を更新できます。

表 11-23. セル管理ツールのオプションと引数、manage-config サブコマンド

オプション	引数	説明
--help(-h)	なし	このサブコマンドで使用可能なオプションの概要を示します。
--delete(-d)	なし	ターゲットの設定を削除します。
--lookup(-l)	なし	ターゲットの設定の値を検索します。
--name(-n)	設定名	ターゲットの設定の名前。 オプション -d、-l、および -v が必要です。
--value(-v)	設定値	ターゲットの設定の値を追加または更新します。

たとえば、[カタログ同期のスロットリングの設定](#)には `manage-config` サブコマンドを使用できます。

カタログ同期のスロットリングの設定

他の組織に公開された、または他の組織からサブスクライブされたカタログ項目が多数ある場合、カタログの同期中にシステムが過負荷にならないように、カタログ同期のスロットリングを設定できます。セル管理ツールの `manage-config` サブコマンドを使用すると、同時に同期できるライブラリ項目の数を制限することで、カタログ同期のスロットリングを設定できます。

サブスクライブされたカタログがカタログ同期を開始すると、公開されたカタログは最初にライブラリ項目を vCenter Server リポジトリから vCloud Director 転送サービス ストレージにダウンロードしてから、サブスクライブされたカタログのダウンロード リンクを作成します。公開されたすべてのカタログが同時にダウンロードできるライブラリ項目の数を制限できます。サブスクライブされたすべてのカタログが同時に同期できるライブラリ項目の数を制限できます。サブスクライブされた単一のカタログが同時に同期できるライブラリ項目の数を制限できません。

セル管理ツールの `manage-config` サブコマンドを使用すると、カタログ スロットリングの設定を更新できます。`manage-config` サブコマンドの使用方法については、[アプリケーションの設定の更新](#) を参照してください。

表 11-24. カタログ スロットリングの設定

設定	デフォルト値	説明
<code>vcloud.tasks.VDC_ENABLE_DOWNLOAD.queue.limit</code>	30	vCloud Director インスタンス内で公開されたすべてのカタログが vCenter Server から vCloud Director に同時にダウンロードできるライブラリ項目の制限値。 vCloud Director インスタンスをまたがってダウンロードする公開されたライブラリ項目の合計数がこの制限値を超えると、ライブラリ項目はこの制限値によって分割され、順番にダウンロードされます。
<code>vcloud.tasks.LIBRARY_ITEM_SYNC.queue.limit</code>	30	vCloud Director インスタンス内のサブスクライブされたすべてのカタログが同時に同期できるライブラリ項目の制限値。 vCloud Director インスタンスをまたがって同期するサブスクライブされたライブラリ項目の合計数がこの制限値を超えると、項目はこの制限値によって分割され、順番に同期されます。
<code>contentLibrary.item.sync.batch.size</code>	10	サブスクライブされた単一のカタログが同時に同期できるライブラリ項目の制限値。 サブスクライブされたカタログがこの制限値を超える数のライブラリ項目を同期すると、項目はこの制限値によって分割され、順番に同期されます。

例：サブスクライブされたカタログの同期のスロットリングの設定

次のコマンドは、サブスクライブされた単一のカタログが同時に同期できるライブラリ項目の制限値を 5 に設定します。

```
[root@cell11 /opt/vmware/vcloud-director/
bin]#./cell-management-tool manage-config -n contentLibrary.item.sync.batch.size -v 5
```

サブスクライブされたカタログに 13 個のライブラリ項目が含まれている場合は、カタログの同期は 3 回に分かれて順次実行されます。最初には 5 個の項目が含まれ、2 番目の部分には次の 5 個の項目が含まれ、最後に残りの 3 個の項目が含まれます。

vCenterServer 仮想マシン検出のデバッグ

セル管理ツールの debug-auto-import サブコマンドを使用すると、vApp の検出メカニズムが vCenter Server 仮想マシンを 1 台以上スキップする原因を調査できます。

デフォルト構成の場合、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リソース プールで作成される vCenterServer 仮想マシンを自動的に検出します。[vApp の検出および採用](#)を参照してください。検出された vApp に vCenterServer 仮想マシンが表示されない場合は、この仮想マシンまたは仮想データセンターに対して debug-auto-import サブコマンドを実行できます。

```
cell-management-tool
debug-auto-import
options
```

debug-auto-import サブコマンドは、検出メカニズムがスキップした vCenter Server 仮想マシンのリスト、およびその潜在的な原因に関する情報を返します。このリストには、メカニズムで検出されたものの、組織仮想データセンターへのインポートに失敗した vCenterServer 仮想マシンも含まれます。

