SoftBank for Biz

ホワイトクラウド ASPIRE
プライベートクラウド

ご利用ガイド

Version 1.05

2023年09月01日

ソフトバンク株式会社

目次

はじめに

本書を読み進める前に、本書の位置付けや対象などについてご確認ください。

本書について

本書は、「ホワイトクラウド ASPIRE プライベートクラウド」（以下「本サービス」という）を利用するための準備、操作手順などについて説明しています。本サービスの概要や仕様については、『ホワイトクラウド ASPIRE プライベートクラウド サービス説明書』をご参照ください。ご不明な点がある場合は、当社担当営業、または、データセンターサポート窓口までご連絡ください。

なお、本書はサービスの開発・改変に伴い、内容が変更される場合があります。あらかじめご了承ください。

本書の対象

本書は、本サービスをご契約いただいたシステム管理者様向けのご利用ガイドです。

商標について

本書に掲載されているソフトウェアおよび周辺機器の名称は、各メーカの商標または登録商標です。

著作権

本書内の記号について

本書で使用している記号には、以下のような意味があります。

重要	ユーザにとって不利益となる操作や、データの破損などを避けるため、注意していただきたい重要なことを記載しています。
補足	知っていると便利な情報や、補足情報などを記載しています。
参照	関連情報の参照先を示しています。

本書内の書式記号について

本書では、一部オブジェクト名の表現に書式記号を使用しています。

オブジェクト名中に含まれる ***X*** / ***Y*** / ***Z*** はそれぞれ1文字の数字を表します。

実際のオブジェクト名に合わせ、適宜読み替えをお願いします。

例）本書の表記：tenant-***XX***-***YYY***-resource***ZZ***

実機のオブジェクト名：tenant-01-002-resource03 , tenant-10-012-resource04 など

本書内の容量表記について

本書および本サービスにて提供されるシステムでは、ストレージ容量を「TiB」または「GiB」にて計算していますが、表記単位は実際のシステムに合わせ「TB」および「GB」と記載しています。

本書の構成

本書の構成は、以下の通りです。

章	内容
はじめに（本章）	本書の位置付けや対象などについて説明しています。
1. プライベートクラウドの提供機能	本サービスで提供される機能とその概要について説明しています。
2. 管理ツールをご利用になる前に	サービス開通後の初期状態について説明しています。
3. システムアカウントの管理について	本サービスで利用するアカウントについて説明しています。
4. 専用ストレージの容量管理について	本サービスで提供される専用ストレージについて説明しています。
5. VMware vCenter Server の操作	VMware vCenter Server の操作について説明しています。
6. VMware NSX-T DataCenter の操作	VMware NSX-T DataCenter の操作について説明しています。
7. vRealize Operations Manager の操作	vRealize Operations Manager の操作について説明しています。
8. 移行ツール (VMware HCX)	移行ツールとして提供される、VMware HCX の操作について説明しています。
9. コンテナ機能 (vSphere with Tanzu)	コンテナ機能として提供される、vSphere with Tanzu の操作について説明しています。
10. Advanced cross vCenter vMotion による移行	vCenter Server の機能である Advanced cross vCenter vMotion を用いた VM 移行の操作について説明しています。
11. エコノミーストレージ	オプションのストレージ提供サービスである、エコノミーストレージについて説明しています。
12. 多機能ロードバランサ (Netwiser VE)	オプションの多機能ロードバランサとして提供される Netwiser Virtual Edition について説明しています。
13. Cloud One Workload Security	オプションのサーバセキュリティ製品として提供される Cloud One Workload Security について説明しています。
14. アンチウイルスオプション	オプションのサーバセキュリティ製品として提供されるアンチウイルスオプション について説明しています。
15. Acronis Cyber Backup powered by ASPIRE	オプションのバックアップ製品として提供される Acronis Cyber Protect Cloud について説明しています。
16. モニタリングオプション(Mackerel)	オプションのモニタリングサービスとして提供される Mackerel について説明しています。
17. Red Hat Cloud Access	お客さま保有の Red Hat ライセンス（RHEL サブスクリプション）の、クラウド環境への持込みについて説明しています。
18. ベアメタルサーバの提供機能	ベアメタルサーバで提供される機能とその概要について説明しています。
19. ベアメタルサーバ用初期設定	ベアメタルサーバ開通後の初期状態について説明しています。

章	内容
20. 専用ストレージの容量管理について(ベアメタル)	ベアメタルサーバ利用時の専用ストレージの容量管理について説明しています。
21. VMware NSX-T DataCenter の操作(ベアメタル)	VMware NSX-T DataCenter のベアメタルサーバ向け操作について説明しています。
22. Lenovo XClarity Controller(XCC)の操作	ベアメタルサーバの管理ツールである Lenovo XClarity Controller(XCC)の操作について説明しています。
23. ライセンスオプションサービス利用手順(ベアメタル)	ベアメタルサーバでライセンスオプションサービスをお申し込みいただいている場合の利用手順について説明しています。
24. 用語集	本書の説明に使われている用語を解説しています。
25. 改訂履歴	本書の改訂履歴です。

1. プライベートクラウドの提供機能

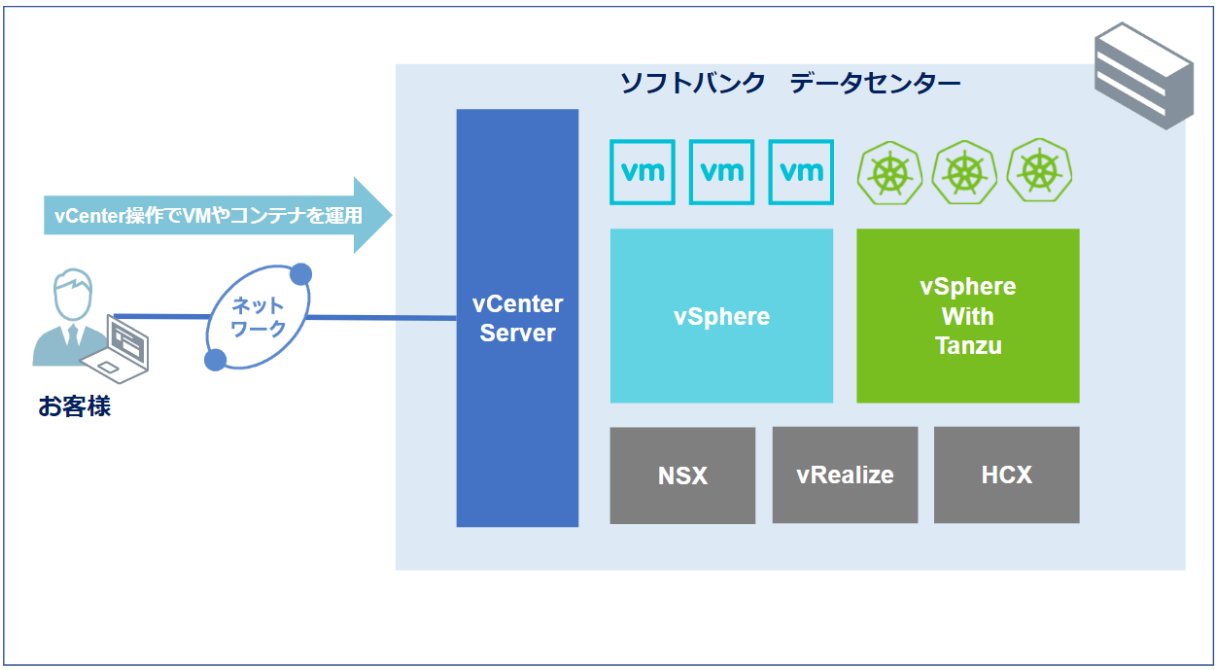
本サービスは、VMware vSphere (以下、vSphereと記載いたします) をベースにしたプライベートクラウドサービスです。当社データセンター内にお客さま専有の物理サーバ、ストレージ、ネットワーク機器を用意し、仮想マシンの実行環境を提供いたします。

お客さまは、本サービスで提供する各種管理ツールにアクセスし、仮想マシンやコンテナ(オプション)などの操作や管理を実施いただけます。

1.1. プライベートクラウドの構成

本サービスでは、お客さまがご契約されたサービスの内容に基づき、仮想化基盤上に下記図の製品群をご提供いたします。各製品は標準提供される標準機能と、お客さま任意にご契約いただくオプション機能により構成されます。

サービス概要図



1.2. 標準機能と管理ツール

本サービスでは下記のソフトウェアと管理ツールを標準機能としてご提供いたします。

各管理ツールの操作方法は後述の操作方法解説ページをご参照ください。

機能	管理ツール	機能概要
VMware vCenter Server	vSphere Client	vSphere 仮想化基盤のベースコンポーネントとなる製品です。 VMware vCenter Server では、代表的なものとして下記の機能をご提供いたします。 • 仮想マシンの作成や仮想ハードウェアスペックの編集、電源ON/OFFなどの操作 • 仮想化基盤のコンピューティングリソース利用状況の把握 • リソースプールの作成・管理 • 仮想マシンへのコンソール接続 • 仮想マシンのタスク、イベント履歴の参照
VMware NSX-T DataCenter	NSX Manager	vSphere 仮想化基盤上の仮想ネットワークを管理する製品です。 仮想マシンで使用する Overlay Network の作成・管理や、ファイアウォール機能、NAT 機能などの各種ネットワーク機能を利用することが可能です。
vRealize Operations Manager	vRealize Operation Manager	vSphere 仮想化基盤上のサーバや仮想マシンの利用状況をモニタリングする製品です。 専用ストレージの容量監視にも利用します。 利用状況を包括的に参照するダッシュボード機能や、各種トラブルの原因特定支援機能があります。

1.3. プライベートクラウドのオプション機能

本サービスでは下記のソフトウェアをオプション機能としてご提供いたします。

各製品の操作方法は後述の操作方法解説ページをご参照ください。

機能	機能概要
移行ツール (VMware HCX)	VMware HCX により、お客さまのオンプレミス環境上の vSphere と本サービス間での VM 移行機能を追加するオプションです。 本オプションでは、VMware HCX のライセンスをご提供いたします。
コンテナ機能 (vSphere with Tanzu)	vSphere with Tanzu により、本サービスの VMware vCenter Server 上に Kubernetes によるコンテナ機能を追加するオプションです。 本オプションでは、vSphere with Tanzu のライセンスをご提供いたします。
エコノミーストレージ	共有ストレージを複数のお客さまでご利用いただくシェアリング型のストレージサービスです。 ストレージ領域は論理的に分割されていますので、割り当てられた領域はお客さま専用としてご利用いただけます。
NSX ロードバランサ	NSX-T によるロードバランサ機能をご提供いたします。 コンテナ機能オプションをご利用の際は必須メニューとなります。
多機能ロードバランサ	セイコーソリューションズ社が提供する多機能ロードバランサ「Netwiser Virtual Edition」をご提供いたします。
Cloud One Workload Security	トレンドマイクロ社が提供するクラウド環境保護ソリューション「Trend Micro Cloud One」のうち、VM のセキュリティ対策製品である「Workload Security」をご利用いただけるサービスです 。
アンチウイルス オプション	ソフォス社が提供する「Central Server Protection」により、VM に対するウイルス対策機能をご利用いただけるサービスです。
Acronis Cyber Backup powered by ASPIRE	アクロニス社が提供する「Acronis Cyber Protect Cloud」により、VM のバックアップ機能をご利用いただけるサービスです。
モニタリング （Mackerel）	はてな社が提供する Mackerel をご利用いただき、仮想マシン監視および外形監視(URL 監視)を行う SaaS 型モニタリングサービスです。

1.4. プライベートクラウド管理ツールの通信要件

本サービスの提供機能をご利用いただくには、各製品の管理ツールへのアクセス経路が必要になります。

各製品の管理ツールへのアクセスは、ご契約時に『ヒアリングシート』にご記入いただいたネットワークからのみ可能です。

各管理ツールを利用するために必要な通信要件は、以下の通りです。

お客さまの端末から以下の「宛先」URLへの名前解決、およびプロトコル/ポート宛の通信が可能となるようご準備ください。「宛先」と対応するIPアドレスについては、『開通通知書』をご参照ください。

管理ツール名称	宛先	プロトコル	ポート
vSphere Client	vca001.aspr.lan	TCP	443
NSX Manager	nsx001.aspr.lan	TCP	443
vRealize Operations Manager	vrops001.aspr.lan	TCP	443

1.5. プライベートクラウド管理のためのソフトウェア要件

各製品の管理ツールを利用するためのソフトウェア要件を下記に記載いたします。

vSphere Client

vSphere Client を使用するには、サポート対象の Web ブラウザが必要です。

次のゲスト OS とブラウザ バージョンはヴイエムウェア社によりテスト済みであり、 vSphere Client でサポートされています。

サポートされるゲストオペレーティングシステム

- Windows 32 ビットおよび 64 ビット
- Mac OS

サポートされるブラウザのバージョン

- Google Chrome 89 以降
- Mozilla Firefox 80 以降
- Microsoft Edge 90 以降

NSX Manager

NSX Manager を使用するには、サポート対象の Web ブラウザが必要です。

ヴイエムウェア社推奨のオペレーティングシステムとブラウザは下記の通りです。

ブラウザ	Windows 10	Mac OS X 10.13, 10.14	Ubuntu 18.04
Google Chrome 80	○	○	○
Mozilla Firefox 72	○	○	○
Microsoft Edge	○	-	-
Apple Safari 13	-	○	-

vRealize Operations Manager

vRealize Operations Manager を使用するには、サポート対象の Web ブラウザが必要です。

本サービスの vRealize Operations Manager では、現在の全ての Web ブラウザがサポートされています。

ただし、 ヴイエムウェア社によりテストされているのは以下のブラウザのみです。

- Google Chrome : バージョン 104 および 105
- Mozilla Firefox : バージョン 104
- Microsoft Edge : バージョン 104 および 105
- Safari : バージョン 15 および 16

2. 管理ツールをご利用になる前に

本章では、サービス開通時のテナントの状態についてご説明いたします。

注意事項

本書の掲載内容についての注意事項を下記に記載いたします。

☑重要

本書記載の設定手順について

本書に掲載されている設定手順は設定例を記載しているものとなります。
各種パラメータの詳細や記載のない設定について確認は、ヴイエムウェア社の公式ドキュメントをご参照ください。

各機能内での禁止操作について

本書の各項目にて指定された禁止操作は行わないようご注意ください。
禁止操作を実施された場合は、その設定対象機能はサポート対象外となります。

各機能内でのサービス提供に必要な当社作成済みオブジェクトについて

本サービスで提供する各機能では、「sb_」または「SB_」が名前の先頭に付与されたオブジェクトが作成された状態となります。

これらのオブジェクトに対する変更操作は、サービスに意図しない影響を与える恐れがあるため、お客さまの変更操作を禁止しています。

管理ツールで使用するアカウントの初期パスワードについて

本サービスで提供する各管理ツールで使用するアカウントと初期パスワードは『開通通知書』に記載されています。各管理ツールをご利用になる前には、必ず初期パスワードの変更を実施してください。

参照 「3.5 パスワード変更手順」

本サービスの管理のためのリソース使用について

本サービスでは、あらかじめサービス提供に必要な仮想マシンやネットワーク・ストレージが構成済みですが、それらはお客さまのユーザ権限では非表示設定となっています。

そのため、各製品の機能にてリソースの使用状況を参照された際、お客さまによる使用分以上に、リソースが使用されているように見える場合があります。

サービス提供に使用されるリソースについては、下記ドキュメントをご参照ください。

参照 『ホワイトクラウド_ASPIRE_プライベートクラウド_サービス説明書』

各製品の構成の上限について

本サービスで提供するVMware各製品の構成上限値は、ヴイエムウェア社の公開情報をご参照ください。

参照 『VMware Configuration Maximums』

2.1. VMware vCenter Server の初期状態

本サービスをご契約後、お客さまへの提供開始時のVMware vCenter Server の状態をご説明いたします。

2.1.1. オブジェクト構成

VMware vCenter Server で管理されるオブジェクトは、全て vCenter Server を頂点とするツリー形式で構成されています。

お客さまへのお引渡し時は、vCenter Server オブジェクト「vca001.aspr.lan」、データセンターオブジェクト「dc01」配下に、各オブジェクトが配置されています。

ホストおよびクラスタ

クラスタオブジェクト「cluster01」が作成済みの状態でご提供いたします。
管理パッケージに含まれるホスト、および追加ホストは「cluster01」配下の ESXi ホスト として登録されます。また、初期リソースプールとして「user_resourcepool」が作成されています。

> **補足** 管理パッケージを追加でご契約いただいた際に、それぞれ「cluster02」、「cluster03」、「cluster04」としてご提供いたします。

仮想マシンおよびテンプレート

初期仮想マシンフォルダとして、次の２つのフォルダが作成された状態でのご提供となります。

- 「Discovered virtual machine」(vSphere 既定の作成済みフォルダ)
- 「user_resource」

ストレージ

ご契約いただいた専用ストレージのサイズに応じたデータストアをご提供いたします。

専用ストレージに構成されたデータストアは、「tenant-***XX***-***YYY***-resource***ZZ***」のデータストア名で登録されます。

また、オプションサービスであるエコノミーストレージをご契約の場合は、「tenant-***XX***-***YYY***-economy***ZZ***」のデータストア名で登録されます。

> **補足** 契約内容に応じて提供される具体的なデータストア名は、『開通通知書』に記載されています。

ネットワーク

VMware NSX-T DataCenter にて使用される分散仮想スイッチ「dswitch01」と、
設定済みアップリンクポート「dswtich-DVUplinks-***XXXX***」が設定された状態でご提供いたします。

コンテンツライブラリ

初期登録済みコンテンツライブラリとして、「sb_library」が登録された状態でご提供いたします。

このコンテンツライブラリには、本サービスにて提供されるOSテンプレートや、ISOイメージが格納されています。

ワークロード

オプションサービスであるコンテナ機能をご契約の場合は、vCenter Server 上の「ワークロード管理」コンテンツが利用可能な状態でご提供いたします。

その際、初期設定済み名前空間として、「vmware-system-registry-*****」が登録された状態でのご提供となります。

2.1.2. 構成済みクラスタの設定

VMware vCenter Server にて構成済みのクラスタには、下記が設定されています。

項目	設定内容
vSphere DRS	自動化レベル - 完全自動化 (移行閾値：3)
Proactive DRS	無効
vSphere HA	有効
Proactive HA	無効
アドミッション コントロール	クラスタリソースの割合を予約し、フェイルオーバーキャパシティを定義 予約済みフェイルオーバー CPU キャパシティ：ご契約内容により変動（ホスト 1 台分の予備を確保） 予約済みフェイルオーバー メモリキャパシティ：ご契約内容により変動（ホスト 1 台分の予備を確保）

重要 クラスタの設定変更は、お客さまのユーザ権限で行うことはできません。

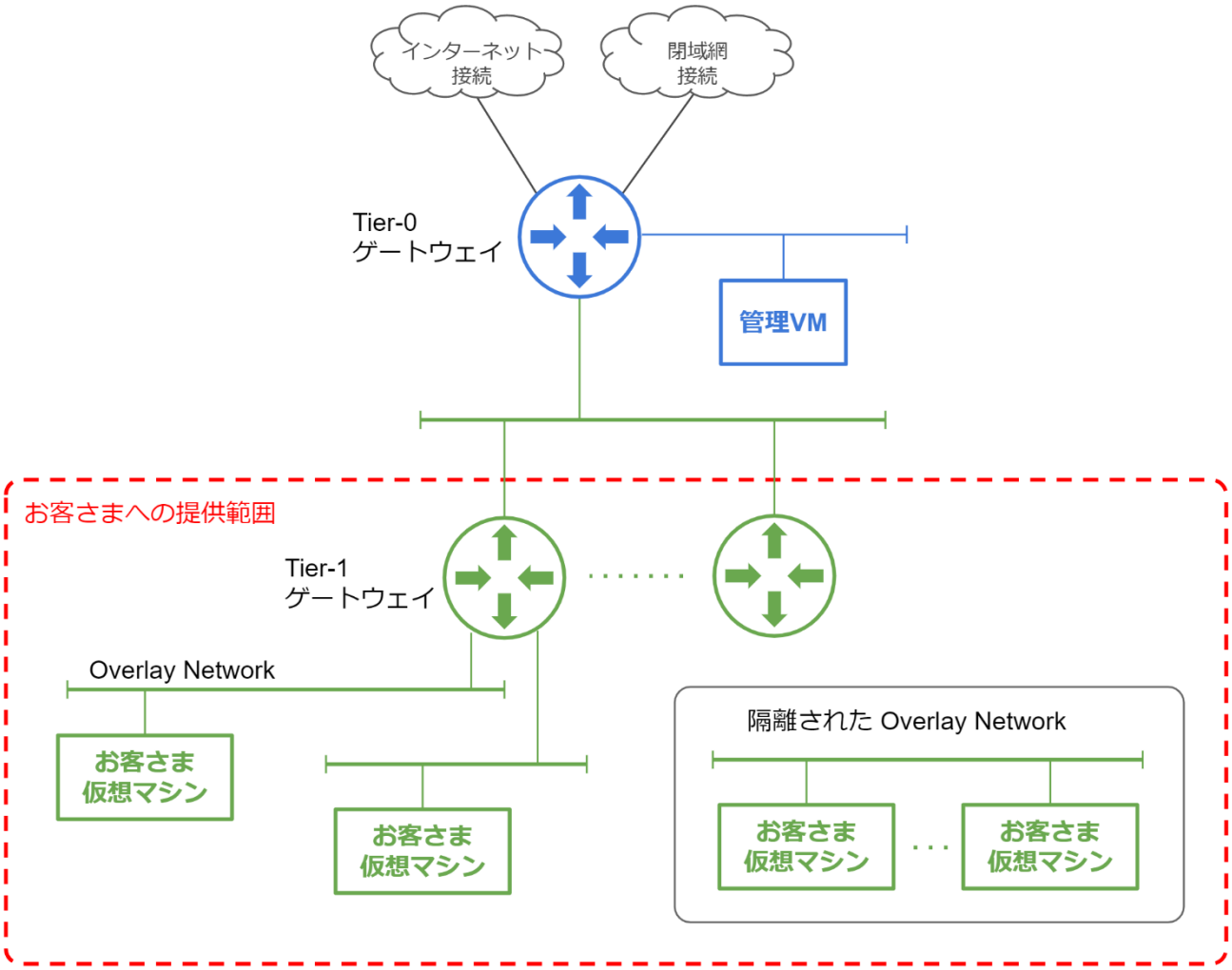
2.2. VMware NSX-T DataCenter の初期状態

本サービスをご契約後、お客さまへの提供開始時の VMware NSX-T DataCenter（以降、「NSX-T」と記載）の状態をご説明いたします。

2.2.1. NSX-T の構成

本サービスにおける NSX-T の構成についてご説明いたします。

プライベートクラウド環境は、外部からのネットワークを接続する Tier-0 ゲートウェイと、お客さま仮想マシンを接続する Tier-1 ゲートウェイによる階層構造となります。お客さまにて操作いただける範囲は Tier-1 ゲートウェイ以下の環境となります。



NSX-Tは、サービス開通時に以下の設定にてご提供いたします。各設定の詳細内容は、「2.2.2 Tier-0 ゲートウェイ」以降の各項目にて記載いたします。

内容	説明
Tier-0 ゲートウェイ	Tier-0 ゲートウェイは外部ネットワークおよび Tier-1 ゲートウェイとの接続を行います。 『ヒアリングシート』に記載いただいた内容に従い下記設定済みの Tire-0 ゲートウェイをご提供いたします。 ・ 他サービス接続用のインターフェイスの作成 ・ スタティックルートの設定 Tier-0 ゲートウェイはお客さまによる新規作成・削除・変更を行うことはできません。
Tier-1 ゲートウェイ※1	Tier-1 ゲートウェイは Overlay Network の作成、NAT、VPN などの各種設定で利用することができます。 サービス開通時点でサンプルとして Tier-1 ゲートウェイが 1 つ作成されております。 Tier-1 ゲートウェイはお客さまによる新規作成・削除・変更を行うことが可能です。
セグメント※1	セグメントを作成することにより Tier-0/Tier-1 ゲートウェイに VLAN や Overlay Network のネットワークを接続できます。 サービス開通時点で当社の管理 VM 用のセグメントを作成していますが、これらの設定の変更や削除は禁止操作となります。
IP プール※1	サービス開通時点で当社管理 VM にて利用する IP プールを 1 つ作成しています。IP プールの新規作成、設定の変更、削除はお客さまでは実施できません。
グループ※1	サービス開通時点でゲートウェイ ファイア ウォールで利用するグループの定義を作成しています。 事前に作成されたグループにはお客さまの VM が外部と通信する際に設定が必要な定義も含まれております。
ゲートウェイ ファイアウォール	ゲートウェイ ファイアウォールは Tier0/Tier1 ゲートウェイまたは、Tier-0 ゲートウェイのアップリンクを通る通信を制御します。 サービス開通時点ではテナント内の通信を制限するためのルールを Tier-0 ゲートウェイおよびアップリンク向けに設定しています。これらの設定の変更や削除は禁止操作となります。

※1： コンテナ機能オプションをご契約の場合は、コンテナ機能により自動生成された設定が追加された状態でのご提供となります。

2.2.2. Tier-0 ゲートウェイ

本サービスでは外部ネットワーク(他サービス)接続用、およびTier-1ゲートウェイとの接続用にTier-0 ゲートウェイを作成しています。

Tier-0 ゲートウェイでは、『ヒアリングシート』に記載いただいた内容に従い、下記を設定いたします。

- 他サービス接続用のインターフェイスの作成
- スタティックルートの設定

重要 新規作成、設定変更、削除はお客さまでは実施できませんので、新規外部ネットワーク(他サービス)の接続、およびそれらのネットワークへのスタティックルートの追加は当社にて実施いたします。必要に応じて担当営業・SEにご依頼ください。

2.2.3. Tier-1 ゲートウェイ

Tier-1 ゲートウェイはOverlay Networkの接続、またはNAT、VPNなどの各種サービスを利用する際に使用します。

Tier-1 ゲートウェイの新規作成、設定の変更、削除はお客さまにて実施いただくことも可能です。詳細は「6.3 Tier-1 ゲートウェイの操作」をご参照ください。お客さまへのお引渡し時点では、以下のパラメータのTier-1 ゲートウェイが作成済みです。このTier-1 ゲートウェイは設定例となりますので不要の場合はお客さまにて削除してください。

項目	設定値
Tier-1 ゲートウェイの名前	tier-1_gateway
リンクされた Tier-0 ゲートウェイ	sb_tier-0_gateway
Edge クラスタ	sb_edgecluster01
Edge プールの割り当てサイズ	ルーティング
スタンバイの再配置を有効にする	有効
ルート アドバタイズ	すべて有効

2.2.4. セグメント

セグメントを作成することで、Tier-0/Tier-1 ゲートウェイに VLAN や Overlay Network のネットワークを接続することが可能になります。

> **重要** お客さまへのお引渡し時点では、当社管理セグメントを以下の通り作成済みです。これらの設定の変更や削除は禁止操作となります。

名前	説明
sb_edge-uplink-segment-a	NSX Edge 通信用セグメント
sb_edge-uplink-segment-b	NSX Edge 通信用セグメント
sb_esxi_vmotion-seg	vMotionネットワーク用セグメント
sb_external-***XX***-seg	外部ネットワーク接続用セグメント※1
sb_mgmt-seg	管理VM用セグメント

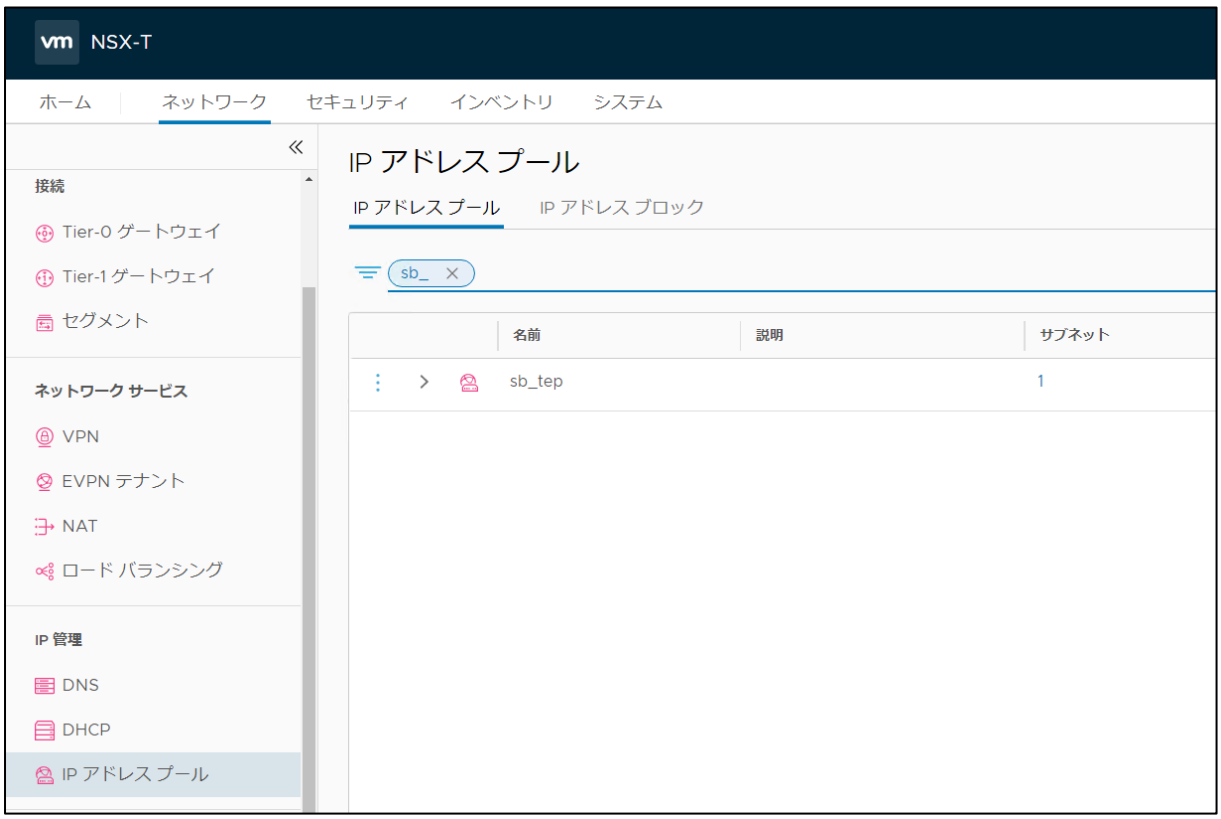
※1：接続しているネットワーク数により、複数存在する場合があります。

2.2.5. IPプール

サービス開通時点で当社管理用仮想マシンにて利用する IP プールを 1 つ作成しています。

> **重要**
> IPプールの新規作成・削除・設定変更は、お客さまでは実施できません。
> また、当社またはシステムにより生成されたIPプールをお客さま操作で使用することは禁止操作とさせていただきます。

名前	説明
sb_tep	Overlay Network 通信で利用するネットワークセグメント定義



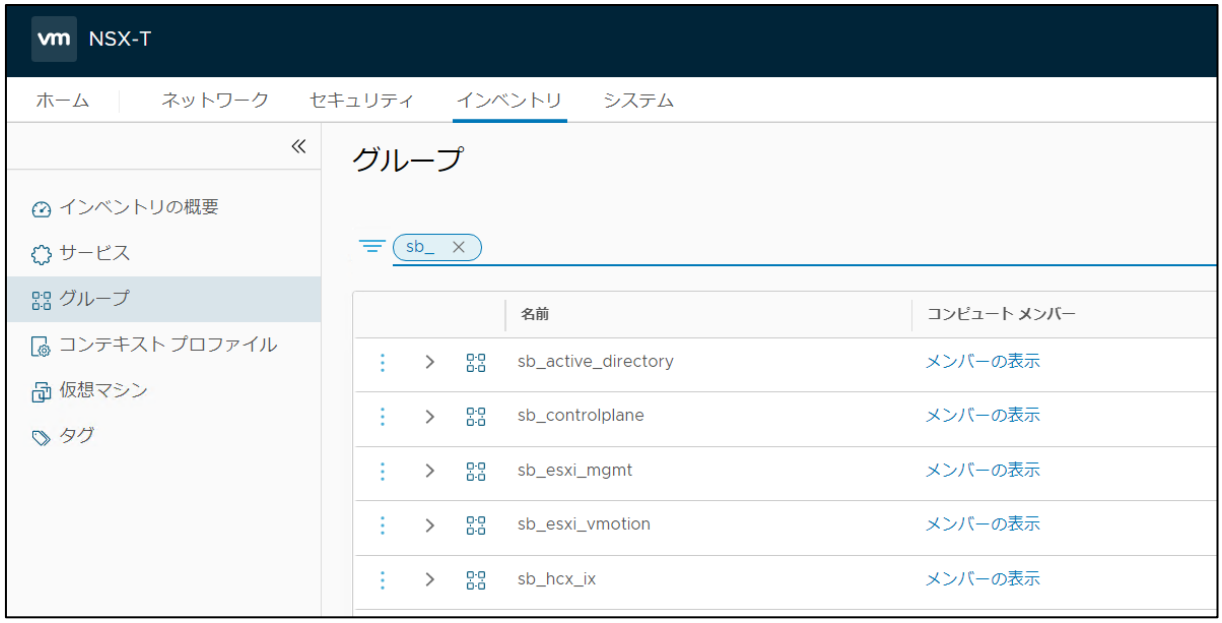
2.2.6. グループ

グループ定義はゲートウェイ ファイアウォールの設定で利用されます。お客さまへのお引渡し時点では、ゲートウェイ ファイアウォールで利用するグループ定義を作成済みです。

これらグループには、お客さまの VM が外部と通信する際に設定が必要となる定義も含まれます。

グループ名	お客さま操作 〇：許可 ×：禁止	説明
sb_active_directory	×	当社管理 VM が使用するグループ定義です。 これらのグループに対する変更や削除は禁止操作となります。
sb_controlplane	×	
sb_esxi_mgmt	×	
sb_esxi_vmotion	×	
sb_hcx_ix	×	
sb_hcx_manager	×	
sb_hcx_ne	×	
sb_mgmt	×	
sb_netwiser	×	
sb_nsx_manager	×	
sb_tanzu	×	
sb_vcenter	×	
sb_vrops	×	
tenant_external	〇	外部から当社管理 VM に接続するネットワークを定義するグループです。 このグループに含まれるメンバーは、当社管理 VM との通信がゲートウェイ ファイアウォールで許可されます。 開通時点では『ヒアリングシート』に記載いただいた IP アドレスを登録済みです。 **☑重要** このグループへのグローバルIP(Any含む)の登録は禁止操作となります。
tenant_external_esxi_mgmt	〇	Advanced cross vCenter vMotion 利用時に使用されます。 お客さま環境の ESXi の管理用 VMkernel IP アドレスを登録することで、プライベートクラウド環境の ESXi との間で Advanced cross vCenter vMotion で必要な通信がゲートウェイ ファイアウォールで許可されます。

グループ名	お客さま操作 〇：許可 ×：禁止	説明
tenant_external_esxi_vmotion	〇	Advanced cross vCenter vMotion 利用時に使用されます。 お客さま環境 ESXi の vMotion 用 VMkernel IP アドレスを登録することで、プライベートクラウド環境の ESXi との間で Advanced cross vCenter vMotion で必要な通信がゲートウェイ ファイアウォールで許可されます。
tenant_external_hcx_ix	〇	移行ツールオプションご契約時に使用されます。 お客さまのオンプレミス環境に構築した HCX-Interconnect の IP アドレスを登録することで、プライベートクラウド環境の HCX-Interconnect との間で必要な通信がゲートウェイ ファイアウォールで許可されます。
tenant_external_hcx_manager	〇	移行ツールオプションご契約時に使用されます。 お客さまのオンプレミス環境に構築した HCX Manager の IP アドレスを登録することで、プライベートクラウド環境の HCX Manager との間で必要な通信がゲートウェイ ファイアウォールで許可されます。
tenant_external_hcx_ne	〇	移行ツール オプションをご契約時に利用します。 お客さまのオンプレミス環境に構築した Network Extension の IP アドレスを登録することで、プライベートクラウド環境の Network Extension との間で必要な通信がゲートウェイ ファイアウォールで許可されます。
tenant_external_vcenter	〇	お客さまオンプレミス環境の vCenter と、プライベートクラウド環境の vCenter 間で、コンテンツライブラリの同期および、Advanced cross vCenter vMotion を実施する時に使用します。 オンプレミス環境の vCenter の IP アドレスを登録することで、プライベートクラウド環境の vCenter との間で必要な通信がゲートウェイ ファイアウォールで許可されます。
tenant_overlay	〇	Overlay Network、NAT や VPN などのサービス IP と外部ネットワークを通信させる際に利用します。 このグループに登録することで、外部ネットワークとの通信が双方向で許可されます。 また、同時に管理ツールとの通信がゲートウェイ ファイアウォールで許可されます。



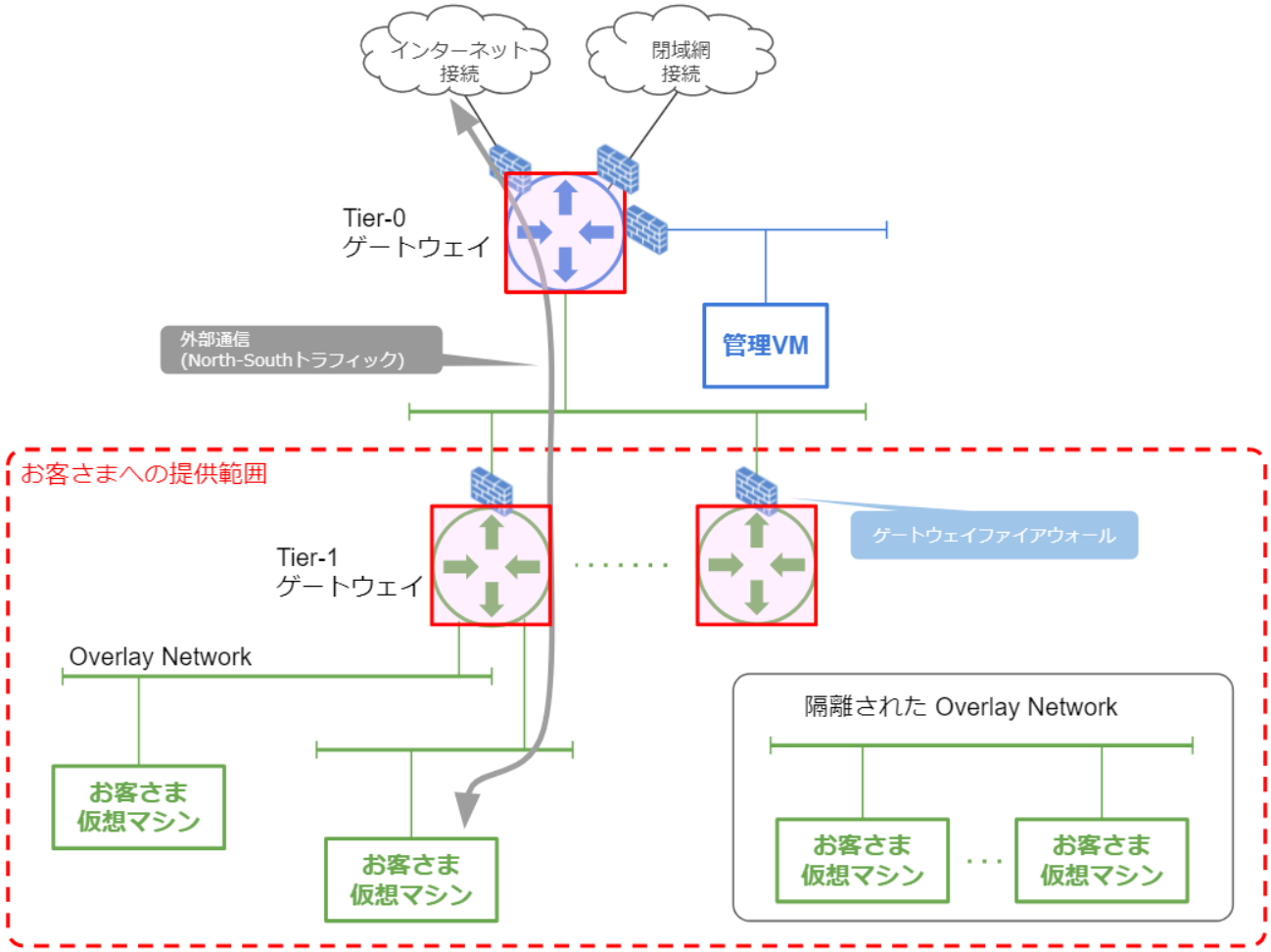
補足

「tenant_overlay」や「tenant_tanzu」への通信を制限する場合は、分散ファイアウォール、または Tier-1ゲートウェイを対象にしたゲートウェイ ファイアウォールをご利用ください。

参照「6.10 分散ファイアウォールの操作」
参照「6.11 ゲートウェイ ファイアウォールの操作」

2.2.7. ゲートウェイ ファイアウォール

外部ネットワークから当社管理用仮想マシンへのアクセスを制限するため、ゲートウェイ ファイアウォールのポリシーを設定済みです。ゲートウェイ ファイアウォールはTier-0 / Tier-1 ゲートウェイ自体、およびTier-0 ゲートウェイのアップリンクを通る通信を制御します。



重要 当社作成のポリシールールは、「事前ルール」-「sb_prerules」配下に設定されています。
当社作成のポリシールールに対するお客さまの削除・設定変更は禁止操作となります。

Tier-0 / Tire-1ゲートウェイのデフォルトルールは下記の通りです。

ゲートウェイ種別	お客さま操作 〇：許可 ×：禁止	デフォルトルール
Tier-0 ゲートウェイ	×	ドロップ
Tier-1 ゲートウェイ	〇	許可

作成済みのデフォルトルール名には、末尾に対象Tier-0/Tier-1 ゲートウェイ名が含まれています。

2.3. vRealize Operations Manager の初期状態

本サービスをご契約後、お客さまへの提供開始時の vRealize Operations Manager の状態をご説明いたします。

2.3.1. 連携済み製品について

vRealize Operations Manager がモニタリングを行う対象として、下記が登録済みです。

VMware vCenter Server

本サービスの vSphere環境上のオブジェクトの稼働状況のモニタリングデータを収集します。
以下のオブジェクトは、自動的にモニタリング対象として登録されます。

- VMware vCenter Server 上で作成した仮想マシンやコンテナ
- VMware NSX-T DataCenter で作成した Overlay Network

専用ストレージ

専用ストレージの残り容量など、詳細な利用状況のモニタリングデータを収集します。

3. システムアカウントの管理について

本章では、本サービスの各種ログインに使用するシステムアカウントの管理方法についてご説明いたします。

3.1. アカウント認証サーバについて

本サービスで提供されるアカウントは認証サーバで統合管理されており、各vSphere製品において共通で使用いたします。

アカウントの追加・削除やパスワードの変更操作は、関連する全てのvSphere製品の認証動作に影響しますので、ご注意ください。

3.2. 提供されるアカウント

本サービスで提供されるアカウントは、ご契約時に入力いただいた『ヒアリングシート』に基づき作成し、サービス開通時に発行する『開通通知書』にてユーザ名および初期パスワードをお知らせします。

3.3. アカウントの種別

本サービスで提供されるアカウントは、権限の異なる２つのアカウントグループのいずれかに所属します。標準構成では各グループにつき１アカウントをご提供いたします。

CustomerAdmins グループアカウント

CustomerAdmins グループに所属するアカウントは、テナントを管理する管理者アカウントです。

このグループに所属するアカウントは、各製品の主な操作権限・設定変更権限を有します。

仮想マシンの作成や起動、設定変更や、新規ネットワークの作成などはこのグループに所属するアカウントをご利用ください。

Customers グループアカウント

Customer グループに所属するアカウントは、各製品の参照権限を持つアカウントです。

このグループに所属するアカウントは、各製品へのログインと、各種情報の参照権限のみ有します。

仮想マシンや基盤システムの動作状況・リソース使用状況の参照のみを行う際はこのグループに所属するアカウントをご利用ください。

3.4. パスワード運用ルール

本サービスで提供されるアカウントのパスワードには、以下のルールが設定されています。

パスワード要件	内容
文字列制限	英数字、記号を含む 8 文字以上の文字列
利用期限	なし
アカウントロック	5 回連続の認証失敗によりロック
ロック解除手順	時間経過による解除(15 分)
過去利用パスワードの制限	過去 5 回までのパスワードは使用不可

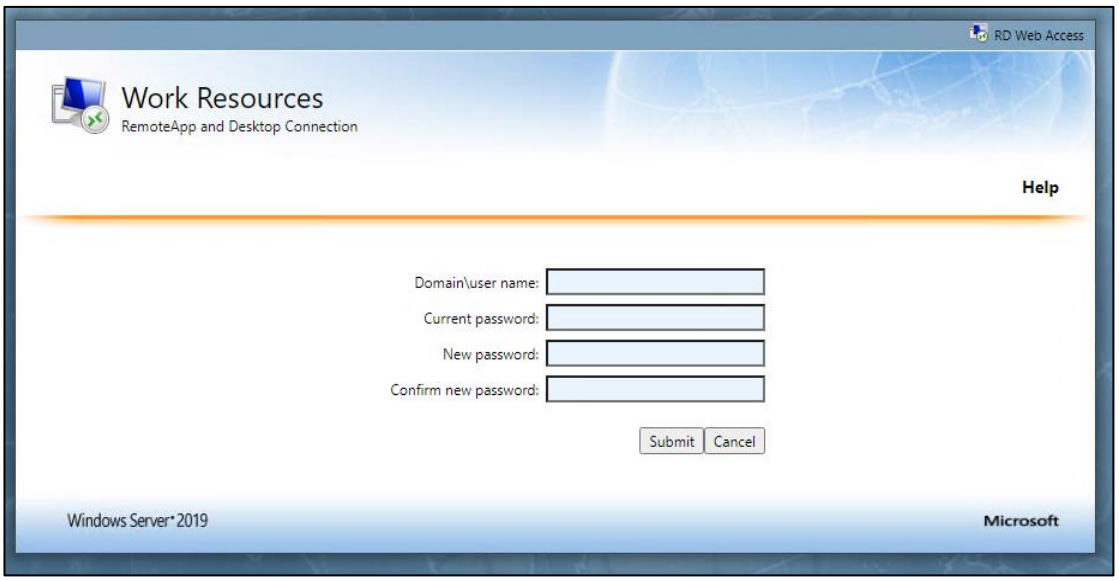
3.5. パスワード変更手順

認証サーバで管理されているアカウントのパスワード変更手順をご説明いたします。

1. Webブラウザより、「RD Web Access」ツールのサイトへアクセスします。

URLは、『開通通知書』の「RD Web Access」に記載されています。

アクセスにより、下記の画面が表示されます。



重要 「RD Web Access」ツールのサイトへのアクセスには、FQDNの名前解決が必要です。
ご利用の端末で『開通通知書』に記載されたFQNDとIPアドレスが名前解決できるように設定を行った上で実施してください。

2. 各入力項目に必要事項を入力し、「Submit」ボタンをクリックします。

パスワードが変更されます。

項目	入力内容
Domain¥user name	aspr¥<パスワード変更を行うユーザ名>
Current password	<現在のパスワード>
New password	<新しいパスワード>
Confirm new password	<新しいパスワード(再度入力)>

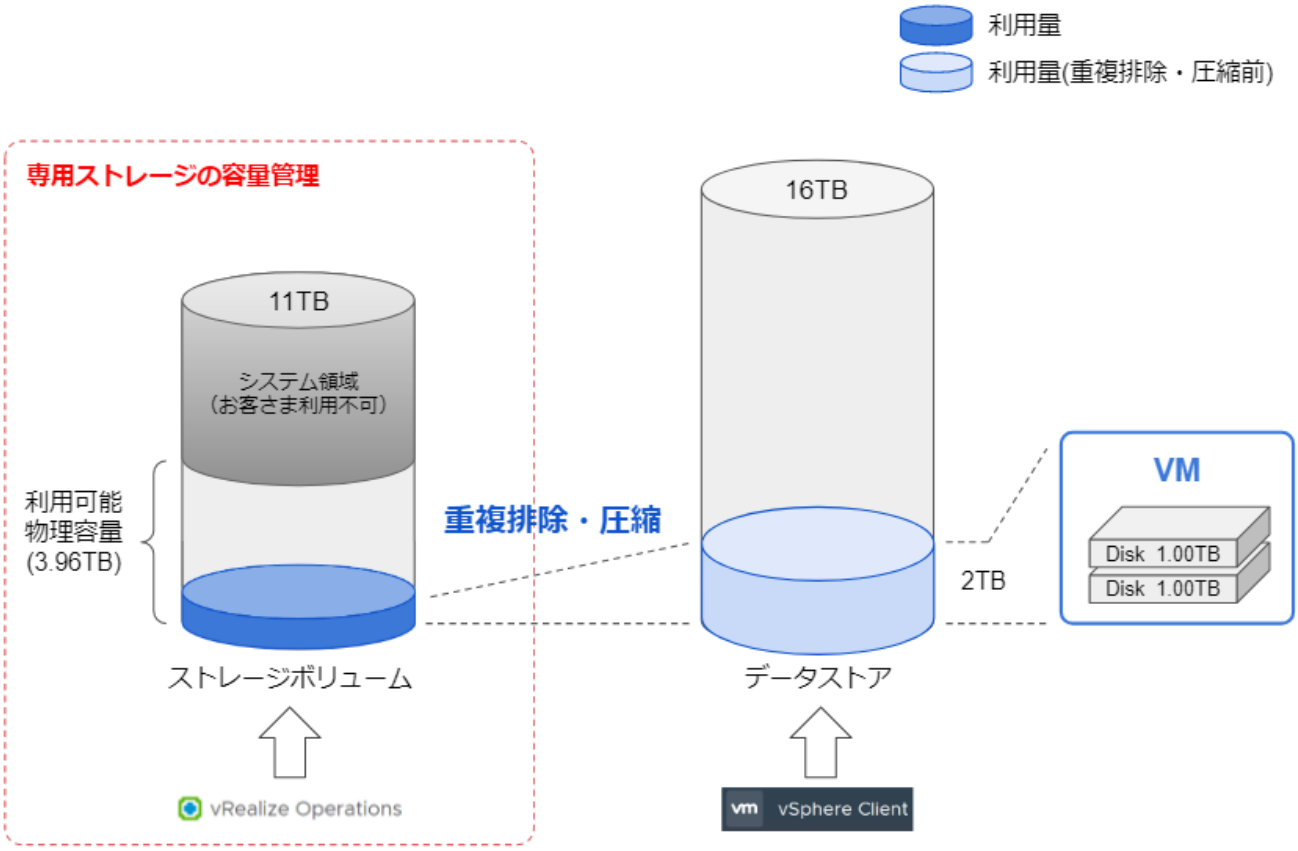
4. 専用ストレージの容量管理について

本章では、ご契約いただいた専用ストレージの容量管理についてご説明いたします。

> **重要** 本章は、本サービスの専用ストレージの利用にあたっての重要事項となります。

専用ストレージの容量管理の考え方

専用ストレージは、ご契約いただいたメニューに応じたサイズの物理容量をご提供いたします。ご利用にあたり、下記の特性・注意事項がありますのでご留意ください。



- vCenter Server 上のデータストア使用量と実際の物理容量の使用量が異なります
- 実際の物理容量使用量は、重複排除・圧縮により軽量化されます
- 重複排除・圧縮率は、格納されたデータの内容により異なります
- 専用ストレージの容量管理は、vCenter Server ではなく vRealize Operations Manager をご利用ください

専用ストレージの利用状況の確認方法

専用ストレージの利用状況は、vRealize Operations Manager のダッシュボード機能にてのみ、確認することが可能です。vCenter Server からは確認できないため、定期的な確認をお願いします。

参照「7.6 カスタムダッシュボードによる専用ストレージの容量管理」

5. VMware vCenter Server の操作

仮想マシンを管理する製品である VMware vCenter Server の操作についてご説明いたします。

ここでは、各機能の代表的な設定手順をご説明いたします。
本ガイドの解説に含まれない内容については、ヴイエムウェア社の公式ドキュメントをご参照ください。

参照 『VMware vSphere ドキュメント』

本サービスの VMware vCenter Server では、以下の機能をご利用いただけます。

項目	お客さま操作可能範囲
ESXi ホスト	**パフォーマンスチャートの参照** ESXi ホストの CPU、メモリなどシステムリソースのパフォーマンスデータを参照することが可能です
データストア	**データストア内のファイル操作** データストアファイルブラウザを使用してファイルの参照、フォルダ作成、削除、ファイルのアップロードおよびダウンロードが可能です
ネットワーク	**NSX-T で作成した Overlay Network の参照** お客さまに作成いただく Overlay Network を参照することが出来ます。 管理操作については NSX Manager からの操作となります
クラスタ	**リソースプール設定** リソースプールの作成、削除、編集が可能です **フォルダ設定** 仮想マシンおよびテンプレートのフォルダ作成、削除、編集が可能です
仮想マシン	**仮想マシンの作成・管理** 仮想の作成、削除やスナップショットの管理などが可能です **アラーム/イベント/タスクの参照** vSphere Client インベントリ内の「タスクおよびイベント」タブに実行中や完了のタスク、発行されたアラートを確認することが可能です
コンテンツライブラリ	ISO イメージ、OVA/OVF ファイル、仮想マシンテンプレートなどのファイルをインポートし、管理・使用することが可能です また、外部のコンテンツライブラリと同期することで、仮想マシンテンプレート以外のファイルを参照することが可能になります
タグの操作	VM などにタグを付けて並べ替えや検索を簡単に行うことが可能です

5.1. vSphere Client の利用について

VMware vCenter Server の操作UIである、vSphere Client へのログイン・ログアウト操作をご説明いたします。

5.1.1. vSphere Client へのログイン

vSphere Client UI へログインします。

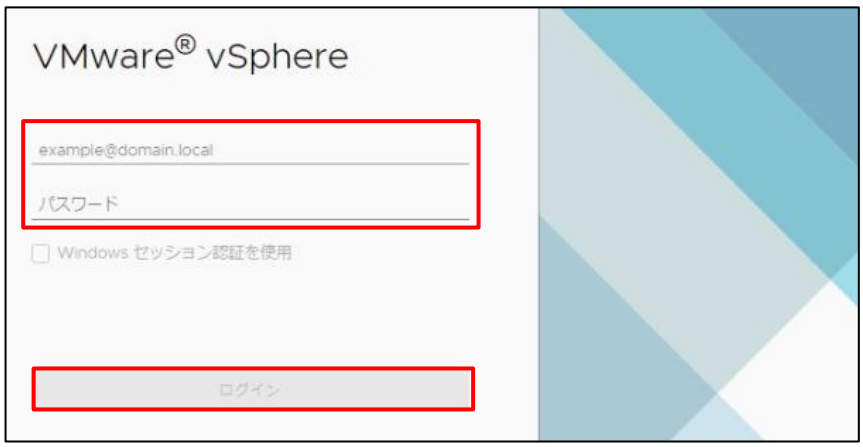
1. **Webブラウザより、vSphere Client の URL にアクセスします。**

   https://vca001.aspr.lan/

2. **「VSPHERE CLIENT (HTML5) の起動」をクリックします。**

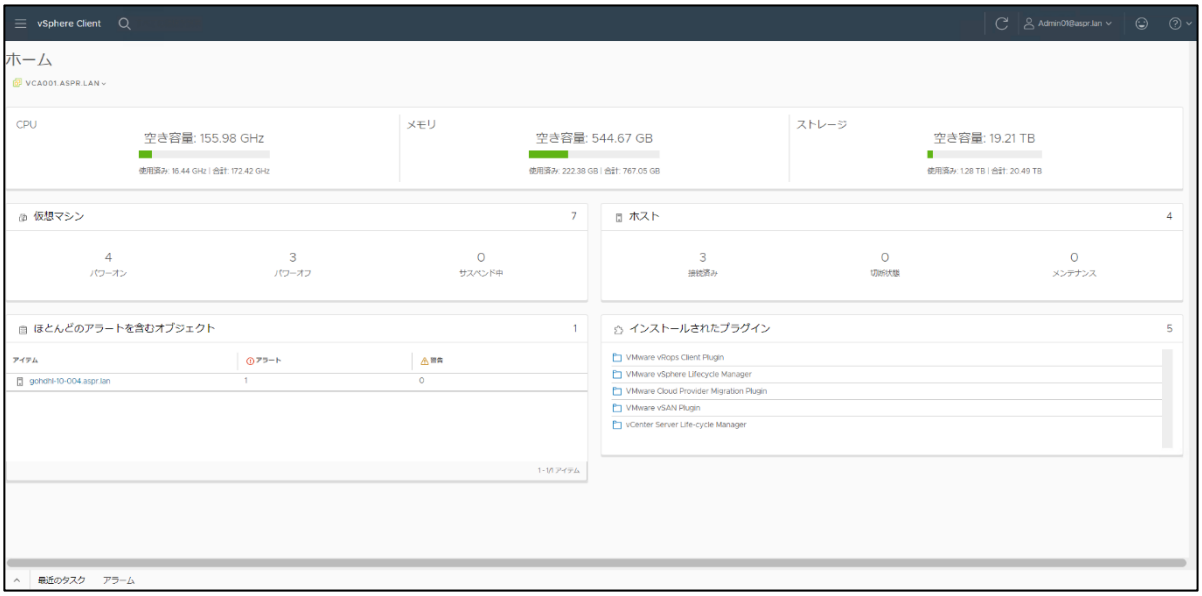
   vSphere Client ログイン画面が表示されます。

3. **ユーザ名とパスワードを入力し、「ログイン」ボタンをクリックします。**



項目	説明
ユーザ名	『開通通知書』に記載されているユーザ名を入力します。
パスワード	上記ユーザ名に設定されたパスワードを入力します。

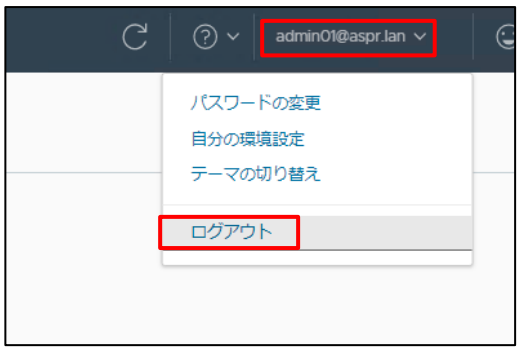
ログインが完了し、以下の画面が表示されます。



5.1.2. vSphere Client からのログアウト

vSphere Client UI からログアウトします。

1. **管理画面の右上のアカウントをクリックし、「ログアウト」をクリックします。**



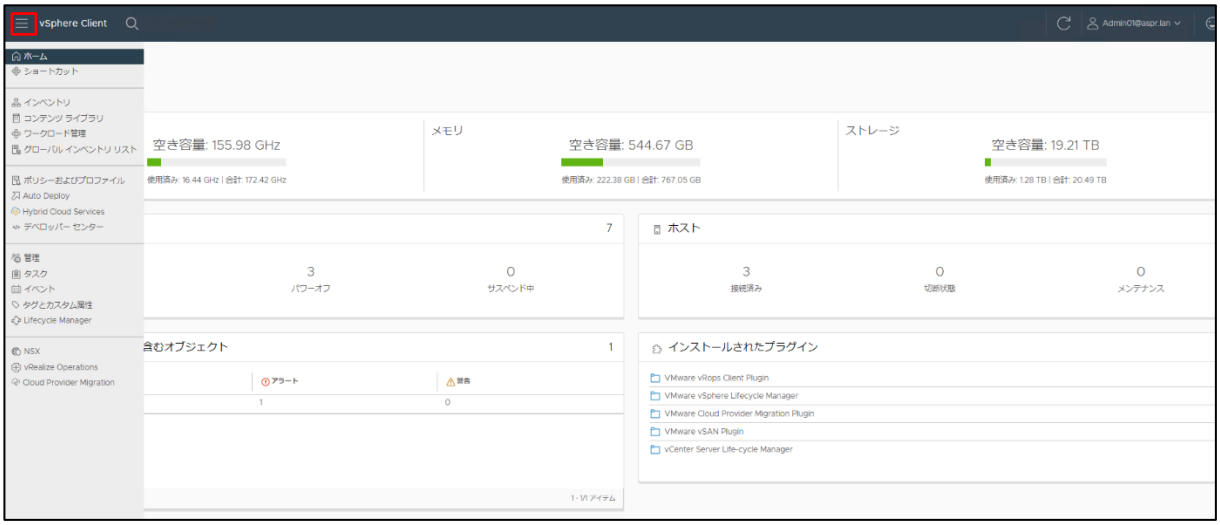
ログアウトが完了し、ログイン画面が表示されます。

5.2. vSphere Client の基本操作

vSphere Client の基本操作をご説明いたします。

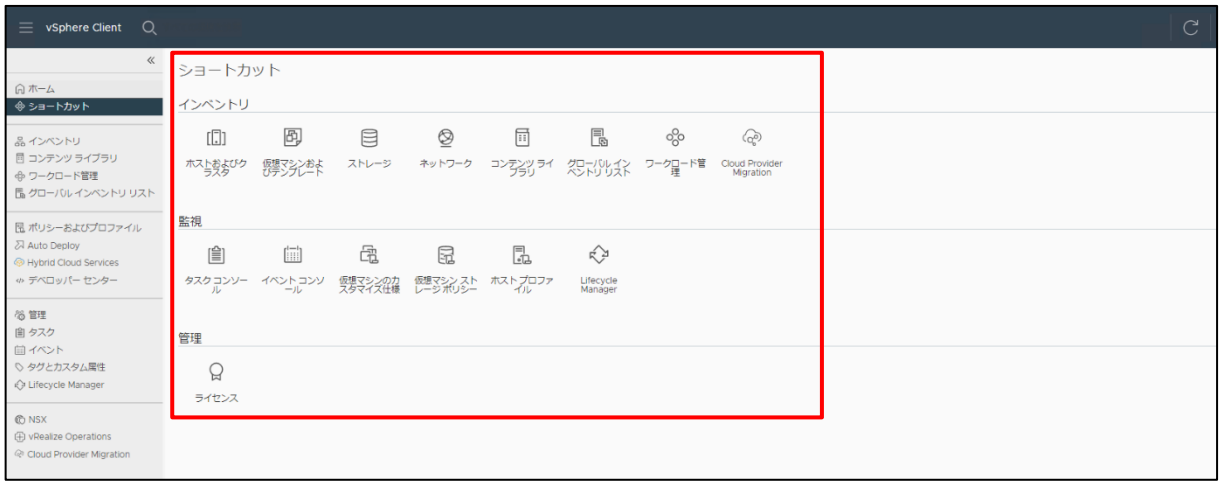
ホームの操作

「ホーム」の下記画面左上の「三」ボタン(赤枠)から、機能の呼び出しや利用状況サマリのダッシュボードを閲覧できます。



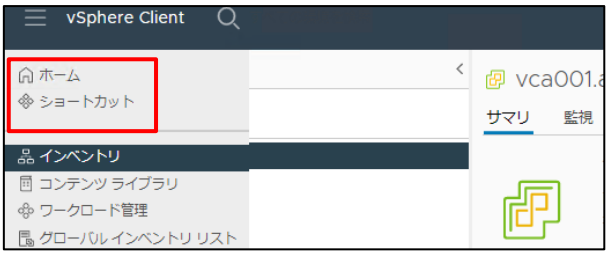
ショートカットからの操作

「ショートカット」のメニューから、機能の呼び出しや、よく使う機能を呼び出せます。

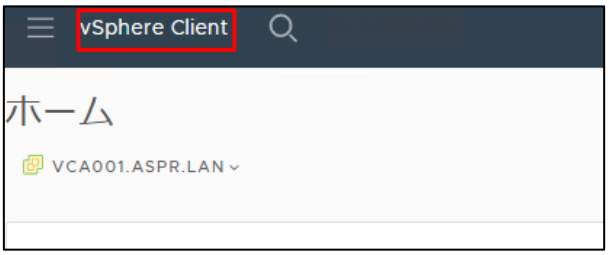


ホームまたはショートカットに戻る操作

各種機能のページからホーム、またはショートカット画面へ戻る際は、画面左上の「三」ボタンをクリックし、表示されたリストから「ホーム」または「ショートカット」をクリックします。



