vCloud Director Service Provider Admin Portal ガイド

2019 年 3 月 28 日

VMware Cloud Director 9.7

vmware®

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

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

目次

vCloud Director Service Provider Admin Portal について

1

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

対象読者

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

関連ドキュメント

組織管理者が vCloud Directorservice provider admin portal の代わりに vCloud Director Web コンソールを使用して利用できる機能については、『vCloud Director 管理者ガイド』を参照してください。

VMware の技術ドキュメントの用語集

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

更新情報

『vCloud Director Service Provider Admin Portal Guide』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 Service Provider Admin Portal Guide』の更新履歴については、次の表をご確認ください。

リビジョン	説明
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 Service Provider Admin Portal の概要

2

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

この章には、次のトピックが含まれています。

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キングされます。

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キングされ、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キングされ、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キングされます。

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キングされます。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 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。

vCloud Director Service Provider Admin Portal へのログイン

Web ブラウザを使用して vCloud DirectorService Provider Admin Portal にアクセスできます。

前提条件

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

手順

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

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

2 システム管理者のユーザー名とパスワードを使用してログインします。

タスクの表示

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

タスク ビューは、サービス プロバイダ管理者ポータル内のタスクのステータスを一目で把握するのに適した方法です。タスク ビューには、タスクが実行された日時と、そのタスクが成功したかどうかが表示されます。このツールは、環境内で発生する問題のトラブルシューティングを行う場合に、最初のステップとして利用できます。

[タスク] アイコン上の青色および赤色のヒント情報は、それぞれ実行したタスクと失敗したタスクの数を示しています。

手順

- 右上のメニューから [タスク] アイコン () を選択します。

結果

最近のタスクのリストが、タスクが実行された時刻およびタスクのステータスと共に表示されます。

進行中のタスクの停止

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

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

前提条件

[最近のタスク] パネルが開いている必要があります。

手順

1 長時間の処理を開始します。

  長時間の処理とは、仮想マシンまたは vApp の作成、仮想マシンや vApp に対して実行される電源操作などの処理です。

2 [最近のタスク] パネルで、[キャンセル] アイコン（  ）をクリックします。

3 [タスクのキャンセル] ダイアログ ボックスで [OK] をクリックして、タスクをキャンセルすることを確認します。

結果

処理が停止します。

イベントの表示

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

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

手順

1 メイン メニュー (☰) から、[イベント] を選択します。

すべてのイベントのリストが、イベントの発生した日時およびイベントのステータスと共に表示されます。

2 イベントについて表示する詳細を変更するには、エディタ アイコン（  ）をクリックします。

3 （オプション） イベントをクリックして、イベントの詳細を表示します。

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

vSphere リソースの管理

3

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キングします。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キング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、vCloud Director 管理者ガイド』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、9 章 SDDC および SDDC プロキシの管理を参照してください。

注： デフォルトでは、vCenter Server インスタンスが接続されている場合、プロバイダ仮想データセンターまたは 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キング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 の両方をバッキングできるように、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 インスタンスの再接続
- vCenter Server インスタンスの更新
- vCenter Server インスタンスのストレージ ポリシーの更新
- vCenter Server インスタンスの登録解除
- NSX Manager 設定の変更
- NSX-T Manager 設定の変更
- NSX-T Manger インスタンスの削除
- マルチサイト リソース リスト

vCenter Server および NSX リソースの追加

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

vCenter Server インスタンスを接続して、そのリソースが vCloud Director で使用可能になるようにします。vCenter Server インスタンスを関連付けられた NSX Manager インスタンスと共に接続することも、vCenter Server インスタンスを単独で接続することもできます。

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

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

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

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

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

前提条件

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

手順

1 vCenter Server インスタンスの追加

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

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

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

vCenter Server インスタンスの追加

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

手順

1 メイン メニュー (☰) から、[vSphere リソース] を選択します。

2 左側のペインで、[vCenter] をクリックし、[追加] をクリックします。

3 マルチサイト vCloud Director デプロイを使用している場合は、[サイト] ドロップダウン メニューから、この vCenter Server インスタンスを追加するサイトを選択し、[次へ] をクリックします。

4 vCloud Director の vCenter Server インスタンスの名前と、オプションで説明を入力します。

5 vCenter Server インスタンスの URL を入力します。

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

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

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

7 （オプション） 登録後に vCenter Server インスタンスを無効にするには、[有効] 切り替えを無効にします。

8 vCenter Server Web Client の URL を設定します。

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

9 [次へ] をクリックします。

10 （オプション） vCenter Server インスタンスに関連付けられている NSX Manager インスタンスの追加をスキップし、登録を完了します。

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

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

a [NSX-V Manager の設定] 画面で、[設定] 切り替えを無効にして、[次へ] をクリックします。

b [設定内容の確認] 画面で詳細を確認し、[完了] をクリックします。

（オプション）関連付けられた NSX Manager インスタンスの追加

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

手順

1 [NSX-V Manager の設定] 画面で、[設定] 切り替えを有効のままにします。

2 NSX Manager インスタンスの URL を入力します。

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

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

3 NSX 管理者アカウントのユーザー名とパスワードを入力します。

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

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

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

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

5 [設定内容の確認] 画面で詳細を確認し、[完了] をクリックします。

次のステップ

- vCenter Server Server で NSX ライセンス キーを割り当てる。
- プロバイダ仮想データセンターの作成に関する詳細については、『vCloud Director 管理者ガイド』を参照してください。

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

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

前提条件

この操作は、システム管理者に制限されます。

手順

1 vCenter Server システムに接続された vSphere Client ホストから、[ホーム] - [ライセンス] の順に選択します。

2 レポート ビューの場合、[資産] を選択します。

3 NSX Manager 資産を右クリックし、[ライセンス キーを変更] を選択します。

4 [このホストに新しいライセンス キーを割り当て] を選択し、[キーを入力] をクリックします。

5 ライセンス キーを入力し、キーの任意のラベルを入力して、[OK] をクリックします。

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 インスタンスで使用できます。

6 [OK] をクリックします。

NSX-T Manager インスタンスの登録

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

手順

1 メイン メニュー (☰) から、[vSphere リソース] を選択します。

2 左側のペインで、[NSX-T Manager] をクリックし、[追加] をクリックします。

3 マルチサイト vCloud Director デプロイを使用している場合は、[サイト] ドロップダウン メニューから、この NSX-T Manager インスタンスを追加するサイトを選択し、[次へ] をクリックします。

4 vCloud Director の NSX-T Manager インスタンスの名前と、オプションで説明を入力します。

5 NSX-T Manager インスタンスの URL を入力します。

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

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

7 [保存] をクリックします。

次のステップ

NSX-T Data Center によってバッキングされるプロバイダ仮想データセンターの作成に関する詳細については、https://code.vmware.com の『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。

vCenter Server インスタンスの表示

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

手順

1 メイン メニュー (☰) から、[vSphere リソース] を選択します。

2 左側のパネルで [vCenter] をクリックします。

結果

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

	説明
[名前]	vCloud Director 内の vCenter Server インスタンスの名前。
[状態]	有効または無効。vCenter Server インスタンスの有効化または無効化を参照してください。
[接続]	vCloud Director に接続されているかどうか。vCenter Server インスタンスの再接続を参照してください。
[VC ホスト]	vCenter Server インスタンスの FQDN。
[バージョン]	vCenter Server のバージョン。
[サービス プロバイダ]	仮想データセンターで使用できるように公開されているかどうか。

	説明
[テナント]	Software-Defined Data Center (SDDC) として使用できるように公開されているかどうか。
[サイト]	vCenter Server インスタンスが属するサイトの vCloud Director FQDN。

vCenter Server 設定の変更

接続済み vCenter Server インスタンスの接続情報が変更された場合や、vCloud Director での名前と説明を変更する場合は、その設定を変更できます。

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

手順

1 メイン メニュー (☰) から、[vSphere リソース] を選択します。

2 左側のペインで [vCenter] をクリックし、変更する vCenter Server インスタンスの名前をクリックします。

3 [vCenter Server 情報] セクションの右上隅にある [編集] をクリックします。

4 vCenter Server 設定を編集して、[保存] をクリックします。

次のステップ

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

vCenter Server インスタンスの有効化または無効化

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

手順

1 メイン メニュー (☰) から、[vSphere リソース] を選択します。

2 左側のパネルで [vCenter] をクリックします。

3 ターゲット vCenter Server インスタンスの名前の横にあるラジオ ボタンをクリックして、[有効化] または [無効化] をクリックします。

4 確認するには、[OK] をクリックします。

vCenter Server インスタンスの再接続

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

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

手順

1. メイン メニュー (☰) から、[vSphere リソース] を選択します。
2. 左側のパネルで [vCenter] をクリックします。
3. ターゲット vCenter Server インスタンスの名前の横にあるラジオ ボタンをクリックして、[再接続] をクリックします。
4. 確認するには、[OK] をクリックします。

vCenter Server インスタンスの更新

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

手順

1. メイン メニュー (☰) から、[vSphere リソース] を選択します。
2. 左側のパネルで [vCenter] をクリックします。
3. ターゲット vCenter Server インスタンスの名前の横にあるラジオ ボタンをクリックして、[更新] をクリックします。
4. 確認するには、[OK] をクリックします。

vCenter Server インスタンスのストレージ ポリシーの更新

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

手順

1. メイン メニュー (☰) から、[vSphere リソース] を選択します。
2. 左側のパネルで [vCenter] をクリックします。
3. ターゲット vCenter Server インスタンスの名前の横にあるラジオ ボタンをクリックして、[ポリシーの更新] をクリックします。
4. 確認するには、[OK] をクリックします。

vCenter Server インスタンスの登録解除

vCenter Server インスタンスのリソースの使用を停止するには、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。

前提条件

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

手順

1. メイン メニュー (☰) から、[vSphere リソース] を選択します。
2. 左側のパネルで [vCenter] をクリックします。
3. ターゲット vCenter Server インスタンスの名前の横にあるラジオ ボタンをクリックして、[登録解除] をクリックします。
4. 確認するには、[OK] をクリックします。

NSX Manager 設定の変更

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

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

手順

1. メイン メニュー (☰) から、[vSphere リソース] を選択します。
2. 左側のペインで [vCenter] をクリックして、ターゲット NSX Manager インスタンスに関連付けられている vCenter Server インスタンスの名前をクリックします。
3. [NSX-V Manager 情報] セクションの右上隅にある [編集] をクリックします。
4. vCenter Server 設定を編集して、[保存] をクリックします。

NSX-T Manager 設定の変更

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

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

手順

1 メイン メニュー (☰) から、[vSphere リソース] を選択します。

2 左側のペインで [NSX-T Manager] をクリックし、変更する NSX-T Manager インスタンスの名前をクリックします。

3 [全般] タブの右上隅にある [編集] をクリックします。

4 NSX-T Manager 設定を編集して、[保存] をクリックします。

NSX-T Manger インスタンスの削除

NSX-T Manager インスタンスのリソースの使用を停止するには、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。

前提条件

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

手順

1 メイン メニュー (☰) から、[vSphere リソース] を選択します。

2 左側のペインで、[NSX-T Manager] をクリックします。

3 削除する NSX-T Manager インスタンス名の横にあるラジオ ボタンをクリックして、[削除] をクリックします。

4 確定するには、[削除] をクリックします。

マルチサイト リソース リスト

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

Service Provider Admin Portal から vSphere およびクラウド リソースを介した移動を容易にするために、バージョン 9.7 以降の vCloud Director にはマルチサイト リソース リストが導入されています。

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

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

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

マルチサイト クラウド リソース リストは、組織 VDC、組織 VDC テンプレート、プロバイダ VDC、クラウド セル、Edge Gateway、外部ネットワーク、およびネットワーク プールでサポートされています。

注： マルチサイト組織リストはサポートされていません。

プロバイダ仮想データセンターの管理 4

プロバイダ仮想データセンターを作成したら、プロバイダ仮想データセンターのプロパティを変更したり、プロバイダ仮想データセンター自体を無効化/削除したり、プロバイダ仮想データセンターのストレージ ポリシーやリソース プールを管理したりできます。

プロバイダ仮想データセンターを作成するには、vCloud Director Web Console または vCloud API を使用する必要があります。vCloud Director Web Console の使用の詳細については、「vCloud Director 管理者ガイド」を参照してください。vCloud API の使用の詳細については、「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。

この章には、次のトピックが含まれています。

プロバイダ仮想データセンターの有効化または無効化

プロバイダ仮想データセンターのリソースを使用する既存の組織仮想データセンターをすべて無効にするには、このプロバイダ仮想データセンターを無効にします。無効になった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を作成することはできません。

実行中の vApp およびパワーオンされた仮想マシンは、このプロバイダ仮想データセンターによってバッキングされている既存の組織仮想データセンターで引き続き実行されますが、追加の vApp または仮想マシンを作成または起動することはできません。

手順

1 メイン メニュー (☰) から、[クラウド リソース] を選択します。

2 左側のパネルで [プロバイダ VDC] をクリックします。

3 ターゲット プロバイダ仮想データセンターの名前の横にあるラジオ ボタンをクリックして、[有効化] または [無効化] をクリックします。

4 確認するには、[OK] をクリックします。

プロバイダ仮想データセンターの削除

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

vSphere の基盤となるリソースは影響を受けません。

前提条件

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

手順

1 メイン メニュー (☰) から、[クラウド リソース] を選択します。

2 左側のパネルで [プロバイダ VDC] をクリックします。

3 削除するプロバイダ仮想データセンター名の横にあるラジオ ボタンをクリックして、[削除] をクリックします。

4 確認するには、[OK] をクリックします。

プロバイダ仮想データセンターの全般設定の編集

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

手順

1 メイン メニュー (☰) から、[クラウド リソース] を選択します。

2 左側のパネルで [プロバイダ VDC] をクリックし、変更するプロバイダ仮想データセンターの名前をクリックします。

3 [設定] - [全般] タブで、右上隅にある [編集] をクリックします。

4 （オプション） プロバイダ仮想データセンターの名前および説明を変更します。

5 （オプション） ドロップダウン メニューから、このプロバイダ仮想データセンターでサポートされている最新のハードウェア バージョンを選択し、[保存] をクリックします。

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

注： プロバイダ仮想データセンターでサポートされるハードウェア バージョンのみをアップグレードできます。ハードウェア バージョンをダウングレードすることはできません。

6 [保存] をクリックします。

プロバイダ仮想データセンターのマージ

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

前提条件

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

手順

1 メイン メニュー (☰) から、[クラウド リソース] を選択します。

2 左側のパネルで [プロバイダ VDC] をクリックします。

3 拡張するプロバイダ仮想データセンターの名前の横にあるラジオ ボタンをクリックして、[マージ] をクリックします。

4 リソースをマージするプロバイダ仮想データセンターの名前の横にあるラジオ ボタンをクリックして、[マージ] をクリックします。

プロバイダ仮想データセンターの組織仮想データセンターの表示

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

手順

1 メイン メニュー (☰) から、[クラウド リソース] を選択します。

2 左側のパネルで [プロバイダ VDC] をクリックし、ターゲット プロバイダ仮想データセンターの名前をクリックします。

3 [組織 VDC] タブをクリックします。

結果

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

次のステップ

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

プロバイダ仮想データセンター上のデータストアの表示

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

手順

1. メイン メニュー ( ) から、[クラウド リソース] を選択します。
2. 左側のパネルで [プロバイダ VDC] をクリックし、ターゲット プロバイダ仮想データセンターの名前をクリックします。
3. [データストア] タブをクリックします。

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

タイトル	説明
[名前]	データストアの名前
[状態]	有効または無効
[タイプ]	データストアが使用するファイル システムのタイプ (仮想マシン ファイル システム (VMFS) またはネットワーク ファイル システム (NFS))
[使用済み]	ログ ファイル、スナップショットおよび仮想ディスクなど、仮想マシン ファイルに使用されているデータストア領域。仮想マシンをパワーオンすると、使用済みストレージ領域にログ ファイルも含まれます。
[プロビジョニング済み]	仮想マシンに保証されているデータストア領域。仮想マシンがシン プロビジョニングを使用している場合、プロビジョニング済み容量の一部は使用されていないため、他の仮想マシンが使用されていない容量を使用できる場合があります。シン プロビジョニングを使用する場合、この値が実際のデータストア容量を超える場合があります。

タイトル	説明
[要求されたストレージ]	データストア上で vCloud Director オブジェクトによってのみ使用されているプロビジョニング済みのストレージで、以下を含みます。 ■ vCloud Director でプロビジョニングされた仮想マシン ■ カタログ アイテム（テンプレートとメディア） ■ NSX Edge ■ 仮想マシンの使用済みおよび未使用のメモリ スワップ要件 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。
[vCenter]	データストアに関連付けられた vCenter Server インスタンス。

プロバイダ仮想データセンターの外部ネットワークの表示

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

手順

1 メイン メニュー (☰) から、[クラウド リソース] を選択します。

2 左側のパネルで [プロバイダ VDC] をクリックし、ターゲット プロバイダ仮想データセンターの名前をクリックします。

3 [外部ネットワーク] タブをクリックします。

結果

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

プロバイダ仮想データセンターでの仮想マシン ストレージ ポリシーの管理

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

プロバイダ仮想データセンターへの仮想マシン ストレージ ポリシーの追加

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

重要： vCloud Director は、暗号化や Storage I/O Control などのホストベースのデータ 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

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

手順

1. メイン メニュー (☰) から、[クラウド リソース] を選択します。
2. 左側のパネルで [プロバイダ VDC] をクリックし、ターゲット プロバイダ仮想データセンターの名前をクリックします。
3. [ストレージ ポリシー] タブで [追加] をクリックします。
4. 追加する 1 個以上のストレージ ポリシーを選択し、[追加] をクリックします。

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

次のステップ

プロバイダ仮想データセンターによってバッキングされている組織仮想データセンターを構成し、ストレージ ポリシーをサポートします。組織仮想データセンターへの仮想マシン ストレージ ポリシーの追加を参照してください。

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

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

手順

1. メイン メニュー (☰) から、[クラウド リソース] を選択します。
2. 左側のパネルで [プロバイダ VDC] をクリックし、ターゲット プロバイダ仮想データセンターの名前をクリックします。
3. [ストレージ ポリシー] タブをクリックします。
4. ターゲット仮想マシン ストレージ ポリシーの横にあるラジオ ボタンをクリックして、[有効化] または [無効化] をクリックします。
5. 確認するには、[OK] をクリックします。

プロバイダ仮想データセンターからの仮想マシン ストレージ ポリシーの削除

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

前提条件

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

手順

1 メイン メニュー (☰) から、[クラウド リソース] を選択します。

2 左側のパネルで [プロバイダ VDC] をクリックし、ターゲット プロバイダ仮想データセンターの名前をクリックします。

3 [ストレージ ポリシー] タブをクリックします。

4 ターゲット仮想マシン ストレージ ポリシーの横にあるラジオ ボタンをクリックして、[削除] をクリックします。

5 確認するには、[削除] をクリックします。

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

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

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

手順

1 メイン メニュー (☰) から、[クラウド リソース] を選択します。

2 左側のパネルで [プロバイダ VDC] をクリックし、ターゲット プロバイダ仮想データセンターの名前をクリックします。

3 [ストレージ ポリシー] タブをクリックします。

4 ターゲット仮想マシン ストレージ ポリシーの横にあるラジオ ボタンをクリックして、[メタデータ] をクリックします。

5 [[編集]]をクリックします。

6 （オプション） キーと値のペアを追加するには、[追加] をクリックして、名前と値を入力し、新しいキーと値のペアのタイプを選択します。

7 （オプション） キーと値のペアを編集するには、新しい名前と値を入力し、キーと値のペアに新しいタイプを選択します。

8 （オプション） キーと値のペアを削除するには、行の右端にある [削除] アイコンをクリックします。

9 [保存] をクリックし、[OK] をクリックします。

プロバイダ仮想データセンターでのリソース プールの管理

プロバイダ仮想データセンターからセカンダリ リソース プールを追加、有効化、無効化、および分離することができます。プロバイダ仮想データセンターでプライマリ リソース プールを無効化または分離することはできません。

プロバイダ仮想データセンターへのリソース プールの追加

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

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

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

前提条件

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

手順

1 メイン メニュー (☰) から、[クラウド リソース] を選択します。

2 左側のパネルで [プロバイダ VDC] をクリックし、ターゲット プロバイダ仮想データセンターの名前をクリックします。

3 [リソース プール] タブで [追加] をクリックします。

4 追加する 1 つ以上のリソース プールを選択し、[追加] 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キングされる従量課金制と割り当てプールの組織仮想データセンターすべてに柔軟性を持たせます。

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上のリソース プールの有効化または無効化

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

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

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

手順

1. メイン メニュー (☰) から、[クラウド リソース] を選択します。
2. 左側のパネルで [プロバイダ VDC] をクリックし、ターゲット プロバイダ仮想データセンターの名前をクリックします。
3. [リソース プール] タブをクリックします。
4. ターゲット リソース プールの横にあるラジオ ボタンをクリックして、[有効化] または [無効化] をクリックします。
5. 確認するには、[OK] をクリックします。

プロバイダ仮想データセンターからのリソース プールの分離

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

前提条件

- プロバイダ仮想データセンターのターゲット リソース プールを無効にします。プロバイダ仮想データセンター上のリソース プールの有効化または無効化を参照してください。
- 仮想マシンをそのリソース プールから有効にされたリソース プールへ移行します。プロバイダ仮想データセンターのリソース プール間で仮想マシンを移行する方法については、vCloud Director 管理者ガイドを参照してください。
- 無効化されたリソース プールの影響を受けるネットワークを再デプロイします。
- 無効化されたリソース プールの影響を受ける Edge ゲートウェイを再デプロイします。

手順

1. メイン メニュー (☰) から、[クラウド リソース] を選択します。
2. 左側のパネルで [プロバイダ VDC] をクリックし、ターゲット プロバイダ仮想データセンターの名前をクリックします。
3. [リソース プール] タブをクリックします。
4. ターゲット リソース プールの横にあるラジオ ボタンをクリックして、[分離] をクリックします。
5. 確認するには、[OK] をクリックします。

プロバイダ仮想データセンターのメタデータの変更

プロバイダ仮想データセンターのメタデータを追加、編集、または削除できます。

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

手順

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

組織の管理

5

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

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

この章には、次のトピックが含まれています。

リースについて

組織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。

組織の作成

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

手順

1 メイン メニュー (☰) から、[クラウド リソース] を選択します。

a 左側のパネルで [組織] を選択します。

既存の組織のリストがグリッド ビューで表示されます。

2 新しい組織を作成するには、[+ 追加] ボタンをクリックします。

[新しい組織] ダイアログが開きます。

3 以下の値を入力します。

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

4 [作成] ボタンをクリックして、作成を完了します。

組織のカタログの設定

組織がサービス カタログを共有する方法を設定できます。

手順

1 メイン メニュー (☰) から、[クラウド リソース] を選択します。

a 左側のパネルで [組織] を選択します。

既存の組織のリストがグリッド ビューで表示されます。

2 各項目の左側にあるリスト バー (⋮) を使用して、各組織に対して実行できるアクションを表示します。

3 [カタログ]をクリックします。

組織の [カタログ設定] ダイアログ ボックスが開きます。

4 次の共有および公開オプションを設定します。

オプション	説明
共有	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。
外部カタログへの公開を許可	組織管理者が vCloud Director のこのインスタンスの外部の組織にカタログを公開することを許可します。
外部カタログのサブスクライブを許可	組織管理者が vCloud Director のこのインスタンスの外部のカタログをサブスクライブすることを許可します。

組織のポリシーの設定

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

前提条件

リースについてを参照してください。

手順

1 メイン メニュー (☰) から、[クラウド リソース] を選択します。

a 左側のパネルで [組織] を選択します。

既存の組織のリストがグリッド ビューで表示されます。

2 各項目の左側にあるリスト バー (⋮) を使用して、各組織に対して実行できるアクションを表示します。

3 [ポリシー] をクリックして、組織のリース、割り当て容量、リソース制限、およびパスワード ポリシーを編集します。

4 次の内容で、vApp のリースを設定します。

オプション	説明
最大ランタイム リース	vApp を実行できる期間。この期間を過ぎると、自動的に停止されます。
最大ストレージ リース	停止した vApp を使用できる期間。この期間を過ぎると、自動的にクリーンアップされます。
ストレージ クリーンアップ	vApp を停止してクリーンアップした後の処理方法。

5 次の内容で、vApp テンプレートのリースを設定します。

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

6 次の内容で、割り当て容量を設定します。

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

7 次の内容で、制限を設定します。

オプション	説明
ユーザーごとのリソースを大量に消費する操作数	ユーザー 1 人あたりのリソースを大量に使用する操作の最大数を入力するか、[システム制限の継承] を選択します。
ユーザーごとのキューに入れられるリソースを大量に消費する操作数	ユーザー 1 人あたりのリソースを大量に使用するキュー登録対象操作の最大数を入力するか、[システム制限の継承] を選択します。
組織ごとのリソースを大量に消費する操作数	組織あたりのリソースを大量に使用する同時操作の最大数を入力するか、[システム制限の継承] を選択します。
組織ごとのキューに入れられるリソースを大量に消費する操作数	組織あたりのリソースを大量に使用するキュー登録対象操作の最大数を入力するか、[システム制限の継承] を選択します。
仮想マシンごとの同時接続数	仮想マシンあたりの同時コンソール接続の最大数を入力するか、[システム制限の継承] を選択します。
組織ごとの仮想データセンターの数	組織あたりの仮想データセンターの最大数を入力するか、[システム割り当て容量の継承] を選択します。

8 次の内容で、パスワード ポリシーを設定します。

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

組織仮想データセンターの管理

6

組織にリソースを提供するには、この組織用の組織仮想データセンターを 1 つ以上作成します。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。

この章には、次のトピックが含まれています。

割り当てモデルについて

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
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ライ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て、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。全般的なシステム設定の変更の詳細については、『vCloud Director 管理者ガイド』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 を作成するときに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もあります。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 *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 6-1. 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	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。
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。

表 6-1. 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	API パラメータ	説明
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 シェアの数を定義します。 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 Configurations	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 6-2. 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	■ 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	■ 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	■ 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。

組織仮想データセンターの作成

組織にリソースを割り当てるには、組織仮想データセンターを作成する必要があります。組織仮想データセンターは、プロバイダ仮想データセンターからリソースを取得します。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

プロバイダ仮想データセンターを作成します。『vCloud Director 管理者ガイド』を参照してください。

手順

1 メイン メニュー (☰) から、[クラウド リソース] を選択します。

2 左側のパネルで、[組織 VDC] をクリックし、[新規] をクリックします。

3 新しい組織仮想データセンターの名前と、オプションで説明を入力します。

4 （オプション） 作成時に新しい組織仮想データセンターを無効にするには、[組織 VDC を有効にします] 切り替えを有効にします。

無効な組織仮想データセンターに vApp をデプロイすることはできません。

5 [次へ] をクリックします。

6 この仮想データセンターを追加する組織の名前の横にあるラジオ ボタンを選択して、[次へ] をクリックします。

7 組織仮想データセンターのコンピューティング リソースおよびストレージ リソースの取得元となるプロバイダ仮想データセンターの名前の横にあるラジオ ボタンを選択して、[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リストには、サイトで有効になっているすべてのプロバイダ仮想データセンターと、使用可能なリソースに関する情報が表示されます。ネットワーク リストには、選択したプロバイダ仮想データセンターで使用できるネットワークの情報が表示されます。

8 この組織仮想データセンターの割り当てモデルを選択して、[次へ] をクリックします。

オプション	説明
割り当てプール	プロバイダ仮想データセンターから割り当てたリソースの割合が、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。
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 を作成するときにのみコミットされます。
予約プール	割り当てたすべてのリソースは、組織仮想データセンターに直ちにコミットされます。
Flex	VDC と各仮想マシン レベルの両方で、リソース使用量を制御できます。Flex 割り当てモデルは、組織 VDC コンピューティング ポリシーの機能をサポートします。Flex 割り当てモデルは、他の割り当てモデルで使用可能なすべての割り当て設定をサポートします。

9 選択した割り当てモデルの割り当て設定を行い、[次へ] をクリックします。

オプション	説明	割り当てモデル
[弾性]	柔軟性のあるプールの機能を有効または無効にします。柔軟性のある組織 VDC は、そのプロバイダ VDC に関連付けられているすべてのリソース プールを使用できます。	Flex
[仮想マシン メモリのオーバーヘッドを含める]	メモリのオーバーヘッドを含めるか、または除外します。	Flex
[CPU の割り当て]	この組織仮想データセンターで実行されている仮想マシンに割り当てる CPU の最大量。	■ 割り当てプール ■ 予約プール ■ Flex
[CPU リソースを予約値を超えて拡張できるようにします]	この組織仮想データセンターに無制限の CPU リソースを提供するには、この切り替えを有効にします。	予約プール
[CPU 割り当て]	この組織仮想データセンターの CPU 使用量の最大値。	■ 従量課金制 ■ Flex
[確保された CPU リソース]	この組織仮想データセンターで実行されている仮想マシンに確保する CPU リソースの割合。100% 未満を確保することで、CPU リソースのオーバー コミットメントを制御できます。 割り当てプールの割り当てモデルの場合、割合の確保によってこの組織仮想データセンターにコミットされる CPU の割り当ての割合も決定されます。	■ 割り当てプール ■ 従量課金制 ■ Flex

オプション	説明	割り当てモデル
[vCPU 速度]	vCPU の速度。組織仮想データセンターで実行されている仮想マシンには、vCPU あたりこの GHz 単位の速度が割り当てられます。	■ 従量課金制 ■ Flex
[メモリの割り当て]	この組織仮想データセンターで実行されている仮想マシンに割り当てるメモリの最大容量。	■ 割り当てプール ■ 予約プール
[メモリ割り当て]	この組織仮想データセンターのメモリ使用量の最大値。	■ 従量課金制 ■ Flex
[確保されたメモリ リソース]	組織仮想データセンターで実行されている仮想マシンに確保するメモリ リソースの割合。100 パーセント未満を確保すると、リソースをオーバーコミットできます。 割り当てプールの割り当てモデルの場合、割合の確保によってこの組織仮想データセンターにコミットされるメモリの割り当ての割合も決定されます。	■ 割り当てプール ■ 従量課金制 ■ Flex
[最大仮想マシン数]	組織仮想データセンターに配置できる仮想マシンの最大数。	■ 割り当てプール ■ 従量課金制 ■ 予約プール ■ Flex

10 この組織仮想データセンターのストレージ設定を行って、[次へ] をクリックします。

リストには、ソース プロバイダ仮想データセンターで有効なストレージ ポリシーが含まれています。

a この組織仮想データセンターに追加する 1 個以上のストレージ ポリシーのチェック ボックスを選択します。

b （オプション） 選択したストレージ ポリシーに割り当てられたストレージ容量を制限するには、[割り当てタイプ] セルのドロップダウン メニューで [制限] を選択し、[割り当て済みストレージ] セルに最大容量を入力します。

c （オプション） デフォルトのストレージ ポリシーを変更するには、[デフォルトのインスタンス化ポリシー] ドロップダウン メニューからターゲット デフォルト ストレージ ポリシーを選択します。

vCloud Director は、ストレージ ポリシーが仮想マシンまたは vApp テンプレートのレベルで指定されていないすべての仮想マシンのプロビジョニング操作で、デフォルトのストレージ ポリシーを使用します。

d （オプション） 組織仮想データセンター内の仮想マシンのシン プロビジョニングを有効にするには、[シン プロビジョニング] 切り替えをオンにします。

e （オプション） 組織仮想データセンター内の仮想マシンの高速プロビジョニングを無効にするには、[高速プロビジョニング] 切り替えを無効にします。

11 この組織仮想データセンターのネットワーク プールの設定を行って、[次へ] をクリックします。

vCloud Director はネットワーク プールを使用して、vApp ネットワークおよび組織仮想データセンターの内部ネットワークを作成します。

- この段階でネットワーク プールの追加をスキップするには、[ネットワーク プールを使用] 切り替えを無効にします。
- ネットワーク プールを設定するには、ターゲット ネットワーク プールの名前の横にあるラジオ ボタンを選択して、この組織仮想データセンターの割り当て容量を入力します。

割り当て容量とは、このネットワーク プールによってバッキングされる組織仮想データセンター内でプロビジョニングされるネットワークの最大数です。選択したネットワーク プールで使用可能なネットワーク数を超えることはできません。

12 [設定内容の確認] 画面の内容を確認し、[完了] をクリックします。

組織仮想データセンターの有効化または無効化

追加の vApp および仮想マシンに対して組織仮想データセンターのコンピューティング リソースおよびストレージ リソースの使用を禁止するには、この組織仮想データセンターを無効にします。実行中の vApp およびパワーオンされた仮想マシンは継続して実行されますが、追加の vApp または仮想マシンを作成したり開始したりすることはできません。

手順

1 メイン メニュー (☰) から、[クラウド リソース] を選択します。

2 左側のパネルで [組織 VDC] をクリックします。

3 ターゲット組織仮想データセンターの名前の横にあるラジオ ボタンを選択して、[有効化] または [無効化] をクリックします。

4 確認するには、[OK] をクリックします。

組織仮想データセンターの削除

組織から組織仮想データセンターのすべてのリソースを削除するには、この組織仮想データセンターを削除します。リソースは、ソース プロバイダ仮想データセンターにそのまま残ります。

重要： この操作を行うと、組織仮想データセンターと、そのすべての仮想マシン、vApp、組織仮想データセンター ネットワーク、および Edge Gateway が完全に削除されます。

前提条件

ターゲット組織仮想データセンターに属する特定の仮想マシン、vApp、vApp テンプレート、またはメディア ファイルを保持する場合は、それらを別の組織仮想データセンターに移動します。

手順

1 メイン メニュー (☰) から、[クラウド リソース] を選択します。

2 左側のパネルで [組織 VDC] をクリックします。

3 削除する組織仮想データセンター名の横にあるラジオ ボタンを選択して、[削除] をクリックします。

4 この組織仮想データセンターに、仮想マシン、vApp、組織仮想データセンター ネットワーク、Edge Gateway などのリソースが含まれている場合は、削除の確定のために各ソース タイプのチェックボックスを選択します。

5 確定するには、[削除] をクリックします。

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が拡大するにつれて、既存の組織仮想データセンターによりわかりやすい名前または説明を割り当てることが必要になる場合があります。

手順

1 メイン メニュー (☰) から、[クラウド リソース] を選択します。

2 左側のパネルで [組織 VDC] をクリックし、ターゲット組織仮想データセンターの名前をクリックします。

3 [全般] タブで、右上隅にある [編集] をクリックします。

4 新しい名前および説明を入力して、[保存] をクリックします。

組織仮想データセンターの割り当てモデルの設定の変更

組織仮想データセンターの割り当てモデルは変更できませんが、組織仮想データセンターの作成時に指定した割り当てモデルの割り当て設定は変更できます。

組織仮想データセンターの作成時に設定した割り当てモデルの割り当て設定は、変更が可能です。手順 9 を参照してください。

手順

1 メイン メニュー (☰) から、[クラウド リソース] を選択します。

2 左側のパネルで [組織 VDC] をクリックし、ターゲット組織仮想データセンターの名前をクリックします。

3 [割り当て] タブで、右上隅にある [編集] をクリックします。

4 割り当てモデルの設定を編集し、[保存] をクリックします。

組織仮想データセンターのストレージ設定の変更

組織仮想データセンターの作成時に設定したストレージ設定は、変更が可能です。

組織仮想データセンターの仮想マシン プロビジョニング設定の変更

組織仮想データセンターを作成するときに設定した仮想マシンのシン プロビジョニングおよび高速プロビジョニングの設定を変更できます。

手順

1 メイン メニュー (☰) から、[クラウド リソース] を選択します。

2 左側のパネルで [組織 VDC] をクリックし、ターゲット組織仮想データセンターの名前をクリックします。

3 [ストレージ] タブで、右上隅にある [編集] をクリックします。

4 （オプション） シン プロビジョニングの設定を変更します。

- 組織仮想データセンター内の仮想マシンのシン プロビジョニングを無効にするには、[シン プロビジョニング] の切り替えを無効にします。
- 組織仮想データセンター内の仮想マシンのシン プロビジョニングを有効にするには、[シン プロビジョニング] の切り替えを有効にします。

5 （オプション） 高速プロビジョニングの設定を変更します。

- 組織仮想データセンター内の仮想マシンの高速プロビジョニングを有効にするには、[高速プロビジョニング] の切り替えを有効にします。
- 組織仮想データセンター内の仮想マシンの高速プロビジョニングを無効にするには、[高速プロビジョニング] 切り替えを無効にします。

6 [[編集]]をクリックします。

組織仮想データセンターへの仮想マシン ストレージ ポリシーの追加

組織仮想データセンターを構成して、バッキング プロバイダ仮想データセンターに以前追加した仮想マシン ストレージ ポリシーをサポートできます。

前提条件

ターゲットの仮想マシン ストレージ ポリシーをソース プロバイダ仮想データセンターに追加していること。プロバイダ仮想データセンターへの仮想マシン ストレージ ポリシーの追加を参照してください。

手順

1 メイン メニュー (☰) から、[クラウド リソース] を選択します。

2 左側のパネルで [組織 VDC] をクリックし、ターゲット組織仮想データセンターの名前をクリックします。

3 [ストレージ] タブをクリックし、[追加] をクリックします。

ソース プロバイダ仮想データセンター内の、使用可能な追加ストレージ ポリシーのリストが表示されます。

4 追加する 1 個以上のストレージ ポリシーのチェック ボックスを選択して、[追加] をクリックします。

組織仮想データセンターのデフォルト ストレージ ポリシーの変更

組織仮想データセンターの作成時に設定したデフォルト ストレージ ポリシーを変更できます。

vCloud Director は、ストレージ ポリシーが仮想マシンまたは vApp テンプレートのレベルで指定されていないすべての仮想マシンのプロビジョニング操作で、デフォルトのストレージ ポリシーを使用します。

前提条件

- ターゲット デフォルト ストレージ ポリシーが、組織仮想データセンターに追加されています。組織仮想データセンターへの仮想マシン ストレージ ポリシーの追加を参照してください。
- ターゲット デフォルト ストレージ ポリシーが、組織仮想データセンターで有効になっています。組織仮想データセンターのストレージ ポリシーの有効化または無効化を参照してください。