表 11-25. セル管理ツールのオプションと引数、debug-auto-import サブコマンド

オプション	引数	説明
--help (-h)	なし	このカテゴリで使用可能なコマンドの概要を示します。
--org	組織名	オプション。指定した組織について、スキップされた仮想マシンに関する情報を一覧表示します。
--vm	仮想マシン名または仮想マシン名の一部	指定した仮想マシン名が含まれる、スキップされた仮想マシンに関する情報を一覧表示します。 --org オプションが使用されている場合は、オプションです。

例：仮想マシン名 test による vCenter Server 仮想マシン検出のデバッグ

以下のコマンドを実行すると、すべての組織においてスキップされた vCenterServer 仮想マシンに関する情報が返されます。

```
[root@cell11 /opt/vmware/vcloud-director/bin]#./cell-management-tool debug-auto-import -vm test
```

```
VM with name:vm22-test (09ad258c-0cb0-4f69-a0a6-201cf3fe7d6b), moref vm-50 in VC testbed-vc
can be skipped for the following reasons:
```

- 1) Virtual machine is already imported in vCD or is managed by vCD
- 2) Virtual machine is created by vCD

```
VM with name:test-vm1 (32210d0d-ef64-4637-b1d6-6400743a6bd9), moref vm-44 in VC testbed-vc
can be skipped for the following reasons:
```

- 1) Virtual machine is not present in a vCD managed resource pool

```
VM with name:import-test3, moref vm-52inVC testbed-vc can be skippedforthe following reasons:
```

- 1) Virtual machine autoimport is either pending,in-progress or has failed and pendingforretry

この例では、検出メカニズムでスキップされた仮想マシンで、仮想マシン名に test という文字列が含まれる 3 台の vCenter Server 仮想マシンに関する情報がシステムのアウプットで返されます。仮想マシン import-test3 は、検出されたものの仮想データセンターへのインポートが失敗した仮想マシンの例です。

マルチサイト拡張ネットワークの MAC アドレスの再生成

同じインストール ID で構成されている 2 つの vCloud Director サイトを関連付けると、これらのサイト間の拡張ネットワークで MAC アドレスの競合が発生する可能性があります。このような競合を回避するには、インストール ID とは異なるカスタム シードに基づいて、いずれかのサイトで MAC アドレスを再生成する必要があります。

vCloud Director の初期セットアップ中に、インストール ID を設定します。vCloud Director はインストール ID を使用して、仮想マシン ネットワーク インターフェイスの MAC アドレスを生成します。同じインストール ID で構成されている 2 つの vCloud Director インストールでは、同じ MAC アドレスが生成されることがあります。MAC アドレスが重複すると、関連付けられた 2 つのサイト間の拡張ネットワークで競合が発生する可能性があります。

同じインストール ID で構成されている、関連付けられたサイト間で拡張ネットワークを作成する前に、セル管理ツールの mac-address-management サブコマンドを使用して、いずれかのサイトで MAC アドレスを再生成する必要があります。

```
cell-management-tool
mac-address-management
options
```

新しい MAC アドレスを生成するには、インストール ID とは異なるカスタム シードを設定します。シードはインストール ID を上書きしませんが、データベースには 2 番目の構成パラメータとして最新のシードが保存され、インストール ID がオーバーライドされます。

mac-address-management サブコマンドは、サーバ グループの任意の vCloud Director メンバーから実行します。このコマンドは vCloud Director データベースに対して実行されるため、1 つのサーバ グループに対して 1 回コマンドを実行します。

重要： MAC アドレスの再生成には、vCloud Director の一定のダウンタイムが必要です。再生成を開始する前に、サーバ グループ内のすべてのセルのアクティビティを休止する必要があります。