また、画面上部の「vSphere Client」ラベルをクリックすることで、ショートカット画面へ戻ることも可能です。



5.3. 仮想マシンの管理操作

vSphere Client を用いた仮想マシンの管理操作をご説明いたします。

5.3.1. 仮想マシンの作成

仮想マシンの作成手順をご説明いたします。

1. **vSphere Client の「三」ボタンより、「インベントリ」をクリックします。**

   「インベントリ」画面へ遷移します。

2. **「仮想マシンおよびテンプレート」のツリーより、フォルダを右クリックし、メニューから「新規仮想マシン」をクリックします。**

   「新規仮想マシン」の作成ウィザード画面が表示されます。

3. **「1.作成タイプの選択」にて、仮想マシンの作成方法を指定します。**
   「新規仮想マシンの作成」を選択し、「Next」ボタンをクリックします。

   「2.名前とフォルダの選択」画面が表示されます。

4. **仮想マシン名を入力後、仮想マシンを作成するフォルダを選択し、「Next」ボタンをクリックします。**

   「3.コンピューティングリソースの選択」画面が表示されます。

5. **仮想マシンを作成するリソースプールを選択し、互換性チェックが成功したことを確認後、「Next」ボタンをクリックします。**

   「4.ストレージの選択」画面が表示されます。

6. **仮想マシンを作成するデータストアを選択し、互換性チェックが成功したことを確認後、「Next」ボタンをクリックします。**

   「5.互換性の選択」画面が表示されます。

7. **仮想マシンの互換対象を選択し、「Next」ボタンをクリックします。**

   「6.ゲストOSを選択」画面が表示されます。

8. **仮想マシンにインストール予定のゲストOSとそのバージョンを選択し、「Next」ボタンをクリックします。**

   「7.ハードウェアのカスタマイズ」画面が表示されます。

9. 仮想マシンに割り当てる仮想ハードウェアスペック、またはオプションを選択し、「Next」ボタンをクリックします。

「8.設定の確認」画面が表示されます。

10. 作成する仮想マシンの設定内容に間違いがないことを確認し、「FINISH」ボタンをクリックします。

仮想マシンの作成タスクが実行され、指定したリソースプール配下に仮想マシンが作成されます。

5.3.2. 仮想マシンの編集

仮想マシンの編集手順をご説明いたします。

1. vSphere Client の「三」ボタンより、「インベントリ」をクリックします。

「インベントリ」画面へ遷移します。

2. 左ペインのツリーより、設定変更を行う仮想マシンを右クリックし、メニューから「設定の編集」をクリックします。

「設定の編集」画面が表示されます。

3. 「仮想ハードウェア」タブにて、仮想マシンのハードウェアスペックを変更します。
デバイスを追加する場合は、「新規デバイスを追加」ボタンから、追加するデバイスをクリックした後、デバイスのスペックを指定します。

4. 「仮想マシンオプション」タブにて、必要なオプション変更を行います。

5. 「OK」ボタンをクリックします。

「仮想マシンの再設定」タスクが実行されます。タスクステータスが「完了」になることを確認します。

5.3.3. 仮想マシンの削除

仮想マシンの削除手順をご説明いたします。

1. **vSphere Client の「三」ボタンより、「インベントリ」をクリックします。**

   「インベントリ」画面へ遷移します。

2. **左ペインのツリーより、削除を行う仮想マシンをクリックします。**

   画面右ペインに、クリックした仮想マシンのサマリ画面が表示されます。

3. **削除を行う仮想マシンが「パワーオフ」状態であることを確認します。**

4. **右ペインの「アクション」をクリックし、メニューより「ディスクから削除」をクリックします。**

   「削除の確認」画面が表示されます。

5. **仮想マシン名に間違いが無いことを確認し、「はい」ボタンをクリックします。**

   「仮想マシンの削除」タスクが実行されます。タスクステータスが「完了」になり、ツリーから仮想マシンが削除されたことを確認します。

> **補足** **仮想マシン削除の注意事項**
>
> 「パワーオン」状態の仮想マシンは削除できません。必ず「パワーオフ」状態であることを確認した上で実行してください。
>
> また、「アクション」メニューの「インベントリから削除」を実行した場合、同様にツリーから仮想マシンは削除されますが、データストア内に仮想マシンデータが残された状態となります。
>
> データストアの容量は消費されたままとなりますので、ご注意ください。

5.3.4. 仮想マシンのパワーオン

仮想マシンのパワーオン手順をご説明いたします。

1. **vSphere Client の「三」ボタンより、「インベントリ」をクリックします。**

   「インベントリ」画面へ遷移します。

2. **左ペインのツリーより、パワーオンを行う仮想マシンをクリックします。**

   画面右ペインに、クリックした仮想マシンのサマリ画面が表示されます。

3. **右ペインの「アクション」をクリックし、メニューより「電源」>「パワーオン」をクリックします。**

   「仮想マシンのパワーオン」タスクが実行されます。タスクステータスが「完了」になることを確認します。

5.3.5. 仮想マシンのゲストOSシャットダウン

仮想マシンで動作中のゲストOSのシャットダウン手順をご説明いたします。

1. **vSphere Client の「三」ボタンより、「インベントリ」をクリックします。**

   「インベントリ」画面へ遷移します。

2. **左ペインのツリーより、シャットダウンを行う仮想マシンをクリックします。**

   画面右ペインに、クリックした仮想マシンのサマリ画面が表示されます。

3. **右ペインの「アクション」をクリックし、メニューより「電源」>「ゲストOSのシャットダウン」をクリックします。**

   「ゲストOSのシャットダウン」タスクが実行されます。タスクステータスが「完了」になることを確認します。

> **補足** **仮想マシンの停止方法の違いについて**
>
> 仮想マシンの停止は、「アクション」メニューの「電源」操作内の「ゲストOSのシャットダウン」のほかに、「パワーオフ」または「強制終了」の操作でも実行可能ですが、それぞれ停止に伴う挙動が異なります。
>
> - 「ゲストOSのシャットダウン」
>
>   仮想マシン上で稼働中のゲストOSにシャットダウンシグナルを発行し、停止させます。
>   ゲストOSのシャットダウンシーケンスに従い、各プロセスの停止が行われた上でパワーオフ状態となります。
>   この操作は、VMware Tools が動作中の仮想マシンのみ実行可能です。
> - 「パワーオフ」
>
>   仮想マシンの電源状態を停止状態に変更します。動作中のゲストOSのシャットダウン処理は行われません。
> - 「強制終了」
>
>   vSphere上の仮想マシンの実行プロセスを強制的に停止します。

5.3.6. 仮想マシンへのコンソール接続

VMware Remote Console機能を用いて、仮想マシンのコンソールへ接続する手順をご説明いたします。

1. **vSphere Client の「三」ボタンより、「インベントリ」をクリックします。**

   「インベントリ」画面へ遷移します。

2. **左ペインのツリーより、コンソール接続を行う仮想マシンをクリックします。**

   画面右ペインに、クリックした仮想マシンのサマリ画面が表示されます。

3. **右ペインのサマリ画面にて「Webコンソールの起動」をクリックします。**

   別ウィンドウにて仮想マシン Webコンソールが表示されます。
   ウィンドウをマウスでクリックし、対象の仮想マシンのコンソール操作ができることを確認します。

> **重要** **VMware Remote Console アプリケーションを使用したコンソール接続について**
>
> 本サービスでは、VMware Remote Console アプリケーションを使用した「Remote Console」機能は利用できません。仮想マシンへのコンソール接続を行う際は、Webコンソールをご利用ください。

5.3.7. VMware Tools のインストール

仮想マシンに VMware Tools をインストールする手順をご説明いたします。

> **重要** **仮想マシンへの VMware Tools インストールについて**
>
> - VMware Tools は必ずインストールしてご利用ください。ゲスト OS に VMware Tools がインストールされていない場合は、運用サポート上の制限が生じる可能性があります。
> - 当社が提供するテンプレートには、VMware Tools が含まれています。
> - VMware Tools のインストール方法の詳細は、ヴイエムウェア社の公式ドキュメントをご参照ください。
>
> 参照 『VMware Tools のインストール』

仮想マシンがLinuxの場合、以下の2種類のいずれかのVMware Toolsをインストールします。

- ヴイエムウェア社提供の VMware Tools
- 各 Linux ディストリビューションからリリースされている open-vm-tools

補足

OSのバージョンにより推奨されるVMware Toolsが異なります。open-vm-toolsの対象OSは、以下のWebサイトをご参照ください

参照 『VMware KB：VMware による open-vm-tools のサポート』

Windows に VMware Tools をインストールする

Windows の仮想マシンに VMware Tools をインストールする方法をご説明いたします。

1. **vSphere Client の「三」ボタンより、「インベントリ」をクリックします。**

   「インベントリ」画面へ遷移します。

2. **左ペインのツリーより、VMware Tools のインストールを行う仮想マシンを右クリックし、メニューから「ゲストOS」>「VMware Tools のインストール」をクリックします。**

   対象仮想マシンに VMware Tools インストーラがマウントされます。

3. **仮想マシンをクリックします。**

   画面右ペインに、クリックした仮想マシンのサマリ画面が表示されます。

4. **右ペインのサマリ画面にて「Webコンソールの起動」をクリックします。**

   別ウィンドウにて仮想マシン Webコンソールが表示されます。

5. **対象仮想マシンに管理者ユーザでログインし、マウントされたメディアから「setup.exe」を実行します。**

   インストールウィザードが起動します。

6. **インストールウィザードに従い、VMware Toolsのインストールを実行します。**

   インストール完了後、システムの再起動を実行するウィンドウが表示されます。

7. **「はい」ボタンをクリックします。**

   ゲストOSが再起動します。画面右ペインに、クリックした仮想マシンのサマリ画面が表示されます。

8. **再度対象仮想マシンにログインし、システムトレイにて VMware Tools のアイコンが表示されていることを確認します。**

Linux に VMware Tools をインストールする

Linux の仮想マシンに VMware Tools をインストールする方法をご説明いたします。

1. vSphere Client の「三」ボタンより、「インベントリ」をクリックします。

「インベントリ」画面へ遷移します。

2. 左ペインのツリーより、VMware Tools のインストールを行う仮想マシンを右クリックし、メニューから「ゲストOS」>「VMware Tools のインストール」をクリックします。

対象仮想マシンに VMware Tools インストーラがマウントされます。

3. 仮想マシンをクリックします。

画面右ペインに、クリックした仮想マシンのサマリ画面が表示されます。

4. 右ペインのサマリ画面にて「Webコンソールの起動」をクリックします。

別ウィンドウにて仮想マシン Webコンソールが表示されます。

5. 対象仮想マシンにroot権限を持つユーザでログインします。

6. 以下のコマンドを実行します。

 # mkdir /mnt/cdrom
 # mount /dev/cdrom /mnt/cdrom（イメージのマウント）
mount: block device /dev/sr0 is write-protected, mounting read-only
 # cd /tmp
 # ls /mnt/cdrom
mainifest.txt VMwareTools-8.3.17-784891.tar.gz（ファイル名を控えてください）
 # tar zxpf /mnt/cdrom/VMwareTools-8.3.17-784891.tar.gz（パッケージの解凍）
 # umount /dev/cdrom（イメージのアンマウント）
 # cd vmware-tools-distrib
 # ./vmware-install.pl（インストールスクリプトの実行）
Creating a new VMware Tools installer database using the tar4 format.

Installing VMware Tools.

In which directory do you want to install the binary files?
[/usr/bin]（**「Enter」キー**）

What is the directory that contains the init directories (rc0.d/ to rc6.d)?
[/etc/rc.d]（**「Enter」キー**）

What is the directory that contains the init scripts?
[/etc/rc.d/initd]（**「Enter」キー**）

In which directory do you want to install the damon files?
[/usr/sbin]（**「Enter」キー**）

In which directory do you want to install the library files?
[/usr/lib/vmware-tools]（**「Enter」キー**）

The path [/usr/lib/vmware-tools] does not exist currently. This program is going to create it, including needed parent directories. Is this what you want? [yes]
（**「Enter」キー**）

In which directory do you want to install the documentation files?
[/usr/share/doc/vmware-tools]（**「Enter」キー**）

The path [/usr/share/doc/vmware-tools] does not exist currently. This program is going to create it, including needed parent directories. Is this what you want? [yes]
（**「Enter」キー**）

The installation of VMware Tools 8.3.17 build-784891 for Linux completed successfully. You can decide to remove this software from your system at any time by invoking the following command: [/usr/bin/vmware-uninstall-tools.pl].

Before running VMware Tools for the first time, you need to configure it by invoking the following command: [/usr/bin/vmware-config-tools.pl]. Do you want this program to invoke the command for you now? [yes]（**「Enter」キー**）

Initializing...

<snip>

The VMware Host-Guest Filesystem allows for shared folders between the host OS and the guest OS in a Fusion or Workstation virtual environment. Do you wish to enable this feature? [no]（**「Enter」キー**）

The vmblock enables dragging of copying files between host and guest in a Fusion or Workstation virtual environment. Do you wish to enable this feature? [no]（「Enter」キー）

<snip>

Please enter a number between 1 and 29:

[3]（**「Enter」キー**）
<snip>
The configuration of VMware Tools 8.3.17 build-784891 for Linux for this running kernel completed successfully.

<snip>

Found VMware Tools CDROM mounted at /media/VMware Tools. Ejecting device /dev/hda ...（インストール、セットアップの完了）

 # exit（ログオフ）

以上でインストールが完了します。

Linux に open-vmware-Tools をインストールする

Linuxの仮想マシンに各Linuxディストリビューションからリリースされているopen-vm-toolsをインストールする方法をご説明いたします。ここでは、例としてCentOS 7にインストールする手順でご説明いたします。

1. vSphere Client の「三」ボタンより、「インベントリ」をクリックします。

「インベントリ」画面へ遷移します。

2. 左ペインのツリーより、VMware Tools のインストールを行う仮想マシンをクリックします。

画面右ペインに、クリックした仮想マシンのサマリ画面が表示されます。

3. 右ペインのサマリ画面にて「Webコンソールの起動」をクリックします。

別ウィンドウにて仮想マシン Webコンソールが表示されます。

4. 対象仮想マシンにroot権限を持つユーザでログインします。

5. 以下のコマンドを実行します。

```
# yum install open-vm-tools （open-vm-toolsのインストールを実行する）
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
* base: ftp.iij.ad.jp
* extras: ftp.iij.ad.jp
* updates: ftp.iij.ad.jp
Resolving Dependencies
--> Running transaction check
---> Package open-vm-tools.x86_64 0:10.1.5-3.el7 will be installed
（中略）
Transaction Summary
================================================================================
================================================================================
====== ========================================
```

```
Install 1 Package (+11 Dependent packages) Upgrade ( 1 Dependent package)
Total download size: 8.7 M
Is this ok [y/d/N]: y （必要なパッケージのダウンロードを許可する）
Downloading packages:
（中略）
Total
18 MB/s | 8.7 MB 00:00:00
Retrieving key from file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
Importing GPG key 0xF4A80EB5:
Userid : "CentOS-7 Key (CentOS 7 Official Signing Key)<security@centos.org>"
Fingerprint : ****
Package : centos-release-7-2.1511.el7.centos.2.10.x86_64 (@anaconda)
From : /etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
Is this ok [y/N]: y （必要なパッケージのインストールを許可する）
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
（中略）
Installed:
open-vm-tools.x86_64 0:10.1.5-3.el7
（中略）
Complete! （インストールの完了）
```

以上でインストールが完了します。

5.4. コンテンツライブラリの操作方法

vSphere Client を用いたコンテンツライブラリの管理操作をご説明いたします。

コンテンツライブラリでは、外部からの仮想マシンイメージ（OVA/OVFファイル）のインポートや、仮想マシンで使用するISOイメージの格納が行えます。

> **重要** **コンテンツアイテムによるデータストア容量の消費について**
>
> コンテンツライブラリに格納したアイテムは、コンテンツライブラリ作成時に指定する専用ストレージ上のデータストアに配置されます。
>
> アイテムの登録や、外部コンテンツライブラリ上のアイテム同期などの操作は専用ストレージのディスク容量を消費しますので、ご注意ください。

5.4.1. コンテンツライブラリ管理画面へのアクセス

vSphere Client を用いて、コンテンツライブラリの管理画面を表示する手順をご説明いたします。

1. **vSphere Client のメニューより、「コンテンツライブラリ」をクリックします。**

   「コンテンツライブラリ」の管理画面へ遷移します。

5.4.2. コンテンツライブラリの作成

新規コンテンツライブラリの作成手順をご説明いたします。

1. **「コンテンツライブラリ」の管理画面にて、右ペインのメニューから「作成」をクリックします。**

   「新しいコンテンツライブラリ」の作成ウィザードが表示されます。

2. **「名前と場所」の入力画面にて、新規コンテンツライブラリ名を入力後、作成する vCenter Server を選択し「Next」ボタンをクリックします。**

   「コンテンツライブラリの設定」画面が表示されます。

3. **ラジオボタンから「ローカルコンテンツライブラリ」を選択し、「Next」ボタンをクリックします。**

   「セキュリティポリシーの適用」画面が表示されます。

4. **必要に応じて設定項目を有効化し、「Next」ボタンをクリックします。**

   「ストレージの追加」画面が表示されます。

5. **ライブラリコンテンツの格納先となるデータストアを選択し、「Next」ボタンをクリックします。**

   「設定の確認」画面が表示されます。

6. **新規コンテンツライブラリの設定に誤りが無いことを確認し、「FINISH」ボタンをクリックします。**

   「ライブラリの作成」タスクが実行されます。タスクステータスが「完了」になることを確認します。

   また、「コンテンツライブラリ」管理画面のリストに、新規コンテンツライブラリが作成されたことを確認します。

5.4.3. アイテムのインポート

コンテンツライブラリへアイテムをインポートする手順をご説明いたします。

1. **「コンテンツライブラリ」管理画面にて、リストから操作する対象のコンテンツライブラリをクリックします。**

   選択したコンテンツライブラリの管理画面が表示されます。

2. **右ペインの「アクション」ボタンをクリックし、メニューから「アイテムのインポート」をクリックします。**

   「ライブラリアイテムのインポート」画面が表示されます。

3. **「ソース」欄にてインポートするファイルのロケーションを指定します。**
   直接URLを指定してダウンロードする場合は「URL」のラジオボタンを選択し、URLを入力します。
   ローカルファイルからアップロードする場合は、「ローカルファイル」のラジオボタンを選択し、「ファイルのアップロード」をクリックし、インポートするファイルを選択します。

4. **「ターゲット」欄にて「アイテム名」「注」をそれぞれ必要に応じて修正・入力し、「インポート」ボタンをクリックします。**

   「ライブラリアイテムへのファイルのアップロード」タスクが実行されます。タスクステータスが「完了」になることを確認します。

5. **左ペインのアイテムリストから、アップロードしたファイルに応じたグループを選択します。**

   左ペイン下部に選択したグループ内のアイテムリストが表示されます。
   アップロードしたアイテムがリスト内に表示されることを確認します。

5.4.4. アイテムの削除

コンテンツライブラリへインポートしたアイテムを削除する手順をご説明いたします。

1. **「コンテンツライブラリ」管理画面にて、削除対象のアイテムが登録されているコンテンツライブラリをクリックします。**

   選択したコンテンツライブラリの管理画面が表示されます。

2. **左ペインのアイテムリストから、削除対象のアイテムが登録されているグループを選択します。**

   左ペイン下部に選択したグループ内のアイテムリストが表示されます。
   削除するアイテムがリスト内に表示されることを確認します。

3. **左ペイン下部のアイテムリストから削除対象のアイテムを右クリックし、表示されたメニューから「削除」をクリックします。**

   「ライブラリアイテムの削除」画面が表示されます。

4. **「はい」ボタンをクリックします。**

   「ライブラリアイテムの削除」タスクが実行されます。タスクステータスが「完了」になることを確認します。
   また、左ペイン下部のアイテムリストから、削除したアイテムが表示されなくなったことを確認します。

5.4.5. OVF/OVAファイルからの仮想マシン作成

コンテンツライブラリへインポートされたOVF/OVAファイルから、仮想マシンを新規作成する手順をご説明いたします。

1. **「コンテンツライブラリ」管理画面のリストから、使用するOVF/OVAファイルがインポートされたコンテンツライブラリをクリックします。**

   選択したコンテンツライブラリの管理画面が表示されます。

2. **左ペインの「OVF&OVAテンプレート」をクリックします。**

   左ペイン下部にインポート済みのテンプレートがリスト表示されます。

3. **左ペイン下部のリストから、新規仮想マシンとしてインポートするテンプレートを右クリックし、メニューから「このテンプレートから仮想マシンを新規作成」をクリックします。**

   「コンテンツライブラリから仮想マシンを新規作成」ウィザードの画面が表示されます。

4. **「1.名前とフォルダの選択」にて、仮想マシン名を入力後、仮想マシンを作成するフォルダを選択し、「Next」ボタンをクリックします。**

   「2.コンピューティングリソースの選択」画面が表示されます。

5. **仮想マシンを作成するリソースプールを選択し、互換性チェックが成功したことを確認後、「Next」ボタンをクリックします。**

   「3.詳細の確認」画面が表示されます。

6. **インポートされるテンプレートの詳細設定に誤りが無いことを確認し、「Next」ボタンをクリックします。**

   「4.ストレージの選択」画面が表示されます。

7. **仮想マシンを作成するデータストアを選択し、互換性チェックが成功したことを確認後、「Next」ボタンをクリックします。**

   「5.ネットワークの選択」画面が表示されます。

8. **作成した仮想マシンが使用するネットワークを選択し、「Next」ボタンをクリックします。**

   「6.設定の確認」画面が表示されます。

9. **作成する仮想マシンの設定内容に間違いがないことを確認し、「FINISH」ボタンをクリックします。**

   「仮想マシンの作成」タスクが実行され、指定したリソースプール配下に仮想マシンが作成されます。

5.4.6. 仮想マシンのテンプレートインポート

仮想マシンのクローンをテンプレートとして、コンテンツライブラリに直接インポートすることができます。

仮想マシンテンプレートをコンテンツライブラリにインポートすることで、バージョンの管理を行うことが可能になります。

1. **vSphere Client の「三」ボタンより、「インベントリ」をクリックします。**
2. **インポート対象の仮想マシンを右クリックし、メニューから「クローン作成」>「テンプレートとしてライブラリにクローン作成」をクリックします。**

   「仮想マシンのクローンをテンプレート化」ウィザードの画面が表示されます。

3. 「テンプレートタイプ」にて仮想マシンテンプレートを選択し、「名前」、「注」、テンプレートの展開先フォルダを選択し、「NEXT」をクリックします。

「2. 場所」画面が表示されます

4. インポート先のライブラリを選択し、「NEXT」をクリックします。

「3. コンピューティングリソースの選択」画面が表示されます。

5. 任意のリソースを選択し、「NEXT」をクリックします。

「4. ストレージの選択」画面が表示されます。

6. 任意のストレージを選択し、「NEXT」をクリックします。

「5. 確認」画面が表示されます。

7. 設定に誤りがないことを確認し、「FINISH」をクリックします。

指定したリソース上に仮想マシンテンプレートが作成されます。

8. vSphere Client の「三」ボタンより「インベントリ」を開き、作成され仮想マシンテンプレートを選択します。

9. 右ペインの「バージョン管理」より、仮想マシンテンプレートのチェックアウト・チェックインが可能です。

補足

チェックアウト・チェックイン

コンテンツライブラリにインポートされた仮想マシンテンプレートは「チェックイン」「チェックアウト」の操作により、バージョン管理を行うことが可能になります。

仮想マシンテンプレートのバージョン管理についての詳細は、ヴイエムウェア社の公式ドキュメントをご参照ください。

参照 『仮想マシン テンプレートの管理 』

5.4.7. 外部コンテンツライブラリとの同期

本サービスの外部に作成された公開済みコンテンツライブラリとの同期手順をご説明いたします。

> ☑重要 **外部コンテンツライブラリとの同期の事前準備**
>
> 外部の公開済みコンテンツライブラリとの同期を行うには、下記設定が必要です。
>
> - vCenter Server での外部コンテンツライブラリURL名前解決設定の追加
> - NSX-T でのファイアウォール通信許可設定の追加
>
> 上記操作はお客さまでは実施いただけません。必要に応じて担当営業・SEへご依頼ください。

1. **公開設定された外部コンテンツライブラリの「サブスクリプションURL」および「パスワード」を確認します。パスワードは公開設定により設定されていない場合もあります。**

2. **「コンテンツライブラリ」画面にて、右ペインの「作成」ボタンをクリックします。**

   「新しいコンテンツライブラリ」画面が表示されます。

3. **「名前」、「メモ」を入力し、「NEXT」をクリックします。**

   「2. コンテンツライブラリの設定」画面が開きます。

4. **「サブスクライブ済みコンテンツライブラリ」を選択し、「サブスクリプションURL」に手順1にて確認したURLを入力します。パスワードが設定されたライブラリの場合には、「認証の有効化」にチェックを入れ、パスワードを入力します。公開ライブラリ内のコンテンツを全てダウンロードする場合は「今すぐ」を、必要なコンテンツのみを都度ダウンロードする場合は「必要に応じて」を選択し、「NEXT」をクリックします。**

   「信頼性を確認できません」という確認画面が表示されます。

5. **「はい」をクリックします。**

   「3. ストレージの追加」画面が表示されます。

6. **任意のストレージを選択し、「NEXT」をクリックします。**

   「4. 設定の確認」画面が表示されます。

7. **設定内容を確認し、「FINISH」をクリックします。**

8. **作成された外部ライブラリをクリックします。**

9. **外部ライブラリのダウンロード設定として「必要に応じて」を選択した場合は、必要なアイテムを選択し、右ペインの「アクション」から「アイテムの同期」をクリックします。**

   同期が完了すると、アイテムのファイルサイズが0Bから更新されます。

5.4.8. ISOイメージを使用したゲストOSインストール

コンテンツライブラリ内のISOイメージを使用して、仮想マシンへゲストOSをインストールする手順をご説明いたします。

1. **vSphere Client の「三」ボタンより、「インベントリ」をクリックします。**

   「インベントリ」画面へ遷移します。

2. **左ペインのツリーより、ゲストOSのインストールを行う新規仮想マシンを右クリックし、メニューから「設定の編集」をクリックします。**

   「設定の編集」画面が表示されます。

3. **「仮想ハードウェア」タブにて、ハードウェアリストから「CD/DVDドライブ1」を選択し、ドロップダウンリストから「コンテンツライブラリISOファイル」を選択します。**

   「マウントするISOイメージを選択」画面が表示されます。

4. **ISOイメージのリストから、ゲストOSのインストールに使用するイメージのラジオボタンをチェックし、「OK」ボタンをクリックします。**

   「設定の編集」画面が表示されます。

5. **「仮想ハードウェア」タブにて、ハードウェアリストから「CD/DVDドライブ1」を選択し、「ステータス」欄の「パワーオン時に接続」のチェックボックスにチェックを入れて「OK」ボタンをクリックします。**

   「仮想マシンの再設定」タスクが実行されます。タスクステータスが「完了」になることを確認します。

6. **左ペインのツリーより、ゲストOSのインストールを行う新規仮想マシンを右クリックし、メニューから「電源」>「パワーオン」をクリックします。**

   「仮想マシンのパワーオン」タスクが実行されます。タスクステータスが「完了」になることを確認します。

7. **左ペインのツリーより、ゲストOSのインストールを行う新規仮想マシンを右クリックし、メニューから「Remote Console を開く」をクリックします。**

   「VMware Remote Console」ウィンドウが表示されます。また、仮想マシンのメディアブート機能により、設定したISOイメージの読み込みが行われ、OSのインストーラが起動します。

8. **設定したOSのインストールウィザードに従い、OSのインストールを実施します。**

5.4.9. 仮想マシンへのISOイメージのマウント

コンテンツライブラリ内のISOイメージを、仮想マシンのCD/DVDドライブへマウントする手順をご説明いたします。

1. **vSphere Client の「三」ボタンより、「インベントリ」をクリックします。**

   「インベントリ」画面へ遷移します。

2. **左ペインのツリーより、ISOイメージのマウントを行う仮想マシンを右クリックし、メニューから「設定の編集」をクリックします。**

   「設定の編集」画面が表示されます。

3. **「仮想ハードウェア」タブにて、ハードウェアリストから「CD/DVDドライブ1」を選択し、ドロップダウンリストから「コンテンツライブラリISOファイル」を選択します。**

   「マウントするISOイメージを選択」画面が表示されます。

4. **コンテンツライブラリ内のISOイメージのリストから、使用するISOイメージのラジオボタンをチェックし、「OK」ボタンをクリックします。**

   「設定の編集」画面が表示されます。

5. **「仮想ハードウェア」タブにて、ハードウェアリストから「CD/DVDドライブ1」を選択し、「接続中」のチェックボックスにチェックを入れて「OK」ボタンをクリックします。**

   「仮想マシンの再設定」タスクが実行されます。タスクステータスが「完了」になることを確認します。

6. **対象の仮想マシンにログインし、CD/DVDドライブにISOイメージがマウントされていることを確認します。**

5.5. ライセンスオプションサービス利用手順

本項では、ライセンスオプションサービスをお申し込みいただいている場合の、仮想マシンやISOイメージの利用手順をご説明いたします。

ライセンスオプションサービスにより提供される仮想マシンテンプレートやISOイメージは、当社により提供されるコンテンツライブラリ「sb_library」に格納されます。

提供される仮想マシンテンプレート名やISOイメージ名については、『ホワイトクラウド ASPIRE プライベートクラウド サービス説明書』をご参照ください。

> **重要** ライセンスオプションサービスを利用した仮想マシンの利用には、ライセンス認証またはソフトウェアアップデートのためのインターネット接続が必要です。

5.5.1. Microsoft SPLA ライセンス を利用する際の Windows Server デプロイ

Microsoft SPLA ライセンスのお申し込みにより提供される Windows Server 仮想マシンのデプロイ手順をご説明いたします。

仮想マシンのカスタマイズ仕様の作成

仮想マシンテンプレートから Windows Server 仮想マシンを作成した場合、作成した仮想マシンの Windows Server OS にてセキュリティID(SID)を再生成する必要があります。

ここでは事前準備として、セキュリティIDを再生成するために使用する「仮想マシンのカスタマイズ仕様」の準備を行う手順をご説明いたします。

1. **vSphere Client の「三」ボタンより、「インベントリ」をクリックします。**

   「インベントリ」画面へ遷移します。

2. **左ペインのリストから「仮想マシンのカスタマイズ仕様」をクリックします。**

   「仮想マシンのカスタマイズ仕様」画面が表示されます。

3. メニューから「sb_windows_customize」を選択し、「複製」ボタンをクリックします。

カスタマイズ仕様の「複製」画面が表示されます。

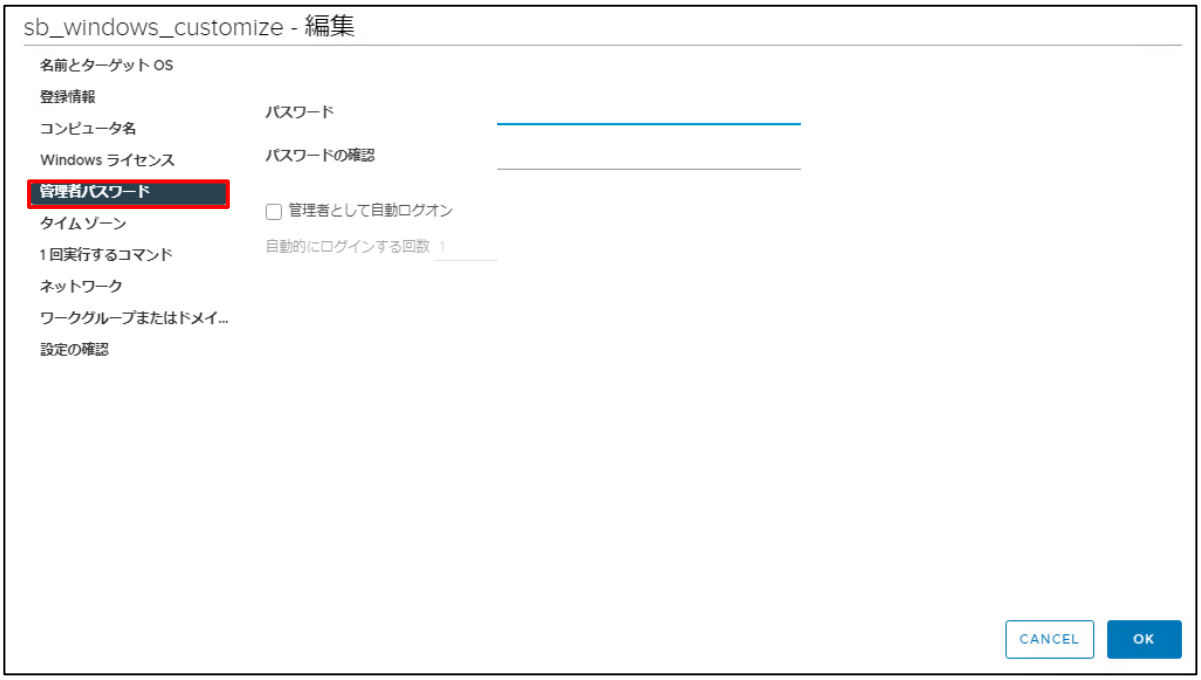
4. 「名前」欄に任意の名前を入力し、「OK」ボタンをクリックします。

「仮想マシンのカスタマイズ仕様」画面が表示されます。

5. メニューから複製したカスタマイズ仕様を選択し、「編集」ボタンをクリックします。

カスタマイズ仕様の「編集」ウィザードが表示されます。

6. 「編集」ウィザード左ペインのメニューから「管理者パスワード」を選択します。



パスワードの設定画面が表示されます。

7. パスワード設定画面にて、以下の項目を入力・選択します。

ここで入力するパスワードは、作成する仮想マシンの Windows Server 管理者ユーザ(Admninistrator) の初期パスワードとして使用されます。

項目	説明
パスワード	任意のパスワードを入力。
パスワードの確認	入力確認の為、上記のパスワードを再入力。
管理者としてログオン	作成した仮想マシンの起動後に管理者ユーザで自動ログインを行う場合はチェックボックスにチェックを入れます。
自動的にログインする回数	上記項目でチェックボックスにチェックを入れている場合、その回数の指定が可能です。

8. 「OK」ボタンをクリックします。

ウィザードが終了し、「仮想マシンのカスタマイズ仕様」画面に戻ります。

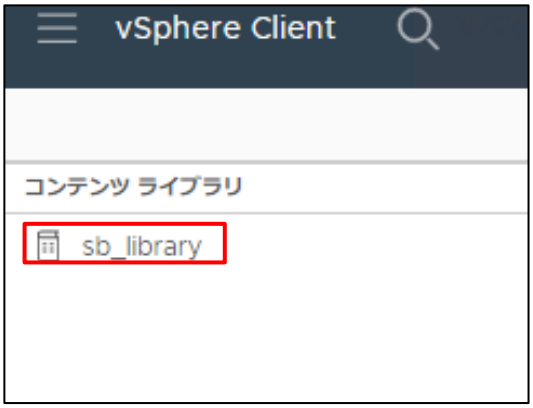
Windows Server 仮想マシンテンプレートを用いた新規仮想マシンの作成

当社より提供するコンテンツライブラリ上の Windows Server 仮想マシンテンプレートを用いて、新規仮想マシンを作成する手順をご説明いたします。

1. vSphere Client の「三」ボタンより、「コンテンツライブラリ」をクリックします。

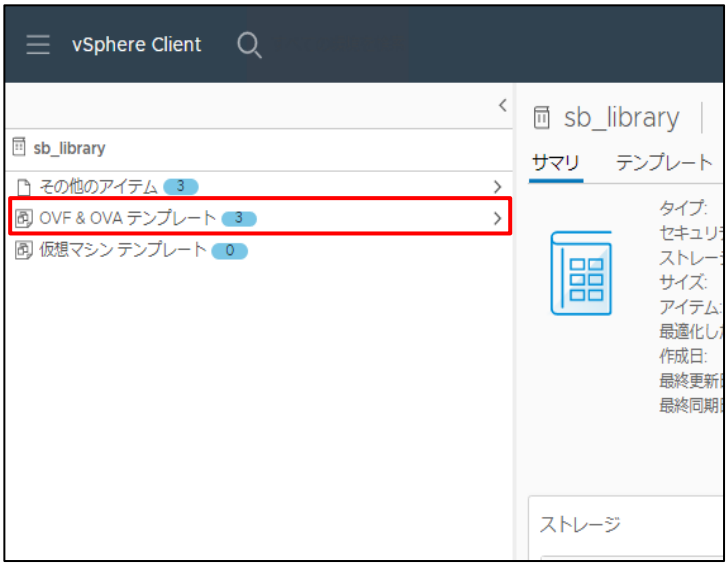
「コンテンツライブラリ」の管理画面へ遷移します。

2. 「コンテンツライブラリ」管理画面のリストから、「sb_library」をクリックします。



「sb_library」のアイテム管理画面が表示されます。

3. 左ペインの「OVF&OVAテンプレート」をクリックします。



左ペイン下部にインポート済みのテンプレートがリスト表示されます。

4. 左ペイン下部のリストから、新規仮想マシンとしてインポートする対象の Windows Server 仮想マシンテンプレートを右クリックし、メニューから「このテンプレートから仮想マシンを新規作成」をクリックします。

「コンテンツライブラリから仮想マシンを新規作成」ウィザードの画面が表示されます。

5. 「1.名前とフォルダの選択」にて、仮想マシン名を入力後、仮想マシンを作成するフォルダを選択し、「Next」ボタンをクリックします。

「2.コンピューティングリソースの選択」画面が表示されます。

6. 仮想マシンを作成するリソースプールを選択し、互換性チェックが成功したことを確認後、「Next」ボタンをクリックします。

「3.詳細の確認」画面が表示されます。

7. インポートされるテンプレートの詳細設定に誤りが無いことを確認し、「Next」ボタンをクリックします。

「4.ストレージの選択」画面が表示されます。

8. 仮想マシンを作成するデータストアを選択し、互換性チェックが成功したことを確認後、「Next」ボタンをクリックします。

「5.ネットワークの選択」画面が表示されます。

9. 作成した仮想マシンが使用するネットワークを選択し、「Next」ボタンをクリックします。

「6.設定の確認」画面が表示されます。

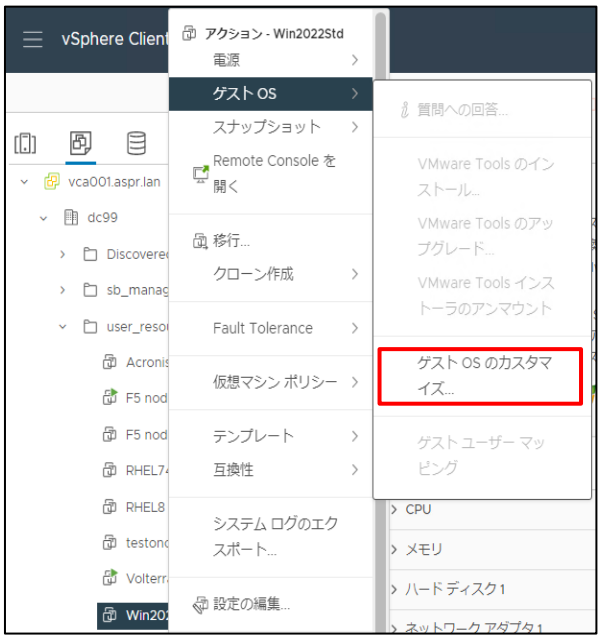
10. 作成する仮想マシンの設定内容に間違いがないことを確認し、「FINISH」ボタンをクリックします。

「OVFテンプレートのデプロイ」タスクが実行され、指定したリソースプール配下に仮想マシンが作成されます。

11. vSphere Client の「三」ボタンより、「インベントリ」をクリックします。

「インベントリ」画面へ遷移します。

12. 左ペインのツリーより、作成した仮想マシンを右クリックし、メニューから「ゲストOS」>「ゲストOSのカスタマイズ」をクリックします。



「ゲストOSのカスタマイズ」画面が表示されます。

13. リストから、前項で作成したカスタマイズ仕様を選択し、「OK」ボタンをクリックします。

「仮想マシンのゲストOSのカスタマイズ」タスクが実行されます。タスクステータスが「完了」になることを確認します。

14. 左ペインのツリーより、作成した仮想マシンを右クリックし、メニューから「電源」>「パワーオン」をクリックします。

「仮想マシンのパワーオン」タスクが実行されます。タスクステータスが「完了」になることを確認します。

仮想マシン上でゲストOSの再起動を含む初期化処理が実行されます。

初期化処理の内容

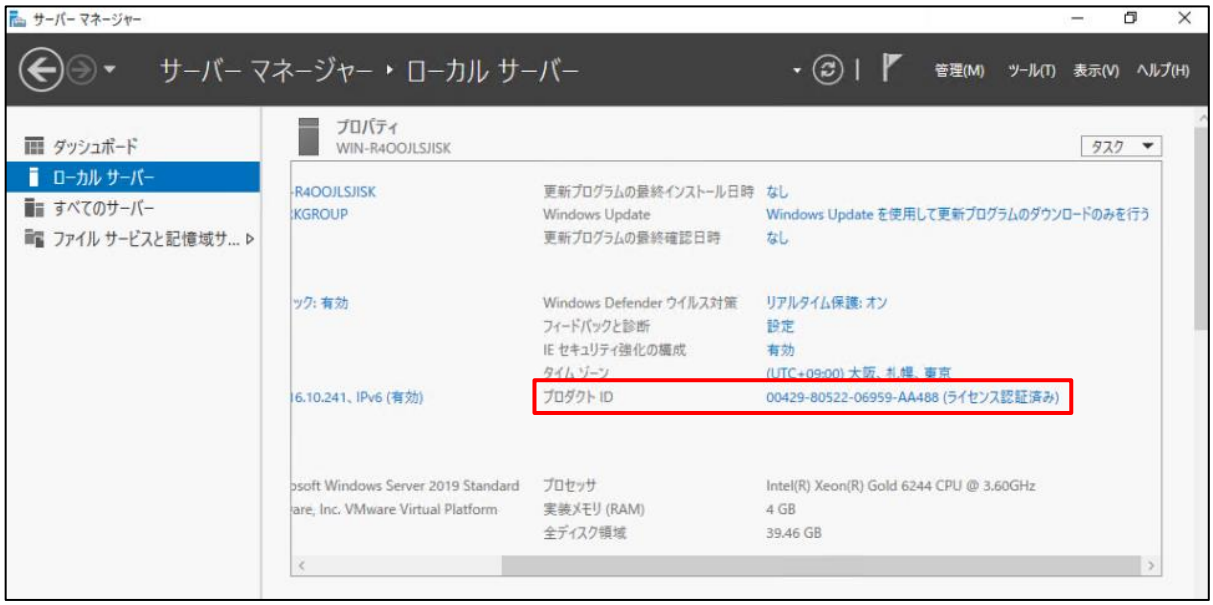
- Windows セキュリティID（SID）の再生成
- Aministratorアカウントの再生成、およびパスワード設定
- ネットワークアダプタの「未接続」化

15. 仮想マシンのコンソール接続を行い、カスタマイズ仕様にて設定した管理者アカウントのパスワードを用いてログインします。

16. ゲストOSがインターネット接続を行うためのネットワーク設定や、仮想マシンの「編集」よりネットワークアダプタの設定を行います。

インターネットへの接続後、自動的にライセンス認証が行われます。

17. ゲストOSの Windows Server にて「サーバーマネージャー」を起動し、「ローカルサーバー」のプロパティ画面からライセンス認証がされていることを確認します。



以後は通常の Windows Server 仮想マシンとしてご利用いただけます。

5.5.2. Microsoft SPLA ライセンス を利用する際の SQL Serverインストール

Microsoft SPLA ライセンスのお申し込みにより提供される Microsoft SQL Server のインストール手順をご説明いたします。

1. vSphere Client の「三」ボタンより、「インベントリ」をクリックします。

「インベントリ」画面へ遷移します。

2. 左ペインのツリーより、SQL Server のインストールを行う仮想マシンを右クリックし、メニューから「設定の編集」をクリックします。

「設定の編集」画面が表示されます。

3. 「仮想ハードウェア」タブにて、ハードウェアリストから「CD/DVDドライブ1」を選択し、ドロップダウンリストから「コンテンツライブラリISOファイル」を選択します。

「マウントするISOイメージを選択」画面が表示されます。

4. ISOイメージのリストから、コンテンツライブラリ「sb_library」に格納された対象バージョンの SQL Server ISOイメージのラジオボタンをチェックし、「OK」ボタンをクリックします。

「設定の編集」画面が表示されます。

5. **「仮想ハードウェア」タブにて、ハードウェアリストから「CD/DVDドライブ1」を選択し、「接続中」のチェックボックスにチェックを入れて「OK」ボタンをクリックします。**

   「仮想マシンの再設定」タスクが実行されます。タスクステータスが「完了」になることを確認します。

6. **対象の仮想マシンにログインし、CD/DVDドライブにマウントされている SQL Server インストールイメージを実行します。**

7. **SQL Server のインストールウィザードに従い、インストールを実施します。**

5.5.3. Remote Desktop Service ライセンスの適用について

Microsoft SPLA ライセンスのお申し込みにより提供される Remote Desktop Service ライセンスを利用する場合、当社オペレーターによるライセンス適用作業を実施する必要があります。

詳しくは、法人テクニカルサポートWebに掲載されている『【ホワイトクラウド ASPIRE】Remote Desktop Service_ライセンス導入手順書』をご参照ください。

5.5.4. Microsoft SPLA ライセンス を利用する際の Office インストール

Microsoft SPLA ライセンスのお申し込みにより提供される Microsoft Office を利用する場合は、当社オペレーターによるライセンス適用手順を実施する必要があります。

Microsoft Office のISOイメージマウント手順およびインストール・ライセンス適用の手順は、
それぞれ下記の項目、またはドキュメントをご参照ください。

参照 「5.4.9 仮想マシンへのISOイメージのマウント」

参照 『ホワイトクラウド ASPIRE サービスご利用ガイド』仮想マシンに Microsoft Office をインストールする

5.5.5. RHELサブスクリプションライセンスの利用

RHELサブスクリプションライセンスのお申し込みにより、コンテンツライブラリ上にRedHat Enterprise Linux 仮想マシンテンプレートが提供されます。

本項では、コンテンツライブラリ上の仮想マシンテンプレートを用いて、RHELサブスクリプションライセンスがアクティベートされた新規仮想マシンを作成する手順をご説明いたします。

重要

- Red Hat Enterprise Linux（以降RHEL）のライセンスオプションをお申し込みのお客さまのみ、テンプレートをご利用いただけます。
- アップデート提供サーバ（RHUIサーバ）へのアクセス（yumコマンドの使用）は、当社が提供するインターネット接続からのアクセスに限定しています。
- 東日本サイトのRHUIサーバ宛には、宛先IPアドレス（118.103.99.11）およびhttps（443/TCP）通信の許可が必要です。FQDNは「eastrhui.aspire.gcf.whitecloud.jp」です。
- 西日本サイトのRHUIサーバ宛には、宛先IPアドレス（221.110.171.251）およびhttps（443/TCP）通信の許可が必要です。FQDNは「westrhui.aspire.gcf.whitecloud.jp」です。
- 当社が提供するテンプレートより上位のバージョンを利用する場合は、お客さまがアップデートする必要があります。

  例）7.5 へアップデートする場合

  yum update redhat-release-server-7.5.8.el7 kernel-3.10.0-862.3.3.el7

  バージョンはお客さまにて事前に確認の上、適切なバージョンを指定してください。
- RHUIサーバは、RHELのライセンスオプションをご契約頂いたサーバ以外からのご利用は禁止事項となります。
- お客さま保有のRed Hatライセンス（RHELサブスクリプション）を、当社クラウド環境へのライセンス持込みについては、「Red Hat Cloud accessご利用の流れ」をご参照ください。
- RHUIサーバの提供パッケージは、RHEL6,RHEL7では「Base」、「Optional」、「RH Common」、「Extras」、「RHSCL」リポジトリの標準パッケージ、RHEL8では[BaseOS] [AppStream] [CodeReady Linux Builder] リポジトリの標準パッケージが対象となります。

  それ以外のパッケージ(「Debug」、「Source」など)は当社提供対象外となります。

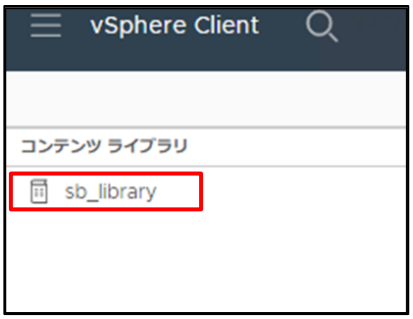
当社が提供するテンプレートは、以下の通りです。

テンプレート名	説明
RHEL68	Redhat Enterprise Linux 6.8
RHEL69	Redhat Enterprise Linux 6.9
RHEL72	Redhat Enterprise Linux 7.2
RHEL74	Redhat Enterprise Linux 7.4
RHEL84	Redhat Enterprise Linux 8.4

1. **vSphere Client の「三」ボタンより、「コンテンツライブラリ」をクリックします。**

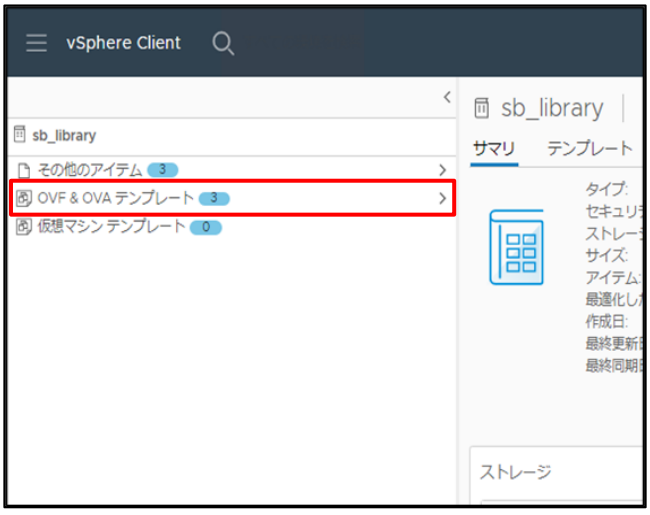
「コンテンツライブラリ」の管理画面へ遷移します。

2. **「コンテンツライブラリ」管理画面のリストから、「sb_library」をクリックします。**



「sb_library」のアイテム管理画面が表示されます。

3. **左ペインの「OVF&OVAテンプレート」をクリックします。**



左ペイン下部にインポート済みのテンプレートがリスト表示されます。

4. 左ペイン下部のリストから、新規仮想マシンとしてインポートする対象の RHEL仮想マシンテンプレートを右クリックし、メニューから「このテンプレートから仮想マシンを新規作成」をクリックします。

「コンテンツライブラリから仮想マシンを新規作成」ウィザードの画面が表示されます。

5. 「1.名前とフォルダの選択」にて、仮想マシン名を入力後、仮想マシンを作成するフォルダを選択し、「Next」ボタンをクリックします。

「2.コンピューティングリソースの選択」画面が表示されます。

6. 仮想マシンを作成するリソースプールを選択し、互換性チェックが成功したことを確認後、「Next」ボタンをクリックします。

「3.詳細の確認」画面が表示されます。

7. インポートされるテンプレートの詳細設定に誤りが無いことを確認し、「Next」ボタンをクリックします。

「4.ストレージの選択」画面が表示されます。

8. 仮想マシンを作成するデータストアを選択し、互換性チェックが成功したことを確認後、「Next」ボタンをクリックします。

「5.ネットワークの選択」画面が表示されます。

9. 作成した仮想マシンが使用するネットワークを選択し、「Next」ボタンをクリックします。

「6.設定の確認」画面が表示されます。

10. 作成する仮想マシンの設定内容に間違いがないことを確認し、「FINISH」ボタンをクリックします。

「OVFテンプレートのデプロイ」タスクが実行され、指定したリソースプール配下に仮想マシンが作成されます。

11. vSphere Client の「三」ボタンより、「インベントリ」をクリックします。

「インベントリ」画面へ遷移します。

12. 左ペインのツリーより、作成した仮想マシンを右クリックし、メニューから「電源」>「パワーオン」をクリックします。

「仮想マシンのパワーオン」タスクが実行されます。タスクステータスが「完了」になることを確認します。

仮想マシン上でゲストOSの起動処理が実行されます。

13. 仮想マシンのコンソール接続を行い、管理者ユーザにてログインします。

管理者ユーザ名・初期パスワードは『開通通知書』をご参照ください。

また、ご利用開始にあたっては、必ず管理者パスワードの変更を行ってください。

以後は通常の RedHat Enterprise Linux 仮想マシンとしてご利用いただけます。

5.6. vSphere Client のそのほかの操作

vSphere Clientから行うことのできる、そのほかの代表的な機能をご説明いたします。

5.6.1. 仮想マシンのクローン

クローンは既存の仮想マシンを複製し、別の仮想マシンを作成する機能です。

ここでは、仮想マシンのクローン作成の手順をご説明いたします。

1. **vSphere Client の「三」ボタンより、「インベントリ」をクリックします。**

   「インベントリ」画面へ遷移します。

2. **左ペインのツリーより、クローン元にする仮想マシンを右クリックし、メニューから「クローン作成」>「仮想マシンにクローン作成」をクリックします。**

   「既存の仮想マシンのクローン作成」画面が表示されます。

3. **「1.名前とフォルダの選択」にて、仮想マシン名を入力後、仮想マシンを作成するフォルダを選択し、「Next」ボタンをクリックします。**

   「2.コンピューティングリソースの選択」画面が表示されます。

4. **仮想マシンを作成するリソースプールを選択し、互換性チェックが成功したことを確認後、「Next」ボタンをクリックします。**

   「3.詳細の確認」画面が表示されます。

5. **仮想マシンを作成するデータストアを選択し、互換性チェックが成功したことを確認後、「Next」ボタンをクリックします。**

   「4.クローンオプションの選択」画面が表示されます。

6. **必要に応じて適用するクローンオプションのチェックボックスにチェックを入れ、「NEXT」ボタンをクリックします。**

   「5.設定の確認」画面が表示されます。

7. **作成する仮想マシンの設定内容に間違いがないことを確認し、「FINISH」ボタンをクリックします。**

   「仮想マシンのクローン作成」タスクが実行され、指定したフォルダ配下に仮想マシンが作成されます。

5.6.2. 仮想マシンテンプレートの利用

仮想マシンテンプレートは、仮想マシン作成時のクローン元として利用できるテンプレートフォーマットの仮想マシンです。

ここでは、テンプレート作成手順、およびテンプレートからの新規仮想マシン作成の手順をご説明いたします。

テンプレートの作成

既存の仮想マシンをテンプレートに変換する手順をご説明いたします。

1. **vSphere Client の「三」ボタンより、「インベントリ」をクリックします。**

   「インベントリ」画面へ遷移します。

2. **左ペインのツリーより、テンプレート化を行う仮想マシンを右クリックし、メニューから「テンプレート」>「テンプレートに変換」をクリックします。**

   「変換の確認」画面が表示されます。

3. **対象仮想マシン名に誤りが無いことを確認し、「はい」をクリックします。**

   「仮想マシンをテンプレートとしてマーク」タスクが実行されます。タスクステータスが「完了」になることを確認します。また、左ペインのツリー内で、対象仮想マシンがテンプレートに変換され、アイコンが変わったことを確認します。

テンプレートを利用した仮想マシンの作成

テンプレートから仮想マシンを作成する手順をご説明いたします。

1. **vSphere Client の「三」ボタンより、「インベントリ」をクリックします。**

   「インベントリ」画面へ遷移します。

2. **左ペインのツリーより、フォルダを右クリックし、メニューから「新規仮想マシン」をクリックします。**

   「新規仮想マシン」の作成ウィザード画面が表示されます。

3. **「1.作成タイプの選択」にて、仮想マシンの作成方法を指定します。**
   「テンプレートからのデプロイ」を選択し、「Next」ボタンをクリックします。

   「2.テンプレートの選択」画面が表示されます。

4. **「コンテンツライブラリ」または「データセンター」のタブを選択し、仮想マシン作成の元となるテンプレート選択し、「Next」ボタンをクリックします。**

   「3.名前とフォルダの選択」画面が表示されます。

5. **新規仮想マシン名を入力後、仮想マシンを作成するフォルダを選択し、「Next」ボタンをクリックします。**

   「4.コンピューティングリソースの選択」画面が表示されます。

6. **仮想マシンを作成するリソースプールを選択し、互換性チェックが成功したことを確認後、「Next」ボタンをクリックします。**

   「5.ストレージの選択」画面が表示されます。

7. **仮想マシンを作成するデータストアを選択し、互換性チェックが成功したことを確認後、「Next」ボタンをクリックします。**

   「6.クローンオプション」画面が表示されます。

8. **必要に応じて適用するクローンオプションにチェックを入れ、「NEXT」ボタンをクリックします。**

   「7.設定の確認」画面が表示されます。

9. **作成する仮想マシンの設定内容に間違いがないことを確認し、「FINISH」ボタンをクリックします。**

   「仮想マシンの作成」タスクが実行され、指定したリソースプール配下に仮想マシンが作成されます。

5.6.3. 仮想マシンスナップショットの利用

仮想マシンスナップショットとは、仮想マシン単位に静止点を作成し、必要に応じてその静止点まで仮想マシンの状態を切り戻す機能です。

ここでは、仮想マシンスナップショットの作成・復元手順をご説明いたします。

> **重要** **仮想マシンスナップショットの利用について**
>
> 仮想マシンスナップショットは一時利用にとどめておくことが推奨されています。
>
> 参照 『VMware KB：vSphere 環境でスナップショットを使用するベスト プラクティス』

スナップショットの作成

新規スナップショットの作成手順をご説明いたします。

1. **vSphere Client の「三」ボタンより、「インベントリ」をクリックします。**

   「インベントリ」画面へ遷移します。

2. **左ペインのツリーより、テンプレート化を行う仮想マシンを右クリックし、メニューから「スナップショット」>「スナップショットの作成」をクリックします。**

   「スナップショットの作成」画面が表示されます。

3. **作成するスナップショットの「名前」「説明」を入力します。**
   オプションのチェックボックスは、必要なものにチェックを入れ、「作成」ボタンをクリックします。

   「仮想マシンのスナップショットの作成」タスクが実行されます。タスクステータスが「完了」になることを確認します。

> **補足** **スナップショット作成時のオプションについて**
>
> スナップショット作成時のオプションは、対象の仮想マシンがパワーオン状態の場合のみ、使用することが可能です。
>
> - 「仮想マシンのメモリを含める」
>
>   チェックを入れると、動作中の仮想マシンのメモリデータを含めてスナップショットに取得することが可能です。このオプションを使用したスナップショットにデータを復元した場合、仮想マシンはパワーオン状態に復元されます。
>
>   このオプションを選択した場合、スナップショットの取得時間が増加する場合があります。
> - 「ゲストファイルシステムを静止する」
>
>   チェックを入れると、パワーオン状態の仮想マシン上で VMware Tools がファイルシステムを一時的に静止することで、仮想マシンのディスク上のデータを最適な状態にしてスナップショットを取得します。

作成したスナップショットへの復元

仮想マシンを、スナップショットを作成した時点へ復元する手順をご説明いたします。

1. vSphere Client の「三」ボタンより、「インベントリ」をクリックします。

「インベントリ」画面へ遷移します。

2. 左ペインのツリーより、スナップショットへの復元を行う仮想マシンを右クリックし、メニューから「スナップショット」>「スナップショットの管理」をクリックします。