手順

1 メイン メニュー (☰) から、[クラウド リソース] を選択します。

2 左側のパネルで [組織 VDC] をクリックし、ターゲット組織仮想データセンターの名前をクリックします。

3 [ストレージ] タブをクリックします。

4 ターゲット デフォルト ストレージ ポリシーの名前の横にあるラジオ ボタンをクリックし、[デフォルトとして設定] をクリックします。

5 確認するには、[OK] をクリックします。

組織仮想データセンターのストレージ ポリシーの制限の編集

組織仮想データセンターの作成時にストレージ ポリシーに対して設定した、割り当て済みストレージ容量の制限を変更できます。

割り当て済みストレージ容量を無制限に設定するか、組織仮想データセンターのストレージ ポリシーに割り当てられるストレージ容量の最大値を設定することができます。

手順

1 メイン メニュー (☰) から、[クラウド リソース] を選択します。

2 左側のパネルで [組織 VDC] をクリックし、ターゲット組織仮想データセンターの名前をクリックします。

3 [ストレージ] タブをクリックします。

4 対象のストレージ ポリシーの名前の横にあるラジオ ボタンをクリックして、[制限の編集] をクリックします。

5 このストレージ ポリシーの制限を設定します。

   - 制限を設定するには、上部のラジオ ボタンを選択し、この組織仮想データセンターのこのストレージ ポリシーに対するストレージ リソースの最大量を入力します。
   - 制限を設定しない場合は、[制限なし] ラジオ ボタンを選択します。

6 [[編集]]をクリックします。

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

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

オブジェクト メタデータを使用すると、ユーザー定義の *name*=*value* ペアに、組織仮想データセンターのストレージ ポリシーを関連付けることができます。vCloud API クエリのフィルタ式内でオブジェクト メタデータを使用できます。

手順

1 メイン メニュー (☰) から、[クラウド リソース] を選択します。

2 左側のパネルで [組織 VDC] をクリックし、ターゲット組織仮想データセンターの名前をクリックします。

3 [ストレージ] タブをクリックします。

4 対象のストレージ ポリシー名の横にあるラジオ ボタンをクリックして、[メタデータ] をクリックします。

5 [[編集]]をクリックします。

6 （オプション） キーと値のペアを追加するには、[追加] をクリックして、名前と値を入力し、新しいキーと値のペアのタイプを選択します。

7 （オプション） キーと値のペアを編集するには、新しい名前と値を入力し、キーと値のペアに新しいタイプを選択します。

8 （オプション） キーと値のペアを削除するには、行の右端にある [削除] アイコンをクリックします。

9 [保存] をクリックし、[OK] をクリックします。

組織仮想データセンターのストレージ ポリシーの有効化または無効化

追加の vApp および仮想マシンに対して組織仮想データセンターのストレージ ポリシーの使用を禁止するには、組織仮想データセンターでこのストレージ ポリシーを無効にします。実行中の vApp およびパワーオンされた仮想マシンは継続して実行されますが、このストレージ ポリシーに関して追加の vApp または仮想マシンを作成したり開始したりすることはできません。

デフォルトのストレージ ポリシーを無効にすることはできません。

前提条件

デフォルトのストレージ ポリシーを無効にする場合は、組織仮想データセンターのデフォルト ストレージ ポリシーの変更。

手順

1 メイン メニュー (☰) から、[クラウド リソース] を選択します。

2 左側のパネルで [組織 VDC] をクリックし、ターゲット組織仮想データセンターの名前をクリックします。

3 [ストレージ] タブをクリックします。

4 ターゲット ストレージ ポリシーの名前の横にあるラジオ ボタンをクリックして、[有効化] または [無効化] をクリックします。

5 確認するには、[OK] をクリックします。

組織仮想データセンターからの仮想マシン ストレージ ポリシーの削除

組織仮想データセンターがストレージ ポリシーを使用しないようにするには、このストレージ ポリシーを組織仮想データセンターから削除します。実行中の vApp およびパワーオンされた仮想マシンは継続して実行されますが、このストレージ ポリシーに関して追加の vApp または仮想マシンを作成したり開始したりすることはできません。

前提条件

削除するストレージ ポリシーを無効にします。組織仮想データセンターのストレージ ポリシーの有効化または無効化を参照してください。

手順

1 メイン メニュー (☰) から、[クラウド リソース] を選択します。

2 左側のパネルで [組織 VDC] をクリックし、ターゲット組織仮想データセンターの名前をクリックします。

3 [ストレージ] タブをクリックします。

4 対象のストレージ ポリシー名の横にあるラジオ ボタンをクリックして、[削除] をクリックします。

5 確認するには、[削除] をクリックします。

組織仮想データセンターのネットワーク設定の編集

組織仮想データセンターで新しいネットワークをプロビジョニングする場合のプロビジョニング元になるネットワーク プールを変更できます。組織仮想データセンターでクロス仮想データセンター ネットワークを有効にすることもできます。

ネットワーク プールは、vApp ネットワーク、経路指定された組織 VDC ネットワーク、および内部の組織 VDC ネットワークを作成するための、区別されていないネットワークのグループです。新しいネットワークのネットワーク プールを変更できます。既存のネットワークでは、引き続き古いネットワーク プールが使用されます。

クロス仮想データセンター ネットワークが有効な組織仮想データセンターを使用すると、関連する権限を持つ組織ユーザーは、データセンター グループを作成し、これらのグループに拡張レイヤー 2 ネットワークを作成することができます。

前提条件

組織仮想データセンターでクロス VDC ネットワークを有効にする場合は、バッキング プロバイダ仮想データセンターに対して Cross-vCenter NSX が構成されていることを確認します。

手順

1 メイン メニュー (☰) から、[クラウド リソース] を選択します。

2 左側のパネルで [組織 VDC] をクリックし、ターゲット組織仮想データセンターの名前をクリックします。

3 [ネットワーク プール] タブで、右上隅にある [編集] をクリックします。

この組織仮想データセンターによって使用されているネットワークの数が表示されます。

4 （オプション） この組織仮想データセンターのネットワーク プールを構成します。

- この組織仮想データセンターのネットワーク プールを使用しない場合は、[ネットワーク プールを使用] 切り替えを無効にします。
- この組織仮想データセンターにネットワーク プールを構成する場合は、次の手順を実行します。
  a [ネットワーク プールを使用] 切り替えを有効にします。

  使用可能なネットワーク プールのリストが、これらの使用状況、使用可能なネットワーク、および容量に関する情報と共に表示されます。

  b ターゲット リソース プールの名前の横にあるラジオ ボタンを選択します。

c この組織仮想データセンター内のこのネットワーク プールの割り当てを設定します。

割り当てとは、プロビジョニングされたネットワークの最大数のことです。選択したネットワーク プールで使用可能なネットワーク数を超えることはできません。

5 この組織仮想データセンターでクロス仮想データセンター ネットワークを有効にするには、[クロス VDC ネットワーク] 切り替えを有効にします。

6 [保存] をクリックします。

結果

vCloud Director テナント ポータルのデータセンターのリストに、クロス仮想データセンター ネットワークが有効な仮想データセンターが表示され、データセンター グループを作成することができます。データセンター グループの作成の詳細については、『vCloud Director Tenant Portal Guide』を参照してください。

組織仮想データセンターのメタデータの変更

組織仮想データセンターのメタデータを追加、編集、または削除できます。

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

手順

1 メイン メニュー (☰) から、[クラウド リソース] を選択します。

2 左側のパネルで [組織 VDC] をクリックし、ターゲット組織仮想データセンターの名前をクリックします。

3 [メタデータ] タブをクリックします。

4 [[編集]]をクリックします。

5 （オプション） キーと値のペアを追加するには、[追加] をクリックして、名前と値を入力し、新しいキーと値のペアのタイプを選択します。

6 （オプション） キーと値のペアを編集するには、新しい名前と値を入力し、キーと値のペアに新しいタイプを選択します。

7 （オプション） キーと値のペアを削除するには、行の右端にある [削除] アイコンをクリックします。

8 [保存] をクリックし、[OK] をクリックします。

組織仮想データセンターのリソース プールの表示

組織仮想データセンターで使用される vCenter Server リソース プールのリストを表示できます。

手順

1 メイン メニュー (☰) から、[クラウド リソース] を選択します。

2 左側のパネルで [組織 VDC] をクリックし、ターゲット組織仮想データセンターの名前をクリックします。

3 [リソース プール] タブをクリックします。

結果

組織仮想データセンターで使用されているリソース プール、および各リソース プールが属する vCenter Server インスタンスが示されたテーブルが表示されます。

組織仮想データセンターの分散ファイアウォールの管理

組織仮想データセンターでレイヤー 3 およびレイヤー 2 ネットワーク セキュリティを提供するには、この組織仮想データセンターで分散ファイアウォールを有効にして、そのルールを作成します。分散ファイアウォール ルールが有効な場合は、組織仮想データセンター内の仮想マシン間で移動するトラフィックを保護できます。

vCloud Director は、NSX Data Center for vSphere によってバッキングされた組織仮想データセンターで分散ファイアウォール サービスをサポートしています。

分散ファイアウォール ルールを作成する場合は、さまざまなグループ オブジェクトとセキュリティ グループを使用できます。オブジェクトのグループ分け（カスタム）および セキュリティ グループの操作 を参照してください。

Edge Gateway との間で送受信されるトラフィックの保護については、Edge Gateway ファイアウォールの管理を参照してください。

組織仮想データセンターの分散ファイアウォールの有効化

組織仮想データセンターで分散ファイアウォール設定を管理するには、この組織仮想データセンターで分散ファイアウォールを有効にしておく必要があります。

vCloud Director は、NSX Data Center for vSphere によってバッキングされた組織仮想データセンターで分散ファイアウォール サービスをサポートしています。

手順

1. メイン メニュー (☰) から、[クラウド リソース] を選択します。
2. 左側のパネルで [組織 VDC] をクリックします。
3. ターゲット組織仮想データセンターの横にあるラジオ ボタンをクリックして、[ファイアウォールの管理] をクリックします。
4. [分散ファイアウォール] - [全般] タブで [分散ファイアウォールの有効化] 切り替えを有効にします。

結果

レイヤー 3 とレイヤー 2 のすべてのトラフィックが組織仮想データセンターを通過できるように設定された、デフォルトのファイアウォール ルールが表示されます。

- [分散ファイアウォール] - [全般] タブに、レイヤー 3 トラフィックのデフォルトの分散ファイアウォール ルール（名前付きのデフォルトの許可ルール）が表示されます。
- [分散ファイアウォール] - [イーサネット] タブに、レイヤー 2 トラフィックのデフォルトの分散ファイアウォール ルール（名前付きのデフォルトの許可ルール）が表示されます。

分散ファイアウォール ルールの追加

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

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

前提条件

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

手順

1. メイン メニュー (☰) から、[クラウド リソース] を選択します。
2. 左側のパネルで [組織 VDC] をクリックします。
3. ターゲット組織仮想データセンターの横にあるラジオ ボタンをクリックして、[ファイアウォールの管理] をクリックします。
4. 作成するルールのタイプを選択します。一般的なルールまたはイーサネット ルールを作成するオプションがあります。

   レイヤー 3 (L3) ルールは [全般] タブで構成されます。レイヤー 2 (L2) ルールは [イーサネット] タブで構成されます。
5. ファイアウォール テーブルの既存のルールの下にルールを追加するには、既存の行をクリックし、[作成] () ボタンをクリックします。

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

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

アクション	説明
[IP] アイコンをクリック	[全般] タブで定義されたルールを適用します。 使用するソースの値を入力します。有効な値は、IP アドレス、CIDR、IP アドレス範囲、またはキーワード **any** です。分散ファイアウォールは、IPv4 形式のみをサポートします。
[+] アイコンをクリック	[+] アイコンを使用し、特定の IP アドレス以外のオブジェクトをソースとして次のように指定します。 ■ [オブジェクトの選択] ウィンドウを使用し、選択内容に一致するオブジェクトを追加し、[保持] をクリックしてそれらをルールに追加します。 ■ ソースをルールから除外するには、[オブジェクトの選択] ウィンドウを使用してこのルールに追加し、次に除外の切り替えアイコンを選択してそのソースをこのルールから除外します。 ソースで除外の切り替えを選択すると、すべてのソース（除外したソースを除く）から受信するトラフィックにルールが適用されます。除外の切り替えを選択しない場合、[オブジェクトの選択] ウィンドウで指定したソースから受信するトラフィックにルールが適用されます。

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

アクション	説明
[IP] アイコンをクリック	[全般] タブで定義されたルールを適用します。 使用するターゲットの値を入力します。有効な値は、IP アドレス、CIDR、IP アドレス範囲、またはキーワード **any** です。分散ファイアウォールは、IPv4 形式のみをサポートします。
[+] アイコンをクリック	[+] アイコンを使用し、特定の IP アドレス以外のオブジェクトをソースとして次のように指定します。 ■ [オブジェクトの選択] ウィンドウを使用し、選択内容に一致するオブジェクトを追加し、[保持] をクリックしてそれらをルールに追加します。 ■ ソースをルールから除外するには、[オブジェクトの選択] ウィンドウを使用してこのルールに追加し、次に除外の切り替えアイコンを選択してそのソースをこのルールから除外します。 ソースで除外の切り替えを選択すると、すべてのソース（除外したソースを除く）から受信するトラフィックにルールが適用されます。除外の切り替えを選択しない場合、[オブジェクトの選択] ウィンドウで指定したソースから受信するトラフィックにルールが適用されます。

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

アクション	説明
[IP] アイコンをクリック	サービスをポートとプロトコルの組み合わせとして指定します。 a サービス プロトコルを選択します。 b ソースとターゲット ポートのポート番号を入力するか、または **任意** を指定し、[保持] をクリックします。
[+] アイコンをクリック	事前定義済みサービスまたはサービス グループを選択するか、または新規のものを定義するには、次のようにします。 a 1 つまたは複数のオブジェクトを選択し、フィルタに追加します。 b [保持] をクリックします。

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

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

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

12 これが [全般] タブのルールである場合、新しいルールの [パケット タイプ] セルで、パケット タイプとして [任意]、[IPV4]、または [IPV6] のいずれかを選択します。

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

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

14 [変更を保存] をクリックします。

分散ファイアウォール ルールの編集

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

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

手順

1 メイン メニュー (☰) から、[クラウド リソース] を選択します。

2 左側のパネルで [組織 VDC] をクリックします。

3 ターゲット組織仮想データセンターの横にあるラジオ ボタンをクリックして、[ファイアウォールの管理] をクリックします。

4 分散ファイアウォール ルールを管理するには、次のいずれかのアクションを実行します。

- ルールを無効にする。これは、[いいえ] セルの緑色のチェック マークをクリックすることで行います。

  緑色のチェック マークは、無効を示す赤色のアイコンになります。無効にしたルールを有効にするには、無効を示す赤色のアイコンをクリックします。

- ルール名を編集する。これは、[名前] セルをダブルクリックして、新しい名前を入力することで行います。
- ルールの設定（ソース設定やアクション設定など）を変更する。これは、該当するセルを選択し、表示されたコントロールを使用することで行います。
- ルールを削除する。これは、ルール テーブルの上にある [削除] (✖) ボタンをクリックすることで行います。

- ルール テーブルでルールを上下に移動する。これは、ルールを選択して、ルール テーブルの上にある上下の矢印ボタンをクリックすることで行います。

5 [変更を保存] をクリックします。

オブジェクトのグループ分け（カスタム）

NSX 環境の vCloud Director ソフトウェアは、特定のエンティティのセットおよびグループを定義する機能を提供します。これは、他のネットワーク関連の設定（ファイアウォール ルールの設定など）を指定するときに使用できます。

ファイアウォール ルールと DHCP リレー設定で使用するための IP アドレス セットの作成

IP セットは、組織仮想データセンター レベルで作成できる IP アドレスのグループのことです。IP セットは、ファイアウォール ルールまたは DHCP リレー設定で送信元または宛先として使用することができます。

IP セットは、[オブジェクトのグループ分け] 画面を使用して作成します。このページを開くには、組織 VDC の分散ファイアウォール設定に移動するか、組織 VDC に属する Edge ゲートウェイのサービス設定に移動する必要があります。

手順

1 [オブジェクトのグループ分け] ページを開きます。

オプション	アクション
組織 VDC の分散ファイアウォール設定から	a メイン メニュー (☰) から、[クラウド リソース] を選択します。 b 左側のパネルで [組織 VDC] をクリックします。 c ターゲット組織仮想データセンターの名前の横にあるラジオ ボタンを選択して、[ファイアウォールの管理] をクリックします。 d [オブジェクトのグループ分け] タブをクリックします。
組織 VDC の Edge Gateway のサービス設定から	a メイン メニュー (☰) から、[クラウド リソース] を選択します。 b 左側のパネルで [Edge ゲートウェイ] をクリックします。 c ターゲット組織仮想データセンターに属する Edge Gateway の名前の横にあるラジオ ボタンを選択して、[サービス] をクリックします。 d [オブジェクトのグループ分け] タブをクリックします。

2 [IP アドレス セット] タブをクリックします。

定義済みの IP アドレス セットが画面に表示されます。

3 IP アドレス セットを追加するには、[作成] (+) ボタンをクリックします。

4 IP セットに含める IP アドレスの他に、IP セットの名前と、オプションで IP セットの説明を入力します。

5 この IP セットを保存するには、[保持] をクリックします。

結果

これで、新しい IP セットをファイアウォール ルールまたは DHCP リレー構成でソースまたはターゲットとして選択できます。

ファイアウォール ルールで使用するための MAC アドレス セットの作成

MAC セットは、組織仮想データセンター レベルで作成できる MAC アドレスのグループです。ファイアウォール ルールの送信元または宛先として MAC セットを使用できます。

MAC セットを作成するには、[オブジェクトのグループ分け] 画面を使用します。この画面を開くには、組織 VDC の分散ファイアウォール設定に移動するか、組織 VDC に属する Edge Gateway のサービス設定に移動する必要があります。

手順

1 [オブジェクトのグループ分け] ページを開きます。

オプション	アクション
組織 VDC の分散ファイアウォール設定から	a メイン メニュー (☰) から、[クラウド リソース] を選択します。 b 左側のパネルで [組織 VDC] をクリックします。 c ターゲット組織仮想データセンターの名前の横にあるラジオ ボタンを選択して、[ファイアウォールの管理] をクリックします。 d [オブジェクトのグループ分け] タブをクリックします。
組織 VDC の Edge Gateway のサービス設定から	a メイン メニュー (☰) から、[クラウド リソース] を選択します。 b 左側のパネルで [Edge ゲートウェイ] をクリックします。 c ターゲット組織仮想データセンターに属する Edge Gateway の名前の横にあるラジオ ボタンを選択して、[サービス] をクリックします。 d [オブジェクトのグループ分け] タブをクリックします。

2 [MAC アドレス セット] タブをクリックします。

定義済みの MAC アドレス セットが画面に表示されます。

3 MAC アドレス セットを追加するには、[作成] () ボタンをクリックします。

4 セット名を入力し、オプションで説明、および MAC アドレス セットに含める MAC アドレスを入力します。

5 MAC アドレス セットを保存するには、[保持] をクリックします。

結果

これで、新しい MAC アドレス セットをファイアウォール ルールでソースまたはターゲットとして選択できます。

ファイアウォール ルールで使用可能なサービスの表示

ファイアウォール ルールで使用できるサービスのリストを表示できます。この場合、サービスとはプロトコルとポートの組み合わせです。

使用可能なサービスを表示するには、[オブジェクトのグループ分け] 画面を使用します。この画面を開くには、組織 VDC の分散ファイアウォール設定に移動するか、組織 VDC に属する Edge Gateway のサービス設定に移動する必要があります。

手順

1 [オブジェクトのグループ分け] ページを開きます。

オプション	アクション
組織 VDC の分散ファイアウォール設定から	a メイン メニュー (☰) から、[クラウド リソース] を選択します。 b 左側のパネルで [組織 VDC] をクリックします。 c ターゲット組織仮想データセンターの名前の横にあるラジオ ボタンを選択して、[ファイアウォールの管理] をクリックします。 d [オブジェクトのグループ分け] タブをクリックします。
組織 VDC の Edge Gateway のサービス設定から	a メイン メニュー (☰) から、[クラウド リソース] を選択します。 b 左側のパネルで [Edge ゲートウェイ] をクリックします。 c ターゲット組織仮想データセンターに属する Edge Gateway の名前の横にあるラジオ ボタンを選択して、[サービス] をクリックします。 d [オブジェクトのグループ分け] タブをクリックします。

2 [サービス] タブをクリックします。

結果

使用可能なサービスが画面に表示されます。

ファイアウォール ルールで使用可能なサービス グループの表示

ファイアウォール ルールで使用できるサービス グループのリストを表示できます。この場合、サービスとはプロトコルとポートの組み合わせであり、サービス グループとはサービスまたは他のサービス グループから成るグループです。

使用可能なサービス グループを表示するには、[オブジェクトのグループ分け] 画面を使用します。この画面を開くには、組織 VDC の分散ファイアウォール設定に移動するか、組織 VDC に属する Edge Gateway のサービス設定に移動する必要があります。

手順

1 [オブジェクトのグループ分け] ページを開きます。

オプション	アクション
組織 VDC の分散ファイアウォール設定から	a メイン メニュー (☰) から、[クラウド リソース] を選択します。 b 左側のパネルで [組織 VDC] をクリックします。 c ターゲット組織仮想データセンターの名前の横にあるラジオ ボタンを選択して、[ファイアウォールの管理] をクリックします。 d [オブジェクトのグループ分け] タブをクリックします。
組織 VDC の Edge Gateway のサービス設定から	a メイン メニュー (☰) から、[クラウド リソース] を選択します。 b 左側のパネルで [Edge ゲートウェイ] をクリックします。 c ターゲット組織仮想データセンターに属する Edge Gateway の名前の横にあるラジオ ボタンを選択して、[サービス] をクリックします。 d [オブジェクトのグループ分け] タブをクリックします。

2 [サービス グループ] タブをクリックします。

結果

使用可能なサービス グループが画面に表示されます。[説明] 列には、サービス グループごとにグループ分けされたサービスが表示されます。

セキュリティ グループの操作

セキュリティ グループとは、仮想マシン、組織仮想データセンター ネットワーク、セキュリティ タグなどのアセットまたはグループ分けオブジェクトの集合です。

セキュリティ グループには、セキュリティ タグ、仮想マシン名、仮想マシンのゲスト OS 名、または仮想マシンのゲスト ホスト名に基づく動的なメンバーシップ基準を設定できます。たとえば、「web」というセキュリティ タグのある仮想マシンは、いずれも Web サーバ向けの特定のセキュリティ グループに自動的に追加されます。セキュリティ グループを作成すると、そのグループにセキュリティ ポリシーが適用されます。

セキュリティ グループの作成

ユーザー定義のセキュリティ グループを作成できます。

前提条件

セキュリティ グループでセキュリティ タグを使用する場合は、セキュリティ タグの作成および割り当てを行います。

手順

1 メイン メニュー (☰) から、[クラウド リソース] を選択します。

2 左側のパネルで [組織 VDC] をクリックします。

3 ターゲット組織仮想データセンターの横にあるラジオ ボタンをクリックして、[ファイアウォールの管理] をクリックします。

4 [オブジェクトのグループ分け] - [セキュリティ グループ] タブをクリックします。

5 [作成]（  ）ボタンをクリックします。

6 セキュリティ グループの名前と、オプションで説明を入力します。

この説明はセキュリティ グループのリスト内に表示されます。わかりやすい説明を追加することにより、セキュリティ グループを簡単に識別できます。

7 （オプション） 動的なメンバー セットを追加します。

a 動的なメンバー セットの下にある [追加]（  ）ボタンをクリックします。

b ステートメントの条件の [任意]の一部または[すべて] に一致させるかどうかを選択します。

c 一致する最初のオブジェクトを入力します。

オプションには、[セキュリティ タグ]、[仮想マシンのゲスト OS の名前]、[仮想マシン名]、[仮想マシンのゲスト ホストの名前] があります。

d [次を含む]、[次の値で始まる]、[次の値で終わる] などの演算子を選択します。

e 値を入力します。

f （オプション） 別のステートメントを追加するには、ブール演算子の [And] または [Or] を使用します。

8 （オプション） メンバーを含めます。

a [次のタイプのオブジェクトを参照] ドロップダウン メニューで、[仮想マシン]、[組織 VDC ネットワーク]、[IP アドレス セット]、[MAC アドレス セット]、[セキュリティ タグ] などのオブジェクト タイプを選択します。

b [メンバーを含める] リストにオブジェクトを含めるには、左側のパネルでオブジェクトを選択し、右矢印をクリックして右側のパネルに移動します。

9 （オプション） メンバーを除外します。

a [次のタイプのオブジェクトを参照] ドロップダウン メニューで、[仮想マシン]、[組織 VDC ネットワーク]、[IP アドレス セット]、[MAC アドレス セット]、[セキュリティ タグ] などのオブジェクト タイプを選択します。

b [メンバーを除外] リストにオブジェクトを含めるには、左側のパネルでオブジェクトを選択し、右矢印をクリックして右側のパネルに移動します。

10 変更内容を維持するには、[保持] をクリックします。

この操作は完了するまでに 1 分かかることがあります。

結果

これで、セキュリティ グループを、ファイアウォール ルールなどのルールで使用できるようになりました。

セキュリティ グループの編集

ユーザー定義のセキュリティ グループを編集できます。

手順

1 メイン メニュー (☰) から、[クラウド リソース] を選択します。

2 左側のパネルで [組織 VDC] をクリックします。

3 ターゲット組織仮想データセンターの横にあるラジオ ボタンをクリックして、[ファイアウォールの管理] をクリックします。

4 [オブジェクトのグループ分け] - [セキュリティ グループ] タブをクリックします。

5 編集するセキュリティ グループを選択します。

セキュリティ グループの詳細は、セキュリティ グループのリストの下に表示されます。

6 （オプション） セキュリティ グループの名前と説明を編集します。

7 （オプション） 動的なメンバー セットを追加します。

a [動的なメンバー セット] の下にある [追加] （ + ） ボタンをクリックします。

b ステートメントの条件の [任意]の一部または[すべて] に一致させるかどうかを選択します。

c 一致する最初のオブジェクトを入力します。

オプションには、[セキュリティ タグ]、[仮想マシンのゲスト OS の名前]、[仮想マシン名]、[仮想マシンのゲスト ホストの名前] があります。

d [次を含む]、[次の値で始まる]、[次の値で終わる] などの演算子を選択します。

e 値を入力します。

f （オプション） 別のステートメントを追加するには、ブール演算子の [And] または [Or] を使用します。

8 （オプション） 編集するメンバー セットの横にある [編集] (⚙) アイコンをクリックして、動的なメンバー セットを編集します。

a 動的なメンバー セットに必要な変更を適用します。

b [OK] をクリックします。

9 （オプション） 削除するメンバー セットの横にある [削除] (✖) アイコンをクリックして、動的なメンバー セットを削除します。

10 （オプション） [メンバーを含める] リストの横にある [編集] (⚙) アイコンをクリックして、含まれているメンバーのリストを編集します。

a [次のタイプのオブジェクトを参照] ドロップダウン メニューで、[仮想マシン]、[組織 VDC ネットワーク]、[IP アドレス セット]、[MAC アドレス セット]、[セキュリティ タグ] などのオブジェクト タイプを選択します。

b [メンバーを含める] リストにオブジェクトを含めるには、左側のパネルでオブジェクトを選択し、右矢印をクリックして右側のパネルに移動します。

c [メンバーを含める] リストからオブジェクトを除外するには、右側のパネルでオブジェクトを選択し、左矢印をクリックして左側のパネルに移動します。

11 （オプション）[メンバーを除外] リストの横にある [編集] (⚙) アイコンをクリックして、除外されたメンバーのリストを編集します。

   a [次のタイプのオブジェクトを参照] ドロップダウン メニューで、[仮想マシン]、[組織 VDC ネットワーク]、[IP アドレス セット]、[MAC アドレス セット]、[セキュリティ タグ] などのオブジェクト タイプを選択します。

   b [メンバーを除外] リストにオブジェクトを含めるには、左側のパネルでオブジェクトを選択し、右矢印をクリックして右側のパネルに移動します。

   c [メンバーを除外] リストからオブジェクトを除外するには、右側のパネルでオブジェクトを選択し、左矢印をクリックして左側のパネルに移動します。

12 [変更を保存] をクリックします。

   セキュリティ グループへの変更が保存されます。

セキュリティ グループの削除

ユーザー定義のセキュリティ グループを削除できます。

手順

1 メイン メニュー (☰) から、[クラウド リソース] を選択します。

2 左側のパネルで [組織 VDC] をクリックします。

3 ターゲット組織仮想データセンターの横にあるラジオ ボタンをクリックして、[ファイアウォールの管理] をクリックします。

4 [オブジェクトのグループ分け] - [セキュリティ グループ] タブをクリックします。

5 削除するセキュリティ グループを選択します。

6 [削除] (✖) ボタンをクリックします。

7 削除を確定するには、[OK] をクリックします。

結果

セキュリティ グループが削除されます。

セキュリティ タグの操作

セキュリティ タグとは、仮想マシンまたは仮想マシンのグループに関連付けることができるラベルです。セキュリティ タグは、セキュリティ グループと共に使用することを想定して設計されています。セキュリティ タグを作成したら、それをファイアウォール ルールで使用できるセキュリティ グループに関連付けます。ユーザー定義セキュリティ タグの作成、編集、割り当てを行うことができます。また、特定のセキュリティ タグが適用されている仮想マシンやセキュリティ グループを表示することもできます。

セキュリティ タグは、通常はオブジェクトを動的にグループ化してファイアウォール ルールを簡素化するために使用します。たとえば、任意の仮想マシンで発生することが予想されるアクティビティの種類に基づき、いくつかの異なるセキュリティ タグを作成できます。セキュリティ タグを、1 つはデータベース サーバ用、もう 1 つはメール サーバ用に作成します。その後、データベース サーバまたはメール サーバを収容する仮想マシンに適切なタグを適用します。後でセキュリティ グループにタグを割り当て、それに対するファイアウォール ルールを記述すれば、仮想マシンで実行されているのがデータベース サーバかメール サーバかによって異なるセキュリティ設定を適用できます。仮想マシンの機能を後で変更する場合は、ファイアウォール ルールを編集するのではなく、セキュリティ タグから仮想マシンを削除して行えます。

セキュリティ タグの作成および割り当て

セキュリティ タグを作成して、仮想マシンまたは仮想マシン グループに割り当てることができます。

セキュリティ タグを作成してから、それを仮想マシンまたは仮想マシン グループに割り当てます。

手順

1 メイン メニュー (☰) から、[クラウド リソース] を選択します。

2 左側のパネルで [組織 VDC] をクリックします。

3 ターゲット組織仮想データセンターの横にあるラジオ ボタンをクリックして、[ファイアウォールの管理] をクリックします。

4 [セキュリティ タグ] タブをクリックします。

5 [作成] () ボタンをクリックし、セキュリティ タグの名前を入力します。

6 (オプション) セキュリティ タグの説明を入力します。

7 (オプション) セキュリティ タグを仮想マシンまたは仮想マシン グループに割り当てます。

[次のタイプのオブジェクトを参照] ドロップダウン メニューでは、[仮想マシン] がデフォルトで選択されています。

a 左側のパネルから仮想マシンを選択します。

b 右矢印をクリックして、選択した仮想マシンにセキュリティ タグを割り当てます。

仮想マシンは右側のパネルに移動し、セキュリティ タグが割り当てられます。

8 選択した仮想マシンへのタグの割り当てが完了したら、[保持] をクリックします。

結果

セキュリティ タグが作成され、(事前に選択してある場合は) 選択した仮想マシンに割り当てられます。

次のステップ

セキュリティ タグは、セキュリティ グループを操作するように設計されています。セキュリティ グループの作成の詳細については、セキュリティ グループの作成を参照してください。

セキュリティ タグの割り当ての変更

セキュリティ タグを作成すると、仮想マシンに手動で割り当てることができます。セキュリティ タグを編集して、セキュリティ タグをすでに割り当てた仮想マシンからタグを削除することもできます。

セキュリティ タグを作成済みの場合、それらを仮想マシンに割り当てることができます。セキュリティ タグを使用すると、ファイアウォール ルールを記述するための仮想マシンをグループ化できます。たとえば、機密性の高いデータがある仮想マシンのグループにセキュリティ タグを割り当てます。

手順

1 メイン メニュー (☰) から、[クラウド リソース] を選択します。

2 左側のパネルで [組織 VDC] をクリックします。

3 ターゲット組織仮想データセンターの横にあるラジオ ボタンをクリックして、[ファイアウォールの管理] をクリックします。

4 [セキュリティ タグ] タブをクリックします。

5 セキュリティ タグのリストから、編集するセキュリティ タグを選択し、[編集] () ボタンをクリックします。

6 左側のパネルから仮想マシンを選択し、右矢印をクリックしてセキュリティ タグを割り当てます。

右側のパネルの仮想マシンには、セキュリティ タグが割り当てられます。

7 右側のパネルで仮想マシンを選択し、左矢印をクリックしてタグを削除します。

左側のパネルの仮想マシンには、セキュリティ タグが割り当てられていません。

8 変更の追加を完了した後、[保持] をクリックします。

結果

セキュリティ タグが、選択した仮想マシンに割り当てられます。

次のステップ

セキュリティ タグは、セキュリティ グループを操作するように設計されています。セキュリティ グループの作成の詳細については、セキュリティ グループの作成を参照してください。

適用されているセキュリティ タグの表示

環境内の仮想マシンに適用されているセキュリティ タグを表示できます。また、環境内のセキュリティ グループに適用されているセキュリティ タグを表示することもできます。

前提条件

セキュリティ タグが作成され、仮想マシンまたはセキュリティ グループに適用されている必要があります。

手順

1 メイン メニュー (☰) から、[クラウド リソース] を選択します。

2 左側のパネルで [組織 VDC] をクリックします。

3 ターゲット組織仮想データセンターの横にあるラジオ ボタンをクリックして、[ファイアウォールの管理] をクリックします。

4 [セキュリティ タグ] タブから、割り当てられているタグを表示します。

   a [セキュリティ タグ] タブで割り当てを確認するセキュリティ タグを選択して、[編集] アイコンをクリックします。

   b [仮想マシンの割り当て/割り当て解除] で、セキュリティ タグに割り当てられている仮想マシンのリストを確認できます。

   c [破棄] をクリックします。

5 [セキュリティ グループ] タブで、割り当てられているタグを表示します。

   a [オブジェクトのグループ分け] タブをクリックし、[セキュリティ グループ] をクリックします。

   b セキュリティ グループを選択します。

   c [メンバーを含める] のリストから、セキュリティ グループに割り当てられているセキュリティ タグを確認できます。

結果

既存のセキュリティ タグのほか、関連付けられている仮想マシンおよびセキュリティ グループを表示できます。この方法で、セキュリティ タグとセキュリティ グループに基づき、ファイアウォール ルールの作成方針を決めることができます。

セキュリティ タグの編集

ユーザー定義のセキュリティ タグを編集できます。

仮想マシンの環境または機能を変更した場合は、別のセキュリティ タグを使用して、新しいマシン構成に対してファイアウォール ルールが適切となるようにすることもできます。たとえば、仮想マシンがある状態で、これ以上機密データを保存しない場合は、別のセキュリティ タグを割り当てて、機密データに適用されるファイアウォール ルールが仮想マシンに対して実行されないようにすることができます。

手順

1 メイン メニュー (☰) から、[クラウド リソース] を選択します。

2 左側のパネルで [組織 VDC] をクリックします。

3 ターゲット組織仮想データセンターの横にあるラジオ ボタンをクリックして、[ファイアウォールの管理] をクリックします。

4 [セキュリティ タグ] タブをクリックします。

5 セキュリティ タグのリストで、編集するセキュリティ タグを選択します。

6 [編集] () ボタンをクリックします。

7 セキュリティ タグの名前と説明を編集します。

8 選択した仮想マシンにタグを割り当てるか、割り当てを削除します。

9 変更内容を保存するには、[保持] をクリックします。

次のステップ

セキュリティ タグを編集すると、関連するセキュリティ グループまたはファイアウォール ルールの編集も必要になる場合があります。セキュリティ グループの詳細については、セキュリティ グループの操作を参照してください

。

セキュリティ タグの削除

ユーザー定義のセキュリティ タグを削除できます。

仮想マシンの機能または環境が変わった場合は、セキュリティ タグを削除できます。たとえば、Oracle データベースのセキュリティ タグがある状態で別のデータベース サーバを使用することにした場合にセキュリティ タグを削除できます。その場合、Oracle データベースに適用されるファイアウォール ルールは、仮想マシンに対して実行されなくなります。

手順

1 メイン メニュー (☰) から、[クラウド リソース] を選択します。

2 左側のパネルで [組織 VDC] をクリックします。

3 ターゲット組織仮想データセンターの横にあるラジオ ボタンをクリックして、[ファイアウォールの管理] をクリックします。

4 [セキュリティ タグ] タブをクリックします。

5 セキュリティ タグのリストから、削除するセキュリティ タグを選択します。

6 [削除] () ボタンをクリックします。

7 削除を確定するには、[OK] をクリックします。

結果

セキュリティ タグが削除されます。

次のステップ

セキュリティ タグを削除すると、関連するセキュリティ グループまたはファイアウォール ルールの編集も必要になる場合があります。セキュリティ グループの詳細については、「セキュリティ グループの操作」を参照してください。

Edge ゲートウェイの管理

7

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。Edge Gateway の再デプロイを参照してください。

重要： バージョン 9.7 以降では、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。

この章には、次のトピックが含まれています。

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 Gateway の再デプロイを参照してください。

Edge クラスタの環境の準備

1 vSphere で、ターゲット Edge クラスタのリソース プールを作成します。

   組織仮想データセンターで VLAN ネットワーク プールが使用されている場合は、この組織仮想データセンターの VLAN ネットワーク プールおよび Edge クラスタが同じ vSphere Distributed Switch に配置されている必要があります。