表 11-26. セル管理ツールのオプションと引数、mac-address-management サブコマンド

オプション	引数	説明
--help (-h)	なし	このカテゴリで使用可能なコマンドの概要を示します。
--regenerate	なし	使用されていないすべての MAC アドレスを削除し、現在のシードに基づいて新しい MAC アドレスを生成します。これまでシードを設定したことがない場合は、MAC アドレスはインストール ID に基づいて再生成されます。使用中の MAC アドレスは保持されます。 注： サーバ グループ内のすべてのセルは非アクティブである必要があります。セル上のアクティビティを休止する方法については、 セルの管理 を参照してください。
--regenerate-with-seed	0 ～ 63 のシード番号	データベースに新しいカスタム シードを設定し、使用されていないすべての MAC アドレスを削除して、新しく設定したシードに基づいて新しい MAC アドレスを生成します。使用中の MAC アドレスは保持されます。 注： サーバ グループ内のすべてのセルは非アクティブである必要があります。セル上のアクティビティを休止する方法については、 セルの管理 を参照してください。
--show-seed	なし	現在のシードと各シードに使用されている MAC アドレスの数を返します。

重要： 使用中の MAC アドレスは保持されます。使用中の MAC アドレスを再生成された MAC アドレスに変更するには、ネットワーク インターフェイスの MAC アドレスをリセットする必要があります。仮想マシンのプロパティの編集については、『vCloud Director Tenant Portal Guide』を参照してください。

例：新しいカスタム シードに基づく MAC アドレスの再生成

次のコマンドを実行すると、現在のシードを 9 に設定し、新しく設定したシードに基づいて、使用されていないすべての MAC アドレスを再生成します。

```
[root@cell11 /opt/vmware/vcloud-director/bin]# ./cell-management-tool --regenerate-with-seed 9
Successfully removed 65,535 unused MAC addresses. Successfully generated new MAC addresses.
```

例：現在のシードと各シードに使用されている MAC アドレスの数の表示

次のコマンドを実行すると、現在のシードと各シードの MAC アドレスの数に関する情報を返します。

```
[root@cell11 /opt/vmware/vcloud-director/bin]# ./cell-management-tool --show-seed
Current MAC address seed is '9' and based on MacAddressSeed config. MAC address seed 9 is in use by 12 MAC addresses
MAC address seed 1 is in use by 1 MAC addresses
```

この例では、現在のシードが 9 であり、12 個の MAC アドレスで使用されていることがシステム出力に示されています。また、1 つ前のシードまたはインストール ID に基づく MAC アドレスが 1 つあることも示されています。

vCloud Director セルのデータベース IP アドレスの更新

セル管理ツールを使用して、データベース高可用性クラスタ内の vCloud Director セルの IP アドレスを更新できます。

前提条件

データベース高可用性クラスタ内のセルの IP アドレスを更新するには、現在のプライマリの IP アドレスを指定する必要があります。IP アドレスを見つけるには、クラスタのステータスを確認して、プライマリ ロールを持つノードを特定します。ノードが実行されている必要があります。この行の `Connection string` 列のホスト値を使用して IP アドレスを特定します。[データベース高可用性クラスタのステータスの確認](#)を参照してください。

手順

- 1 クラスタ内のいずれかのセルの OS に、**root** としてログインするか、SSH で接続します。
- 2 セルがそのノードで実行されているかどうかを確認します。

```
service vmware-vcd pid cell
```

セルのプロセス ID が NULL でない場合は、vCloud Director セルは実行されており、vCloud Director セルを再起動せずにデータベースの IP アドレスを変更できます。

- 3 サーバ グループ内のすべてのセルの IP アドレスを更新するには、次のコマンドを実行します。

```
/opt/vmware/vcloud-director/bin/cell-management-tool reconfigure-database --database-host
primary node IP address --pid cell process ID --remote-sudo-user postgres --private-key-
path /opt/vmware/vcloud-director/id_rsa
```

システム出力は、再設定が成功したことを示します。

- 4 (オプション) 各 vCloud Director セルが正しいデータベース IP アドレスを参照しているかどうかを確認します。

```
grep "database.jdbcUrl" /opt/vmware/vcloud-director/etc/global.properties
```

システム出力は、セルが更新されたことを示します。

- 5 いずれかのセルが更新されていない場合は、次のコマンドを実行して再設定します。

- セルが実行されていない場合は、次のコマンドを実行します。

```
/opt/vmware/vcloud-director/bin/cell-management-tool reconfigure-database --database-host primary node IP address
```

- セルが実行されている場合は、次のコマンドを実行します。

```
/opt/vmware/vcloud-director/bin/cell-management-tool reconfigure-database --database-host primary node IP address -i cell process ID
```

- 6 実行されていないセルを再設定した場合は、次のコマンドを実行して vCloud Director を再起動します。

```
service vmware-vcd restart
```