右ペインに「スナップショットの管理」画面が表示されます。スナップショットツリーには、過去に作成したスナップショットが現在点までのツリー形式で表示されています。

3. スナップショットツリーから、使用するスナップショットを選択し、画面上部の「元に戻す」ボタンをクリックします。

「選択したスナップショットに戻す」画面が表示されます。

4. 使用するスナップショットに間違いがないことを確認し、「元に戻す」ボタンをクリックします。

「スナップショットに戻す」タスクが実行されます。タスクステータスが「完了」になることを確認します。

スナップショットの削除

過去に作成したスナップショットを削除する手順をご説明いたします。

1. vSphere Client の「三」ボタンより、「インベントリ」をクリックします。

「インベントリ」画面へ遷移します。

2. 左ペインのツリーより、スナップショットへの復元を行う仮想マシンを右クリックし、メニューから「スナップショット」>「スナップショットの管理」をクリックします。

右ペインに「スナップショットの管理」画面が表示されます。

スナップショットツリーには、過去に作成したスナップショットが現在点までのツリー形式で表示されています。

3. スナップショットツリーから、削除するスナップショットを選択し、画面上部の「削除」ボタンをクリックします。

「スナップショットの削除」画面が表示されます。

4. 削除するスナップショットに間違いがないことを確認し、「削除」ボタンをクリックします。

「スナップショットの削除」タスクが実行されます。タスクステータスが「完了」になることを確認します。
また、スナップショットツリー上から、対象のスナップショットが削除されたことを確認します。

5.6.4. リソースプールの操作

リソースプールは、クラスタ内の全てのリソースを区分化し、管理するために使用します。
ここでは、仮想マシンを管理するためのリソースプールの操作方法をご説明いたします。

リソースプールの作成

新規リソースプールを作成する手順をご説明いたします。

1. vSphere Client の「三」ボタンより、「インベントリ」をクリックします。

「インベントリ」画面へ遷移します。

2. 左ペインのツリーより、リソースプールの親オブジェクト（クラスタ、または別のリソースプール）を右クリックし、メニューから「新規リソースプール」をクリックします。

「新規リソースプール」画面が表示されます。

3. 作成するリソースプールの「名前」を入力し、「CPU」「メモリ」の各項目に、リソースプールに割り当てるコンピューティングリソースの割り当て方法を入力し、「OK」ボタンをクリックします。
オプションのチェックボックスは、必要なものにチェックを入れ、「作成」ボタンをクリックします。

「リソースプールの作成」タスクが実行されます。タスクステータスが「完了」になることを確認します。
また、左ペインのオブジェクトツリーに、作成したリソースプールが追加されたことを確認します。

項目	説明
シェア	親オブジェクトの合計リソースに対する、このリソースプールのシェア値を指定します。これにより、兄弟のリソースプールと予約と制限の範囲内で相対的なシェア値に従ってリソースを共有します。
予約	リソースプールで確保する CPU またはメモリの割り当て量を指定します。デフォルトは「0」(予約なし)となります。 「0」以外を指定した場合、親オブジェクトの未予約のリソースから差し引かれます。予約したリソースは、仮想マシンの使用に関係なく、予約済みとみなされます。
拡張可能な予約	有効な場合、このリソースプール内の仮想マシンの予約の合計がリソースプールの予約値よりも大きくなった場合に、リソースプールは親オブジェクトのリソースを予約値を越えて使用することが可能です。

制限	リソースプールに割り当てる CPU またはメモリの上限値を設定します。

リソースプールの編集と管理

作成済みリソースプールの編集手順をご説明いたします。

1. **vSphere Client の「三」ボタンより、「インベントリ」をクリックします。**
   「インベントリ」画面へ遷移します。

2. **左ペインのツリーより、編集を行うリソースプールを右クリックし、メニューから「リソース設定の編集」をクリックします。**
   「リソース設定の編集」画面が表示されます。

3. **「CPU」「メモリ」の各項目の入力値を変更し、「OK」ボタンをクリックします。**
   「リソースプール構成の更新」タスクが実行されます。タスクステータスが「完了」になることを確認します。

5.6.5. フォルダの操作

フォルダは、仮想マシンをグループ化することで、管理を容易にするために使用します。

フォルダの作成

新規フォルダを作成する手順をご説明いたします。

1. **vSphere Client の「三」ボタンより、「インベントリ」をクリックします。**
   「インベントリ」画面へ遷移します。

2. **「仮想マシンおよびテンプレート」のツリーより、データセンターオブジェクト「dc01」を右クリックし、メニューから「新規フォルダ」>「新規仮想マシンおよびテンプレートフォルダ」をクリックします。**
   「新規フォルダ」画面が表示されます。

3. **作成するフォルダの「名前」を入力し、「OK」ボタンをクリックします。**
   「フォルダの作成」タスクが実行されます。タスクステータスが「完了」になることを確認します。
   また、左ペインのオブジェクトツリーに、作成したフォルダが追加されたことを確認します。

フォルダの管理

フォルダには編集すべきパラメータはありません。フォルダを移動してほかのフォルダの配下へ配置することや、ほかのオブジェクトをフォルダ内に収容することが可能です。

フォルダの移動は、対象フォルダを右クリックし、メニューから「移動先」をクリックして行います。

仮想マシンのフォルダへの移動は、対象仮想マシンを右クリックし、メニューから「フォルダに移動」をクリックして行います。

また、仮想マシンツリー上でのドラッグ＆ドロップにより同じ操作を行うことも可能です。

5.6.6. リソース利用状況の把握

本サービスで提供する基盤や仮想マシンのコンピューティングリソース利用状況の確認手順をご説明いたします。

仮想マシンのリソース利用状況の確認

個々の仮想マシンに割り当てられたリソースについて、利用状況の確認手順をご説明いたします。

1. **vSphere Client の「三」ボタンより、「インベントリ」をクリックします。**

   「インベントリ」画面へ遷移します。

2. **左ペインのツリーより、リソース利用状況を確認する仮想マシンをクリックします。**

   右ペインに、選択した仮想マシンのサマリ画面が表示されます。

3. **右ペインのメニュータブより、「監視」をクリックします。**

   右ペインに、「監視」タブのメニューが表示されます。

4. **「使用率」をクリックします。**

   右ペインに、選択した仮想マシンのリソース使用率を表示する画面が表示されます。

クラスタとESXiホストのリソース利用状況の把握

クラスタ全体と、個々のESXiホストのコンピューティングリソースの利用状況の確認手順をご説明いたします。

1. vSphere Client の「三」ボタンより、「インベントリ」をクリックします。

「インベントリ」画面へ遷移します。

2. 左ペインのツリーより、クラスタオブジェクト「cluster01」をクリックします。

右ペインに、選択したクラスタのサマリ画面が表示されます。

3. 右ペインのメニュータブより、「監視」をクリックします。

右ペインに、「監視」タブのメニューが表示されます。

4. 「使用率」をクリックします。

右ペインに、クラスタ全体のリソース使用率を表示する画面が表示されます。

5. 右ペインのメニュータブより、「ホスト」をクリックします。

ESXiホストが一覧表示され、各ホストのCPU使用率・メモリ使用率も表示されます。

パフォーマンスグラフの参照

vSphere Client では、仮想マシンやホスト・クラスタの利用状況についてのパフォーマンスグラフを参照することが可能です。

ここでは、仮想マシンのパフォーマンスグラフを参照する手順をご説明いたします。

1. vSphere Client の「三」ボタンより、「インベントリ」をクリックします。

「インベントリ」のツリー表示画面へ遷移します。

2. 左ペインのツリーより、パフォーマンスグラフを参照する仮想マシンをクリックします。

右ペインに、選択した仮想マシンのサマリ画面が表示されます。

3. 右ペインのメニュータブより、「監視」をクリックします。

右ペインに、「監視」タブのメニューが表示されます。

4. **「パフォーマンス」配下の「概要」をクリックします。**

   右ペインに、選択した仮想マシンのパフォーマンス概要のサマリとグラフ表示されます。

   「期間」欄のドロップダウンリストを選択することで、表示する期間を変更することが可能です。

   また、「表示」欄のドロップダウンリストを選択することで、表示する対象のリソースを変更することが可能です。

5. **「パフォーマンス」配下の「詳細」をクリックします。**

   右ペインに、選択した仮想マシンの詳細なパフォーマンスチャートが表示されます。

   「期間」欄のドロップダウンリストを選択することで、表示する期間を変更することが可能です。

   また、「表示」欄のドロップダウンリストを選択することで、表示する対象のリソースを変更することが可能です。

5.6.7. タグの操作

タグおよび属性を使用すると、vSphere インベントリ内のオブジェクトにメタデータを添付して、オブジェクトの並べ替えや検索を行うことが可能になります。

vSphere Client を用いてタグを操作する手順は、ヴイエムウェア社の公式ドキュメントをご参照ください。

参照 『vSphere のタグおよび属性』

5.6.8. そのほかの操作

VMware vCenter Server のそのほかの機能については、ヴイエムウェア社の公式ドキュメントをご参照ください。

参照 『vSphere 仮想マシン管理について』

6. VMware NSX-T DataCenter の操作

本章ではテナント内の仮想ネットワークを設定するためのNSX-Tの操作についてご説明いたします。

本書に含まれない内容については、ヴイエムウェア社の公式ドキュメントをご参照ください。

参照 『NSX-T Data Center 管理ガイド』

本サービスの VMware NSX-T DataCenter では、以下の機能を利用いただけます。

項目	説明
Tier-1 ゲートウェイ	**Tier-1 ゲートウェイの作成、削除、編集** 新規 Tier-1 ゲートウェイの作成・削除・編集操作を行うことが可能です。作成した Tier-1 ゲートウェイは Overlay Network の作成、NAT、VPN などの各種設定で利用することができます。
セグメント	**Overlay Network の作成、削除、編集** 新規 Overlay Network の作成・削除・編集操作を行うことが可能です。作成した Overlay Network に仮想マシンを接続することで、外部との通信が可能になります。 **セグメントプロファイルの作成、削除、編集** 作成した Overlay Network で利用する QoS 設定などの定義を行うことが可能です。
VPN	**IPsec VPN の設定** ポリシーベースの IPsec VPN の設定を行うことが可能です。
NAT	**NAT の設定** DNAT(Destination NAT) / SNAT(Source NAT)の設定を行うことが可能です。
DNS	**DNS の設定** DNS フォワーダーの設定を行うことが可能です
DHCP	**DHCP の設定** 作成した Overlay Network で利用する DHCP サーバの設定を行うことが可能です
ネットワーク プロファイル	**ゲートウェイ QOS プロファイルの作成、削除、編集** Tier-1 ゲートウェイのトラフィックを制御するためのネットワークプロファイルの定義を行うことが可能です。
分散ファイアウォール	**分散ファイアウォールの設定** 分散ファイアウォールを使用し、仮想マシン単位にトラフィックの制限をかけることが可能です。
ゲートウェイ ファイアウォール	**ゲートウェイ ファイアウォールの設定** ゲートウェイ ファイアウォールを使用し、Tier-1 ゲートウェイを通るトラフィックの制限をかけることができます。

項目	説明
セキュリティ プロファイル	**セキュリティプロファイルの作成、削除、編集** ファイアウォールの動作を調整する、セキュリティプロファイルの定義を行うことが可能です。
インベントリ	**インベントリの作成、削除、編集** 各種設定で利用するサービス定義や、宛先や送信元として使用するグループの設定を行うことが可能です
ロードバランサ (オプション)	**ロードバランサの作成、削除、編集** ロードバランサ機能を設定することができます。 本機能はオプションサービスとなります。

補足

本サービスにおけるNSX-Tコンポーネントサイズは以下の通りです。

標準

NSX Manager：Medium

NSX Edge：Large (2台でEdge Clusterを構成)

管理パッケージが2つ以上の場合

NSX Manager：Large

NSX Edge：Large (2台でEdge Clusterを構成)

構成の上限を確認する場合は上記構成に合わせてご確認ください。

参照 「各製品の構成の上限について」

6.1. NSX Manager の利用について

NSX Managerでは、プライベートクラウド環境の仮想ネットワークやNAT、VPN、FWなどのサービスの構成・管理を行えます

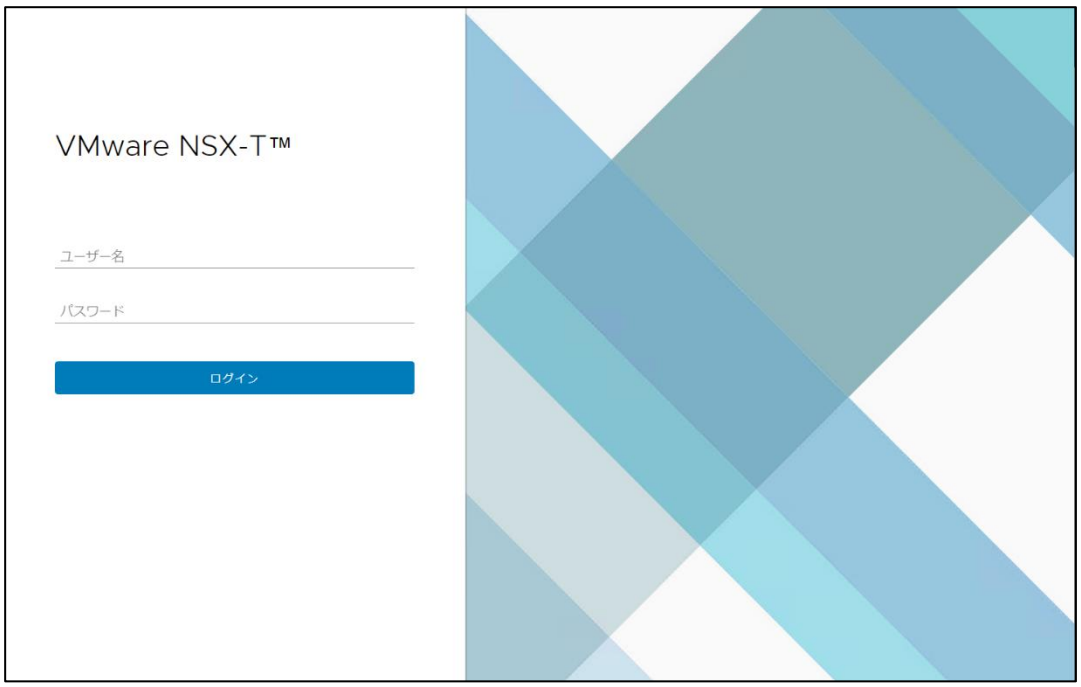
6.1.1. NSX Manager へのログイン

NSX Managerの管理画面にログインします。

1. **NSX Managerの管理画面のURLにアクセスします。**

   https://nsx001.aspr.lan/login.jsp

   NSX Managerのログイン画面が表示されます

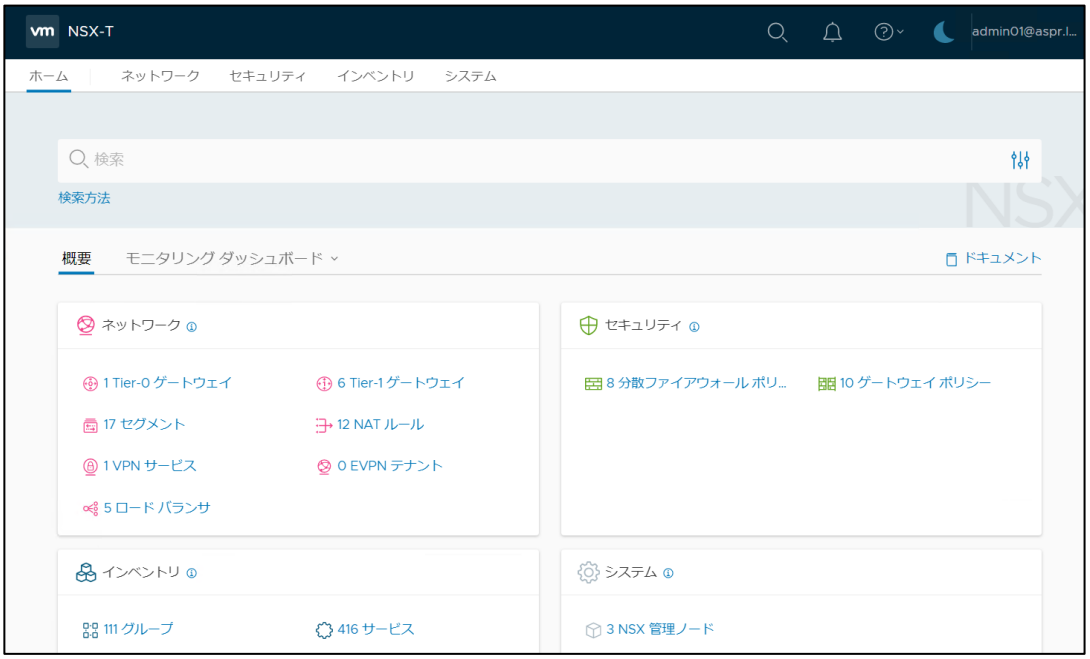


補足 ログインに5回連続して失敗すると、アカウントは15分間ロックされます。

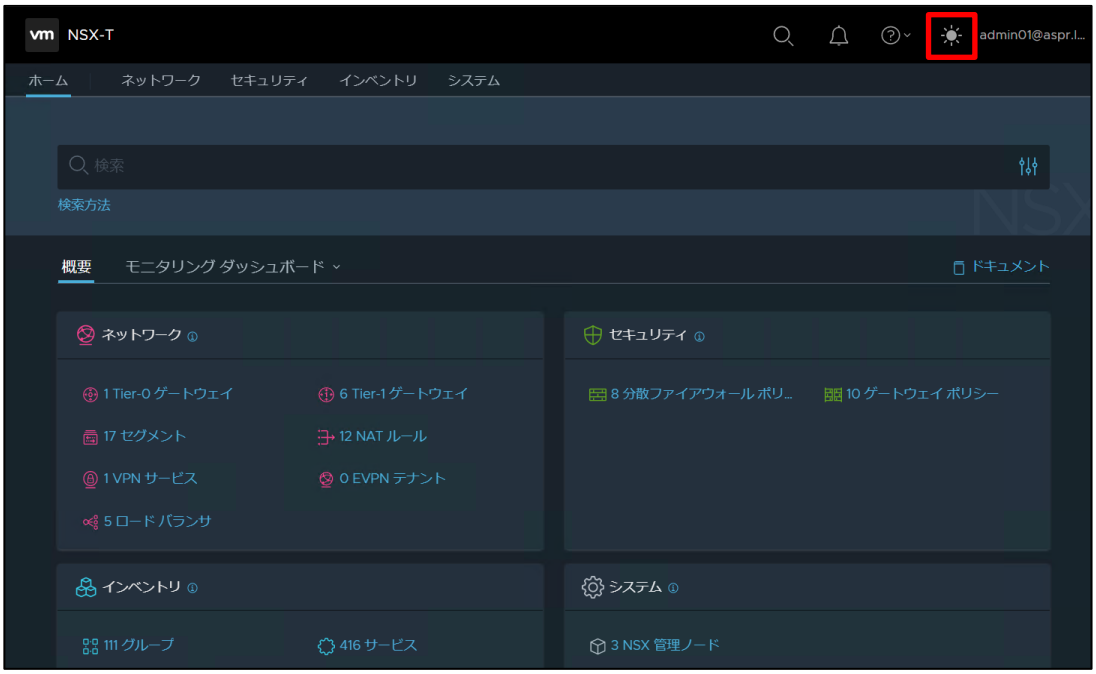
2. ユーザ名とパスワードを入力し、「ログイン」ボタンをクリックします。

項目	説明
ユーザ名	『開通通知書』に記載されているユーザ名を入力します。
パスワード	上記ユーザ名に設定されたパスワードを入力します。

ログインが完了し、以下の画面が表示されます。



画面右上のアイコンをクリックすることで ダーク モードとライト モードを切り替えることが可能です。

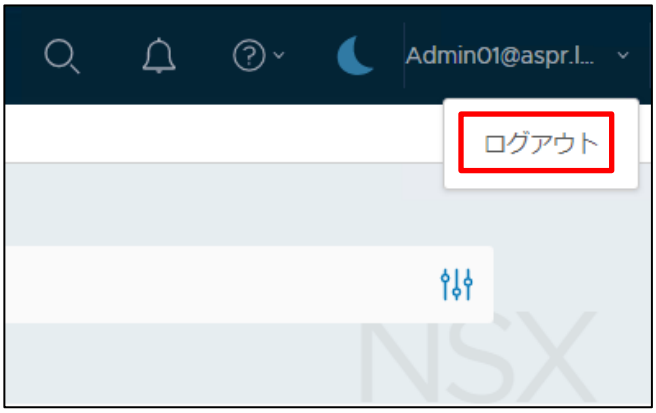


補足 本書掲載の画像はライト モードで説明しています。

6.1.2. NSX Manager からのログアウト

NSX Managerの管理画面からログアウトします。

1. **管理画面の右上のアカウントをクリックし、「ログアウト」をクリックします。**



ログアウトが完了し、ログイン画面が表示されます。

6.2. NSX Managerの基本操作

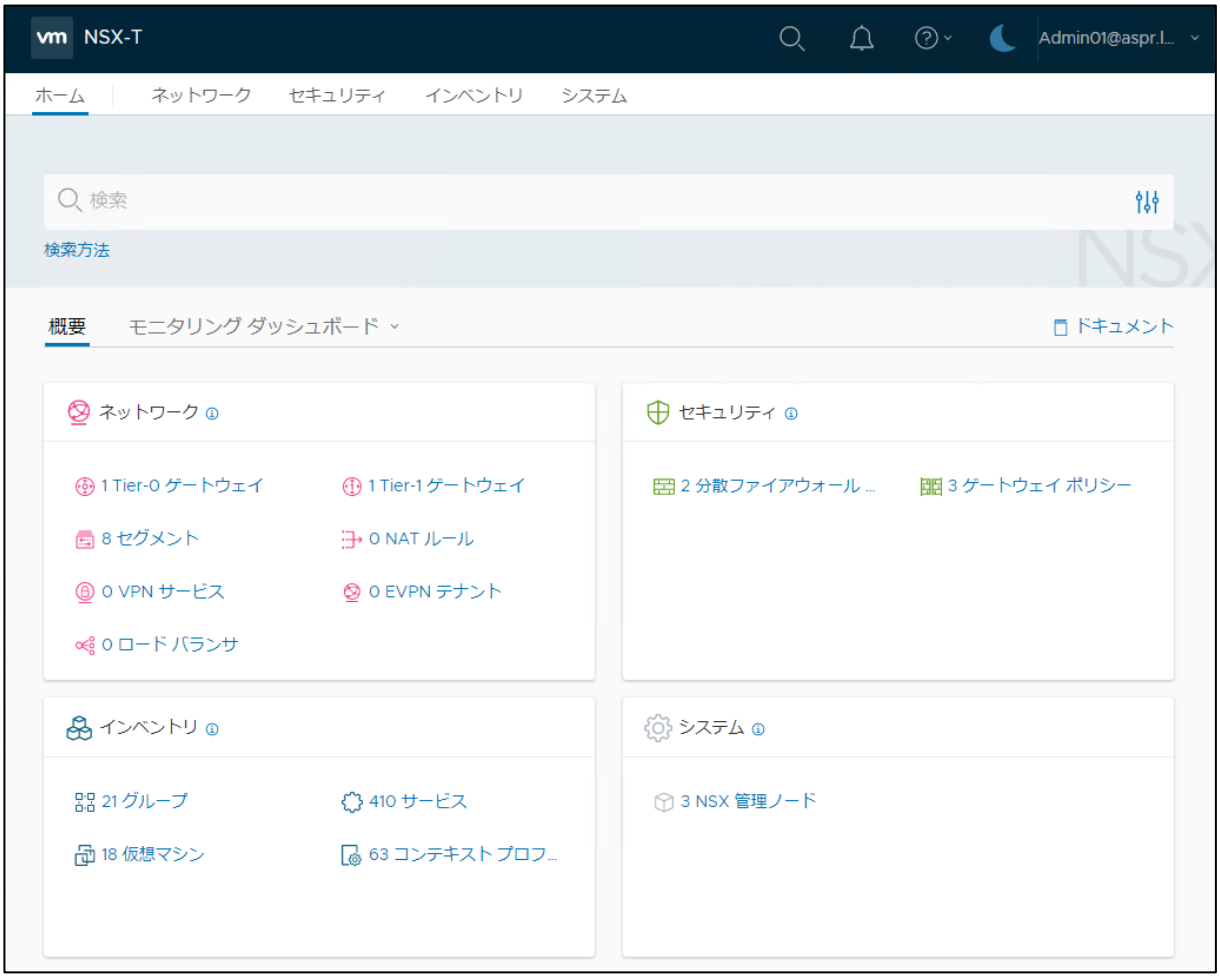
NSX ManagerはNSX環境の管理に利用します。

本項ではNSX Manager管理画面の基本的な操作についてご説明いたします。

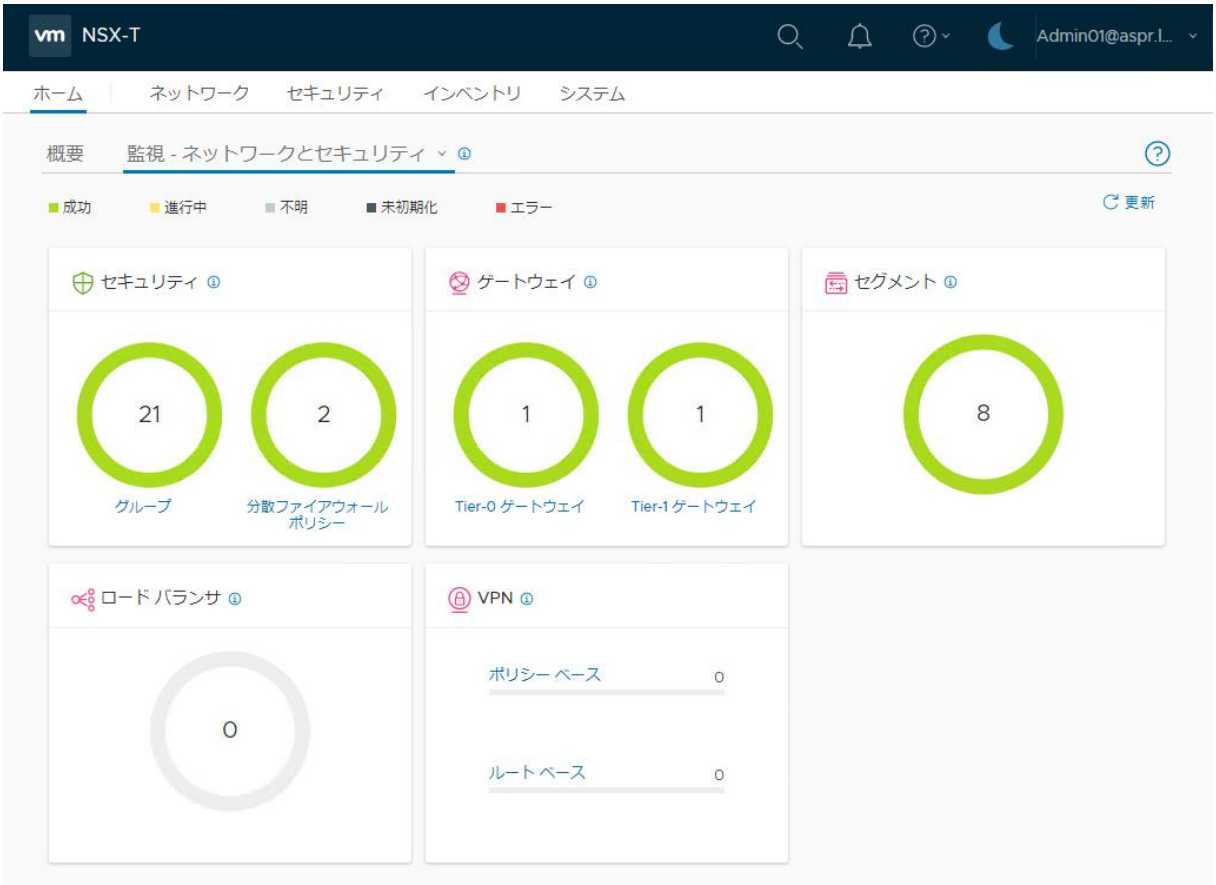
6.2.1. ホーム画面

NSX Managerにログインするとホーム画面が表示されます。

ホーム画面ではNSX環境の設定の概要のほか、モニタリング ダッシュボードから各コンポーネントのステータスのサマリが確認できます。



ネットワークとセキュリティ画面からはVPNやゲートウェイなどのステータスが確認できます。



補足 カスタム ダッシュボードは、お客さまの権限では作成することはできません。

6.2.2. 設定概要画面について

各設定カテゴリの概要からは、そのカテゴリの各種設定状況のサマリが確認できます。

例えば「ネットワーク」の「ネットワークの概要」からはTier-1ゲートウェイやNATなどのネットワーク設定に関わる設定数などの情報が参照できます。

6.2.3. 編集操作について

NSX Managerでの編集操作についてご説明いたします。

NSX Managerでのオブジェクトの編集操作は、編集対象横の「：」をクリックし「編集」を選択し実施します。

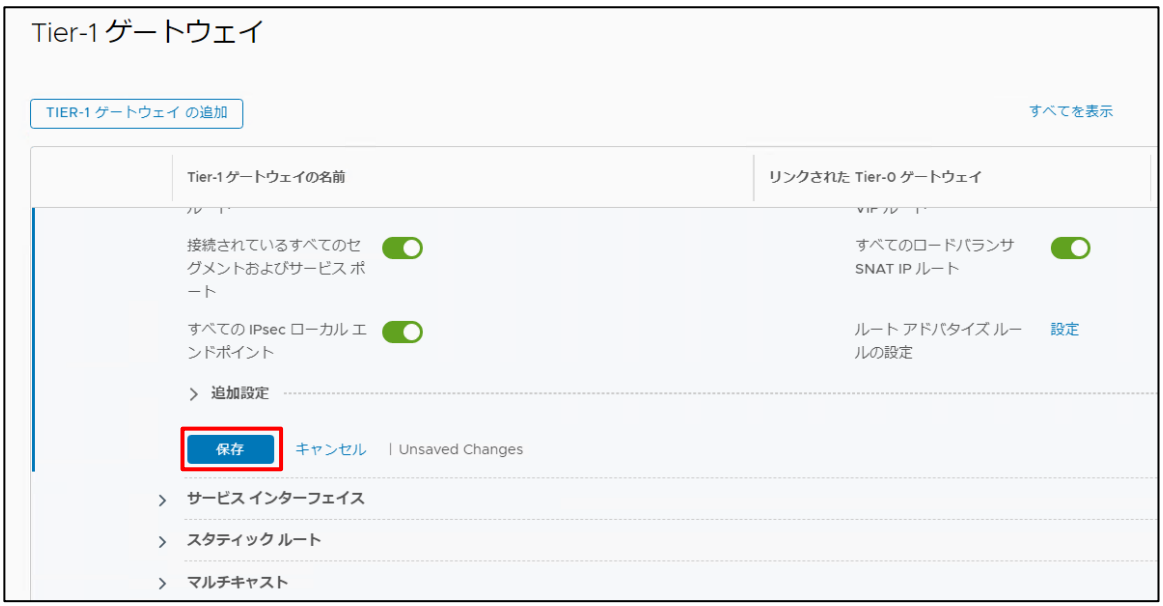
> **補足** システムにより作成されたデフォルトプロファイルなどは「編集」を行うことが出来ません。
> デフォルトプロファイルから値を変更する場合は、別途プロファイルを作成し、適用してください。

以下はTier-1 ゲートウェイの編集操作の例となります。

1. **編集を実施するTier-1 ゲートウェイ横の「：」をクリックし「編集」をクリックします。**

Tier-1ゲートウェイの設定編集画面が開きます。

2. **設定の編集を実施後「保存」をクリックします。**



編集内容が保存されます。

3. 「編集を終了」をクリックします。

編集画面が終了します。

6.2.4. 削除操作について

NSX Managerでの削除操作についてご説明いたします。

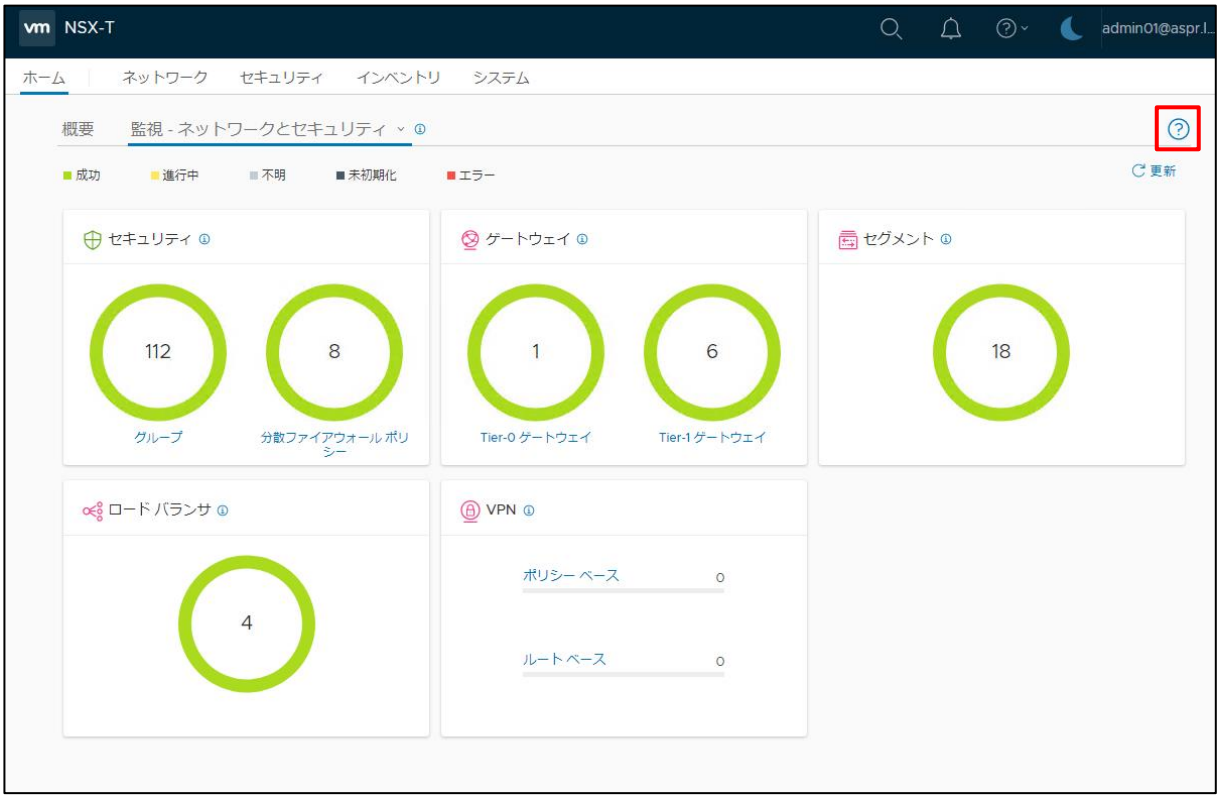
NSX Managerでのオブジェクトの削除を行う際は対象のオブジェクトが利用されていないように設定を解除する必要があります。例えば、セグメント プロファイルの削除を行う場合、対象のプロファイルがセグメントに適用されている状態で削除を行おうとするとエラーが表示され、削除を行うことができません。

> **補足** デフォルトで存在するプロファイルなどにつきましては「削除」を行うことが出来ません。

実際の削除操作につきましては各項目の削除手順をご参照ください。

6.2.5. 各機能のヘルプの参照について

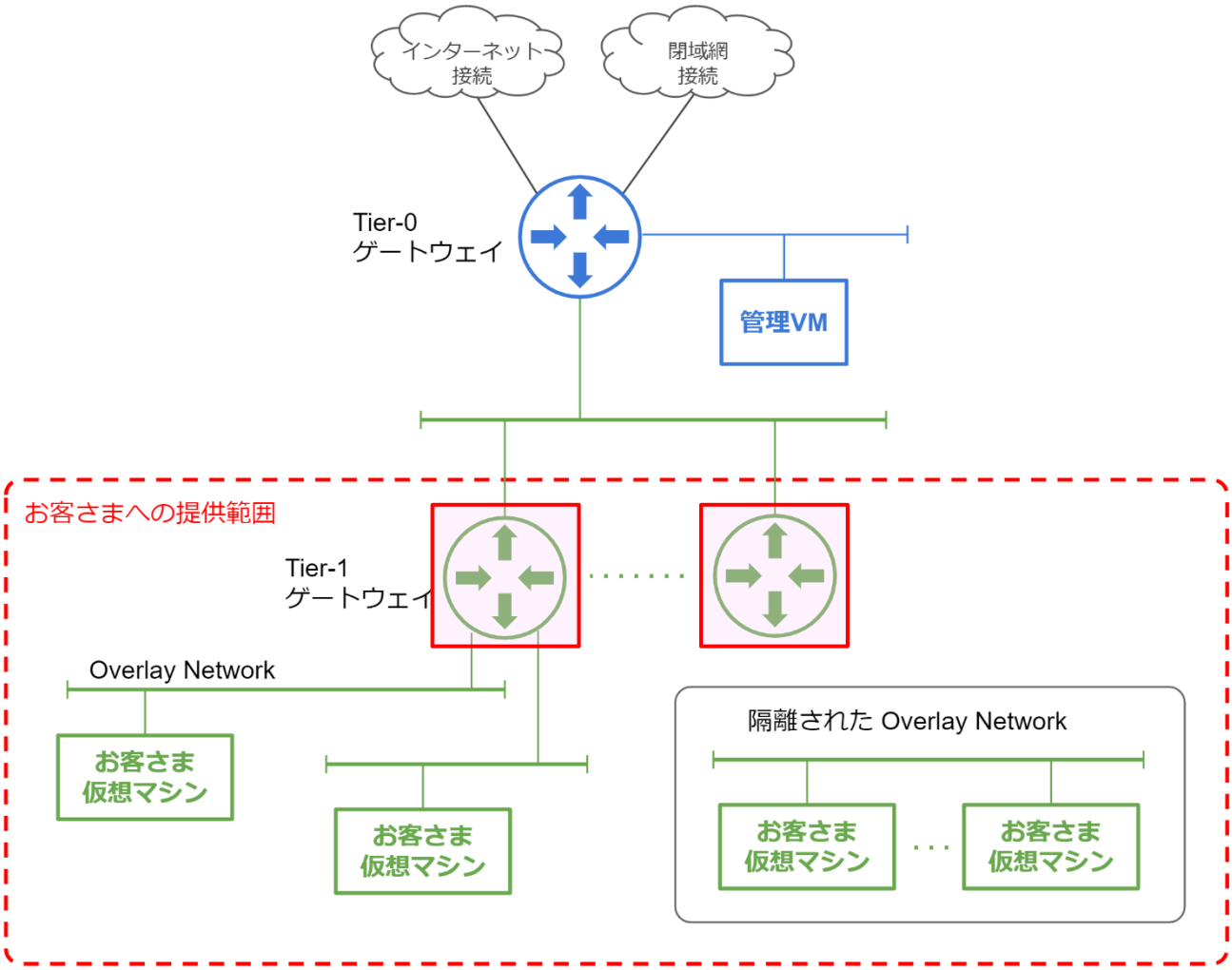
NSX-T Manager の各操作画面にはヘルプを参照するためのリンクボタンが配置されています。
機能の詳細な説明や設定方法を確認したい場合は、画面右上の「？」ボタンをクリックしてください。



6.3. Tier-1 ゲートウェイの操作

Tier-1ゲートウェイは外部ネットワークに抜けるTier-0ゲートウェイと、VMが接続されるOverlay Network に接続されます。

NATやVPNを構成する際は、Tier-1 ゲートウェイに対して構成します。



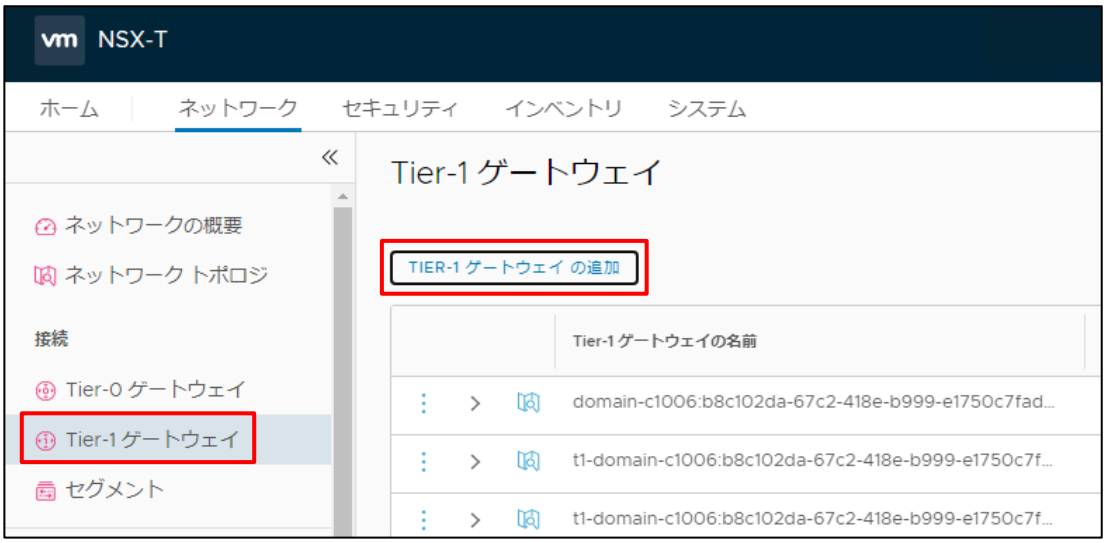
6.3.1. Tier-1 ゲートウェイの作成

ここでは設定例として、本サービスの仮想マシンを外部と接続するためのTier-1 ゲートウェイの作成手順をご説明いたします。

1. **NSX Managerにログインします。**

2. **「ネットワーク」をクリックします。**

3. **「Tier-1 ゲートウェイ」をクリックし「TIER-1 ゲートウェイの追加」をクリックします。**



Tier-1 ゲートウェイの作成画面が表示されます。

4. 各入力項目に必要なパラメータを入力します。

項目	設定値
Tier-1 ゲートウェイの名前	任意の名前を入力
リンクされた Tier-0 ゲートウェイ	sb_tier-0_gateway ※1
Edge クラスタ	sb_edgecluster01
Edge プールの割り当てサイズ	ルーティング※2
スタンバイの再配置を有効にする	有効
ルートアドバタイズ	すべて有効※3

※1：外部と接続を行う際に指定してください。外部との接続が不要な場合は指定の必要はありません

※2：オプションのNSX ロードバランサを使用する際は、作成するLBサイズを選択してください

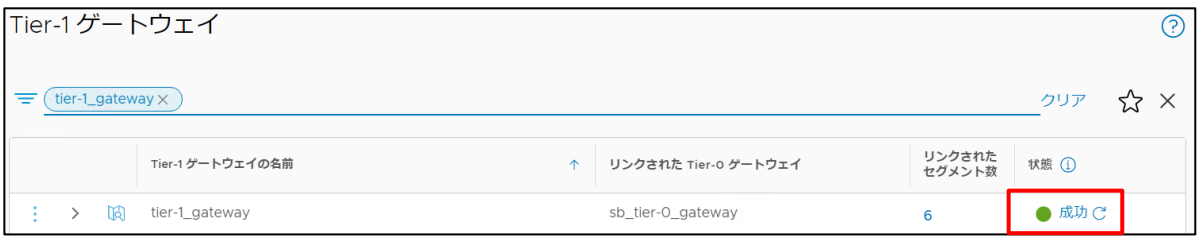
※3：接続するネットワークが外部への通信を行わない場合は無効にしてください

5. 「保存」をクリックします。

Tier-1 ゲートウェイが作成されます。

6. 「いいえ」をクリックします。

7. 作成したTier-1ゲートウェイの状態が「成功」になることを確認します。



6.3.2. Tier-1 ゲートウェイの削除

Tier-1 ゲートウェイの削除手順をご説明いたします。

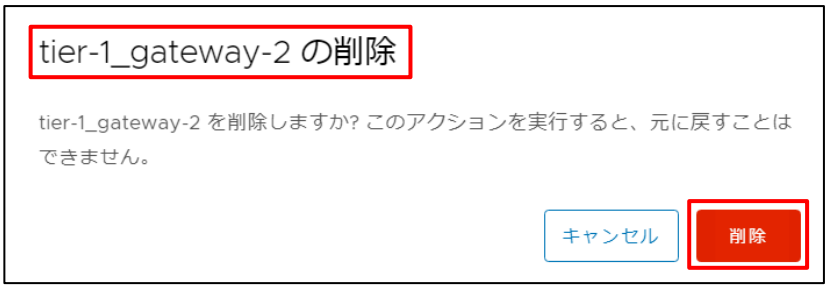
1. **NSX Managerにログインします。**

2. **「ネットワーク」から「Tier-1 ゲートウェイ」をクリックします。**

3. **削除対象のTier-1 ゲートウェイ横の「⋮」をクリックし「削除」をクリックします。**

確認画面が開きます。

4. **確認画面で対象に間違いが無いことを確認し「削除」をクリックします。**



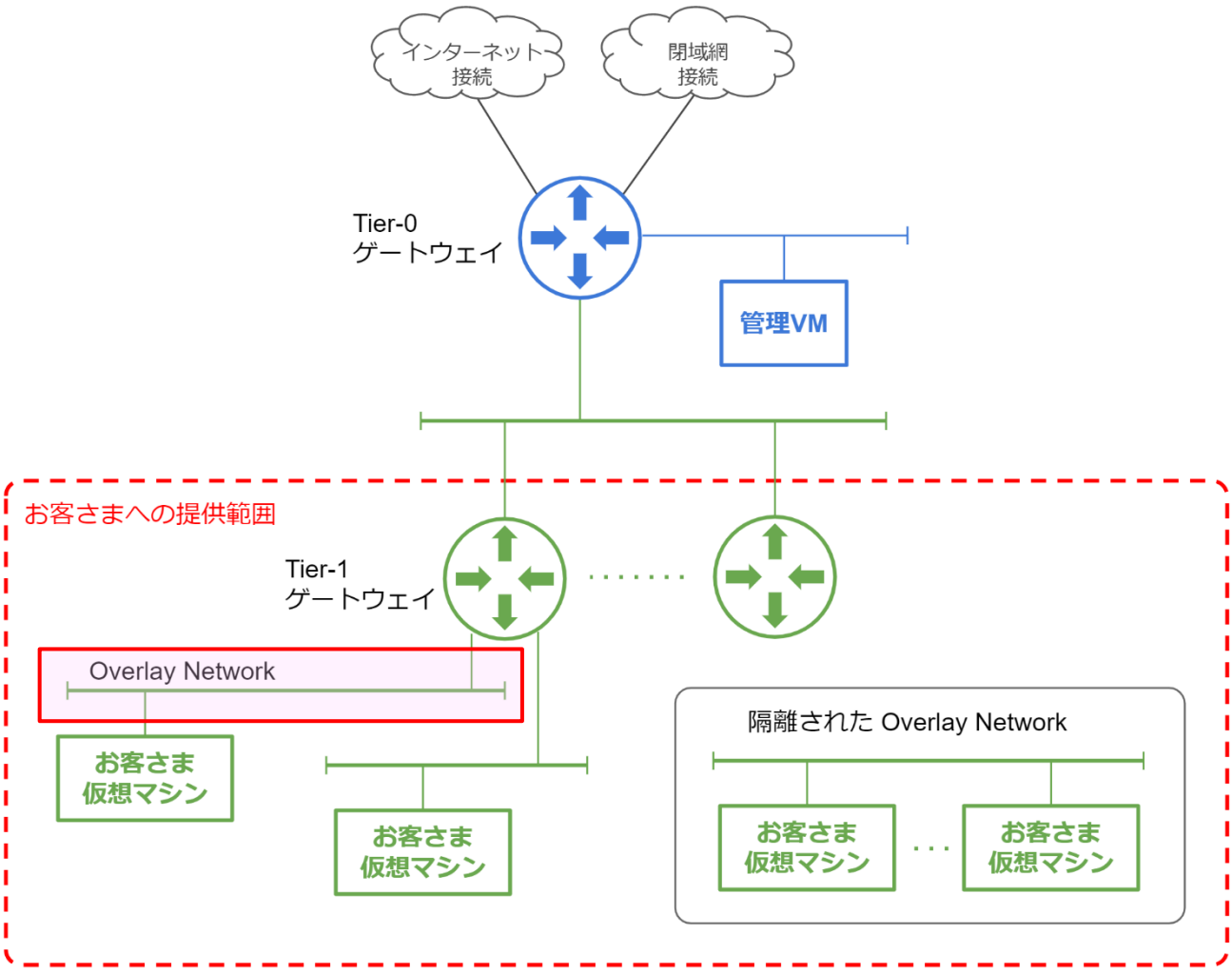
削除処理が実施されます。

5. 対象のTier-1 ゲートウェイが一覧から削除されたことを確認します。

6.4. Overlay Network に関する操作

ここでは Overlay Network の作成・削除手順をご説明いたします。

Overlay Networkを作成すると、vCenter上でポートグループとして自動追加されます。
仮想マシンのネットワーク アダプタに割り当てることで、作成したOverlay Networkに接続することが可能です。

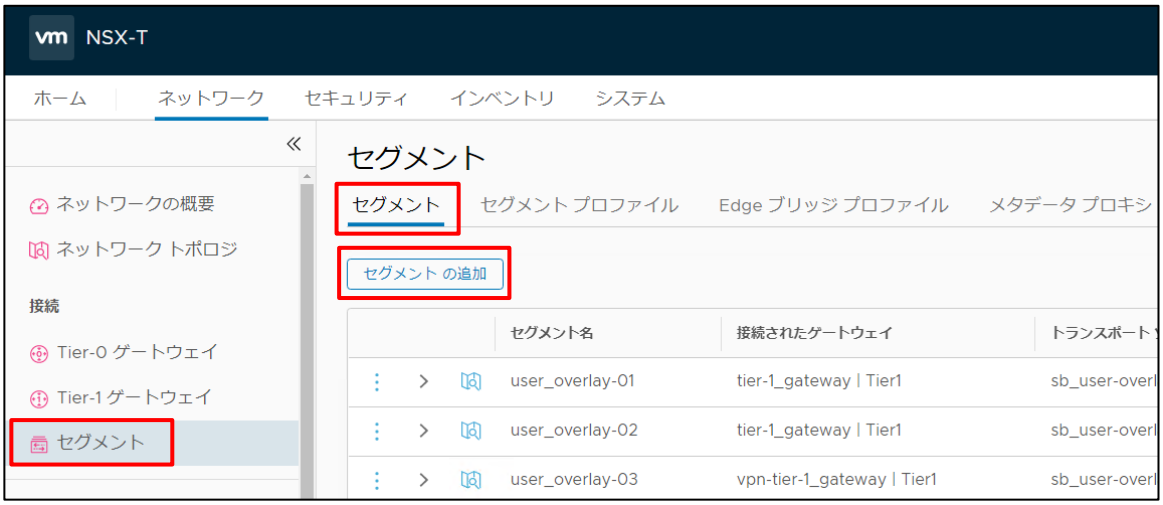


6.4.1. Overlay Networkの作成

Overlay Networkの作成手順をご説明いたします。

1. **NSX Managerにログインします。**

2. **「ネットワーク」タブをクリックし、メニューリストから「セグメント」をクリックします。右ペインに表示された「セグメント」タブから「セグメントの追加」をクリックします。**



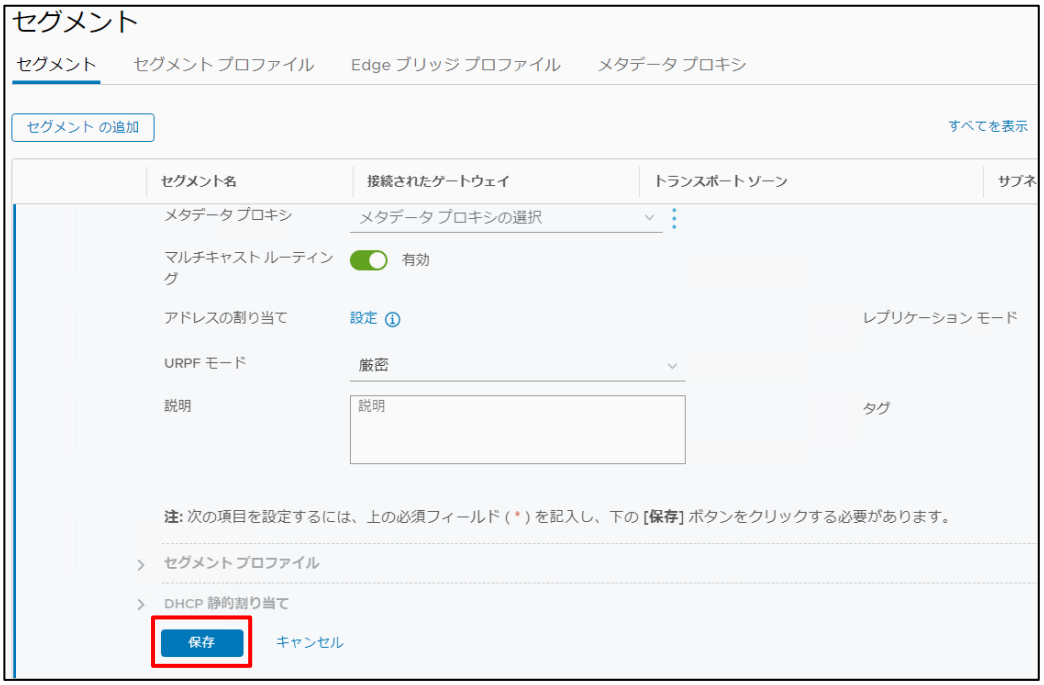
セグメントの作成画面が表示されます。

3. **以下のパラメータを入力します。**

項目	設定値
セグメント名	任意の名前を入力します。
接続されたゲートウェイ	対象のセグメントを接続するTier-1 ゲートウェイを選択します。 ☑重要 Tier-0 ゲートウェイを選択するのは禁止操作となります。
トランスポートゾーン	user-overlay-tz ☑重要 上記以外のトランスポート ゾーンの指定は禁止操作となります。
項目	設定値
サブネット – ゲートウェイ CIDR IPv4	作成するOverlay Networkのゲートウェイ IPアドレスをCIDR形式で入力します。このIPアドレスはTier-1ゲートウェイに割り当てられます。

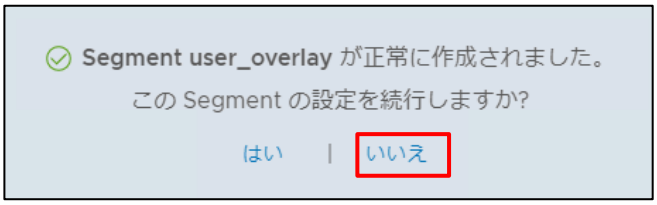
☑重要 VLANの利用は禁止操作となります。

4. 「保存」をクリックします。

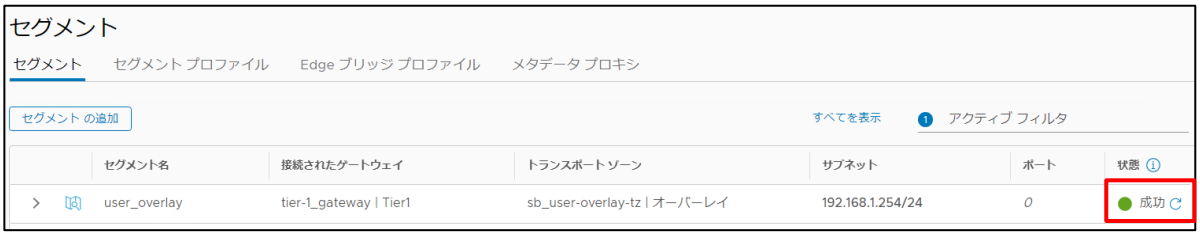


セグメントが作成されます。

5. 「いいえ」をクリックします。

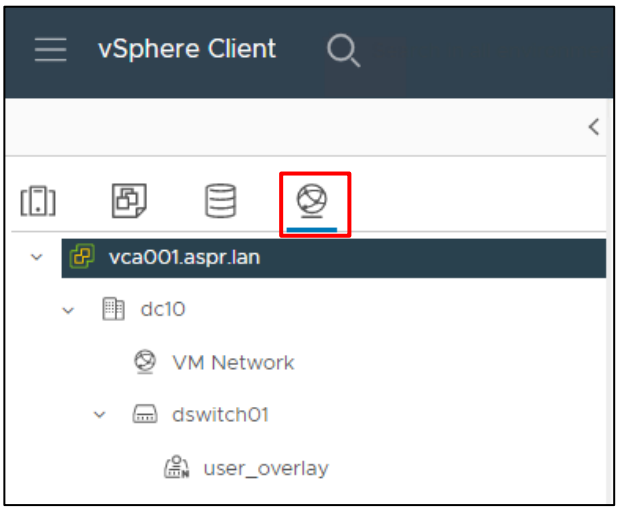


6. 作成したOverlay Networkの状態が「成功」になることを確認します。



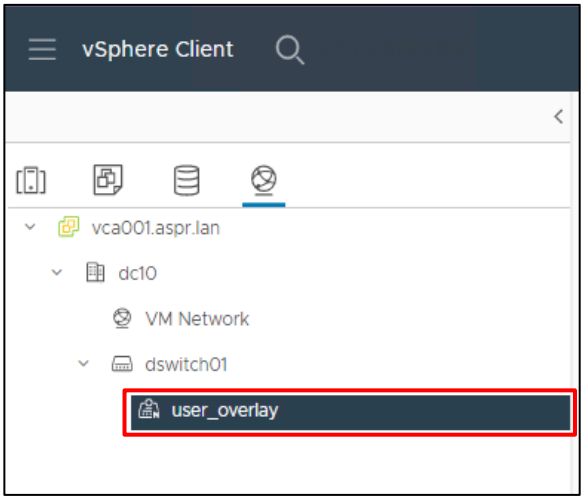
7. vSphere Clientにログインします。

8. 画面左上「三」ボタン - 「インベントリ」で「ネットワーク」タブをクリックします。



ネットワークの画面が表示されます。

9. **「dc01」 - 「dswitch01」配下に作成したOverlay Networkと同じ名前のポートグループが作成されていることを確認します。**



> **重要** 作成したセグメントを外部ネットワークと通信できるようにするには、対象のセグメントをtenant_overlayのグループに登録する必要があります。
>
> 参照 「6.14 当社作成済みグループの編集」

6.4.2. Overlay Networkの削除

Overlay Networkの削除手順をご説明いたします。

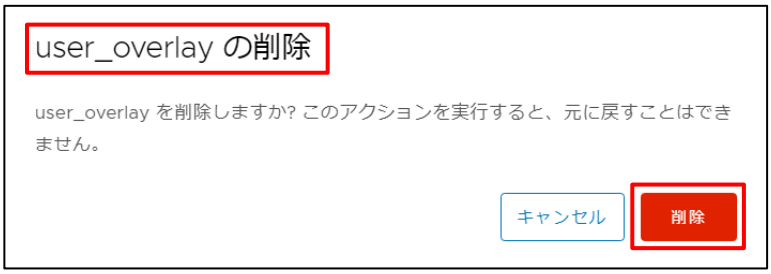
1. **NSX Managerにログインします。**

2. **「ネットワーク」から「セグメント」をクリックします。**

3. **「セグメント」タブから削除対象のOverlay Network横の「⋮」をクリックし「削除」をクリックします。**

確認画面が表示されます。

4. **確認画面で対象に間違いが無いことを確認し「削除」をクリックします。**



削除処理が実施されます。

5. **対象のOverlay Networkが一覧から削除されたことを確認します。**

6.4.3. Overlay Network の詳細設定

セグメントプロファイルを利用することで、作成したOverlay Network について詳細な設定を行うことが可能です。

セグメントプロファイルの詳細な説明や設定方法については、ヴイエムウェア社の公式ドキュメントをご参照ください。

参照 『 セグメントプロファイル』

6.5. VPNの操作

本サービスでは Tier-1 ゲートウェイへの ポリシーベースの IPsec VPN の設定が利用可能です。

> **重要**
> - 本サービスでは L2 VPN , ルートベースの IPsec VPN は非サポートとなります
> - お客さま設備の VPN 接続対応機器のサポート、およびサイト・ツー・サイト VPN 接続確立の保証はいたしません
> - DNAT は、ポリシーベースの IPSec VPN が設定されている Tier-1 ゲートウェイでサポートされていません