2 組織仮想データセンターで VXLAN ネットワーク プールが使用されている場合は、NSX で、VXLAN トランスポート ゾーンに Edge クラスタを追加し、その後で 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場合は、プライマリ Edge クラスタまたはセカンダリ Edge クラスタとして割り当てることができます。

セカンダリ Edge クラスタを割り当てない場合は、HA モードの Edge Gateway のスタンバイ Edge アプライアンスがプライマリ Edge クラスタにデプロイされますが、プライマリ Edge アプライアンスを実行しているホストとは異なるホストに配置されます。

組織仮想データセンター ネットワーク プロファイルを更新、表示、および削除するには、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 Gateway の再デプロイを参照してください。

Edge ゲートウェイの追加

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 バランシング、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 9.7 以降では、Edge Gateway は、事前に作成されて組織仮想データセンターに割り当てられた Edge クラスタにデプロイされます。

1 つ以上の外部ネットワークに接続する IPv4 または IPv6 Edge ゲートウェイを追加できます。

注： IPv6 Edge ゲートウェイではサポートされるサービスが制限されます。IPv6 Edge Gateway は Edge ファイアウォール、分散ファイアウォール、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 メイン メニュー (☰) から、[クラウド リソース] を選択します。

2 左側のペインで、[Edge ゲートウェイ] をクリックし、[新規] をクリックします。

3 Edge ゲートウェイを作成する組織仮想データセンターの名前の横にあるラジオ ボタンをクリックして、[次へ] をクリックします。

4 新しい Edge ゲートウェイの名前と、オプションで説明を入力します。

5 全般的な Edge ゲートウェイの設定をそれぞれ有効にするか、無効のままにします。

全般設定	説明
分散ルーティング	分散論理ルーティングを指定するよう Edge ゲートウェイを構成します。
FIPS モード	NSX FIPS モードを使用するよう Edge ゲートウェイを構成します。
高可用性	バックアップ Edge ゲートウェイへの自動フェイルオーバーを有効にします。

6 システム リソースの Edge ゲートウェイ構成を選択して、[次へ] をクリックします。

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 リソースが少なくて済みます。
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使用します。
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。

7 Edge ゲートウェイが接続できる外部ネットワークから 1 つ以上のサブネットを選択し、[次へ] をクリックします。

Edge クラスタが組織仮想データセンターに割り当てられていると、表示されるリストには、この Edge クラスタからアクセス可能な外部ネットワークが含まれます。

8 （オプション） ネットワークをデフォルト ゲートウェイとして構成します。

a [デフォルト ゲートウェイの構成] 切り替えを有効にします。

b ターゲット外部ネットワークの名前の横にあるラジオ ボタンを選択し、宛先 IP アドレスの横にあるラジオ ボタンを選択します。

c （オプション） [DNS リレーにデフォルト ゲートウェイを使用] 切り替えを有効にします。

9 [次へ] をクリックします。

10 詳細 Edge ゲートウェイの設定をそれぞれ有効にするか、無効のままにして、[次へ] をクリックします。

詳細設定	説明
IP アドレス設定	Edge Gateway の各サブネットの IP アドレスを手動で指定できます。
IP プールの細分割り当て	Edge ゲートウェイ上の各外部ネットワークの使用可能な IP アドレス プールを複数の固定 IP アドレス プールに細分割り当てすることができます。
レート制限	Edge ゲートウェイのそれぞれの外部ネットワークについて着信および発信のレート制限を設定できます。

11 （オプション） 手順 手順 10 で 1 つ以上の詳細設定を有効にした場合は、有効にした各設定を適用します。

詳細設定	ステップ
[IP アドレス設定]	Edge Gateway のネットワークごとに、[IP アドレス] セルに IP アドレスを入力し、[次へ] をクリックします。 ネットワークの IP アドレスを入力しない場合は、このネットワークに任意の IP アドレスが割り当てられます。
[IP プールの細分割り当て]	1 外部ネットワーク名の横にあるラジオ ボタンをクリックして、[編集] をクリックします。 この外部ネットワークに使用可能な IP アドレス プールと、現在細分割り当てされている IP アドレス プール（設定されている場合）が表示されます。 2 この外部ネットワークに細分割り当てされている IP アドレス プールを編集し、[保存] をクリックします。 使用可能な IP アドレス プールの範囲から IP アドレスと IP アドレス範囲を追加できます。 3 [保存] をクリックします。 システムは重複する IP アドレス範囲を結合します。 4 [次へ] をクリックします。 **注：** Edge Gateway への IP アドレスの割り当ては、プロバイダが IP アドレスの所有権をゲートウェイに割り当てるプロセスです。vCloud Director の割り当てプロセス中に、該当するゲートウェイ インターフェイスにセカンダリ アドレスが自動的に設定されます。IP アドレスのいずれかが vCloud Director の外部で使用されている場合は、IP アドレスが競合する可能性があります。
[レート制限]	Edge Gateway 上の外部ネットワークごとに、[有効化] 切り替えを有効にし、[着信レート] セルおよび [発信レート] セルに制限を入力して、[次へ] をクリックします。

12 [設定内容の確認] 画面の内容を確認し、[完了] をクリックします。

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 ファイアウォールの管理

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

組織仮想データセンター内の仮想マシン間で移動するトラフィックの保護方法については、組織仮想データセンターの分散ファイアウォールの管理を参照してください。

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

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

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

2 ユーザー定義ルール。

3 デフォルト ルール。

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

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

Edge Gateway ファイアウォール ルールの追加

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

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

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

手順

1 Edge Gateway サービスを開きます。

   a メイン メニュー (☰) から、[クラウド リソース] を選択します。

   b 左側のパネルで [Edge ゲートウェイ] をクリックします。

   c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[サービス] をクリックします。

2 [ファイアウォール ルール] 画面が表示されない場合は、[ファイアウォール] タブをクリックします。

3 ファイアウォール ルール テーブルで既存のルールの下にルールを追加するには、その既存の行をクリックし、[作成] ボタンをクリックします。

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

4 [名前] セルをクリックし、名前を入力します。

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

オプション	説明
[IP] アイコンをクリック	使用するソースの値を入力します。有効な値は、IP アドレス、CIDR、IP アドレス範囲、またはキーワード **any** です。Edge ゲートウェイ ファイアウォールは、IPv4 と IPv6 の両方の形式をサポートしています。
[+] アイコンをクリック	[+] アイコンを使用し、特定の IP アドレス以外のオブジェクトをソースとして次のように指定します。 ■ [オブジェクトの選択] ウィンドウを使用し、選択内容に一致するオブジェクトを追加し、[保持] をクリックしてそれらをルールに追加します。 ■ ソースをルールから除外するには、[オブジェクトの選択] ウィンドウを使用してこのルールに追加し、次に除外の切り替えアイコンを選択してそのソースをこのルールから除外します。 ソースで除外の切り替えを選択すると、すべてのソース（除外したソースを除く）から受信するトラフィックにルールが適用されます。除外の切り替えを選択しない場合、[オブジェクトの選択] ウィンドウで指定したソースから受信するトラフィックにルールが適用されます。

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

オプション	説明
[IP] アイコンをクリック	使用するターゲットの値を入力します。有効な値は、IP アドレス、CIDR、IP アドレス範囲、またはキーワード **any** です。Edge ゲートウェイ ファイアウォールは、IPv4 と IPv6 の両方の形式をサポートしています。
[+] アイコンをクリック	[+] アイコンを使用し、特定の IP アドレス以外のオブジェクトをソースとして次のように指定します。 ■ [オブジェクトの選択] ウィンドウを使用し、選択内容に一致するオブジェクトを追加し、[保持] をクリックしてそれらをルールに追加します。 ■ ソースをルールから除外するには、[オブジェクトの選択] ウィンドウを使用してこのルールに追加し、次に除外の切り替えアイコンを選択してそのソースをこのルールから除外します。 ソースで除外の切り替えを選択すると、すべてのソース（除外したソースを除く）から受信するトラフィックにルールが適用されます。除外の切り替えを選択しない場合、[オブジェクトの選択] ウィンドウで指定したソースから受信するトラフィックにルールが適用されます。

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

a サービス プロトコルを選択します。

b ソース ポートとターゲット ポートのポート番号を入力するか、**任意** を指定します。

c [保持] をクリックします。

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

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

9 [変更を保存] をクリックします。

保存操作が完了するまでに 1 分ほどかかることがあります。

Edge Gateway ファイアウォール ルールの変更

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

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

手順

1 Edge Gateway サービスを開きます。

a メイン メニュー (☰) から、[クラウド リソース] を選択します。

b 左側のパネルで [Edge ゲートウェイ] をクリックします。

c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[サービス] をクリックします。

2 [ファイアウォール] タブをクリックします。

3 ファイアウォール ルールを管理します。

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

4 [変更を保存] をクリックします。

Edge ゲートウェイへの Syslog サーバー設定の適用

1 つ以上の Edge Gateway ファイアウォール ルールのログを有効にした場合、Edge Gateway は Syslog サーバに接続されます。Syslog サーバの初期構成の前に Edge Gateway を作成した場合、または Syslog サーバの設定を変更した場合は、この Edge Gateway の Syslog サーバ設定を同期する必要があります。

手順

1 メイン メニュー (☰) から、[クラウド リソース] を選択します。

2 左側のパネルで [Edge ゲートウェイ] をクリックします。

3 ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[Syslog の同期] をクリックします。

4 確認するには、[OK] をクリックします。

Edge Gateway の DHCP の管理

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

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

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

- DHCP 検出のために Edge Gateway の内部インターフェイスで待機します。
- すべてのクライアントのデフォルト ゲートウェイ アドレスとして、Edge Gateway の内部インターフェイスの IP アドレスを使用します。
- コンテナ ネットワークに対し、内部インターフェイスのブロードキャストとサブネット マスクの値を使用します。

次の状況では、DHCP が割り当てられた IP アドレスを持つクライアント仮想マシンで DHCP サービスを再起動する必要があります。

- DHCP プール、デフォルト ゲートウェイ、または DNS サーバを変更または削除した場合。
- Edge ゲートウェイ インスタンスの内部 IP アドレスを変更した場合。

注： DHCP 対応の Edge ゲートウェイ上の DNS 設定を変更すると、Edge ゲートウェイは DHCP サービスを提供しなくなります。このような状況が発生した場合は、[DHCP プール] 画面の [DHCP サービスのステータス] 切り替えを使用して、その Edge ゲートウェイの DHCP を無効にしてから再度有効にします。DHCP IP プールの追加 を参照してください。

DHCP IP プールの追加

詳細 Edge Gateway の DHCP サービスに必要な IP プールは構成することができます。DHCP は、組織仮想データセンター ネットワークに接続された仮想マシンへの IP アドレスの割り当てを自動化します。

『NSX 管理ガイド』に説明されているとおり、DHCP サービスには IP アドレスのプールが必要です。IP プールとは、ネットワーク内の連続した IP アドレスの範囲です。アドレス バインディングを持たない Edge ゲートウェイによって保護されている仮想マシンには、このプールから IP アドレスが割り当てられます。IP プールの範囲が互いに交わることはないため、1 つの IP アドレスが属することができるのは 1 つの IP プールのみです。

注： DHCP サービスのステータスをオンにするには、少なくとも 1 つの DHCP IP プールを設定する必要があります。

手順

1 Edge Gateway サービスを開きます。

   a メイン メニュー (☰) から、[クラウド リソース] を選択します。

   b 左側のパネルで [Edge ゲートウェイ] をクリックします。

   c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[サービス] をクリックします。

2 [DHCP] - [プール] の順に移動します。

3 DHCP サービスが現在有効でない場合は、[DHCP サービスのステータス] の切り替えをオンにします。

   注： [DHCP サービスのステータス] の切り替えをオンにした後には、変更を保存する前に少なくとも 1 つの DHCP IP アドレス プールを追加します。画面に DHCP IP プールが表示されておらず、[DHCP サービスのステータス] の切り替えをオンにして変更内容を保存する場合には、画面は切り替えがオフになって表示されます。

4 DHCP プールで、[作成] () ボタンをクリックし、DHCP プールの詳細を指定して [保持] をクリックします。

オプション	説明
IP の範囲	IP アドレスの範囲を入力します。
ドメイン名	DNS サーバのドメイン名。
DNS の自動構成	この IP プールの DNS バインディングに DNS サービス構成を使用するには、この切り替えを有効にします。 有効にすると、[プライマリ ネーム サーバ] と [セカンダリ ネーム サーバ] は [自動] に設定されます。
プライマリ ネーム サーバ	[DNS の自動構成] を有効にしない場合は、プライマリ DNS サーバの IP アドレスを入力します。 この IP アドレスは、ホスト名 - IP アドレス解決のために使用されます。
セカンダリ ネーム サーバ	[DNS の自動構成] を有効にしない場合は、セカンダリ DNS サーバの IP アドレスを入力します。 この IP アドレスは、ホスト名 - IP アドレス解決のために使用されます。
デフォルト ゲートウェイ	デフォルト ゲートウェイ アドレスを入力します。 デフォルト ゲートウェイ IP アドレスを指定しない場合は、Edge ゲートウェイ インスタンスの内部インターフェイスがデフォルト ゲートウェイとして使用されます。
サブネット マスク	Edge Gateway インターフェイスのサブネット マスクを入力します。

オプション	説明
リースには有効期限がありません	このプールから割り当てられた IP アドレスが、割り当てられている仮想マシンに永続的にバインドされるようにするには、この切り替えを有効にします。 このオプションを選択すると、[リース時間] は無限に設定されます。
リース時間 (秒)	DHCP 割り当ての IP アドレスがクライアントにリースされる時間の長さ（秒単位）。 デフォルトのリース時間は、1 日（86,400 秒）です。 **注：** [リースには有効期限がありません] を選択すると、リース時間を指定することはできません。

5 [変更を保存] をクリックします。

結果

vCloud Director は、DHCP サービスを提供するために Edge ゲートウェイを更新します。

DHCP バインディングの追加

サービスが動作中の仮想マシンで、IP アドレスが変更されないようにする場合は、仮想マシンの MAC アドレスを IP アドレスにバインドできます。バインドする IP アドレスは、DHCP IP プールと重複しないようにしてください。

前提条件

バインディングを設定する仮想マシンの MAC アドレスを手元に控えておきます。

手順

1 Edge Gateway サービスを開きます。

a メイン メニュー (☰) から、[クラウド リソース] を選択します。

b 左側のパネルで [Edge ゲートウェイ] をクリックします。

c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[サービス] をクリックします。

2 [DHCP] - [バインディング] タブで [作成] () ボタンをクリックして、バインディングの詳細を指定し、[保持] をクリックします。

オプション	説明
MAC アドレス	IP アドレスにバインドする仮想マシンの MAC アドレスを入力します。
ホスト名	仮想マシンが DHCP リースを要求するときに、その仮想マシンに設定するホスト名を入力します。
IP アドレス	MAC アドレスにバインドする IP アドレスを入力します。
サブネット マスク	Edge Gateway インターフェイスのサブネット マスクを入力します。
ドメイン名	DNS サーバのドメイン名を入力します。

オプション	説明
DNS の自動構成	この DNS バインディングに DNS サービス構成を使用するには、この切り替えを有効にします。 有効にすると、[プライマリ ネーム サーバ] と [セカンダリ ネーム サーバ] は [自動] に設定されます。
プライマリ ネーム サーバ	[DNS の自動構成] を選択しない場合は、プライマリ DNS サーバの IP アドレスを入力します。 この IP アドレスは、ホスト名 - IP アドレス解決のために使用されます。
セカンダリ ネーム サーバ	[DNS の自動構成] を選択しない場合は、セカンダリ DNS サーバの IP アドレスを入力します。 この IP アドレスは、ホスト名 - IP アドレス解決のために使用されます。
デフォルト ゲートウェイ	デフォルト ゲートウェイ アドレスを入力します。 デフォルト ゲートウェイ IP アドレスを指定しない場合は、Edge ゲートウェイ インスタンスの内部インターフェイスがデフォルト ゲートウェイとして使用されます。
リースには有効期限がありません	IP アドレスがその MAC アドレスに永続的にバインドされるようにするには、この切り替えを有効にします。 このオプションを選択すると、[リース時間] は無限に設定されます。
リース時間 (秒)	DHCP 割り当ての IP アドレスがクライアントにリースされる時間の長さ（秒単位）。 デフォルトのリース時間は、1 日（86,400 秒）です。 **注：** [リースには有効期限がありません] を選択すると、リース時間を指定することはできません。

3 [変更を保存] をクリックします。

Edge ゲートウェイの DHCP リレーの設定

vCloud Director 環境の NSX が提供する DHCP リレー機能により、既存の DHCP インフラストラクチャでの IP アドレス管理を中断せずに、vCloud Director 環境内で既存の DHCP インフラストラクチャを活用できます。DHCP メッセージは、仮想マシンから、物理 DHCP インフラストラクチャにある指定された DHCP サーバにリレーされます。これにより、NSX ソフトウェアが制御する IP アドレスは、DHCP 制御された環境内にある他の IP アドレスと引き続き同期されます。

Edge Gateway の DHCP リレー構成では、複数の DHCP サーバをリストできます。要求は、リストされたすべてのサーバに送信されます。仮想マシンから DHCP 要求をリレーする間、Edge ゲートウェイはゲートウェイの IP アドレスを要求に追加します。外部 DHCP サーバはこのゲートウェイ アドレスを使用してプールを照合し、要求の IP アドレスを割り当てます。ゲートウェイ アドレスは、Edge Gateway のインターフェイスのサブネットに属している必要があります。

各 Edge ゲートウェイには異なる DHCP サーバを構成できるほか、各 Edge ゲートウェイでは、複数の IP アドレスのドメインに対応するため、複数の DHCP サーバを構成できます。

注：

- DHCP リレーでは、重複する IP アドレス空間はサポートされません。
- DHCP リレーと DHCP サービスを同じ vNIC で同時に実行することはできません。vNIC にリレー エージェントが構成されている場合、その vNIC のサブネットで DHCP プールを構成することはできません。詳細については、『NSX 管理ガイド』を参照してください。

Edge Gateway の DHCP リレー構成の指定

vCloud Director 環境内の NSX ソフトウェアにより、Edge Gateway は vCloud Director 組織仮想データセンターの外部にある DHCP サーバに DHCP メッセージをリレーできます。Edge Gateway の DHCP リレー機能を設定できます。

『NSX 管理ガイド』で説明するように、既存の IP アドレス セット、IP アドレスのブロック、ドメイン、またはこれらのすべての組み合わせを使用して、DHCP サーバを指定できます。DHCP メッセージは、指定した各 DHCP サーバにリレーされます。

少なくとも 1 つの DHCP リレー エージェントを設定する必要があります。DHCP リレー エージェントは、DHCP リクエストを外部 DHCP サーバにリレーする Edge ゲートウェイ上のインターフェイスです。

前提条件

IP セットを使用して DHCP サーバを指定する場合は、その IP セットを Edge Gateway がオブジェクトのグループ分けに使用できることを確認します。ファイアウォール ルールと DHCP リレー設定で使用するための IP アドレス セットの作成を参照してください。

手順

1 Edge Gateway サービスを開きます。

   a メイン メニュー (☰) から、[クラウド リソース] を選択します。

   b 左側のパネルで [Edge ゲートウェイ] をクリックします。

   c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[サービス] をクリックします。

2 [DHCP] - [リレー] の順に移動します。

3 画面に表示されるフィールドを使用して、IP アドレス、ドメイン名、または IP アドレス セットで DHCP サーバを指定します。

   [追加] (+) ボタンを使用して、既存の IP セットから利用できる IP セットを選択します。

4 DHCP リレー エージェントを設定し、その設定を画面上のテーブルに追加するには、[追加] () ボタンをクリックし、vNIC とそのゲートウェイ IP アドレスを選択し、[保持] をクリックします。

デフォルトで、ゲートウェイ IP アドレスは選択されている vNIC のプライマリ アドレスと一致します。デフォルトを保持できるほか、その vNIC で代替アドレスを使用可能な場合にはそれを選択できます。

5 [変更を保存] をクリックします。

SNAT または DNAT ルールの追加

ソース IP アドレスをパブリックからプライベート IP アドレスへ、またはその逆方向へ変更するには、ソース NAT (SNAT) ルールを作成します。ターゲット IP アドレスをパブリックからプライベート IP アドレスへ、またはその逆方向へ変更するには、ターゲット NAT (DNAT) ルールを作成します。

NAT ルールを作成するときには、次の形式を使用して、元の IP アドレスと変換先の IP アドレスを指定できます。

- IP アドレス。たとえば、192.0.2.0 とします。
- IP アドレス範囲。たとえば、192.0.2.0-192.0.2.24 とします。
- IP アドレス/サブネット マスク。たとえば、192.0.2.0/24 とします。
- any

vCloud Director 環境の Edge Gateway で SNAT ルールまたは DNAT ルールを設定する場合は、常に組織仮想データセンターの観点からルールを設定します。SNAT ルールでは、組織仮想データセンター ネットワークから外部ネットワークまたは別の組織仮想データセンター ネットワークに送信されるパケットのソース IP アドレスを変換します。DNAT ルールでは、外部ネットワークまたは別の組織仮想データセンター ネットワークから送信されて組織仮想データセンター ネットワークで受信されるパケットの IP アドレスを変換し、オプションでそのポートを変換します。

前提条件

パブリック IP アドレスを、ルールを追加する Edge ゲートウェイインターフェイスに追加しておく必要があります。DNAT ルールの場合、元の（パブリック）IP アドレスを Edge ゲートウェイ インターフェイスに追加しておく必要があります。SNAT ルールの場合、変換先の（パブリック）IP アドレスを Edge ゲートウェイ インターフェイスに追加しておく必要があります。

手順

1 Edge Gateway サービスを開きます。

a メイン メニュー (☰) から、[クラウド リソース] を選択します。

b 左側のパネルで [Edge ゲートウェイ] をクリックします。

c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[サービス] をクリックします。

2 [NAT] をクリックして、[NAT ルール] 画面を表示します。

3 どのタイプの NAT ルールを作成しているかに応じて、[DNAT ルール] または [SNAT ルール] をクリックします。

4 ターゲット NAT ルール（外部から内部へ）を設定します。

オプション	説明
適用対象	ルールを適用するインターフェイスを選択します。
元の IP/範囲	必要な IP アドレスを入力します。 このアドレスは、DNAT ルールを設定する Edge ゲートウェイのパブリック IP アドレスにする必要があります。検査対象のパケットでは、この IP アドレスまたはアドレス範囲がパケットのターゲット IP アドレスとして表示されます。これらのパケット ターゲット アドレスは、この DNAT ルールによって変換されたものです。
プロトコル	ルールを適用するプロトコルを選択します。このルールをすべてのプロトコルに適用するには、[任意] を選択します。
元のポート	（オプション）仮想マシンが接続されている内部ネットワークに接続するために Edge ゲートウェイで受信トラフィックが使用するポートまたはポート範囲を選択します。これは、[プロトコル] が [ICMP] または [任意] に設定されているときには選択できません。
ICMP タイプ	[プロトコル] に [ICMP]（デバイス間でエラー情報を通信するために使用されるエラー報告と診断のユーティリティ）を選択する場合は、ドロップダウン メニューから [ICMP タイプ] を選択します。 ICMP メッセージは、タイプのフィールドで識別されます。デフォルトで、[ICMP タイプ] は [任意] に設定されています。
変換された IP/範囲	着信パケット上のターゲット アドレスの変換先となる IP アドレスまたは IP アドレス範囲を入力します。 これらのアドレスは、外部ネットワークからトラフィックを受信できるように DNAT を設定している 1 台以上の仮想マシンの IP アドレスです。
変換されたポート	（オプション）内部ネットワークの仮想マシン上で着信トラフィックが接続しているポートまたはポート範囲を選択します。仮想マシンに着信したパケットは、DNAT ルールによってこれらのポートに変換されます。
説明	（オプション）このルールで何を識別するのかがわかるように説明を入力します。
有効	このルールを有効にするには、オンに切り替えます。
ログの有効化	このルールによって実行されたアドレス変換をログに記録するには、オンにします。

5 ソース NAT ルール（内部から外部へ）を設定します。

オプション	説明
適用対象	ルールを適用するインターフェイスを選択します。
元のソース IP/範囲	このルールに適用する元の IP アドレスまたは IP アドレス範囲を入力します。 これらのアドレスは、外部ネットワークにトラフィックを送信できるように SNAT ルールを設定している 1 台以上の仮想マシンの IP アドレスです。
変換されたソース IP/範囲	必要な IP アドレスを入力します。 このアドレスは、常に SNAT ルールを設定するゲートウェイのパブリック IP アドレスにする必要があります。外部ネットワークにトラフィックを送信するときに、発信パケット上のソース アドレス（仮想マシン）が変換される IP アドレスを指定します。
説明	（オプション）このルールで何を識別するのかがわかるように説明を入力します。
有効	このルールを有効にするには、オンに切り替えます。
ログの有効化	このルールによって実行されたアドレス変換をログに記録するには、オンにします。

6 [保持] をクリックして、画面上のテーブルにルールを追加します。

7 設定するルールごとに、この手順を繰り返します。

8 [変更を保存] をクリックして、システムにルールを保存します。

次のステップ

設定した SNAT ルールまたは DNAT ルールに対応する Edge ゲートウェイ ファイアウォール ルールを追加します。Edge Gateway ファイアウォール ルールの追加を参照してください。

高度なルーティングの設定

NSX ソフトウェアによって提供されるスタティック ルーティングおよび動的ルーティング機能を Edge Gateway に設定できます。

動的ルーティングを有効にするには、Border Gateway Protocol (BGP) または Open Shortest Path First (OSPF) プロトコルを使用して詳細 Edge ゲートウェイを設定します。

NSX が提供するルーティング機能の詳細については、『NSX 管理ガイド』の「ルーティング」を参照してください。

詳細 Edge ゲートウェイごとにスタティック ルーティングおよび動的ルーティングを指定できます。動的ルーティング機能は、レイヤー 2 ブロードキャスト ドメイン間で必要な転送情報を提供します。これにより、レイヤー 2 ブロードキャスト ドメインを削減し、ネットワークの効率を高め、規模を拡大することができます。NSX は、このインテリジェンスを East-West ルーティングのワークロードがある場所まで拡張します。この機能により、余分なコストや時間をかけずにホップを拡張して、仮想マシン間でより直接的な通信を実現できます。

Edge ゲートウェイのデフォルトのルーティング設定の指定

Edge ゲートウェイに対して、スタティック ルーティングおよび動的ルーティングのデフォルト設定を指定できます。

注： 設定されているすべてのルーティング設定を削除するには、[ルーティング設定] 画面の下部にある [グローバル構成をクリア] ボタンを使用します。このアクションにより、デフォルトのルーティング設定、スタティック ルート、OSPF、BGP、ルート再配分の各サブ画面で現在指定されているすべてのルーティング設定が削除されます。

手順

1 Edge Gateway サービスを開きます。

   a メイン メニュー (☰) から、[クラウド リソース] を選択します。

   b 左側のパネルで [Edge ゲートウェイ] をクリックします。

   c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[サービス] をクリックします。

2 [ルーティング] - [ルーティング設定] の順に選択します。

3 この Edge ゲートウェイで等価コスト マルチパス (ECMP) ルーティングを有効にするには、[ECMP] 切り替えをオンにします。

『NSX 管理』ドキュメントで説明されているとおり、ECMP は、単一のターゲットへのネクスト ホップ パケット転送が複数のベスト パスで行われるようにするルーティング戦略です。NSX は、これらのベスト パスの決定を、統計に基づくか、設定済みのスタティック ルートを使用するか、または OSPF や BGP などの動的ルーティング プロトコルによるメトリック計算の結果として行います。[スタティック ルート] 画面で複数のネクスト ホップを指定することで、スタティック ルートに対する複数のパスを指定できます。

ECMP と NSX の詳細については、『NSX トラブルシューティング ガイド』のルーティングに関するトピックを参照してください。

4 デフォルトのルーティング ゲートウェイの設定を指定します。

a [適用対象] ドロップ ダウン リストを使用して、ターゲット ネットワークに向かうネクスト ホップに到達できるインターフェイスを選択します。

選択したインターフェイスの詳細を表示するには、青い情報アイコンをクリックします。

b ゲートウェイ IP アドレスを入力します。

c MTU を入力します。

d （オプション） オプションで、説明を入力します。

e [変更を保存] をクリックします。

5 デフォルトの動的ルーティング設定を指定します。

注： 環境で IPsec VPN を設定してある場合は、動的ルーティングを使用しないでください。

a ルーター ID を選択します。

リストからルーター ID を選択するか、[+] アイコンを使用して新しいルーター ID を入力します。このルーター ID は、動的ルーティングのためにルートをカーネルにプッシュする Edge ゲートウェイの最初のアップリンク IP アドレスになります。

b [ログの有効化] 切り替えをオンにし、ログ レベルを選択することにより、ログ記録を設定します。

c [OK] をクリックします。

6 [変更を保存] をクリックします。

次のステップ

スタティック ルートを追加します。スタティック ルートの追加を参照してください。

ルート再配分を設定します。ルート再配分の設定を参照してください。

動的ルーティングを設定します。次のトピックを参照してください。

- BGP の設定
- OSPF の設定

スタティック ルートの追加

宛先のサブネットまたはホストにスタティック ルートを追加できます。

デフォルトのルーティング設定で ECMP が有効になっている場合は、スタティック ルートに複数のネクスト ホップを指定できます。ECMP を有効にする手順については、Edge ゲートウェイのデフォルトのルーティング設定の指定を参照してください。

前提条件

NSX のドキュメントで説明されているとおり、スタティック ルートのネクスト ホップ IP アドレスは、Edge Gateway のインターフェイスのいずれかに関連付けられているサブネット内に存在している必要があります。異なる場合、そのスタティック ルートの設定は失敗します。

手順

1 Edge Gateway サービスを開きます。

   a メイン メニュー (☰) から、[クラウド リソース] を選択します。

   b 左側のパネルで [Edge ゲートウェイ] をクリックします。

   c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[サービス] をクリックします。

2 [ルーティング] - [スタティック ルート] の順に移動します。

3 [作成] (+) ボタンをクリックします。

4 スタティック ルートの次のオプションを設定します。

オプション	説明
ネットワーク	ネットワークを CIDR 表記で入力します。
ネクスト ホップ	ネクスト ホップの IP アドレスを入力します。 ネクスト ホップ IP アドレスは、Edge Gateway のインターフェイスのいずれかに関連付けられているサブネット内に存在している必要があります。 ECMP が有効になっている場合は、複数のネクスト ホップを入力できます。
MTU	データ パケットの最大転送値を編集します。 MTU 値は、選択された Edge ゲートウェイ インターフェイスに設定された MTU 値を超える値にすることはできません。デフォルトでは、[ルーティング設定] 画面に、Edge ゲートウェイ インターフェイスで設定された MTU を表示できます。
インターフェイス	オプションで、スタティック ルートを追加する Edge ゲートウェイ インターフェイスを選択します。デフォルトで、ネクスト ホップのアドレスに一致するインターフェイスが選択されます。
説明	オプションで、スタティック ルートの説明を入力します。

5 [変更を保存] をクリックします。

次のステップ

スタティック ルートの NAT ルールを設定します。SNAT または DNAT ルールの追加を参照してください。

トラフィックがスタティック ルートを経由することを許可するファイアウォール ルールを追加します。Edge Gateway ファイアウォール ルールの追加を参照してください。

OSPF の設定

Edge ゲートウェイの動的ルーティング機能を使用するように、Open Shortest Path First (OSPF) ルーティング プロトコルを設定できます。vCloud Director 環境に置かれた Edge ゲートウェイの OSPF は、一般に、vCloud Director の Edge ゲートウェイ間でルーティング情報を交換する目的に使用されます。

NSX Edge ゲートウェイがサポートする OSPF は、単一のルーティング ドメイン内のみで IP パケットをルーティングする Interior Gateway Protocol です。『NSX 管理ガイド』に記載されているように、NSX Edge Gateway に OSPF を設定すると、Edge Gateway はルートを学習して通知できるようになります。Edge ゲートウェイは OSPF を使用して、使用可能な Edge ゲートウェイからリンク状態に関する情報を収集し、ネットワークのトポロジ マッピングを構築します。このトポロジによって、インターネット レイヤーに提供されるルーティング テーブルが決まり、IP パケット内にあるターゲット IP アドレスに基づいてルーティングに関する決定が行われます。

その結果、OSPF ルーティング ポリシーはコストが等しいルート間でトラフィックのロード バランシングを動的に処理できるようになります。OSPF ネットワークは、トラフィック フローを最適化して、ルーティング テーブルのサイズを制限するために、複数のルーティング領域に分割されています。領域とは、同じ領域 ID を持つ OSPF ネットワーク、ルーター、およびリンクの論理的な集合のことです。領域は領域 ID で識別されます。

前提条件

ルーター ID を設定する必要があります。Edge ゲートウェイのデフォルトのルーティング設定の指定。

手順

1 Edge Gateway サービスを開きます。

   a メイン メニュー (☰) から、[クラウド リソース] を選択します。

   b 左側のパネルで [Edge ゲートウェイ] をクリックします。

   c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[サービス] をクリックします。

2 [ルーティング] - [OSPF] の順に移動します。

3 OSPF が現在有効でない場合は、[OSPF の有効化] 切り替えを使用して、OSPF を有効にします。

4 組織のニーズに合わせて OSPF 設定を行います。

オプション	説明
グレースフル リスタートの有効化	OSPF サービスの再起動時にパケット転送が中断されないように指定します。
デフォルトの広告の有効化	Edge ゲートウェイが OSPF ピアに自分自身をデフォルト ゲートウェイとして通知できるようにします。

5 (オプション) [変更を保存] をクリックするか、または引き続き領域の定義やインターフェイス マッピングを設定することができます。

6 [追加] () ボタンをクリックし、OSPF エリア定義を追加します。ダイアログ ボックスでマッピングの詳細を指定し、[保持] をクリックします。

注： デフォルトでは、領域 ID が 51 の Not-So-Stubby Area (NSSA) が設定されます。この領域は OSPF 画面の領域定義テーブルに自動的に表示されます。NSSA 領域を変更または削除できます。

オプション	説明
領域 ID	領域 ID を IP アドレスまたは 10 進数の形式で入力します。
領域タイプ	[標準] または [NSSA] を選択します。 NSSA は、AS 外部の Link-State Advertisement (LSA) が NSSA に大量に送信されるのを防ぎます。NSSA は外部ターゲットへのデフォルト ルーティングを利用します。そのため、NSSA は OSPF ルーティング ドメインのエッジに配置する必要があります。NSSA は外部ルートを OSPF ルーティング ドメインにインポートできます。これにより、OSPF ルーティング ドメインに属さない小規模なルーティング ドメインにトランジット サービスを提供することができます。
領域認証	OSPF が領域レベルで実行する認証タイプを選択します。 領域内のすべての Edge ゲートウェイに、同一の認証と対応するパスワードを設定しておく必要があります。MD5 認証を有効にするには、レシーバとトランスミッタの両方に同じ MD5 キーが必要です。 選択肢は次のとおりです。 ■ [なし] 認証は不要です。 ■ [パスワード] このオプションを選択した場合は、[領域認証値] フィールドで指定したパスワードが送信パケットに含まれます。 ■ [MD5] このオプションを選択した場合、認証には MD5 (Message Digest type 5) 暗号化が使用されます。MD5 チェックサムが送信パケットに含まれます。[領域認証値] フィールドに MD5 キーを入力します。

7 [変更を保存] をクリックして、インターフェイス マッピングを追加するときに、新たに設定した領域定義を選択できるようにします。

8 [追加] () ボタンをクリックし、インターフェイスのマッピングを追加します。ダイアログ ボックスでマッピングの詳細を指定し、[保持] をクリックします。

これらのマッピングによって、Edge Gateway のインターフェイスが領域にマップされます。

a ダイアログ ボックスで、領域定義にマッピングするインターフェイスを選択します。

このインターフェイスによって、両方の Edge ゲートウェイの接続先となる外部ネットワークが指定されます。

b 選択したインターフェイスにマッピングする領域の領域 ID を選択します。

c （オプション） OSPF の設定をデフォルト値から変更し、このインターフェイスのマッピングに合わせてカスタマイズします。

新しいマッピングを設定するときには、これらの設定のデフォルト値が表示されます。通常は、デフォルト設定をそのまま使用することをお勧めします。設定を変更する場合は、OSPF ピアで同じ設定が使用されることを確認してください。

オプション	説明
Hello 間隔	インターフェイスに送信される Hello パケットの間隔（秒）です。
Dead 間隔	少なくとも 1 つの Hello パケットをネイバーから受信してから、ネイバーが停止していると宣言されるまでの間隔（秒）です。
優先度	インターフェイスの優先度です。優先順位が最高のインターフェイスが、Edge ゲートウェイ ルーターに指定されます。
コスト	該当するインターフェイスを越えてパケットを送信するために必要なオーバーヘッドです。インターフェイスのコストは、そのインターフェイスのバンド幅に反比例します。バンド幅が大きくなるほど、コストは小さくなります。

d [保持] をクリックします。

9 OSPF 画面で [変更を保存] をクリックします。

次のステップ

ルーティング情報の交換相手となる他の Edge ゲートウェイで、OSPF を設定します。

OSPF 対応 Edge ゲートウェイ間のトラフィックを許可するファイアウォール ルールを追加します。Edge Gateway ファイアウォール ルールの追加を参照してください。

ルートの再分散およびファイアウォール設定を使用して正しいルートを通知できることを確認します。ルート再配分の設定を参照してください。

BGP の設定

Edge Gateway の動的ルーティング機能を使用するように Border Gateway Protocol (BGP) を設定できます。

『NSX 管理ガイド』に記載されているように、BGP は、複数の自律システム間のネットワーク到達可能性を指定する IP ネットワークまたはプレフィックスのテーブルを使用することでルーティングを決定します。ネットワークの分野では、BGP スピーカーという用語は、BGP を実行しているネットワーク デバイスを表します。2 つの BGP スピーカーが接続を確立してから、ルーティング情報が交換されます。BGP ネイバーという用語は、接続などを確立した BGP スピーカーを表します。接続を確立すると、デバイスはルートを交換して、テーブルを同期させます。各デバイスはキープ アライブ メッセージを送信して、この関係を維持します。

手順

1 Edge Gateway サービスを開きます。

   a メイン メニュー (☰) から、[クラウド リソース] を選択します。

   b 左側のパネルで [Edge ゲートウェイ] をクリックします。

   c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[サービス] をクリックします。

2 [ルーティング] - [BGP] の順に移動します。

3 BGP が現在有効でない場合は、[BGP の有効化] 切り替えを使用して、BGP を有効にします。

4 組織のニーズに応じて BGP 設定を行います。

オプション	説明
グレースフル リスタートの有効化	BGP サービスの再起動時にパケット転送が中断されないように指定します。
デフォルトの広告の有効化	Edge ゲートウェイが BGP ネイバーに自分自身をデフォルト ゲートウェイとして通知できるようにします。
ローカル AS	必須項目です。プロトコルのローカルの自律システム (AS) 機能に使用するための AS ID 番号を指定します。指定する値は 1 ～ 65534 の数字で、グローバルで一意な値にする必要があります。 ローカル AS は、BGP の機能です。設定している Edge ゲートウェイにシステムからローカル AS 番号が割り当てられます。Edge ゲートウェイが他の自律システム内の BGP ネイバーとピアリングする場合は、この ID を通知します。ターゲットの最適パスの選択時、ルートが経由する自律システムのパスは、動的ルーティング アルゴリズムのメトリックの 1 つとして使用されます。

5 [変更を保存] をクリックするか、BGP ルーティング ネイバーを引き続き設定することができます。

6 [追加] () ボタンをクリックし、BGP ネイバー設定を追加します。ダイアログ ボックスでネイバーの詳細を指定し、[保持] をクリックします。

オプション	説明
IP アドレス	この Edge ゲートウェイの BGP ネイバーの IP アドレスを入力します。
リモート AS	この BGP ネイバーが属している自律システムのグローバルに一意な番号を 1 ～ 65534 の範囲内で入力します。このリモート AS の番号は、システムの BGP ネイバー テーブル内の BGP ネイバー エントリに使用されます。
ウェイト	ネイバー接続のデフォルトのウェイトです。組織の要求に合わせて調整します。
キープ アライブ時間	ソフトウェアがピアにキープ アライブ メッセージを送信する頻度です。デフォルトの頻度は 60 秒です。組織の要求に合わせて調整します。

オプション	説明
ホールド ダウン時間	ソフトウェアがキープ アライブ メッセージを受信しなくなってから、ピアが停止していると宣言するまでの間隔です。この間隔は、キープ アライブ間隔の 3 倍にする必要があります。デフォルトの間隔は 180 秒です。組織の要求に合わせて調整します。 2 つの BGP ネイバー間でピアリングが確立されると、Edge ゲートウェイはホールド ダウン タイマーを開始します。Edge ゲートウェイがネイバーからキープ アライブ メッセージを受信するたびに、ホールド ダウン タイマーは 0 にリセットされます。Edge ゲートウェイがキープ アライブ メッセージの受信を 3 回連続で失敗し、ホールド ダウン タイマーがキープ アライブ間隔の 3 倍に到達すると、Edge ゲートウェイはネイバーが停止していると見なして、このネイバーからルートを削除します。
パスワード	この BGP ネイバーが認証を必要としている場合は、認証パスワードを入力します。 ネイバー間の接続で送信されるセグメントごとに検証が行われます。MD5 認証を設定するには、両方の BGP ネイバーで同じパスワードを設定する必要があります。使用しない場合、これらの間に接続が確立されません。
BGP フィルタ	このテーブルを使用して、この BGP ネイバーのプレフィックス リストを使用したルート フィルタリングを指定します。 **注意：** フィルタの最後で、`block all` ルールが適用されます。 [+] アイコンをクリックし、オプションを設定して、テーブルにフィルタを追加します。[保持] をクリックして、各フィルタを保存します。 ■ 方向を選択して、ネイバーへの受信トラフィックと送信トラフィックのいずれをフィルタするかを指定します。 ■ アクションを選択して、トラフィックの許可または拒否のいずれかを指定します。 ■ ネイバーへの送受信をフィルタするネットワークを入力します。ANY を入力するか、またはネットワークを CIDR 形式で入力します。 ■ [IP プリフィックス GE] および [IP プリフィックス LE] に入力して、IP プリフィックス リストで `le` および `ge` キーワードを使用します。

7 [変更を保存] をクリックして、システムに設定を保存します。

次のステップ

ルーティング情報の交換相手となる他の Edge ゲートウェイで、BGP を設定します。

BGP が設定された Edge ゲートウェイへの送受信トラフィックを許可するファイアウォール ルールを追加します。詳細については、Edge Gateway ファイアウォール ルールの追加を参照してください。

ルート再配分の設定

デフォルトでは、ルーターは同じプロトコルを実行している他のルーターとのみルートを共有します。マルチプロトコル環境を設定した場合は、クロスプロトコル ルート共有を使用するようにルート再配分を設定する必要があります。ルート再配分は Edge Gateway に対して設定できます。

手順

1 Edge Gateway サービスを開きます。

a メイン メニュー (☰) から、[クラウド リソース] を選択します。

b 左側のパネルで [Edge ゲートウェイ] をクリックします。

c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[サービス] をクリックします。

2 [ルーティング] - [ルートの再分散] に移動します。

3 プロトコルの切り替えを使用して、ルートの再分散を有効にするプロトコルをオンにします。

4 画面上のテーブルに IP プリフィックスを追加します。

a [追加] () ボタンをクリックします。

b ネットワークの名前および IP アドレスを CIDR 形式で入力します。

c [保持] をクリックします。

5 [追加] () ボタンをクリックして各 IP プリフィックスに再分散基準を指定します。ダイアログ ボックスで基準を指定し、[保持] をクリックします。

テーブル内のエントリは順番に処理されます。上下の矢印を使用して順番を調整します。

オプション	説明
プリフィックス名	特定の IP プリフィックスを選択してこの基準を適用するか、または [任意] を選択してすべてのネットワーク ルートに基準を適用します。
学習者プロトコル	この再分散基準で他のプロトコルからルートを学習するプロトコルを選択します。
次からの学習を許可	[学習者プロトコル] リストで選択したプロトコルでルートを学習できるネットワークのタイプを選択します。
アクション	選択したネットワーク タイプからの再分散の許可または拒否のいずれかを選択します。

6 [変更を保存] をクリックします。

ロード バランシング

ロード バランサーは、ユーザーに対してロードの分散が透過的に行われるように、受信サービス リクエストを複数のサーバに均等に分散します。ロード バランシングは、最適なリソース使用率の達成、スループットの最大化、応答時間の最小化、過負荷の回避に役立ちます。

ロード バランシングについて

NSX ロード バランサーは、2 つのロード バランシング エンジンをサポートします。レイヤー 4 ロード バランサーはパケット ベースであり、高速パス処理を提供します。レイヤー 7 ロード バランサーはソケット ベースであり、バックエンド サービスの高度なトラフィック管理戦略と DDOS 緩和をサポートします。

Edge Gateway は外部ネットワークからの受信トラフィックのロード バランシングを行うため、Edge Gateway のロード バランシングを外部インターフェイスで設定します。ロード バランシング用の仮想サーバを構成する場合、組織仮想データセンターにある使用可能な IP アドレスのいずれかを指定します。『vCloud Director ユーザー ガイド』を参照してください。

ロード バランシングの戦略と概念

パケット ベースのロード バランシング戦略は TCP および UDP レイヤーに実装されます。パケット ベースのロード バランシングでは、接続の停止または要求全体のバッファリングを行いません。代わりに、パケットの操作後に、選択したサーバに直接パケットを送信します。1 つのセッションのパケットが同じサーバに送信されるように TCP および UDP セッションはロード バランサー内で維持されます。グローバル構成および関連する仮想サーバ構成の両方で [アクセラレーションが有効] を選択し、パケット ベースのロード バランシングを有効にできます。

ソケット ベースのロード バランシング戦略はソケット インターフェイス上に実装されます。1 つの要求に対してクライアント側の接続とサーバ側の接続の 2 つの接続が確立されます。サーバ側の接続は、サーバの選択後に確立されます。HTTP ソケット ベースの実装の場合、要求全体を受信した後、オプションの L7 操作によって選択されたサーバに要求を送信します。HTTPS ソケット ベースの実装の場合、クライアント側の接続またはサーバ側の接続のいずれかで認証情報を交換します。ソケット ベースのロード バランシングは、TCP、HTTP、および HTTPS 仮想サーバのデフォルト モードです。

NSX ロード バランサーの主な概念は、仮想サーバ、サーバ プール、サーバ プール メンバー、およびサービス監視です。

仮想サーバ

アプリケーション サービスの抽象概念。IP アドレス、ポート、プロトコル、およびアプリケーション プロファイル（TCP、UDP など）の一意の組み合わせで表されます。

サーバ プール

バックエンド サーバのグループ。

サーバ プール メンバー

バックエンド サーバをプール内のメンバーとして表します。

サービス モニター

バックエンド サーバの健全性ステータスを調べる方法を定義します。

アプリケーション プロファイル

特定のアプリケーションの TCP、UDP、永続性、および証明書設定を表します。

設定の概要

最初に、ロード バランサーのグローバル オプションを設定します。バックエンド サーバ メンバーで構成されるサーバ プールを作成し、サービス モニターをプールに関連付けて、バックエンド サーバを効率的に管理および共有します。

次に、アプリケーション プロファイルを作成し、クライアント SSL、サーバ SSL、X-Forwarded-For、永続性など、ロード バランサーでアプリケーションの共通の動作を定義します。永続性では、同様の特性（送信元の IP アドレスまたは Cookie を同じプール メンバーに送信する必要があるなど）を持つ後続の要求が、ロード バランシング アルゴリズムを実行せずに送信されます。アプリケーション プロファイルは、仮想サーバ全体で再利用できます。

オプションのアプリケーション ルールを作成し、トラフィックの操作に関するアプリケーション固有の設定を行います。たとえば、特定の URL またはホスト名と照合し、異なる要求を異なるプールで処理できるようにします。次に、アプリケーションに固有のサービス モニターを作成します。既存のサービス モニターがニーズを満たしている場合はそのサービス モニターを使用することもできます。

必要に応じて、L7 仮想サーバの高度な機能をサポートするアプリケーション ルールを作成できます。アプリケーション ルールの使用事例として、コンテンツの切り替え、ヘッダーの操作、セキュリティ ルール、DOS 保護があります。

最後に、サーバ プール、アプリケーション プロファイル、およびあらゆるアプリケーション ルールをまとめて接続する仮想サーバを作成します。

仮想サーバが要求を受信すると、ロード バランシング アルゴリズムはプール メンバーの設定とランタイム ステータスを考慮します。次に、アルゴリズムは、1 つ以上のメンバーで構成される、トラフィックを分散するための適切なプールを計算します。プール メンバーの設定には、ウェイト、最大接続、および状態ステータスなどの設定が含まれます。ランタイム ステータスには、現在の接続、応答時間、および健全性チェックのステータス情報が含まれます。計算方法として、ラウンドロビン、重み付きラウンドロビン、最小接続、送信元 IP アドレス ハッシュ、重み付き最小接続、URL、URI、または HTTP ヘッダーを使用できます。

各プールは、関連付けられたサービス モニターで監視されます。ロード バランサーがプール メンバーの問題を検出すると、メンバーは DOWN としてマークされます。サーバ プールからサーバを選択するときは、UP のサーバのみが選択されます。サーバ プールがサービス モニターと共に構成されていない場合、すべてのプール メンバーが UP とみなされます。

ロード バランサー サービスの設定

ロード バランサーのグローバル設定パラメータには、全体の有効化、レイヤー 4 エンジンまたはレイヤー 7 エンジンの選択、およびログに記録するイベント タイプの仕様などがあります。

手順

1 Edge Gateway サービスを開きます。

   a メイン メニュー (☰) から、[クラウド リソース] を選択します。

   b 左側のパネルで [Edge ゲートウェイ] をクリックします。

   c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[サービス] をクリックします。

2 [ロード バランサー] > [グローバル構成] の順に移動します。

3 有効にするオプションを選択します。

オプション	アクション
ステータス	切り替えアイコンをクリックして、ロード バランサーを有効にします。 [アクセラレーションが有効] を有効にして、L7 エンジンではなく、より高速な L4 エンジンを使用するようにロード バランサーを設定します。L4 TCP VIP は Edge ゲートウェイのファイアウォールの前に処理されるため、[許可] ファイアウォール ルールは必要ありません。 **注：** HTTP および HTTPS 用の L7 VIP はファイアウォールの後に処理されるため、アクセラレーションが有効でない場合は、これらのプロトコルについて、L7 VIP へのアクセスを許可するための Edge ゲートウェイファイアウォール ルールが必要です。アクセラレーションが有効であり、サーバ プールが非透過モードの場合は、SNAT ルールが追加されるため、Edge ゲートウェイでファイアウォールを有効であることを確認する必要があります。
ログの有効化	Edge ゲートウェイのロード バランサーでトラフィック ログを収集するように、ログを有効にします。
ログ レベル	ログに収集するイベントの重要度を選択します。

4 [変更を保存] をクリックします。

保存操作が完了するまでに 1 分ほどかかることがあります。

次のステップ

ロード バランサーのアプリケーション プロファイルを設定します。アプリケーション プロファイルの作成を参照してください。

アプリケーション プロファイルの作成

アプリケーション プロファイルは、特定のタイプのネットワーク トラフィックに関するロード バランサーの動作を定義します。プロファイルを設定したら、仮想サーバに関連付けます。関連付けられた仮想サーバは、プロファイルに指定した値に基づいてトラフィックを処理します。プロファイルを使用すると、ネットワーク トラフィックの管理機能を強化し、トラフィック管理タスクをより簡単に、効率的に行うことができます。

HTTPS トラフィックのプロファイルを作成するときは、次の HTTPS トラフィック パターンを使用できます。

- クライアント -> HTTPS -> LB（SSL を終了） -> HTTP -> サーバ
- クライアント -> HTTPS -> LB（SSL を終了） -> HTTPS -> サーバ
- クライアント -> HTTPS -> LB（SSL パススルー） -> HTTPS -> サーバ
- クライアント -> HTTP -> LB-> HTTP -> サーバ

手順

1 Edge Gateway サービスを開きます。

a メイン メニュー (☰) から、[クラウド リソース] を選択します。

b 左側のパネルで [Edge ゲートウェイ] をクリックします。

c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[サービス] をクリックします。

2 [ロード バランサー] > [アプリケーション プロファイル] の順に移動します。

3 [作成]（  ）ボタンをクリックします。

4 プロファイルの名前を入力します。

5 アプリケーション プロファイルを設定します。

オプション	説明
タイプ	サーバに要求を送信するためのプロトコルの種類を選択します。必須パラメータのリストは、選択したプロトコルによって変わります。選択したプロトコルに当てはまらないパラメータは入力できません。その他のパラメータはすべて必須です。
SSL パススルーの有効化	クリックすると、仮想サーバに対し、SSL 認証のパススルーが有効になります。 それ以外の場合は、ターゲット アドレスで SSL 認証が実行されます。
HTTP リダイレクト URL	(HTTP および HTTPS) ターゲット アドレスに届いたトラフィックのリダイレクト先 URL を入力します。
永続性	プロファイルの永続性メカニズムを指定します。 永続性により、セッション データ（クライアント要求を処理した特定のプール メンバーなど）が追跡および格納されます。その結果、セッション中または後続のセッション中、クライアント要求は同じプール メンバーに転送されます。次のオプションがあります。 ■ [ソース IP] ソース IP パーシステンスは、ソース IP アドレスに基づいてセッションを追跡します。ソース アドレスのアフィニティの永続性をサポートする仮想サーバへの接続をクライアントが要求すると、ロード バランサーはそのクライアントの過去の接続を確認し、過去の接続が見つかるとそのクライアントを同じプール メンバーに返します。 ■ [MSRDP] (TCP のみ) Microsoft Remote Desktop Protocol (MSRDP) パーシステンスは、Microsoft Remote Desktop Protocol (RDP) サービスを実行する Windows クライアントと Windows サーバ間の永続性セッションを維持します。MSRDP による永続性を有効にする推奨シナリオは、Windows Server ゲスト OS を実行中のメンバーで構成するロード バランシング プールを作成し、すべてのメンバーが Windows クラスタに属し、Windows セッション ディレクトリに参加するようにすることです。
Cookie 名	(HTTP および HTTPS) 永続性メカニズムとして [Cookie] を指定した場合は、Cookie 名を入力します。[Cookie] は、Cookie を使用して、クライアントが最初にサイトにアクセスするときのセッションを一意に識別します。ロード バランサーは、セッションで後続の要求を接続するときに、この Cookie を参照してすべての要求を同じ仮想サーバに送ります。

オプション	説明
モード	Cookie の挿入に使用するモードを選択します。次のモードがサポートされています。 ■ [挿入] Edge ゲートウェイが Cookie を送信します。サーバが 1 つ以上の Cookie を送信すると、クライアントはもう 1 つ Cookie を受信します（サーバの Cookie と Edge ゲートウェイの Cookie）。サーバが Cookie を送信しない場合、クライアントは Edge ゲートウェイの Cookie のみを受信します。 ■ [プレフィックス] クライアントが複数の Cookie をサポートしていない場合は、このオプションを選択します。 **注：** すべてのブラウザは、複数の Cookie を受け付けます。ただし、1 つの Cookie のみをサポートする専用クライアントを使用した専用アプリケーションを使用している場合があります。その場合、Web サーバは Cookie を通常通り送信します。Edge ゲートウェイは、その Cookie 情報を（プレフィックスとして）サーバの Cookie 値に挿入します。この Cookie が追加された情報は、Edge ゲートウェイがサーバに送信したときに削除されます。 ■ [アプリケーション セッション] このオプションではサーバは Cookie を送信しません。代わりに、ユーザー セッション情報を URL として送信します。たとえば、`http://example.com/admin/UpdateUserServlet;jsessionid=OI24B9ASD7BSSD` の場合、`jsessionid` がユーザー セッション情報で、永続性のために使用されています。トラブルシューティングのためにアプリケーション セッションの永続性テーブルを見ることはできません。
有効期限 (秒)	永続性の有効期間を秒単位で入力します。1 ～ 86,400 の正の整数を指定します。 **注：** TCP でソース IP アドレスによる永続性を使用する L7 ロード バランシングでは、一定期間に新規の TCP 接続がない場合、接続が継続中であっても永続性エントリがタイムアウトになります。
X-Forwarded-For HTTP ヘッダーの挿入	(HTTP および HTTPS) ロード バランサーを介して Web サーバに接続するクライアントの送信元 IP アドレスを識別するには、[X-Forwarded-For HTTP ヘッダーの挿入] を選択します。
プール側の SSL の有効化	(HTTPS のみ) サーバ側からのロード バランサーの認証に使用する証明書、CA、または CRL を定義するには、[プール証明書] タブの [プール側の SSL の有効化] を選択します。

6 （HTTPS のみ）アプリケーション プロファイルで使用する証明書を設定します。必要な証明書がない場合は、[証明書] タブから作成できます。

オプション	説明
仮想サーバ証明書	HTTPS トラフィックの復号化に使用する証明書、CA、または CRL を選択します。
プール証明書	サーバ側からのロード バランサーの認証に使用する証明書、CA、または CRL を定義します。 **注：** このタブを有効にするには、[プール側の SSL の有効化] を選択します。
暗号	SSL/TLS ハンドシェイク時にネゴシエートされる暗号アルゴリズム（または暗号スイート）を選択します。
クライアント認証	クライアント認証を無視するか、必須にするかどうかを指定します。 **注：** 必須に設定すると、クライアントは、要求またはハンドシェイクがキャンセルされた後、証明書を提供する必要があります。

7 変更内容を維持するには、[保持] をクリックします。

この操作は完了するまでに 1 分かかることがあります。

次のステップ

さまざまなタイプのネットワーク トラフィックの健全性チェックを定義するには、ロード バランサーのサービス監視を追加します。サービス監視の作成を参照してください。

サービス監視の作成

特定のタイプのネットワーク トラフィックの健全性チェック パラメータを定義するには、サービス監視を作成します。サービス監視をプールに関連付けると、サービス監視パラメータに基づいてプール メンバーが監視されます。

手順

1 Edge Gateway サービスを開きます。

a メイン メニュー (☰) から、[クラウド リソース] を選択します。

b 左側のパネルで [Edge ゲートウェイ] をクリックします。

c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[サービス] をクリックします。

2 [ロード バランサー] > [サービス監視] の順に移動します。

3 [作成]（+）ボタンをクリックします。

4 サービス監視の名前を入力します。

5 （オプション） サービス監視に関する次のオプションを設定します。

オプション	説明
間隔	指定した [メソッド] を使用してサーバが監視する間隔を入力します。
タイムアウト	サーバからの応答を受信する必要のある期間の最大値（秒）を入力します。
最大試行回数	指定した監視の [メソッド] が連続して失敗できる回数を入力します。この回数を超えるとサーバは停止状態と判断されます。
タイプ	健全性チェック要求をサーバに送信する方法（HTTP、HTTPS、TCP、ICMP、または UDP）を選択します。 選択したタイプに応じて、[新規サービス監視] ダイアログの他のオプションが有効または無効になります。
予測	(HTTP および HTTPS）監視が HTTP または HTTPS 応答のステータス行で照合する文字列を入力します（HTTP/1.1 など）。
メソッド	(HTTP および HTTPS）サーバ ステータスの検出に使用するメソッドを選択します。
URL	(HTTP および HTTPS）サーバ ステータス要求で使用する URL を入力します。 **注：** メソッドとして POST を選択した場合は、[送信] の値を指定する必要があります。
送信	(HTTP、HTTPS、UDP）送信するデータを入力します。

オプション	説明
受信	(HTTP、HTTPS、および UDP) 応答コンテンツで照合する文字列を入力します。 **注：** [予測] が一致しない場合、監視は [受信] のコンテンツを照合しません。

拡張	(すべて) サービス監視の詳細パラメータをキーと値のペアで入力します。たとえば、「warning=10」は、10 秒以内にサーバが応答しない場合に、そのステータスを警告に設定することを示します。拡張項目はすべて、キャリッジ リターン文字で区切る必要があります。以下にその例を挙げます。
	`<extension>delay=2`
	`critical=3`
	`escape</extension>`

6 変更内容を維持するには、[保持] をクリックします。

この操作は完了するまでに 1 分かかることがあります。

例： 各プロトコルでサポートされる拡張機能

表 7-1. HTTP/HTTPS プロトコルの拡張機能

監視の拡張機能	説明
no-body	ドキュメントの本文を待たずに、HTTP/HTTPS ヘッダーの後で読み取りを停止します。 **注：** HTTP GET または HTTP POST は送信されますが、HEAD メソッドは送信されません。
max-age=*SECONDS*	ドキュメントが SECONDS より古い場合は警告します。数値は、分の場合は 10m、時間の場合は 10h、日の場合は 10d の形式で指定します。
content-type=*STRING*	POST 呼び出しでの Content-Type ヘッダーのメディア タイプを指定します。
linespan	正規表現で改行記号を許可します (-r または R より前に指定する必要があります)。
regex=*STRING* または ereg=*STRING*	正規表現の STRING をページで検索します。
eregi=*STRING*	大文字小文字を区別して正規表現の STRING をページで検索します。
invert-regex	見つかった場合は CRITICAL、見つからなかった場合は OK を返します。
proxy-authorization=*AUTH_PAIR*	基本認証を使用するプロキシ サーバのユーザー名とパスワード (username:password) を指定します。
useragent=*STRING*	HTTP ヘッダーの文字列を `User Agent` として送信します。
header=*STRING*	HTTP ヘッダー内のその他のタグを送信します。追加のヘッダーで複数回使用できます。
onredirect=ok|warning|critical|follow|sticky|stickyport	リダイレクト ページの処理方法を示します。 `sticky` は `follow` に似ていますが、指定した IP アドレスと連携します。`stickyport` は、ポートが同じであることを確認します。
pagesize=*INTEGER:INTEGER*	必要なページ サイズの最小値と最大値をバイト単位で指定します。

表 7-1. HTTP/HTTPS プロトコルの拡張機能 （続き）

監視の拡張機能	説明
warning=DOUBLE	警告ステータスになる応答時間を秒単位で指定します。
critical=DOUBLE	重大ステータスになる応答時間を秒単位で指定します。

表 7-2. HTTPS プロトコルのみを対象とした拡張機能

監視の拡張機能	説明
sni	SSL/TLS のホスト名拡張機能のサポート (SNI) を有効にします。
certificate=[INTEGER]	証明書の最低有効日数を指定します。ポートのデフォルト値は 443 です。このオプションを使用すると、URL はチェックされません。
authorization=AUTH_PAIR	基本認証を使用するサイトのユーザー名とパスワード (username:password) を指定します。

表 7-3. TCP プロトコルの拡張機能

監視の拡張機能	説明
escape	send または quit 文字列で、\n、\r、\t、または \ の使用を許可します。send または quit オプションの前に指定する必要があります。デフォルトでは、send には何も追加されず、quit の最後には \r\n が追加されます。
all	すべての expect 文字列がサーバ応答に含まれている必要があることを指定します。デフォルトでは、any が使用されます。
quit=*STRING*	接続を正常に終了するため、サーバに文字列を送信します。
refuse=ok|warn|crit	ok、warn、または criti の状態で TCP 拒否を受け入れます。デフォルトでは、crit の状態を使用します。
mismatch=ok|warn|crit	ok、warn、または crit の状態で、想定される文字列の不一致を受け入れます。デフォルトでは、warn の状態を使用します。
jail	TCP ソケットからの出力を非表示にします。
maxbytes=*INTEGER*	指定数より多いバイト数を受信すると、接続を閉じます。
delay=*INTEGER*	文字列の送信から応答のポーリングまで、指定秒数を待機します。
certificate=*INTEGER*[,*INTEGER*]	証明書の最低有効日数を指定します。最初の値は警告まで、2 番目の値は重大までの #days です（指定されない場合は 0）。
ssl	接続に SSL を使用します。
warning=DOUBLE	警告ステータスになる応答時間を秒単位で指定します。
critical=DOUBLE	重大ステータスになる応答時間を秒単位で指定します。

次のステップ

ロード バランサーのサーバ プールを追加します。ロード バランシングのサーバ プールの追加を参照してください。

ロード バランシングのサーバ プールの追加

バックエンド サーバを柔軟かつ効率的に管理および共有するために、サーバ プールを追加できます。プールはロード バランサーの分散メソッドを管理し、健全性チェック パラメータのためにサービス モニターが接続されています。

手順

1 Edge Gateway サービスを開きます。

a メイン メニュー (☰) から、[クラウド リソース] を選択します。

b 左側のパネルで [Edge ゲートウェイ] をクリックします。

c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[サービス] をクリックします。

2 [ロード バランサー] > [プール] の順に移動します。

3 [作成] () ボタンをクリックします。

4 ロード バランサー プールの名前と、必要に応じて説明を入力します。

5 [アルゴリズム] ドロップダウン メニューから、サービスのバランシング メソッドを選択します。

オプション	説明
ROUND_ROBIN	各サーバーは、割り当てられたウェイトに従って、順に使用されます。これは、サーバの処理時間が等しく分散されたままである場合に、最もスムーズで公平なアルゴリズムです。
IP_HASH	各パケットのソースおよびターゲット IP アドレスのハッシュに基づいてサーバーを選択します。
LEASTCONN	クライアントの要求を、サーバ上の既存の接続数に基づいて複数のサーバに分散させます。新しい接続は、オープン接続数が最も少ないサーバに送信されます。
URI	URI の左側の部分（クエスチョン マークの前）は、ハッシュされ、実行中のサーバの全体のウェイトで割られます。その結果により、要求を受け取るサーバが指定されます。このオプションにより、サーバが停止しない限り、URI は必ず同じサーバに転送されます。
HTTPHEADER	HTTP ヘッダー名が各 HTTP 要求で検索されます。カッコで囲まれているヘッダー名は大文字小文字が区別されません。これは ACL 'hdr()' 関数と同様です。ヘッダーが存在しないか、どの値も含まれていない場合には、ラウンド ロビン アルゴリズムが適用されます。HTTP HEADER アルゴリズム パラメータには、1 つのオプション `headerName=<name>` があります。たとえば、HTTP HEADER アルゴリズム パラメータとして **`host`** を使用できます。
URL	引数で指定した URL パラメータが、各 HTTP GET 要求のクエリ文字列内で検索されます。パラメータに等号 (=) と値が続く場合、値はハッシュされ、実行中のサーバの重みの合計で除算されます。結果により、要求を受信するサーバが指定されます。このプロセスを使用して要求内のユーザー ID を追跡し、サーバが起動したり停止したりしない限り、同じユーザー ID が常に同じサーバに確実に送信されるようにします。値またはパラメータが見つからない場合、ラウンド ロビン アルゴリズムが適用されます。URL アルゴリズム パラメータには、1 つのオプション `urlParam=<url>` があります。

6 メンバーをプールに追加します。

a [追加] () ボタンをクリックします。

b プール メンバーの名前を入力します。

c プール メンバーの IP アドレスを入力します。

d メンバーがロード バランサーからトラフィックを受信するポートを入力します。

e メンバーが健全性モニターの要求を受信する監視ポートを入力します。

f [ウェイト] テキスト ボックスに、このメンバーが処理するトラフィックの割合を入力します。1 ～ 256 の範囲の整数にする必要があります。

g （オプション）[最大接続数] テキスト ボックスに、メンバーが処理できる同時接続の最大数を入力します。

受信要求の数が最大を超えた場合、要求はキューに入れられ、ロード バランサーは接続が解放されるのを待機します。

h （オプション）[最小接続数] テキスト ボックスに、メンバーが必ず受け入れなければならない同時接続数の最小数を入力します。

i [保持] をクリックして、新しいメンバーをプールに追加します。

この操作は完了するまでに 1 分かかることがあります。

7 （オプション） クライアント IP アドレスをバックエンド サーバに表示するには、[透過的] を選択します。

[透過的] が選択されていない場合（デフォルト値）、バックエンド サーバは、ロード バランサーの内部 IP アドレスとして、トラフィック ソースの IP アドレスを参照します。

[透過的] が選択されている場合、ソース IP アドレスは、クライアントの実際の IP アドレスであり、Edge ゲートウェイをデフォルト ゲートウェイとして設定し、戻りパケットが Edge ゲートウェイを確実に経由するようにします。

8 変更内容を維持するには、[保持] をクリックします。

この操作は完了するまでに 1 分かかることがあります。

次のステップ

ロード バランサーの仮想サーバを追加します。仮想サーバには公開 IP アドレスがあり、すべての受信クライアント要求を処理します。 仮想サーバの追加を参照してください。

アプリケーション ルールの追加

アプリケーション ルールを作成して、IP アプリケーション トラフィックの操作と管理を直接行うことができます。

手順

1 Edge Gateway サービスを開きます。

a メイン メニュー (☰) から、[クラウド リソース] を選択します。

b 左側のパネルで [Edge ゲートウェイ] をクリックします。

c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[サービス] をクリックします。

2 [ロード バランサー] > [アプリケーション ルール] の順に移動します。

3 [追加]（  ）ボタンをクリックします。

4 アプリケーション ルールの名前を入力します。

5 アプリケーション ルールのスクリプトを入力します。

アプリケーション ルールの構文については、http://cbonte.github.io/haproxy-dconv/configuration-1.5.html を参照してください。

6 変更内容を維持するには、[保持] をクリックします。

この操作は完了するまでに 1 分かかることがあります。

次のステップ

ロード バランサーに追加する仮想サーバに新しいアプリケーション ルールを関連付けます。 仮想サーバの追加を参照してください。

仮想サーバの追加

仮想サーバとして Edge ゲートウェイ内部インターフェイスまたはアップリンク インターフェイスを追加します。仮想サーバには公開 IP アドレスがあり、すべての受信クライアント要求を処理します。

デフォルトでは、ロード バランサーは、各クライアント要求の後にサーバ TCP 接続を閉じます。

手順

1 Edge Gateway サービスを開きます。

a メイン メニュー (☰) から、[クラウド リソース] を選択します。

b 左側のパネルで [Edge ゲートウェイ] をクリックします。

c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[サービス] をクリックします。

2 [ロード バランサー] > [仮想サーバ] の順に移動します。

3 [追加] (+) ボタンをクリックします。

4 [全般] タブで、仮想サーバの次のオプションを設定します。

オプション	説明
仮想サーバの有効化	クリックして、仮想サーバを有効にします。
アクセラレーションの有効化	クリックしてアクセラレーションを有効にします。
アプリケーション プロファイル	仮想サーバに関連付けるアプリケーション プロファイルを選択します。
名前	仮想サーバーの名前を入力します。
説明	必要に応じて仮想サーバの説明を入力します。
IP アドレス	ロード バランサーがリスンする IP アドレスを入力するか、参照して選択します。
プロトコル	仮想サーバが受け入れるプロトコルを選択します。選択した [アプリケーション プロファイル] により使用されるものと同じプロトコルを選択する必要があります。
ポート	ロード バランサーが待機するポート番号を入力します。
デフォルトのプール	ロード バランサーが使用するサーバ プールを選択します。

オプション	説明
接続制限	（オプション）仮想サーバが処理できる最大同時接続数を入力します。
接続速度の制限 (CPS)	（オプション）1 秒あたり最大の受信新規接続要求を入力します。

5 （オプション） アプリケーション ルールを仮想サーバに関連付けるために、[詳細] タブをクリックし、次の手順を実行します。

a [追加]（  ）ボタンをクリックします。

ロード バランサー用に作成されたアプリケーション ルールが表示されます。必要に応じて、ロード バランサーのアプリケーション ルールを追加します。アプリケーション ルールの追加を参照してください。

6 変更内容を維持するには、[保持] をクリックします。

この操作は完了するまでに 1 分かかることがあります。

次のステップ

新しい仮想サーバ（ターゲット IP アドレス）へのトラフィックを許可する、Edge ゲートウェイ ファイアウォール ルールを作成します。Edge Gateway ファイアウォール ルールの追加を参照してください。

仮想プライベート ネットワークを使用したセキュアなアクセス

Edge Gateway の NSX ソフトウェアによって提供される VPN 機能を設定できます。組織仮想データセンターに VPN 接続を設定する際は、SSL VPN-Plus トンネル、IPsec VPN トンネル、または L2 VPN トンネルを使用します。

『NSX 管理ガイド』で説明されているように、NSX Edge ゲートウェイは以下の VPN サービスをサポートしています。

- SSL VPN Plus。リモート ユーザーがプライベートの企業アプリケーションにアクセスできます。
- IPsec VPN。NSX Edge ゲートウェイと、同じく NSX を備えているかサードパーティ製ハードウェア ルーターまたは VPN ゲートウェイを備えているリモート サイトとの間に、サイト間接続を提供します。
- L2 VPN。仮想マシンが地理的境界を越えて同じ IP アドレスを維持しながらネットワーク接続を保持できるよう許可することにより、組織仮想データセンターの拡張を実現します。

vCloud Director 環境では、以下の組み合わせの間に VPN トンネルを作成できます。

- 同じ組織内の組織仮想データセンター ネットワーク
- 異なる組織内の組織仮想データセンター ネットワーク
- 組織仮想データセンター ネットワークと外部ネットワーク

注： vCloud Director は、2 つの同じ Edge ゲートウェイ間の複数の VPN トンネルをサポートしていません。2 つの Edge ゲートウェイ間に既存のトンネルがあり、そのトンネルに別のサブネットを追加する場合は、既存の VPN トンネルを削除して、新しいサブネットを含む新しい VPN トンネルを作成してください。

Edge Gateway の VPN トンネルを構成した後は、リモートの場所から VPN クライアントを使用して、その Edge Gateway によってバッキングされている組織仮想データセンターに接続できます。

SSL VPN-Plus の設定

vCloud Director 環境の Edge Gateway に SSL VPN-Plus サービスを使用すると、リモート ユーザーはこの Edge Gateway でバッキングされている組織仮想データセンター内のプライベート ネットワークおよびアプリケーションに安全に接続できるようになります。Edge Gateway にさまざまな SSL VPN-Plus サービスを設定できます。

vCloud Director 環境の場合は、Edge Gateway の SSL VPN-Plus 機能によってネットワーク アクセス モードがサポートされます。リモート ユーザーが安全に接続して、Edge ゲートウェイの背後にあるネットワークおよびアプリケーションにアクセスできるようにするには、SSL クライアントをインストールする必要があります。Edge Gateway の SSL VPN-Plus 設定の一部として、オペレーティング システムに対応したインストール パッケージを追加し、特定のパラメータを設定します。詳細については、SSL VPN-Plus クライアントのインストール パッケージの追加を参照してください。

Edge ゲートウェイで SSL VPN-Plus を設定するには、複数の手順を実行します。

前提条件

SSL VPN-Plus に必要なすべての SSL 証明書が、[証明書] 画面に追加されていることを確認します。SSL 証明書の管理を参照してください。

注： Edge ゲートウェイで HTTPS に使用されるデフォルト ポートは、ポート 443 です。SSL VPN 機能を使用するには、Edge Gateway の HTTPS ポートに外部ネットワークからアクセスできる必要があります。SSL VPN クライアントが機能するには、[SSL VPN-Plus] タブの [サーバー設定] 画面で設定された Edge Gateway の IP アドレスおよびポートに、クライアント システムからアクセスできる必要があります。SSL VPN サーバの設定を参照してください。

手順

1 SSL-VPN Plus 画面への移動

SSL-VPN Plus 画面に移動して、Edge Gateway に SSL-VPN Plus サービスを設定することができます。

2 SSL VPN サーバの設定

このサーバ設定では、サービスがリスンする IP アドレスとポート、サービスの暗号リスト、およびそのサービス証明書など、SSL VPN サーバの設定を行います。Edge Gateway に接続するときに、リモート ユーザーはこれらのサーバ設定と同じ IP アドレスとポートを指定します。