6.5.1. VPNの設定

本項ではIPsecVPNの設定例について記載いたします。

実際の設定内容はお客さまの環境により異なりますのでご注意ください。また、対向の機器の設定につきましてはお客さまにてご確認ください。

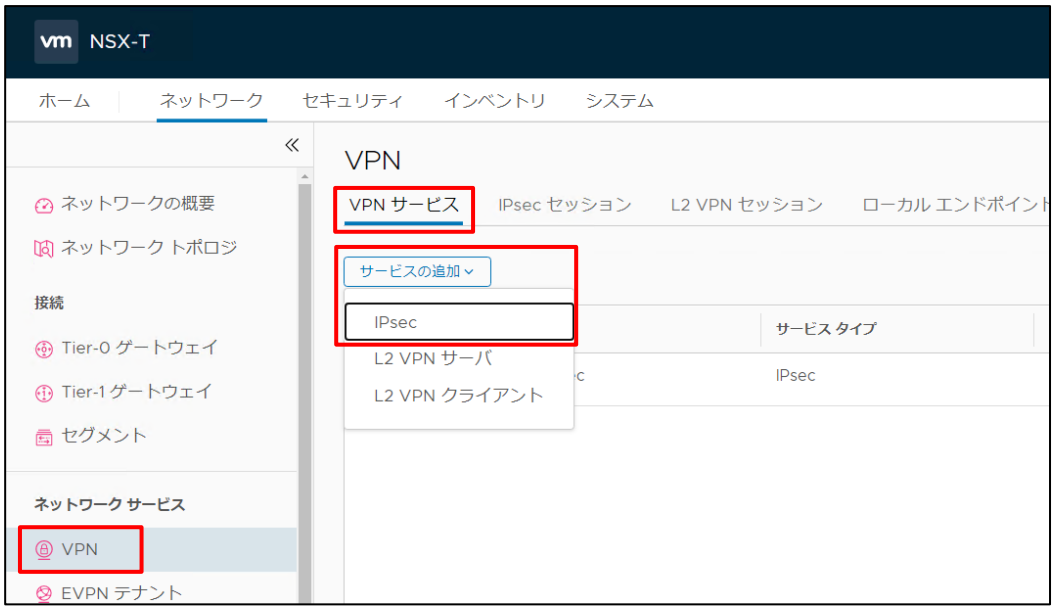
VPNサービスの作成

VPNサービスの作成手順をご説明いたします。

1. **NSX Managerにログインします。**

2. **「ネットワーク」をクリックします。**

3. **左ペインから「VPN」を選択します。「VPN サービス」タブを開き、「サービスの追加」から「IPsec」を選択します。**



IPsecサービスの作成画面が表示されます。

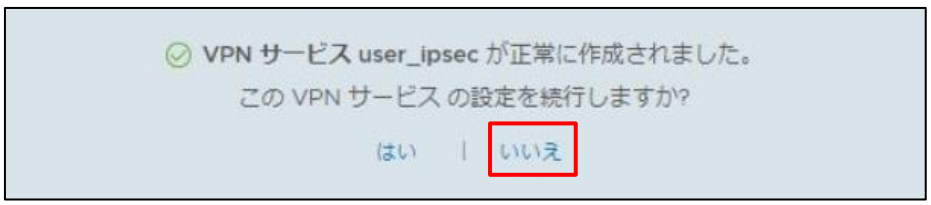
4. 以下のパラメータを入力します。

項目	設定値
名前	任意の名前を入力します。
Tier-0/Tier-1 ゲートウェイ	VPNサービスを利用するTier-1 ゲートウェイを選択します。 ☑重要 Tier-0 ゲートウェイは選択しないでください。

5. 「保存」をクリックします。

VPNサービスが作成されます

6. 「いいえ」をクリックします。



7. 作成したVPNサービスの状態が「成功」になることを確認します。

ローカルエンドポイント作成

ローカルエンドポイントの作成手順をご説明いたします。

> **補足**
> • ローカルエンドポイントを外部ネットワークと通信できるように、対象のアドレスを事前に「tenant_overlay」のグループに登録する必要があります。
> 参照 「当社作成済みグループの編集」
>
> • 証明書を利用する場合は事前に証明書のインポートをする必要があります。
> 参照 「証明書の操作」

1. NSX Managerにログインします。

2. 「ネットワーク」から「VPN」をクリックします。

3. 「ローカル エンドポイント」タブから「ローカル エンドポイントの追加」をクリックします。

ローカル エンドポイントの作成画面が表示されます。

4. 以下のパラメータを入力します。

項目	設定値
名前	任意の名前を入力します。
VPN サービス	作成したVPNサービスを選択します。
IP アドレス	VPN接続で利用するIPアドレスを入力します。
ローカル ID	IPアドレスと同じ値を入力します。

5. 「保存」をクリックします。

ローカル エンドポイントが作成されます。

6. 作成したローカル エンドポイントの状態が「成功」になることを確認します。

VPN プロファイルの作成

VPNプロファイルの作成手順をご説明いたします。

VPN接続の確立で利用されるIPsecやIKE、DPDのプロファイルはデフォルトで用意されていますが、対向機器との接続でデフォルト以外の設定が必要な場合はプロファイルを作成します。

1. NSX Managerにログインします。

2. 「ネットワーク」から「VPN」をクリックします。

3. 「プロファイル」タブをクリックし「プロファイル タイプの選択」から作成したいプロファイルの種類を選択します。

選択したプロファイルの一覧画面が表示されます。

4. 「<選択したプロファイル名>の追加」をクリックします

以下はIKEプロファイルの画面となります。

プロファイルの作成画面が表示されます。

5. 各種パラメータを入力し、「保存」をクリックします。

入力するパラメータは対向機器の設定に合わせて入力してください。

以下はIKEプロファイルの設定画面となります。

6. 作成したプロファイルの状態が「成功」になることを確認します。

IPsec セッションの作成

IPsecc セッションの作成手順をご説明いたします。

1. NSX Managerにログインします。

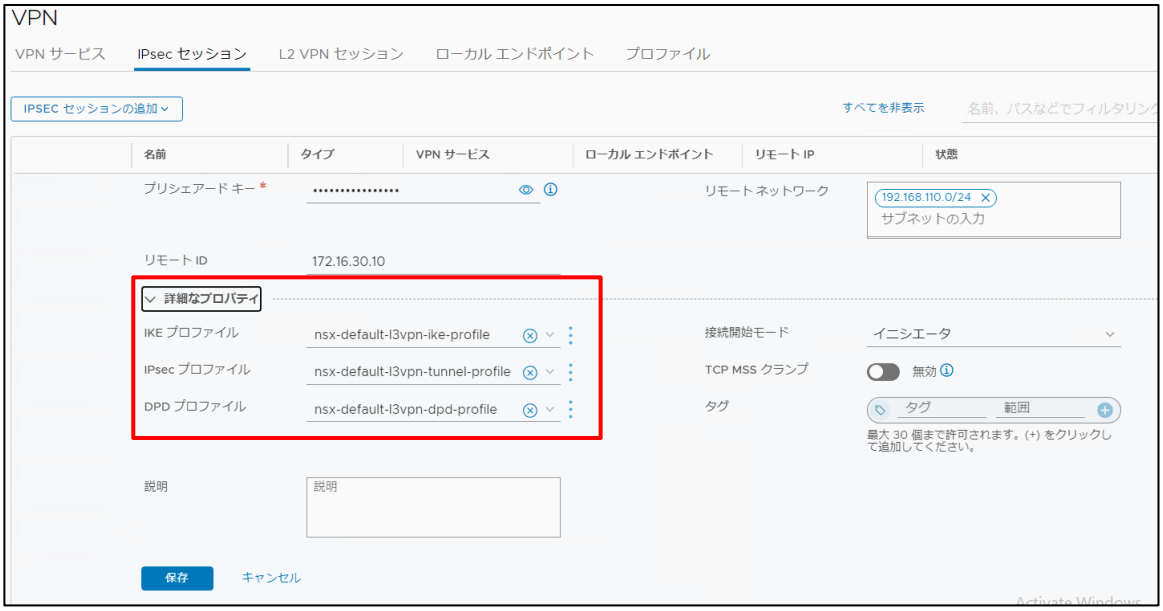
2. 「ネットワーク」から「VPN」をクリックします。

3. 「IPsecセッション」タブから「IPSEC セッションの追加」をクリックし「ポリシー ベース」をクリックします。

IPsecセッションの作成画面が表示されます。

4. 以下のパラメータを入力します。

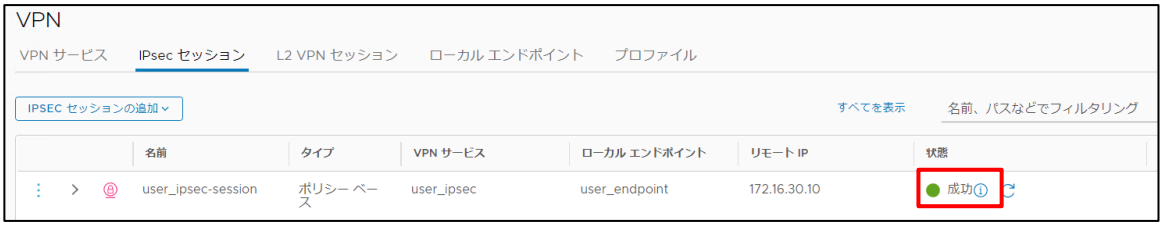
項目	設定値
名前	任意の名前を入力します。
VPN サービス	作成したVPNサービスを選択します。
ローカル エンドポイント	作成したローカル エンドポイントを選択します。
リモート IP	VPN接続先のIPアドレスを入力します。
プリシェアード キー	接続先との認証で利用するキーを入力します
リモート ID	接続先のリモートID を入力します。
ローカル ネットワーク	VPN接続元のローカル ネットワークを指定します。
リモート ネットワーク	VPN接続先のリモート ネットワークを指定します。
IKE プロファイル	デフォルト以外のものを使用する場合はここで指定します。
IPsec プロファイル	デフォルト以外のものを使用する場合はここで指定します。
DPD プロファイル	デフォルト以外のものを使用する場合はここで指定します。



5. 「保存」をクリックします。

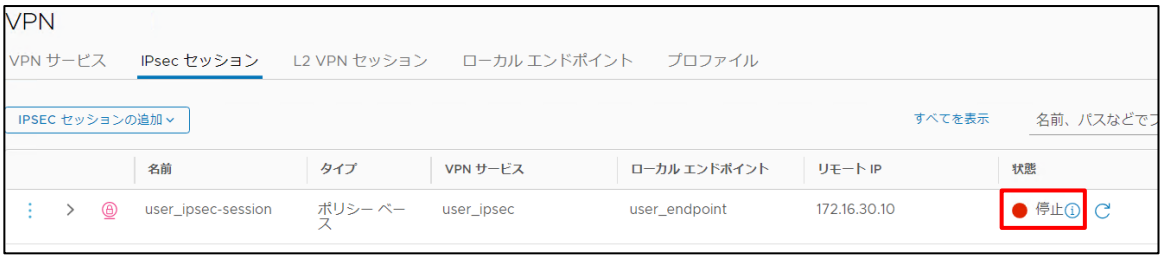
IPsec セッションが作成されます。

6. 作成したIPsec セッションの状態を確認します。



対向機器とVPN接続が確立できた場合「成功」となりますが、対向の機器の設定が完了していないなどで接続が確立できない場合は「停止」となります。

対向機器の設定が完了していない場合は設定を完了させ、「成功」となることを確認します。



6.5.2. VPN設定の削除

本項では IPsecVPN 設定の削除について記載いたします。

IPSec セッションの削除

IPsecc セッションの削除手順をご説明いたします。

1. **NSX Managerにログインします。**

2. **「ネットワーク」から「VPN」をクリックします。**

3. **「IPsecセッション」タブから削除対象のIPsec セッション横の「⋮」をクリックし「削除」をクリックします。**

確認画面が表示されます。

4. **確認画面で対象に間違いが無いことを確認し「削除」をクリックします。**

削除処理が実施されます。

5. 対象のIPsec セッションが一覧から削除されたことを確認します。

ローカル エンドポイントの削除

ローカル エンドポイントの削除手順をご説明いたします。

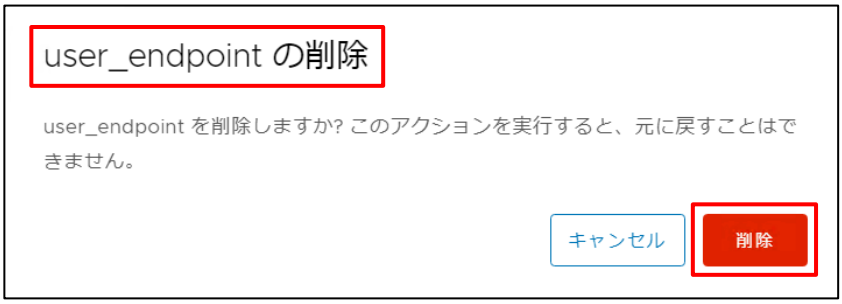
1. **NSX Managerにログインします。**

2. **「ネットワーク」から「VPN」をクリックします。**

3. **「ローカル エンドポイント」タブから削除対象のローカル エンドポイント横の「⋮」をクリックし「削除」をクリックします。**

確認画面が表示されます。

4. **確認画面で対象に間違いが無いことを確認し「削除」をクリックします。**



削除処理が実施されます。

5. **対象のローカル エンドポイントが一覧から削除されたことを確認します。**

VPN サービスの削除

VPN サービスの削除手順をご説明いたします。

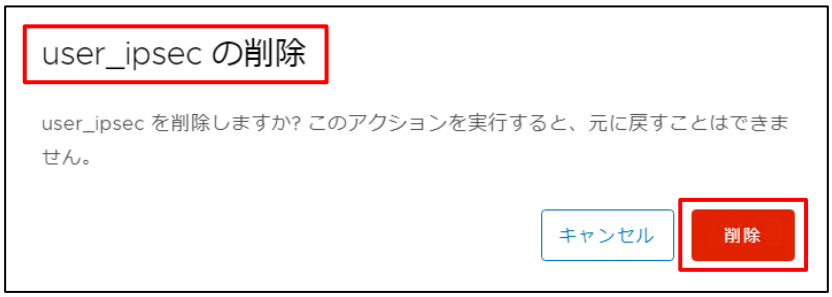
1. **NSX Managerにログインします。**

2. **「ネットワーク」から「VPN」をクリックします。**

3. **「VPN サービス」タブから削除対象のVPN サービス横の「：」をクリックし「削除」をクリックします。**

確認画面が表示されます。

4. **確認画面で対象に間違いが無いことを確認し「削除」をクリックします。**



削除処理が実施されます。

5. **対象のVPN サービスが一連から削除されたことを確認します。**

VPN プロファイルの削除

VPN プロファイルの削除手順をご説明いたします。

1. **NSX Managerにログインします。**

2. **「ネットワーク」から「VPN」をクリックします。**

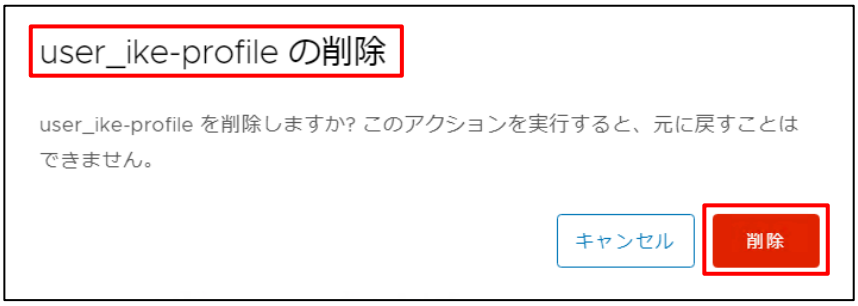
3. **「プロファイル」タブをクリックし「プロファイル タイプの選択」から削除したいプロファイルの種類を選択します。**

4. **削除対象のプロファイル横の「⋮」をクリックし「削除」をクリックします。**

※以下はIKE プロファイルの画面となります。

確認画面が表示されます。

5. 確認画面で対象に間違いが無いことを確認し「削除」をクリックします。



削除処理が実施されます。

6. 対象のプロファイルが一覧から削除されたことを確認します。

6.6. NATの操作

本サービスでは Tier-1 ゲートウェイへのNATの設定が利用可能です。

6.6.1. NATの設定

本項ではDNAT/SNATの設定例について記載いたします。

> **重要** **既知の不具合について**
>
> ルールにて設定した変換前port番号と変換後Port番号が、入れ替わった動作になってしまいます。
>
> ポート番号の変換を伴うDNAT機能のご利用はお控えください。
>
> 参照『NSX-T NAT port reverted issue (86356)』

> **重要** **ベアメタルサーバ用 ネットワーク向けのNATについて**
>
> ベアメタルサーバのOSが接続するネットワーク(sb_baremetal_os-seg-XX)に対してのDNATは NSX-Tの動作仕様上サポートされておりません。
>
> ベアメタルサーバのネットワークについては以下をご参照ください
>
> 参照『19.1 ベアメタルサーバ用 NSX-T設定』

DNATの設定

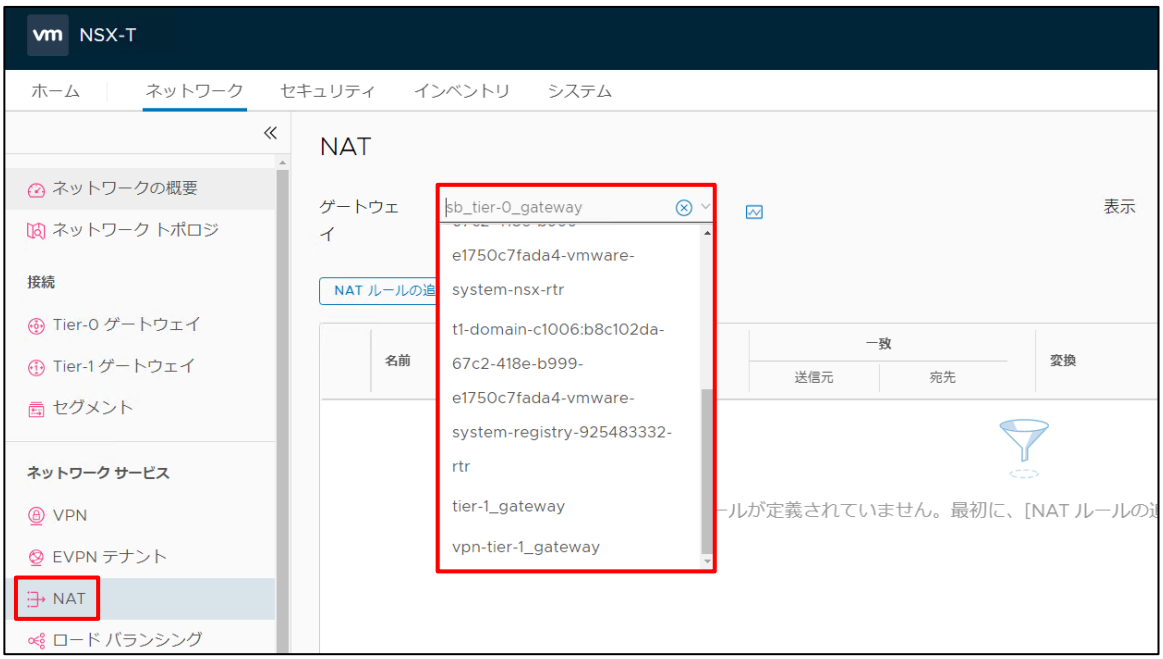
DNATの設定手順をご説明いたします。

1. **NSX Managerにログインします。**

2. **「ネットワーク」をクリックします。**

3. **「NAT」をクリックし「ゲートウェイ」からNATを設定するTier-1 ゲートウェイをクリックします。**

> **重要** Tier-0 ゲートウェイへのNAT設定は禁止操作となります。



対象のTier-1 ゲートウェイのNAT設定画面が表示されます。

4. 「NATルール」の追加をクリックします。

項目	設定値
名前	任意の名前を入力します。
アクション	DNAT を指定します
宛先	通信を受ける IP アドレスを指定します。
変換	宛先 IP アドレスの変換先 IP アドレスを指定します。
ファイアウォール	以下からお客さま環境に合わせて選択します。 ・「外部アドレスと一致」: 変換後の IP アドレスとポートの組み合わせに一致するファイアウォール ルールによって処理されます。 ・「内部アドレスと一致」: 変換前の IP アドレスとポートの組み合わせに一致するファイアウォール ルールによって処理されます。 ・「バイパス」: ファイアウォール ルールをバイパスします。

5. 以下のパラメータを入力します。

6. 「保存」をクリックします。

NATが作成されます

7. 作成したNATの状態が「成功」になることを確認します。

SNATの設定

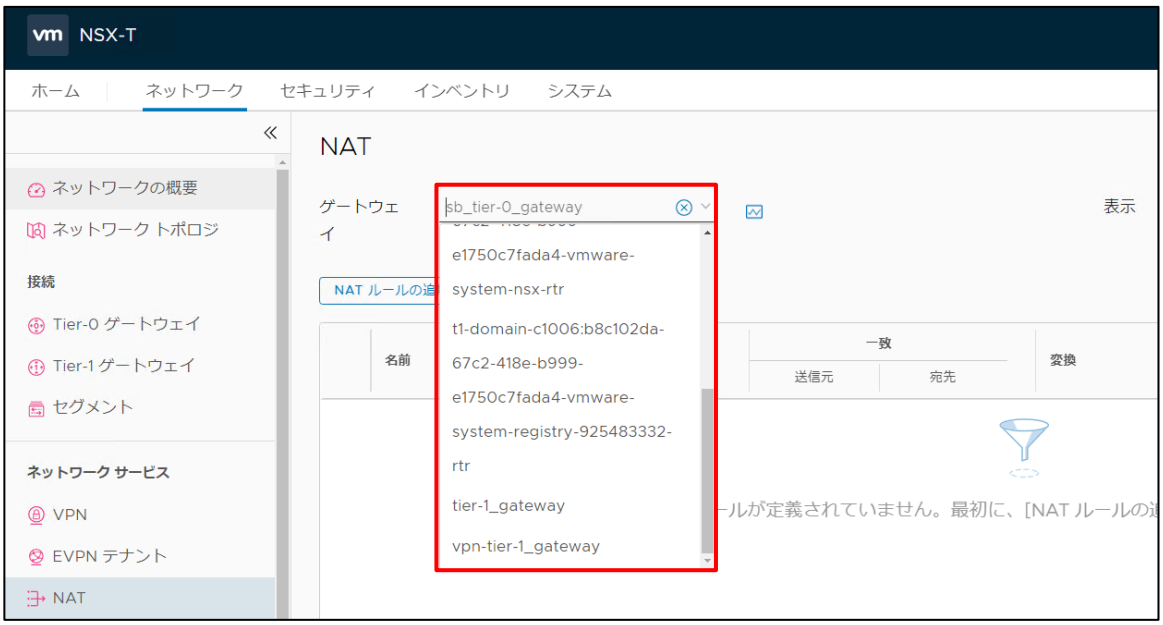
SNATの設定手順をご説明いたします。

1. NSX Managerにログインします。

2. 「ネットワーク」から「NAT」をクリックします。

3. 「ゲートウェイ」からNATを設定するTier-1 ゲートウェイをクリックします。

> **重要** Tier-0 ゲートウェイへのNAT設定は禁止操作となります。



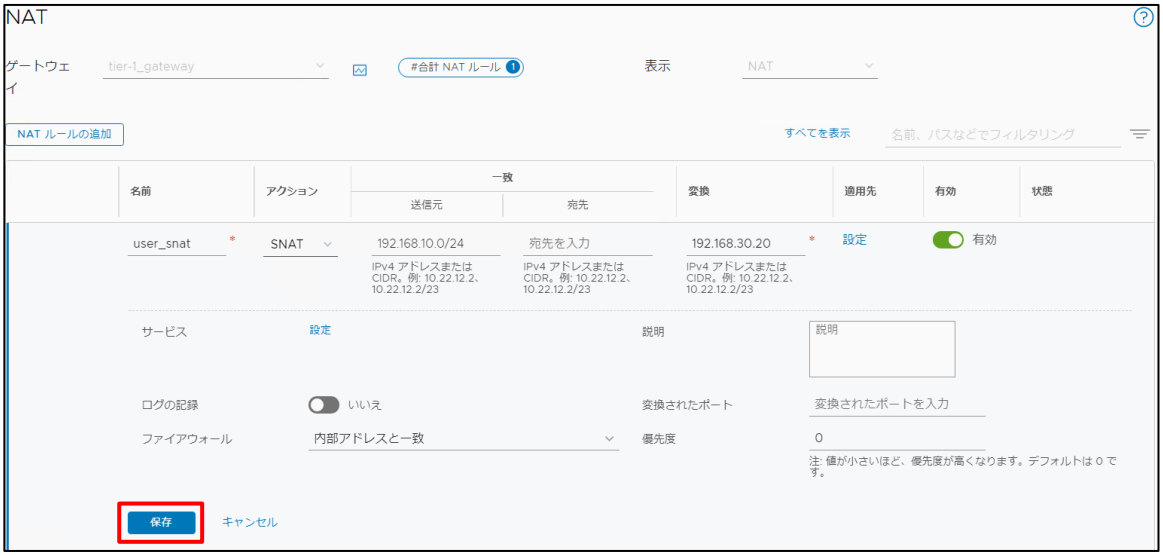
対象のTier-1 ゲートウェイのNAT設定画面が表示されます。

4. 「NATルール」の追加をクリックします。

5. 以下のパラメータを入力します。

項目	設定値
名前	任意の名前を入力します。
アクション	SNAT を指定します
送信元	SNAT で変換をする対象の送信元 IP アドレスまたはアドレスレンジを指定します。 送信元を指定しない場合、この NAT ルールはローカル サブネットの全ての送信元に適用されます
変換	送信元からの通信の変換先 IP アドレスを指定します。
ファイアウォール	以下からお客さま環境に合わせて選択します。 ・「外部アドレスと一致」: 変換後の IP アドレスとポートの組み合わせに一致するファイアウォール ルールによって処理されます。 ・「内部アドレスと一致」: 変換前の IP アドレスとポートの組み合わせに一致するファイアウォール ルールによって処理されます。 ・「バイパス」: ファイアウォール ルールをバイパスします。

6. 「保存」をクリックします。



NATが作成されます。

7. 作成したNATの状態が「成功」になることを確認します。

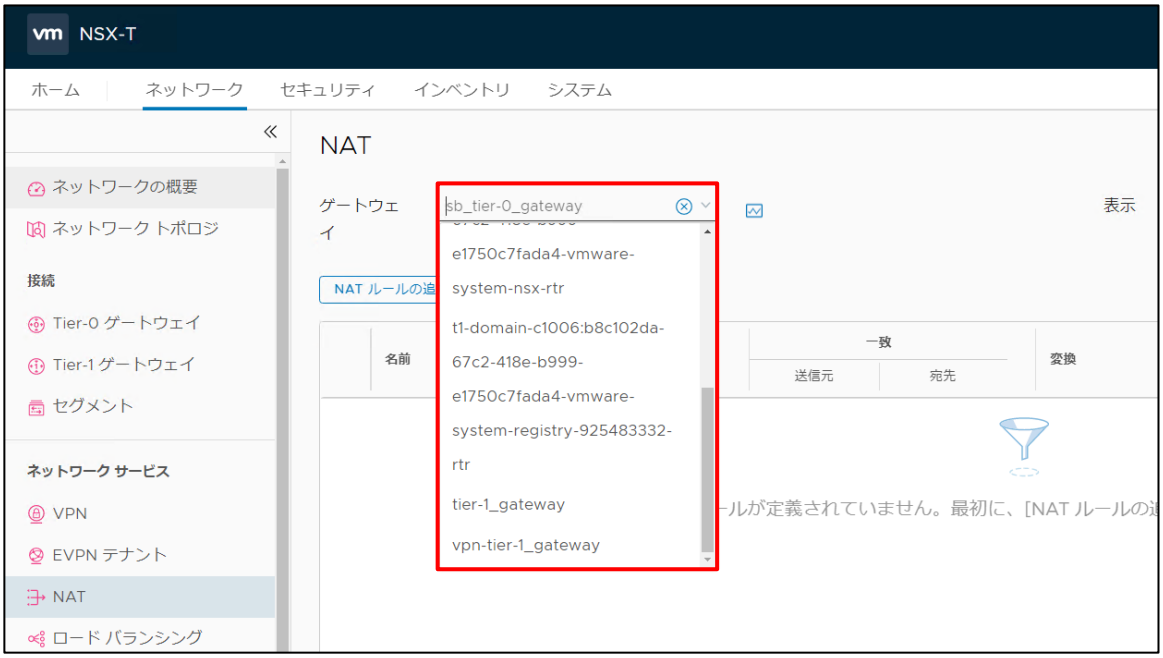
6.6.2. NAT設定の削除

NAT設定の削除手順にについてご説明いたします。

1. **NSX Managerにログインします。**

2. **「ネットワーク」から「NAT」をクリックします。**

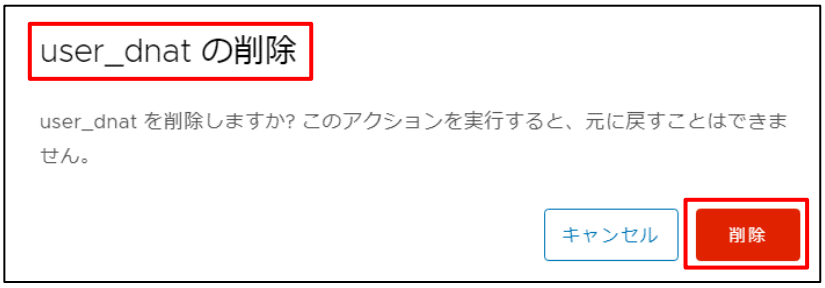
3. **「ゲートウェイ」から削除対象のNATが設定されているTier-1 ゲートウェイをクリックします。**



4. **削除対象のNAT設定 横の「：」をクリックし「削除」をクリックします。**

確認画面が表示されます。

5. 確認画面で対象に間違いが無いことを確認し「削除」をクリックします。



削除処理が実施されます。

6. 対象のNAT設定が一覧から削除されたことを確認します。

6.7. DNSの操作

本サービスでは Tier-1 ゲートウェイへのDNSの設定が利用可能です。

本項では、DNSフォワード機能に関する設定例をご説明いたします。

デフォルト ゾーン(フォワーダ相当)とFQDN ゾーン(条件付きフォワーダ相当)を定義しDNSサービスに割り当てることで、Tier-1ゲートウェイをDNSサーバ(フォワーダ機能のみ)として利用することができます。

6.7.1. DNSの設定

本項ではDNSの設定例について記載いたします。

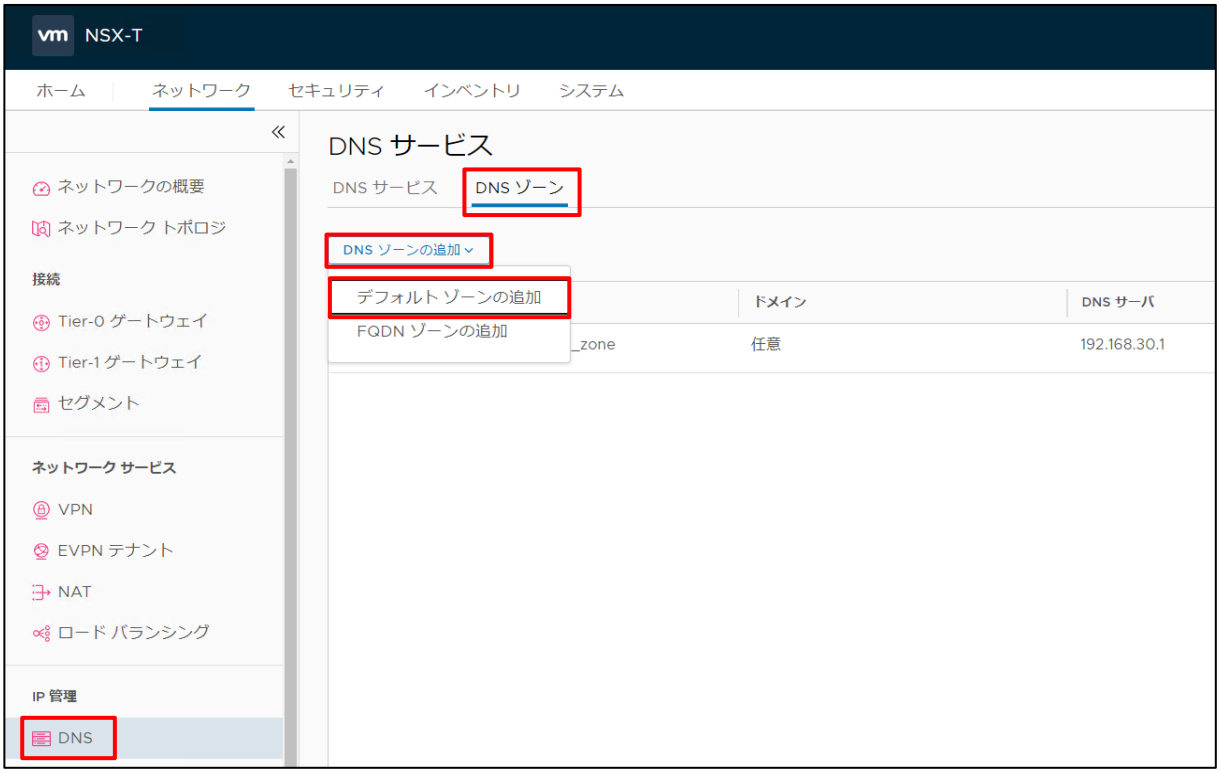
デフォルト ゾーンの作成

デフォルト ゾーンの作成手順についてご説明いたします。

1. **NSX Managerにログインします。**

2. **「ネットワーク」をクリックします。**

3. **「DNS」をクリックし「DNS ゾーン」タブから「DNS ゾーンの追加」をクリックし、「デフォルト ゾーンの追加」をクリックします。**



デフォルト ゾーンの作成画面が表示されます。

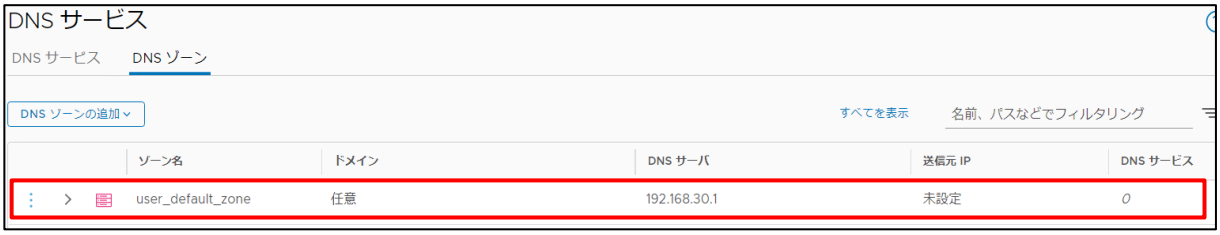
4. 以下のパラメータを入力します。

項目	設定値
ゾーン名	任意の名前を入力します。
DNS サーバ	DNSクエリの転送先DNSサーバのIPアドレスを入力します。

5. 「保存」をクリックします。

デフォルト ゾーンが作成されます

6. デフォルトゾーンが作成されたことを確認します。



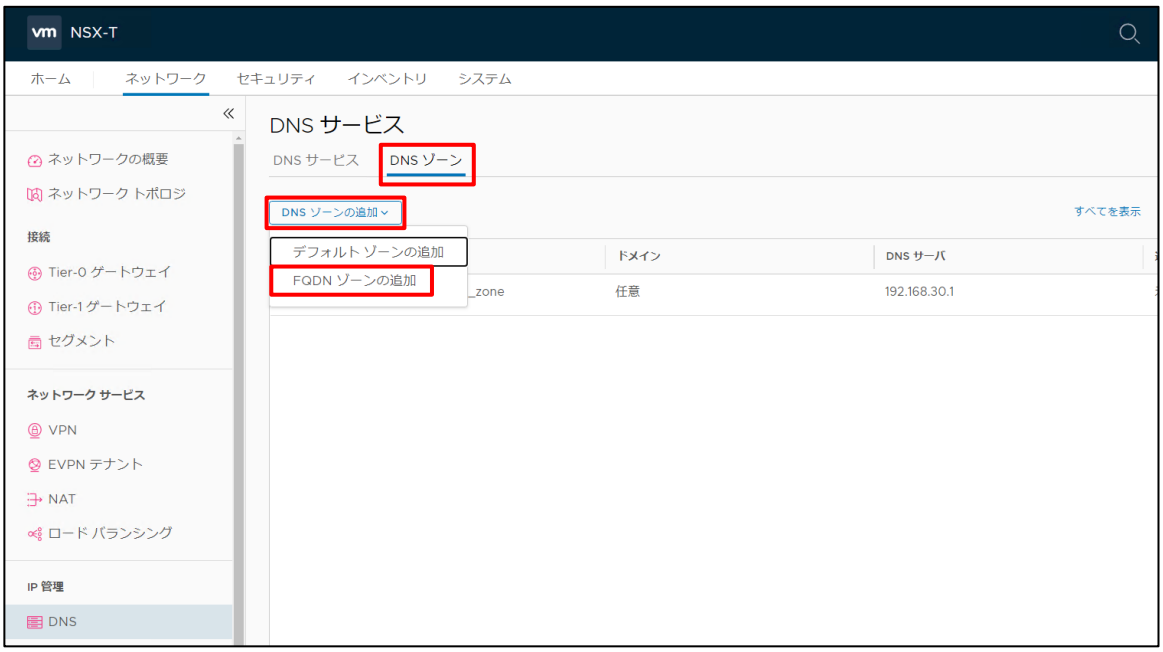
FQDNゾーンの作成

FQDN ゾーンの作成手順についてご説明いたします。

1. **NSX Managerにログインします。**

2. **「ネットワーク」から「DNS」をクリックします。**

3. **「DNS ゾーン」タブから「DNS ゾーンの追加」をクリックし、「FQDN ゾーンの追加」をクリックします。**



FQDNゾーンの作成画面が表示されます。

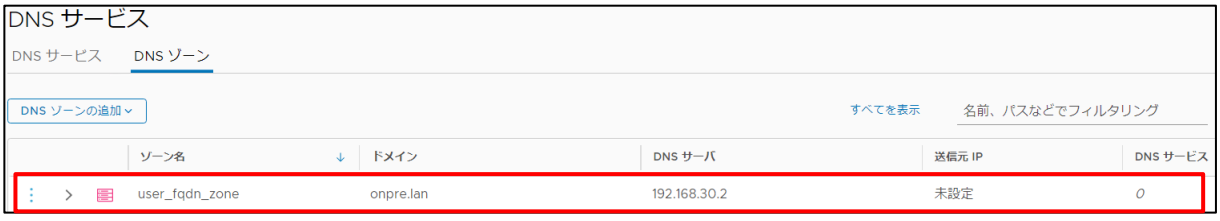
4. 以下のパラメータを入力します。

項目	設定値
ゾーン名	任意の名前を入力します。
ドメイン	FQDNゾーンで転送をするドメイン名を入力します。
DNS サーバ	DNSクエリの転送先DNSサーバのIPアドレスを入力します。

5. 「保存」をクリックします。

FQDN ゾーンが作成されます

6. FQDN ゾーンが作成されたことを確認します。



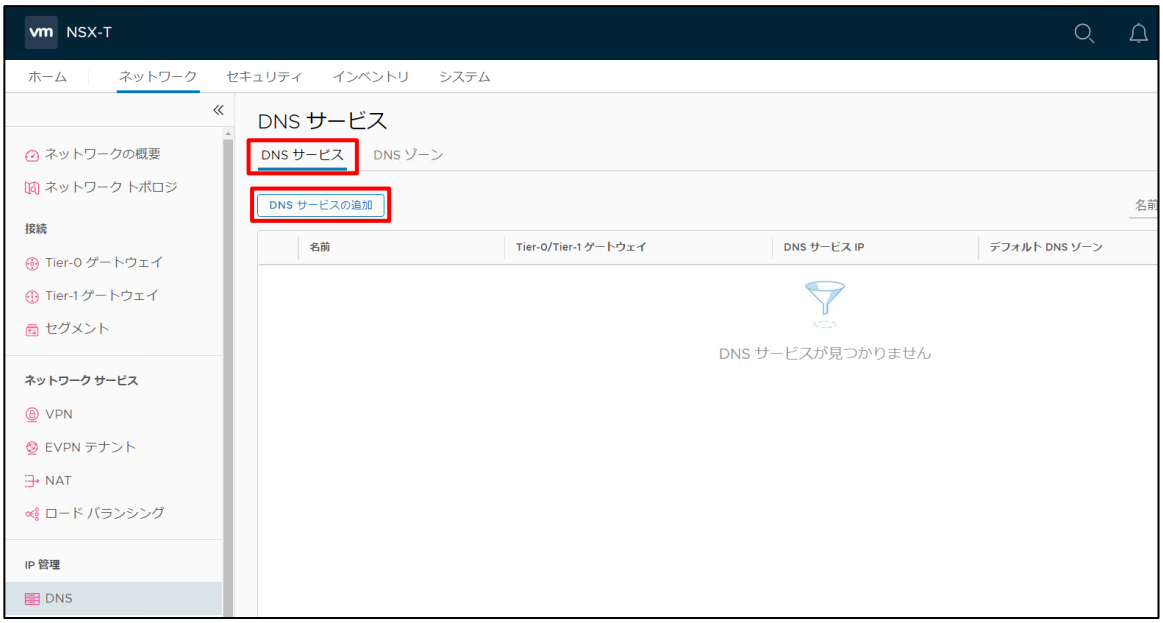
DNSサービスの作成

DNSサービスの作成手順についてご説明いたします。

1. NSX Managerにログインします。

2. 「ネットワーク」から「DNS」をクリックします。

3. 「DNS サービス」タブから「DNS サービスの追加」をクリックします。



DNSサービスの作成画面が表示されます。

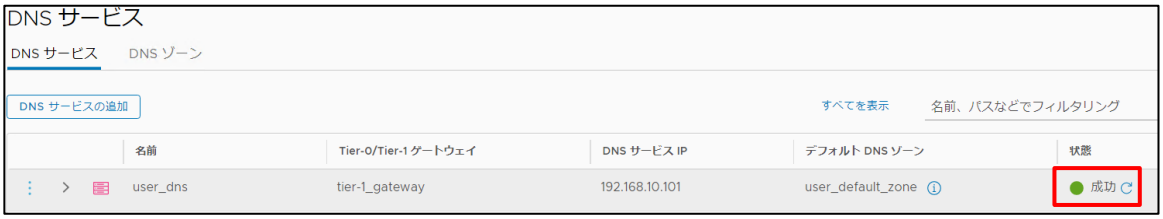
4. 以下のパラメータを入力します。

項目	設定値
名前	任意の名前を入力します。
Tier-0/Tier-1 ゲートウェイ	DNSサービスを利用するTier-1 ゲートウェイを選択します。 ☑重要 Tier-0 ゲートウェイは選択しないでください。
DNS サービス IP	DNSサーバとして利用するIPアドレスを指定します。
デフォルト DNS ゾーン	デフォルトDNSゾーン(フォワーダ)を指定します。
FQDN ゾーン	FQDNゾーン(条件付きフォワーダ)を指定します。 不要な場合は空欄とします。

5. 「保存」をクリックします。

DNSサービスが作成されます

6. 作成したDNSサービスの状態が「成功」になることを確認します。



6.7.2. DNS設定の削除

本項ではDNS設定の削除手順について記載いたします。

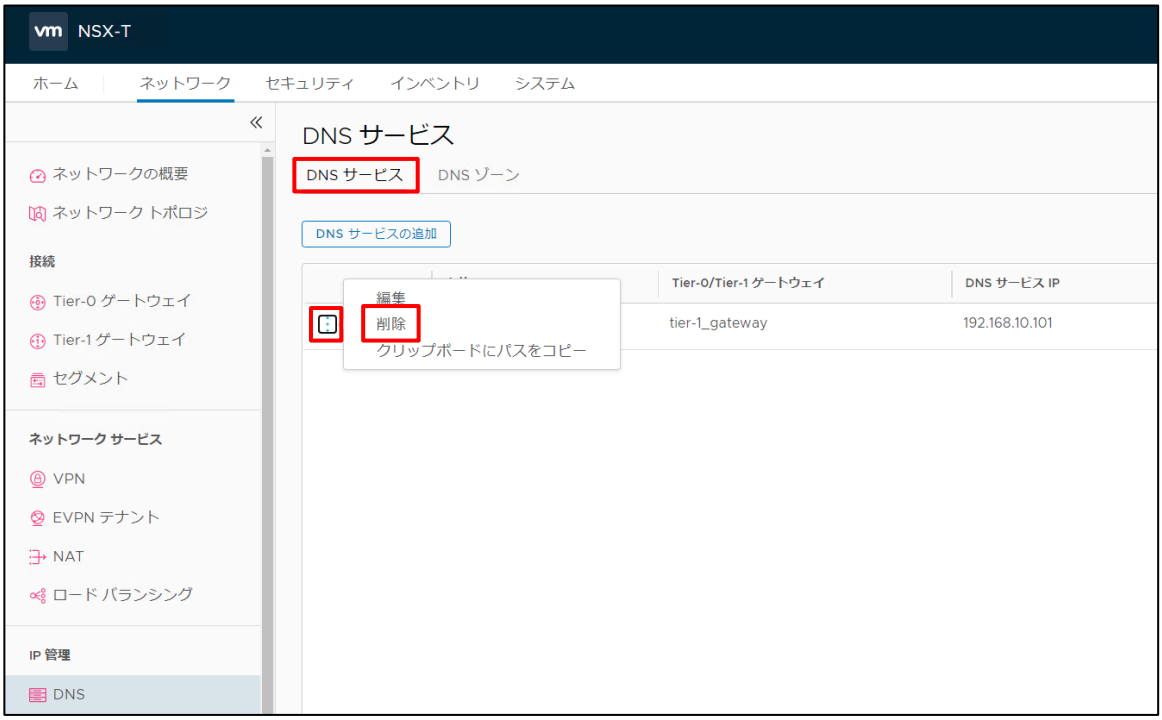
DNSサービスの削除

DNSサービスの削除手順をご説明いたします。

1. **NSX Managerにログインします。**

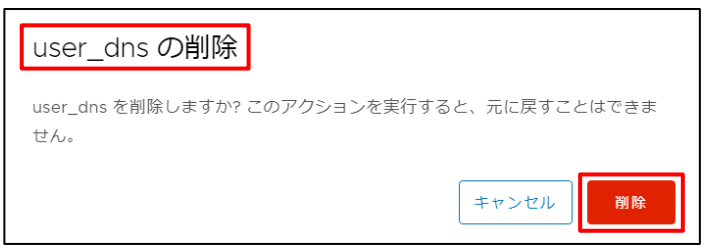
2. **「ネットワーク」から「DNS」をクリックします。**

3. **「DNSサービス」タブから削除対象のDNSサービス横の「⋮」をクリックし「削除」をクリックします。**



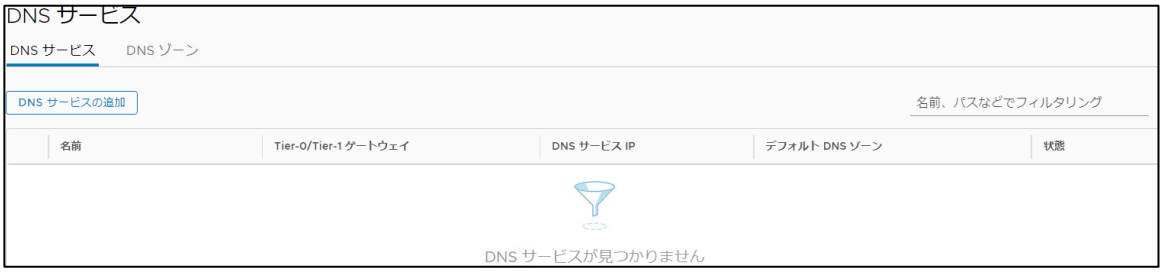
確認画面が表示されます。

4. **確認画面で対象に間違いが無いことを確認し「削除」をクリックします。**



削除処理が実施されます。

5. 対象のDNSサービスが一覧から削除されたことを確認します。



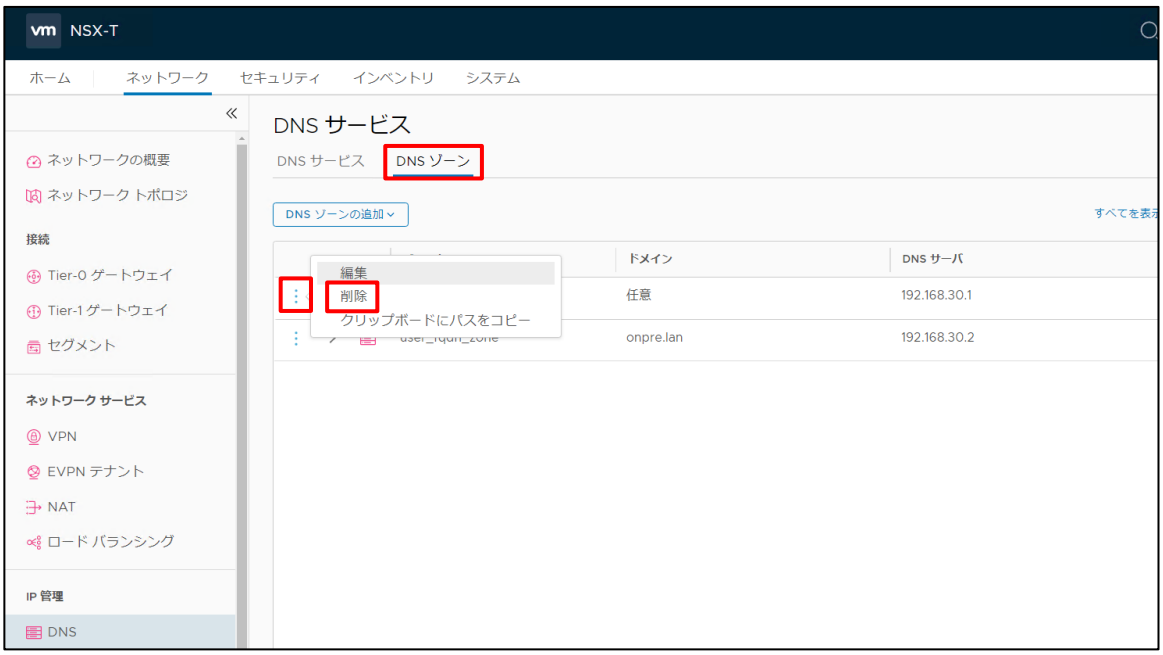
DNSゾーンの削除

DNSゾーン(デフォルト、FQDN共通)の削除手順をご説明いたします。

1. NSX Managerにログインします。

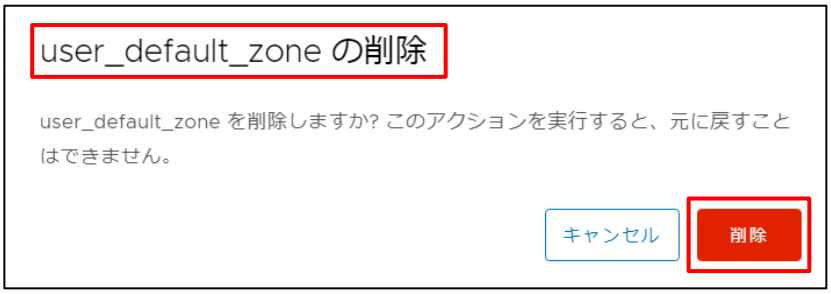
2. 「ネットワーク」から「DNS」をクリックします。

3. 「DNSゾーン」タブから削除対象のDNSゾーン横の「：」をクリックし「削除」をクリックします。



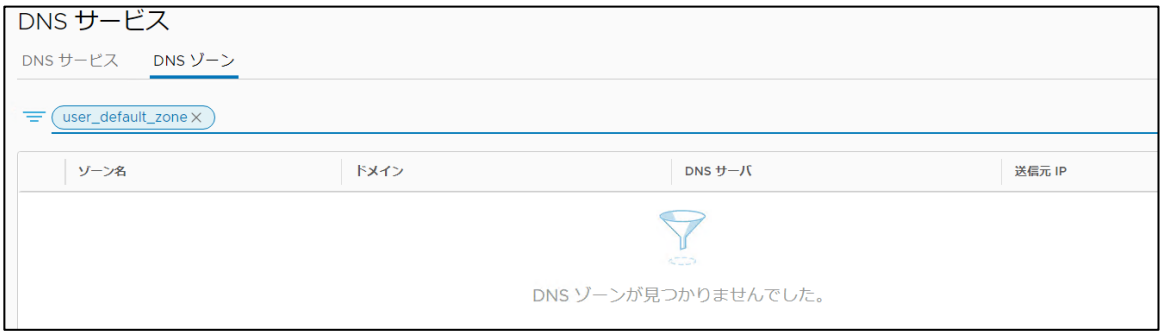
確認画面が表示されます。

4. 確認画面で対象に間違いが無いことを確認し「削除」をクリックします。



削除処理が実施されます。

5. 対象のDNSゾーンが一覧から削除されたことを確認します。



6.8. DHCPの操作

本サービスでは Tier-1 ゲートウェイへのDHCPの設定が利用可能です。

NSXのDHCPは以下の構成がご利用いただけます。

- DHCP ローカル サーバ：セグメント単位でプロファイルを適用し DHCP サーバを構成します
- ゲートウェイ DHCP：Tier-1 ゲートウェイにプロファイルを適用し DHCP サーバを構成します
- DHCP リレー：リモートの DHCP サーバに DHCP トラフィックを中継できます

6.8.1. DHCPの設定

本項ではゲートウェイDHCPの設定例についてご説明いたします。

DHCPサーバ プロファイルの作成

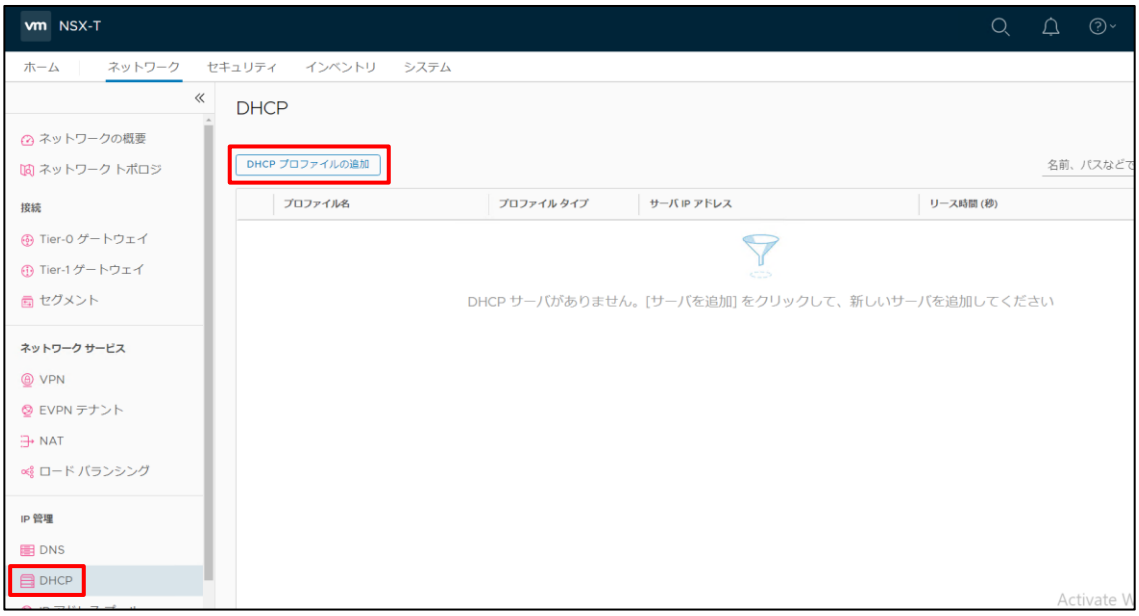
DHCPサーバ プロファイルの作成手順をご説明いたします。

DHCPサーバ プロファイルはDHCPローカル サーバ、ゲートウェイDHCPで利用します。

1. NSX Managerにログインします。

2. 「ネットワーク」をクリックします。

3. 「DHCP」をクリックし「DHCP プロファイルの追加」をクリックします。



DHCP プロファイルの作成画面が表示されます。

4. 以下のパラメータを入力します。

項目	設定値
プロファイル名	任意の名前を入力します。
プロファイル タイプ	DHCPサーバを選択します。
サーバ IP アドレス	DHCPサーバとして利用するIPアドレスをCIDR形式で入力します。 ※IPを指定しない場合 100.96.0.1/30 が自動的に割り当てられます。
Edge クラスタ	sb_edgecluster01 を選択します。

5. 「保存」をクリックします。

DHCPサーバ プロファイルが作成されます

6. DHCPサーバ プロファイルが作成されたことを確認します。

ゲートウェイDHCPの設定

ゲートウェイ DHCPの設定手順をご説明いたします。

ゲートウェイDHCPはゲートウェイに接続している全てのセグメントの仮想マシンに、IP とそのほかのネットワーク構成を動的に割り当てます。

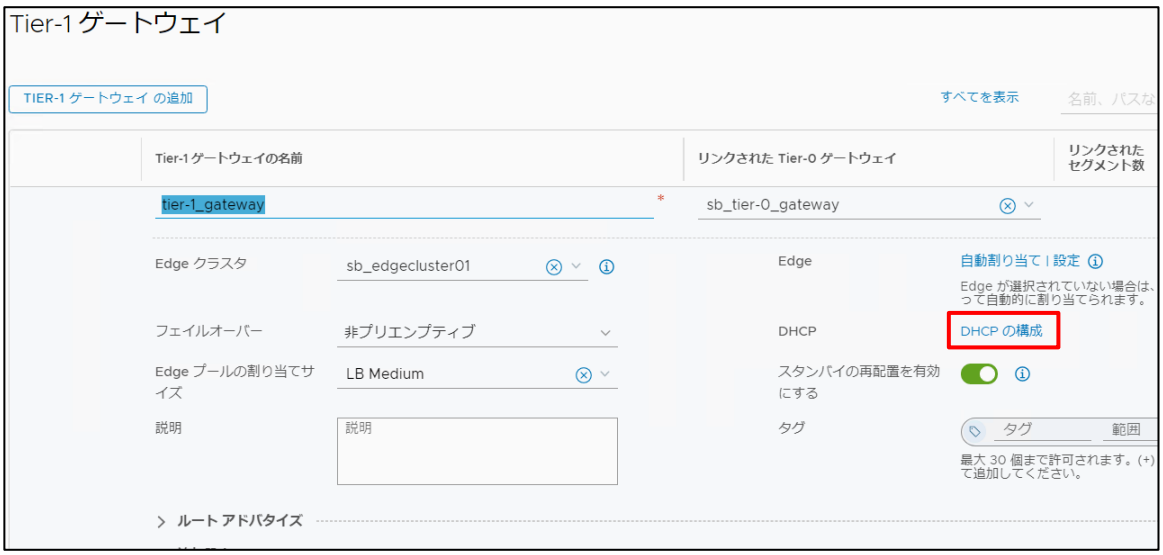
1. **NSX Managerにログインします。**

2. **「ネットワーク」から「Tier-1 ゲートウェイ」をクリックします。**

3. **ゲートウェイDHCPを設定するTier-1 ゲートウェイ横の「⋮」をクリックし「編集」をクリックします。**

Tier-1ゲートウェイの設定編集画面が開きます。

4. **「DHCPの構成」をクリックします。**



5. 以下のパラメータを入力します。

項目	設定値
タイプ	「DHCP サーバ」を選択します
DHCP サーバ プロファイル	作成した DHCP サーバプロファイルを指定します。

6. 「保存」をクリックします。

7. 「保存」をクリックします。

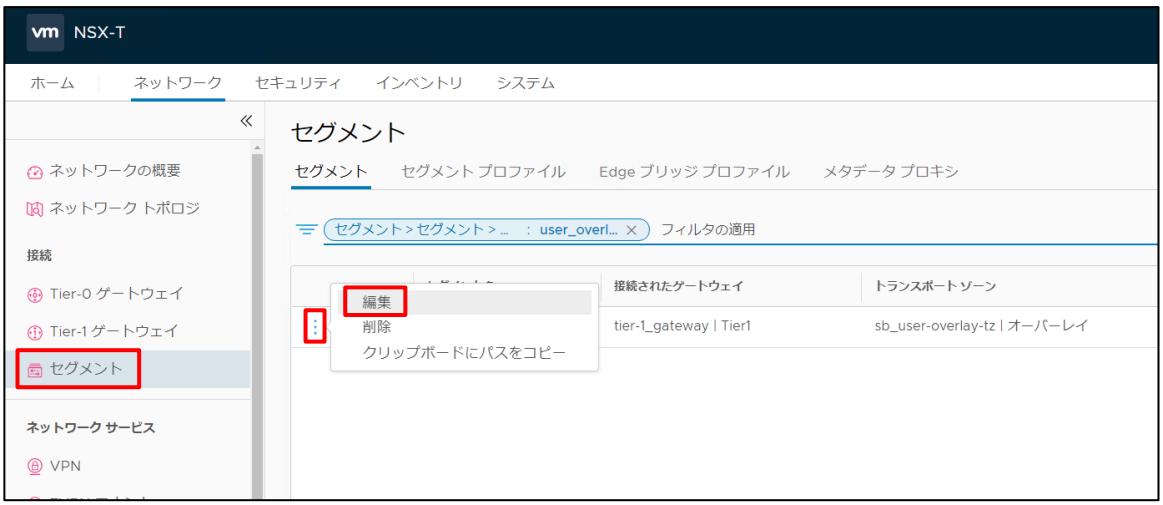
設定が保存されます。

8. 「編集を終了」をクリックします。

編集画面が終了します。

9. 「セグメント」をクリックし「セグメント」タブからゲートウェイ DHCPを利用するOverlay Network横の「⋮」をクリックし「編集」をクリックします。

> **補足** 対象のセグメントはDHCP サーバ プロファイルを適用したTier-1ゲートウェイに接続している必要があります。



セグメントの設定編集画面が表示されます。

10. 「DHCP構成を行う」をクリックします。

DHCP構成の設定が表示されます。

11. 以下のパラメータを入力します

項目	設定値
DHCP タイプ	「ゲートウェイ DHCP サーバ」を選択します
DHCP 構成	有効にします。
DHCP 範囲	DHCP クライアントへ払い出す IP を指定します。 IP アドレスを CIDR 形式で指定するか、範囲の開始と終了 IP アドレスを入力し、IP アドレスを範囲として入力することもできます。例：172.16.10.10-172.16.10.100
DNS サーバ	DHCP クライアントに割り当てる DNS サーバの IP アドレスを指定します。