3 Edge Gateway 上で SSL VPN-Plus と使用するための IP アドレス プールの作成

[SSL VPN-Plus] タブの [IP プール] 画面を使用して設定した固定 IP アドレス プールに含まれる仮想 IP アドレスが、リモート ユーザーに割り当てられます。

4 Edge Gateway 上で SSL VPN-Plus とともに使用するためのプライベート ネットワークの追加

プライベート ネットワークを構成するには、[SSL VPN-Plus] タブにある [プライベート ネットワーク] 画面を使用します。プライベート ネットワークは、リモート ユーザーが VPN クライアントと SSL VPN トンネルを使用して接続するときに、VPN クライアントがアクセスするネットワークです。有効なプライベート ネットワークは、VPN クライアントのルーティング テーブルに組み込まれます。

5 Edge Gateway での SSL VPN-Plus の認証サービスの設定

[SSL VPN-Plus] タブにある [認証] 画面を使用して、Edge Gateway の SSL VPN サービスのローカル認証サーバを設定し、オプションでクライアント証明書の認証を有効にします。この認証サーバを使用して、接続しているユーザーを認証します。ローカル認証サーバに設定されているすべてのユーザーが認証されます。

6 ローカルの SSL VPN-Plus 認証サーバへの SSL VPN-Plus ユーザーの追加

[SSL VPN-Plus] タブの [ユーザー] 画面を使用して、Edge Gateway の SSL VPN サービスのローカル認証サーバに、リモート ユーザーのアカウントを追加します。

7 SSL VPN-Plus クライアントのインストール パッケージの追加

[SSL VPN-Plus] タブにある [インストール パッケージ] 画面を使用して、リモート ユーザー用の SSL VPN-Plus クライアントの名前付きインストール パッケージを作成します。

8 SSL VPN-Plus クライアント構成の編集

[SSL VPN-Plus] タブの [クライアント構成] 画面を使用して、リモート ユーザーが SSL VPN にログインしたときの SSL VPN クライアント トンネルの応答方法をカスタマイズします。

9 Edge Gateway での SSL VPN-Plus の全般設定のカスタマイズ

vCloud Director 環境の Edge Gateway では、一部の SSL VPN-Plus 設定がデフォルトで設定されています。vCloud Director テナント ポータルの [SSL VPN-Plus] タブの [全般設定] を使用して、これらの設定をカスタマイズします。

SSL-VPN Plus 画面への移動

SSL-VPN Plus 画面に移動して、Edge Gateway に SSL-VPN Plus サービスを設定することができます。

手順

1 Edge Gateway サービスを開きます。

a メイン メニュー (☰) から、[クラウド リソース] を選択します。

b 左側のパネルで [Edge ゲートウェイ] をクリックします。

c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[サービス] をクリックします。

2 [SSL VPN-Plus] タブをクリックします。

次のステップ

[全般] 画面で、SSL VPN-Plus のデフォルト設定を行います。Edge Gateway での SSL VPN-Plus の全般設定のカスタマイズを参照してください。

SSL VPN サーバの設定

このサーバ設定では、サービスがリスンする IP アドレスとポート、サービスの暗号リスト、およびそのサービス証明書など、SSL VPN サーバの設定を行います。Edge Gateway に接続するときに、リモート ユーザーはこれらのサーバ設定と同じ IP アドレスとポートを指定します。

Edge Gateway がその外部インターフェイス上の複数のオーバーレイ IP アドレス ネットワークで構成されている場合、SSL VPN サーバに対して選択した IP アドレスが、Edge Gateway のデフォルトの外部インターフェイスとは異なる可能性があります。

SSL VPN サーバの設定時に、SSL VPN トンネルで使用する暗号化アルゴリズムを選択する必要があります。1 つ以上の暗号を選択できます。選択した暗号の長所と短所を照らし合わせながら、慎重に選択します。

デフォルトでは、Edge Gateway ごとに SSL VPN トンネルのデフォルトのサーバ ID 証明書として生成されたデフォルトの自己署名証明書が使用されます。このデフォルトの証明書ではなく、[証明書] 画面でシステムに追加したデジタル証明書を使用することもできます。

前提条件

- SSL VPN-Plus の設定で説明されている前提条件を満たしていることを確認します。
- デフォルトとは異なるサービス証明書を使用する場合は、必要な証明書をシステムにインポートします。Edge Gateway へのサービス証明書の追加を参照してください。
- SSL-VPN Plus 画面への移動。

手順

1. [SSL VPN-Plus] 画面で、[サーバ設定] をクリックします。
2. [有効] をクリックします。
3. ドロップダウン メニューから IP アドレスを選択します。
4. （オプション） TCP のポート番号を入力します。

   この TCP ポート番号は、SSL クライアント インストール パッケージで使用されます。デフォルトでは、HTTPS/SSL トラフィックのデフォルト ポートのポート 443 が使用されます。ポート番号が必要な場合でも、通信用の任意の TCP ポートを設定できます。

   注： SSL VPN クライアントでは、ここで設定した IP アドレスとポートにリモート ユーザーのクライアント システムからアクセスできる必要があります。ポート番号をデフォルトから変更する場合は、変更後の IP アドレスとポートに対象ユーザーのシステムから確実にアクセスできるようにします。
5. 暗号リストから暗号化方式を選択します。
6. サービスの Syslog のログ ポリシーを設定します。

   デフォルトではログは有効です。ログに記録するメッセージのレベルを変更するか、ログを無効にできます。
7. （オプション） システムが生成したデフォルトの自己署名証明書ではなくサービス証明書を使用する場合は、[サーバ証明書を変更] をクリックし、証明書を選択して [OK] をクリックします。
8. [変更を保存] をクリックします。

次のステップ

注： 設定した Edge Gateway の IP アドレスと TCP ポート番号にリモート ユーザーがアクセスできる必要があります。この手順で設定した SSL VPN-Plus の IP アドレスとポートへのアクセスを許可する、Edge Gateway のファイアウォール ルールを追加します。Edge Gateway ファイアウォール ルールの追加を参照してください。

リモート ユーザーが SSL VPN-Plus を使用して接続したときにリモート ユーザーに IP アドレスが割り当てられるように IP プールを追加します。Edge Gateway 上で SSL VPN-Plus と使用するための IP アドレス プールの作成を参照してください。

Edge Gateway 上で SSL VPN-Plus と使用するための IP アドレス プールの作成

[SSL VPN-Plus] タブの [IP プール] 画面を使用して設定した固定 IP アドレス プールに含まれる仮想 IP アドレスが、リモート ユーザーに割り当てられます。

この画面で追加された各 IP アドレス プールは、Edge Gateway に設定される IP アドレス サブネットになります。これらの IP アドレス プールで使用される IP アドレスの範囲は、Edge Gateway で設定されている他のすべてのネットワークとは異なっている必要があります。

注： SSL VPN は、IP アドレス プールの IP アドレスを、画面上のテーブルに表示される IP アドレス プールの順に、リモート ユーザーに割り当てます。IP アドレス プールを画面上のテーブルに追加した後は、上下の矢印を使用して、テーブル内のアドレス プールの位置を調整できます。

前提条件

- SSL-VPN Plus 画面への移動。
- SSL VPN サーバの設定。

手順

1 [SSL VPN-Plus] タブで、[IP プール] をクリックします。

2 [作成]（  ）ボタンをクリックします。

3 IP プールを設定します。

オプション	アクション
IP の範囲	**127.0.0.1–127.0.0.9.** のように、この IP アドレス プールの IP アドレスの範囲を入力します。 VPN クライアントを認証し、SSL VPN トンネルに接続するときに、これらの IP アドレスが割り当てられます。
ネットマスク	**255.255.255.0** など、IP アドレス プールのネットマスクを入力します。
ゲートウェイ	Edge Gateway でこの IP アドレス プールのゲートウェイ アドレスとして作成して割り当てる IP アドレスを入力します。 IP アドレス プールが作成されると、Edge Gateway 仮想マシンで仮想アダプタが作成され、この IP アドレスはその仮想インターフェイスに設定されます。この IP アドレスには、[IP の範囲] フィールドで指定した範囲に含まれないサブネットの任意の IP アドレスも指定できます。
説明	（オプション）この IP アドレス プールの説明を入力します。
ステータス	この IP アドレス プールを有効にするか無効にするかを選択します。
プライマリ DNS	（オプション）これらの仮想 IP アドレスの名前解決のために使用するプライマリ DNS サーバの名前を入力します。
セカンダリ DNS	（オプション）使用するセカンダリ DNS サーバの名前を入力します。

オプション	アクション
DNS サフィックス	（オプション）ドメインベースのホスト名解決のために、クライアント システムがホストされているドメインの DNS サフィックスを入力します。
WINS サーバ	（オプション）組織のニーズに合わせて、WINS サーバ アドレスを入力します。

4 [保持] をクリックします。

結果

IP アドレス プールの構成が画面上のテーブルに追加されます。

次のステップ

SSL VPN-Plus を使用して接続するリモート ユーザーにアクセスを許可するプライベート ネットワークを追加します。Edge Gateway 上で SSL VPN-Plus とともに使用するためのプライベート ネットワークの追加を参照してください。

Edge Gateway 上で SSL VPN-Plus とともに使用するためのプライベート ネットワークの追加

プライベート ネットワークを構成するには、[SSL VPN-Plus] タブにある [プライベート ネットワーク] 画面を使用します。プライベート ネットワークは、リモート ユーザーが VPN クライアントと SSL VPN トンネルを使用して接続するときに、VPN クライアントがアクセスするネットワークです。有効なプライベート ネットワークは、VPN クライアントのルーティング テーブルに組み込まれます。

プライベート ネットワークは、VPN クライアントのトラフィックを暗号化する、または暗号化から除外する Edge Gateway の背後にあるすべてのアクセス可能な IP アドレス ネットワークのリストです。SSL VPN トンネル経由でアクセスする必要がある各プライベート ネットワークは、個別のエントリとして追加する必要があります。エントリの数は、ルート要約の手法を使用して制限できます。

- SSL VPN-Plus は、リモート ユーザーによるプライベート ネットワークへのアクセスを、画面上のテーブルに表示される IP アドレス プールの順（上から下）に許可します。プライベート ネットワークを画面上のテーブルに追加した後は、上下の矢印を使用して、テーブル内のネットワークの位置を調整できます。
- プライベート ネットワークに対して TCP 最適化の有効化を選択すると、アクティブ モードの FTP などの一部のアプリケーションがそのサブネット内で動作しない場合があります。アクティブ モードで構成されている FTP サーバを追加するには、その FTP サーバ用に別のプライベート ネットワークを追加し、そのプライベート ネットワークの TCP 最適化を無効にする必要があります。また、その FTP サーバのプライベート ネットワークを有効にし、画面上のテーブルで、TCP が最適化されたプライベート ネットワークより上に表示されるようにする必要があります。

前提条件

- SSL-VPN Plus 画面への移動。
- Edge Gateway 上で SSL VPN-Plus と使用するための IP アドレス プールの作成。

手順

1 [SSL VPN-Plus] タブで、[プライベート ネットワーク] をクリックします。

2 [追加]（  ）ボタンをクリックします。

3 プライベート ネットワークを構成します。

オプション	アクション
ネットワーク	プライベート ネットワークの IP アドレスを、**192169.1.0/24** などの CIDR 形式で入力します。
説明	（オプション）ネットワークの説明を入力します。
トラフィックを送信	VPN クライアントでプライベート ネットワークとインターネット トラフィックを送信する方法を指定します。 ■ ［トンネルを経由］ VPN クライアントは、プライベート ネットワークとインターネット トラフィックを SSL VPN-Plus が有効な Edge Gateway を経由して送信します。 ■ ［トンネルを迂回］ VPN クライアントは Edge Gateway をバイパスし、トラフィックをプライベート サーバに直接送信します。
TCP 最適化を有効化	（オプション）インターネットの速度を最適化するには、トラフィックの送信に [トンネルを経由] を選択した際に、[TCP 最適化を有効化] も選択する必要があります。 このオプションを選択すると、VPN トンネルでの TCP パケットのパフォーマンスが向上しますが、UDP トラフィックのパフォーマンスは向上しません。 従来のフルアクセス SSL VPN トンネルは、インターネット上の暗号化で、2 番目の TCP/IP スタックの TCP/IP データを送信します。この従来の方法では、アプリケーション レイヤーのデータを 2 つの別々の TCP ストリームにカプセル化します。パケット ロスは最適なインターネット条件下でも発生しますが、これが起こると、TCP-over-TCP メルトダウンと呼ばれるパフォーマンス劣化効果が生じます。TCP-over-TCP メルトダウンでは、2 つの TCP 計測ツールが 1 つの IP アドレス データ パケットを修正することにより、ネットワークのスループットが低下し、接続がタイムアウトになります。[TCP 最適化を有効化] を選択すると、この TCP-over-TCP の問題が発生するリスクを回避できます。 **注：** TCP 最適化を有効にする際には、以下を考慮する必要があります。 ■ インターネット トラフィックを最適化するポート番号を入力する必要があります。 ■ SSL VPN サーバは、VPN クライアントの代わりに TCP 接続を開始します。SSL VPN サーバが TCP 接続を開始すると、最初に自動生成される Edge ファイアウォール ルールが適用されます。このルールは、Edge Gateway から開始されたすべての接続の通過を許可します。最適化されていないトラフィックは、通常の Edge ファイアウォール ルールによって評価されます。デフォルトで生成された TCP ルールでは、任意の接続が許可されます。
ポート	[トンネルを経由] を選択した場合は、リモート ユーザーが内部サーバにアクセスするために開くポート番号の範囲を入力します。FTP トラフィックの場合は **20–21**、HTTP トラフィックの場合は **80–81** のようになります。 ユーザーに無制限のアクセス権を付与する場合は、このフィールドを空白のままにします。
ステータス	プライベート ネットワークの有効/無効を切り替えます。

4 [保持] をクリックします。

5 [変更を保存] をクリックして、システムに設定を保存します。

次のステップ

認証サーバを追加します。Edge Gateway での SSL VPN-Plus の認証サービスの設定 を参照してください。

重要： この画面で追加したプライベート ネットワークへのネットワーク トラフィックを許可するため、対応するファイアウォール ルールを追加します。Edge Gateway ファイアウォール ルールの追加を参照してください。

Edge Gateway での SSL VPN-Plus の認証サービスの設定

[SSL VPN-Plus] タブにある [認証] 画面を使用して、Edge Gateway の SSL VPN サービスのローカル認証サーバを設定し、オプションでクライアント証明書の認証を有効にします。この認証サーバを使用して、接続しているユーザーを認証します。ローカル認証サーバに設定されているすべてのユーザーが認証されます。

1 台のローカル SSL VPN-Plus 認証サーバのみを Edge Gateway に設定できます。[+ ローカル] をクリックして追加の認証サーバを指定した場合、設定の保存を試みるとエラー メッセージが表示されます。

SSL VPN 経由での認証の最大時間は、3 分です。この最大数は認証以外のタイムアウトによって決定されます。この値を設定することはできず、デフォルト値は 3 分です。このため、チェーン認証に複数の認証サーバがあり、ユーザー認証に 3 分を超える時間がかかる場合、ユーザーは認証されません。

前提条件

- SSL-VPN Plus 画面への移動。
- Edge Gateway 上で SSL VPN-Plus とともに使用するためのプライベート ネットワークの追加。
- クライアント証明書認証を有効にする場合は、CA 証明書が Edge Gateway に追加されていることを確認します。SSL 証明書の信頼性検証のための Edge Gateway への CA 証明書の追加 を参照してください。

手順

1 [SSL VPN-Plus] タブおよび [認証] をクリックします。

2 [ローカル] をクリックします。

3 認証サーバを設定します。

a （オプション） パスワード ポリシーを有効にして設定します。

オプション	説明
パスワード ポリシーを有効化	ここで設定するパスワード ポリシーを適用します。
パスワードの長さ	パスワードの長さで許可される最大文字数と最小文字数を入力します。
英字の最小数	（オプション）パスワードに必要な英字の最小数を入力します。
数字の最小数	（オプション）パスワードに必要な数字の最小数を入力します。
特殊文字の最小数	（オプション）アンパサンド (&)、ハッシュ タグ (#)、パーセント記号 (%) など、パスワードに必要な特殊文字の最小数を入力します。
パスワードにはユーザー ID を含めないでください	（オプション）パスワードにユーザー ID を含めることを禁止するには、このオプションを有効にします。
パスワードの有効期間	（オプション）ユーザーによる変更が必要になるまでパスワードが存続できる最大日数を入力します。
有効期限の通知 (期限切れになるまでの日数を指定)	（オプション）[パスワードの有効期間] の値の何日前に、パスワードの有効期限が近づいていることをユーザーに通知するかを入力します。

b （オプション） アカウントのロックアウト ポリシーを有効にして設定します。

オプション	説明
アカウントのロックアウト ポリシーを有効化	ここで設定するアカウント ロックアウト ポリシーを適用します。
再試行の回数	ユーザーが自分のアカウントへのアクセスを再試行できる回数を入力します。
再試行の期間	ログインが成功しなかった場合にユーザー アカウントがロックされる期間を分単位で入力します。 たとえば、[再試行の回数] を 5 に、[再試行の期間] を 1 分間に設定した場合、1 分間のうちにログインに 5 回失敗すると、ユーザーのアカウントがロックされることになります。
ロックアウトの期間	ユーザー アカウントをロック状態にする期間を入力します。 この期間が経過すると、アカウントのロックは自動的に解除されます。

c [ステータス] セクションでこの認証サーバを有効にします。

d （オプション） セカンダリ認証を設定します。

オプション	説明
このサーバをセカンダリ認証に使用	（オプション）認証の第 2 レベルとしてサーバを使用するかどうかを指定します。
認証が失敗した場合はセッションを終了	（オプション）認証の失敗時に VPN セッションを終了するかどうかを指定します。

e [保持] をクリックします。

4 （オプション） クライアント認定の認証を有効にするは、[証明書を変更] をクリックして有効/無効の切り替えをオンにし、使用する CA 証明書を選択して [OK] をクリックします。

次のステップ

ローカル認証サーバにローカル ユーザーを追加し、これらのユーザーが SSL VPN-Plus を使用して接続できるようにします。ローカルの SSL VPN-Plus 認証サーバへの SSL VPN-Plus ユーザーの追加 を参照してください。

リモート ユーザーがローカル システムにインストールできるようにするために、SSL クライアントを含むインストール パッケージを作成します。SSL VPN-Plus クライアントのインストール パッケージの追加 を参照してください。

ローカルの SSL VPN-Plus 認証サーバへの SSL VPN-Plus ユーザーの追加

[SSL VPN-Plus] タブの [ユーザー] 画面を使用して、Edge Gateway の SSL VPN サービスのローカル認証サーバに、リモート ユーザーのアカウントを追加します。

注： ローカル認証サーバがまだ構成されていない場合、[ユーザー] 画面でユーザーを追加すると、ローカル認証サーバがデフォルト値で自動的に追加されます。[認証] 画面の編集ボタンを使用して、デフォルト値を表示して編集します。[認証] 画面の使用の詳細については、「Edge Gateway での SSL VPN-Plus の認証サービスの設定」を参照してください。

前提条件

SSL-VPN Plus 画面への移動。

手順

1 [SSL VPN-Plus] タブで、[ユーザー] をクリックします。

2 [作成] () ボタンをクリックします。

3 ユーザーの次のオプションを設定します。

オプション	説明
ユーザー ID	ユーザー ID を入力します。
パスワード	ユーザーのパスワードを入力します。
パスワードを再入力	パスワードを再入力します。
名	(オプション) ユーザーの名を入力します。
姓	(オプション) ユーザーの姓を入力します。
説明	(オプション) ユーザーの説明を入力します。
有効	ユーザーを有効にするか無効にするかを指定します。
パスワードを無期限にする	(オプション) このユーザーに対して常に同じパスワードを保持するかどうかを指定します。
パスワードの変更を許可	(オプション) ユーザーがパスワードを変更できるようにするかどうかを指定します。
次回のログインでパスワードを変更	(オプション) このユーザーの次回ログイン時に、パスワードを変更するように依頼するかどうかを指定します。

4 [保持] をクリックします。

5 ユーザーを追加するには、手順を繰り返します。

次のステップ

ローカル認証サーバにローカル ユーザーを追加し、これらのユーザーが SSL VPN-Plus を使用して接続できるようにします。ローカルの SSL VPN-Plus 認証サーバへの SSL VPN-Plus ユーザーの追加 を参照してください。

リモート ユーザーがローカル システムにインストールできるようにするために、SSL クライアントを含むインストール パッケージを作成します。SSL VPN-Plus クライアントのインストール パッケージの追加 を参照してください。

SSL VPN-Plus クライアントのインストール パッケージの追加

[SSL VPN-Plus] タブにある [インストール パッケージ] 画面を使用して、リモート ユーザー用の SSL VPN-Plus クライアントの名前付きインストール パッケージを作成します。

SSL VPN-Plus クライアント インストール パッケージは、Edge Gateway に追加できます。新しいユーザーは、最初に VPN 接続を使用してログインする際に、このパッケージをダウンロードしてインストールするように求められます。これらのクライアント インストール パッケージを追加すると、Edge Gateway のパブリック インターフェイスの FQDN からダウンロードできるようになります。

Windows、Linux、および Mac オペレーティング システムで実行するインストール パッケージを作成することができます。SSL VPN クライアントごとに異なるインストール パラメータを必要とする場合は、構成ごとにインストール パッケージを作成します。

前提条件

SSL-VPN Plus 画面への移動

手順

1 このテナント ポータルの [SSL VPN-Plus] タブで、[インストール パッケージ] をクリックします。

2 [追加]（  ）ボタンをクリックします。

3 インストール パッケージを設定します。

オプション	説明
プロファイル名	このインストール パッケージのプロファイル名を入力します。 この名前は、Edge Gateway へのこの SSL VPN 接続を識別するためにリモート ユーザーに表示されます。
ゲートウェイ	Edge Gateway のパブリック インターフェイスの IP アドレスまたは FQDN を入力します。 入力した IP アドレスまたは FQDN は、SSL VPN クライアントにバインドされます。クライアントがリモート ユーザーのローカル システムにインストールされている場合、この IP アドレスまたは FQDN が SSL VPN クライアントに表示されます。 この SSL VPN クライアントに追加の Edge Gateway アップリンク インターフェイスをバインドするには、[追加]（  ）ボタンをクリックして行を追加し、インターフェイスの IP アドレスまたは FQDN とポートを入力します。
ポート	（オプション）表示されるデフォルトの値からポート値を変更するには、値をダブルクリックして新しい値を入力します。

オプション	説明
Windows **Linux** **Mac**	インストール パッケージを作成するオペレーティング システムを選択します。
説明	（オプション）ユーザーの説明を入力します。
有効	このパッケージを有効にするか無効にするかを指定します。

4 Windows のインストール パラメータを選択します。

オプション	説明
ログイン時にクライアントを起動	リモート ユーザーがローカル システムにログインするときに、SSL VPN クライアントを起動します。
パスワードの保存を許可	ユーザーのパスワードをクライアントで記憶できるようにします。
サイレント モードのインストールを有効化	リモート ユーザーに対してインストール コマンドを表示しません。
SSL クライアント ネットワーク アダプタを非表示	VMware SSL VPN-Plus アダプタを非表示にします。このアダプタは、SSL VPN クライアント インストール パッケージと一緒にリモート ユーザーのコンピュータにインストールされます。
クライアント システム トレイ アイコンを非表示	VPN 接続がアクティブかアクティブでないかを示す SSL VPN トレイ アイコンを非表示にします。
デスクトップ アイコンを作成	ユーザー デスクトップに SSL クライアントを起動するアイコンを作成します。
サイレント モードの操作を有効化	インストールが完了したことを示すウィンドウを非表示にします。
サーバ セキュリティ証明書の検証	SSL VPN クライアントが安全な接続を確立する前に SSL VPN サーバ証明書を検証します。

5 [保持] をクリックします。

次のステップ

クライアントの設定を編集します。SSL VPN-Plus クライアント構成の編集 を参照してください。

SSL VPN-Plus クライアント構成の編集

[SSL VPN-Plus] タブの [クライアント構成] 画面を使用して、リモート ユーザーが SSL VPN にログインしたときの SSL VPN クライアント トンネルの応答方法をカスタマイズします。

前提条件

SSL-VPN Plus 画面への移動

手順

1 [SSL VPN-Plus] タブで、[クライアント構成] をクリックします。

2 [トンネリング モード] を選択します。

- 分割トンネル モードでは、VPN トラフィックのみが Edge Gateway を通過します。
- フル トンネル モードでは、Edge Gateway がリモート ユーザーのデフォルト ゲートウェイとなり、すべてのトラフィック（VPN、ローカル、インターネットなど）が Edge Gateway を通過します。

3 フル トンネル モードを選択した場合、リモート ユーザーのクライアントで使用するデフォルト ゲートウェイの IP アドレスを入力します。また、必要に応じて、ローカル サブネットのトラフィックのフローを VPN トンネルから除外するかどうかを選択できます。

4 （オプション） 自動再接続を無効にします。

デフォルトでは [自動再接続を有効化] は有効です。自動再接続が有効な場合は、ユーザーが切断されると、SSL VPN クライアントによって自動的に再接続します。

5 （オプション） 必要に応じて、クライアントのアップグレードが利用可能な場合にリモート ユーザーに通知するためのクライアントの機能を有効にします。

デフォルトではこのオプションは無効です。このオプションを有効にした場合、リモート ユーザーはアップグレードのインストールを選択できます。

6 [変更を保存] をクリックします。

Edge Gateway での SSL VPN-Plus の全般設定のカスタマイズ

vCloud Director 環境の Edge Gateway では、一部の SSL VPN-Plus 設定がデフォルトで設定されています。vCloud Director テナント ポータルの [SSL VPN-Plus] タブの [全般設定] を使用して、これらの設定をカスタマイズします。

前提条件

SSL-VPN Plus 画面への移動。

手順

1 [SSL VPN-Plus] タブで、[全般設定] をクリックします。

2 組織のニーズに合わせて、必要に応じて全般設定を編集します。

オプション	説明
同じユーザー名を使用した複数のログインを禁止する	オンにすると、リモート ユーザーが同じユーザー名で使用できるアクティブなログイン セッションが 1 つのみに制限されます。
圧縮	オンにすると、TCP ベースのインテリジェント データ圧縮が有効になり、データ転送速度が向上します。
ログの有効化	オンにすると、SSL VPN ゲートウェイを通過するトラフィックのログが保持されます。 デフォルトではログは有効です。
仮想キーボードを強制する	オンにすると、リモート ユーザーは画面上の仮想キーボードのみを使用してログイン情報を入力する必要があります。
仮想キーボードのキーをランダム化する	オンにすると、仮想キーボードでランダムなキー レイアウトが使用されます。
セッション アイドル タイムアウト	セッション アイドル タイムアウトを分単位で入力します。 指定された期間、ユーザーのセッションでアクティビティがない場合、ユーザーのセッションを切断します。システムのデフォルトは 10 分です。
ユーザー通知	リモート ユーザーがログインした後、リモート ユーザーに表示するメッセージを入力します。
パブリック URL アクセスを有効化	オンにすると、リモート ユーザーは、リモート ユーザー アクセスが明示的に設定されていないサイトにアクセスできます。

オプション	説明
強制タイムアウトを有効化	オンにすると、[強制タイムアウト] フィールドで指定した期間の経過後にリモート ユーザーを切断します。
強制タイムアウト	タイムアウト時間を分単位で入力します。 [強制タイムアウトを有効化] をオンに切り替えると、このフィールドが表示されます。

3 [変更を保存] をクリックします。

IPsec VPN の構成

vCloud Director 環境に置かれた Edge Gateway は、組織仮想データセンター ネットワーク間、または組織仮想データセンター ネットワークと外部 IP アドレス間の VPN トンネルを保護するために、サイト間の Internet Protocol Security (IPsec) をサポートしています。IPsec VPN サービスは Edge Gateway に設定できます。

最も一般的なシナリオは、リモート ネットワークから組織仮想データセンターへの IPsec VPN 接続を設定することです。NSX ソフトウェアでは、証明書認証、事前共有キー モード、自身とリモート VPN ルーター間の IP ユニキャスト トラフィックのサポートなどの Edge Gateway の IPsec VPN 機能が提供されます。複数のサブネットが Edge ゲートウェイの背後にある内部ネットワークに IPsec トンネル経由で接続するような設定も可能です。IPsec トンネルを経由して内部ネットワークに接続するように複数のサブネットを設定する場合は、これらのサブネットおよび Edge ゲートウェイの背後にある内部ネットワークのアドレス範囲が重複しないようにする必要があります。

注： IPsec トンネルの両側にあるローカル ピアとリモート ピアで IP アドレスが重複している場合は、ローカルに接続されたルートおよび自動配管ルートの有無に応じて、このトンネルを通って転送されるトラフィックに一貫性がなくなることがあります。

次の IPsec VPN アルゴリズムがサポートされています。

- AES (AES128 CBC)
- AES256 (AES265 CBC)
- トリプル DES (3DES192-CBC)
- AES-GCM (AES128 GCM)
- DH-2（Diffie-Hellman グループ 2）
- DH-5（Diffie-Hellman グループ 5）
- DH-14（Diffie-Hellman グループ 14）

注： IPsec VPN では、動的ルーティング プロトコルはサポートされていません。組織仮想データセンターの Edge Gateway とリモート サイトの物理ゲートウェイ VPN の間に IPsec VPN トンネルを構成する場合は、その接続の動的ルーティングを構成できません。リモート サイトの IP アドレスを、Edge Gateway のアップリンク上の動的ルーティングによって学習することはできません。

『NSX 管理ガイド』のトピック「IPsec VPN の概要」に記載されているように、Edge Gateway でサポートされている最大トンネル数は、設定されているサイズ（コンパクト、大、特大、超特大）によって決まります。Edge Gateway のサイズを表示するには、vCloud Director Web コンソールにログインし、Edge Gateway に移動し、[プロパティ] アクションを使用して Edge Gateway の設定を表示します。vCloud Director Web コンソールの使用法については、『vCloud Director 管理者ガイド』を参照してください。

Edge ゲートウェイで IPsec VPN を設定するには、複数の手順を実行します。

注： トンネルのエンドポイント間にファイアウォールが配置されている場合は、IPsec VPN サービスを設定した後に、次の IP プロトコルおよび UDP ポートを許可するようにルールを更新します。

- IP プロトコル ID 50 (ESP)
- IP プロトコル ID 51 (AH)
- UDP ポート 500 (IKE)
- UDP ポート 4500

手順

1 [IPsec VPN] 画面への移動

[IPsec VPN] 画面で、Edge Gateway の IPsec VPN サービスの設定を開始できます。

2 Edge ゲートウェイの IPsec VPN サイト接続の設定

Edge Gateway の IPsec VPN 機能を使用して、組織仮想データセンターと別のサイトの間に IPsec VPN 接続を確立するために必要な設定を行うには、vCloud Director テナント ポータルで [IPsec VPN サイト] 画面を使用します。

3 Edge ゲートウェイでの IPsec VPN サービスの有効化

1 つ以上の IPsec VPN 接続が設定されている場合は、Edge Gateway で IPsec VPN サービスを有効にできます。

4 グローバル IPsec VPN 設定の指定

[グローバル構成] 画面を使用して、IPsec VPN の認証を Edge Gateway レベルで設定します。この画面では、グローバルの事前共有キーを設定し、証明書認証を有効にすることができます。

[IPsec VPN] 画面への移動

[IPsec VPN] 画面で、Edge Gateway の IPsec VPN サービスの設定を開始できます。

手順

1 Edge Gateway サービスを開きます。

a メイン メニュー (☰) から、[クラウド リソース] を選択します。

b 左側のパネルで [Edge ゲートウェイ] をクリックします。

c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[サービス] をクリックします。

2 [VPN] - [IPsec VPN] の順に選択します。

次のステップ

[IPsec VPN サイト] 画面を使用して、IPsec VPN 接続を設定します。Edge ゲートウェイで IPsec VPN サービスを有効にするには、少なくとも 1 つの接続を事前に設定する必要があります。Edge ゲートウェイの IPsec VPN サイト接続の設定を参照してください。

Edge ゲートウェイの IPsec VPN サイト接続の設定

Edge Gateway の IPsec VPN 機能を使用して、組織仮想データセンターと別のサイトの間に IPsec VPN 接続を確立するために必要な設定を行うには、vCloud Director テナント ポータルで [IPsec VPN サイト] 画面を使用します。

サイト間に IPsec VPN 接続を設定する場合は、現在の場所から見て接続を設定します。接続の設定には、VPN 接続を正しく設定できるように、vCloud Director 環境のコンテキスト内での接続の概念について理解している必要があります。

- ローカル サブネットおよびピア サブネットによって、VPN の接続先ネットワークが指定されます。IPsec VPN サイトの設定内でこれらのサブネットを指定する場合は、特定の IP アドレスではなく、ネットワーク範囲を入力します。**192.168.99.0/24** などの CIDR 形式を使用します。
- ピア ID は、VPN 接続を終端するリモート デバイスを一意に識別する ID のことで、通常はパブリック IP アドレスです。証明書認証を使用するピアの場合、この ID はピアの証明書で設定された識別名である必要があります。PSK ピアの場合、この ID には任意の文字列を指定できます。NSX のベスト プラクティスは、リモート デバイスのパブリック IP アドレスまたは完全修飾ドメイン名 (FQDN) をピア ID として使用することです。ピア IP アドレスが別の組織仮想データセンター ネットワークから取得されている場合は、ピアのネイティブ IP アドレスを入力します。ピアに NAT が設定されている場合は、ピアのプライベート IP アドレスを入力します。
- ピア エンドポイントは、ユーザーが接続しているリモート デバイスのパブリック IP アドレスを指定します。ピアのゲートウェイにインターネットから直接アクセスできず、別のデバイスを介して接続されている場合は、ピア エンドポイントのアドレスがピアの ID と異なることがあります。ピアに NAT が設定されている場合は、デバイスが NAT に使用しているパブリック IP アドレスを入力します。
- ローカル ID は、組織仮想データセンターの Edge Gateway のパブリック IP アドレスを指定します。Edge Gateway のファイアウォールと、IP アドレスまたはホスト名を入力することができます。
- ローカル エンドポイントは、Edge Gateway が送信を行う組織仮想データセンター内のネットワークを指定します。通常は、Edge Gateway の外部ネットワークがローカル エンドポイントになります。

前提条件

- [IPsec VPN] 画面への移動。
- IPsec VPN の構成。
- 認証方法としてグローバル証明書を使用する場合は、[グローバル構成] 画面で証明書認証が有効になっていることを確認します。グローバル IPsec VPN 設定の指定を参照してください。

手順

1 [IPsec VPN] タブで、[IPsec VPN サイト] をクリックします。

2 [追加] () ボタンをクリックします。

3 IPsec VPN 接続を設定します。

オプション	アクション
有効	この接続を 2 台の VPN エンドポイント間で有効にします。
Perfect Forward Secrecy (PFS) の有効化	このオプションを有効にすると、システムはユーザーが開始したすべての IPsec VPN セッションに対して一意のパブリック キーを生成します。 PFS を有効にすると、Edge Gateway のプライベート キーと各セッション キーの間にリンクが作成されなくなります。 セッション キーが危険にさらされても、このキーによって保護された特定のセッション内で交換されたデータ以外に影響はありません。サーバのプライベート キーが危険にさらされると、アーカイブされたセッションまたは今後のセッションの復号化にこのキーを使用できなくなります。 PFS が有効な場合は、この Edge ゲートウェイとの IPsec VPN 接続を処理するときに、若干のオーバーヘッドが発生します。 **重要：** 追加キーの取得元として、一意のセッション キーを使用しないでください。また、IPsec VPN トンネルが機能するには、トンネルの両側で PFS をサポートする必要があります。
名前	（オプション）接続の名前を入力します。
ローカル ID	Edge Gateway インスタンスの外部 IP アドレスを入力します。これは、Edge Gateway のパブリック IP アドレスです。 この IP アドレスは、リモート サイトの IPsec VPN 設定でピア ID に使用されます。
ローカル エンドポイント	この接続のローカル エンドポイントであるネットワークを入力します。 ローカル エンドポイントは、Edge Gateway が送信を行う組織仮想データセンター内のネットワークを指定します。通常は、外部ネットワークがローカル エンドポイントになります。 事前共有キーを使用して IP 間トンネルを追加する場合は、ローカル ID とローカル エンドポイントの IP アドレスを同じにすることができます。
ローカル サブネット	サイト間で共有するネットワークを入力します。複数のサブネットを入力するには、区切り文字にカンマを使用します。 特定の IP アドレスではなく、IP アドレスを CIDR 形式（**192.168.99.0/24** など）で指定してネットワーク範囲を入力します。
ピア ID	ピア サイトを一意に識別するピア ID を入力します。 ピア ID は、VPN 接続を終端するリモート デバイスを一意に識別する ID のことで、通常はパブリック IP アドレスです。 証明書認証を使用するピアの場合、この ID はピアの証明書に含まれている識別名である必要があります。PSK ピアの場合、この ID には任意の文字列を指定できます。NSX のベスト プラクティスは、リモート デバイスのパブリック IP アドレスまたは完全修飾ドメイン名 (FQDN) をピア ID として使用することです。 ピア IP アドレスが別の組織仮想データセンター ネットワークから取得されている場合は、ピアのネイティブ IP アドレスを入力します。ピアに NAT が設定されている場合は、ピアのプライベート IP アドレスを入力します。
ピア エンドポイント	接続先リモート デバイスのパブリック側アドレスである、ピア サイトの IP アドレスまたは完全修飾ドメイン名 (FQDN) を入力します。 **注：** ピアに NAT が設定されている場合は、デバイスが NAT に使用しているパブリック IP アドレスを入力します。

オプション	アクション
ピア サブネット	VPN の接続先となるリモート ネットワークを入力します。複数のサブネットを入力するには、区切り文字にカンマを使用します。 特定の IP アドレスではなく、IP アドレスを CIDR 形式（**192.168.99.0/24** など）で指定してネットワーク範囲を入力します。
暗号化アルゴリズム	ドロップダウン メニューから暗号化アルゴリズムのタイプを選択します。 **注：** 選択する暗号化タイプは、リモート サイトの VPN デバイスで設定されている暗号化タイプと一致する必要があります。
認証	認証を選択します。次のオプションがあります。 ■ [PSK] 事前共有キー (PSK) を選択すると、Edge Gateway とピア サイト間で共有されるプライベート キーを認証に使用するように指定されます。 ■ [証明書] 証明書の認証では、グローバル レベルで定義された証明書を認証に使用するように指定されます。このオプションは、[IPsec VPN] タブの [グローバル構成] 画面でグローバル証明書が設定されている場合以外は使用できません。
共有キーを変更	（オプション）既存の接続の設定を更新している場合は、このオプションを有効にして [事前共有キー] フィールドを使用可能にし、共有キーを更新できるようにします。
事前共有キー	認証タイプに [PSK] を選択した場合、英数字のシークレット文字列を入力します。これは、最大長が 128 バイトの文字列です。 **注：** 共有キーは、リモート サイトの VPN デバイスで設定されたキーと一致する必要があります。ベスト プラクティスは、匿名サイトが VPN サービスに接続するときに共有キーを設定することです。
共有キーの表示	（オプション）このオプションを有効にすると、共有キーを画面に表示できるようになります。
Diffie-Hellman グループ	ピア サイトおよびこの Edge Gateway が、セキュアでない通信チャネルを介して共有シークレットを確立できるようにする暗号化スキームを選択します。 **注：** [Diffie-Hellman グループ] は、リモート サイトの VPN デバイスで設定された内容と一致する必要があります。
拡張	（オプション）次のオプションのいずれかを入力します。 ■ `securelocaltrafficbyip=`*IPAddress*：IPsec VPN トンネルを介して Edge Gateway のローカル トラフィックをリダイレクトします。 これはデフォルト値です。 ■ `passthroughSubnets=`*PeerSubnetIPAddress*：重複するサブネットをサポートします。

4 [保持] をクリックします。

5 [変更を保存] をクリックします。

保存操作が完了するまでに 1 分ほどかかることがあります。

次のステップ

リモート サイトの接続を設定します。接続の両側（組織仮想データセンターおよびピア サイト）で、IPsec VPN 接続を設定する必要があります。

この Edge ゲートウェイで IPsec VPN サービスを有効にします。少なくとも 1 つの IPsec VPN 接続が設定されている場合は、サービスを有効にできます。Edge ゲートウェイでの IPsec VPN サービスの有効化 を参照してください。

Edge ゲートウェイでの IPsec VPN サービスの有効化

1 つ以上の IPsec VPN 接続が設定されている場合は、Edge Gateway で IPsec VPN サービスを有効にできます。

前提条件

- [IPsec VPN] 画面への移動。
- この Edge ゲートウェイに、少なくとも 1 つの IPsec VPN 接続が設定されていることを確認します。Edge ゲートウェイの IPsec VPN サイト接続の設定で説明されている手順を参照してください。

手順

1 [IPsec VPN] タブで、[アクティベーションのステータス] をクリックします。

2 [IPsec VPN サービス ステータス] をクリックして、IPsec VPN サービスを有効にします。

3 [変更を保存] をクリックします。

結果

Edge ゲートウェイの IPsec VPN サービスがアクティブになります。

グローバル IPsec VPN 設定の指定

[グローバル構成] 画面を使用して、IPsec VPN の認証を Edge Gateway レベルで設定します。この画面では、グローバルの事前共有キーを設定し、証明書認証を有効にすることができます。

グローバルの事前共有キーは、ピア エンドポイントが **any** に設定されたサイトで使用されます。

前提条件

- 証明書認証を有効にする場合は、1 つ以上のサービス証明書と、それに対応する CA 署名付き証明書を保持していることを [証明書] 画面で確認します。IPsec VPN には、自己署名証明書は使用できません。Edge Gateway へのサービス証明書の追加を参照してください。
- [IPsec VPN] 画面への移動。

手順

1 Edge Gateway サービスを開きます。

   a メイン メニュー (☰) から、[クラウド リソース] を選択します。

   b 左側のパネルで [Edge ゲートウェイ] をクリックします。

   c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[サービス] をクリックします。

2 [IPsec VPN] タブで、[グローバル構成] をクリックします。

3 （オプション） 次のようにして、グローバル事前共有キーを設定します。

a [共有キーを変更] オプションを有効にします。

b 事前共有キーを有効にします。

グローバルの事前共有キー (PSK) は、ピア エンドポイントが「any」に設定されたすべてのサイトによって共有されます。グローバルの PSK がすでに設定されている場合、PSK を空の値に変更して保存しても既存の設定には影響しません。

c （オプション） 必要に応じて [共有キーの表示] を有効にして、事前共有キーを表示します。

d [変更を保存] をクリックします。

4 証明書認証を設定します。

a [証明書認証の有効化] を有効にします。

b 適切なサービス証明書、CA 証明書、CRL を選択します。

c [変更を保存] をクリックします。

次のステップ

必要に応じて、Edge Gateway の IPsec VPN サービスのログを有効にできます。Edge Gateway の統計情報とログ を参照してください。

L2 VPN の構成

vCloud Director 環境の Edge Gateway では、L2 VPN がサポートされます。L2 VPN は、地理的境界を越えて同じ IP アドレスを保持しながら仮想マシンを常にネットワークに接続できるようになるため、組織仮想データセンターの拡張が可能になります。L2 VPN サービスを Edge Gateway に設定できます。

NSX ソフトウェアは、Edge Gateway の L2 VPN 機能を提供します。L2 VPN では、2 つのサイト間のトンネルを設定できます。これらのサイト間で移動した場合も、仮想マシンは同じサブネット上にとどまるため、L2 VPN を使用してネットワークを拡張することにより、組織仮想データセンターを拡張することができます。一方のサイトの Edge ゲートウェイから、他方のサイトの仮想マシンにすべてのサービスを提供できます。

L2 VPN トンネルを作成するには、L2 VPN サーバおよび L2 VPN クライアントを設定します。『NSX 管理ガイド』に記載されているように、L2 VPN サーバがターゲット Edge Gateway に、L2 VPN クライアントがソース Edge Gateway になります。各 Edge ゲートウェイで L2 VPN を設定した後に、サーバとクライアントの両方で L2 VPN サービスを有効にする必要があります。

注： サブインターフェイスとして作成された経路指定済みの組織仮想データセンター ネットワークは、Edge Gateway 上になければなりません。経路指定された外部の組織仮想データセンター ネットワークを作成する手順については、『vCloud Director 管理者ガイド』を参照してください。

手順

1 [L2 VPN] 画面への移動

Edge Gateway の L2 VPN サービスの設定を開始するには、[L2 VPN] 画面に移動する必要があります。

2 L2 VPN サーバとしての Edge ゲートウェイ の構成

L2 VPN サーバは、L2 VPN クライアントが接続するターゲット NSX Edge です。

3 L2 VPN クライアントとしての Edge Gateway の構成

L2 VPN クライアントは、ターゲット NSX Edge (L2 VPN サーバ) との通信を開始するソース NSX Edge です。

4 Edge Gateway での L2 VPN サービスの有効化

必要な L2 VPN 設定が行われている場合は、Edge Gateway で L2 VPN サービスを有効にできます。

[L2 VPN] 画面への移動

Edge Gateway の L2 VPN サービスの設定を開始するには、[L2 VPN] 画面に移動する必要があります。

手順

1 Edge Gateway サービスを開きます。

a メイン メニュー (☰) から、[クラウド リソース] を選択します。

b 左側のパネルで [Edge ゲートウェイ] をクリックします。

c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[サービス] をクリックします。

2 [VPN] - [L2 VPN] の順に選択します。

次のステップ

L2 VPN サーバを設定します。L2 VPN サーバとしての Edge ゲートウェイ の構成を参照してください。

L2 VPN サーバとしての Edge ゲートウェイ の構成

L2 VPN サーバは、L2 VPN クライアントが接続するターゲット NSX Edge です。

『NSX 管理ガイド』に記載されているように、複数のピア サイトをこの L2 VPN サーバに接続できます。

注： サイトの構成を変更すると、Edge ゲートウェイは既存のすべての接続から切断され、再接続されます。

前提条件

- Edge Gateway に、Edge Gateway のサブインターフェイスとして構成されている、経路指定された組織仮想データセンター ネットワークがあることを確認してください。経路指定された外部の組織仮想データセンター ネットワークを作成する手順については、『vCloud Director 管理者ガイド』を参照してください。
- [L2 VPN] 画面への移動。
- サービス証明書を L2 VPN 接続にバインドする場合は、サーバ証明書が Edge ゲートウェイにすでにアップロードされていることを確認します。Edge Gateway へのサービス証明書の追加を参照してください。
- L2 VPN サービスを有効にするには、サーバのリスナー IP アドレス、リスナー ポート、暗号化アルゴリズム、および少なくとも 1 つのピア サイトを構成しておく必要があります。

手順

1 [L2 VPN] タブで、L2 VPN モードの [サーバ] を選択します。

2 [サーバー グローバル] タブで、L2 VPN サーバのグローバル構成の詳細を設定します。

オプション	アクション
リスナー IP アドレス	Edge Gateway の外部インターフェイスのプライマリまたはセカンダリ IP アドレスを選択します。
リスナー ポート	組織のニーズに合わせて、表示される値を編集します。 L2 VPN サービスのデフォルト ポートは 443 です。
暗号化アルゴリズム	サーバとクライアント間の通信に使用する暗号化アルゴリズムを選択します。
サービス証明書の詳細	[サーバ証明書を変更] をクリックして、L2 VPN サーバにバインドする証明書を選択します。 [サーバ証明書を変更] ウィンドウで、[サーバ証明書の検証] を有効にし、リストからサーバ証明書を選択して [OK] をクリックします。

3 ピア サイトを構成するには、[サーバー サイト] タブをクリックします。

4 [追加] () ボタンをクリックします。

5 L2 VPN ピア サイトの設定をします。

オプション	アクション
有効	このピア サイトを有効にします。
名前	ピア サイトの一意の名前を入力します。
説明	(オプション) 説明を入力します。
ユーザー ID **パスワード** **パスワードを確認**	ピア サイトの認証に使用するユーザー名とパスワードを入力します。 ピア サイトのユーザー認証情報は、クライアント側の認証情報と同じにする必要があります。
拡張インターフェイス	クライアントで拡張されるサブインターフェイスを 1 つ以上選択します。 選択できるサブインターフェイスは、Edge Gateway でサブインターフェイスとして構成された組織仮想データセンター ネットワークのサブインターフェイスです。
出力方向最適化ゲートウェイ アドレス	(オプション) 仮想マシンのデフォルト ゲートウェイが 2 つのサイトで同じである場合は、L2 VPN トンネルを介してトラフィックをローカルに経路指定またはブロックするサブインターフェイスのゲートウェイ IP アドレスを入力します。

6 [保持] をクリックします。

7 [変更を保存] をクリックします。

保存操作が完了するまでに 1 分ほどかかることがあります。

次のステップ

この Edge ゲートウェイで L2 VPN サービスを有効にします。Edge Gateway での L2 VPN サービスの有効化を参照してください。

L2 VPN クライアントとしての Edge Gateway の構成

L2 VPN クライアントは、ターゲット NSX Edge（L2 VPN サーバ）との通信を開始するソース NSX Edge です。

前提条件

- [L2 VPN] 画面への移動。
- この L2 VPN クライアントが、サーバ証明書を使用する L2 VPN サーバに接続している場合は、この L2 VPN クライアントのサーバ証明書を検証できるようにするために、対応する認証局 (CA) 証明書が Edge Gateway にアップロードされていることを確認します。SSL 証明書の信頼性検証のための Edge Gateway への CA 証明書の追加を参照してください。

手順

1 [L2 VPN] タブで、L2 VPN モードの [クライアント] を選択します。

2 [クライアント グローバル] タブで、L2 VPN クライアントのグローバル構成の詳細を設定します。

オプション	説明
サーバ アドレス	このクライアントが接続する L2 VPN サーバの IP アドレスを入力します。
サーバ ポート	クライアントが接続する L2 VPN サーバのポートを入力します。 デフォルト ポートは 443 です。
暗号化アルゴリズム	サーバと通信するための暗号化アルゴリズムを選択します。
拡張インターフェイス	サーバに拡張するサブインターフェイスを選択します。 選択できるサブインターフェイスは、Edge Gateway でサブインターフェイスとして構成された組織仮想データセンター ネットワークのサブインターフェイスです。
出力方向最適化ゲートウェイ アドレス	（オプション）仮想マシンのデフォルト ゲートウェイが 2 つのサイト間で同じ場合、サブインターフェイスのゲートウェイ IP アドレスか、トラフィックをトンネル経由でフローさせない IP アドレスを入力します。
ユーザー詳細	サーバ認証で使用するユーザー ID とパスワードを入力します。

3 [変更を保存] をクリックします。

保存操作が完了するまでに 1 分ほどかかることがあります。

4 （オプション） 詳細オプションを設定するには、[クライアント詳細] タブをクリックします。

5 この L2 VPN クライアント Edge がインターネットに直接アクセスできず、プロキシ サーバを使用して L2 VPN サーバ Edge にアクセスする必要がある場合は、プロキシ設定を指定します。

オプション	説明
セキュア プロキシの有効化	選択してセキュアなプロキシを有効にします。
アドレス	プロキシ サーバの IP アドレスを入力します。
ポート	プロキシ サーバ ポートを入力します。
ユーザー名 **パスワード**	プロキシ サーバの認証情報を入力します。

6 サーバ認定の検証を有効にするには、[CA 証明書を変更] をクリックし、適切な CA 証明書を選択します。

7 [変更を保存] をクリックします。

保存操作が完了するまでに 1 分ほどかかることがあります。

次のステップ

この Edge ゲートウェイで L2 VPN サービスを有効にします。Edge Gateway での L2 VPN サービスの有効化を参照してください。

Edge Gateway での L2 VPN サービスの有効化

必要な L2 VPN 設定が行われている場合は、Edge Gateway で L2 VPN サービスを有効にできます。

注： この Edge Gateway で HA がすでに構成されている場合、Edge Gateway に 1 つ以上の内部インターフェイスを確実に構成します。1 つのインターフェイスだけがあり、そのインターフェイスが HA 機能によってすでに使用されている場合、同じ内部インターフェイス上の L2 VPN 構成は機能しません。

前提条件

- この Edge Gateway が L2 VPN サーバ（宛先の NSX Edge）の場合、L2 VPN サーバの必要な設定が行われており、1 つ以上の L2 VPN ピア サイトが構成されていることを確認します。L2 VPN サーバとしての Edge ゲートウェイ の構成で説明されている手順を参照してください。
- この Edge Gateway が L2 VPN クライアント（送信元 NSX Edge）の場合、L2 VPN クライアントが設定されていることを確認します。L2 VPN クライアントとしての Edge Gateway の構成で説明されている手順を参照してください。
- [L2 VPN] 画面への移動。

手順

1 [L2 VPN] タブで [有効化] 切り替えボタンをクリックします。

2 [変更を保存] をクリックします。

結果

Edge Gateway の L2 VPN サービスがアクティブになります。

次のステップ

ファイアウォールのインターネット側で NAT またはファイアウォール ルールを作成し、L2 VPN サーバが L2 VPN クライアントに接続できるようにします。

Edge ゲートウェイからの L2 VPN サービス構成の削除

Edge Gateway の既存の L2 VPN サービス構成は削除することができます。このアクションにより、Edge ゲートウェイの L2 VPN サービスも無効になります。

前提条件

[L2 VPN] 画面への移動

手順

1 [L2 VPN] 画面の一番下までスクロールし、[構成の削除] をクリックします。

2 削除を確定するには、[OK] をクリックします。

結果

L2 VPN サービスが無効になり、構成の詳細が Edge ゲートウェイから削除されます。

SSL 証明書の管理

vCloud Director 環境内の NSX ソフトウェアは、Edge ゲートウェイに設定した SSL VPN-Plus および IPsec VPN トンネルで Secure Sockets Layer (SSL) 証明書を使用する機能を提供します。

vCloud Director 環境の Edge ゲートウェイでは、自己署名証明書、認証局 (CA) 署名付き証明書、および CA によって生成、署名された証明書がサポートされます。証明書署名リクエスト (CSR) の生成、証明書のインポート、インポートした証明書の管理、証明書失効リスト (CRL) の作成を実行できます。

組織仮想データセンターでの証明書の使用について

vCloud Director 組織仮想データセンターの以下のネットワーク領域について、証明書を管理できます。

- 組織仮想データセンター ネットワークとリモート ネットワークの間の IPsec VPN トンネル
- プライベート ネットワークのリモート ユーザーと組織仮想データセンター内の Web リソースの間の SSL VPN-Plus 接続
- 2 つの NSX Edge ゲートウェイの間の L2 VPN トンネル
- 組織仮想データセンターでロード バランシングが設定されている仮想サーバおよびプール サーバ

クライアント証明書の使用方法

CAI コマンドまたは REST 呼び出しを通じてクライアント証明書を作成できます。その後、この証明書をリモート ユーザーに配布し、リモート ユーザーが証明書を各自の Web ブラウザにインストールできます。

クライアント証明書の導入の主なメリットは、各リモート ユーザーに関するリファレンス クライアント証明書を保存し、リモート ユーザーが提示するクライアント証明書に照らして確認できるという点にあります。特定のユーザーからの今後の接続を防ぐために、セキュリティ サーバのクライアント証明書のリストからリファレンス証明書を削除することができます。証明書を削除すると、そのユーザーからの接続が拒否されます。

Edge Gateway の証明書署名リクエストの生成

認証局 (CA) に署名付き証明書を要求するか、自己署名証明書を作成するには、Edge Gateway の証明書署名リクエスト (CSR) を生成しておく必要があります。

CSR は、SSL 証明書を必要とする NSX Edge Gateway で生成する必要があるエンコードされたファイルです。CSR を使用すると、会社名とドメイン名を識別する情報とともにパブリック キーを送信する方法が標準化されます。

Edge Gateway に保存しておく必要がある、一致するプライベート キーのファイルを使用して CSR を生成します。CSR には、一致するパブリック キーと他の情報（組織の名前、場所、ドメイン名など）が含まれます。

手順

1 Edge Gateway サービスを開きます。

a メイン メニュー (☰) から、[クラウド リソース] を選択します。

b 左側のパネルで [Edge ゲートウェイ] をクリックします。

c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[サービス] をクリックします。

2 [証明書] タブをクリックします。

3 [証明書] タブで [CSR] をクリックします。

4 CSR の次のオプションを設定します。

オプション	説明
コモン ネーム	使用する証明書の対象組織の完全修飾ドメイン名 (FQDN) を入力します（`www.example.com` など）。 コモン ネームに `http://` または `https://` のプリフィックスを含めないでください。
組織単位	このフィールドは、この証明書が関連付けられている vCloud Director 組織内の部門を区別する場合に使用します。「エンジニアリング」や「販売」などを入力します。
組織名	どの名前で会社が法的に登録されているかを入力します。 記載する組織は、証明書要求内のドメイン名の法的登録者でなければなりません。
地域	会社が法的に登録されている市または地域を入力します。
都道府県名	会社が法的に登録されている都道府県の完全な名前を入力します（短縮形を使用しない）。
国コード	会社が法的に登録されている国の名前を入力します。
プライベート キー アルゴリズム	証明書のキー タイプ（RSA または DSA）を入力します。 通常は RSA を使用します。キー タイプは、ホスト間の通信の暗号化アルゴリズムを定義します。 **注：** SSL VPN-Plus は RSA 証明書のみをサポートします。
キーのサイズ	キー サイズをビット数で入力します。 最小サイズは、2,048 ビットです。
説明	（オプション）証明書の説明を入力します。

5 [保持] をクリックします。

CSR が生成され、CSR タイプの新しいエントリが画面上のリストに追加されます。

結果

画面上のリストで CSR タイプのエントリを選択すると、その CSR の詳細が画面に表示されます。表示された、CSR の PEM 形式のデータをコピーし、それを認証局 (CA) に送信して CA 署名付き証明書を取得できます。

次のステップ

CSR を使用してサービス証明書を作成するには、次の 2 つのオプションのいずれかを使用します。

- CSR を CA に送信して、CA 署名付き証明書を取得します。認証局 (CA) から署名付き証明書を受け取ったら、署名付き証明書をシステムにインポートします。Edge Gateway 用に生成された CSR に対応する CA 署名付き証明書のインポートを参照してください。
- CSR を使用して、自己署名証明書を作成します。自己署名サービス証明書の構成 を参照してください。

Edge Gateway 用に生成された CSR に対応する CA 署名付き証明書のインポート

証明書署名リクエスト (CSR) を生成し、その CSR に基づく CA 署名付き証明書を取得した後、CA 署名付き証明書をインポートして Edge Gateway で使用できます。

前提条件

CSR に対応する CA 署名付き証明書を取得していることを確認します。CA 署名付き証明書内のプライベート キーが、選択した CSR のプライベート キーと一致しない場合、インポート プロセスは失敗します。

手順

1 Edge Gateway サービスを開きます。

   a メイン メニュー (☰) から、[クラウド リソース] を選択します。

   b 左側のパネルで [Edge ゲートウェイ] をクリックします。

   c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[サービス] をクリックします。

2 [証明書] タブをクリックします。

3 画面上のテーブルで、インポートする CA 署名付き証明書の対象の CSR を選択します。

4 署名付き証明書をインポートします。

   a [CSR 用に生成された署名付き証明書] をクリックします。

   b CA 署名証明書の PEM データを指定します。

      - 参照可能なシステム上の PEM ファイルにデータがある場合は、[アップロード] ボタンをクリックしてそのファイルを参照し、選択します。
      - PEM データをコピーして貼り付けることができる場合、[署名付き証明書 (PEM 形式)] フィールドに PEM データを貼り付けます。

        `------BEGIN CERTIFICATE------` と `------END CERTIFICATE------` の行を含めます。

   c （オプション） 説明を入力します。

   d [保持] をクリックします。

   注： CA 署名付き証明書内のプライベート キーが、[証明書] 画面で選択した CSR のプライベート キーと一致しない場合、インポート プロセスは失敗します。

結果

サービス証明書タイプの CA 署名付き証明書が画面上のリストに表示されます。

次のステップ

必要に応じて、SSL VPN-Plus トンネルまたは IPsec VPN トンネルに CA 署名付き証明書を接続します。SSL VPN サーバの設定および グローバル IPsec VPN 設定の指定 を参照してください。

自己署名サービス証明書の構成

Edge Gateway の VPN 関連の機能で使用するために、Edge Gateway に自己署名サービス証明書を構成できます。また、自己署名証明書を作成、インストール、および管理できます。

サービス証明書が [証明書] 画面で使用可能な場合は、Edge Gateway の VPN 関連の設定を行うときにそのサービスの証明書を指定できます。VPN は、その VPN にアクセスするクライアントに指定されたサービス証明書を提示します。

前提条件

1 つ以上の CSR が Edge Gateway の [証明書] 画面で使用可能になっていること。Edge Gateway の証明書署名リクエストの生成を参照してください。

手順

1 Edge Gateway サービスを開きます。

   a メイン メニュー (☰) から、[クラウド リソース] を選択します。

   b 左側のパネルで [Edge ゲートウェイ] をクリックします。

   c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[サービス] をクリックします。

2 [証明書] タブをクリックします。

3 この自己署名証明書に使用する CSR をリストから選択し、[CSR を自己署名] をクリックします。

4 自己署名証明書の有効日数を入力します。

5 [保持] をクリックします。

   システムが自己署名証明書を生成し、[サービス証明書] タイプの新しいエントリを画面上のリストに追加します。

結果

自己署名証明書は、Edge Gateway で使用可能です。画面上のリストで [サービス証明書] タイプのエントリを選択すると、その詳細が画面に表示されます。

SSL 証明書の信頼性検証のための Edge Gateway への CA 証明書の追加

Edge Gateway に CA 証明書を追加すると、認証のために Edge Gateway に提示された SSL 証明書（通常は Edge Gateway への VPN 接続で使用されるクライアント証明書）の信頼性を検証できます。

通常は、会社または組織のルート証明書を CA 証明書として追加します。一般的な用途は、証明書を使用して VPN クライアントを認証する際の SSL VPN です。クライアント証明書は VPN クライアントに配布でき、VPN クライアントからの接続時にそのクライアント証明書が CA 証明書に対して検証されます。

注： CA 証明書を追加する際、通常は関連する証明書失効リスト (CRL) を設定します。CRL は、失効した証明書を提示するクライアントを阻止します。Edge Gateway への証明書失効リストの追加を参照してください。

前提条件

PEM 形式の CA 証明書のデータがあることを確認します。ユーザー インターフェイスで、CA 証明書の PEM データを貼り付けるか、そのデータが格納されている、ネットワークで利用可能なファイルをローカル システム内で参照することができます。

手順

1 Edge Gateway サービスを開きます。

   a メイン メニュー (☰) から、[クラウド リソース] を選択します。

   b 左側のパネルで [Edge ゲートウェイ] をクリックします。

   c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[サービス] をクリックします。

2 [証明書] タブをクリックします。

3 [CA 証明書] をクリックします。

4 CA 証明書のデータを提供します。

   - 参照可能なシステム上の PEM ファイルにデータがある場合は、[アップロード] ボタンをクリックしてそのファイルを参照し、選択します。
   - PEM データのコピーと貼り付けが可能な場合は、[CA 証明書 (PEM 形式)] フィールドに貼り付けます。

     `-----BEGIN CERTIFICATE-----` と `-----END CERTIFICATE-----` の行を含めます。

5 （オプション） 説明を入力します。

6 [保持] をクリックします。

結果

[CA 証明書] タイプの CA 証明書が画面上のリストに表示されます。Edge Gateway の VPN 関連の設定を行うときに、この CA 証明書を指定できるようになりました。

Edge Gateway への証明書失効リストの追加

証明書失効リスト (CRL) は、発行元の証明書機関 (CA) から失効と主張されているデジタル証明書のリストです。これを使用すると、失効した証明書を提示するユーザーを信頼しないように、システムを更新できます。Edge Gateway に CRL を追加できます。

『NSX 管理ガイド』の説明のように、CRL には次の項目が含まれます。

- 失効した証明書と失効の理由

- 証明書の発行日
- 証明書を発行した機関
- 次のリリースの提案日

ある潜在的ユーザーがサーバへのアクセスを試みた場合、サーバは、その特定のユーザーに関する CRL エントリに基づいてアクセスの許可または拒否を行います。

手順

1 Edge Gateway サービスを開きます。

   a メイン メニュー (☰) から、[クラウド リソース] を選択します。

   b 左側のパネルで [Edge ゲートウェイ] をクリックします。

   c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[サービス] をクリックします。

2 [証明書] タブをクリックします。

3 [CRL] をクリックします。

4 CRL のデータを提供します。

   - 参照可能なシステム上の PEM ファイルにデータがある場合は、[アップロード] ボタンをクリックしてそのファイルを参照し、選択します。
   - PEM データのコピーと貼り付けが可能な場合は、[CRL (PEM 形式)] フィールドに貼り付けます。

     `-----BEGIN X509 CRL-----` と `-----END X509 CRL-----` の行を含めます。

5 （オプション） 説明を入力します。

6 [保持] をクリックします。

結果

CRL が画面上のリストに表示されます。

Edge Gateway へのサービス証明書の追加

Edge Gateway にサービス証明書を追加すると、これらの証明書が Edge Gateway の VPN 関連設定で使用できるようになります。[証明書] 画面にサービス証明書を追加できます。

前提条件

サービス証明書とそのプライベート キーが PEM 形式になっていることを確認します。ユーザー インターフェイスで、PEM データを貼り付けるか、そのデータを格納する、ローカル システムから利用可能なネットワーク内のファイルを参照できます。

手順

1 Edge Gateway サービスを開きます。

   a メイン メニュー (☰) から、[クラウド リソース] を選択します。

   b 左側のパネルで [Edge ゲートウェイ] をクリックします。

   c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[サービス] をクリックします。

2 [証明書] タブをクリックします。

3 [サービス証明書] をクリックします。

4 サービス証明書のデータを PEM 形式で入力します。

   - 参照可能なシステム上の PEM ファイルにデータがある場合は、[アップロード] ボタンをクリックしてそのファイルを参照し、選択します。
   - PEM データのコピーと貼り付けが可能な場合は、[サービス証明書 (PEM 形式)] フィールドに貼り付けます。

     `-----BEGIN CERTIFICATE-----` と `-----END CERTIFICATE-----` の行を含めます。

5 証明書プライベート キーのデータを PEM 形式で入力します。

   - 参照可能なシステム上の PEM ファイルにデータがある場合は、[アップロード] ボタンをクリックしてそのファイルを参照し、選択します。
   - PEM データのコピーと貼り付けが可能な場合は、[プライベート キー (PEM 形式)] フィールドに貼り付けます。

     `-----BEGIN RSA PRIVATE KEY-----` と `-----END RSA PRIVATE KEY-----` の行を含めます。

6 プライベート キーのパスフレーズを入力して確認します。

7 （オプション） 説明を入力します。

8 [保持] をクリックします。

結果

[サービス証明書] タイプの証明書が画面上のリストに表示されます。Edge Gateway の VPN 関連の設定を行うときに、このサービス証明書を選択できるようになりました。

オブジェクトのグループ分け（カスタム）

NSX 環境の vCloud Director ソフトウェアは、特定のエンティティのセットおよびグループを定義する機能を提供します。これは、他のネットワーク関連の設定（ファイアウォール ルールの設定など）を指定するときに使用できます。

ファイアウォール ルールと DHCP リレー設定で使用するための IP アドレス セットの作成

IP セットは、組織仮想データセンター レベルで作成できる IP アドレスのグループのことです。IP セットは、ファイアウォール ルールまたは DHCP リレー設定で送信元または宛先として使用することができます。

IP セットは、[オブジェクトのグループ分け] 画面を使用して作成します。このページを開くには、組織 VDC の分散ファイアウォール設定に移動するか、組織 VDC に属する Edge ゲートウェイのサービス設定に移動する必要があります。

手順

1 [オブジェクトのグループ分け] ページを開きます。

オプション	アクション
組織 VDC の分散ファイアウォール設定から	a メイン メニュー (☰) から、[クラウド リソース] を選択します。 b 左側のパネルで [組織 VDC] をクリックします。 c ターゲット組織仮想データセンターの名前の横にあるラジオ ボタンを選択して、[ファイアウォールの管理] をクリックします。 d [オブジェクトのグループ分け] タブをクリックします。
組織 VDC の Edge Gateway のサービス設定から	a メイン メニュー (☰) から、[クラウド リソース] を選択します。 b 左側のパネルで [Edge ゲートウェイ] をクリックします。 c ターゲット組織仮想データセンターに属する Edge Gateway の名前の横にあるラジオ ボタンを選択して、[サービス] をクリックします。 d [オブジェクトのグループ分け] タブをクリックします。

2 [IP アドレス セット] タブをクリックします。

定義済みの IP アドレス セットが画面に表示されます。

3 IP アドレス セットを追加するには、[作成] (+) ボタンをクリックします。

4 IP セットに含める IP アドレスの他に、IP セットの名前と、オプションで IP セットの説明を入力します。

5 この IP セットを保存するには、[保持] をクリックします。

結果

これで、新しい IP セットをファイアウォール ルールまたは DHCP リレー構成でソースまたはターゲットとして選択できます。

ファイアウォール ルールで使用するための MAC アドレス セットの作成

MAC セットは、組織仮想データセンター レベルで作成できる MAC アドレスのグループです。ファイアウォール ルールの送信元または宛先として MAC セットを使用できます。

MAC セットを作成するには、[オブジェクトのグループ分け] 画面を使用します。この画面を開くには、組織 VDC の分散ファイアウォール設定に移動するか、組織 VDC に属する Edge Gateway のサービス設定に移動する必要があります。

手順

1 [オブジェクトのグループ分け] ページを開きます。

オプション	アクション
組織 VDC の分散ファイアウォール設定から	a メイン メニュー (☰) から、[クラウド リソース] を選択します。 b 左側のパネルで [組織 VDC] をクリックします。 c ターゲット組織仮想データセンターの名前の横にあるラジオ ボタンを選択して、[ファイアウォールの管理] をクリックします。 d [オブジェクトのグループ分け] タブをクリックします。
組織 VDC の Edge Gateway のサービス設定から	a メイン メニュー (☰) から、[クラウド リソース] を選択します。 b 左側のパネルで [Edge ゲートウェイ] をクリックします。 c ターゲット組織仮想データセンターに属する Edge Gateway の名前の横にあるラジオ ボタンを選択して、[サービス] をクリックします。 d [オブジェクトのグループ分け] タブをクリックします。

2 [MAC アドレス セット] タブをクリックします。

定義済みの MAC アドレス セットが画面に表示されます。

3 MAC アドレス セットを追加するには、[作成] (+) ボタンをクリックします。

4 セット名を入力し、オプションで説明、および MAC アドレス セットに含める MAC アドレスを入力します。

5 MAC アドレス セットを保存するには、[保持] をクリックします。

結果

これで、新しい MAC アドレス セットをファイアウォール ルールでソースまたはターゲットとして選択できます。

ファイアウォール ルールで使用可能なサービスの表示

ファイアウォール ルールで使用できるサービスのリストを表示できます。この場合、サービスとはプロトコルとポートの組み合わせです。

使用可能なサービスを表示するには、[オブジェクトのグループ分け] 画面を使用します。この画面を開くには、組織 VDC の分散ファイアウォール設定に移動するか、組織 VDC に属する Edge Gateway のサービス設定に移動する必要があります。

手順

1 [オブジェクトのグループ分け] ページを開きます。

オプション	アクション
組織 VDC の分散ファイアウォール設定から	a メイン メニュー (☰) から、[クラウド リソース] を選択します。 b 左側のパネルで [組織 VDC] をクリックします。 c ターゲット組織仮想データセンターの名前の横にあるラジオ ボタンを選択して、[ファイアウォールの管理] をクリックします。 d [オブジェクトのグループ分け] タブをクリックします。
組織 VDC の Edge Gateway のサービス設定から	a メイン メニュー (☰) から、[クラウド リソース] を選択します。 b 左側のパネルで [Edge ゲートウェイ] をクリックします。 c ターゲット組織仮想データセンターに属する Edge Gateway の名前の横にあるラジオ ボタンを選択して、[サービス] をクリックします。 d [オブジェクトのグループ分け] タブをクリックします。

2 [サービス] タブをクリックします。

結果

使用可能なサービスが画面に表示されます。

ファイアウォール ルールで使用可能なサービス グループの表示

ファイアウォール ルールで使用できるサービス グループのリストを表示できます。この場合、サービスとはプロトコルとポートの組み合わせであり、サービス グループとはサービスまたは他のサービス グループから成るグループです。

使用可能なサービス グループを表示するには、[オブジェクトのグループ分け] 画面を使用します。この画面を開くには、組織 VDC の分散ファイアウォール設定に移動するか、組織 VDC に属する Edge Gateway のサービス設定に移動する必要があります。

手順

1 [オブジェクトのグループ分け] ページを開きます。

オプション	アクション
組織 VDC の分散ファイアウォール設定から	a メイン メニュー (☰) から、[クラウド リソース] を選択します。 b 左側のパネルで [組織 VDC] をクリックします。 c ターゲット組織仮想データセンターの名前の横にあるラジオ ボタンを選択して、[ファイアウォールの管理] をクリックします。 d [オブジェクトのグループ分け] タブをクリックします。
組織 VDC の Edge Gateway のサービス設定から	a メイン メニュー (☰) から、[クラウド リソース] を選択します。 b 左側のパネルで [Edge ゲートウェイ] をクリックします。 c ターゲット組織仮想データセンターに属する Edge Gateway の名前の横にあるラジオ ボタンを選択して、[サービス] をクリックします。 d [オブジェクトのグループ分け] タブをクリックします。

2 [サービス グループ] タブをクリックします。

結果

使用可能なサービス グループが画面に表示されます。[説明] 列には、サービス グループごとにグループ分けされたサービスが表示されます。

Edge Gateway のネットワーク使用と IP 割り当ての表示

Edge Gateway のネットワーク、および IP アドレス プールの使用とサブネットに関する情報を表示できます。各ネットワークに割り当てられた IP アドレスを表示することもできます。

手順

1 メイン メニュー (☰) から、[クラウド リソース] を選択します。

2 左側のパネルで [Edge ゲートウェイ] をクリックし、ターゲット Edge ゲートウェイの名前をクリックします。

3 外部ネットワーク、および IP アドレス プールの使用とサブネットに関する情報を表示するには、[外部ネットワーク] - [ネットワークおよびサブネット] タブをクリックします。

4 外部ネットワーク、および IP アドレスとカテゴリに関する情報を表示するには、[外部ネットワーク] - [IP の割り当て] タブをクリックします。

Edge ゲートウェイのプロパティの編集

Edge Gateway での分散ルーティングの有効化または無効化

Edge Gateway で vCloud Director 分散ルーティングを有効にすると、組織管理者は、この Edge Gateway に接続された分散インターフェイスを持つ経路指定された組織仮想データセンター ネットワークを多数作成できるようになります。これらのネットワーク上のトラフィックは、仮想マシン間の通信用に最適化されます。

前提条件

バッキング NSX Manager インスタンスには、NSX Controller クラスタが構成されています。『NSX 管理ガイド』を参照してください。

手順

1. メイン メニュー (☰) から、[クラウド リソース] を選択します。
2. 左側のパネルで [Edge ゲートウェイ] をクリックします。
3. ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[分散ルーティングの有効化] または [分散ルーティングの無効化] をクリックします。
4. 確認するには、[OK] をクリックします。

外部ネットワークと Edge Gateway 設定の変更

外部ネットワークと Edge Gateway の設定を変更するには、Edge Gateway の作成に使用したウィザードと同じページが含まれている [Edge ゲートウェイの編集] ウィザードを使用します。

Edge Gateway を追加したときの設定を変更できます。Edge ゲートウェイの追加を参照してください。

分散ルーティングの設定を変更するには、Edge Gateway での分散ルーティングの有効化または無効化を参照してください。

手順

1. メイン メニュー (☰) から、[クラウド リソース] を選択します。
2. 左側のパネルで [Edge ゲートウェイ] をクリックします。
3. 変更する Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[編集] をクリックします。
4. Edge Gateway の設定を変更するには、[次へ] をクリックして [Edge ゲートウェイの編集] ウィザードのページに移動し、[設定内容の確認] ページで [完了] をクリックします。