12. 「適用」をクリックします。

DHCPの構成の設定が終了します。

13. 「保存」をクリックします。

設定内容が保存されます。

14. 「編集を終了」をクリックします。

編集画面が終了します。

6.8.2. DHCP設定の削除

本項ではゲートウェイ DHCP 設定の削除手順について記載いたします。

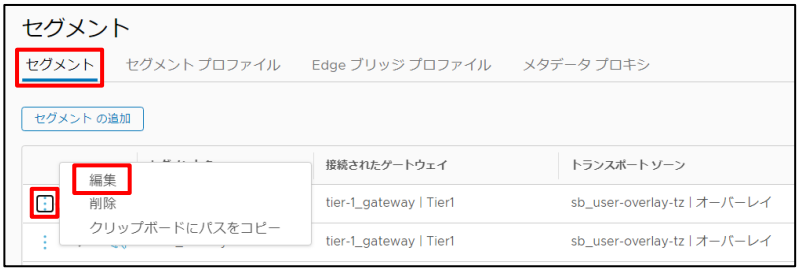
ゲートウェイDHCP設定の削除

ゲートウェイ DHCP設定の削除手順をご説明いたします。

1. NSX Managerにログインします。

2. 「ネットワーク」から「セグメント」をクリックします。

3. 「セグメント」タブから削除対象のゲートウェイDHCPを利用するOverlay Network横の「⋮」をクリックし「編集」をクリックします。



セグメントの設定編集画面が表示されます。

4. 「DHCP構成の削除」をクリックします。

DHCP構成の設定が表示されます。

5. 確認画面で「削除」をクリックします。

DHCP設定が削除されます。

6. 「保存」をクリックします。

設定内容が保存されます。

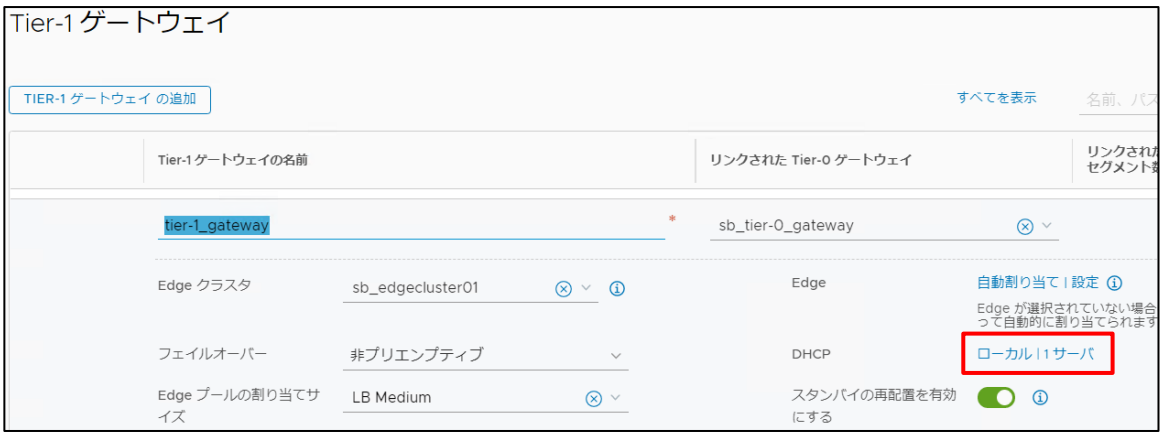
7. 「編集を終了」をクリックします。

編集画面が終了します。

8. 「Tier-1 ゲートウェイ」をクリックしゲートウェイDHCPの設定を削除するTier-1 ゲートウェイ横の「：」をクリックし「編集」をクリックします。

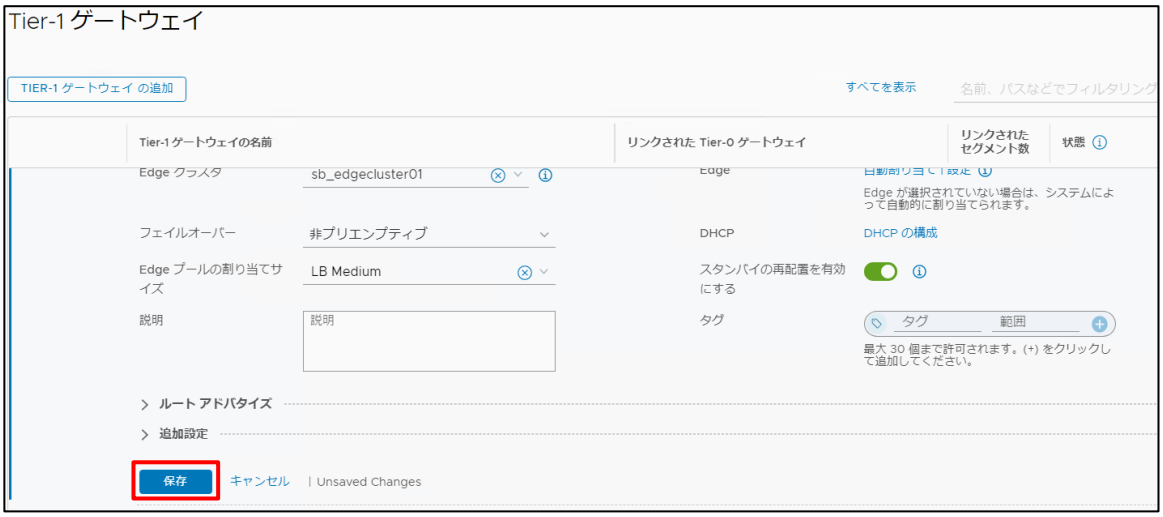
Tier-1ゲートウェイの設定編集画面が開きます。

9. 「DHCP」横の「ローカル | 1サーバ」の表示をクリックします。



10. 「タイプ」を「動的IP アドレスを割り当てない」に変更し、「保存」をクリックします。

11. 「保存」をクリックします。



設定が保存されます。

12. 「編集を終了」をクリックします。

編集画面が終了します。

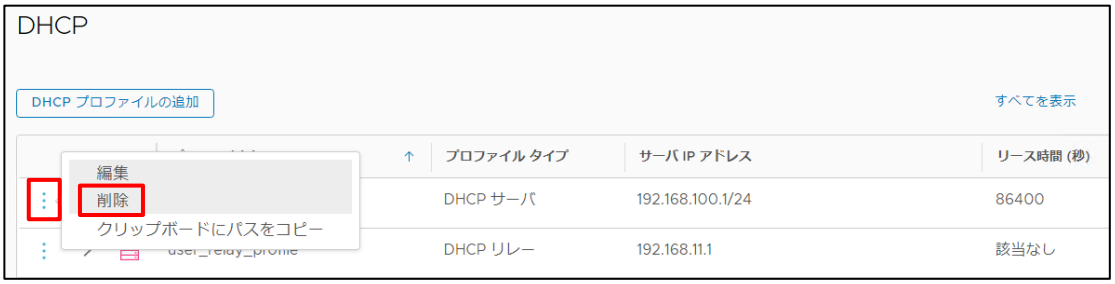
DHCPプロファイルの削除

DHCPプロファイルの削除手順をご説明いたします。

1. **NSX Managerにログインします。**

2. **「ネットワーク」から「DHCP」をクリックします。**

3. **削除対象のDHCPプロファイル横の「⋮」をクリックし「削除」をクリックします。**



確認画面が表示されます。

4. **確認画面で対象に間違いが無いことを確認し「削除」をクリックします。**

削除処理が実施されます。

5. **対象のDHCPプロファイルが一覧から削除されたことを確認します。**

6.9. ネットワーク プロファイルの操作

本サービスではネットワーク プロファイルの操作はゲートウェイ QoS プロファイルの操作のみ可能です。

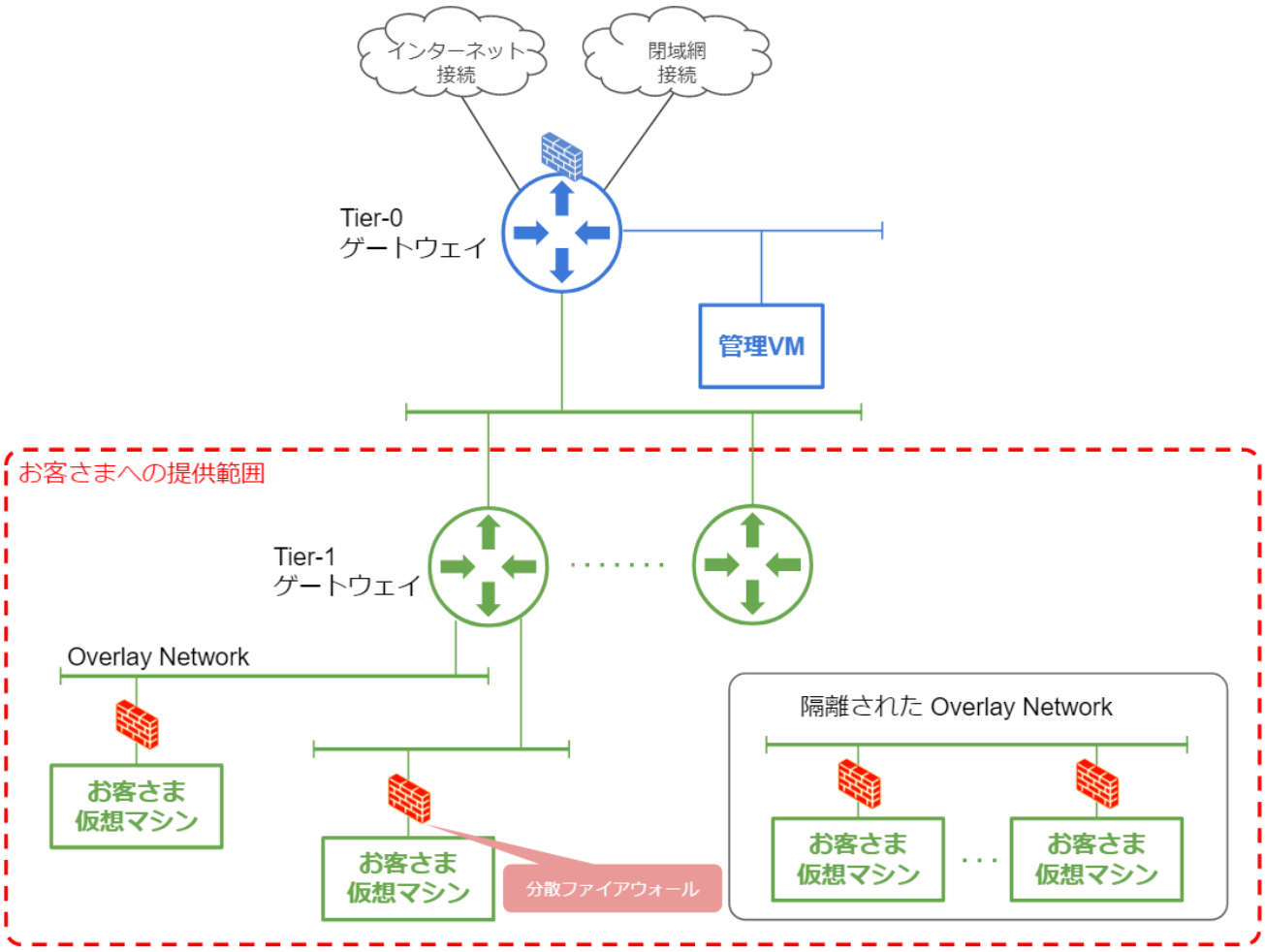
ゲートウェイQoS プロファイルにてトラフィック速度の制限を定義し、Tier-1ゲートウェイごとにトラフィックを制限することができます。

> 重要 QoS ポリシーに準拠していないトラフィックは全てドロップされます。
> 参照 『ゲートウェイ QoS プロファイルの追加 』

6.10. 分散ファイアウォールの操作

本サービスでは分散ファイアウォールが利用可能です。

分散ファイアウォールは仮想マシンのネットワークインターフェース単位でトラフィックの制御を実施することが可能です。



6.10.1. 分散ファイアウォールの設定

本項では分散ファイアウォールの設定例についてご説明いたします。

> **重要** **分散ファイアウォールルール作成時の注意事項**
>
> 分散ファイアウォールルールにて記録されたログは、お客さまにて閲覧することができません。
> また、膨大なログによりESXiサーバの動作に影響を及ぼす可能性があるため、ロギングの有効化は禁止操作となります。
>
> 参照 『ESXi hosts may experience operational issues if L2 DFW default rule logging is enabled (86355)』

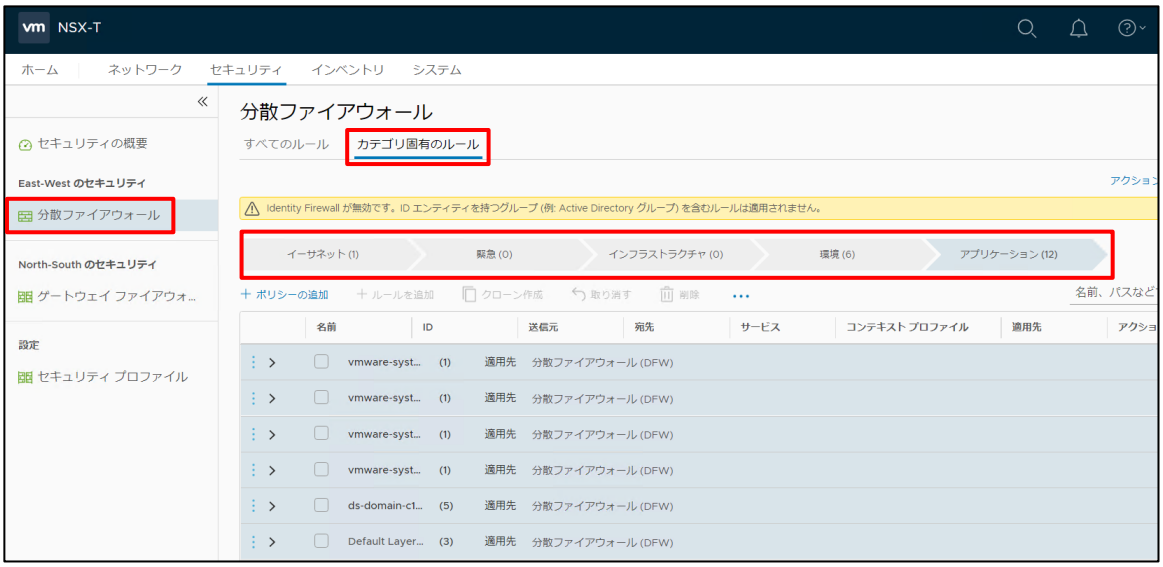
ファイアウォール ルールの追加

分散ファイアウォールの新規ルール追加手順をご説明いたします。

1. **NSX Managerにログインします。**

2. **「セキュリティ」をクリックします。**

3. 「分散ファイアウォール」をクリックし「カテゴリ固有のルール」タブを選択し、ルールを追加するカテゴリをクリックします。



重要

分散ファイアウォールのカテゴリは左から右にかけて評価され、同じカテゴリ内では上から下にかけて評価されます。カテゴリごとの説明についてはヴイエムウェア社の公式ドキュメントをご参照ください。

参照 『分散ファイアウォール』

補足

以下の警告は Identity Firewall を無効にしているため表示されています。

本サービスでは Identity Firewall の利用はできないため、こちらの警告については無視してください。

4. 「ポリシーの追加」をクリックします。

新規ポリシーが追加されます。

> **補足** 既存のポリシーにルールを追加する場合は、ポリシーの追加は不要です。

5. 新規ポリシーに任意の名前を設定します。

6. 設定対象のポリシー横の「⋮」を選択し「ルールを追加」をクリックします。

新規ルールが追加されます。

7. ルールを設定します。

ポリシーやルールの設定は「発行」をクリックするまで有効になりません。

補足

送信元や適用先のグループやサービスの定義などはお客さまにて作成いただくことが可能です。

参照 「6.13 インベントリの操作」

分散ファイアウォールのルール設定についての詳細な説明は、ヴイエムウェア社の公式ドキュメントをご参照ください。

参照 『分散ファイアウォールの追加』

重要

分散ファイアウォールのデフォルトの適用先「分散ファイアウォール(DFW)」は、設定したルールが全ての仮想マシンのネットワークインターフェースに対して適用されます。

仮想マシンのネットワークインターフェースには、ルール設定数の上限があります。
上限値を超えるようなルールを作成する可能性がある場合は、適用先をグループで定義して不要なルールが適用されないようにご注意ください。

製品の上限値については、ヴイエムウェア社の公開情報をご参照ください。

参照 「各製品の構成の上限について」

8. ルールの設定が完了したら「発行」をクリックします。

分散ファイアウォールの設定が更新されます

9. 設定を実施したポリシーのステータスが「成功」となったことを確認します。

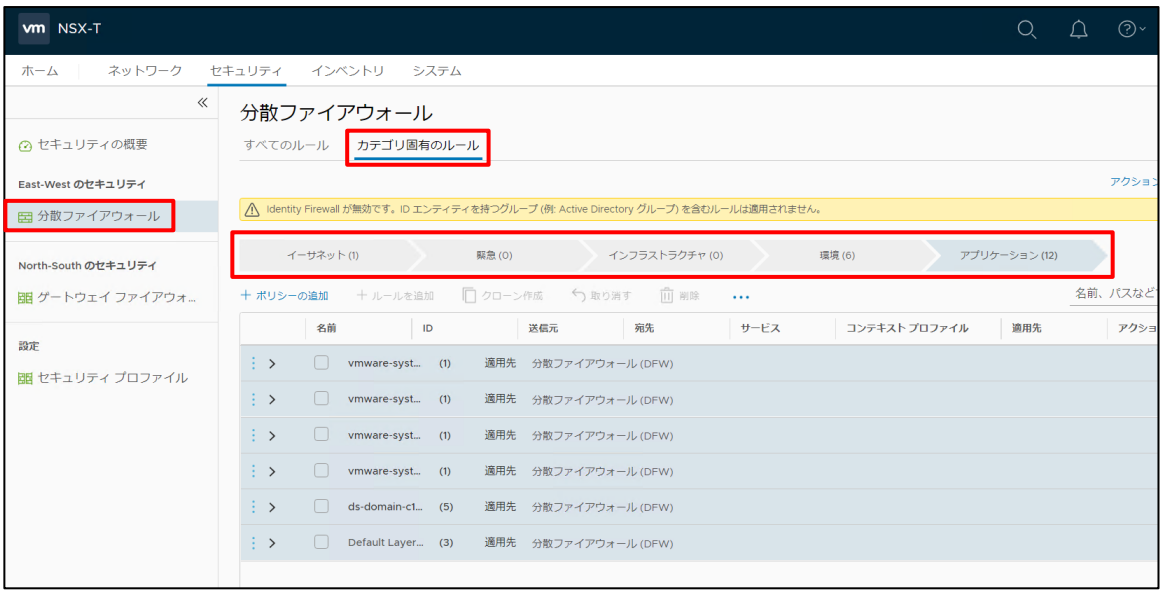
ファイアウォール ルールの削除

分散ファイアウォールのルール削除手順をご説明いたします。

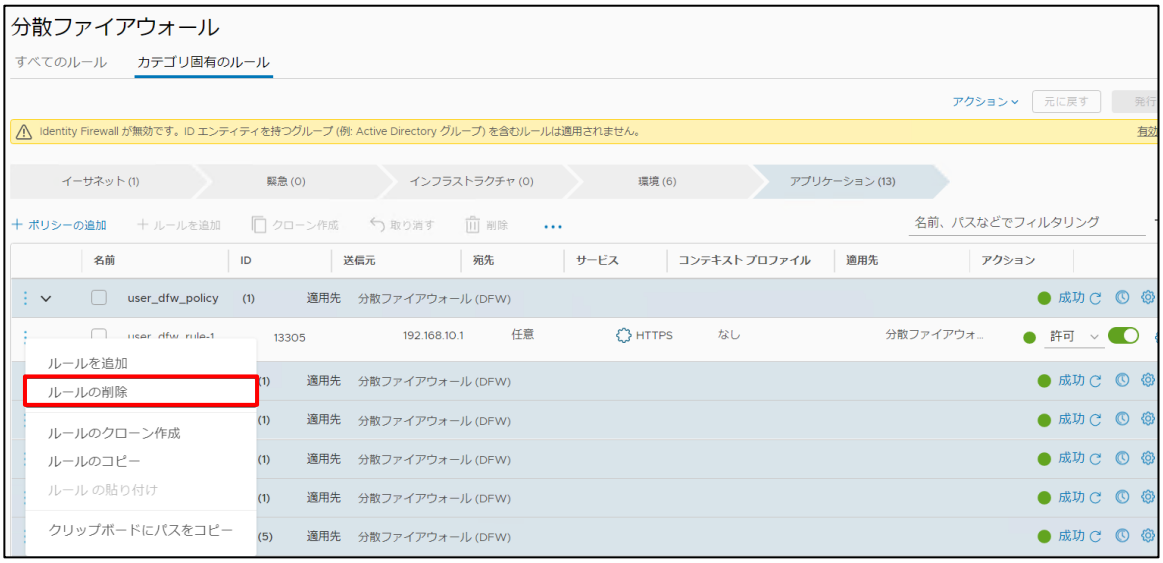
1. NSX Managerにログインします。

2. 「セキュリティ」をクリックします。

3. 「分散ファイアウォール」をクリックし「カテゴリ固有のルール」タブを選択し、削除対象のルールが存在するカテゴリをクリックします。



4. 削除対象のルール横の「⋮」をクリックし「ルールの削除」をクリックします。



対象のルールが画面上から削除されますが、「発行」をクリックするまで反映されません。

> **補足** ポリシーを削除すると紐づくルールが全て削除されます。

5. ルールの削除が完了したら「発行」をクリックします。

分散ファイアウォールの設定が更新されます。

6. ルールが削除され設定を実施したポリシーのステータスが「成功」となったことを確認します。

6.10.2. ドラフトの操作

ドラフトとは、特定時点での分散ファイアウォールの設定を保存したものです。
デフォルトではドラフトの自動保存が有効になっており、設定を発行するたびに自動でドラフトが作成されます。また、手動でドラフトを保存することも可能です。
保存したドラフトをロードすることでドラフト保存時の設定に戻すことができます。

> **補足** 最大で 100 個の自動ドラフトと 10 個の手動ドラフトが保存可能です。

ドラフトの確認

保存されているドラフトの確認手順についてご説明いたします。

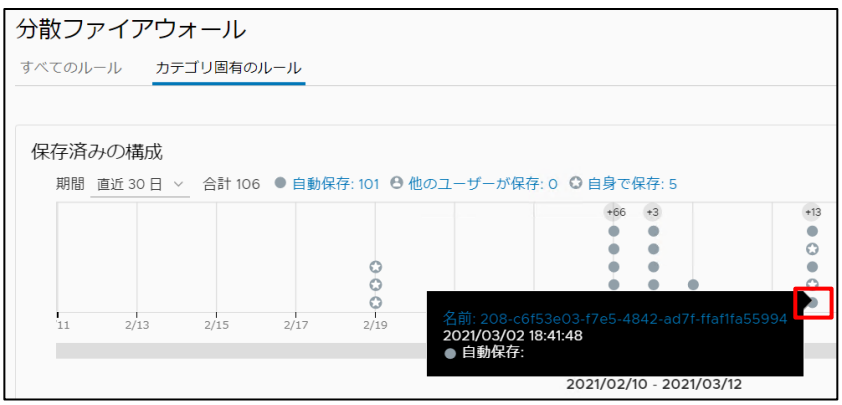
1. **NSX Managerにログインします。**

2. **「セキュリティ」から「分散ファイアウォール」をクリックします。**

3. **「アクション」から「表示」をクリックします。**

ドラフトの一覧が表示されます。

4. **内容を確認したいドラフトにカーソルを合わせて名前クリックします。**



対象のドラフトの詳細が表示されます。

5. ドラフトの内容を確認します。

ドラフトの手動保存

ドラフトを手動で保存する手順についてご説明いたします。

1. NSX Managerにログインします。

2. 「セキュリティ」から「分散ファイアウォール」をクリックします。

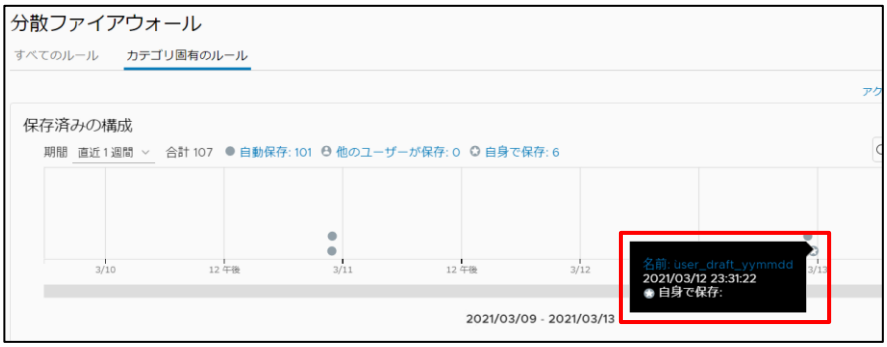
3. 「アクション」から「保存」をクリックします。

ドラフトの保存画面が表示されます。

4. ドラフトの情報を入力し「保存」をクリックします。

ドラフトが保存されます。

5. ドラフトが保存されたことを確認します。



ドラフトのロード

保存してあるドラフトから設定をロードする手順についてご説明いたします。

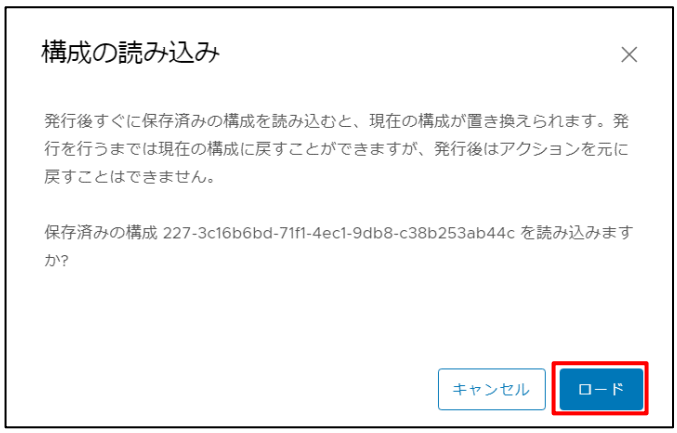
1. 「ドラフトの確認」を参照しロード対象のドラフトを選択します。

2. 「ロード」をクリックします。

確認画面が表示されます。

> **補足** 「ドラフトの変更」の項にはロードを実行した際の変更内容が表示されています。
> 内容を確認の上ロードを実施してください。

3. 「ロード」をクリックします。



ロードしたドラフトの設定に合わせて分散ファイアウォールの設定が変更されます。

(発行をするまで設定は反映されません)

4. 「発行」をクリックします

分散ファイアウォールの設定変更が反映されます。

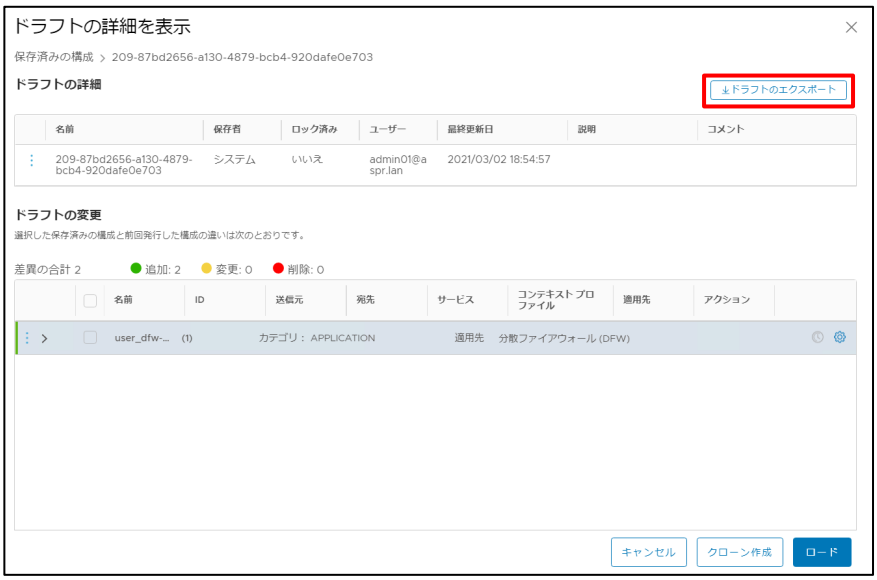
5. 設定が変更されたポリシーのステータスが「成功」となったことを確認します。

ドラフトのエクスポート

ドラフトをエクスポートする手順についてご説明いたします。
保存したドラフトをエクスポートすることでファイルとして外部に保存することができます。

1. 「ドラフトの確認」を参照しエクスポート対象のドラフトを選択します。

2. 「ドラフトのエクスポート」をクリックします。



ファイアウォール ドラフトのエクスポートが表示されます。

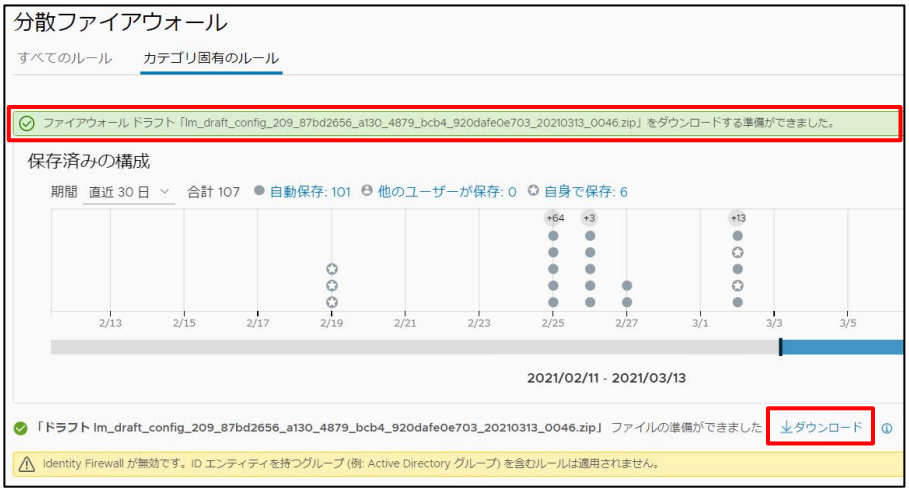
3. 任意のパスフレーズを指定し「エクスポート」をクリックします。

ドラフトのエクスポート処理が実施されます。

4. 「キャンセル」をクリックしドラフトの詳細画面を閉じます。

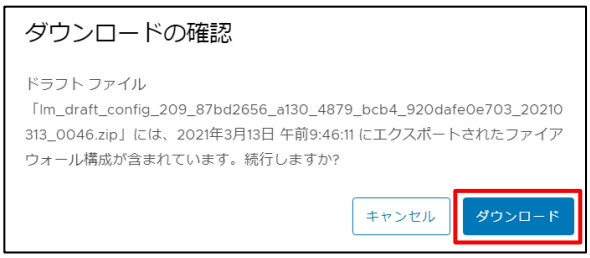
5. ドラフトのダウンロードする準備ができましたというメッセージを確認し、「ダウンロード」をクリックします。

メッセージが表示されない場合はF5キーなどブラウザの画面更新を実施して表示されるかご確認ください。



ダウンロードの確認画面が表示されます。

6. 「ダウンロード」をクリックします。



ファイルがダウンロードされます。(保存先などはブラウザの設定に依存します)

ドラフトのインポート

ドラフトのインポート手順についてご説明いたします。

ドラフトのインポートではエクスポートしたドラフトや、FW構成をドラフトとして登録することができます。

1. NSX Managerにログインします。

2. 「セキュリティ」から「分散ファイアウォール」をクリックします。

3. 「アクション」から「インポート」をクリックします。

ドラフトのインポート画面が表示されます。

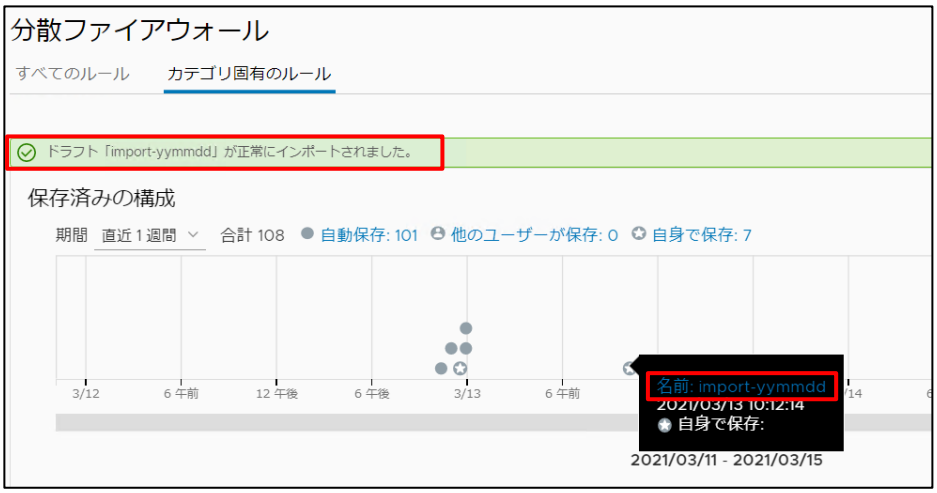
4. 以下のパラメータを入力します。

項目	設定値
ファイルの選択	「参照」をクリックしインポートするファイルを選択します。
パスフレーズ	ファイルをエクスポートする際に指定したパスフレーズを入力します。 パスフレーズが間違っている場合インポートが失敗します。
名前	任意の名前を入力します。
説明	任意の説明を入力します。

5. 「インポート」をクリックします。

エクスポートした内容がインポートされ、ドラフトとして登録されます。

6. **「正常にインポートされました」と表示されることを確認し、指定した名前でドラフトとして登録されていることを確認します。**



補足 登録されたドラフトは、自動保存したものなどと同様の操作でロードなどが出来ます。

6.10.3. 全般設定

分散ファイアウォールの全般設定の設定手順についてご説明いたします。

分散ファイアウォールの全般設定では、分散ファイアウォール全体の無効化やドラフトの自動保存の無効化ができます。

1. **NSX Managerにログインします。**

2. **「セキュリティ」から「分散ファイアウォール」をクリックします。**

3. **「アクション」から「全般設定」をクリックします。**

全般設定の設定画面が表示されます。

4. **全般設定の設定をし「保存」をクリックします。**

補足 本サービスでは ID ファイアウォールは利用できません。

6.10.4. 除外リストの設定

除外リストの設定手順についてご説明いたします。

除外リストに登録されたグループは分散ファイアウォール ルールの適用から除外されます。

除外リストに登録できるのはグループのみで、またグループの設定で「IP セット」、「MAC セット」、「Active Directory グループ」が設定されている場合は、ファイアウォール除外リストに追加できません。

グループの操作について下記手順をご参照ください。

参照 「6.13.2 グループの設定」

1. **NSX Managerにログインします。**

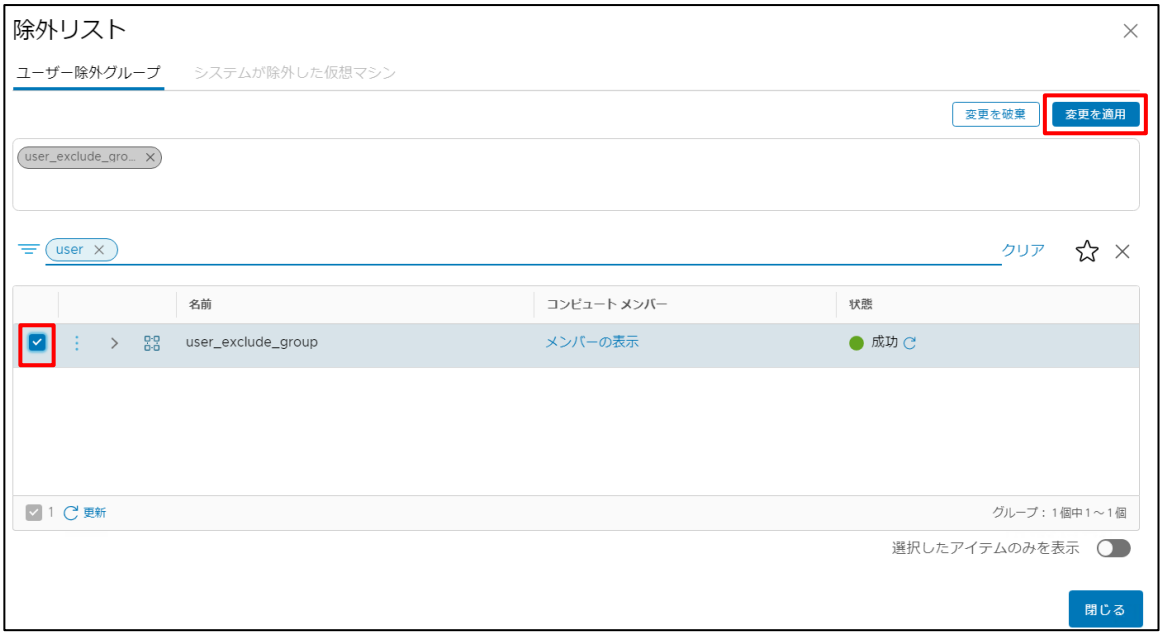
2. **「セキュリティ」から「分散ファイアウォール」をクリックします。**

3. **「アクション」から「除外リスト」をクリックします。**

除外リストの設定画面が表示されます。

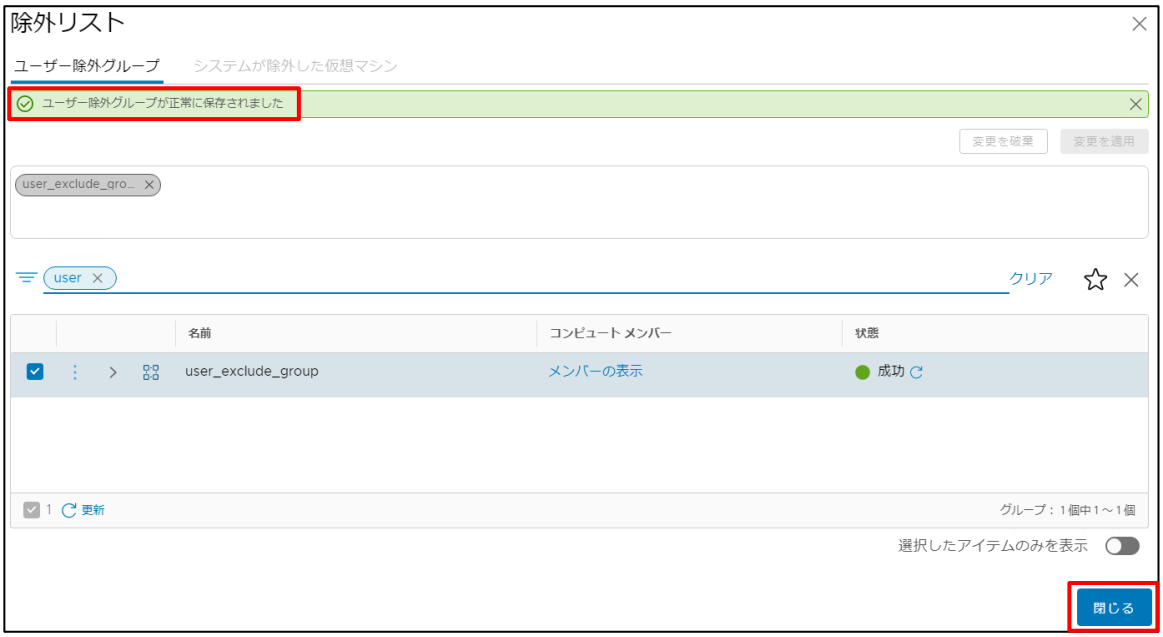
4. 除外したいグループにチェックを入れ、「変更を適用」をクリックします。

除外リストから削除したい場合はチェックを外すか、上部の登録されているグループの表示から×をクリックします。



除外リストの設定が更新されます。

5. 「正常に保存されました」と表示されたことを確認し「閉じる」をクリックします。

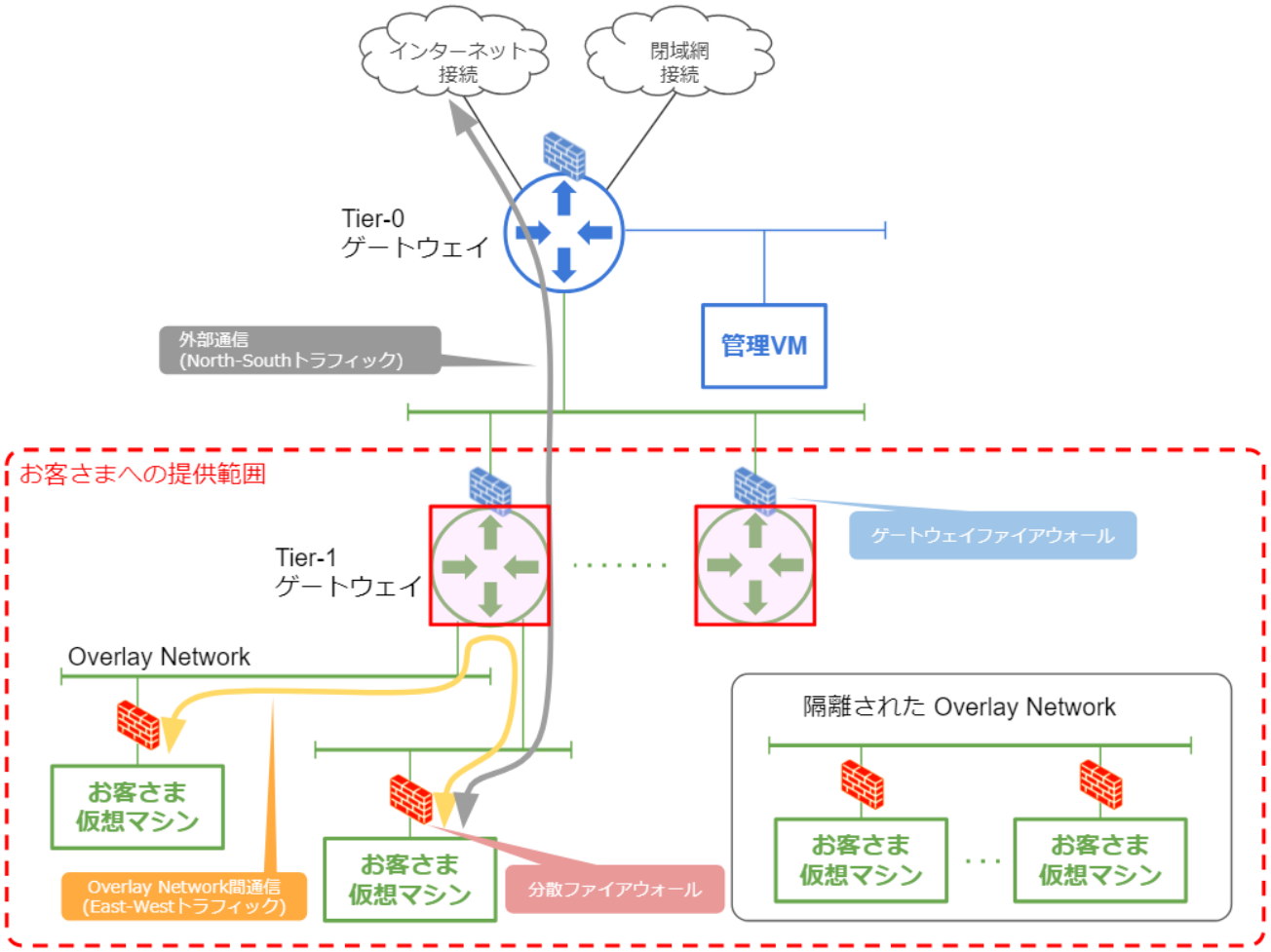


除外リストの設定画面が閉じます。

6.11.ゲートウェイ ファイアウォールの操作

ゲートウェイ ファイアウォールは Tier-0 / Tier-1 ゲートウェイ自体、もしくは Tier-0 ゲートウェイのアップリンクに対して適用でき、適用先を通るトラフィックに対して制御を実施します。

本サービスでは Tier-1 ゲートウェイを対象としたゲートウェイ固有のルールのみ利用可能です。



補足 NSX-T の Overlay Network 間の通信は分散ファイアウォールをご利用ください。
同一 Tier-1 ゲートウェイに接続されている Overlay Network 同士の通信ではネットワークが異なっていても、接続している Tier-1 ゲートウェイのゲートウェイ ファイアウォールのルールが適用されません。

重要 サービス開始時点で当社管理上のFWルールを設定しています。これらのルールのお客さまによる設定変更、削除などは禁止操作となります。
参照 「2.2.7 ゲートウェイ ファイアウォール」

6.11.1. ゲートウェイ ファイアウォールの設定

本項ではゲートウェイ ファイアウォールの設定例についてご説明いたします。

> **重要** **既知の不具合について**
>
> 異なるゲートウェイに同じ名称のゲートウェイ ファイアウォール ポリシーを作成すると、「General error has occurred」というポップアップが表示され、ゲートウェイ ファイアウォールの設定画面が操作出来なくなります。
>
> 本事象が発生した場合には、REST APIによる削除操作が必要となります。
>
> 参照 『When accessing gateway firewall rules in NSX-T manager you encounter “General error has occurred” (84464)』

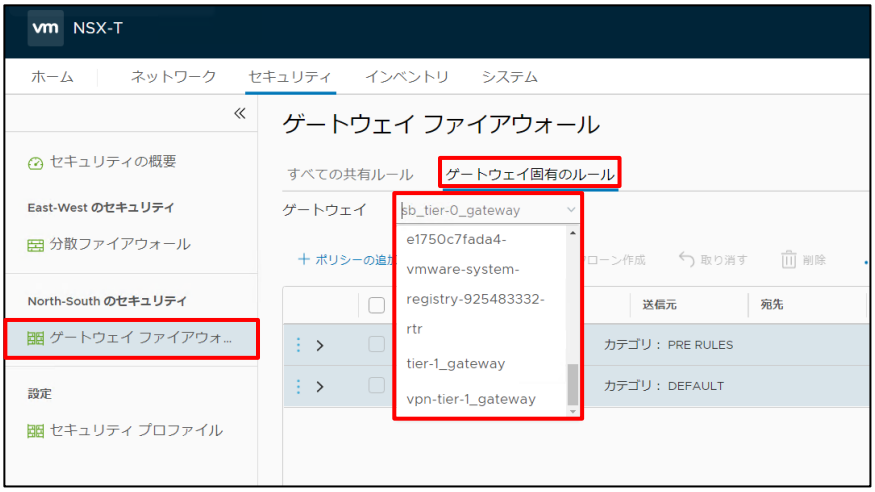
ゲートウェイ ファイアウォール ルールの追加

ゲートウェイ ファイアウォールの新規ルール追加手順をご説明いたします。

1. **NSX Managerにログインします。**

2. **「セキュリティ」をクリックします。**

3. **「ゲートウェイ ファイアウォール」をクリックし「ゲートウェイ固有のルール」タブから、ルールを追加するゲートウェイを選択します。**



> **重要** Tier-0 ゲートウェイへのルール追加は禁止操作となります。

4. 「ポリシーの追加」をクリックします。

新規ポリシーが追加されます。

補足 既存のポリシーにルールを追加する場合は、ポリシーの追加は不要です。

5. 新規ポリシーに任意の名前を設定します。

6. 設定対象のポリシー横の「：」を選択し「ルールを追加」をクリックします。

新規ルールが追加されます。

補足 ゲートウェイ ファイアウォールのルールは上から下にかけて評価されます。

7. ルールを設定します。

ポリシーやルールの設定は「発行」をクリックするまで有効になりません。

> **補足** 送信元や適用先のグループやサービスの定義などはお客さまにて作成いただくことが可能です。
> 参照 「6.13 インベントリの操作」

8. ルールの設定が完了したら「発行」をクリックします。

ゲートウェイ ファイアウォールの設定が更新されます

9. 設定を実施したポリシーのステータスが「成功」となったことを確認します。

ゲートウェイ ファイアウォール ルールの削除

ゲートウェイ ファイアウォールのルール削除手順をご説明いたします。

1. NSX Managerにログインします。

2. 「セキュリティ」をクリックします。

3. 「ゲートウェイ ファイアウォール」をクリックし「ゲートウェイ 固有のルール」タブから、対象のルールが設定されているTier-1 ゲートウェイを選択します。

4. 削除対象のルール横の「⋮」をクリックし「ルールの削除」をクリックします。

対象のルールが削除されますが、「発行」をクリックするまで反映されません。

> **補足** ポリシーを削除すると紐づくルールが全て削除されます。
> また、ポリシー内のルールが全て削除されるとポリシーも合わせて削除されます。

5. ルールの削除が完了したら「発行」をクリックします。

ゲートウェイ ファイアウォールの設定が更新されます。

6. ルールが削除され設定を実施したポリシーのステータスが「成功」となったことを確認します。

ゲートウェイ ファイアウォール ルール 補足

ゲートウェイ ファイアウォールから 「すべての共有ルール」を選択すると分散ファイアウォール同様カテゴリが確認できます。

本サービスでは「ゲートウェイ 固有のルール」以外で「システム」カテゴリなど設定によって自動で設定されるものを除き、お客さまにて設定を実施されるのは禁止操作となります。

補足 当社で事前に設定しているルールは「事前ルール」に定義しています。

重要 「ゲートウェイ 固有のルール」以外の「システム」カテゴリなど、設定によって自動で設定されるものを除き、お客さまにて設定を実施されるのは禁止操作となります。

6.12. セキュリティ プロファイルの操作

セキュリティプロファイルはファイアウォールの動作を調整するプロファイルとなります。

本項ではセキュリティ プロファイルの操作についてご説明いたします。

6.12.1. セッション タイマー プロファイルの作成

セッション タイマー プロファイルの作成手順についてご説明いたします。

セッション タイマーは、セッションが非アクティブ状態になった後にファイアウォールでそのセッションが保持される期間を定義します。

1. **NSX Managerにログインします。**

2. **「セキュリティ」をクリックします。**

3. **「セキュリティ プロファイル」をクリックし「セッション タイマー」タブから「プロファイルの追加」をクリックします。**

セッション タイマー プロファイルの作成画面が表示されます。

各パラメータの値を入力し、「保存」をクリックします。
プロファイル適用先を設定する場合は、「適用先」の「設定」ボタンをクリックして設定してください。

セッションタイマープロファイルが作成されます。

補足

セッション タイマー プロファイルに設定する各パラメータはヴイエムウェア社の公式ドキュメントをご参照ください。

参照 『セッション タイマーの作成』

重要

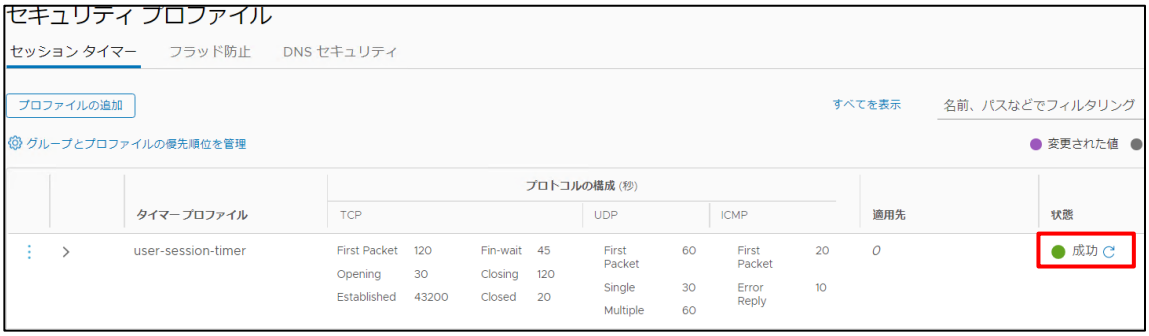
セッション タイマーをデフォルト値より長くする場合は「適用先」の設定時にTier-0ゲートウェイ(sb_tier-0_gateway)も含めるようにしてください。

Tier-0 ゲートウェイに関わる設定になりますが、本設定については、例外的にお客さまに実施いただいて問題ありません。

Tier-0 ゲートウェイを含めないとTier-1ゲートウェイ側のセッション タイマーによる切断より先に経路上のTier-0ゲートウェイ側のデフォルトのセッション タイマーによりセッションが切断されてしまいます。

参照 『セッション タイマーのデフォルト値』

4. **作成したセッション タイマー プロファイルの状態が「成功」になることを確認します。**



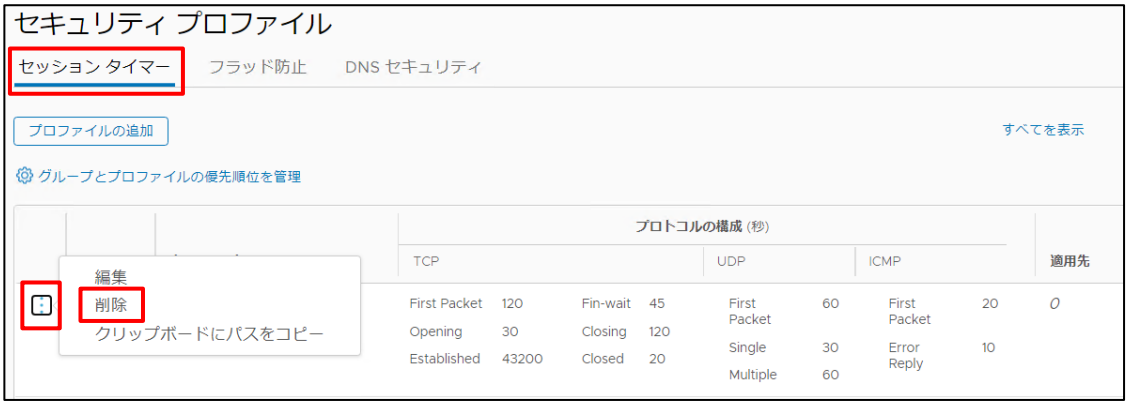
6.12.2. セッション タイマー プロファイルの削除

セッション タイマー プロファイルの削除手順についてご説明いたします。

1. **NSX Managerにログインします。**

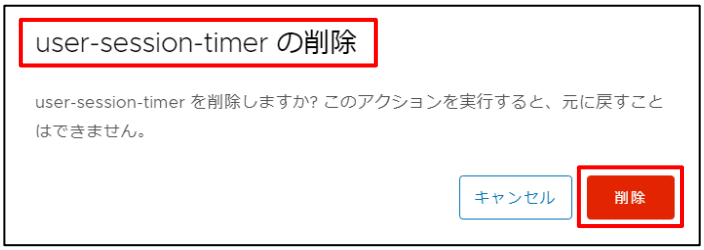
2. **「セキュリティ」から「セキュリティ プロファイル」をクリックします。**

3. **「セッション タイマー」タブから削除対象のセッション タイマー プロファイル横の「⋮」をクリックし「削除」をクリックします。**



確認画面が表示されます。

4. 確認画面で対象に間違いが無いことを確認し「削除」をクリックします。



削除処理が実施されます。

5. 対象のセッションタイマー プロファイルが一覧から削除されたことを確認します。

6.12.3. フラッド防止 プロファイルの作成

フラッド防止 プロファイルの作成手順についてご説明いたします。

フラッド防止はサービス拒否 (DDoS) 攻撃に対する保護に役立ちます。フラッド防止プロファイルを作成すると、ICMP、UDP、ハーフオープンの TCP フローに対してアクティブなセッション制限を適用できます。

1. **NSX Managerにログインします。**

2. **「セキュリティ」から「セキュリティ プロファイル」をクリックします。**

3. **「フラッド防止」タブから「プロファイルの追加」をクリックし適用対象に合わせ「Edge ゲートウェイ プロファイルの追加」か「ファイアウォール プロファイルの追加」を選択します。**

フラッド防止 プロファイルの作成画面が表示されます。

4. 各パラメータの値を入力します。
プロファイル適用先を設定する場合は、「適用先」の「設定」ボタンをクリックして設定してください。
入力完了後、「保存」をクリックします。

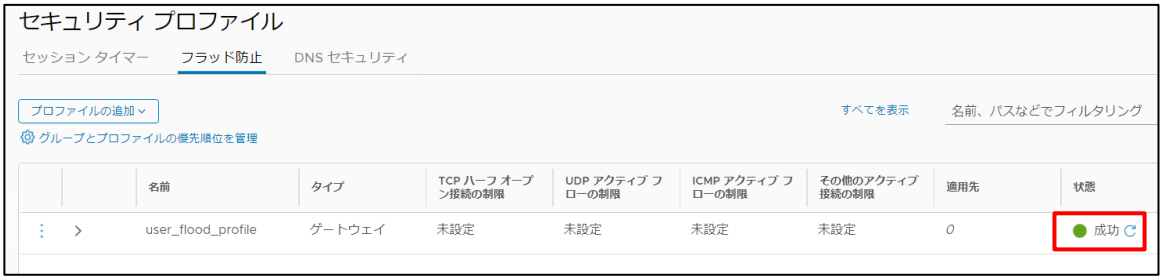
以下Edge ゲートウェイプロファイルの作成画面となります

フラッド防止 プロファイルが作成されます。

> **補足** フラッド防止プロファイルに設定する各パラメータはヴイエムウェア社の公式ドキュメントをご参照ください。
> **参照** 『フラッド防止』

> **重要** フラッド防止プロファイルのパラメータをデフォルト値より大きくする場合は「適用先」の設定時にTier-0ゲートウェイ(sb_tier-0_gateway)も含めるようにしてください。
> Tier-0 ゲートウェイに関わる設定になりますが、本設定については、例外的にお客さまに実施いただいて問題ありません。

5. 作成したフラッド防止 プロファイルの状態が「成功」になることを確認します。



6.12.4. フラッド防止 プロファイルの削除

フラッド防止 プロファイルの削除手順についてご説明いたします。

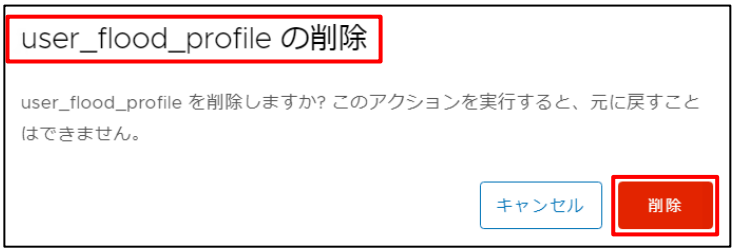
1. **NSX Managerにログインします。**

2. **「セキュリティ」から「セキュリティ プロファイル」をクリックします。**

3. **「フラッド防止」タブからから削除対象のフラッド防止 プロファイル横の「⋮」をクリックし「削除」をクリックします。**

確認画面が表示されます。

4. **確認画面で対象に間違いが無いことを確認し「削除」をクリックします。**



削除処理が実施されます。

5. **対象のフラッド防止 プロファイルが一覧から削除されたことを確認します。**

6.13.インベントリの操作

インベントリの操作についてご説明いたします。

インベントリではファイアウォールなどで利用する、サービスやグループの定義を作成、編集することができます。

6.13.1. サービスの設定

本項ではサービスの設定についてご説明いたします。

サービスとは、プロトコルとポートの組合せの定義で、NSX-T のオブジェクトとして登録しておくことで、ファイアウォールや NAT などの設定時に定義名を指定して利用することが可能になります。

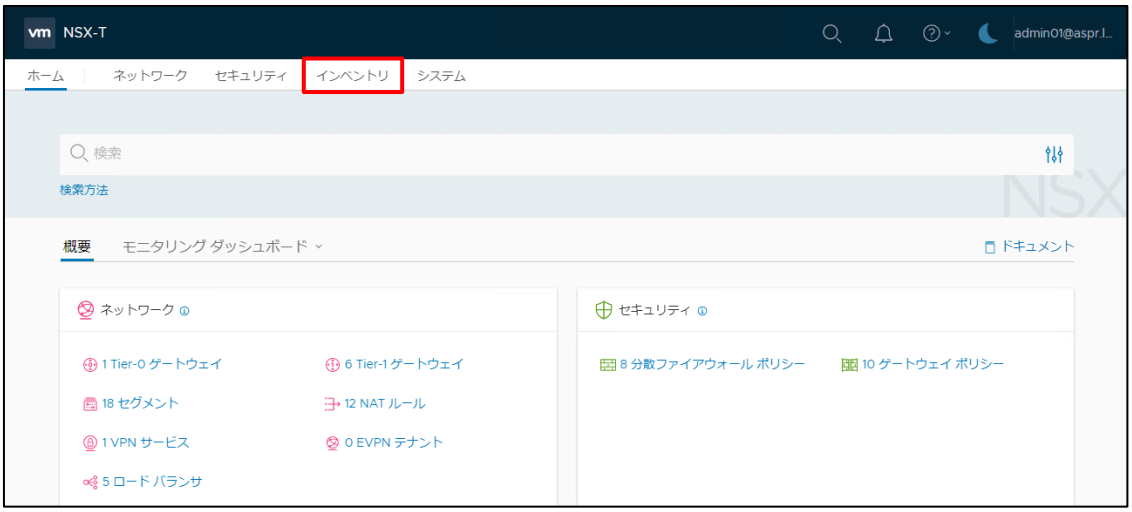
デフォルトで定義されているサービス以外にお客さま固有の定義を作成することができます。