Edge Gateway の全般設定の編集

Edge Gateway の名前と説明の変更、FIPS モードと高可用性状態の有効/無効の切り替え、Edge Gateway のサイズ設定の変更が可能です。

手順

1. メイン メニュー (☰) から、[クラウド リソース] を選択します。
2. 左側のパネルで [Edge ゲートウェイ] をクリックし、ターゲット Edge ゲートウェイの名前をクリックします。

3 [全般] タブで、右上隅にある [編集] をクリックします。

4 （オプション） Edge Gateway の名前と説明を編集します。

5 （オプション） Edge Gateway の全般設定をそれぞれ有効または無効にします。

全般設定	説明
FIPS モード	NSX FIPS モードを使用するよう Edge ゲートウェイを構成します。
高可用性	バックアップ Edge ゲートウェイへの自動フェイルオーバーを有効にします。

6 （オプション） システム リソースの Edge Gateway 構成を変更します。

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 リソースが少なくて済みます。
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使用します。
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。

7 変更を確定するには、[保存] をクリックします。

Edge Gateway のデフォルト ゲートウェイの編集

Edge Gateway がデフォルト ゲートウェイとして使用するネットワークを変更できます。

手順

1 メイン メニュー (☰) から、[クラウド リソース] を選択します。

2 左側のパネルで [Edge ゲートウェイ] をクリックし、ターゲット Edge ゲートウェイの名前をクリックします。

3 [外部ネットワーク] - [デフォルト ゲートウェイ] タブで、右上隅にある [編集] をクリックします。

4 （オプション） ネットワークをデフォルト ゲートウェイとして構成します。

   a [デフォルト ゲートウェイの構成] 切り替えを有効にします。

   b ターゲット外部ネットワークの名前の横にあるラジオ ボタンを選択し、宛先 IP アドレスの横にあるラジオ ボタンを選択します。

   c （オプション） [DNS リレーにデフォルト ゲートウェイを使用] 切り替えを有効にします。

5 変更を確定するには、[保存] をクリックします。

Edge Gateway の IP アドレスの設定の編集

Edge Gateway の外部ネットワークの IP アドレス設定を変更できます。

手順

1 メイン メニュー (☰) から、[クラウド リソース] を選択します。

2 左側のパネルで [Edge ゲートウェイ] をクリックし、ターゲット Edge ゲートウェイの名前をクリックします。

3 [外部ネットワーク] - [IP アドレス設定] タブで [編集] をクリックします。

4 Edge Gateway のネットワークごとに、[IP アドレス] セルに IP アドレスを入力するか、セルを空白のままにします。

ネットワークの IP アドレスを入力しない場合は、このネットワークに任意の IP アドレスが割り当てられます。

5 変更を確定するには、[保存] をクリックします。

Edge ゲートウェイ上の細分割り当てされた IP アドレス プールの編集

Edge ゲートウェイ上の外部ネットワークの使用可能な IP アドレス プールを複数の固定 IP アドレス プールに細分割り当てすることができます。

注： 細分割り当てによる Edge Gateway への IP アドレスの割り当ては、プロバイダが IP アドレスの所有権をゲートウェイに割り当てるプロセスです。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 メイン メニュー (☰) から、[クラウド リソース] を選択します。

2 左側のパネルで [Edge ゲートウェイ] をクリックし、ターゲット Edge ゲートウェイの名前をクリックします。

3 [外部ネットワーク] - [細分割り当て済み IP プール] タブの順にクリックします。

この Edge ゲートウェイ上のそれぞれの外部ネットワークについて現在の細分割り当て済み IP アドレス プールが表示されます。

4 外部ネットワーク名の横にあるラジオ ボタンをクリックして、[編集] をクリックします。

この外部ネットワークに使用可能な IP アドレス プールと、現在細分割り当てされている IP アドレス プール（設定されている場合）が表示されます。

5 この外部ネットワークに細分割り当てされている IP アドレス プールを編集し、[保存] をクリックします。

使用可能な IP アドレス プールの範囲から IP アドレスと IP アドレス範囲を追加、変更、および削除できます。

結果

システムは重複する IP アドレス範囲を結合します。

Edge ゲートウェイ上のレート制限の編集

Edge ゲートウェイのそれぞれの外部ネットワークについて着信および発信のレート制限を設定できます。

レート制限は、静的結合の分散ポート グループによりバッ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 メイン メニュー (☰) から、[クラウド リソース] を選択します。

2 左側のパネルで [Edge ゲートウェイ] をクリックし、ターゲット Edge ゲートウェイの名前をクリックします。

3 [外部ネットワーク] - [レート制限] タブで、右上隅にある [編集] をクリックします。

この Edge ゲートウェイ上のそれぞれの外部ネットワークについて現在のレート制限が表示されます。

4 レート制限を編集して、[保存] をクリックします。

Edge ゲートウェイ上のそれぞれの外部ネットワークについて、レート制限を有効または無効にしたり、着信および発信レートを変更することができます。

Edge Gateway の再デプロイ

新しい Edge Gateway アプライアンスを削除し、最新の構成を使用してデプロイすることができます。

Edge サービスが予期されたとおりに動作しない場合は、Edge Gateway アプライアンスを再デプロイできます。

レガシーの Edge Gateway を再デプロイし、Edge Gateway を新しく作成した Edge クラスタに移行できます。

Edge Gateway を再デプロイすると、vCloud Director は Edge Gateway を削除した後、最新の構成で再作成します。

手順

1 メイン メニュー (☰) から、[クラウド リソース] を選択します。

2 左側のパネルで [Edge ゲートウェイ] をクリックします。

3 対象の Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[再デプロイ] をクリックします。

4 確認するには、[OK] をクリックします。

結果

Edge Gateway 仮想マシンが新しい仮想マシンに置き換えられ、すべてのサービスがリストアされます。

Edge ゲートウェイの削除

組織仮想データセンターから Edge Gateway を削除できます。

前提条件

対象の Edge Gateway を使用するすべての組織仮想データセンター ネットワークを削除します。

手順

1 メイン メニュー (☰) から、[クラウド リソース] を選択します。

2 左側のパネルで [Edge ゲートウェイ] をクリックします。

3 対象の Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[削除] をクリックします。

4 確定するには、[削除] をクリックします。

Edge Gateway の統計情報とログ

Edge Gateway の統計情報およびログを表示できます。

統計情報の表示

[Edge ゲートウェイ サービス] 画面に統計情報を表示できます。

手順

1 Edge Gateway サービスを開きます。

   a メイン メニュー (☰) から、[クラウド リソース] を選択します。

   b 左側のパネルで [Edge ゲートウェイ] をクリックします。

   c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[サービス] をクリックします。

2 [統計情報] タブをクリックします。

3 表示する統計情報のタイプに応じて、タブを移動します。

オプション	説明
接続	[接続] 画面に運用状況が示されます。この画面には、選択した Edge ゲートウェイのインターフェイスを流れるトラフィックのグラフと、ファイアウォール サービスとロード バランサー サービスの接続統計が表示されます。 ステータスを表示する期間を選択します。
IPsec VPN	[IPsec VPN] 画面には、IPsec VPN のステータスと統計情報、および各トンネルのステータスと統計情報が表示されます。
L2 VPN	[L2 VPN] 画面には、L2 VPN のステータスと統計情報が表示されます。

ログの有効化

Edge Gateway のログを有効にできます。設定を完了するには、ログ データを収集する機能のログ設定を有効にするだけでなく、Syslog サーバが収集したログ データを受信できるように設定する必要があります。[Edge 設定] 画面で Syslog サーバをすると、その Syslog サーバから記録されたデータにアクセスできるようになります。

前提条件

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

手順

1 Edge Gateway サービスを開きます。

   a メイン メニュー (☰) から、[クラウド リソース] を選択します。

   b 左側のパネルで [Edge ゲートウェイ] をクリックします。

   c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[サービス] をクリックします。

2 [Edge 設定] タブで [Syslog サーバーの編集] ボタンをクリックします。

ログが有効なサービスに対して Edge Gateway のネットワーク関連ログが記録されるように、Syslog サーバをカスタマイズできます。

vCloud Director システム管理者が vCloud Director 環境用に Syslog サーバを構成した場合は、デフォルトでこの Syslog サーバが使用され、[Edge 設定] 画面にその IP アドレスが表示されます。

3 機能ごとにログを有効にします。

- [NAT] タブで [DNAT ルール] ボタンをクリックし、[ログの有効化] 切り替えを有効にします。

  アドレス変換のログを記録します。

- [NAT] タブで [SNAT ルール] ボタンをクリックし、[ログの有効化] 切り替えを有効にします。

  アドレス変換のログを記録します。

- [ルーティング] タブで [ルーティング設定] をクリックし、[動的ルーティングの設定] で [ログの有効化] 切り替えを有効にします。

  動的ルーティングのアクティビティのログを記録します。[ログ レベル] ドロップダウン メニューで、ログを記録するメッセージ ステータス レベルの下限を選択します。

- [ロード バランサー] タブで [グローバル構成] をクリックし、[ログの有効化] 切り替えを有効にします。

  ロード バランサーのトラフィック フローのログを記録します。[ログ レベル] ドロップダウン メニューで、ログを記録するメッセージ ステータス レベルの下限を選択します。

- [VPN] タブで [IPSec VPN] - [ログ設定] の順に選択し、[ログの有効化] 切り替えを有効にします。

  ローカル サブネットとピア サブネットの間のトラフィック フローのログを記録します。[ログ レベル] ドロップダウン メニューで、ログを記録するメッセージ ステータス レベルの下限を選択します。

- [SSL VPN-Plus] タブで [全般設定] をクリックし、[ログの有効化] 切り替えを有効にします。

  SSL VPN ゲートウェイを通過するトラフィックのログを保持します。

- [SSL VPN-Plus] タブで [サーバー設定] をクリックし、[ログの有効化] 切り替えを有効にします。

  SSL VPN サーバで発生するアクティビティのログを Syslog に記録します。[ログ レベル] ドロップダウン メニューで、ログを記録するメッセージ ステータス レベルの下限を選択します。

SSH コマンドラインによる Edge Gateway へのアクセスの有効化

SSH コマンドラインによる Edge Gateway へのアクセスを有効にすることができます。

手順

1 Edge Gateway サービスを開きます。

   a メイン メニュー (☰) から、[クラウド リソース] を選択します。

   b 左側のパネルで [Edge ゲートウェイ] をクリックします。

   c ターゲット Edge Gateway の名前の横にあるラジオ ボタンをクリックして、[サービス] をクリックします。

2 [Edge 設定] タブをクリックします。

3 SSH を設定します。

オプション	説明
ユーザー名 **パスワード** **パスワードを再入力**	SSH がこの Edge Gateway にアクセスする場合に使用する認証情報を入力します。 デフォルトでは、SSH のユーザー名は admin です。
パスワードの有効期限	パスワードの有効期間を日数で入力します。
ログイン バナー	Edge Gateway への SSH 接続を開始するときにユーザーに表示されるテキストを入力します。

4 [有効] 切り替えをオンにします。

次のステップ

SSH によるこの Edge ゲートウェイへのアクセスを許可するように、該当する NAT またはファイアウォール ルールを設定します。

組織仮想データセンター ネットワークの管理

8

この章には、次のトピックが含まれています。

NSX-T 組織仮想データセンター ネットワークの管理

NSX-T 論理スイッチをベースとする組織仮想データセンター ネットワークを作成、変更、削除できるのは、システム管理者のみです。

組織仮想データセンター ネットワークを管理するには、システム管理者が Service Provider Admin Portal にログインし、ターゲット組織の vCloud Director テナント ポータルに移動する必要があります。

NSX Data Center for vSphere をベースとする組織仮想データセンター ネットワーク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。

NSX-T 組織仮想データセンター ネットワークの追加

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

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

前提条件

- ターゲット組織仮想データセンターをバッキングするプロバイダ仮想データセンターは、NSX-T Manager インスタンスに関連付けられている必要があります。
- 他の組織仮想データセンター ネットワークに使用されていない NSX-T 論理スイッチを 1 台以上作成していること。

NSX-T 論理スイッチの構成については、『NSX-T 管理ガイド』を参照してください。NSX-T Manager インスタンスでバッキング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。

手順

1 ターゲット組織の vCloud Director テナント ポータルに移動します。

   a メイン メニュー (☰) から、[クラウド リソース] を選択します。

   b [組織] で、ターゲット組織の名前をクリックします。

   この組織の vCloud Director テナント ポータルの [データセンター] ビューにリダイレクトされます。

2 組織内に複数の仮想データセンターがある場合は、ターゲット組織仮想データセンターのカードをクリックします。

3 左側のパネルの [ネットワーク] で、[ネットワーク] をクリックします。

4 [インポート] をクリックします。

   [論理スイッチのインポート] ウィザードが表示されます。

5 新しい組織仮想データセンター ネットワークの名前と、オプションで説明を入力し、[次へ] をクリックします。

6 利用可能な NSX-T 論理スイッチのリストから、スイッチ名の横にあるラジオ ボタンをクリックしてターゲット スイッチを選択し、[次へ] をクリックします。

7 ネットワークの Classless Inter-Domain Routing (CIDR) 設定を入力します。

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

   スイッチがサブネットで構成されている場合、この情報は自動入力されます。

8 （オプション） DNS 設定と固定 IP アドレス プールを指定します。

   複数の IP アドレスおよび IP アドレス範囲を追加することができます。

9 [次へ] をクリックします。

10 [設定内容の確認] ページの内容を確認して、[完了] をクリックします。

NSX-T 組織仮想データセンター ネットワークの編集

NSX-T 論理スイッチをベースとする組織仮想データセンター ネットワークの名前、説明、DNS 設定、および固定 IP アドレス プールを変更できます。ネットワークの Classless Inter-Domain Routing (CIDR) 設定は編集できません。

手順

1 ターゲット組織の vCloud Director テナント ポータルに移動します。

   a メイン メニュー (☰) から、[クラウド リソース] を選択します。

   b [組織] で、ターゲット組織の名前をクリックします。

   この組織の vCloud Director テナント ポータルの [データセンター] ビューにリダイレクトされます。

2 組織内に複数の仮想データセンターがある場合は、ターゲット組織仮想データセンターのカードをクリックします。

3 左側のパネルの [ネットワーク] で、[ネットワーク] をクリックします。

4 ターゲット ネットワーク名の横にあるラジオ ボタンをクリックして、[変更] をクリックします。

[組織 VDC ネットワークの編集] ウィザードが開きます。

5 （オプション） [全般] タブでネットワーク名および説明を編集します。

6 （オプション） [ネットワークの構成] タブで DNS 設定およびネットワークの固定 IP アドレス プールを編集します。

IP アドレスおよび IP アドレス範囲は追加、変更、および削除できます。

7 [保存] をクリックします。

NSX-T 組織仮想データセンター ネットワークの削除

不要な NSX-T 組織仮想データセンター ネットワークがある場合には、このネットワークを削除できます。

手順

1 ターゲット組織の vCloud Director テナント ポータルに移動します。

a メイン メニュー (☰) から、[クラウド リソース] を選択します。

b [組織] で、ターゲット組織の名前をクリックします。

この組織の vCloud Director テナント ポータルの [データセンター] ビューにリダイレクトされます。

2 組織内に複数の仮想データセンターがある場合は、ターゲット組織仮想データセンターのカードをクリックします。

3 左側のパネルの [ネットワーク] で、[ネットワーク] をクリックします。

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

5 確認するには、[OK] をクリックします。

SDDC および SDDC プロキシの管理

9

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 インスタンスを単独、または NSX Manager インスタンスと共に接続するを参照してください。

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キング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 の両方をバッキングできるように、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キングされる SSDC 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。組織からのプラグインの公開または公開解除を参照してください。

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。

システム管理者およびロールの管理 10

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。

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。

組織の権限

組織の権限とは、組織が使用できる権限の完全なセットを指します。組織の権限は複数の権限バンドルで構成されますが、組織管理者およびユーザーにはフラットな権限セットが表示され、テナント固有のロールを作成および変更する際に使用できるようになります。

ロールに関する用語

ロール

ロールとは、1 つまたは複数のユーザーおよびグループに割り当てることができる権限セットを指します。ユーザーまたはグループを作成またはインポートするときは、ロールを割り当てる必要があります。

プロバイダ ロール

プロバイダ ロールとは、プロバイダ組織のみが使用できるロール セットを指します。プロバイダ ロールは、プロバイダ ユーザーにのみ割り当てることができます。システム管理者は、カスタム プロバイダ ロールを作成できます。

テナント ロール

テナント ロールとは、組織が使用できるロール セットのことです。

システム管理者は、グローバル テナント ロールを作成および編集し、1 つ以上の組織に公開することができます。グローバル テナント ロールは、公開先の組織内のテナント ユーザーに割り当てることができます。組織管理者は、グローバル テナント ロールを編集できません。

注： テナント ユーザーは、組織に公開されているロール内の権限のみを使用できます。

テナント固有のロール

組織管理者は、組織に対してローカルなテナント固有のロールを作成および編集できます。テナント固有のロールは、所属先の組織内のテナント ユーザーにのみ割り当てることができます。テナント固有のロールには、組織の権限のサブセットのみを含めることができます。

テナント固有のロールの管理の詳細については、『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。

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

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 10-1. 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			
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				

表 10-1. 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
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				
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				
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				

表 10-1. 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
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				
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			

表 10-1. 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				
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

表 10-1. 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：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	
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
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。

権限バンドルの管理

システム管理者は権限バンドルを作成し、クラウド内の 1 つ以上の組織に公開できます。既存の権限バンドルを編集および削除できます。クラウド内の組織から権限バンドルの公開を解除することができます。

権限バンドルの作成

権限のセットを権限バンドルとしてグループ化し、システム内の 1 つ以上の組織に公開できます。

手順

1 メイン メニュー (☰) から、[管理] を選択します。

2 左側のパネルの [テナント アクセス コントロール] で、[権限バンドル] をクリックします。

3 [追加] をクリックします。

4 新しい権限バンドルの名前と、オプションで説明を入力します。

5 このバンドルに関連付ける権限を選択します。

権限は、関連するオブジェクトへのアクセス権を表示および管理するために、カテゴリとサブカテゴリにグループ化されています。

権限はサブカテゴリ別に表示または管理するか、グローバルに表示または管理して、個別に選択することができます。

カテゴリー	説明
アクセス コントロール	組織、権限、ロール、およびユーザーを表示して管理するための権限が含まれています。
管理	一般的な設定やマルチサイトの設定を表示して管理するための権限が含まれています。
コンピュート	組織およびプロバイダの仮想データセンター、vApp、組織仮想データセンター テンプレート、および仮想マシンの監視を表示して管理するための権限が含まれています。
拡張機能	vCloud Director プラグインおよび拡張機能を表示して管理するための権限が含まれています。
インフラストラクチャ	vSphere リソースを表示して管理するための権限が含まれています。
ライブラリ	カタログおよびカタログ項目を表示して管理するための権限が含まれています。
ネットワーク	ネットワーク リソースを表示して管理するための権限が含まれています。

6 [保存] をクリックします。

次のステップ

新しく作成した権限バンドルは、システム内の 1 つ以上の組織に公開できます。権限バンドルの公開または公開の解除を参照してください。

権限バンドルの公開または公開の解除

権限バンドルをシステム内の 1 つ以上の組織に公開できます。権限バンドルを組織に公開すると、このバンドル内の権限は組織の権限セットの一部となります。

組織の権限は複数の権限バンドルで構成されますが、組織管理者およびユーザーにはフラットな権限セットが表示され、これらを使用してロールを作成および変更できるようになります。

手順

1 メイン メニュー (☰) から、[管理] を選択します。

2 左側のパネルの [テナント アクセス コントロール] で、[権限バンドル] をクリックします。

3 ターゲット バンドルの横にあるラジオ ボタンを選択して、[公開] をクリックします。

4 バンドルを公開するには：

a [テナントに公開] を選択します。

b ロールを公開する組織を選択します。

- バンドルをシステム内のすべての既存の組織および新規に作成された組織に公開する場合は、[すべてのテナントに公開] を選択します。
- システム内の特定の組織にバンドルを公開する場合は、組織を個別に選択します。

5 バンドルの公開を解除するには：

- システム内のすべての組織からバンドルの公開を解除する場合は、[テナントに公開] を選択解除します。
- システム内の特定の組織からバンドルを公開解除する場合は、[すべてのテナントに公開] を選択解除して、組織を個別に選択解除します。

6 [保存] をクリックします。

結果

公開されたバンドル内の権限は選択した組織内で使用することができ、これらの組織内のロールで使用することができます。

公開解除されたロール内の権限は選択した組織から削除され、これらの組織内のロールで使用できなくなります。

権限バンドルの表示および編集

権限バンドルに含まれている権限を表示できます。バンドルの名前、説明、および権限を変更できます。

手順

1 メイン メニュー (☰) から、[管理] を選択します。

2 左側のパネルの [テナント アクセス コントロール] で、[権限バンドル] をクリックします。

3 ターゲット バンドルの名前をクリックします。

権限カテゴリを展開して、バンドルに関連付けられている権限を表示できます。

4 バンドルを編集して、[保持] をクリックします。

結果

バンドルの権限を変更した場合、新しい権限セットが権限バンドルの公開先となるすべての組織に適用されます。

権限バンドルの削除

組織で使用しなくなった権限バンドルは削除することができます。

手順

1 メイン メニュー (☰) から、[管理] を選択します。

2 左側のパネルの [テナント アクセス コントロール] で、[権限バンドル] をクリックします。

3 対象のバンドルの横にあるラジオ ボタンを選択し、[削除] をクリックします。

4 確認するには、[OK] をクリックします。

グローバル テナント ロールの管理

システム管理者はグローバル テナント ロールを作成し、作成したロールをクラウド内の 1 つ以上の組織に公開できます。既存のグローバル テナント ロールを編集および削除できます。クラウド内の個別の組織でグローバル テナントロールの公開を解除できます。

vCloud Director の初回インストールおよびセットアップを行うと、システムには、すべての組織に公開されている事前定義済みのグローバル テナントのセットが含まれます。事前定義ロールとその権限を参照してください。

グローバル テナント ロールの作成

システム内の 1 つ以上の組織に公開できるグローバル テナント ロールを作成できます。

vCloud Director の初回インストールおよびセットアップ後、システムには、すべての組織に公開される事前定義済みグローバル テナント ロールが含まれています。事前定義済みロールの詳細については、「事前定義ロールとその権限」を参照してください。

システムにカスタム グローバル ロールを追加することもできます。

手順

1 メイン メニュー (☰) から、[管理] を選択します。

2 左側のパネルの [テナント アクセス コントロール] で、[グローバル ロール] をクリックします。

3 [追加] をクリックします。

4 新しいロールの名前と、オプションで説明を入力します。

5 ロールに関連付ける権限を選択します。

権限は、関連するオブジェクトへのアクセス権を表示および管理するために、カテゴリとサブカテゴリにグループ化されています。

権限はサブカテゴリ別に表示または管理するか、グローバルに表示または管理して、個別に選択することができます。

カテゴリー	説明
アクセス コントロール	組織、権限、ロール、およびユーザーを表示して管理するための権限が含まれています。
管理	一般的な設定やマルチサイトの設定を表示して管理するための権限が含まれています。
コンピュート	組織およびプロバイダの仮想データセンター、vApp、組織仮想データセンター テンプレート、および仮想マシンの監視を表示して管理するための権限が含まれています。
拡張機能	vCloud Director プラグインおよび拡張機能を表示して管理するための権限が含まれています。
インフラストラクチャ	vSphere リソースを表示して管理するための権限が含まれています。

カテゴリー	説明
ライブラリ	カタログおよびカタログ項目を表示して管理するための権限が含まれています。
ネットワーク	ネットワーク リソースを表示して管理するための権限が含まれています。

6 [保持] をクリックします。

結果

作成時、新しいグローバル テナント権限は、vCloud Director プロバイダの組織のみが利用できます。

次のステップ

新しく作成したロールは、システム内の 1 つ以上の組織に公開できます。グローバル テナント ロールの公開または公開の解除を参照してください。

グローバル テナント ロールの公開または公開の解除

グローバル テナント ロールをシステム内の 1 つ以上の組織に公開できます。ロールを組織に公開すると、このロールはテナント ロールの組織セットの一部となります。

前提条件

組織からグローバル テナント ロールの公開を解除する場合は、このロールに割り当てられたユーザーが組織内にいないことを確認します。

手順

1 メイン メニュー (☰) から、[管理] を選択します。

2 左側のパネルの [テナント アクセス コントロール] で、[グローバル ロール] をクリックします。

3 ターゲット ロールの横にあるラジオ ボタンを選択して、[公開] をクリックします。

4 ロールを公開するには：

   a [テナントに公開] を選択します。

   b ロールを公開する組織を選択します。

      - ロールをシステム内のすべての既存の組織および新規に作成された組織に公開する場合は、[すべてのテナントに公開] を選択します。
      - システム内の特定の組織にロールを公開する場合は、組織を個別に選択します。

5 ロールの公開を解除するには：

   - システム内のすべての組織でロールの公開を解除する場合は、[テナントに公開] を選択解除します。
   - システム内の特定の組織でロールの公開を解除する場合は、[すべてのテナントに公開] を選択解除して、組織を個別に選択解除します。

6 [保存] をクリックします。

結果

公開されたロールは、選択した組織内で使用することができ、組織内のユーザーに割り当てることができます。組織管理者は、組織に公開されたグローバル テナント ロールを編集できません。

公開解除されたロールは選択した組織から削除されるため、これらの組織内のユーザーに割り当てることはできません。

グローバル テナント ロールの表示および編集

グローバル テナント ロールに含まれている権限を表示できます。グローバル テナント ロールの名前、説明、および権限を変更できます。

手順

1. メイン メニュー (☰) から、[管理] を選択します。
2. 左側のパネルの [テナント アクセス コントロール] で、[グローバル ロール] をクリックします。
3. ターゲット ロールの名前をクリックします。

   ロールに関連付けられた権限は、権限カテゴリを展開して表示することができます。
4. ロールの名前、説明、または権限を変更するには、[編集] をクリックします。
5. ロールを編集して、[保持] をクリックします。

結果

ロールの権限を変更した場合は、このロールに割り当てられているすべての組織のユーザーに新しい権限セットが適用されます。

グローバル テナント ロールの削除

組織で使用しなくなったグローバル テナント ロールは削除することができます。

前提条件

削除するグローバル テナント ロールがすべての組織において、いずれのユーザーにも割り当てられていないこと。

手順

1. メイン メニュー (☰) から、[管理] を選択します。
2. 左側のパネルの [テナント アクセス コントロール] で、[グローバル ロール] をクリックします。
3. ターゲット ロールの横にあるラジオ ボタンを選択して、[削除] をクリックします。
4. 確認するには、[OK] をクリックします。

プロバイダ ロールの管理

vCloud Director プロバイダ組織でロールを作成して管理することができます。

テナント ロールの管理の詳細については、『vCloud Director Tenant Portal Guide』を参照してください。

プロバイダ ロールの作成

vCloud Director プロバイダの組織内にロールを作成することができます。

vCloud Director の初回インストールとセットアップ後、システムには、プロバイダ組織のローカルな事前定義済みロールと、すべての組織に対するグローバルな事前定義済みロールが含まれています。事前定義済みロールの詳細については、「事前定義ロールとその権限」を参照してください。

プロバイダ組織には、カスタムのプロバイダ ロールを追加できます。

手順

1 メイン メニュー (☰) から、[管理] を選択します。

2 左側のパネルの [プロバイダ アクセス コントロール] で、[ロール] をクリックします。

3 [新規] をクリックします。

4 新しいロールの名前と、オプションで説明を入力します。

5 ロールに関連付ける権限を選択します。

権限は、関連するオブジェクトへのアクセス権を表示および管理するために、カテゴリとサブカテゴリにグループ化されています。

権限はサブカテゴリ別に表示または管理するか、グローバルに表示または管理して、個別に選択することができます。

カテゴリー	説明
アクセス コントロール	組織、権限、ロール、およびユーザーを表示して管理するための権限が含まれています。
管理	一般的な設定やマルチサイトの設定を表示して管理するための権限が含まれています。
コンピュート	組織およびプロバイダの仮想データセンター、vApp、組織仮想データセンター テンプレート、および仮想マシンの監視を表示して管理するための権限が含まれています。
拡張機能	vCloud Director プラグインおよび拡張機能を表示して管理するための権限が含まれています。
インフラストラクチャ	vSphere リソースを表示して管理するための権限が含まれています。
ライブラリ	カタログおよびカタログ項目を表示して管理するための権限が含まれています。
ネットワーク	ネットワーク リソースを表示して管理するための権限が含まれています。

6 [保存] をクリックします。

結果

新しく作成したロールは、プロバイダ組織のユーザーに割り当てることができます。

プロバイダ ロールの表示または編集

vCloud Director プロバイダ組織のローカル ロールに含まれている権限を表示できます。ロールの名前、説明、および権限を変更できます。

手順

1 メイン メニュー (☰) から、[管理] を選択します。

2 左側のパネルの [プロバイダ アクセス コントロール] で、[ロール] をクリックします。

3 ターゲット ロールの名前をクリックします。

ロールに関連付けられた権限は、権限カテゴリを展開して表示することができます。

4 ロールの名前、説明、または権限を変更するには、[編集] をクリックします。

5 ロールを編集して、[保存] をクリックします。

結果

ロールの権限を変更した場合は、このロールに割り当てられているユーザーに新しい権限セットが適用されます。

プロバイダ ロールの削除

vCloud Director プロバイダの組織で使用しなくなったロールは削除することができます。

前提条件

削除するロールがいずれのユーザーにも割り当てられていないこと。

手順

1 メイン メニュー (☰) から、[管理] を選択します。

2 左側のパネルの [プロバイダ アクセス コントロール] で、[ロール] をクリックします。

3 ターゲット ロールの横にあるラジオ ボタンを選択して、[削除] をクリックします。

4 確認するには、[OK] をクリックします。

プロバイダ ユーザーおよびグループの管理

ユーザーおよびグループを vCloud Director プロバイダ組織に追加およびインポートできます。

組織ユーザーおよびグループの管理の詳細については、『vCloud Director Tenant Portal Guide』を参照してください。

プロバイダ ユーザーの管理

プロバイダ組織内のユーザーを管理するには、Service Provider Admin Portal を使用します。

組織内のテナント ユーザーの管理の詳細については、『vCloud Director Tenant Portal Guide』を参照してください。

プロバイダ ユーザーの作成

vCloud Director プロバイダの組織内にユーザーを作成することができます。

vCloud Director のインストールおよびセットアップ時に、システム管理者アカウントを作成します。初期セットアップ後、追加の管理者およびユーザーをプロバイダの組織に作成できます。

手順

1 メイン メニュー (☰) から、[管理] を選択します。

2 左側のパネルの [プロバイダ アクセス コントロール] で、[ユーザー] をクリックします。

3 [新規] をクリックします。

4 新規ユーザーのユーザー名とパスワードを入力します。

パスワードには 6 文字以上を含める必要があります。

5 作成時にユーザーを有効にするかどうかを選択します。

6 [使用可能なロール] ドロップダウン メニューから、ユーザーのロールを選択します。

使用可能なロールのリストには、グローバル ロールと、システム組織のローカル ロールが構成されています。

7 （オプション） ユーザーの連絡先情報を入力します。

フル ネーム、メール アドレス、電話番号、インスタント メッセージ ID が入力可能です。

8 （オプション） ユーザーの割り当てを設定します。

a ユーザーによって所有される仮想マシンの制限を設定するか、または [制限なし] を選択できます。

b ユーザーが所有する実行中の仮想マシンの制限を設定するか、または [制限なし] を選択できます。

プロバイダ ユーザーのインポート

以前に設定された LDAP または SAML ID プロバイダから vCloud Director プロバイダ組織にユーザーをインポートできます。

前提条件

「システムの LDAP 接続の構成」または「システムでの SAML ID プロバイダの使用を有効化」。

手順

1 メイン メニュー (☰) から、[管理] を選択します。

2 左側のパネルの [プロバイダ アクセス コントロール] で、[ユーザー] をクリックします。

3 [ユーザーのインポート] をクリックします。

4 [ソース] ドロップダウン メニューで、ID プロバイダのタイプを選択します。

[LDAP] または [SAML] を選択できます。

設定した ID プロバイダが 1 つのみの場合は、このオプションはハードコードされます。

5 ユーザーを指定します。

オプション	説明
LDAP	a ユーザーの完全な名前または名前の一部を入力し、[検索] をクリックします。 b 検索結果でインポートするユーザーを選択します。 c [ロールの割り当て] ドロップダウン メニューでインポートされたユーザーのロールを選択します。
SAML	a SAML ID プロバイダでサポートされている名前識別子の形式でインポートするユーザーの名前を入力します。 ユーザー名ごとに新しい行を使用します。 b [ロールの割り当て] ドロップダウン メニューでインポートされたユーザーのロールを選択します。

6 [保存] をクリックします。

結果

ユーザーのリストでインポートされたユーザーを確認できます。

プロバイダ ユーザーの編集

プロバイダ組織内のユーザーのパスワード、ロール、連絡先情報、および割り当て容量を変更できます。ユーザー名は変更できません。

手順

1 メイン メニュー (☰) から、[管理] を選択します。

2 左側のパネルの [プロバイダ アクセス コントロール] で、[ユーザー] をクリックします。

3 ターゲット ユーザー名の横にあるラジオ ボタンをクリックして、[編集] をクリックします。

4 ユーザーの詳細を編集して、[保存] をクリックします。

プロバイダ ユーザーの無効化または有効化

ユーザーを無効にすると、そのユーザーは vCloud Director にログインできなくなります。

手順

1 メイン メニュー (☰) から、[管理] を選択します。

2 左側のパネルの [プロバイダ アクセス コントロール] で、[ユーザー] をクリックします。

3 ターゲット ユーザーの名前の横にあるラジオ ボタンをクリックして、[無効化] または [有効化].をクリックします。

4 ユーザーを無効にする場合は、[OK] をクリックして確認します。

プロバイダ ユーザーの削除

vCloud Director プロバイダの組織からユーザーを削除するには、そのユーザー アカウントを削除します。

前提条件

削除するユーザーを無効にする。プロバイダ ユーザーの無効化または有効化を参照してください。

手順

1 メイン メニュー (☰) から、[管理] を選択します。

2 左側のパネルの [プロバイダ アクセス コントロール] で、[ユーザー] をクリックします。

3 対象のユーザー名の横にあるラジオ ボタンをクリックし、[削除] をクリックします。

4 確認するには、[OK] をクリックします。

プロバイダ ユーザーのロック解除

パスワード ポリシー システム設定でアカウントのロックアウトを有効にした場合に、ユーザーが無効なログインを特定の回数だけ試行すると、アカウントがロックされる可能性があります。ロックアウトにアカウントのロックアウト間隔が設定されている場合でも、ロックが期限切れになるのを待たずに、ユーザー アカウントのロックを解除できます。

アカウント ロックアウト ポリシーの設定の詳細については、『vCloud Director 管理者ガイド』を参照してください。

手順

1 メイン メニュー (☰) から、[管理] を選択します。

2 左側のパネルの [プロバイダ アクセス コントロール] で、[ユーザー] をクリックします。

3 ターゲット ユーザーの名前の横にあるラジオ ボタンをクリックして、[ロック解除] をクリックします。

プロバイダ グループの管理

Service Provider Admin Portal を使用して、プロバイダ組織からグループをインポート、編集、および削除できます。

組織内のグループの管理の詳細については、『vCloud Director Tenant Portal Guide』を参照してください。

プロバイダ グループのインポート

以前に設定された LDAP または SAML ID プロバイダから vCloud Director プロバイダ組織にグループをインポートできます。

前提条件

「システムの LDAP 接続の構成」または「システムでの SAML ID プロバイダの使用を有効化」。

手順

1 メイン メニュー (☰) から、[管理] を選択します。

2 左側のパネルの [プロバイダ アクセス コントロール] で、[グループ] をクリックします。

3 [グループのインポート] をクリックします。

4 [ソース] ドロップダウン メニューで、ID プロバイダのタイプを選択します。

[LDAP] または [SAML] を選択できます。

設定した ID プロバイダが 1 つのみの場合は、このオプションはハードコードされます。

5 ユーザーを指定します。

オプション	説明
LDAP	a グループの完全な名前または名前の一部を入力し、[検索] をクリックします。 b 検索結果でインポートするグループを選択します。 c [ロールの割り当て] ドロップダウン メニューから、インポートされたグループ内のユーザーにロールを選択します。
SAML	a SAML ID プロバイダでサポートされている名前識別子の形式でインポートするグループの名前を入力します。 グループ名ごとに新しい行を使用します。 b [ロールの割り当て] ドロップダウン メニューから、インポートされたグループ内のユーザーにロールを選択します。

6 [保存] をクリックします。

プロバイダ グループの編集

vCloud Director プロバイダ組織に以前にインポートしたグループの説明を編集したり、グループのメンバーのロールを変更することができます。

手順

1 メイン メニュー (☰) から、[管理] を選択します。

2 左側のパネルの [プロバイダ アクセス コントロール] で、[グループ] をクリックします。

3 ターゲット グループ名の横にあるラジオ ボタンをクリックして、[編集] をクリックします。

4 グループの詳細を編集して、[保存] をクリックします。

プロバイダ グループの削除

vCloud Director プロバイダの組織からグループを削除することができます。

手順

1 メイン メニュー (☰) から、[管理] を選択します。

2 左側のパネルの [プロバイダ アクセス コントロール] で、[グループ] をクリックします。

3 対象のグループ名の横にあるラジオ ボタンをクリックし、[削除] をクリックします。

4 確認するには、[OK] をクリックします。

システム設定の管理

11

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。

ID プロバイダの管理

クラウドを外部 ID プロバイダと連携させて、ユーザーおよびグループを組織にインポートすることができます。LDAP サーバ接続はシステム レベルまたは組織レベルで設定できます。SAML 連携は組織レベルで設定できます。

LDAP 接続の管理

システム管理者は、ユーザーおよびグループの送信元として LDAP サーバを使用するよう、vCloud Director システムの組織およびシステム内の別の任意の組織を設定できます。組織はシステムの LDAP 接続またはプライベート LDAP 接続のいずれかを使用できます。

システムの LDAP 接続の構成

vCloud Director および組織に、ユーザーおよびグループへの共有アクセスを提供するには、LDAP 接続をシステム レベルで構成できます。

手順

1 メイン メニュー (☰) から、[管理] を選択します。

2 左側のパネルの [ID プロバイダ] で、[LDAP] をクリックします。

現在の LDAP の設定が表示されます。

次のステップ

LDAP 接続の設定、テスト、および同期。

組織 LDAP 接続の設定

組織で、ユーザーおよびグループの共有ソースとしてシステムの LDAP 接続が使用されるように設定できます。組織で、ユーザーおよびグループのプライベート ソースとして個別の LDAP 接続が使用されるように設定できます。

手順

1 メイン メニュー (☰) から、[クラウド リソース] を選択します。

2 左側のパネルで [組織] をクリックします。

3 ターゲット組織の名前をクリックします。

組織の vCloud Director テナント ポータルにリダイレクトされます。

4 メイン メニュー (☰) から、[管理] を選択します。

5 左側のパネルの [ID プロバイダ] で、[LDAP] をクリックします。

現在の LDAP の設定が表示されます。

6 [LDAP オプション] タブで、[編集] をクリックします。

7 この組織のユーザーおよびグループの LDAP ソースを設定し、[保存] をクリックします。

オプション	説明
[LDAP を使用しない]	組織は、組織のユーザーおよびグループのソースとして LDAP サーバを使用しません。
[VCD システム LDAP サービス]	組織は、設定済みの vCloud Director システムの LDAP 接続を使用します。 システムの LDAP 接続の構成を参照してください。
[カスタム LDAP サービス]	組織は、組織のユーザーおよびグループのソースとしてプライベート LDAP サーバを使用します。 [カスタム LDAP] タブをクリックし、「LDAP 接続の設定、テスト、および同期」を実行します。

LDAP 接続の設定、テスト、および同期

システムまたは組織の LDAP 接続を設定するには、LDAP サーバの詳細を設定します。接続をテストすることで、設定が適切に入力されていることと、ユーザーおよびグループ属性が適切にマッピングされていることを確認できます。LDAP 接続が正常に完了すると、vCloud Director と LDAP サーバをいつでも同期できます。

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。

手順

1 [接続] タブで、LDAP 接続に必要な情報を入力します。

必要な情報	説明
[サーバ]	LDAP サーバのホスト名または IP アドレス。
[ポート]	LDAP サーバが待機するポート番号。 LDAP のデフォルト ポート番号は 389 です。LDAPS のデフォルト ポート番号は 636 です。
[ベースの識別名]	ベース識別名 (DN) は、vCloud Director が接続する LDAP ディレクトリ内の場所です。 ルートで接続するには、**DC=example,DC=com** のようにドメイン コンポーネントのみを入力します。 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。
[コネクタ タイプ]	LDAP サーバのタイプ。[Active Directory] または [OpenLDAP] を使用できます。
[SSL を使用]	サーバが LDAPS の場合は、このチェック ボックスを選択します。
[すべての証明書を承認]	サーバが LDAPS の場合は、このチェック ボックスを選択するか、または LDAP の SSL 証明書をアップロードします。
[カスタム トラストストア]	サーバが LDAPS の場合は、アップロード アイコン ( ) をクリックして LDAP の SSL 証明書をインポートするか、[すべての証明書を承認] を選択します。
[認証方法]	シンプル認証では、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。 Kerberos を使用する場合は、vCloud Director Web Client を使用して LDAP 接続を設定する必要があります。詳細については、『vCloud Director 管理者ガイド』を参照してください。
[ユーザー名]	LDAP サーバへの接続に使用する完全な LDAP DN ユーザー名。 LDAP サーバで匿名読み取り対応が有効になっている場合は、これらのテキスト ボックスを空白にしておくことができます。
[パスワード]	LDAP サーバへの接続に使用するパスワード。 LDAP サーバで匿名読み取り対応が有効になっている場合は、これらのテキスト ボックスを空白にしておくことができます。

2 [ユーザー属性] タブをクリックして、ユーザー属性のデフォルト値を確認します。LDAP ディレクトリで別のスキーマが使用されている場合には、値を変更します。

3 [グループ属性] タブをクリックして、グループ属性のデフォルト値を確認します。LDAP ディレクトリで別のスキーマが使用されている場合には、値を変更します。

4 [保存] をクリックします。

5 LDAP 接続の設定と LDAP 属性のマッピングをテストするには、以下の手順を実行します。

a [テスト] をクリックします。

b 設定した LDAP サーバ ユーザーのパスワードを入力し、[テスト] をクリックします。

正常に接続されている場合は、緑色のチェック マークが表示されます。

取得したユーザーおよびグループ属性の値がテーブルに表示されます。LDAP 属性に正常にマッピングされた値には、緑色のチェック マークが付けられます。マッピングされた LDAP 属性以外の値は空白になり、赤色の感嘆符が付けられます。

c 終了するには [キャンセル] をクリックします。

6 vCloud Director を設定した LDAP サーバと同期するには、[同期] をクリックします。

vCloud Director は、システムの全般設定で指定された同期間隔に基づき、ユーザーおよびグループ情報を LDAP サーバと定期的に同期します。

同期が完了するまで数分間待機します。

結果

ユーザーとグループは、新たに設定した LDAP サーバからインポートできます。

システムでの SAML ID プロバイダの使用を有効化

SAML ID プロバイダからユーザーおよびグループをシステム組織にインポートする場合は、その SAML の ID プロバイダで、システム組織を構成する必要があります。インポートされたユーザーは、SAML ID プロバイダで確立した認証情報を使用してシステム組織にログインできます。

vCloud Director を SAML の ID プロバイダで構成するには、SAML サービス プロバイダと ID プロバイダのメタデータを交換して相互信頼を確立します。

インポートされたユーザーがログインすると、システムは SAML トークンから以下の属性を抽出し（使用可能な場合）、それらをユーザーに関する情報の対応する要素の解釈に使用します。

- `email address = "EmailAddress"`
- `user name = "UserName"`
- `full name = "FullName"`
- `user's groups = "Groups"`
- `user's roles = "Roles"`（この属性は設定可能です）

ユーザーが直接インポートされない場合、インポートしたグループのメンバーシップによってユーザーがログインする際には、グループ情報が使用されます。ユーザーは複数のグループに所属することができます。したがって、1 人のユーザーがセッション中に複数のロールを持つ場合があります。

インポートしたユーザーまたはグループに [ID プロバイダに従う] ロールが割り当てられている場合は、トークンの Roles 属性から収集された情報に基づいてロールが割り当てられます。別の属性が使用されている場合、この属性名は API を使用して設定可能です。また、設定できるのは Roles 属性のみとなります。[ID プロバイダに従う] ロールが使用されているにもかかわらずロール情報を抽出できない場合、ユーザーはログインできますが、操作を実行する権限は与えられません。

前提条件

- SAML 2.0 に準拠した ID プロバイダへのアクセス権があることを確認します。
- SAML の ID プロバイダからの次のメタデータを含む XML ファイルを取得します。
  - Single Sign-On サービスの場所
  - シングル ログアウト サービスの場所
  - サービスの X.509 証明書の場所

  構成方法および SAML プロバイダからのメタデータの取得方法については、SAML プロバイダのドキュメントを参照してください。

手順

1 メイン メニュー (☰) から、[管理] を選択します。

2 左側のパネルで、ID プロバイダの下で、[SAML] をクリックし、[編集] をクリックします。

  現在の SAML 設定が表示されます。

3 [サービス プロバイダ] タブから、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 システム組織のエンティティ ID を入力します。

    エンティティ ID は、ID プロバイダがシステム組織を識別するためのものです。

  b 証明書の有効期限を確認し、期限切れが近い場合、[再生成] をクリックして、証明書を再生成します。

    証明書は SAML メタデータに含まれ、暗号化と署名の両方に使用されます。組織と SAML ID プロバイダ間の信頼の確立方法によっては、これらのいずれかまたは両方が必要になることがあります。

  c [メタデータ] リンクをクリックします。

    リンクは、`https://VCD_host_name/cloud/org/System/saml/metadata/alias/vcd` のようになります。

    ブラウザで、ID プロバイダに提供する必要のある SAML サービス プロバイダのメタデータが、XML ファイル形式でダウンロードされます。

4 [ID プロバイダ] タブで、ID プロバイダから以前に受信した SAML メタデータをアップロードします。

  a [SAML の ID プロバイダを使用する] を選択します。

  b [参照] アイコン (↑) をクリックしてファイルをアップロードするか、またはファイルのコンテンツをコピーして [メタデータ XML] テキスト ボックスに貼り付けます。

5 [保存] をクリックします。

結果

プラグインの管理

vCloud Director プラグインは、Service Provider Admin Portal および vCloud Director Tenant Portal の機能を拡張します。Service Provider Admin Portal からプラグインをアップロード、無効化、および削除できます。また、サービス プロバイダや個々の組織にプラグインを公開できます。

一部のプラグインは、vCloud Director の一部としてインストールされます。

CPOM 拡張機能

vCloud Director Tenant Portal を使用して SDDC および SDDC プロキシを表示および管理する機能を提供します。

ポータルのカスタマイズ

vCloud Director Service Provider Admin Portal および vCloud Director Tenant Portal をカスタマイズする機能を提供します。

vCloud Availability

VMware vCloud® Availability™ プラグインには、vCloud Director のユーザー インターフェイスから vCloud Availability Portal に直接アクセスできる機能があります。詳細については、vCloud Availability のドキュメントを参照してください。

プラグインのアップロード

サービス プロバイダやクラウド内の組織が使用できるように、追加のプラグインを vCloud Director Service Provider Admin Portal にアップロードすることができます。

前提条件

プラグインのインストール ファイルをダウンロードします。

手順

1. メイン メニュー (☰) で [ポータルのカスタマイズ] を選択します。
2. [アップロード] をクリックします。
3. [プラグイン ファイルの選択] をクリックして、ターゲット インストール ファイルを参照し、[開く] をクリックします。
4. [次へ] をクリックします。
5. このプラグインの範囲を選択します。

オプション	説明
サービス プロバイダ	プラグイン機能は、vCloud Director Service Provider Admin Portal で使用可能になります。
テナント	プラグイン機能は、選択した組織の vCloud Director Service Provider Admin Portal で使用可能になります。

6 プラグインの範囲をテナントに設定した場合は、このプラグインを公開する組織を選択します。

7 [確認して完了] 画面を確認し、[完了] をクリックします。

プラグインの有効化または無効化

すべての組織がプラグインを使用できないようにするには、プラグインを無効にします。

手順

1 メイン メニュー (☰) で [ポータルのカスタマイズ] を選択します。

2 対象のプラグインの名前の横にあるチェック ボックスを選択し、[有効化] または [無効化] をクリックします。

プラグインの削除

1 つ以上のプラグインを vCloud Director Service Provider Admin Portal から削除できます。

手順

1 メイン メニュー (☰) で [ポータルのカスタマイズ] を選択します。

2 削除するプラグインの名前の横にあるチェック ボックスを選択して、[削除] をクリックします。

3 確認するには、[保存] をクリックします。

組織からのプラグインの公開または公開解除

プラグインが提供する機能を使用できる組織の組み合わせは、変更することができます。

組織の組み合わせは、複数のプラグインに対して変更できます。

手順

1 メイン メニュー (☰) で [ポータルのカスタマイズ] を選択します。

2 ターゲット プラグインの名前の横にあるチェック ボックスを選択し、[公開] をクリックします。

3 このプラグインの範囲を選択します。

オプション	説明
サービス プロバイダ	プラグイン機能は、vCloud Director Service Provider Admin Portal で使用可能になります。
テナント	プラグイン機能は、選択した組織の vCloud Director Service Provider Admin Portal で使用可能になります。

4 プラグインの範囲をテナントに設定した場合は、このプラグインを公開する組織を選択します。

5 [保存] をクリックします。

vCloud Director ポータルのカスタマイズ

企業のブランディング基準を満たし、完全に独自のクラウド エクスペリエンスを実現するには、vCloud Director Service Provider Admin Portal および各組織の vCloud Director Tenant Portal にロゴとテーマを設定します。また、vCloud Director ポータルの右上にある 2 つのメニューを変更して、カスタム リンクを追加することもできます。

注： ブランディングの属性およびリンクをカスタマイズするには、`branding` vCloud OpenAPI メソッドを使用する必要があります。https://code.vmware.com にある vCloud OpenAPI のスタート ガイドを参照してください。

ポータル ブランディング

vCloud Director には、インストールの一部として、2 つのテーマ（デフォルト テーマとダーク テーマ）が含まれています。ユーザーはカスタム テーマを作成、管理、および適用できます。ポータル名、ロゴ、およびブラウザ アイコンも変更できます。また、ブラウザのタイトルには設定したポータル名が使用されます。

ブランディングの属性をシステム レベルで設定すると、vCloud Director Service Provider Admin Portal をカスタマイズできます。特定のテナントにブランディング属性を設定した場合以外は、各組織の vCloud Director Tenant Portal にはシステム ブランディング属性が使用されます。

特定のテナントに、ポータル名、背景色、ロゴ、アイコン、テーマ、およびカスタム リンクの任意の組み合わせを選択して、オーバーライドすることができます。設定しなかった値には、対応するシステムのデフォルト値が使用されます。

注： デフォルトでは、ログインしたセッション以外の場所に個々のテナント ブランディングは表示されません。テナント間で他のテナントの存在を認識できないように、ログインおよびログアウト画面には各テナントのブランディングは表示されません。ログインしたセッション以外の場所でブランディングを有効にするには、次のセル管理ツールを使用します。

```
manage-config -n backend.branding.requireAuthForBranding -v false
```

セル管理ツールの使用については、vCloud Director 管理者ガイドを参照してください。

カスタム リンク

カスタム リンクは、ポータル ブランディングのコンポーネントです。カスタム リンクには、次の 2 種類があります。

- `override` メニュー項目は、[ヘルプ]、[バージョン情報]、および [VMRC のダウンロード] のメニュー項目の既存のリンクを置き換えます。デフォルトでは、ユーザーは [VMRC のダウンロード] から https://my.vmware.com にリダイレクトされ、VMRC をダウンロードできます。ユーザーが VMRC をダウンロードするには、アカウントを登録している必要があります。このリンクをオーバーライドすることで、VMRC インストーラを独自のサーバに再配置できます。
- `link` メニュー項目は、ポータルの右上隅にある [ログアウト] メニュー項目に追加される新しいリンクです。新しいカスタム リンクは、API 呼び出し内で指定した順序で表示されます。

これらのカスタム リンクを整理するには、section および separator のメニュー項目を使用します。section メニュー項目はメニューにヘッダーを追加し、separator メニュー項目はメニューに行を追加します。

カスタム リンクはカスタム変数をサポートします。カスタム変数は、識別情報をクエリ パラメータの形式で他のアプリケーションに渡す場合に使用できます。

vCloud Director では、カスタム リンクの url 値に次のカスタム変数を使用できます。

表 11-1. カスタム リンクのカスタム変数

変数	説明
${TENANT_NAME}	組織名
${TENANT_ID}	組織 ID
${SESSION_TOKEN}	x-vcloud-authorization トークン

たとえば、次のようになります。

```
url: https://host:port/tenant/${TENANT_NAME}/vdcs
```

組織 myorg の vCloud Director Tenant Portal であれば、次のようになります。

```
url: https://host:port/tenant/myorg/vdcs
```

vCloud Director の監視

12

システム管理者は、完了した操作と処理中の操作を監視し、プロバイダ仮想データセンター、組織仮想データセンター、およびデータストア レベルでリソース使用状況情報を表示できます。

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

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。

プロバイダ仮想データセンターの使用情報の表示

プロバイダ仮想データセンターは、コンピューティング リソース、メモリ リソース、およびストレージ リソースを組織仮想データセンターに提供します。プロバイダ仮想データセンター リソースの使用を監視して、リソースを追加するかどうかを決定できます。

手順

1 メイン メニュー (☰) から、[クラウド リソース] を選択します。

2 左側のパネルで [プロバイダ VDC] をクリックし、ターゲット プロバイダ仮想データセンターの名前をクリックします。

3 [設定] - [メトリック] タブの順にクリックします。

4 各パラメータの詳細については、各情報アイコンをクリックします。

サービスの管理

13

vCloud Director Service Provider Admin Portal の [コンテンツ ライブラリ] ビューには、vRealize Orchestrator と統合するためのインターフェイスが用意されています。vRealize Orchestrator ワークフローは、サービス プロバイダの管理者がテナントまたはその他のサービス プロバイダに公開できるサービスのカタログとして使用することができます。この方法で、サービスプロバイダが提供する一連の機能および管理機能を拡張することができます。

この章には、次のトピックが含まれています。

vRealize Orchestrator と vCloud Director の統合

vRealize Orchestrator と vCloud Director を統合するには、vCloud Director Service Provider Admin Portal を使用します。

vRealize Orchestrator と vCloud Director を統合すると、vCloud Director の基本機能が拡張され、サービス プロバイダの管理者がワークフローのオーケストレーションおよびサードパーティ プラグインを利用して複雑な自動化タスクを開発できるようになります。

サービス プロバイダの管理者は vCloud Director Service Provider Admin Portal を使用して、登録された vRealize Orchestrator サーバ インスタンスからワークフローを表示、インポート、および実行できます。

vCloud Director Service Provider Admin Portal で vRealize Orchestrator ワークフローをサービス プロバイダまたはテナントに公開することにより、クイック アクセス制御を許可し、カスタム サービスと組み込みサービスを両方とも実行できるようになります。

vRealize Orchestrator の詳細なワークフロー ライブラリには、特定の課題を解決し、一般的な管理者タスクを実行するために設計された事前作成済みのタスクが含まれています。サードパーティ プラグインは VMware Solution Exchange で入手することもできます。

vCloud Director への vRealize Orchestrator インスタンスの登録

vCloud Director で vRealize Orchestrator を使用してワークフローのオーケストレーションとタスクの自動化を利用するには、vCloud Director Service Provider Admin Portal に vRealize Orchestrator インスタンスを登録します。

前提条件

- vRealize Orchestrator サーバ インスタンスを展開して、設定します。詳細については、vRealize Orchestrator ドキュメントの『VMware vRealize Orchestrator のインストールと構成』を参照してください。
- 認証プロバイダとして vSphere を使用するように vRealize Orchestrator を設定します。
- vCloud Director に、vRealize Orchestrator で認証に使用される vCenter Single Sign-On と同じ Platform Services Controller の Lookup Service が登録されていることを確認します。

手順

1 メイン メニュー (☰) から、[コンテンツ ライブラリ] を選択します。

   a 左側のパネルで [サービス管理] を選択します。

   登録されている vRealize Orchestrator サーバのリストが表示されます。

2 新しい vRealize Orchestrator サーバを登録するには、＋ ボタンをクリックします。

   [vRealize Orchestrator の登録] ダイアログが表示されます。

3 以下の値を入力します。

オプション	説明
名前	登録されている vRealize Orchestrator インスタンスの名前。
説明	登録されている vRealize Orchestrator サーバ インスタンスの説明。
ホスト名	vRealize Orchestrator サーバの完全修飾ドメイン名およびサーバ ポート。デフォルト HTTPS ポートの値は 8281 です。 **注：** vCloud Director は vRealize Orchestrator の API インターフェイスに接続されます。
ユーザー名	vRealize Orchestrator 管理者グループのメンバーであるユーザー アカウント。
パスワード	vRealize Orchestrator 管理者アカウントのパスワード。
トラスト アンカー	PEM 形式の vRealize Orchestrator サーバの SSL 証明書。 アップロード アイコン (↑) をクリックして、`.pem` ファイルを検索して選択します。

4 [OK] をクリックして、登録を完了します。

   vRealize Orchestrator サーバが vCloud Director に登録されました。

サービス カテゴリの作成

サービスをサービス カテゴリで分類できます。

手順

1 メイン メニュー (☰) から、[コンテンツ ライブラリ] を選択します。

a 左側のパネルで [サービス管理] を選択します。

b [サービス カテゴリ] タブに移動します。

既存のサーバ カテゴリのリストが表示されます。

2 新しいサービス カテゴリを作成するには、＋ ボタンをクリックします。

[サービス カテゴリの新規作成] ダイアログが表示されます。

3 以下の値を入力します。

オプション	説明
名前	サービス カテゴリの名前。
アイコン	サービス カテゴリ用に表示されているアイコンをインポートします。
説明	サービス カテゴリの短い説明。

サービス カテゴリの編集

既存のサービス カテゴリを編集できます。

手順

1 メイン メニュー (☰) から、[コンテンツ ライブラリ] を選択します。

a 左側のパネルで [サービス管理] を選択します。

b [サービス カテゴリ] タブに移動します。

既存のサーバ カテゴリのリストが表示されます。

2 選択したサービス カテゴリの左側にあるリスト バー（ ⋮ ）を使用して、[編集] をクリックします。

3 次の値を編集します。

オプション	説明
名前	サービス カテゴリの名前。
アイコン	サービス カテゴリ用に表示されているアイコンをインポートします。
説明	サービス カテゴリの短い説明。

サービスのインポート

vCloud Director に登録されている vRealize Orchestrator インスタンスのワークフロー ライブラリから、サービスをインポートできます。

前提条件

- vRealize Orchestrator インスタンスを登録します。 vCloud Director への vRealize Orchestrator インスタンスの登録 を参照してください。
- サービス カテゴリを作成します。サービス カテゴリの作成 を参照してください。

手順

1 メイン メニュー (☰) から、[コンテンツ ライブラリ] を選択します。

a 左側のパネルで [サービス ライブラリ] を選択します。

使用可能なサービスがカード ビューで表示されます。カード ビューにはページあたり 12 個の項目が表示され、名前を基準としてアルファベット順にソートされます。各カードは項目が vRealize Orchestrator ワークフローであることを示していて、このワークフローがインポートされるサービスの名前およびサービス カテゴリに対応するタグが表示されます。

2 新しいサービスをインポートするには、[インポート] ボタンをクリックします。

3 [インポート] ウィザードの手順に沿って処理を進めます。

オプション	説明
ターゲット ライブラリにインポート	サービスをインポートするサービス カテゴリを選択します。
ソースを選択	ワークフローのインポート元の vRealize Orchestrator インスタンスを選択します。
ワークフローを選択	階層ツリー ビューを展開して、インポートする 1 つまたは複数のワークフローを選択します。
確認	詳細を確認し、[完了] をクリックしてインポートを完了します。

インポートされたワークフローが、[サービス ライブラリ] カード ビューに表示されます。

サービスの検索

サービスは、名前またはサービスが属しているサービス カテゴリで検索できます。

手順

1 メイン メニュー (☰) から、[コンテンツ ライブラリ] を選択します。

a 左側のパネルで [サービス ライブラリ] を選択します。

使用可能なサービスがカード ビューで表示されます。カード ビューにはページあたり 12 個の項目が表示され、名前を基準としてアルファベット順にソートされます。各カードは項目が vRealize Orchestrator ワークフローであることを示していて、このワークフローがインポートされるサービスの名前およびサービス カテゴリに対応するタグが表示されます。

2 ページ上部の [検索] テキスト ボックスに、検索するサービスまたはサービス カテゴリの名前を表す語句または文字を入力します。

a サービスの名前で検索するのか、それともサービス カテゴリで検索するかを選択します。

検索結果がカード ビューで表示されます。カード ビューにはページあたり 12 個の項目が表示され、名前を基準としてアルファベット順にソートされます。

サービスの実行

vRealize Orchestrator ワークフローをインポートされたサービスとして実行できます。

手順

1 メイン メニュー (☰) から、[コンテンツ ライブラリ] を選択します。

a 左側のパネルで [サービス ライブラリ] を選択します。

使用可能なサービスがカード ビューで表示されます。カード ビューにはページあたり 12 個の項目が表示され、名前を基準としてアルファベット順にソートされます。各カードは項目が vRealize Orchestrator ワークフローであることを示していて、このワークフローがインポートされるサービスの名前およびサービス カテゴリに対応するタグが表示されます。

2 サービスを実行するには、選択したサービスのカードで [実行] をクリックします。

[サービスの実行] ウィザードが表示されます。

3 サービスの必須の入力パラメータを入力し、[完了] をクリックします。

結果

実行のステータスは、[最近のタスク] ビューで監視できます。詳細については、タスクの表示を参照してください。

注： vRealize Orchestrator ワークフローを vCloud Director サービスとして開始すると、vCloud Director はワークフローの実行コンテキストにカスタム パラメータをいくつか追加します。

カスタム プロパティ	説明
`_vcd_orgName`	サービスを実行するユーザーが属している組織の名前。
`_vcd_orgId`	サービスを実行するユーザーが属している組織の ID。
`_vcd_userName`	サービスを実行するユーザーの名前。
`_vcd_isAdmin`	サービスを実行するユーザーが管理者である場合は、値が `True` になります。
`_vdc_isAdmin`	廃止されました。サービスを実行するユーザーが管理者である場合は、値が `True` になります。
`_vdc_userName`	廃止されました。サービスを実行するユーザーの名前。
`_vcd_sessionToken`	vCloud Director に対する認証の成功後に受信した認証トークン
`_vcd_apiEndpoint`	vCloud Director REST API エンドポイント

サービス カテゴリの変更

サービスが属しているカテゴリを変更できます。

手順

1 メイン メニュー (☰) から、[コンテンツ ライブラリ] を選択します。

a 左側のパネルで [サービス ライブラリ] を選択します。

使用可能なサービスがカード ビューで表示されます。カード ビューにはページあたり 12 個の項目が表示され、名前を基準としてアルファベット順にソートされます。各カードは項目が vRealize Orchestrator ワークフローであることを示していて、このワークフローがインポートされるサービスの名前およびサービス カテゴリに対応するタグが表示されます。

2 選択したサービスのカードで、[管理] - [カテゴリの変更] の順に選択します。

[カテゴリの変更] ダイアログが開きます。

3 サービスを配置するカテゴリを選択して、[保存] をクリックします。

サービスの登録解除

サービス プロバイダとテナントの両方のサービスへのアクセス権を削除するには、サービスを登録解除します。

手順

1 メイン メニュー (☰) から、[コンテンツ ライブラリ] を選択します。

a 左側のパネルで [サービス ライブラリ] を選択します。

使用可能なサービスがカード ビューで表示されます。カード ビューにはページあたり 12 個の項目が表示され、名前を基準としてアルファベット順にソートされます。各カードは項目が vRealize Orchestrator ワークフローであることを示していて、このワークフローがインポートされるサービスの名前およびサービス カテゴリに対応するタグが表示されます。

2 選択したサービスのカードで、[管理] - [ワークフローの登録解除] の順に選択します。

[ワークフローの登録解除] ダイアログが開きます。

3 サービス ライブラリからサービスを削除するには、[削除] をクリックします。

サービスの公開

サービスを公開することにより、サービス プロバイダおよびテナントからサービスへのアクセスを制御できます。

手順

1 メイン メニュー (☰) から、[コンテンツ ライブラリ] を選択します。

a 左側のパネルで [サービス ライブラリ] を選択します。

使用可能なサービスがカード ビューで表示されます。カード ビューにはページあたり 12 個の項目が表示され、名前を基準としてアルファベット順にソートされます。各カードは項目が vRealize Orchestrator ワークフローであることを示していて、このワークフローがインポートされるサービスの名前およびサービス カテゴリに対応するタグが表示されます。

2 選択したサービスのカードで、[管理] - [ワークフローの公開] の順に選択します。

[ワークフローの公開] ダイアログが表示されます。

3 サービス プロバイダに公開するには、[サービス プロバイダに公開] を選択して、[保存] をクリックします。

4 特定のテナント組織に公開するには、[テナントに公開] ボタンを選択します。

a 使用可能なテナント組織のリストが表示されます。ワークフローを公開するテナント組織を選択して、[保存] をクリックします。

5 すべてのテナント組織に公開するには、[すべてのテナントに公開] を選択して、[保存] をクリックします。

カスタム エンティティの管理

14

vCloud Director のカスタム エンティティ定義は、vRealize Orchestrator オブジェクト タイプにバインドされているオブジェクト タイプです。サービス プロバイダがカスタム エンティティ定義を別のサービス プロバイダに公開しているか、または 1 つ以上のテナントに公開している場合、vCloud Director ユーザーは必要に応じてこれらのタイプを所有、管理、および変更することができます。サービス プロバイダのユーザーおよび組織のユーザーは、サービスを実行することでカスタム エンティティをインスタンス化し、オブジェクトのインスタンスにアクションを適用することができます。

この章には、次のトピックが含まれています。

カスタム エンティティの検索

カスタム エンティティを名前で検索できます。

手順

1 メイン メニュー (☰) から、[コンテンツ ライブラリ] を選択します。

   a 左側のパネルで [カスタム エンティティ定義] を選択します。

   カスタム エンティティのリストがカード ビューで表示されます。カード ビューにはページあたり 12 個の項目が、名前を基準としてアルファベット順に表示されます。各カードには、カスタム エンティティの名前、エンティティがマッピングされている vRealize Orchestrator タイプ、エンティティのタイプ、および説明が表示されます（これらの情報を入手できる場合）。

2 ページ上部の [検索] テキスト ボックスに、検索するエンティティの名前を表す語句または文字を入力します。

検索結果がカード ビューで表示されます。カード ビューにはページあたり 12 個の項目が表示され、名前を基準としてアルファベット順にソートされます。

カスタム エンティティ定義の編集

カスタム エンティティの名前および説明を変更できます。エンティティのタイプまたはエンティティのバインド先の vRealize Orchestrator オブジェクト タイプは変更できません。これらは、カスタム エンティティのデフォルト プロパティです。デフォルト プロパティを変更する場合は、カスタム エンティティ定義を削除して、再作成する必要があります。

手順

1 メイン メニュー (☰) から、[コンテンツ ライブラリ] を選択します。

a 左側のパネルで [カスタム エンティティ定義] を選択します。

カスタム エンティティのリストがカード ビューで表示されます。カード ビューにはページあたり 12 個の項目が、名前を基準としてアルファベット順に表示されます。各カードには、カスタム エンティティの名前、エンティティがマッピングされている vRealize Orchestrator タイプ、エンティティのタイプ、および説明が表示されます（これらの情報を入手できる場合）。

2 選択したカスタム エンティティのカードで、[アクション] - [編集] の順に選択します。

新しいダイアログが開きます。

3 カスタム エンティティ定義の名前または説明を変更します。

4 [OK] をクリックして、変更を確定します。

カスタム エンティティ定義の追加

カスタム エンティティを作成して、既存の vRealize Orchestrator オブジェクト タイプにマッピングできます。

手順

1 メイン メニュー (☰) から、[コンテンツ ライブラリ] を選択します。

a 左側のパネルで [カスタム エンティティ定義] を選択します。

カスタム エンティティのリストがカード ビューで表示されます。カード ビューにはページあたり 12 個の項目が、名前を基準としてアルファベット順に表示されます。各カードには、カスタム エンティティの名前、エンティティがマッピングされている vRealize Orchestrator タイプ、エンティティのタイプ、および説明が表示されます（これらの情報を入手できる場合）。

2 ＋ アイコンをクリックして、新しいカスタム エンティティを追加します。

新しいダイアログが開きます。

3 [カスタム エンティティ定義] ウィザードの手順に沿って処理を進めます。

手順	
名前と説明	新しいエンティティの名前と、オプションで説明を入力します。 エンティティ タイプの名前（sshHost など）を入力します。
vRO	ドロップダウン メニューで、カスタム エンティティ定義のマッピングに使用する vRealize Orchestrator を選択します。 **注：** 複数の vRealize Orchestrator サーバがある場合は、それぞれにカスタム エンティティ定義を個別に作成する必要があります。
タイプ	リストの表示アイコン ( ) をクリックして、使用可能な vRealize Orchestrator オブジェクト タイプをプラグイン別にグループ化して参照します。たとえば、[SSH] - [ホスト] の順に選択します。 タイプの名前がわかっている場合は、テキスト ボックスに直接入力できます。例：SSH:Host。
確認	指定した詳細を確認し、[完了] をクリックして作成を完了します。

結果

カード ビューに新しいカスタム エンティティ定義が表示されます。

カスタム エンティティ インスタンス

vCloud Director でカスタム エンティティ定義としてすでに定義されているオブジェクト タイプを入力パラメータとして指定して、vRealize Orchestrator ワークフローを実行すると、出力パラメータにカスタム エンティティのインスタンスが表示されます。

手順

1 メイン メニュー ( ) から、[コンテンツ ライブラリ] を選択します。

a 左側のパネルで [カスタム エンティティ定義] を選択します。

カスタム エンティティのリストがカード ビューで表示されます。カード ビューにはページあたり 12 個の項目が、名前を基準としてアルファベット順に表示されます。各カードには、カスタム エンティティの名前、エンティティがマッピングされている vRealize Orchestrator タイプ、エンティティのタイプ、および説明が表示されます（これらの情報を入手できる場合）。

2 選択したカスタム エンティティのカードで、[インスタンス] をクリックします。

使用可能なインスタンスがグリッド ビューで表示されます。

3 各エンティティの左側にあるリスト バー ( ) をクリックして、関連付けられたワークフローを表示します。

ワークフローをクリックすると、入力パラメータとしてエンティティのインスタンスを使用するワークフローが実行されます。

カスタム エンティティへのアクションの関連付け

カスタム エンティティ定義にアクションを関連付けると、特定のカスタム エンティティのインスタンス上で一連の vRealize Orchestrator ワークフローを実行できるようになります。

手順

1 メイン メニュー (☰) から、[コンテンツ ライブラリ] を選択します。

a 左側のパネルで [カスタム エンティティ定義] を選択します。

カスタム エンティティのリストがカード ビューで表示されます。カード ビューにはページあたり 12 個の項目が、名前を基準としてアルファベット順に表示されます。各カードには、カスタム エンティティの名前、エンティティがマッピングされている vRealize Orchestrator タイプ、エンティティのタイプ、および説明が表示されます（これらの情報を入手できる場合）。

2 選択したカスタム エンティティのカードで、[アクション] - [アクションの関連付け] の順に選択します。

新しいダイアログが開きます。

3 [カスタム エンティティを VRO ワークフローに関連付け] ウィザードの手順に沿って処理を進めます。

手順	詳細
vRO ワークフローの選択	表示されたワークフローのいずれかを選択します。これらは、[サービス ライブラリ] ページで使用可能なワークフローです。
ワークフローの入力パラメータの選択	リストから使用できる入力パラメータを選択します。vRealize Orchestrator ワークフローのタイプにカスタム エンティティ定義のタイプを関連付けます。
関連付けの確認	指定した詳細を確認し、[完了] をクリックして関連付けを完了します。

例

たとえば、タイプが `SSH:Host` のカスタム エンティティがある場合は、カスタム エンティティのタイプと一致する `sshHost` 入力パラメータを選択して、このエンティティを `Add a Root Folder to SSH Host` ワークフローに関連付けることができます。

カスタム エンティティからのアクションの関連付け解除

関連付けられたアクションのリストから vRealize Orchestrator ワークフローを削除できます。

手順

1 メイン メニュー (☰) から、[コンテンツ ライブラリ] を選択します。

a 左側のパネルで [カスタム エンティティ定義] を選択します。

カスタム エンティティのリストがカード ビューで表示されます。カード ビューにはページあたり 12 個の項目が、名前を基準としてアルファベット順に表示されます。各カードには、カスタム エンティティの名前、エンティティがマッピングされている vRealize Orchestrator タイプ、エンティティのタイプ、および説明が表示されます（これらの情報を入手できる場合）。

2 選択したカスタム エンティティのカードで、[アクション] - [アクションの関連付け解除] の順に選択します。

新しいダイアログが開きます。

3 削除するワークフローを選択して、[アクションの関連付け解除] をクリックします。

vRealize Orchestrator ワークフローとカスタム エンティティの関連付けが解除されました。

カスタム エンティティの公開

他のテナントまたはサービス プロバイダのユーザーが、入力パラメータとしてカスタム エンティティのインスタンスを使用してワークフローを実行できるようにするには、カスタム エンティティを公開する必要があります。

手順

1 メイン メニュー (☰) から、[コンテンツ ライブラリ] を選択します。

a 左側のパネルで [カスタム エンティティ定義] を選択します。

カスタム エンティティのリストがカード ビューで表示されます。カード ビューにはページあたり 12 個の項目が、名前を基準としてアルファベット順に表示されます。各カードには、カスタム エンティティの名前、エンティティがマッピングされている vRealize Orchestrator タイプ、エンティティのタイプ、および説明が表示されます（これらの情報を入手できる場合）。

2 選択したカスタム エンティティのカードで、[アクション] - [公開] の順に選択します。

新しいダイアログが開きます。

3 カスタム エンティティ定義をサービス プロバイダに公開するのか、すべてのテナントに公開するのか、または選択したテナントのみに公開するのかを選択します。

4 [保存] をクリックして、変更を確定します。

選択した公開先がカスタム エンティティ定義を使用できるようになります。

カスタム エンティティの削除

カスタム エンティティが使用されなくなった場合、正しく設定されていなかった場合、または vRealize Orchestrator タイプを別のカスタム エンティティにマッピングする場合は、カスタム エンティティ定義を削除できます。

手順

1 メイン メニュー (☰) から、[コンテンツ ライブラリ] を選択します。

a 左側のパネルで [カスタム エンティティ定義] を選択します。

カスタム エンティティのリストがカード ビューで表示されます。カード ビューにはページあたり 12 個の項目が、名前を基準としてアルファベット順に表示されます。各カードには、カスタム エンティティの名前、エンティティがマッピングされている vRealize Orchestrator タイプ、エンティティのタイプ、および説明が表示されます（これらの情報を入手できる場合）。

2 選択したカスタム エンティティのカードで、[アクション] - [削除] の順に選択します。

3 削除を確認します。

カード ビューからカスタム エンティティが削除されます。