サービスの作成

サービス定義の作成手順についてご説明いたします。

1. NSX Managerにログインします。

2. 「インベントリ」をクリックします。



3. 「サービス」をクリックし「サービスの追加」クリックします。

サービスの追加画面が表示されます。

4. 任意の名前を入力し「サービス エントリの設定」をクリックします。

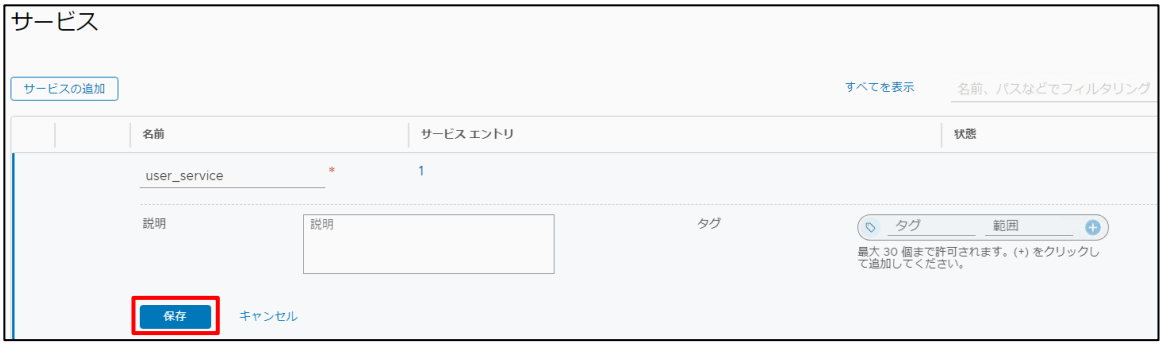
サービスエントリの設定画面が表示されます。

5. サービスの定義を入力し「適用」をクリックします。

以下TCPの宛先ポート 443と9443 を指定したサービスの定義の例です。

サービス エントリの設定が適用されます。

6. 「保存」をクリックします。



サービスの定義が作成されます。

7. 作成したサービスの状態が「成功」になることを確認します。

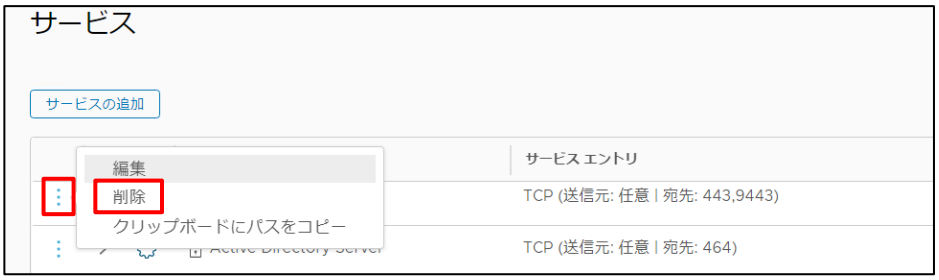
サービスの削除

サービス定義の削除手順についてご説明いたします。

1. **NSX Managerにログインします。**

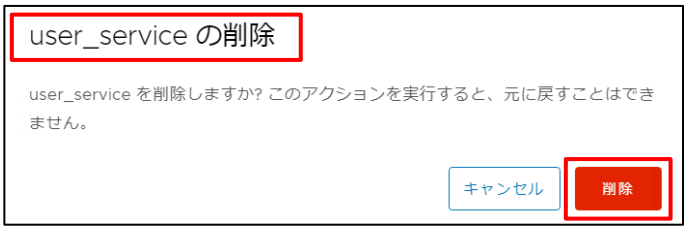
2. **「インベントリ」から「サービス」をクリックします。**

3. **削除対象のサービス横の「⋮」をクリックし「削除」をクリックします。**



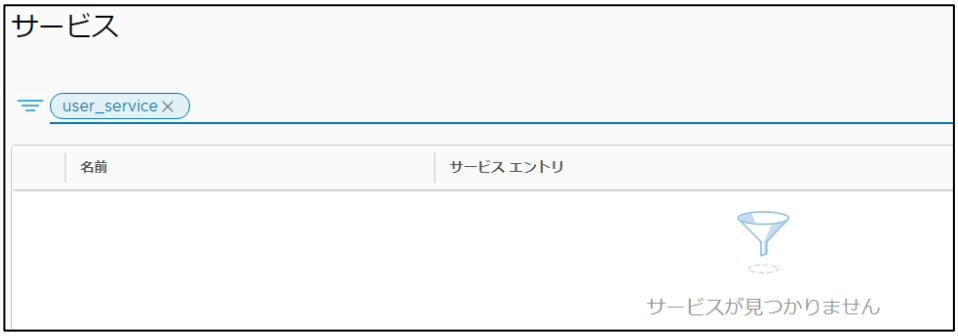
確認画面が表示されます。

4. **確認画面で対象に間違いが無いことを確認し「削除」をクリックします。**



削除処理が実施されます。

5. **対象のサービスが一覧から削除されたことを確認します。**



6.13.2. グループの設定

本項ではグループの設定についてご説明いたします。

IP アドレスや仮想マシン、セグメントなどを組み合わせてグループとして定義し、グループに対してファイアウォールの設定などを実施することができます。

> **重要** **既知の不具合について**
>
> グループ作成時のメンバーの設定で「メンバーシップの基準」に「IPセット」を指定すると、ESXiホストにてPSODが発生する可能性がある不具合があります。そのため「IPセット」は使用しないでください。
>
> 参照 『VMware KB :ESXi host fails with PSOD "#PF Exception 14 in world xxxx:vmnic0-pollW IP" during vMotions in an NSX-T Environment (88415)』

グループの作成

グループ定義の作成手順についてご説明いたします。

1. **NSX Managerにログインします。**

2. **「インベントリ」をクリックします。**

3. **「グループ」をクリックし「グループの追加」クリックします。**

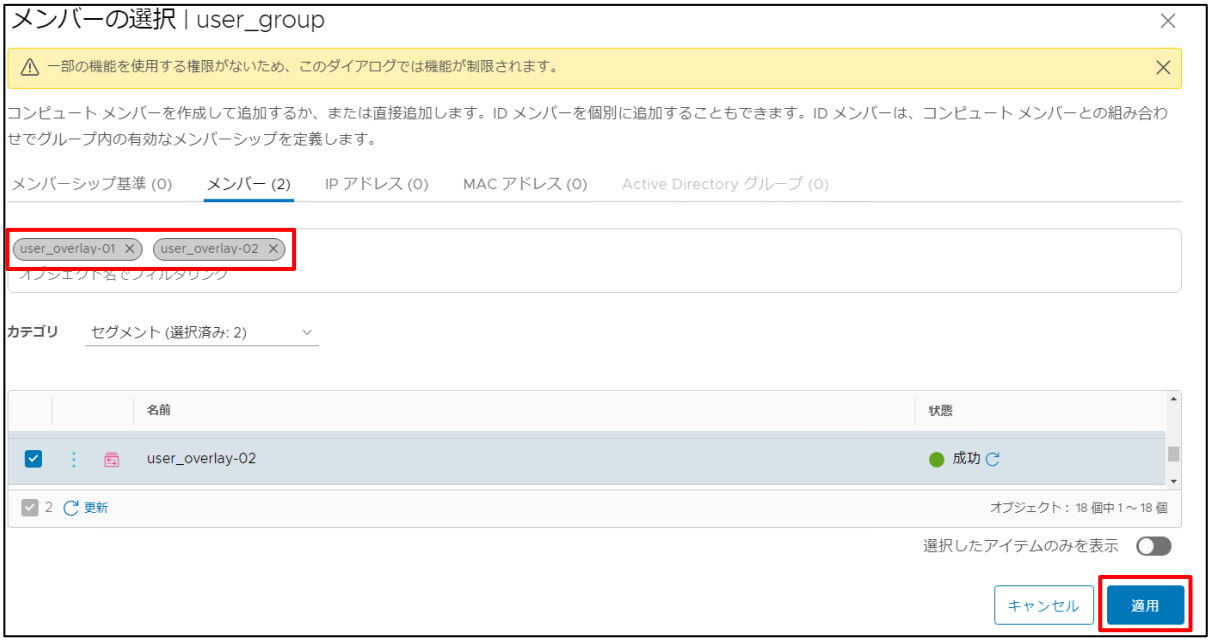
グループの追加画面が表示されます。

4. 任意の名前を入力し「メンバーの設定」をクリックします。

メンバーの設定画面が表示されます。

5. メンバーを追加し「適用」をクリックします。

以下Overlay Networkを2つメンバーとして登録した際の例です。



メンバーの設定が適用されます。

重要

NSX Manager上では当社管理VMが参照でき、グループのメンバー候補に表示されますが
メンバーに含めないでください。

当社の管理VMの仮想マシン名は「sb_」あるいは「SB_」で始まるものになります。

6. 「保存」をクリックします。

グループが作成されます。

7. 作成したグループの状態が「成功」になることを確認します。

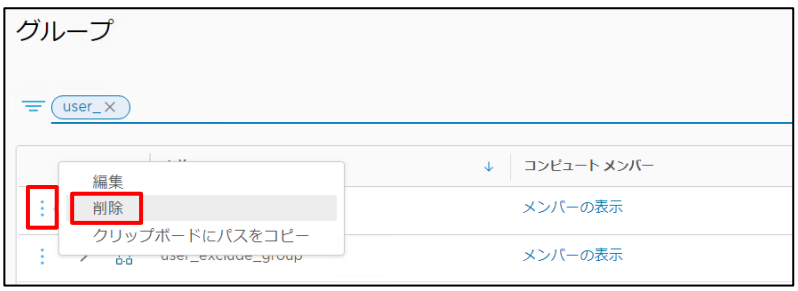
グループの削除

グループの削除手順についてご説明いたします。

1. NSX Managerにログインします。

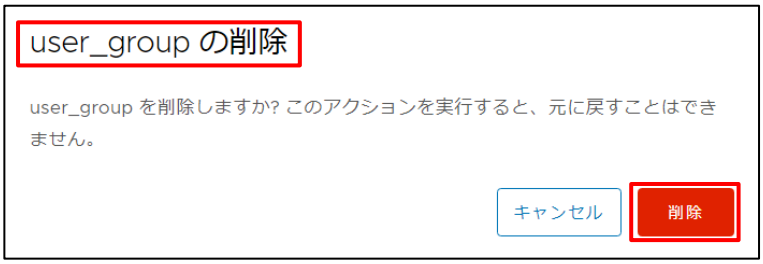
2. 「インベントリ」から「グループ」をクリックします。

3. 削除対象のグループ横の「⋮」をクリックし「削除」をクリックします。



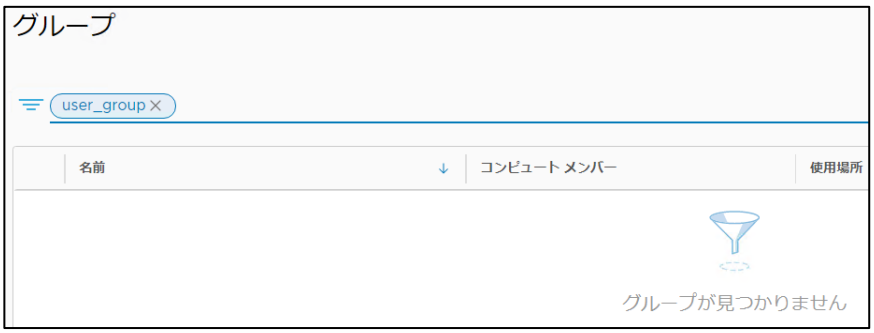
確認画面が表示されます。

4. 確認画面で対象に間違いが無いことを確認し「削除」をクリックします。



削除処理が実施されます。

5. 対象のグループが一覧から削除されたことを確認します。



6.13.3. 仮想マシンの設定

「仮想マシン」の画面からは仮想マシンへのタグの設定が可能です。

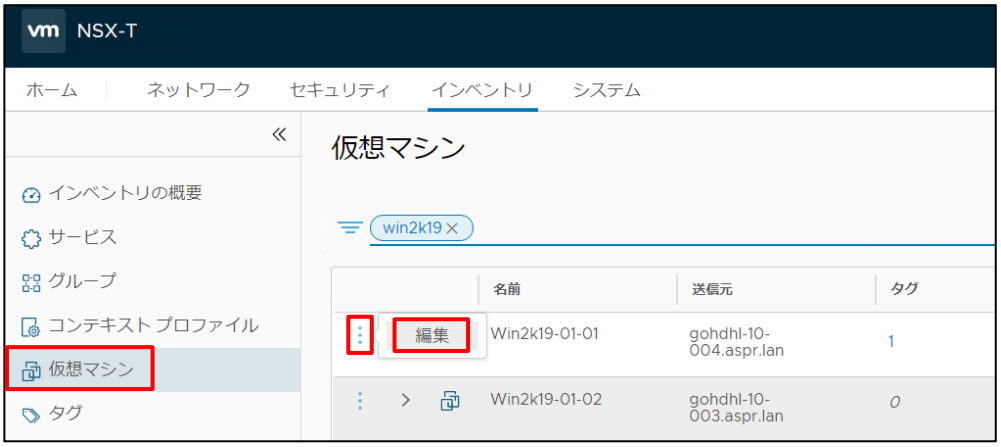
仮想マシンの情報はNSX ManagerとvCenterが連携しvCenter上の仮想マシンが自動で登録されます。

参照 「6.13.4 タグの設定」

1. **NSX Managerにログインします。**

2. **「インベントリ」をクリックします。**

3. **「仮想マシン」から操作対象仮想マシン横の「⋮」をクリックし「編集」をクリックします。**



編集画面が表示されます。

重要

NSX Manager上では当社管理VMが参照できますが、これら管理VMへのタグ付けは実施しないでください。

当社の管理VMの仮想マシン名は「sb_」あるいは「SB_」で始まるものになります。

4. タグの付与、または削除をし「保存」をクリックします。

タグの付与は「タグ」をクリックし一覧から対象のタグを選択し「+」をクリックします。

存在しないタグの名前を指定して「＋」をクリックすると、タグを作成することが出来ます。

タグの削除は付与されているタグ横の「×」をクリックします。

設定が保存されます。

5. 対象仮想マシンの「タグ」下の数字をクリックしタグが付与されたことを確認します。

6.13.4. タグの設定

本項ではタグの作成手順についてご説明いたします。

NSX環境ではオブジェクトにタグを付けることができ、これによりオブジェクトの検索やフィルタリング、トラブルシューティングやトレースなどのタスクをすばやく実行できます。

タグは各オブジェクト設定画面の「タグ」から追加することもできます。

補足 **タグの削除について**

- 本項の「タグ」から追加したタグは割り当て先が無くなった後、5日後に自動で削除されます(手動での削除ができません)。
- 各オブジェクトの設定画面(「6.13.3 仮想マシンの設定」など)で作成したタグは、そのタグを利用しているオブジェクトが無くなるとただちに自動で削除されます。

参照 『VMware KB：割り当てられている仮想マシンが 0 個の NSX-T タグを削除できない』

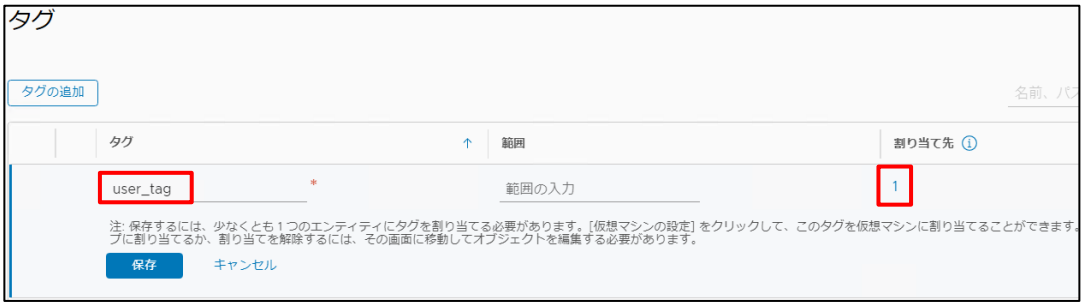
1. **NSX Managerにログインします。**

2. **「インベントリ」をクリックします。**

3. **「タグ」をクリックし「タグの追加」をクリックします。**

タグの作成画面が表示されます。

4. タグの名前と割り当て先仮想マシンを設定し「保存」をクリックします。



タグが作成されます。

> **補足** この設定画面からタグを追加できる対象は「仮想マシン」のみです。
> ほかのオブジェクト(セグメント、Tier-1ゲートウェイ など)にタグを追加したい場合は、対象オブジェクトの「編集」から実施します。

5. 作成したタグの前回の割り当て状態が「成功」になることを確認します。

6.14. 当社作成済みグループの編集

当社にてサービス開通時点で作成しているグループの編集についてご説明いたします。

当社サービス開始時点で作成しているグループのうち「tenant_」から始まる名前のグループにつきましては、お客さまにてメンバーの設定をいただくことが可能です。

例えば下記のような操作を行う場合は、本項の手順を参照し、作成済みグループへのメンバー設定の追加を行う必要があります。

- 外部ネットワークへアクセス可能な Overlay Network を作成する
- 本サービスの管理ツールへアクセス可能な外部ネットワークを追加する
- Advanced cross vCenter vMotion の移行元のネットワークを登録する

当社にて作成済みのメンバーの一覧と用途について下記をご参照ください。

参照 「2.2.6 グループ」

6.14.1. 外部ネットワークへアクセス可能な Overlay Network の追加

新規にOverlay Network作成をした場合、Overlay NetworkのIPセグメントを外部と通信(Tier-0ゲートウェイを経由)できるようにするためには、「tenant_overlay」のグループに対象のIPレンジ、或いはセグメント自体などを登録する必要があります。

以下は「user_overlay-01(サブネット 192.168.15.0/24)」というOverlay Networkの作成後に「tenant_overlay」に登録し外部と通信できるようにする場合の設定例です。

1. **NSX Managerにログインします。**

2. **「インベントリ」から「グループ」をクリックします。**

3. **「tenant_overlay」横の「⋮」をクリックし「編集」をクリックします。**

グループの編集画面が表示されます。

4. **コンピュートメンバー下の項目をクリックします。**

ここに表示される内容はグループに設定している内容により異なります

メンバーの設定画面が表示されます。

5. IPアドレスで許可をする場合は「IP アドレス」タブから一覧に「192.168.15.0/24」を追加し適用をクリックします。

メンバーが追加されます。

6. 「保存」をクリックします。

グループの設定が保存されます。

7. **グループの状態が「成功」になることを確認します。**

これで192.168.15.0/24 のIPレンジのVMは外部ネットワークとの双方向の全てのアクセスと、管理VMとの管理用通信が可能になります。

> **補足** tenant_overlayと外部ネットワークとの通信を制限したい場合は、ゲートウェイ ファイアウォールか分散ファイアウォールをご利用ください。

6.14.2. 管理ツールへアクセス可能な外部ネットワークの追加

外部から当社管理ツールにアクセス可能なネットワークは、Tier-0 ゲートウェイに設定しているゲートウェイ ファイアウォールのポリシーで、「tenant_external」のグループに登録されているネットワークに制限をしています。

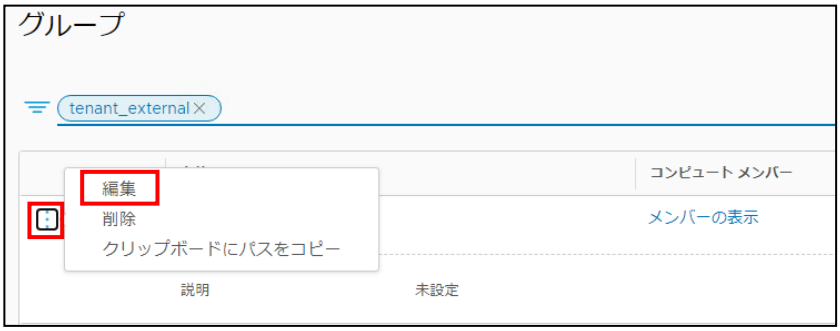
本項では管理ツールへアクセスするための外部ネットワークアドレスを追加する手順をご説明いたします。

> **補足** Overlay Networkから管理ツールへのアクセスは「tenant_overlay」のグループに登録することによりアクセスが可能となります。

1. **NSX Managerにログインします。**

2. **「インベントリ」から「グループ」をクリックします。**

3. **「tenant_external」横の「⋮」をクリックし「編集」をクリックします。**



グループの編集画面が表示されます。

4. コンピュート メンバー下の項目をクリックします。

ここに表示される内容はグループに設定している内容により異なります

メンバーの設定画面が表示されます。

5. 「IP アドレス」タブから一覧にアクセスを許可したいIPレンジを追加し「適用」をクリックします。

> **重要** 「tenant_external」へのグローバルIPレンジおよび、0.0.0.0/0(任意のアドレス)の登録は禁止操作となります。

メンバーが追加されます。

6. 「保存」をクリックします。

グループの設定が保存されます。

7. グループの状態が「成功」になることを確認します。

追加したIPレンジは管理ツールとの通信が可能になります。

6.14.3. Advanced Cross vCenter vMotionの移行元ネットワークの登録

Advanced Cross vCenter vMotionを利用する場合、移行元となるお客さま環境のvCenterおよびESXiがプライベートクラウド環境と通信(Tier-0ゲートウェイを経由)できるようにするために、以下グループに対象のIPアドレスを登録する必要があります。

グループ名	説明
tenant_external_esxi_mgmt	お客さま環境 ESXi の管理用 VMkernel IP アドレスを登録します。
tenant_external_esxi_vmotion	お客さま環境 ESXi の vMotion 用 VMkernel IP アドレスを登録します。
tenant_external_vcenter	お客さま環境の vCenter の IP アドレスを登録します。

以下は「tenant_external_esxi_mgmt」にお客さま環境のESXi管理用IPアドレス (サブネット172.16.21.0/24)を登録する場合の設定例です。

1. **NSX Managerにログインします。**

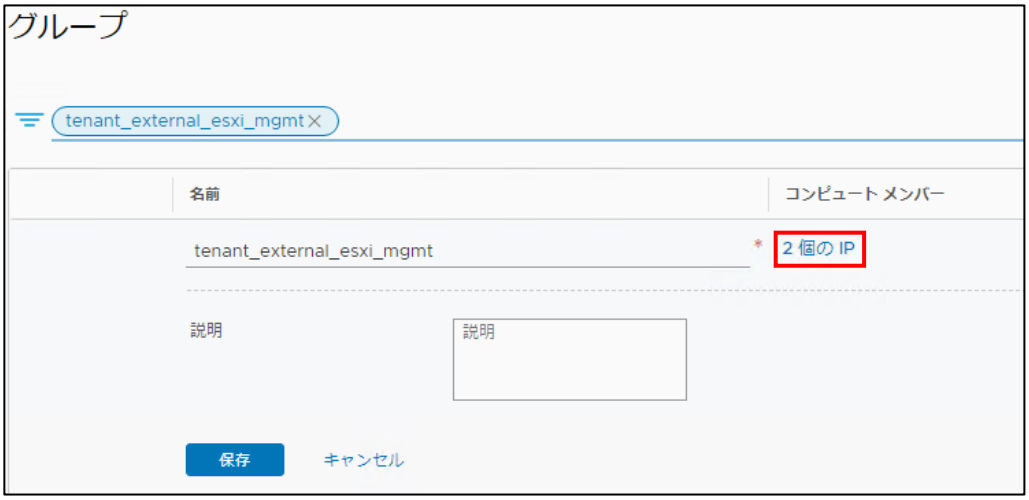
2. **「インベントリ」から「グループ」をクリックします。**

3. **「tenant_external_esxi_mgmt」横の「⋮」をクリックし「編集」をクリックします。**

グループの編集画面が表示されます。

4. コンピュートメンバー下の項目をクリックします。

ここに表示される内容はグループに設定している内容により異なります

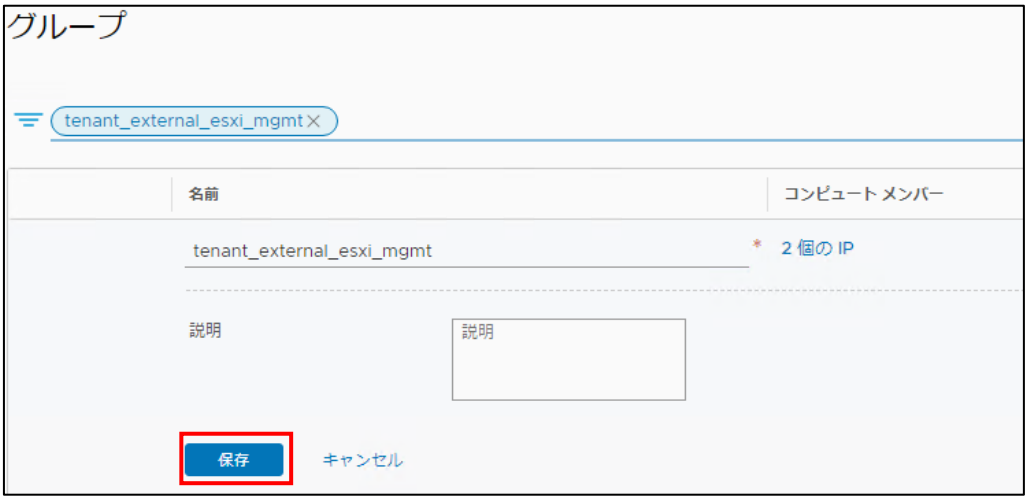


メンバーの設定画面が表示されます。

5. 「IP アドレス」タブから一覧に「172.16.21.0/24」を追加し適用をクリックします。

メンバーが追加されます。

6. 「保存」をクリックします。

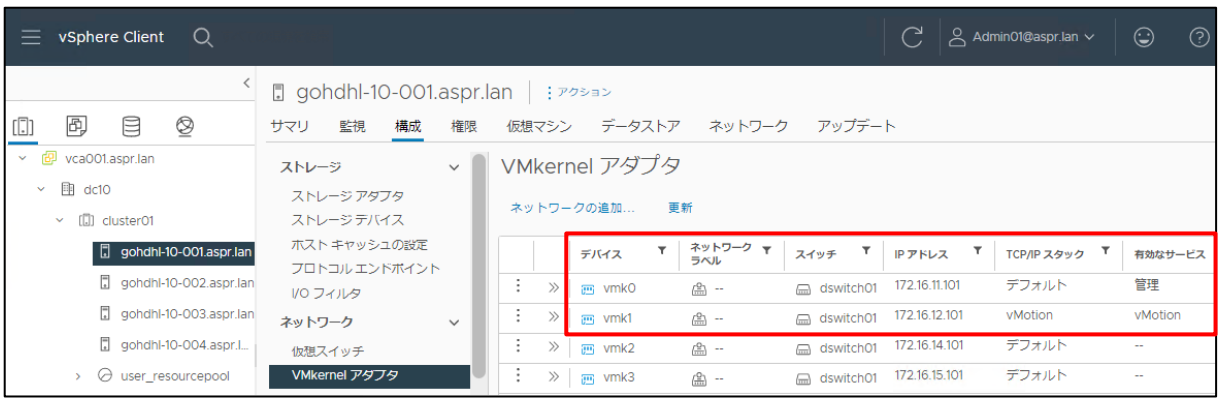


グループの設定が保存されます。

7. グループの状態が「成功」になることを確認します。

8. 同様に「tenant_external_esxi_vmotion」「tenant_external_vcenter」にネットワークを登録します。

9. お客さま環境とプライベートクラウド環境間の疎通確認を実施します。プライベートクラウド環境のvCenter ServerのIPアドレスは開通通知書を、ESXiのIPアドレスはvCenter Serverよりご確認ください。



6.15. 証明書の操作

NSX 環境で利用する証明書の操作についてご説明いたします。

ロードバランサや VPN で利用する証明書と CRL をインポートすることができます。

> **重要**
>
> **既知の不具合について**
>
> １つの仮想サーバに対し、同一の証明書を異なった名称で適用してしまうと、ロードバランサの動作に不具合が発生する場合があります。
>
> 本事象発生時の修正はお客さまにて実施いただけないため、当社サポート窓口までご連絡ください。
>
> 参照『NSX-T Load-Balancers and Virtual Server are not working and in "Unknown" states (85499)』

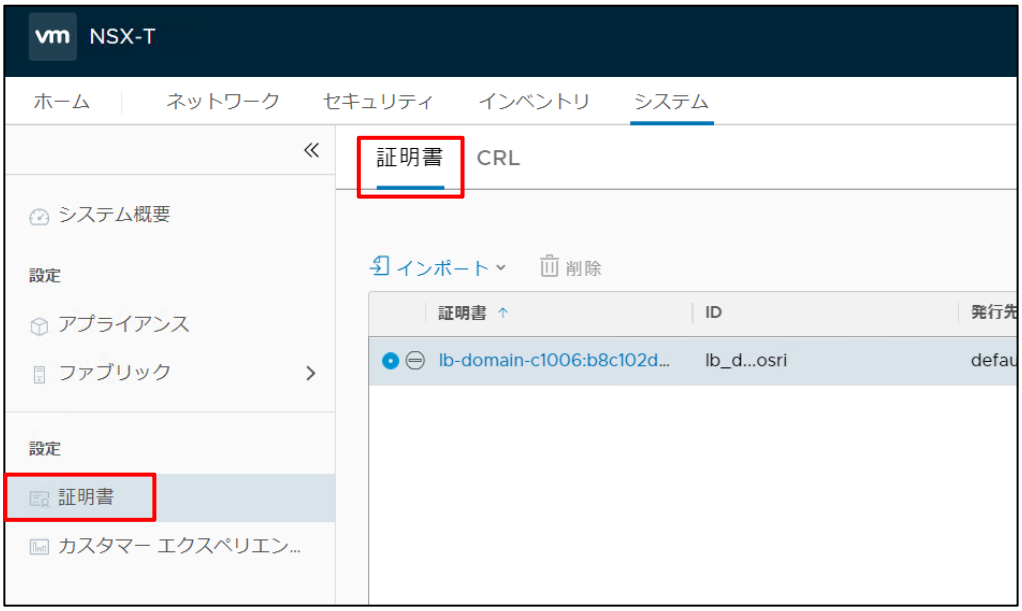
6.15.1. 証明書のインポート

証明書のインポート手順についてご説明いたします。

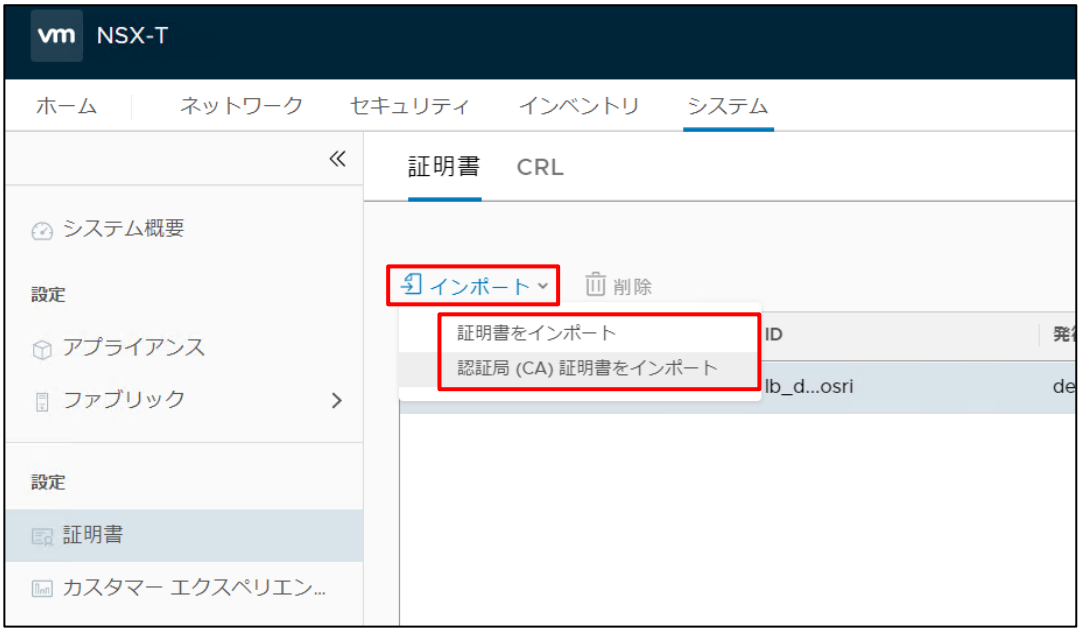
1. **NSX Managerにログインします。**

2. **「システム」をクリックします。**

3. 「証明書」から「証明書」タブをクリックします。



4. 「インポート」 をクリックし証明書の種類に合わせて「証明書をインポート」または「認証局(CA)証明書をインポートします」をクリックします。



5. 名前と証明書の情報を入力し「インポート」をクリックします。

以下「認証局(CA)証明書をインポート」の画面となります。

6. 証明書が登録されたことを確認します。

登録した証明書はVPNの設定などで使用できます。

6.15.2. CRLのインポート

CRL のインポート手順についてご説明いたします。

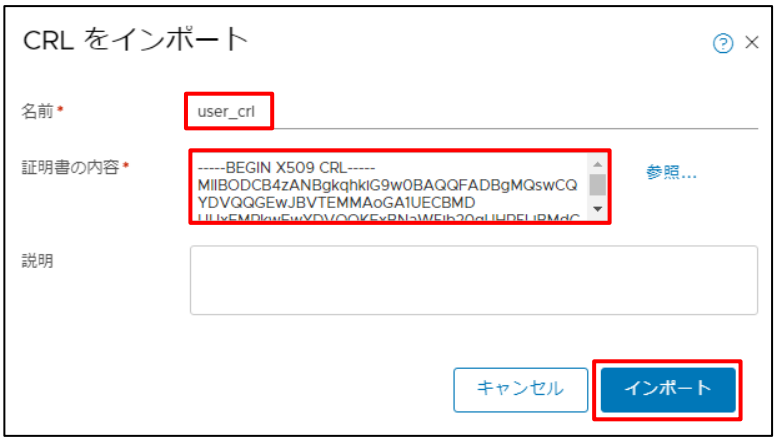
1. **NSX Managerにログインします。**

2. **「システム」から「証明書」をクリックします。**

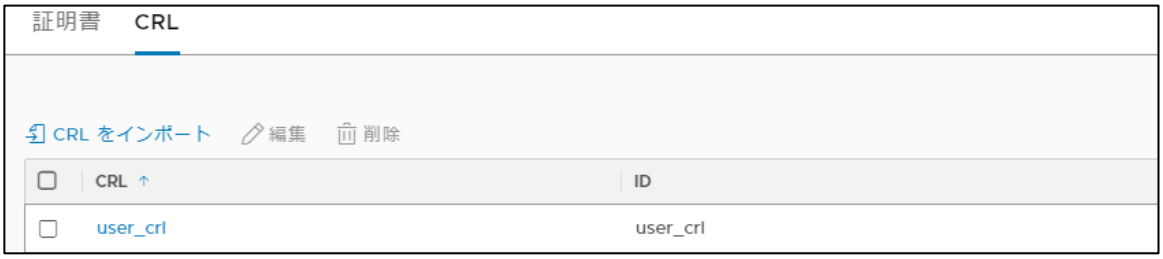
3. **「CRL」タブから「CRLをインポート」 をクリックします。**

CRLのインポート画面が開きます。

4. **名前とCRLの情報を入力し「インポート」をクリックします。**



5. **CRLが登録されたことを確認します。**



登録したCRLはVPNの設定などで使用できます。

6.15.3. 証明書の削除

証明書の削除手順についてご説明いたします。

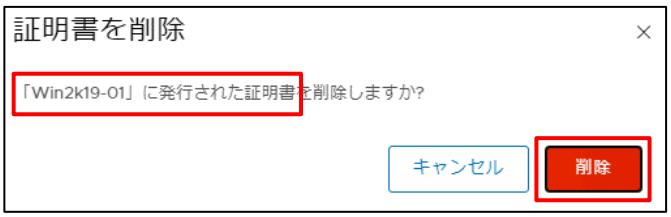
1. **NSX Managerにログインします。**

2. **「システム」から「証明書」をクリックします。**

3. **「証明書」タブから削除対象の証明書を選択し「削除」をクリックします。**

確認画面が表示されます。

4. **確認画面で対象に間違いが無いことを確認し「削除」をクリックします。**



削除処理が実施されます。

5. **対象の証明書が一覧から削除されたことを確認します。**

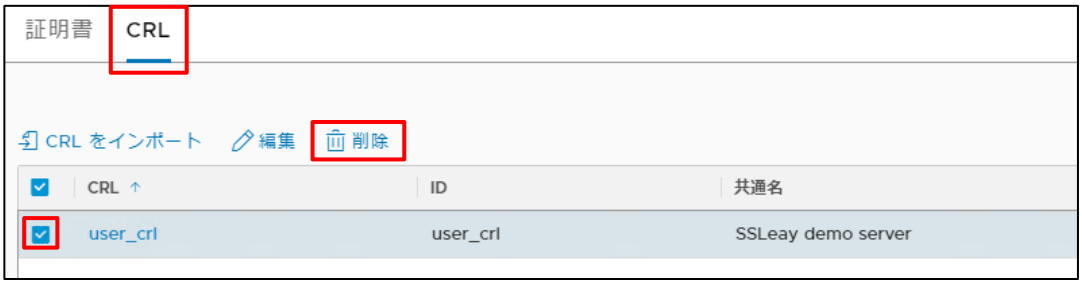
6.15.4. CRLの削除

CRL の削除手順についてご説明いたします。

1. **NSX Managerにログインします。**

2. **「システム」から「証明書」をクリックします。**

3. **「CRL」タブから削除対象のCRLをチェックし「削除」をクリックします。**

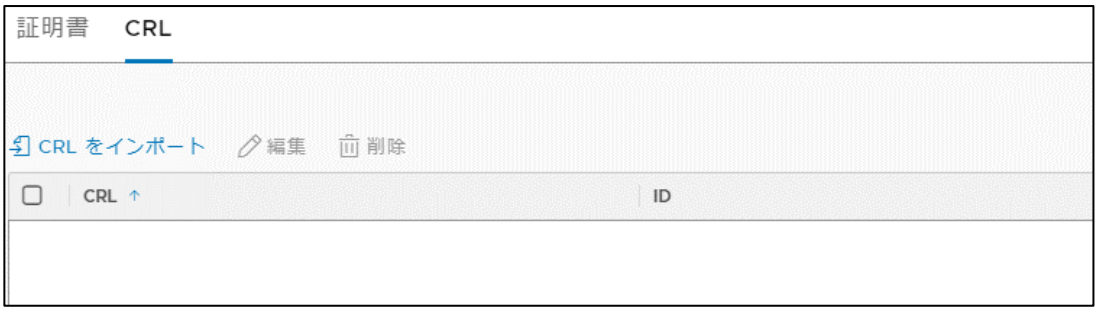


確認画面が表示されます。

4. **確認画面で対象に間違いが無いことを確認し「削除」をクリックします。**

削除処理が実施されます。

5. **対象のCRLが一覧から削除されたことを確認します。**



6.16. NSX ロードバランサの操作(オプション)

本項ではNSX ロードバランサ の操作についてご説明いたします。

> **補足**
> 本サービスではNSX ロードバランサ 機能はオプションサービスとしてご提供いたします。
> 本オプションを申込いただいたお客さまにはロードバランサの操作権限が付与され、
> Tire-1ゲートウェイのロードバランサ機能をご利用いただくことが可能になります。

> **重要**
> **既知の不具合について**
> Firefoxを利用してロードバランシングされたサーバへアクセスした際、正常に動作しない場合があります。詳細は以下のKBをご確認ください。
>
> 参照 『Web traffic traversing an NSX-T Data Center Load balancer may hang when using Firefox web browser (86288)』

6.16.1. ロード バランシングの設定

NSXロードバランサの設定例をご説明いたします。

本設定の前にTier-1 ゲートウェイの「Edge プールの割り当てサイズ」の設定が作成予定のロードバランサのサイズに合わせた設定になっていることを確認してください。

参照 「6.3.1 Tier-1 ゲートウェイの作成」

ロード バランサの作成

ロード バランサの作成手順についてご説明いたします。

1. **NSX Managerにログインします。**

2. **「ネットワーク」をクリックします。**

3. 「ロード バランシング」をクリックし「ロード バランサ」タブから「ロード バランサの追加」をクリックします。

ロード バランサの作成画面が表示されます。

4. 以下のパラメータを入力します。

項目	設定値
名前	任意の名前を入力します。
サイズ	作成予定のサイズを指定します。 サイズは利用する tier-1 ゲートウェイの「Edge プールの割り当てサイズ」と同じである必要があります。
接続	ロードバランサを利用する Tier-1 ゲートウェイを選択します。

5. 「保存」をクリックします。

ロード バランサが作成されます

6. 「いいえ」をクリックします。

7. 作成したロード バランサの状態が「成功」になることを確認します。

ロード バランシング プロファイルの作成

ロードバランシングプロファイルを利用することで、作成したロードバランサの動作について詳細な設定を行うことが可能です。

プロファイルにはアプリケーション・パーシステンス・SSLの3種類があります

> **補足** 詳細設定項目を含む各種プロファイルの設定は、以下のヴイエムウェア社の公式ドキュメントをご参照ください。
>
> **参照** 『仮想サーバ コンポーネントの設定』

モニターの作成

モニターの作成手順をご説明いたします。

モニターはロードバランサの健全性をチェックする機能となり、アクティブ モニターとパッシ ブモニターが存在します。

> 補足 詳細設定項目を含むモニターの設定は、以下のヴイエムウェア社の公式ドキュメントをご参照ください。
>
> 参照 『アクティブモニターの追加』
>
> 参照 『パッシブモニターの追加』

サーバ プールの作成

サーバ プールの作成手順をご説明いたします。

サーバ プールにはアプリケーションを実行するサーバを登録し、ロード バランシング方式、モニターなど定義します。

以下2台のサーバに通信を振り分けるサーバ プールの設定例です。

1. NSX Managerにログインします。

2. 「ネットワーク」から「ロード バランシング」をクリックします。

3. 「サーバ プール」タブから「サーバ プールの追加」をクリックします。

4. 各パラメータを設定し、「メンバーの選択」をクリックします。

項目	設定値
名前	任意の名前を入力します。
アルゴリズム	ロード バランシング アルゴリズムを選択します。 ※以下例では ラウンド ロビンを選択しています。 ご利用の際は用途に合わせて選択してください。

メンバーの設定画面が表示されます。

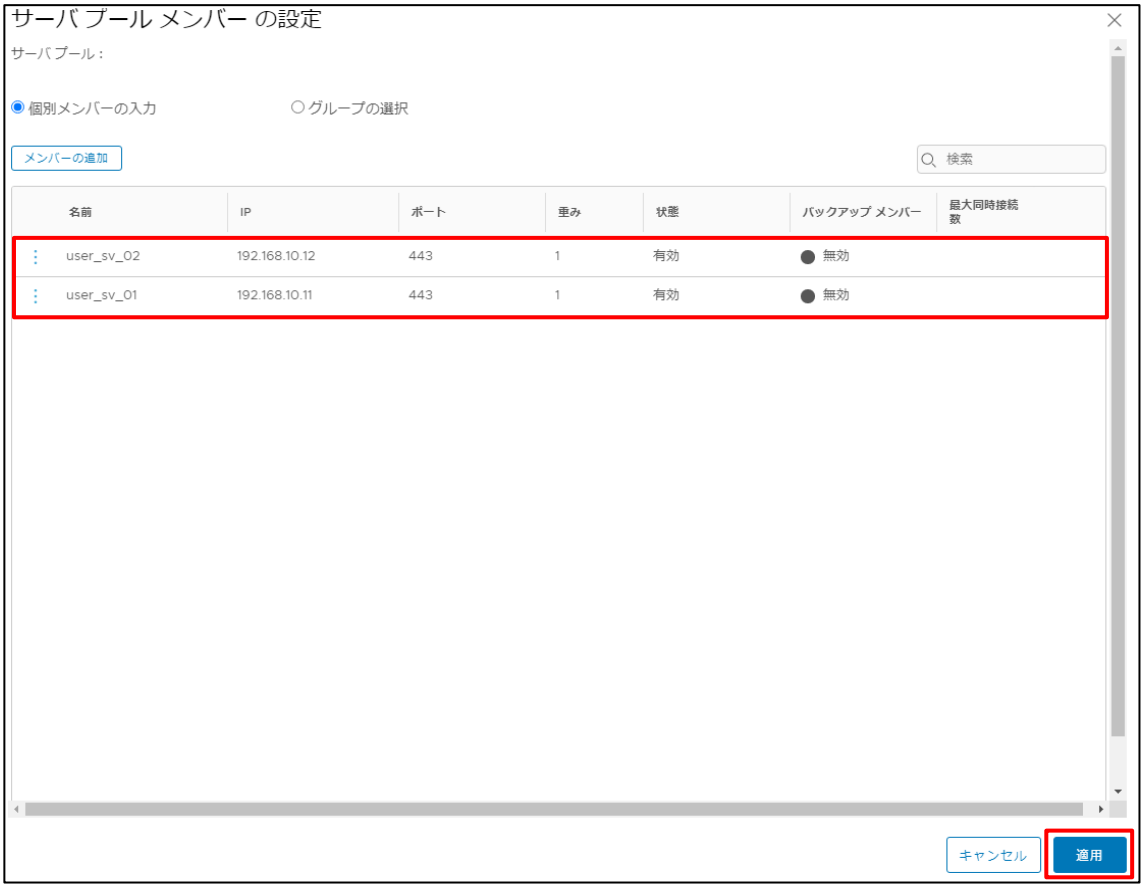
5. 「メンバーの追加」をクリックします。

6. メンバー サーバの設定を入力し、「保存」をクリックします。

項目	設定値
名前	任意の名前を入力します。
IP	メンバー サーバの IP アドレスを入力します。
ポート	ポート番号を入力します。

メンバーの設定が保存されます。

7. 同様にメンバー サーバを必要に応じて登録し、「適用」をクリックします。



メンバーサーバの情報が保存されます。

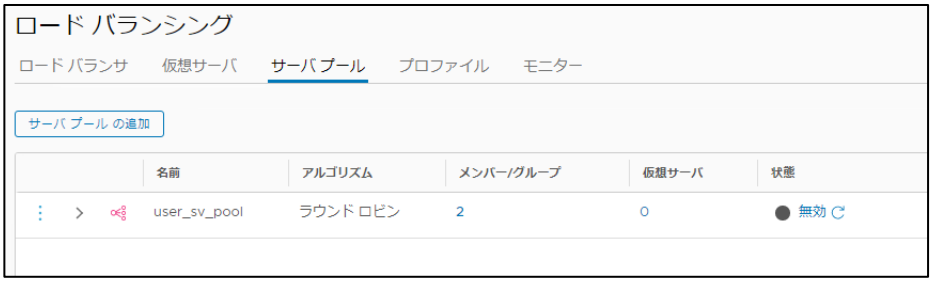
8. 設定の入力が完了したら「保存」をクリックします。

前項で作成したアクティブ モニターやパッシブ モニターを利用する際はここで設定します。

サーバ プールが作成されます

9. サーバ プールが追加されたことを確認します。

仮想サーバで利用されていない サーバ プールの状態は「無効」となります。



仮想サーバの作成

仮想サーバの作成手順をご説明いたします。

仮想サーバはクライアントからの接続を受け、関連付けられたサーバ プールのメンバーに通信を分散します。

以下 L4 TCPの仮想サーバの設定例です。

重要

既知の不具合について

仮想サーバの作成時 ポートに[000],[03389]などの0から始まる数字のような不適切な値を指定した際、ロード バランサの全体の動作に影響を及ぼす不具合があります。指定の際はご注意ください。

参照 『VMware KB :Any newly created Virtual Servers will not change to 'success' status and would remain down. While existing Virtual Servers have no issue. (87138)』

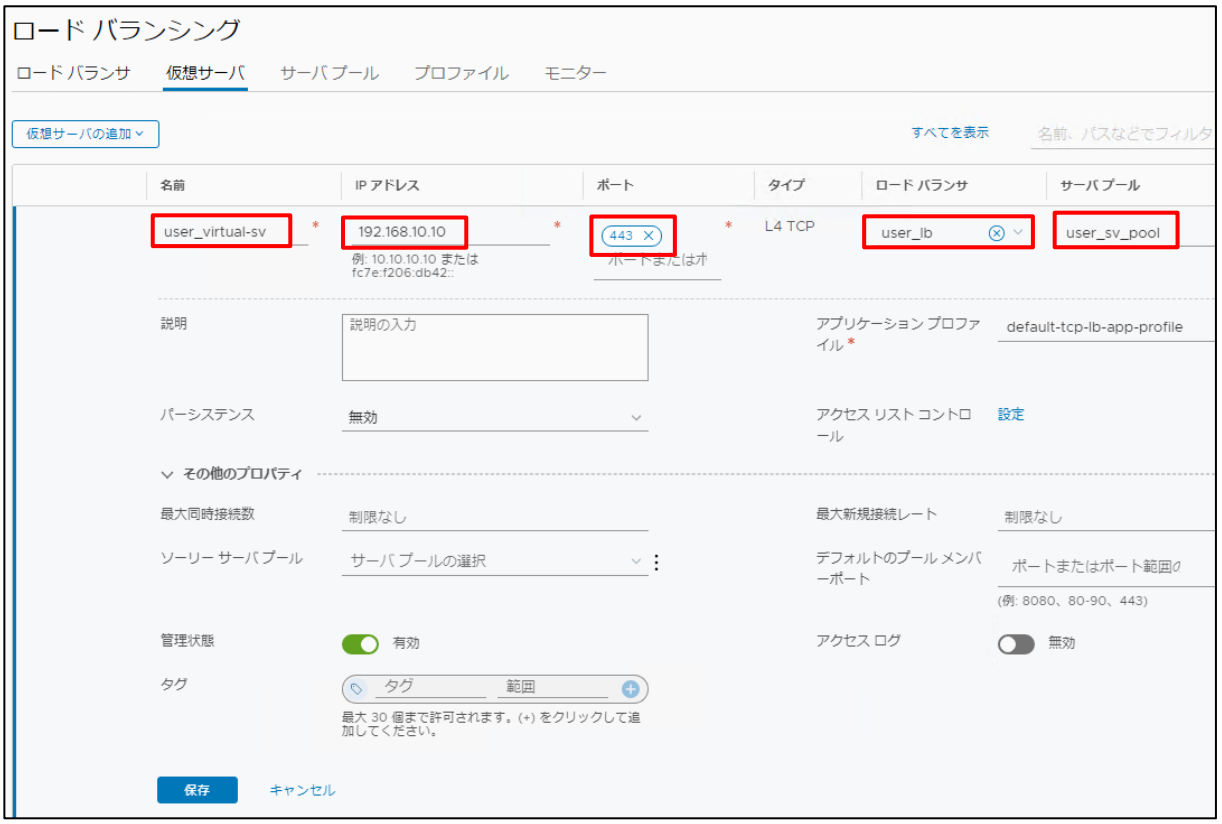
1. **NSX Managerにログインします。**

2. **「ネットワーク」から「ロード バランシング」をクリックします。**

3. **「仮想サーバ」タブから「仮想サーバの追加」をクリックし、作成する仮想サーバの種類を選択します。**

4. 以下のパラメータを入力します。

項目	設定値
名前	任意の名前を入力します。
IP アドレス	仮想サーバの IP アドレスを入力します。
ポート	仮想サーバのポート番号を入力します。
ロード バランサ	仮想サーバで利用するロード バランサを選択します。
サーバ プール	通信を振り分けるサーバ プールを選択します。

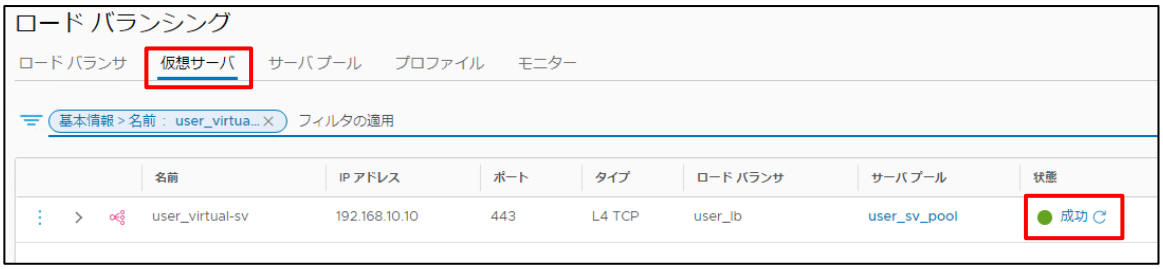


5. 設定の入力が完了したら「保存」をクリックします。

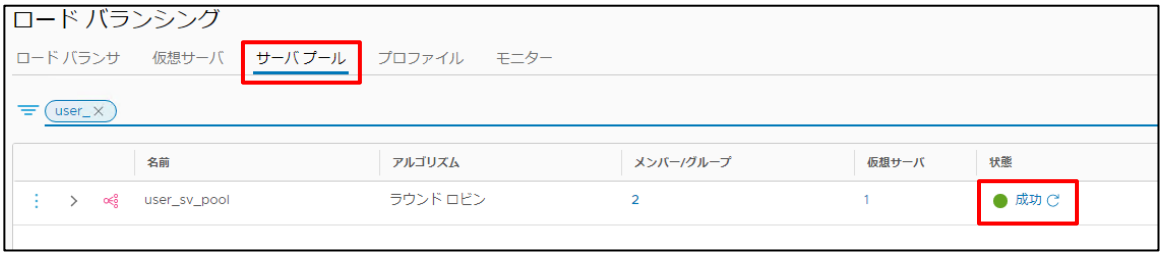
作成したプロファイルを利用する際はここで設定します。

仮想サーバが作成されます。

6. 作成した仮想サーバの状態が「成功」になることを確認します。



7. 「サーバ プール」タブをクリックし、サーバ プールの状態が「成功」になることを確認します。



6.16.2. ロード バランサ設定の削除

本項ではロード バランサ設定の削除手順について記載いたします。

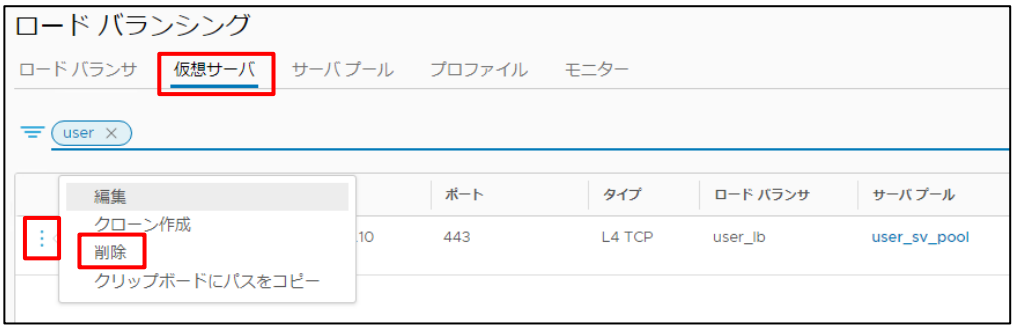
仮想サーバの削除

仮想サーバの削除手順についてご説明いたします。

1. **NSX Managerにログインします。**

2. **「ネットワーク」から「ロード バランシング」をクリックします。**

3. **「仮想サーバ」タブから削除対象仮想サーバ横の「⋮」をクリックし「削除」をクリックします。**



確認画面が表示されます。

4. **確認画面で対象に間違いが無いことを確認し「削除」をクリックします。**

削除処理が実施されます。

5. **対象の仮想サーバが一覧から削除されたことを確認します。**

サーバ プールの削除

サーバ プールの削除手順についてご説明いたします。

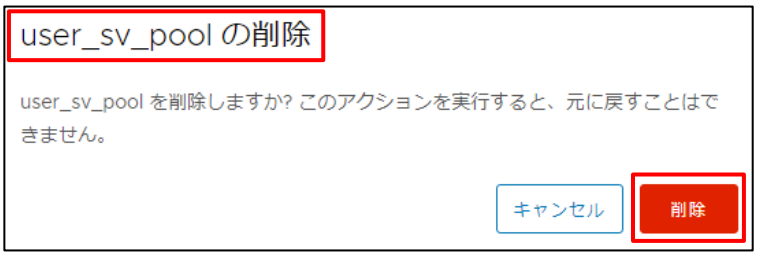
1. **NSX Managerにログインします。**

2. **「ネットワーク」から「ロード バランシング」をクリックします。**

3. **「サーバ プール」タブから削除対象サーバプール横の「⋮」をクリックし「削除」をクリックします。**

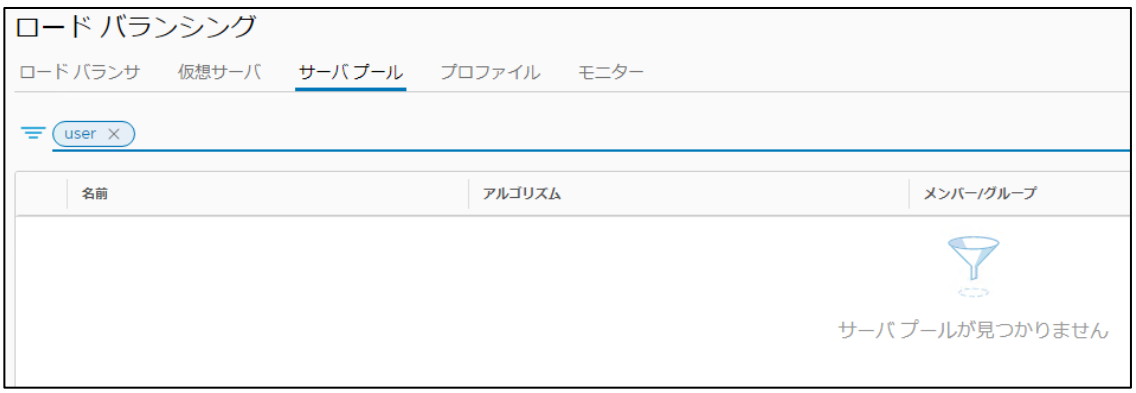
確認画面が表示されます。

4. **確認画面で対象に間違いが無いことを確認し「削除」をクリックします。**



削除処理が実施されます。

5. **対象のサーバ プールが一覧から削除されたことを確認します。**



モニターの削除

モニターの削除手順についてご説明いたします。

1. **NSX Managerにログインします。**

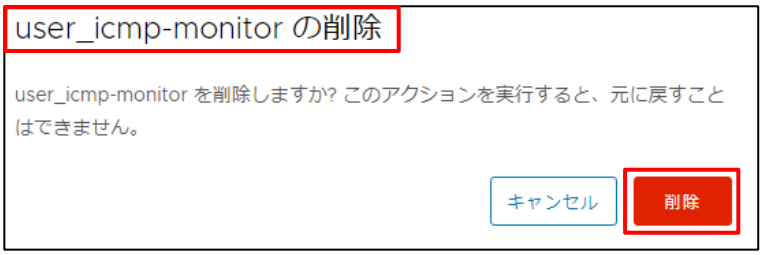
2. **「ネットワーク」から「ロード バランシング」をクリックします。**

3. **「モニター」タブから「モニター タイプの選択」をクリックし、削除対象モニターのタイプを選択します。**

4. **削除対象モニター横の「⋮」をクリックし「削除」をクリックします。**

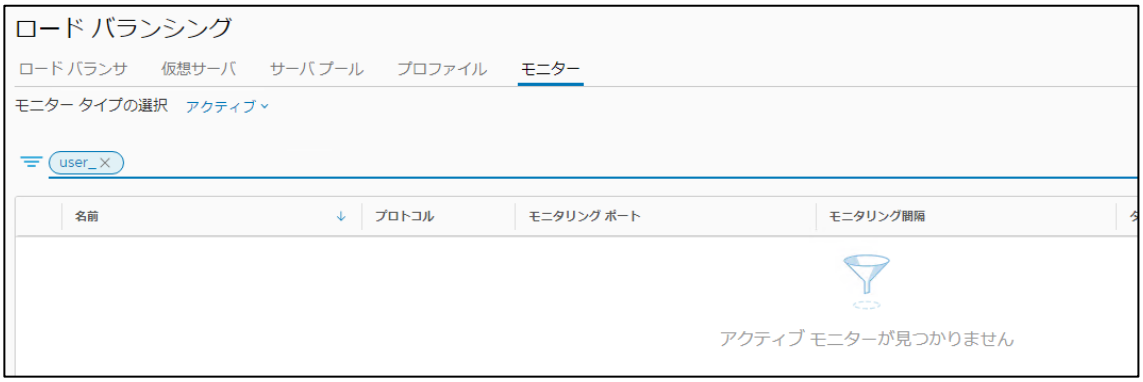
確認画面が表示されます。

5. **確認画面で対象に間違いが無いことを確認し「削除」をクリックします。**



削除処理が実施されます。

6. 対象のモニターが一覧から削除されたことを確認します。



ロード バランシング プロファイルの削除

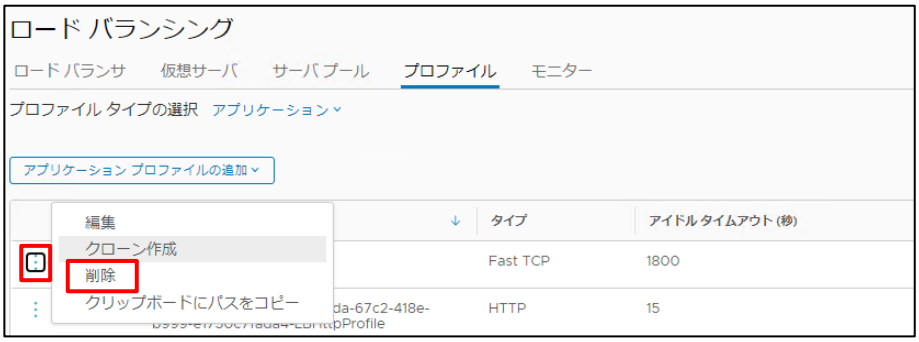
ロード バランシング プロファイルの削除手順についてご説明いたします。

1. NSX Managerにログインします。

2. 「ネットワーク」から「ロード バランシング」をクリックします。

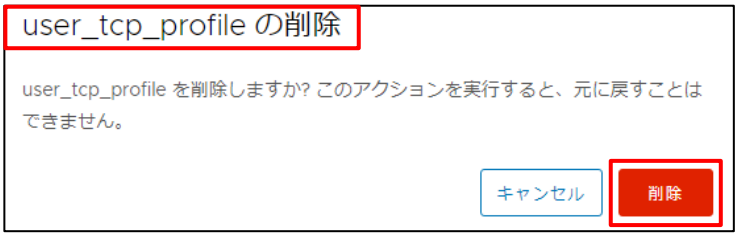
3. 「プロファイル」タブから「プロファイル タイプの選択」をクリックし、削除対象プロファイルのタイプを選択します。

4. 削除対象プロファイル横の「⋮」をクリックし「削除」をクリックします。



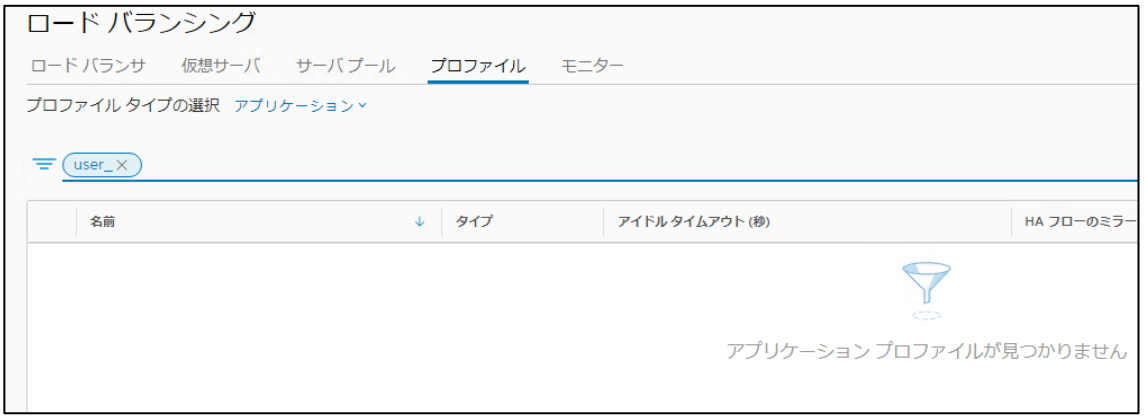
確認画面が表示されます。

5. 確認画面で対象に間違いが無いことを確認し「削除」をクリックします。



削除処理が実施されます。

6. 対象のプロファイルが一覧から削除されたことを確認します。



ロード バランサの削除

ロード バランサの削除手順についてご説明いたします。

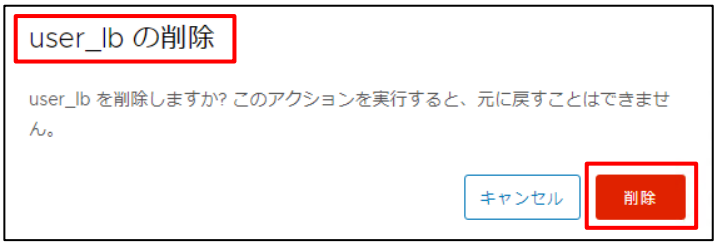
1. NSX Managerにログインします。

2. 「ネットワーク」から「ロード バランシング」をクリックします。

3. 「ロード バランサ」タブから削除対象ロード バランサ横の「⋮」をクリックし「削除」をクリックします。

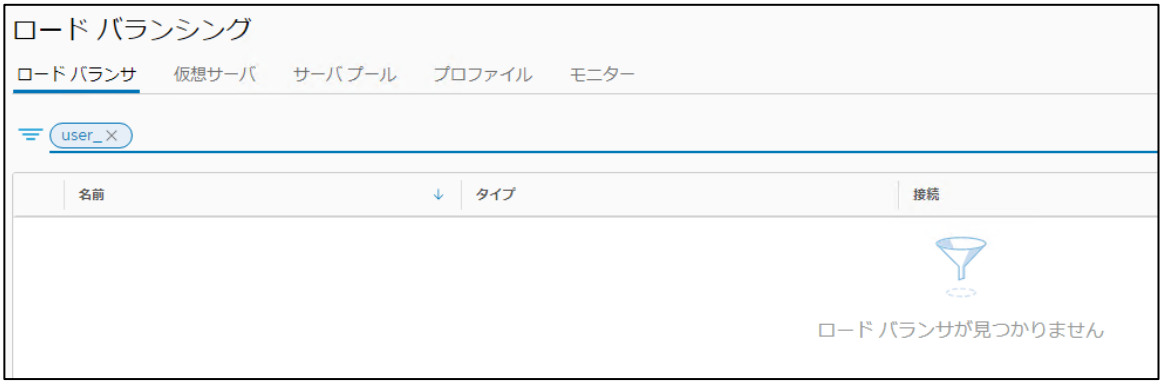
確認画面が表示されます。

4. 確認画面で対象に間違いが無いことを確認し「削除」をクリックします。



削除処理が実施されます。

5. 対象のロード バランサが一覧から削除されたことを確認します。



6.17. 多機能ロードバランサを冗長構成で利用する場合の準備（オプション）

多機能ロードバランサ（Netwiser Virtual Edition）の冗長構成を利用する場合、多機能ロードバランサを接続する Overlay Network で MAC ラーニングを有効にする必要があります。

Overlay Network でMACラーニングを有効にする場合、セグメント プロファイルを作成し、Overlay Network に適用する必要があります。

本項では Overlay Network でMACラーニングを有効にする手順をご説明いたします。

> **補足**
> • 冗長構成を利用しない場合は本項の操作は不要です。

6.17.1. MACラーニングを有効にしたセグメント プロファイルの作成

セグメント プロファイルの作成手順をご説明いたします。

1. **NSX Managerにログインします。**

2. **「ネットワーク」をクリックします。**

3. 「セグメント」を選択し「セグメント プロファイル」タブを開きます。「セグメント プロファイルの追加」から「MACアドレス検出」をクリックします。

セグメント プロファイルの作成画面が表示されます。

4. MACラーニングを有効にして、「保存」をクリックします。

補足

MACラーニング以外のパラメータにつきましてはお客さま環境に合わせて指定してください。

その他のパラメータの詳細情報は、ヴイエムウェア社の公式ドキュメントをご参照ください。

参照 『MAC アドレス検出セグメント プロファイルの作成』

5. 作成したセグメント プロファイルの状態が「成功」になることを確認します。

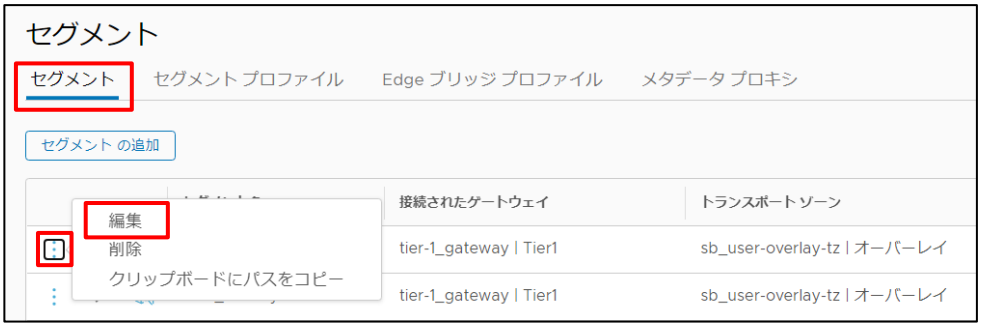
6.17.2. セグメント プロファイルの適用

作成したセグメント プロファイルをOverlay Networkに適用する手順をご説明いたします。

1. **NSX Managerにログインします。**

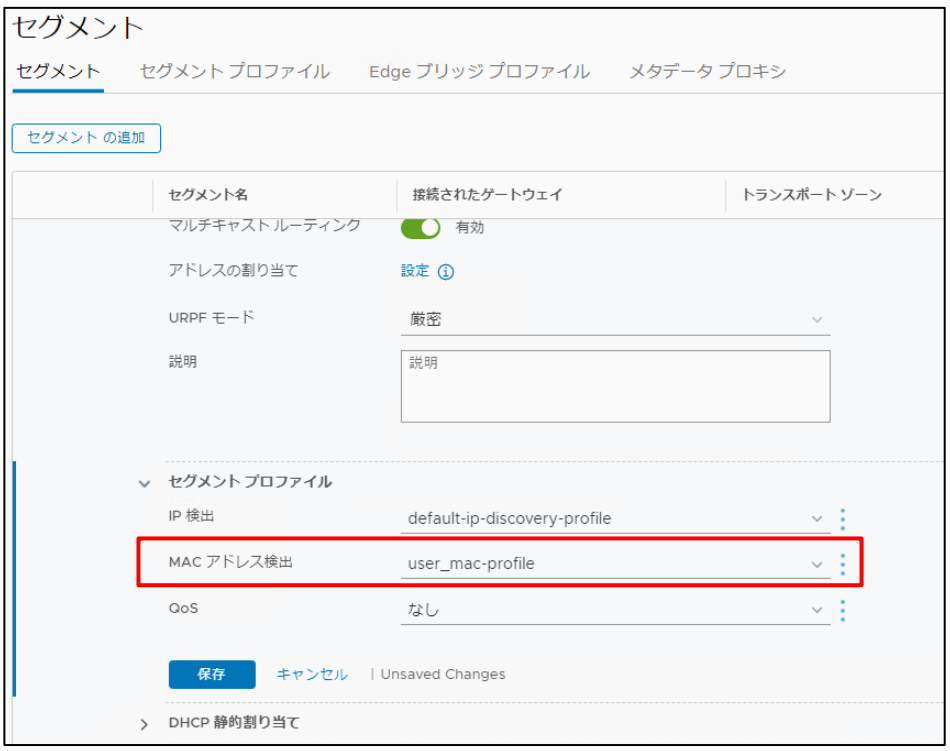
2. **「ネットワーク」から「セグメント」をクリックしします。**

3. **「セグメント」タブから多機能ロードバランサを接続する Overlay Network 横の「⋮」をクリックし「編集」をクリックします。**

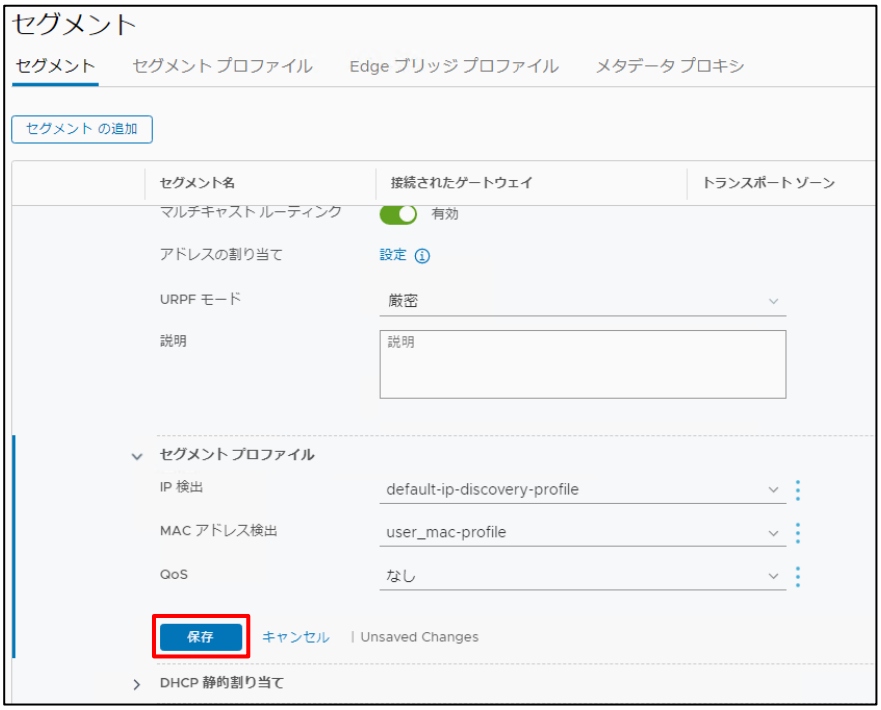


セグメントの設定編集画面が表示されます。

4. **「セグメント プロファイル」配下の「MACアドレス検出」から作成したセグメントプロファイルを選択します。**



5. 設定の編集を実施後「保存」をクリックします。



編集内容が保存されます。

6. 「編集を終了」をクリックします。

編集画面が終了します。

重要

本項の手順を完了後、引き続き当社作業による多機能ロードバランサの設定対応を実施する必要があります。

作業完了後は、当社サポート窓口または担当営業・SEへご連絡ください。

6.18. NSX Manager の禁止操作および非サポート操作

NSX Managerの製品仕様上、操作画面上で本サービスではサポートされない機能が一部表示されており、それらは禁止操作、または非サポート操作となります。対象の操作は、以下の通りです。

禁止操作

項目	説明
セグメント	VLAN セグメントの作成

非サポート操作

項目	説明
セグメント	・ EDGE ブリッジプロファイルの設定 ・ メタデータ プロキシの設定
VPN	・ IPsec VPN ルート ベースの設定 ・ L2 VPN の設定 ・ EVPN の設定 ・ EVPN / VXLAN VNI プールの設定
ネットワーク プロファイル	・ IPV6 プロファイルの設定 ・ マルチキャストプロファイルの設定 ・ BFD プロファイルの設定

6.18.1. セグメントの禁止操作および非サポート操作

セグメントの項目における禁止操作および非サポート操作についてご説明いたします。

VLANセグメントの作成

「6.4.1 Overlay Networkの作成」手順内、セグメントの作成設定において「VLAN」にVLAN番号の入力をするのは禁止操作となります。

作成を確認した際は当社にて削除させていただきます。

EDGE ブリッジプロファイルの設定

EDGE ブリッジプロファイルの設定は非サポート操作となります。

該当する設定箇所は下記となります。

メタデータ プロキシの設定

メタデータ プロキシの設定は非サポート操作となります。

該当する設定箇所は下記となります。

6.18.2. VPNの非サポート操作

VPN の項目におけるサポート操作についてご説明いたします。

ルート ベースIPsec VPNの設定

ルート ベースIPsec VPN の設定は非サポート操作となります。

該当する設定箇所は「IPsec セッションの作成」の「IPSEC セッションの追加」配下の「ルート ベース」となります。

L2 VPNの設定

L2 VPN の設定は非サポート操作となります。

該当する設定箇所は「VPNサービスの作成」の「サービスの追加」配下の「L2 VPN サーバ」および「L2 VPN クライアント」となります。

EVPNの設定

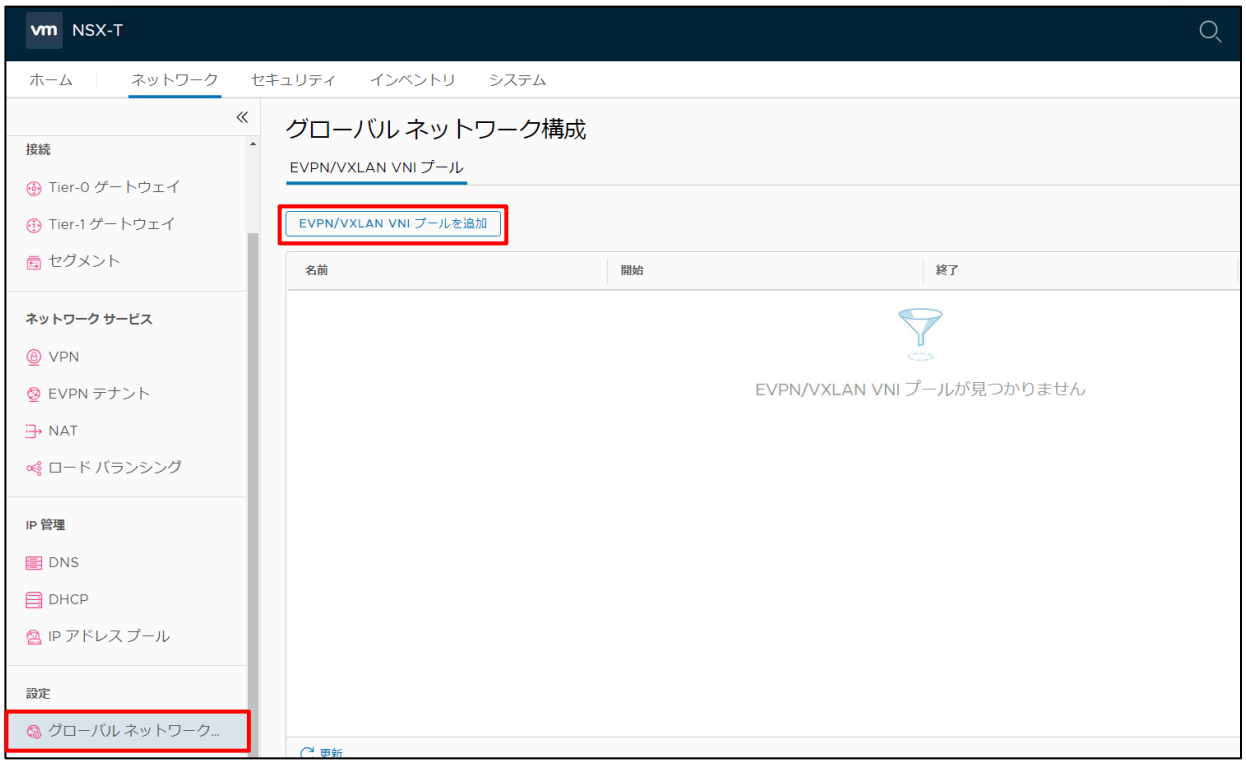
EVPNの設定は非サポート操作となります。

該当する設定箇所は下記となります。

EVPN / VXLAN VNI プールの設定

EVPN / VXLAN VNI プールの設定は非サポート操作となります。

該当する設定箇所は下記となります。



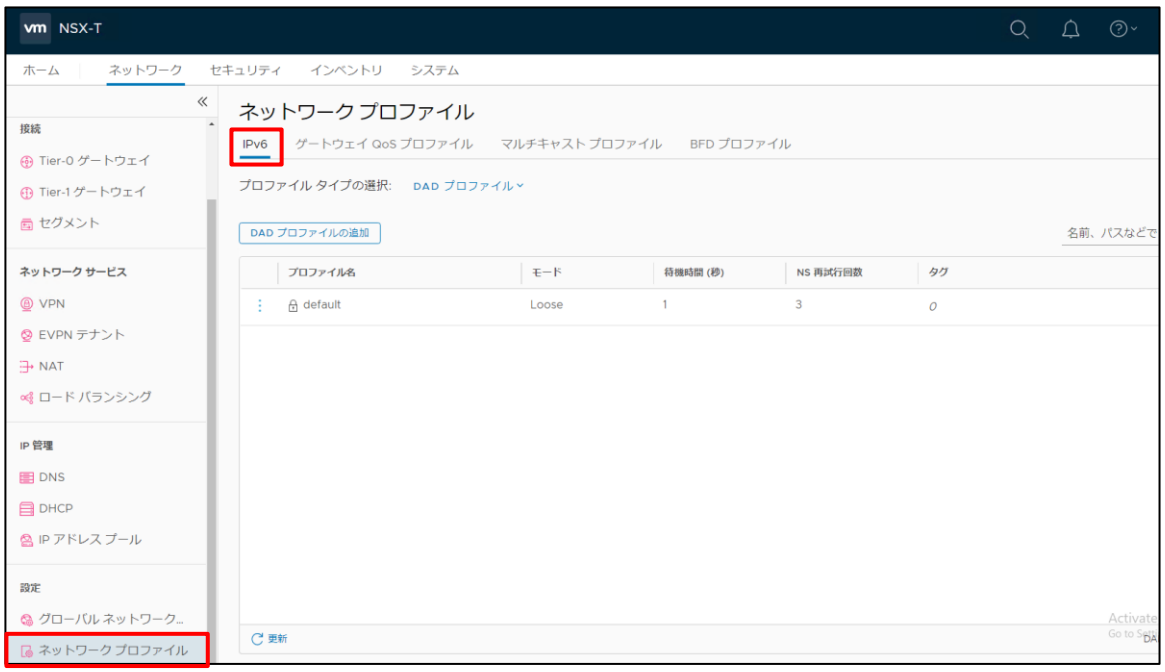
6.18.3. ネットワーク プロファイルの非サポート操作

ネットワーク プロファイルの項目における非サポート操作についてご説明いたします。

IPV6 プロファイルの設定

IPV6 プロファイルの設定は非サポート操作となります。

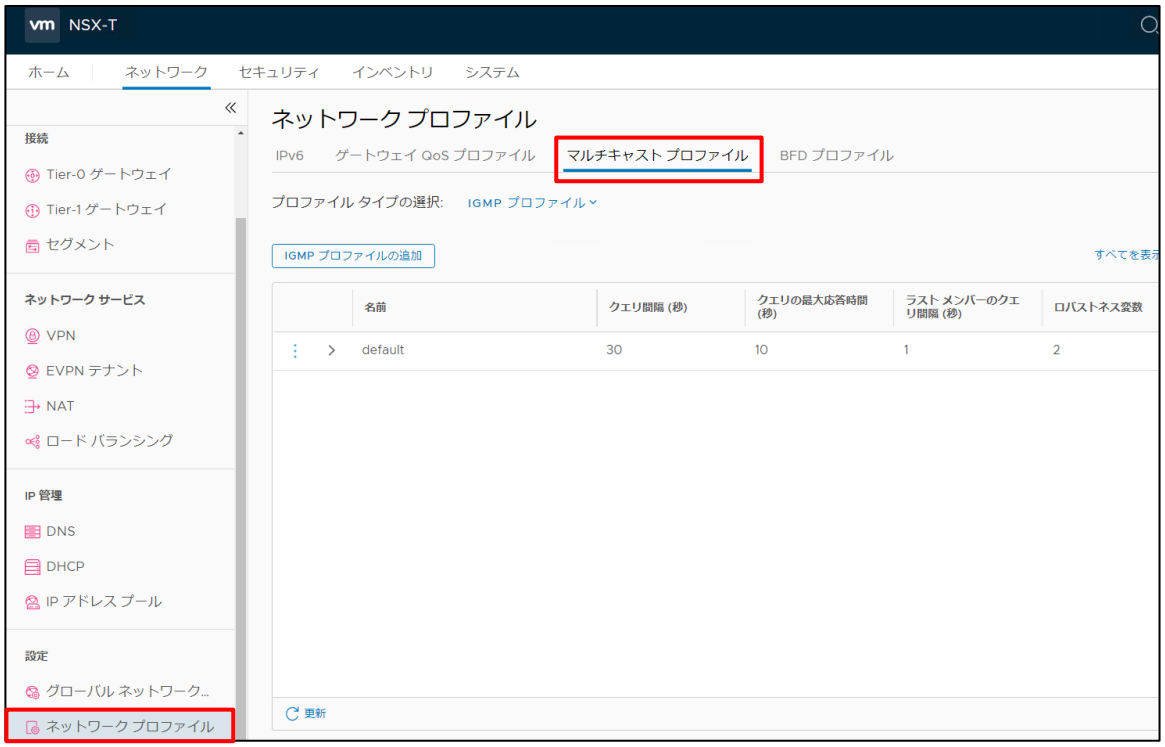
該当する設定箇所は下記となります。



マルチキャスト プロファイルの設定

マルチキャスト プロファイルの設定は非サポート操作となります。

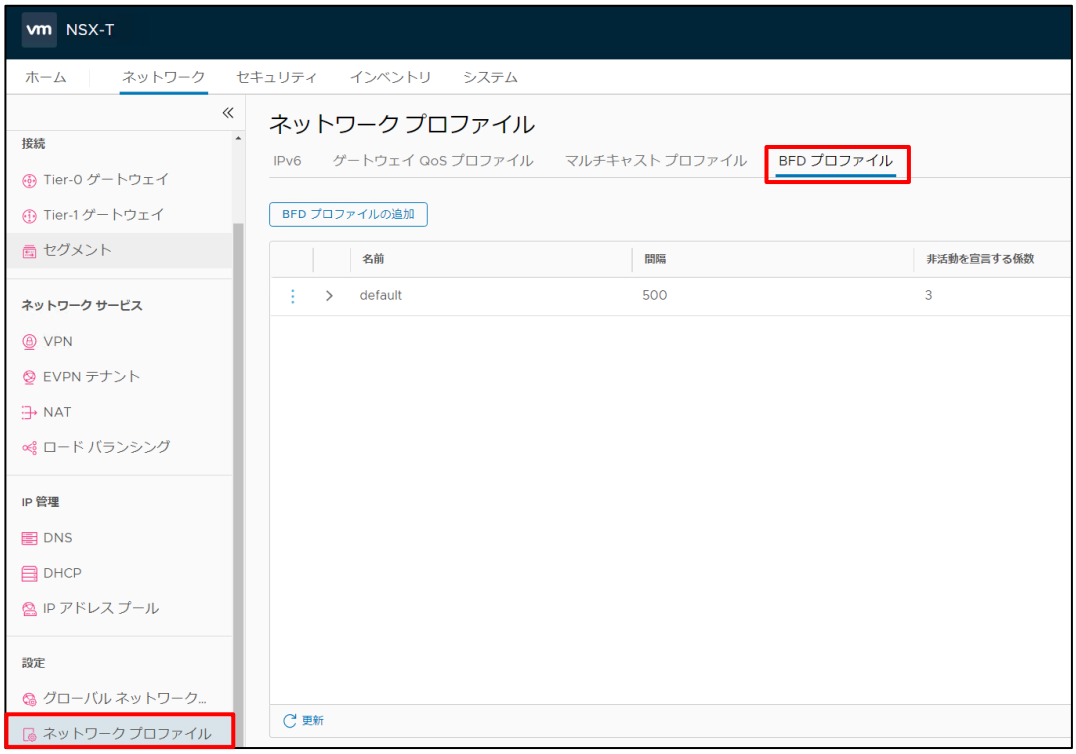
該当する設定箇所は下記となります。



BFD プロファイルの設定

BFD プロファイルの設定は非サポート操作となります。

該当する設定箇所は下記となります。



7. vRealize Operations Manager の操作

仮想化基盤のモニタリングを行う製品である vRealize Operations Manager の操作についてご説明いたします。

本サービスの vRealize Operations Manager では、以下の機能を利用いただけます。

項目	機能概要
分析機能	vRealize Operations Manager の備える各種分析機能をご利用いただけます リソース配分の最適化やキャパシティ評価、トラブルシューティングを行うことが可能です
ダッシュボード	各種ダッシュボードを参照し、システム稼働状態の把握を行えます カスタムダッシュボードの作成や、レポートの生成を行うことも可能です
稼働状況の確認	vRealize Operations Manager でデータ収集している個々のオブジェクトを指定して、稼働状況を参照することが可能です

ここでは、各機能の代表的な利用方法をご説明いたします。

本ガイドの解説に含まれない内容については、ヴイエムウェア社の公式ドキュメントをご参照ください。

参照 『vRealize Operations Manager のドキュメント』

重要

お客さまに提供される vRealize Operations Manager のアカウント権限は、標準の ContentAdmin権限をベースに当社にてカスタマイズをしています。

vRealize Operations Manager のコンテンツ（ビュー、レポート、ダッシュボード、カスタム グループなど）を管理できますが、アラート通知等一部の機能について制限が加えられています。

7.1. vRealize Operations Manager へのアクセスについて

vRealize Operations Manager の管理UIへのログイン・ログアウト操作をご説明いたします。

7.1.1. vRealize Operations Manager へのログイン

vRealize Operations Manager UI へログインします。

1. Webブラウザより、vRealize Operations Manager の URL にアクセスします。

https://vrops001.aspr.lan/ui/login.action

2. 認証ソースを選択し、ユーザ名とパスワードを入力後、「ログイン」ボタンをクリックします。

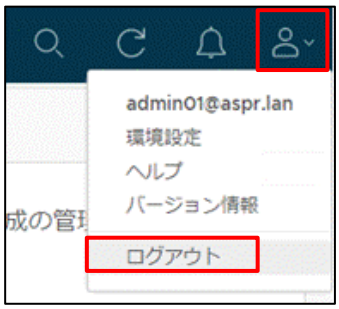
項目	説明
認証ソース	aspr.lan を選択します。
ユーザ名	『開通通知書』に記載されているユーザ名を入力します。
パスワード	上記ユーザ名に設定されたパスワードを入力します。

ログインが完了し、以下の画面が表示されます。

7.1.2. vRealize Operations Manager からのログアウト

vRealize Operations Manager UI からログアウトします。

1. 管理画面の右上のアカウントをクリックし、「ログアウト」をクリックします。



ログアウトが完了し、ログイン画面が表示されます。

7.2. vRealize Operations Manager の基本操作

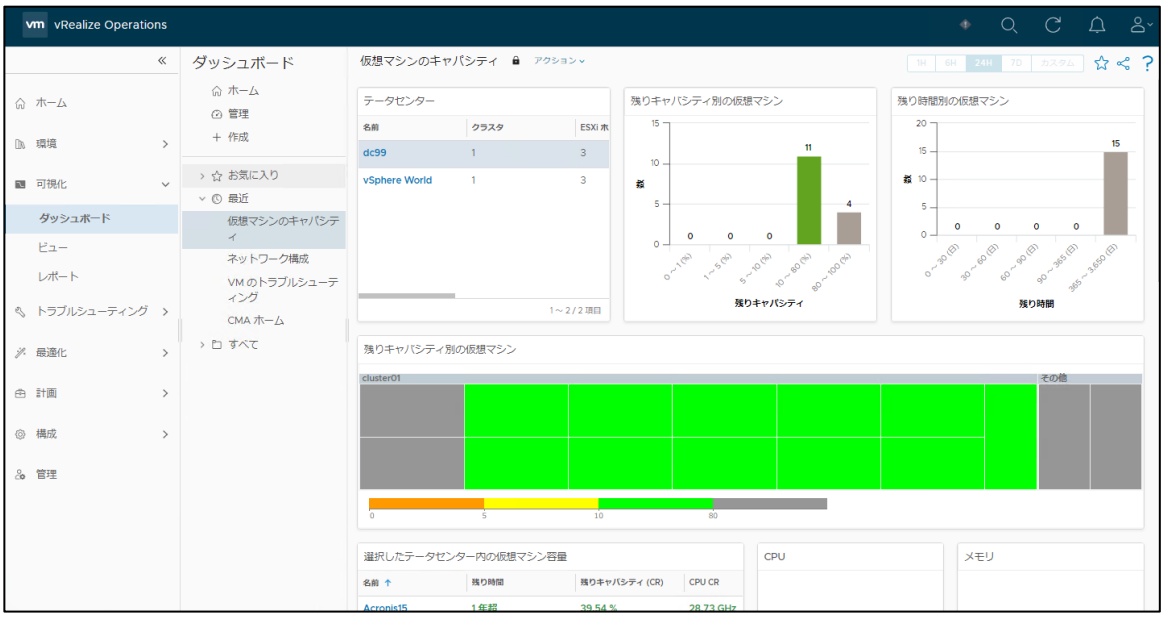
vRealize Operations Manager の基本操作をご説明いたします。

ホームの操作

「ホーム」をクリックすることで、「クイックスタート」画面が表示されます。
「クイックスタート」画面からは、vRealize Operations Manager の各機能へのショートカットを選択することが可能です。

ダッシュボードの操作

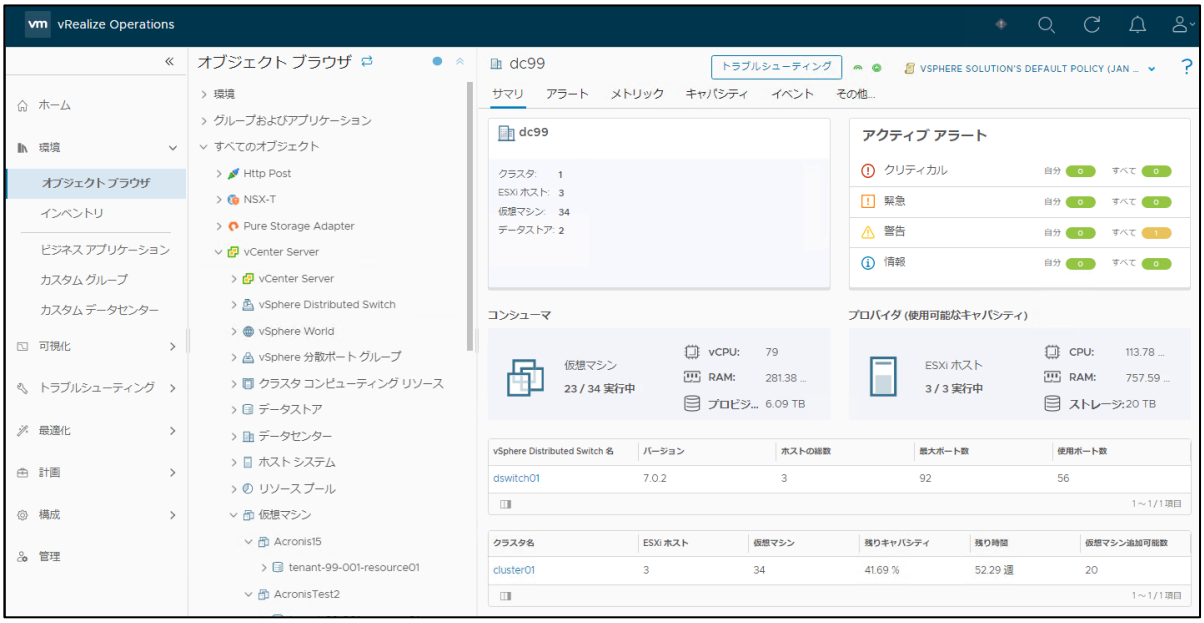
vRealize Operations Manager に定義された様々なダッシュボードを参照することができます。
ダッシュボードをカスタマイズして、独自のダッシュボードを作成することも可能です。
ダッシュボードの操作は「可視化」より「ダッシュボード」を選択します。



環境の操作

vRealize Operations Manager でモニタリングを行っているオブジェクトについて、対象を個別指定して利用状況を参照することができます。

オブジェクトの指定は「環境」より「オブジェクト ブラウザ」を選択します。



7.3. 分析機能

vRealize Operations Manager では、システム上で収集したデータを元に様々な分析機能を利用することで、構成の最適化を図ることが可能です。

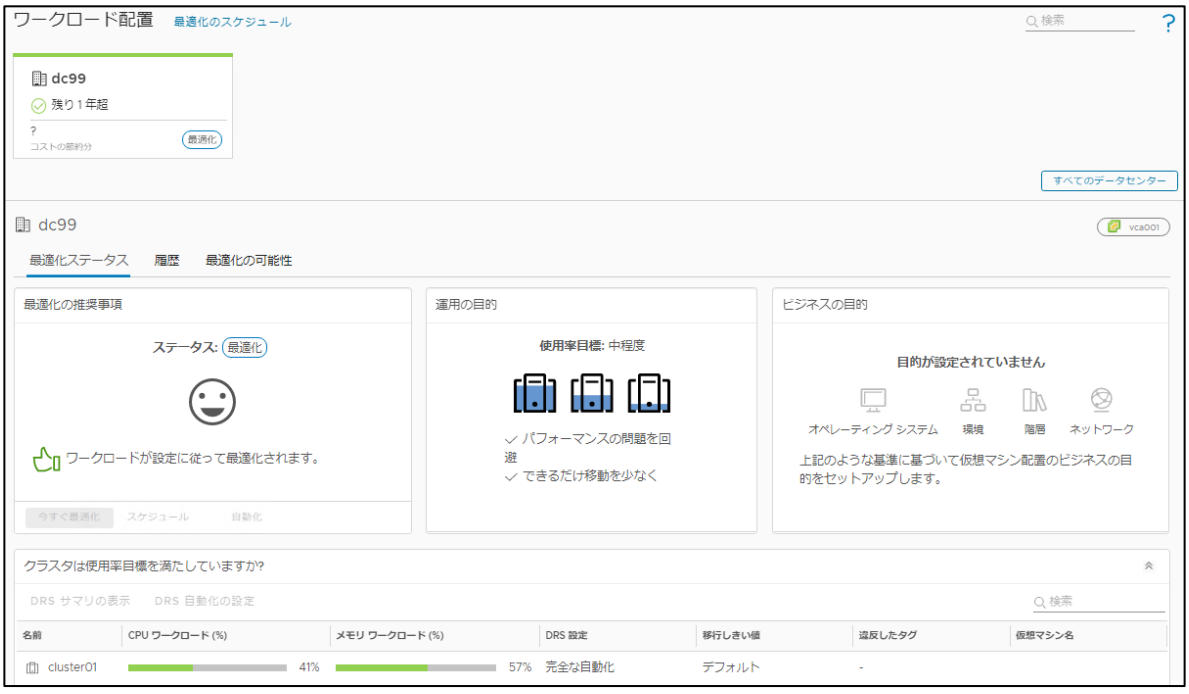
ここでは、その代表的な機能と利用方法をご説明いたします。

「ホーム」メニューの「クイックスタート」ページより、各機能画面を表示できます。

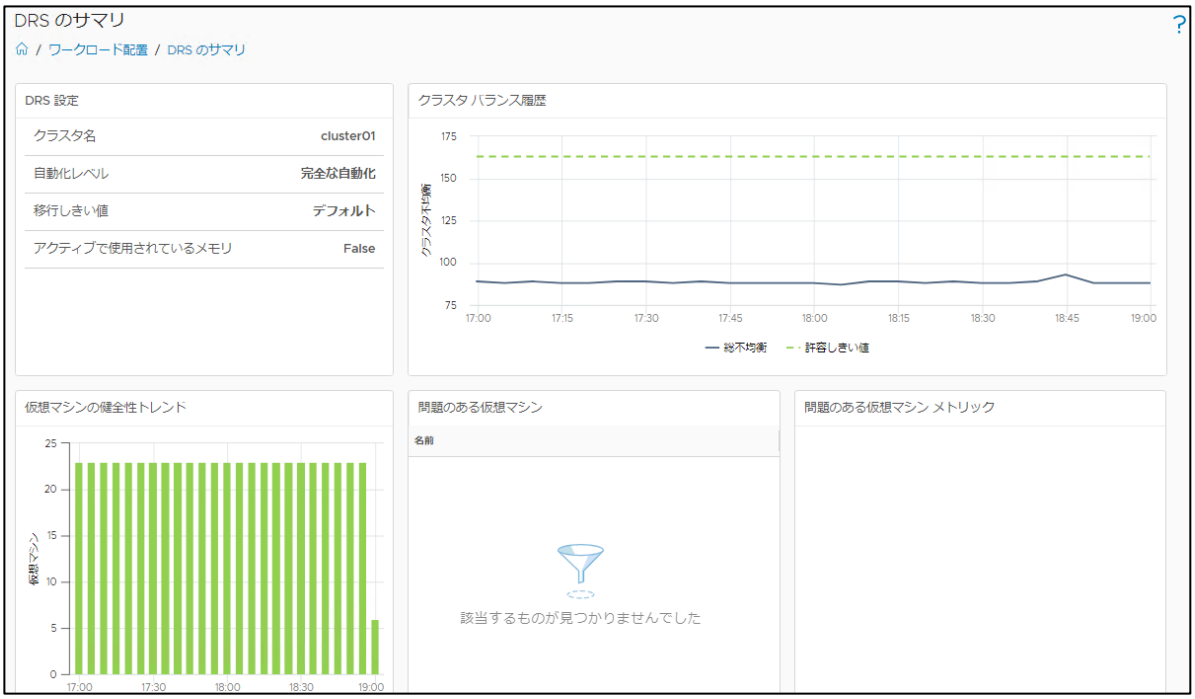
7.3.1. パフォーマンスの最適化

ワークロード最適化

「ワークロード最適化」機能では、仮想マシンの配置状況の評価を参照することが可能です。



1. **画面最下部のクラスタリストから、参照するクラスタを選択し、「DRSサマリの表示」をクリックします。**



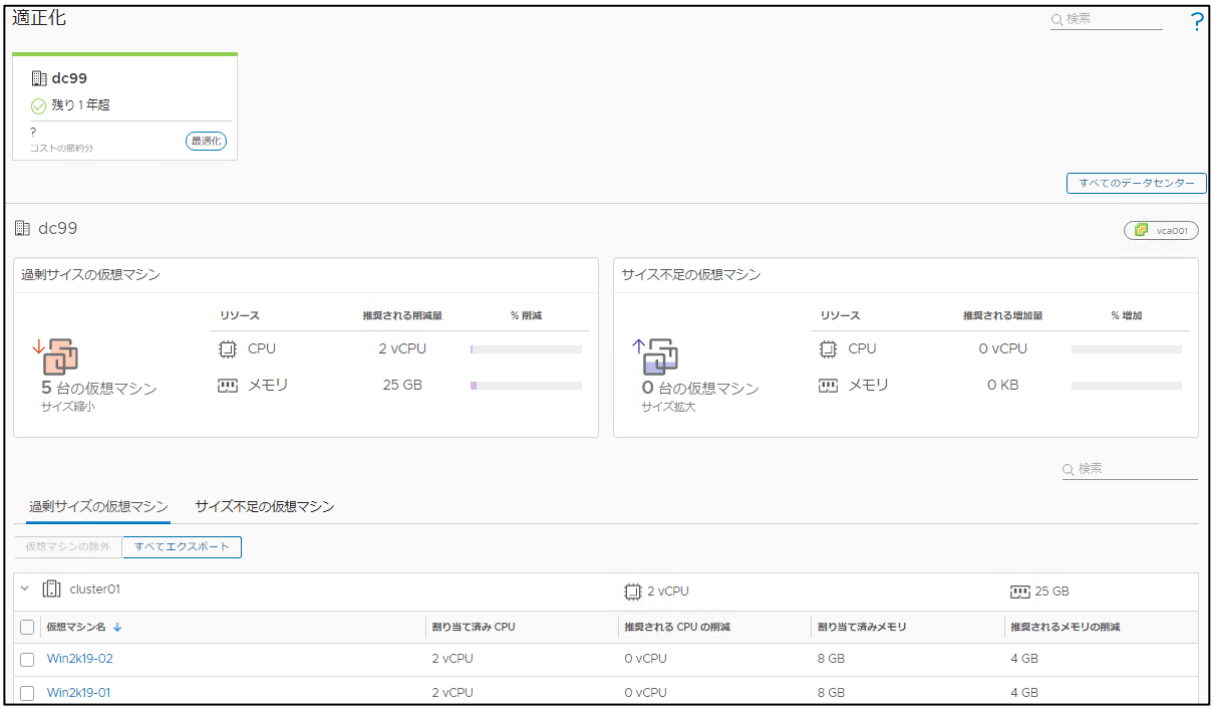
「DRSのサマリ」画面が表示されます。

「DRSのサマリ」画面では、DRS機能によるクラスタのバランスの履歴や健全性のトレンドを確認できます。

健全性に問題のある仮想マシンが存在した場合は、「問題のある仮想マシン」欄に表示されます。

適正化

「適正化」機能では、仮想マシンの利用状況から推測される、スペック過剰な仮想マシンまたはスペック不足の仮想マシンのリストを参照できます。



■ **「過剰サイズの仮想マシン」をクリックし、表示するクラスタの「＞」をクリックします。**

選択したクラスタ内の「過剰サイズの仮想マシン」のリストが表示されます。
各仮想マシンの行には、割り当て済みのCPU/メモリサイズと、これまでの稼働状況から推奨されるCPU/メモリの削減サイズが表示されます。

■ **「サイズ不足の仮想マシン」をクリックし、表示するクラスタの「＞」をクリックします。**

選択したクラスタ内の「サイズ不足の仮想マシン」のリストが表示されます。
各仮想マシンの行には、割り当て済みのCPU/メモリサイズと、これまでの稼働状況から推奨されるCPU/メモリサイズの増加サイズが表示されます。

7.3.2. キャパシティの最適化

キャパシティの評価

「キャパシティの評価」機能では、クラスタの利用状況のトレンドから推測されるリソース利用予測と残り時間を参照することが可能です。

「クラスタ利用率」欄の「並べ替え基準」「履歴の表示時間帯」「予測の表示時間帯」を変更することで、参照するCPU・メモリ・ディスク容量の予測表示を切り替えることが可能です。

再利用

「再利用」機能では、過去の利用状況のトレンドから推測される、利用されていない仮想マシンと、その仮想マシンを削除することで解放されるリソースサイズが、「再利用可能なキャパシティ」として表示されます。

「パワーオフ状態の仮想マシン」「アイドル状態の仮想マシン」をクリックし、表示されるクラスタの「＞」をクリックして展開することで、削除可能であると推測される仮想マシンのリストと、それにより解放されるCPU・メモリ・ディスク容量が表示されます。

また、「スナップショット」「実体なしディスク」をクリックし、表示されるクラスタの「＞」をクリックして展開することで、不要であると推測されるスナップショット、またはディスクを保持している仮想マシンとそのディスク容量が表示されます。

What-if分析

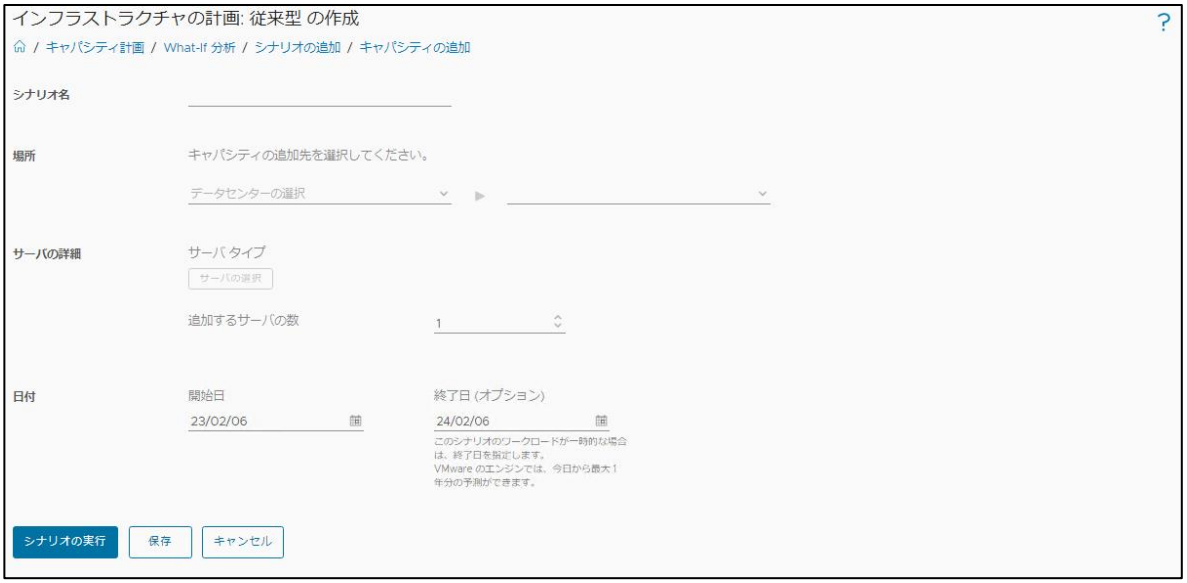
「What-if分析」機能では、過去の利用状況からのトレンド予測をベースに、仮想マシンの追加・削除やESXiホストの追加・削除を行った場合のリソース利用状況のシミュレーションを行うことが可能です。

「What-if分析」の操作は「クイックスタート」ページの「計画」より「What-if分析」を選択します。

ここでは、ESXiホストを1台追加した場合のシミュレーション手順をご説明いたします。

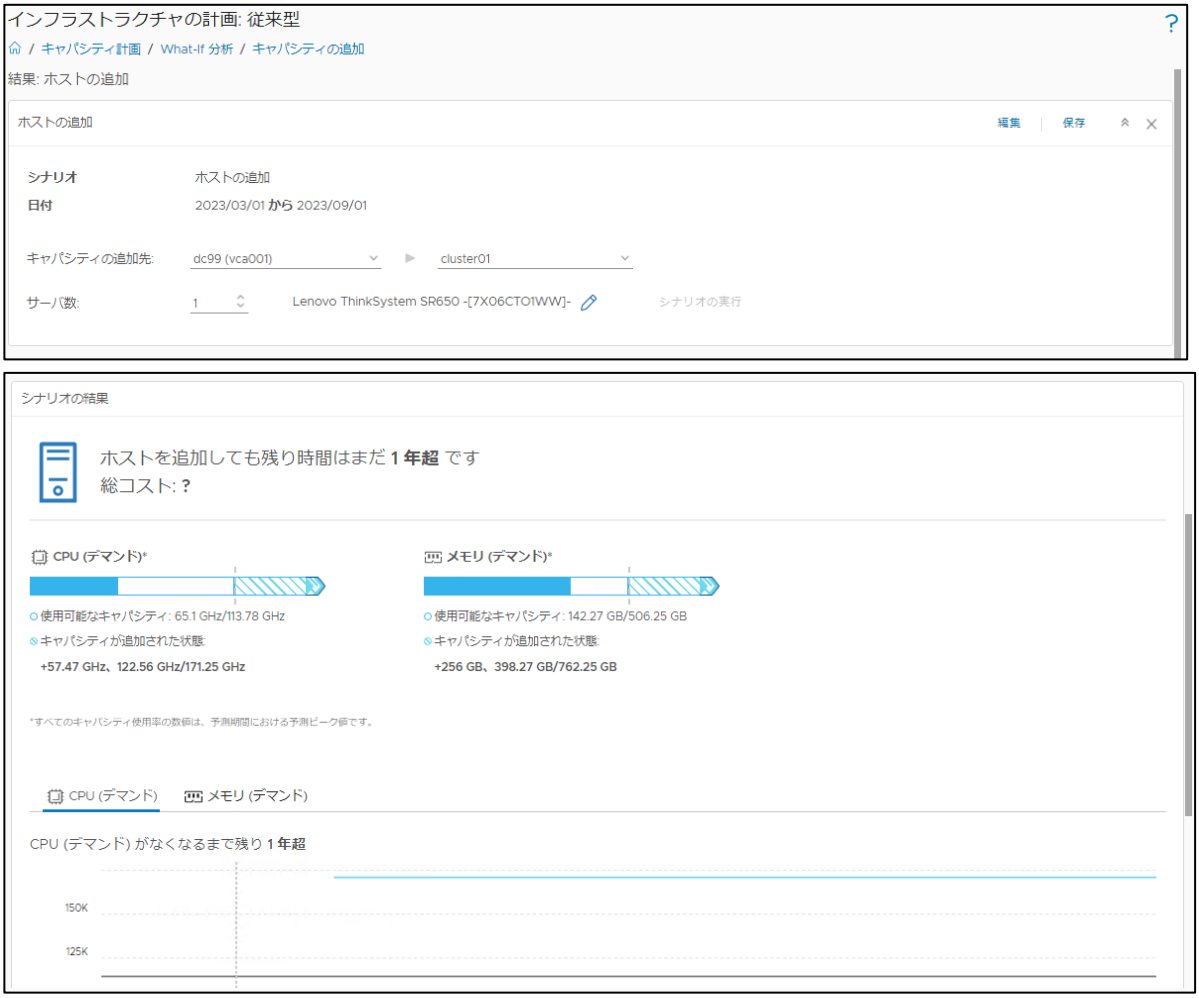
1. 「What-if分析」画面から、「インフラストラクチャの計画：従来型」欄の「ホストの追加」ボタンをクリックします。

「ホストの追加」画面が表示されます。



2. **「シナリオ名」を入力し、ESXiホストの追加先とする「データセンター名」「クラスタ名」を選択します。**
   「サーバの詳細」にて「サーバの選択」ボタンをクリックして追加するサーバ種別を選択し、追加するサーバ台数を入力します。
   「日付」欄では、追加を行う日付・終了する日付を指定します。
   全て入力後、「シナリオの実行」ボタンをクリックします。

   「結果」画面が表示されます。



3. **「結果」画面では結果の参照と、シミュレーション条件の変更を行うことが可能です。**
   CPU・メモリタブを切り替えることで表示するリソース種別を変更できます。

7.4. ダッシュボードの利用

本サービスの利用状況の把握には、vRealize Operations Manager のダッシュボード機能のご利用が有効です。
目的に合わせたダッシュボードを参照することで、各オブジェクトの利用状況を横断的に参照することが可能です。

7.4.1. ダッシュボードの参照

定義済みのダッシュボードの参照手順をご説明いたします。

1. **vRealize Operations Manager の「可視化」より「ダッシュボード」をクリックします。**

   直近で開いていたダッシュボードが表示されます。直近で開いていたダッシュボードが無い場合は「ホーム」の画面が表示されます。

2. **「管理」をクリックし表示されるダッシュボードリストから、ダッシュボードをクリックします。**

   「最近」リストの最上部に選択したダッシュボードが追加され、
   また、画面右ペインに、選択したダッシュボードの内容が表示されます。

> 補足 **定義済みダッシュボード**
>
> 事前定義されたダッシュボードは、一部の当社作成のものを除き、製品標準のダッシュボードが用意されています。
> 製品標準の定義済みダッシュボードの詳細は、ヴイエムウェア社の公式ドキュメントをご参照ください。
>
> 参照 『事前定義されたダッシュボード』

7.4.2. 最近のダッシュボードリスト

「最近」のリストには、過去に表示したことのあるダッシュボードがリスト表示されています。
そのため、頻繁に利用するダッシュボードは、ダッシュボードリストから再選択することなく、表示することが可能です。

7.4.3. カスタムダッシュボードの作成と管理

ダッシュボードメニューでは、定義済みのダッシュボードの参照だけでなく、ウィジェットとメトリックを組み合わせたカスタムダッシュボードを作成することも可能です。

1. **vRealize Operations Manager の「可視化」より「ダッシュボード」をクリックします。**

   直近で開いていたダッシュボードが表示されます。直近で開いていたダッシュボードが無い場合は「ホーム」の画面が表示されます。

2. **「作成」をクリックします。**

   「ダッシュボードの作成」画面が表示されます。

3. **「新規ダッシュボード」を選択し、作成するダッシュボード名を入力します。**

4. **画面下部のウィジェット一覧より、ダッシュボードに表示するウィジェット、またはビューをドラッグ＆ドロップします。**

   カスタムダッシュボード上に選択したウィジェット、またはビューが配置・表示されます。

5. **配置したウィジェットにマウスポインタを合わせると表示されるツールバーから、「ウィジェットの編集」ボタンをクリックします。**

   「ダッシュボード・ウィジェットの構成」画面が表示されます。

6. **左ペインにリストアップされたウィジェットリストから、編集するウィジェットを選択します。**

   右ペインに選択したウィジェットの構成情報が表示されます。

7. **右ペインの構成メニューにて、ウィジェットの詳細設定を行います。**

   設定完了後は「保存」をクリックします。

   > **補足** **ウィジェットの詳細設定**
   >
   > ダッシュボード上の各ウィジェットが表示する情報は、詳細設定画面にて指定したメトリックの情報となります。
   >
   > 指定可能なメトリック、および表示内容・表示方法は、選択したウィジェットにより異なります。
   >
   > ウィジェットごとの設定項目の詳細は、ヴイエムウェア社の公式ドキュメントをご参照ください。
   >
   > **参照** 『ウィジェット定義リスト』

8. **「相互作用を表示」をクリックします。**

   ウィジェット間の相互作用編集画面が表示されます。

9. 相互作用を設定する送信側ウィジェットのプロバイダプラグをクリックし、受信側ウィジェットにドラッグします。

編集画面上のウィジェット間に、相互作用関係を示すラインが表示されます。

10. 「相互作用を非表示」をクリックします。

「ダッシュボードの作成」画面に戻ります。

11. 「保存」ボタンをクリックします。

作成したダッシュボードが表示され、ダッシュボードは「最近」に追加されます。

> 補足 **ダッシュボードの作成と構成**
>
> 本項で紹介した手順は一例となります。より詳細な作成と構成の解説については、ヴイエムウェア社の公式ドキュメントをご参照ください。
>
> 参照 『ダッシュボードの作成と構成』

7.5. オブジェクトごとの稼働状況の確認

「環境」タブのメニューよりオブジェクトを選択することで、確認する対象のオブジェクトを絞って情報を参照することが可能です。

7.5.1. 特定の仮想マシンの稼働状況の確認

「環境」メニューのオブジェクトブラウザから任意のオブジェクトを選択可能です。

1. vRealize Operations Manager の「環境」より「カスタム グループ」をクリックします。

「カスタム グループ」画面が表示されます。

2. 表示されている任意の定義済みカスタムグループをクリックします。

初期状態では、定義済みカスタムグループとして下記が登録済みです。

グループ	登録オブジェクト
Universe	登録されている全てのオブジェクト
vSphere World	クラスタ・ESXi ホストや仮想マシンなど、vSphere 環境を構成するオブジェクト
PureStorage World	専用ストレージとして登録されているオブジェクト

関連するオブジェクトが表示されます。

> **補足** 定義済みカスタムグループや、お客さまにてカスタムグループを作成する際にメンバーシップ条件等で、参照権限が無い当社管理用オブジェクトが含まれる規則(オブジェクト名の正規表現など)で設定された場合、グループ内でお客さまが参照できるオブジェクト数と「サマリ」や「キャパシティ」に表示されるオブジェクト数に差分が発生する可能性がございます。

3. オブジェクトグループを展開し、利用状況を参照するオブジェクトをクリックします。

選択したオブジェクトの情報が表示されます。

4. オブジェクト情報の詳細画面では、参照したい情報のメニュータブをクリックします。

選択したメニュータブの情報が表示されます。

• サマリ

サマリタブでは、選択したオブジェクトの各種情報が一覧で表示されます。

表示される内容はオブジェクトのタイプにより異なります。

例えば仮想マシンを選択した場合、サマリタブには下記の情報が表示されます。

ウィジェット	表示内容
オブジェクトサマリ	オブジェクトの電源状態や IP アドレス、ハードウェア情報
アクティブアラート	発生中のアラート
残り時間	仮想マシンのリソース利用状況が、割り当てられたリソースサイズを超過するまでの想定残り期間。CPU、メモリ、ディスクのうち最も制約が大きいリソースと、リソース利用状況のトレンドから計算されます
残りキャパシティ	CPU、メモリ、ディスクのうち最も制約が大きいリソースの残り容量
使用率	CPU、メモリ、ディスクの利用状況
パフォーマンス	CPU、メモリ、ディスクのパフォーマンス情報
構成	割り当てられたリソースやネットワークの接続情報
ping 統計情報	Ping による監視の統計情報。本サービスでは有効になっていません

• アラート

アラートタブには、現在までに発生したアラートの履歴が表示されます。

• メトリック

メトリックタブでは、対象オブジェクトで収集されている全てのデータメトリックを選択して表示することが可能です。

メトリックのリストから表示させるメトリックをダブルクリックして、メトリックグラフを表示させます。

• キャパシティ

キャパシティタブでは、CPU、メモリ、ディスクのそれぞれの予測された「残り時間」と「残りキャパシティ」を表示することが可能です。

• イベント

イベントタブでは、現在までに発生したイベントや、トリガされたシンプトム・アラートの履歴を参照することが可能です。

補足 イベントとは、オブジェクトに対する何らかの変更のことで、そのオブジェクトのメトリックの変化によって定義されます。オブジェクトへの変更をシンプトムやほかのデータと比較して、発生したアラートの考えられる原因を特定できます。

• 詳細

詳細タブでは、オブジェクトに関連するビュー、ヒートマップ、ワークロードを参照することが可能です。

• 環境

環境タブでは、オブジェクトの依存関係と、関連オブジェクトのリストを参照することが可能です。
依存関係の表示では、各オブジェクトの健全性評価をあわせて確認することが可能になっており、発生した問題の影響範囲を特定できます。

• レポート

レポートタブでは、オブジェクトが含まれるレポートテンプレートの一覧と、生成済みレポートが表示されます。
レポートテンプレートの一覧では、選択したレポートの生成実行や編集・実行スケジュールの設定を行うことが可能です。

7.6. カスタムダッシュボードによる専用ストレージの容量管理

本サービスでは、専用ストレージの利用状況を確認するためのカスタムダッシュボードをご提供いたします。
カスタムダッシュボードは、下記手順で参照可能です。

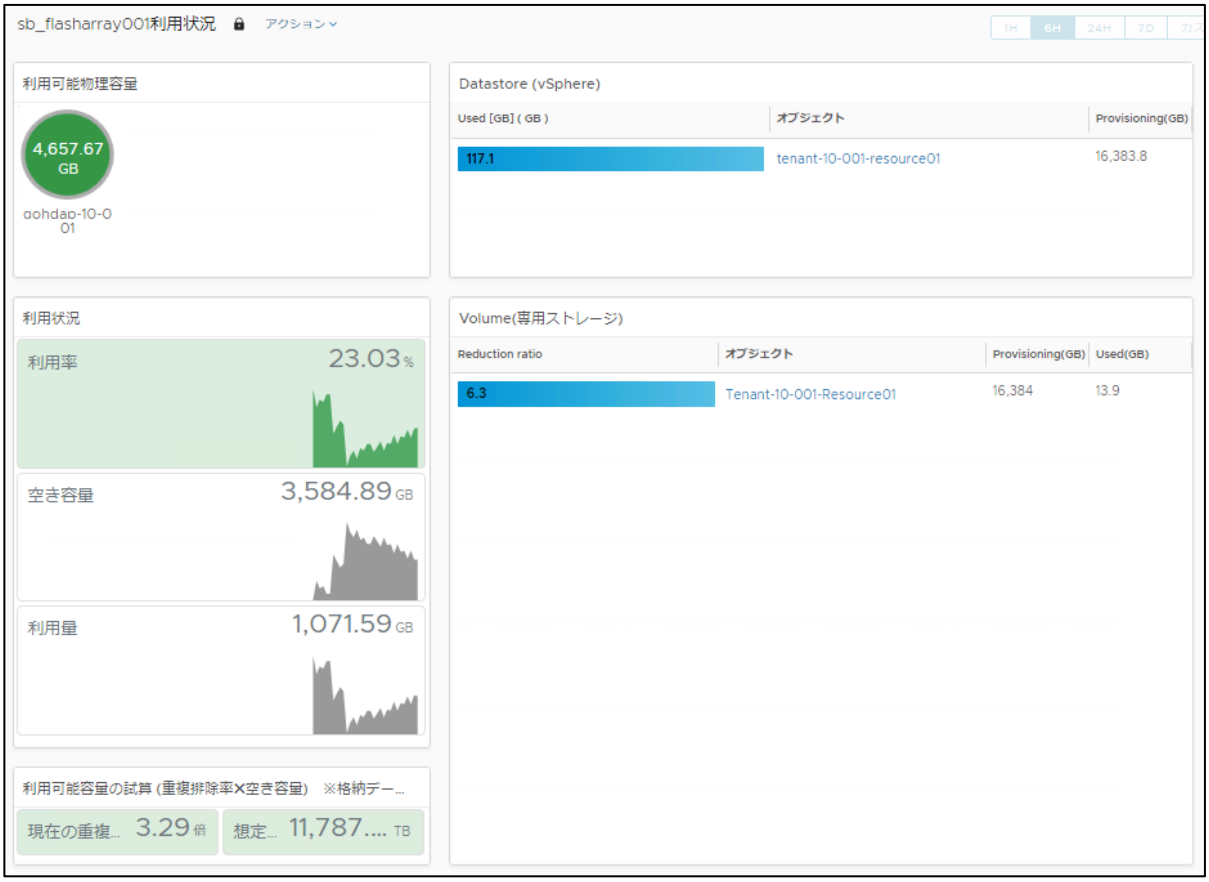
> **重要**
>
> **専用ストレージの残り容量管理について**
>
> 本サービスでご提供する専用ストレージの使用容量・残り空き容量は、本機能にてご確認いただく必要があります。
> VMware vCenter Server から確認できるデータストアの空き容量は、実際の残り空き容量とは異なりますので、本機能にて定期的にご確認をお願いいたします。

1. **vRealize Operations Manager の「可視化」より「ダッシュボード」をクリックします。**

   直近で開いていたダッシュボードが表示されます。直近で開いていたダッシュボードが無い場合は「ホーム」の画面が表示されます。

2. **「管理」より一覧から、「sb_flasharray001 利用状況」をクリックします。**

   「sb_flasharray001 利用状況」ダッシュボードが表示されます。



ウィジェット	表示内容
利用可能物理容量	専用ストレージの、ご利用いただける全体容量
利用状況	下記 3 点の使用状況表示と、直近 30 日の推移のグラフ ・ 利用率：現在のストレージ使用量が利用可能物理容量に占める割合 ・ 空き容量：未使用のストレージ容量（＝利用可能物理容量 - 現在の使用量） ・ 利用量：現在のストレージ使用量
利用可能容量の試算	現在の重複排除・圧縮率を維持した場合に利用できる容量の想定値。 （= 重複排除・圧縮率 × 残り容量）
Datastore(vSphere)	vCenter から見たデータストアごとの使用量の一覧表示。 重複排除や圧縮がかかっていない状態の使用量を表示。
Volume(専用ストレージ)	専用ストレージ内の Volume ごとの使用量の一覧表示。 重複排除や圧縮がかかった状態の使用量を表示 **補足** ベアメタルサーバご利用時、ベアメタルサーバ用Volumeの情報がここに表示されます。

補足 利用量などの計算には当社管理用に利用している領域も含まれます。

重要 **利用可能容量の試算について**

「利用可能容量の試算」の値は、現在の重複排除率を維持した場合に利用できる残り空き容量の予想サイズです。
重複排除率の値は、格納されたデータの内容により変動しますので、残り容量と合わせて、定期的なご確認をお願いいたします。

8. 移行ツール（VMware HCX）

2つのvSphere環境間でのVM移行機能をご提供いたします。

本項では、お客さまvSphere環境を移行元サイト、当社プライベートクラウド環境を移行先サイトとして手順を記載いたします。

重要

移行ツールの提供形態について

本オプションはライセンスのみのご提供となります。

製品仕様や操作方法に関するお問い合わせはお受けできません。

移行ツールの提供バージョンについて

VMware HCXはインストール時に最新版に自動アップデートされるため、実際の手順および動作が本書記載の説明と異なる場合があります。最新の製品仕様に関しましては、ヴイエムウェア社の公式ドキュメントをご参照ください。

参照 『VMware HCX Documentation』

移行ツールを構成する仮想マシンは以下の通りです。

サーバ名	機能概要
HCX Manager	移行先サイトにて VMware HCX を管理します
HCX Connector	移行元サイトにて VMware HCX を管理します
HCX Interconnect	仮想マシン移行時のデータ転送を実施します
HCX Network Extension	移行元サイトと移行先サイト間で L2 ネットワークを延伸します

本サービスでは以下の４つの方式が利用可能です。

利用可能な方式	機能概要および必須要件
Cold Migration	パワーオフ状態の仮想マシンを移行する際に自動で本方式が選択されます。 **お客さま環境要件** ・ vCenter Server：5.5 以降 ・ ESXi：5.5 以降 ・ 閉域ネットワークの帯域が 100Mbps 以上 ・ X86 アーキテクチャであること **移行対象仮想マシンの要件** ・ 仮想マシンバージョンが 9 ~ 17 であること ・ VMware Tools がインストールされていること

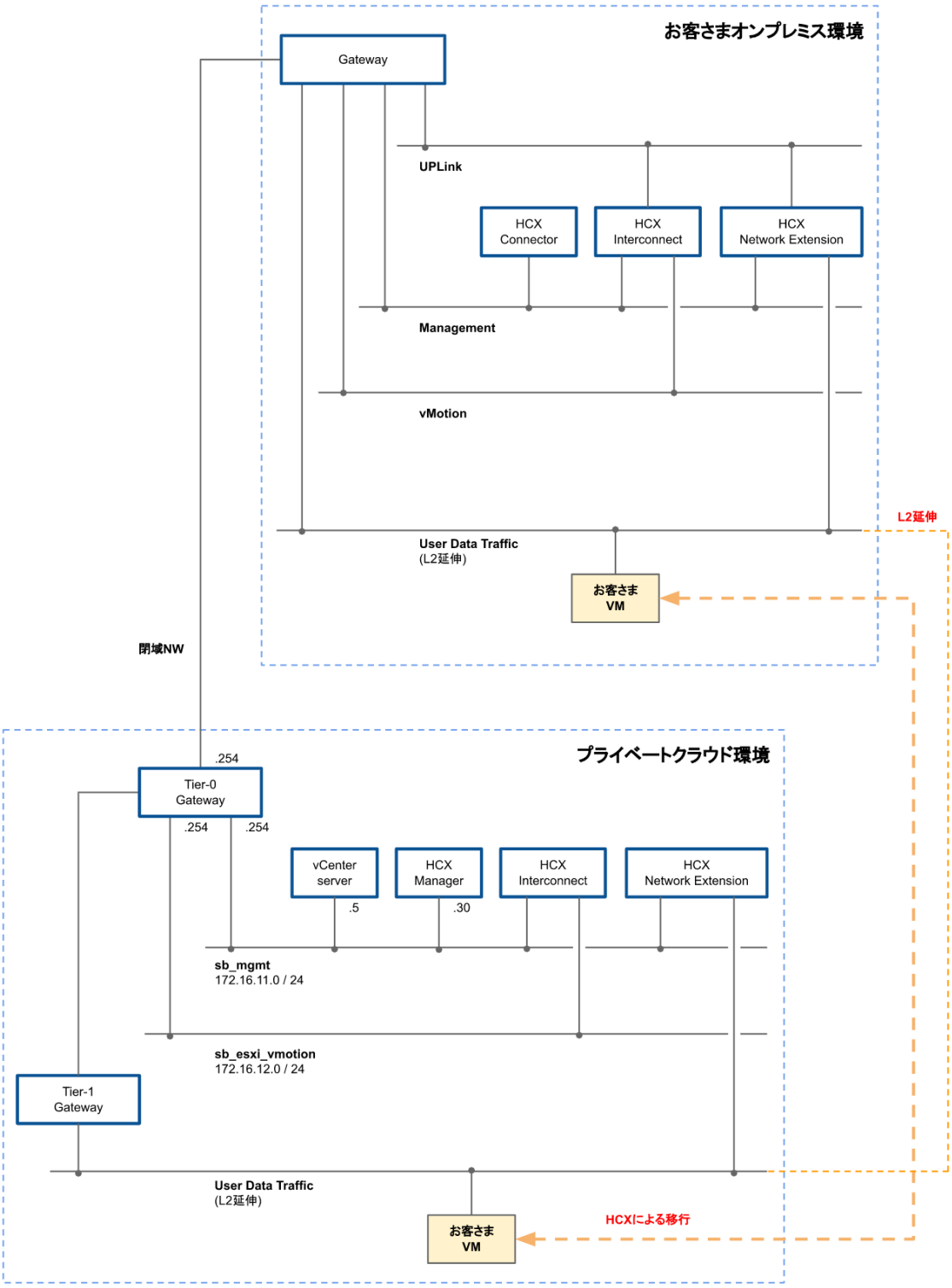
利用可能な方式	機能概要および必須要件
vMotion	vSphere 環境における vMotion と同様の方式ですが、 1 台ずつの移行となります。 **お客さま環境要件** ・ vCenter Server：5.5 以降 ・ ESXi：5.5 以降 ・ 閉域ネットワークの帯域が 100Mbps 以上 ・ X86 アーキテクチャであること **移行対象仮想マシンの要件** ・ 仮想マシンバージョンが 9 ~ 17 であること VMware Tools がインストールされていること
Bulk Migration	複数台の仮想マシンを並行してレプリケーションを実施します。レプリケーション中はソースサイトにてパワーオン状態を継続し、仮想マシンのパワーオフをもってデスティネーションサイトへの切り替えが発生します。ソースサイトには別名にて仮想マシンが保存されるため、切り戻しが容易に行えます。 **お客さま環境要件** ・ vCenter Server：5.1 以降 ・ ESXi：5.0 以降 **移行対象仮想マシンの要件** ・ 仮想マシンバージョンが 7 ~ 17 であること VMware Tools がインストールされていること
Replication-Assisted vMotion※1	複数台の仮想マシンを並行してレプリケーションを実施します。デスティネーションサイトへの切り替えは vMotion 方式で実施されるため、Bulk Migration のようなダウンは発生しません。ソースサイトに仮想マシンは残りません。 **お客さま環境要件** vCenter Server：5.5 以降 ESXi：5.5 以降 **移行対象仮想マシンの要件** 仮想マシンバージョンが 9 ~ 17 であること VMware Tools がインストールされていること

※1：「Replication-Assisted vMotion」のご利用には、「Enterprise」エディションが必要です

8.1. VMware HCXのインストール

お客さまのオンプレミス環境へVMware HCXのインストールを実施します。当社プライベートクラウド環境側の構築完了のお知らせ後、本手順を実施してください。

本項で説明する手順では、下記ネットワーク構成のvSphere7環境での構築を例に記載しています。
お客さまの環境に合わせ、適宜読み替えを行ってください。



8.1.1. インストーラの準備

以下の手順にて、VMware HCX Connectorのovaファイルをダウンロードします。

1. **プライベートクラウドのHCX Managerへアクセスします。URLは『開通通知書』をご確認ください。**

   VMware HCXのログイン画面が表示されます。

2. **『開通通知書』に記載されている、VMware HCX連携用アカウントにてログインします。**

3. **「Administration」 > 「System Updates」 をクリックします。**

4. **「REQUEST DOWNLOAD LINK」 をクリックします。**

   「COPY LINK」 が表示されます。

5. **「COPY LINK」 をクリックします。**

   クリップボードにダウンロードのURLがコピーされます。

6. **お客さまのオンプレミス環境にて、先のURLからHCX Connectorのダウンロードを実施します。**

8.1.2. HCX Connectorの展開

本項では、VMware HCX Connectorのインストール手順をご説明いたします。

1. **お客さまオンプレミス環境のvCenter Serverへログインします。**

2. **HCX Connectorの展開先のクラスタを右クリックし、「OVFテンプレートのデプロイ」を選択します。**

   「OVFテンプレートのデプロイ」のウィザード画面が開き、「1 OVFテンプレートの選択」画面が表示されます。

3. **「ローカルファイル」から先ほどダウンロードしたovaファイルを指定し、「次へ」をクリックします。**

   「2 名前とフォルダの選択」画面に遷移します。

4. **「仮想マシン名」と仮想マシンの場所を選択し、「次へ」をクリックします。**

   「3 コンピューティングリソースの選択」画面に遷移します。

5. **コンピューティングリソースを選択し、「次へ」をクリックします。**

   「4 詳細の確認」画面に遷移します。

6. **表示された内容を確認のうえ、「次へ」をクリックします。**

   「5 使用許諾契約書」画面に遷移します。

7. **仕様許諾契約書を確認のうえ、「すべての仕様許諾契約書に同意します」にチェックを入れ、「次へ」をクリックします。**

   「6 ストレージの選択」画面に遷移します。

8. **「仮想ディスクフォーマットの選択」、「仮想マシンストレージポリシー」を選択し、「次へ」をクリックします。**

   「7 ネットワークの選択」画面に遷移します。

9. **「ターゲットネットワーク」にてHCX Connector向けの管理セグメントを選択し、「次へ」をクリックします。**

   「8 テンプレートのカスタマイズ」画面に遷移します。

10. 「Password」，「ネットワークプロパティ」，「Static Route」，「DNS」，「サービスの構成」を設定し、「次へ」をクリックします。

「9 設定の確認」画面に遷移します。

> **補足** Static Route は HCX Manager に対して通信が通るよう設定してください。

11. 内容を確認し、「完了」をクリックします。

vCenter Server上にHCX Connectorが展開されます。

8.1.3. HCX Connectorの初期設定

VMware HCX Connectorを初期設定します。

1. **お客さまオンプレミス環境のvCenter Serverへログインします。**

2. **HCX Connectorを右クリックし、「電源」 > 「パワーオン」を選択します。**

   HCX Connectorが起動します。

3. **Webブラウザを開き、下記のURLへアクセスします。**

   https://<HCX ConnectorのIPアドレスまたはホスト名>:9443/login.jsp

4. **ユーザは “admin” , パスワードはHCX Connectorの展開時に設定したパスワードを入力し、「LOG IN」をクリックします。**

   「Activate your HCX instance」画面が開きます。

5. **「HCX License Key」にて、『開通通知書』に記載されているライセンスキーを入力し、「ACTIVATE」をクリックします。**

   ライセンスが認証されると、「Where is your HCX system location?」 画面に遷移します。

6. **「Location of your datacenter (nearest city)」にて、お客さま環境のロケーションを設定し、「CONTINUE」をクリックします。**

   「System Name」画面に遷移します。

7. **「System Name」 に任意の名称を設定し、「CONTINUE」をクリックします。**

   「Congratulations! You have successfully activated your HCX.」 画面に遷移します。

8. **「YES, CONTINUE」をクリックします。**

   「Connect your vCenter」画面に遷移します。

9. **「vCenter Server」,「Username」,「Password」 を入力し、「CONTINUE」をクリックします。**

   「Configure SSO/PSC」画面に遷移します。

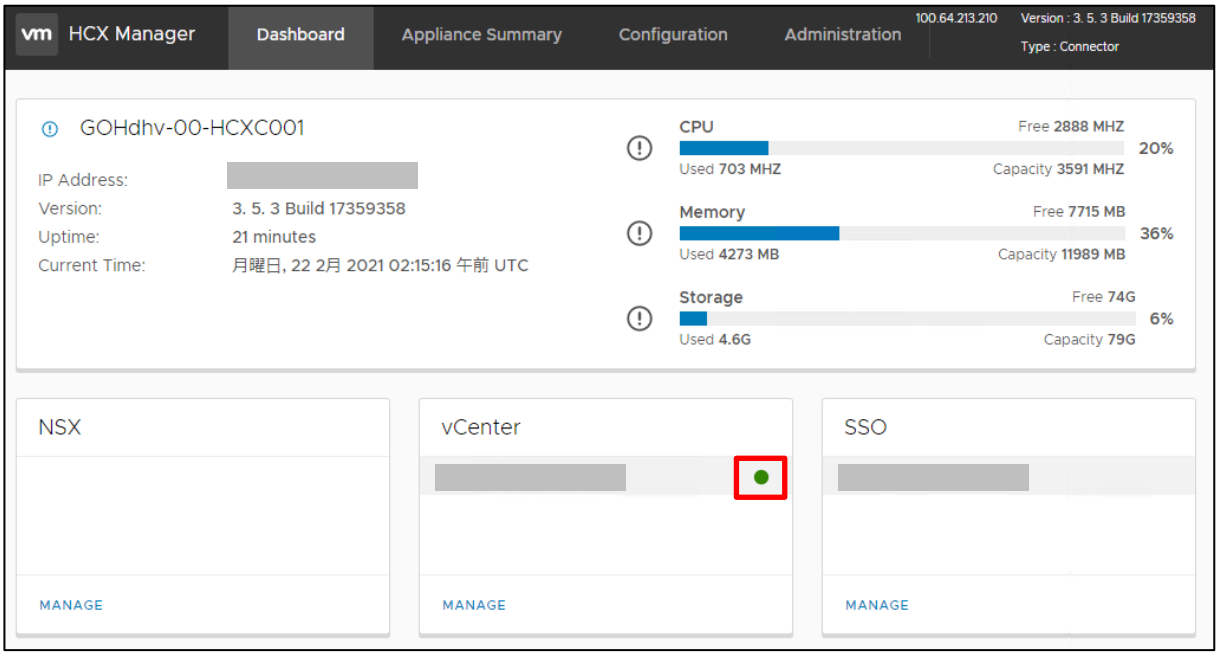
10. **「Identity Sources」を設定し、「CONTINUE」をクリックします。**

    「Conguratulations!」 画面に遷移します。

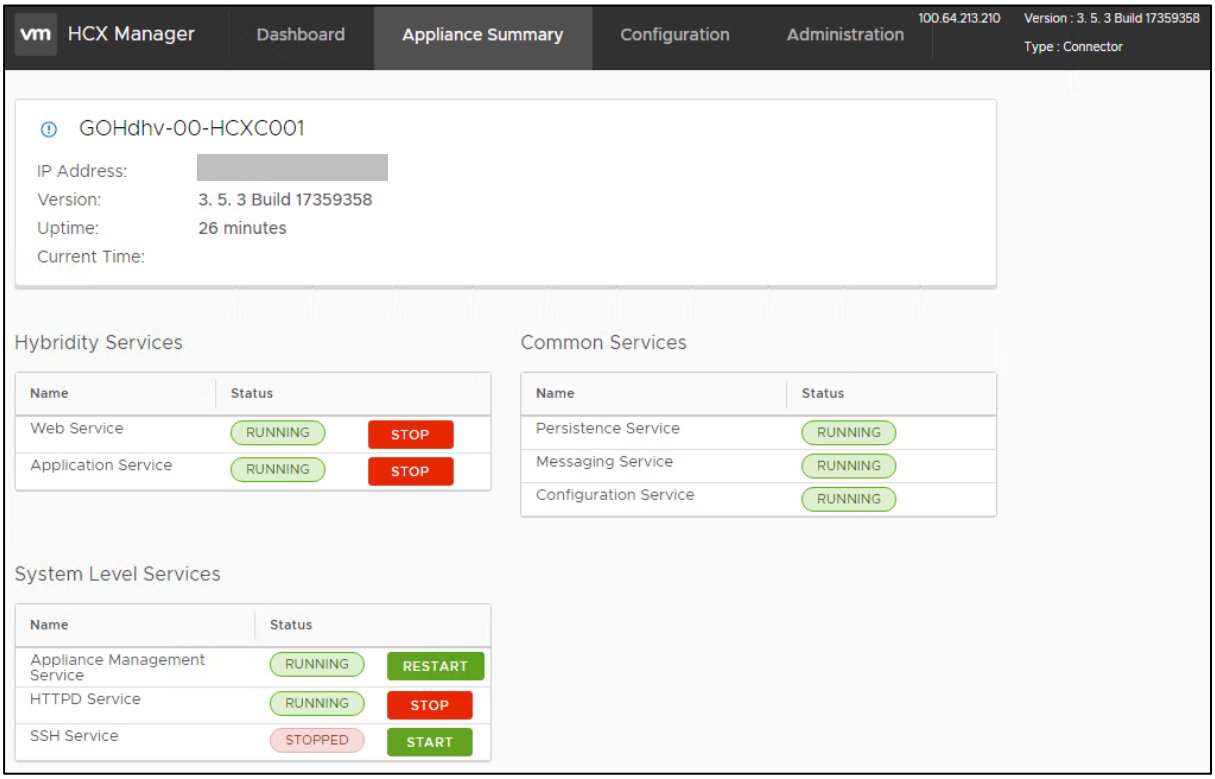
11. これまでの設定内容を確認の上、「RESTART」をクリックします。

「Dashboard」画面に自動遷移します。

12. vCenter Server欄がグリーンであることを確認します。



13. 「Appliance Summary」タブを開き、SSHを除く各種サービスが「RUNNING」であることを確認します。



8.1.4. プライベートクラウドとの連携

当社プライベートクラウド環境とお客さまオンプレミス環境のVMware HCXを連携します。

環境間の Site Pairing

1. **お客さまオンプレミス環境にて、下記URLへアクセスし、初期設定時に指定したIdentity Source上のアカウントにてログインします。**

   https://<HCX ConnectorのIPアドレスまたはホスト名>/hybridity/ui/hcx-client/index.html#/login

   参照 「8.1.3 HCX Connectorの初期設定」

2. **「Infrastructure」 >「Site Pairing」 を開き、「CONNECT TO REMOTE SITE」 をクリックします。**

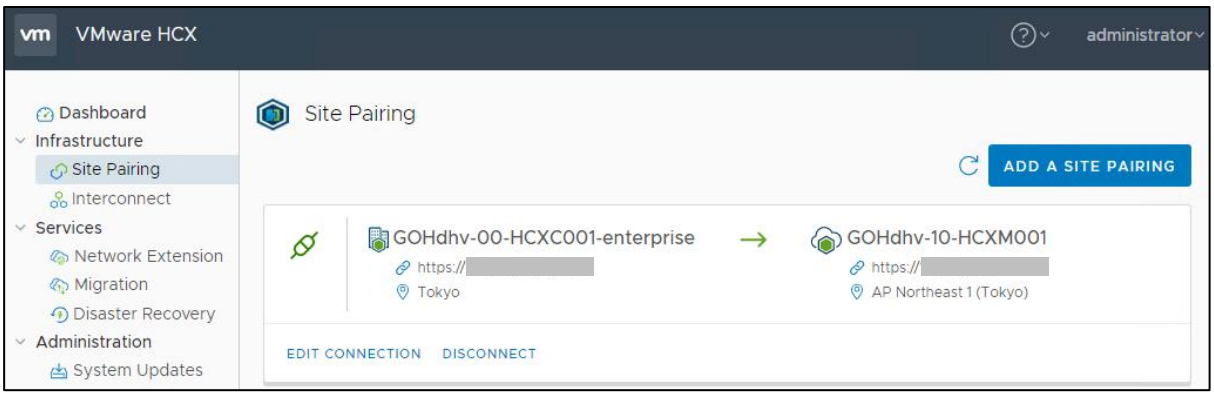
   「Connect to Remote Site」画面が開きます。

3. **「Remote HCX URL」,「Username」,「Password」 に『開通通知書』に記載された値を入力し、「CONNECT」をクリックします。**

   「Certificate Warning」画面が表示されます。

4. **「IMPORT CERTIFICATE」をクリックします。**

   プライベートクラウド環境との通信が成功すると、下記画面が表示されます。



Network Profile の作成

Network Profileは今後の手順で自動展開されるVMware HCXのアプライアンスに対するネットワーク設定を定義するものです。

1. **「Infrastructure」 > 「Interconnect」 > 「Network Profiles」タブを開き、「CREATE NETWORK PROFILE」をクリックします。**

2. **「vCenter」,「Network」,「Name」,「IP Pools」,「MTU」 をお客さま環境に合わせて設定し、「CREATE」をクリックします。**

> **補足** 当社プライベートクラウド環境では、プライベートクラウド側HCX Managerとの通信用のアップリンク、各種アプライアンスの管理ネットワーク、vMotionネットワークの3つのプロファイルを定義しています。

Compute Profile の作成

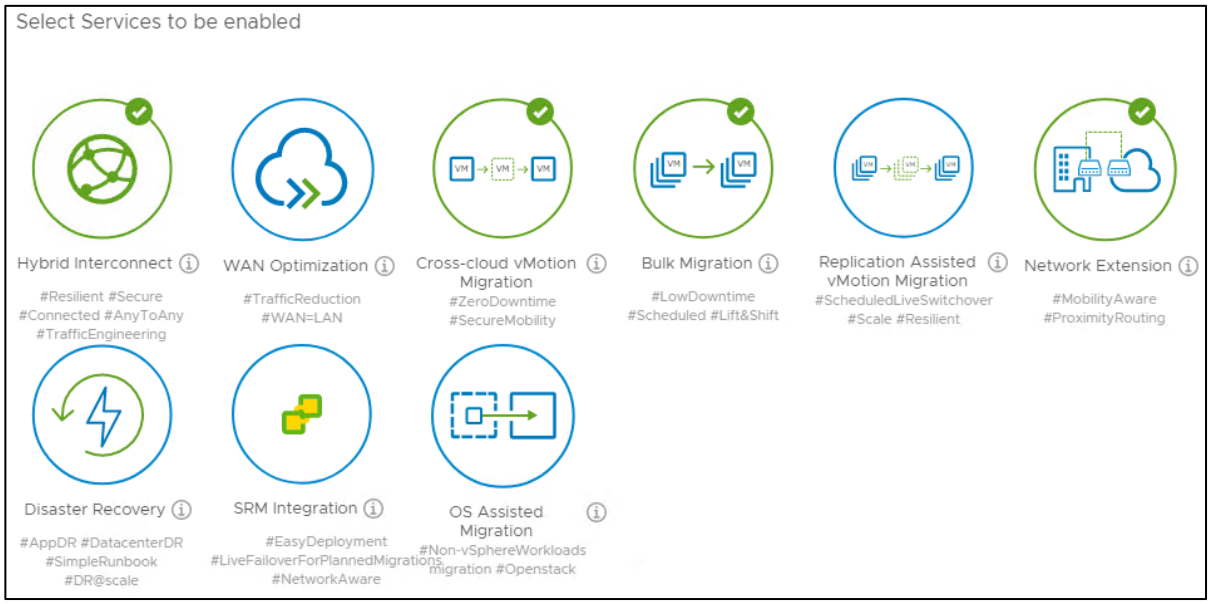
1. **「Infrastructure」 > 「Interconnect」 > 「Compute Profiles」タブを開き、「CREATE COMPUTE PROFILE」をクリックします。**

   「Name your Compute Profile」画面が開きます。

2. **「Name your Compute Profile」にて任意の名称を入力し、「CONTINUE」をクリックします。**

   「Select Service to be enabled」画面が開きます。

3. **「Hybrid Interconnect」,「Cross-cloud vMotion」,「Bulk Migration」,「Network Extension」 にチェックを入れ、「WAN Optimization」,「Disaster Recovery」,「SRM Integration」,「OS Assisted Migration」からチェックを外します。「Enterprise」エディションをお申込み済みのお客さまについては、「Replication Assisted vMotion Migration」にもチェックを入れ、「CONTINUE」をクリックします。**



「Select Service Resource」画面に遷移します。

4. **「Select Resource」にて、アプライアンスの展開先を指定し、「CONTINUE」をクリックします。**

   「Select Deployment Resource and Reservation」画面に遷移します。

5. 「Select Resource」,「Select Datastore」,「Select Folder」,「CPU Reservation」,「Memory Reservation」をお客さま環境に合わせて設定し、「CONTINUE」をクリックします。

「Select Management Network Profile」画面に遷移します。

6. 「Select Management Network Profile」にて、先ほど作成した管理ネットワーク向けの Network Profile を指定し、「CONTINUE」をクリックします。

「Select Uplink Network Profile」画面に遷移します。

7. 「Select Uplink Network Profile」にて、先ほど作成したアップリンク向けの Network Profile を指定し、「CONTINUE」をクリックします。

「Select vMotion Network Profile」画面に遷移します。

8. 「Select vMotion Network Profile」にて、先ほど作成したvMotion向けの Network Profile を指定し、「CONTINUE」をクリックします。

「Select vSphere Replication Network Profile」画面に遷移します。

9. 「Select vSphere Replication Network Profile」にて、先ほど作成した管理ネットワーク向けの Network Profile を指定し、「CONTINUE」をクリックします。

「Select Network Containers Eligible for Network Extension」画面に遷移します。

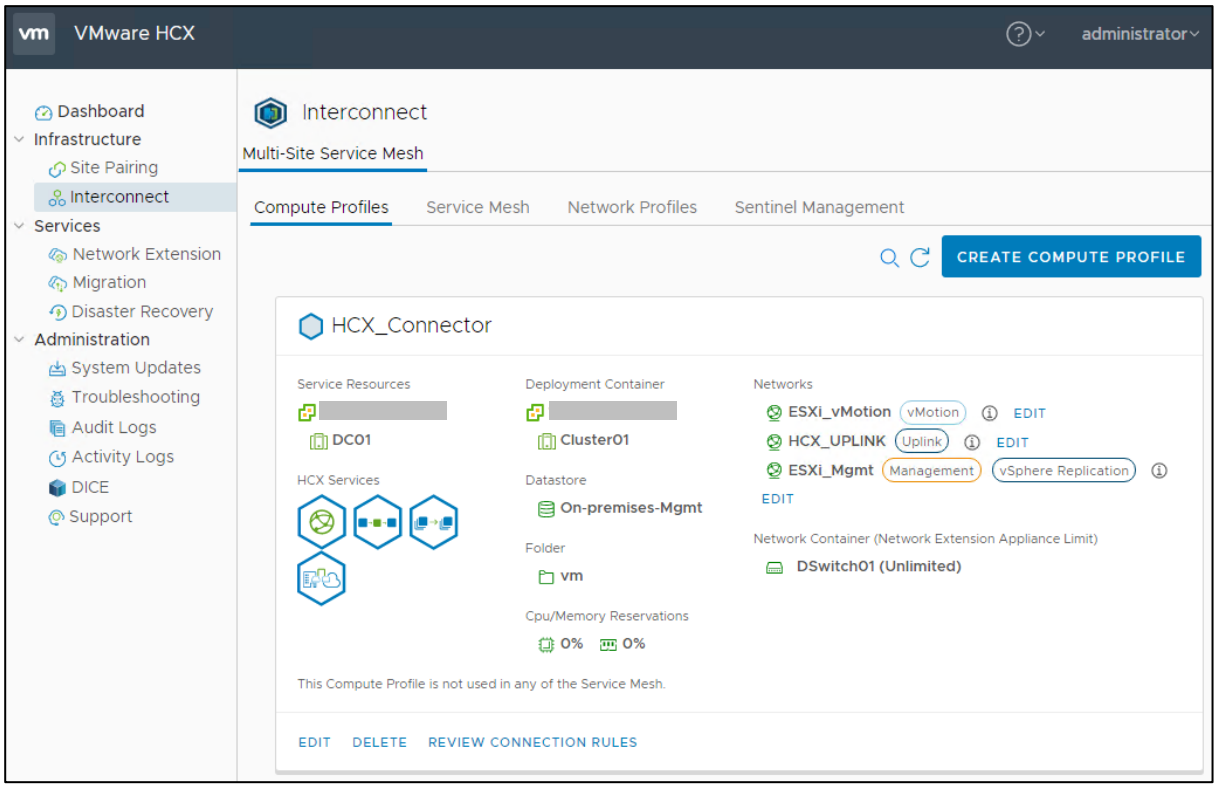
10. 「Select Network Containers」にて、ネットワークのL2延伸をする任意の仮想スイッチを選択し、「CONTINUE」をクリックします。

「Review Connection Rules」画面に遷移します。

11. VMware HCXの構成に必要な通信要件が表示されるので、お客さまネットワーク環境のファイアウォール設定にて通信要件が満たされていることを確認し、「CONTINUE」をクリックします。

「Ready to Complete」画面に遷移します。

12. 「FINISH」をクリックします。



Service Mesh の作成

1. 「Infrastruncure」 > 「Interconnect」 > 「Service Mesh」 を開き、「CREATE SERVICE MESH」をクリックします。

「Select Sites」画面が開きます。

2. VMware HCXを構成するHCX Connector(お客さまオンプレミス環境)およびHCX Manager(当社プライベートクラウド環境)を選択し、「CONTINUE」をクリックします。

「Select Compute Profiles」画面に遷移します。

3. 「Select Source Compute Profile」にて、お客さまの作成したCompute Profileを指定し、「Select Remote Compute Profile」にて「sb_compute_profile」を指定し、「CONTINUE」をクリックします。

「Select Service to be enabled」画面に遷移します。

4. 「Hybrid Interconnect」,「Cross-cloud vMotion Migration」,「Bulk Migration」,「Network Extension」,「Replication Assisted vMotion Migration」(Enterprise オプションをご契約の場合のみ)が選択されていることを確認し、「CONTINUE」をクリックします。

「Advanced Configuration - Override Uplink Network profiles (Optional)」画面に遷移します。

5. 「Select Source Site Uplink Network Profile(s) 」にて、アップリンク向けのプロファイルを、「Select Destination Site Uplink Network Profile(s)」にて「sb_mgmt」を指定し、「CONTINUE」をクリックします。

「Advanced Configuration - Network Extension Appliance Scale Out」画面に遷移します。

6. デフォルト設定のまま、「CONTINUE」をクリックします。

「Advanced Configuration - Traffic Engineering」画面に遷移します。

7. 必要に応じ、「Application Path Resiliency」,「TCP Flow Conditioning」の設定を有効化し、「CONTINUE」をクリックします。

「Review Topology Preview」画面に遷移します。

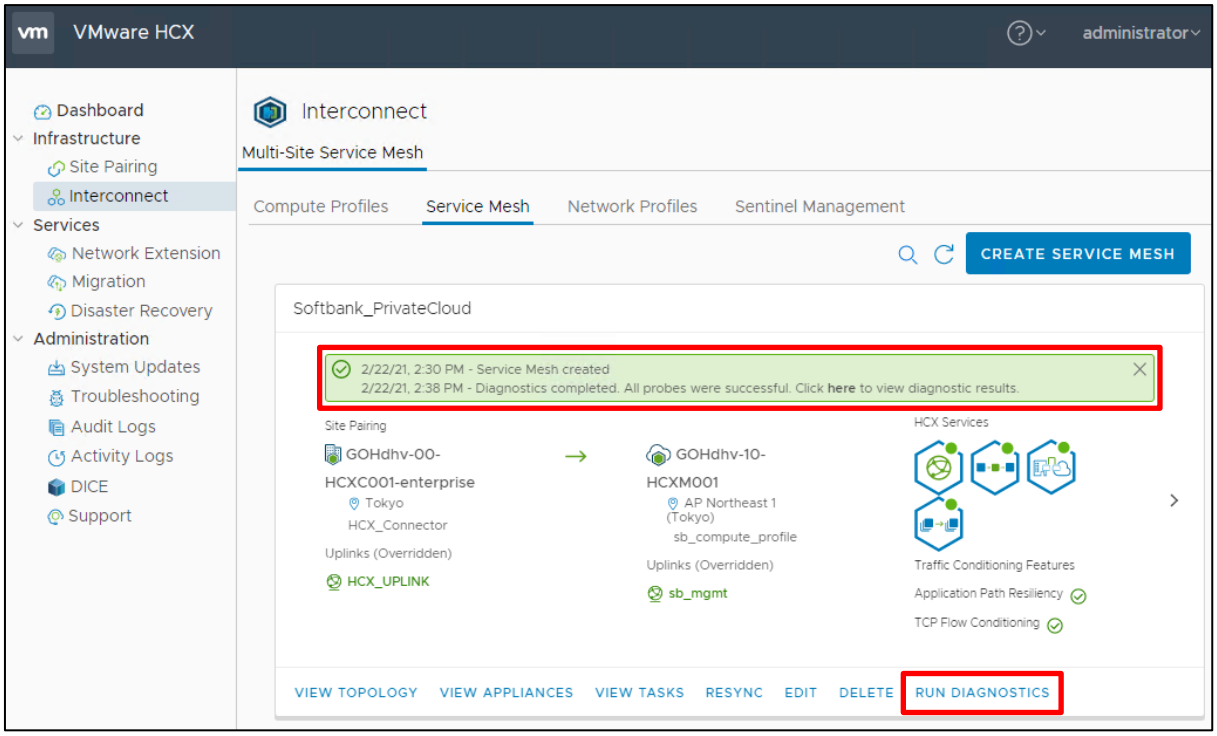
8. 「CONTINUE」をクリックします。

「Ready to Complete」画面に遷移します。

9. 「Provide a user friendly name for this Service Mesh」に任意の Service Mesh Name を入力し、「FINISH」をクリックします。

お客さま環境にて、< Service Mesh Name >-IXI1 および < Service Mesh Name >-NEI1 という仮想マシンが自動で展開されます。また、< Service Mesh Name >-IXI1 にアサインされた管理用IPアドレスにて仮想的なESXiが構築されます。当社プライベートクラウド環境に対しても同様に、< Service Mesh Name >-IXR1 および < Service Mesh Name >-NER1 が自動展開され、仮想的なESXiが構築されます。

10. 「RUN DIAGNOSTICS」をクリックし、「Diagnostics completed. All probes were successful」　と表示されることを確認します。



「RUN DIAGNOSTICS」の実施により接続の問題を検知した場合は、画面上に通信条件を満たしていない項目が示されます。

Network Extension の設定

Network Extension の設定は、お客さまオンプレミス環境のネットワークと、当社プライベートクラウド環境の間でのL2延伸を実施するための手順です。

移行前後で仮想マシンが接続するネットワークを変更したくない場合は、本設定を行ってください。

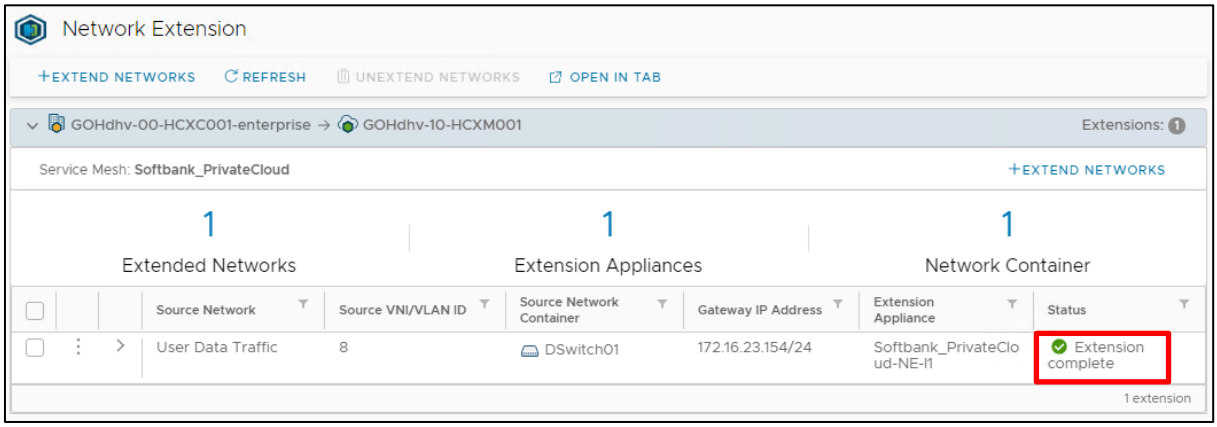
1. **「Services」 > 「Network Extension」を開き、「CREATE A NETWORK EXTENSION」をクリックします。**

   「Select source networks for extension to remote site」画面が開きます。

2. **「Select Service Mesh」にて先ほど作成したService Meshを指定します。当社プライベートクラウド環境へ延伸したいネットワークにチェックを入れ、「NEXT」をクリックします。**

3. **「Destination First Hop Router」にて「tier-1_gateway」を選択し、「Gateway IP Address」に延伸するネットワークから払い出した空きIPアドレスを入力し、「SUBMIT」をクリックします。**

4. **「Extension complete」と表示されることを確認します。**



8.2. VMware HCXによるVMの移行

お客さまのオンプレミス環境から当社プライベートクラウド環境への移行操作について記載いたします。

8.2.1. Cold Migration

パワーオフの状態の仮想マシンを移行する方式です。

1. **お客さまオンプレミス環境にてHCX Connectorへアクセスします。**

2. **「Services」 > 「Migration」 を開き、「MIGRATE」をクリックします。**
   「Workload Mobility」 画面が表示されます。

3. **「Group Name」に任意の名称を入力します。**

4. **移行対象の仮想マシンを選択し、「ADD」をクリックします。**
   移行先リソースを設定する画面へ移行します。

5. **「Transfer and Placement」 > 「(Mandatory: Compute Container)」にて移行先のクラスタまたはリソースプールを選択します。**

> ☑重要
> ・プライベートクラウド環境のリソースを指定する際、「sb_」から始まる名称のリソースは当社管理用リソースのため選択しないでください(権限不足のため移行が失敗します)
> ・以降の手順で選択するフォルダ、データストアに関しても同様です。

6. **「Transfer and Placement」 > 「(Specify Destination Folder)」にて移行先のフォルダを選択します。**

7. **「Transfer and Placement」 > 「(Mandatory: Storage)」にて移行先のデータストアを選択します。**

> ☑重要
> 移行先のデータストア選択にエコノミーストレージデータストアは指定しないでください。

8. **仮想マシンのDisk Formatを変更する際は、「Transfer and Placement」 > 「(Same format as source)」より選択します。**

9. 「VM for Migration」 > 「MigrationProfile」 が 「Cold Migration」であることを確認します。

10. 「VALIDATE」をクリックし、「Validation is Successful, You can proceed with Migration」と表示されることを確認します。

11. 「GO」をクリックします。

「Migration completed」と表示されるまで待ちます。

12. プライベートクラウド環境の指定したリソースに仮想マシンが移行していることを確認します。

8.2.2. vMotion

パワーオン状態の仮想マシンを１台ずつ移行する方式です。当社プライベートクラウドへの切り替わり際に移行対象のVMネットワークに瞬断が発生します。

1. **お客さまオンプレミス環境にてHCX Connectorへアクセスします。**

2. **「Services」 > 「Migration」 を開き、「MIGRATE」をクリックします。**
   「Workload Mobility」 画面が表示されます。

3. **「Group Name」に任意の名称を入力します。**

4. **移行対象の仮想マシンを選択し、「ADD」をクリックします。**
   移行先リソースを設定する画面へ移行します。

5. **「Transfer and Placement」 > 「(Mandatory: Compute Container)」にて移行先のクラスタまたはリソースプールを選択します。**

> **重要**
> ・プライベートクラウド環境のリソースを指定する際、「sb_」から始まる名称のリソースは当社管理用リソースのため選択しないでください(権限不足のため移行が失敗します)
> ・以降の手順で選択するフォルダ、データストアに関しても同様です。

6. **「Transfer and Placement」 > 「(Specify Destination Folder)」にて移行先のフォルダを選択します。**

7. **「Transfer and Placement」 > 「(Mandatory: Storage)」にて移行先のデータストアを選択します。**

> **重要**
> 移行先のデータストア選択にエコノミーストレージデータストアは指定しないでください。

8. **仮想マシンのDisk Formatを変更する際は、「Transfer and Placement」 > 「(Same format as source)」より選択します。**

9. **「Transfer and Placement」 > 「(Migration Profile)」より「vMotion」を選択します。**

10.「VALIDATE」をクリックし、「Validation is Successful, You can proceed with Migration」と表示されることを確認します。

11.「GO」をクリックします。

「vMotion Transfer In Progress」と表示されるので、「Migration completed」と表示されるまで待ちます。

12. プライベートクラウド環境の指定したリソースに仮想マシンが移行していることを確認します。

8.2.3. Bulk Migration

パワーオン状態の仮想マシンを複数平行してプライベートクラウド環境へレプリケーションし、切り替わりの際に仮想マシンの再起動が発生します。

1. **お客さまオンプレミス環境にてHCX Connectorへアクセスします。**

2. **「Services」 > 「Migration」 を開き、「MIGRATE」をクリックします。**
   「Workload Mobility」 画面が表示されます。

3. **「Group Name」に任意の名称を入力します。**

4. **移行対象の仮想マシンを選択し、「ADD」をクリックします。**
   移行先リソースを設定する画面へ移行します。

5. **「Transfer and Placement」 > 「(Mandatory: Compute Container)」にて移行先のクラスタまたはリソースプールを選択します。**

> **重要**
> ・プライベートクラウド環境のリソースを指定する際、「sb_」から始まる名称のリソースは当社管理用リソースのため選択しないでください(権限不足のため移行が失敗します)
> ・以降の手順で選択するフォルダ、データストアに関しても同様です。

6. **「Transfer and Placement」 > 「(Specify Destination Folder)」にて移行先のフォルダを選択します。**

7. **「Transfer and Placement」 > 「(Mandatory: Storage)」にて移行先のデータストアを選択します。**

> **重要**
> 移行先のデータストア選択にエコノミーストレージデータストアは指定しないでください。

8. **仮想マシンのDisk Formatを変更する際は、「Transfer and Placement」 > 「(Same format as source)」より選択します。**

9. **「Transfer and Placement」 > 「(Migration Profile)」より「Bulk Migration」を選択します。**

10. 「Transfer and Placement」 > 「(Option: Switchover Schedule)」より、移行仮想マシンの切り替わり(仮想マシンのシャットダウン)をスケジュールします。

補足	・「Ignore failover windows and start migration as soon as possible」 にチェックを入れた場合は、データのレプリケーションが完了次第、プライベートクラウド環境への切り替え（仮想マシンの再起動）が実施されます。 ・Switchover schedule にて指定した日時まで、仮想マシンはお客さまオンプレミス環境上で動作します。

11. 「VALIDATE」をクリックし、「Validation is Successful, You can proceed with Migration」と表示されることを確認します。

12. 「GO」をクリックします。

データのレプリケーションが完了すると、「Waiting for schedule switchover window」と表示されます。

「Ignore failover windows and start migration as soon as possible」オプションにチェックを入れた場合は引き続き「switchover started」, 「Migration completed」と処理されます。

補足	• 「Waiting for schedule switchover window」 と表示された仮想マシンについては、個別にスケジュール設定の変更を実施することで、即座にプライベートクラウド環境への切り替え処理を実施可能です。 • 対象の仮想マシンにチェックを入れ、「SCHEDULE」ボタンをクリックします。「Ignore failover windows and start migration as soon as possible」にチェックし、「APPLY」ボタンをクリックすることで、処理が実行されます。 • 本手順により、複数の仮想マシンを同時にBulk Migrationを実施した場合にも、仮想マシンごとに再起動のタイミングを制御することが可能です。

13. プライベートクラウド環境の指定したリソースに仮想マシンが移行していることを確認します。

補足	**Bulk Migration 移行実施後の移行元仮想マシンについて** Bulk Migration による移行を実施した仮想マシンは、移行元にはリネームされた状態で仮想マシンが保存された状態となります。 万一切り戻しを行う際は、移行先の仮想マシンを停止し、移行元のリネームされた仮想マシンを起動することで、迅速な復旧を行うことが可能です。

8.2.4. Replication-Assisted vMotion

パワーオン状態の仮想マシンを複数台同時に移行する方式です。当社プライベートクラウドへの切り替わり際に移行対象の仮想マシンネットワークに瞬断が発生します。

1. **お客さまオンプレミス環境にてHCX Connectorへアクセスします。**

2. **「Services」 > 「Migration」 を開き、「MIGRATE」をクリックします。**
   「Workload Mobility」 画面が表示されます。

3. **「Group Name」に任意の名称を入力します。**

4. **移行対象の仮想マシンを選択し、「ADD」をクリックします。**
   移行先リソースを設定する画面へ移行します。

5. **「Transfer and Placement」 > 「(Mandatory: Compute Container)」にて移行先のクラスタまたはリソースプールを選択します。**

> **重要**
> ・プライベートクラウド環境のリソースを指定する際、「sb_」から始まる名称のリソースは当社管理用リソースのため選択しないでください(権限不足のため移行が失敗します)
> ・以降の手順で選択するフォルダ、データストアに関しても同様です。

6. **「Transfer and Placement」 > 「(Specify Destination Folder)」にて移行先のフォルダを選択します。**

7. **「Transfer and Placement」 > 「(Mandatory: Storage)」にて移行先のデータストアを選択します。**

> **重要**
> 移行先のデータストア選択にエコノミーストレージデータストアは指定しないでください。

8. **仮想マシンのDisk Formatを変更する際は、「Transfer and Placement」 > 「(Same format as source)」より選択します。**

9. **「Transfer and Placement」 > 「(Migration Profile)」より「Replication-assisted vMotion」を選択します。**

10.「VALIDATE」をクリックし、「Validation is Successful, You can proceed with Migration」と表示されることを確認します。

11.「GO」をクリックします。

「Migration completed」と表示されるまで待ちます。

12. プライベートクラウド環境の指定したリソースに仮想マシンが移行していることを確認します。

8.3. VMware HCXのアンインストール

お客さまのオンプレミス環境からVMware HCXのアンインストールを実施します。下記手順に従いオンプレミス環境からアンインストールを実施した後、当社サポート窓口または担当営業・SEへご連絡ください。当社プライベートクラウド上のお客さまテナントより、HCX Managerの削除を実施します。

8.3.1. アンインストール

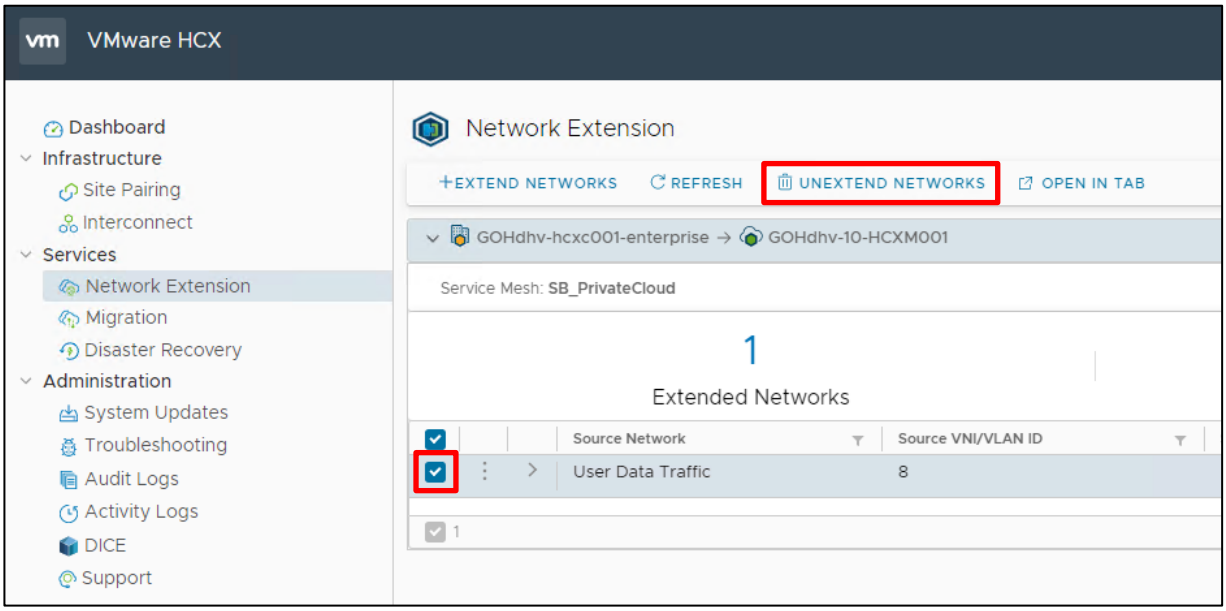
VMware HCXおよび関連する仮想マシンをアンインストールします。

> **重要**
> ・本手順を実施する前に、オンプレミス環境とプライベートクラウド環境間を移行中の仮想マシンが
> 存在しないことを確認してください。またプライベートクラウド環境に移行した仮想マシンが、L2延伸をしたネットワークを利用していないことをご確認ください。
> ・本書と異なる環境や設定を実施された場合は、必要に応じヴイエムウェア社の公式ドキュメントをご参照くださいの上、アンインストールを実施してください。
> **参照** 『Uninstalling VMware HCX』

1. **Webブラウザよりお客さまオンプレミス環境のVMware HCXの管理画面にログインします。**

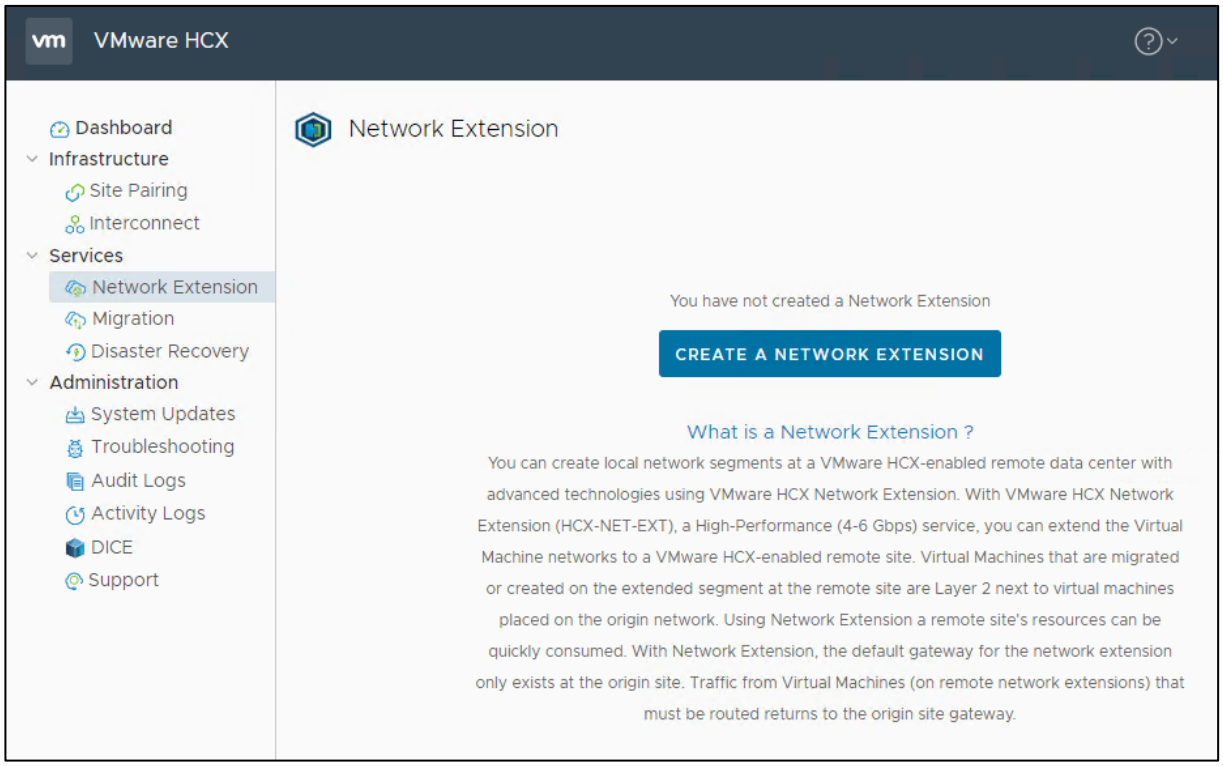
2. **左ペインより「Services」 > 「Network Extension」 をクリックします。**

3. **全てのネットワークにチェックを入れ、「UNEXTEND NETWORK」をクリックします。**
   「Unextend Networks」 画面が表示されます。



4. 「UNEXTED」ボタンをクリックします。

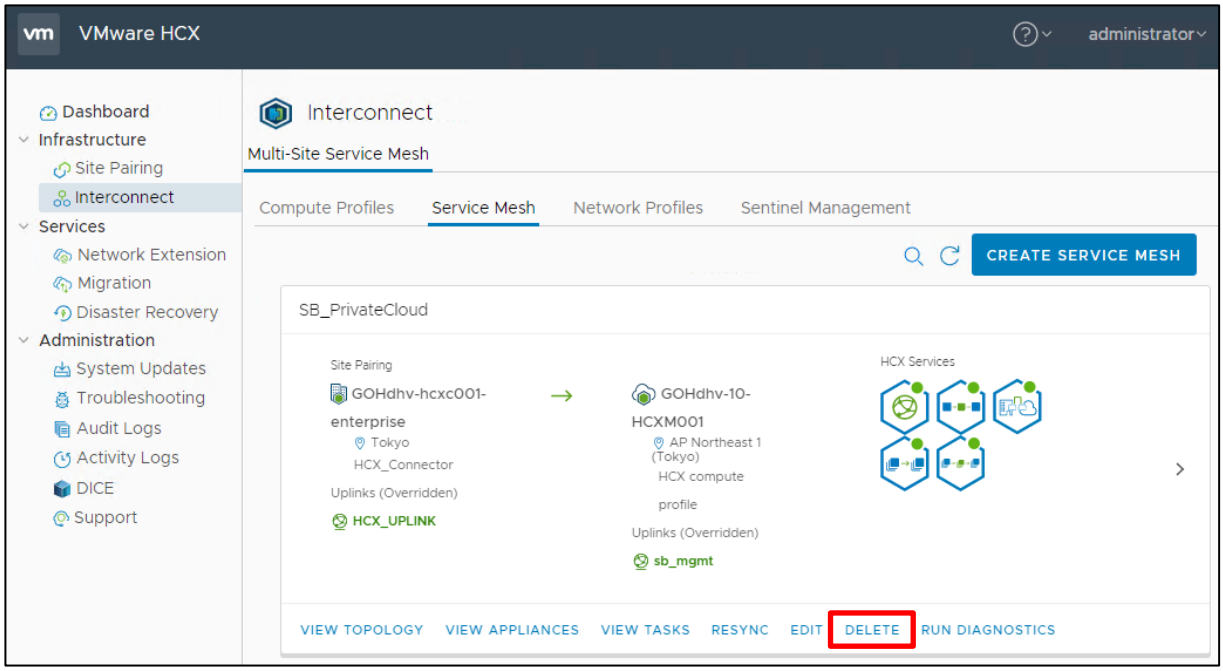
「Status」 欄に処理の進捗が表示されるので、下記画面に遷移するまで待ちます。



5. 左ペインより 「Infrastructure」 > 「Interconnect」 をクリックします。

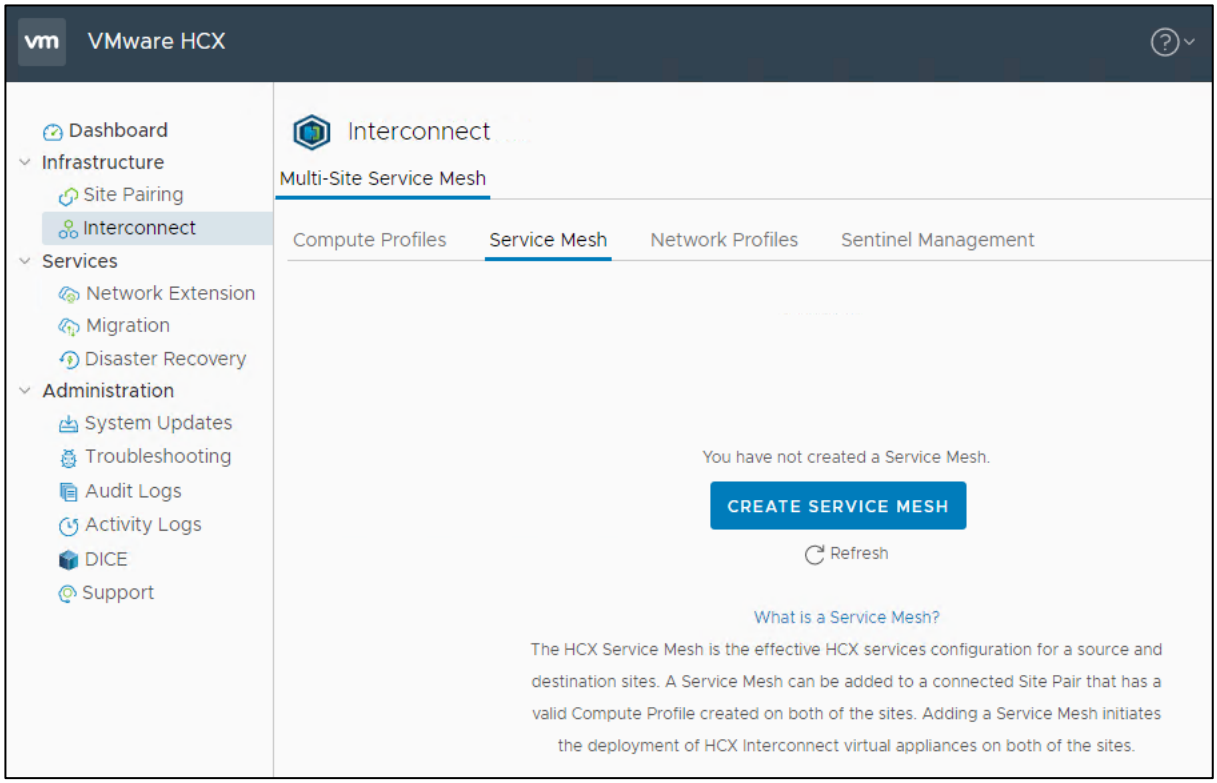
6. 「Service Mesh」タブを開き、「DELETE」 をクリックします。

「Delete Service Mesh」 画面が表示されます。



7. 「DELETE」 ボタンをクリックします。

「Removing Service Mesh : Waiting for remote site state confirmation.」 とメッセージが表示されるので、処理が完了するまで待ちます。



> **補足** Service Meshの削除に伴い、VMware HCX関連の仮想マシン（***<Service Mesh名>***-NW-I1 および ***<Service Mesh名>***-IX-I1）が自動で削除されます。

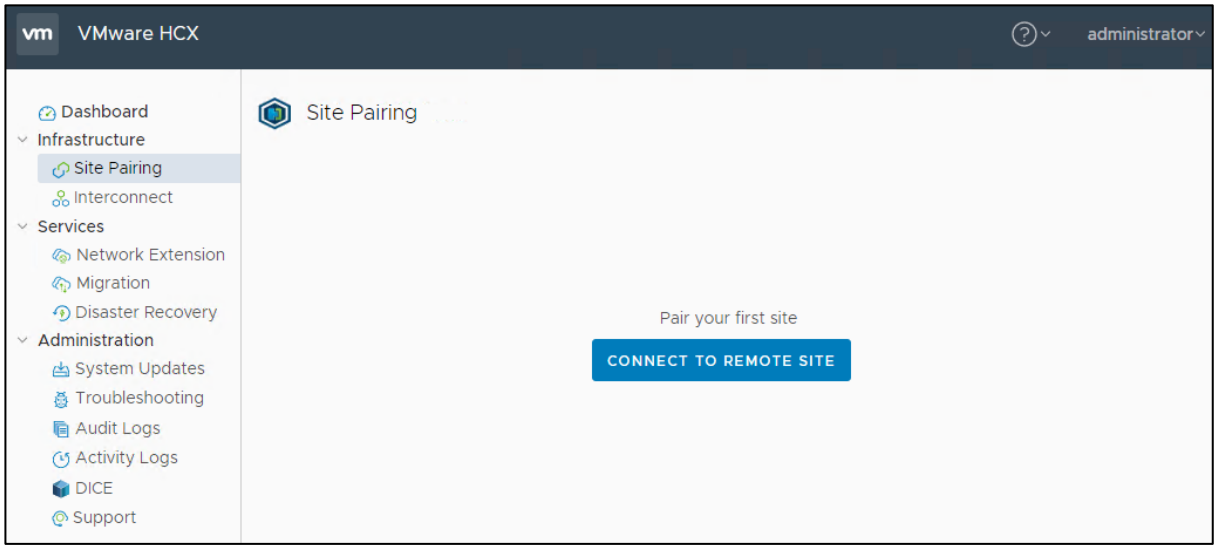
8. 左ペインより 「Infrastructure」 > 「Site Pairing」 を開きます。

9. 「DISCONNECT」 をクリックします。

「Disconnecting with remote site?」 画面が表示されます。

10. 「DISCONNECT] をクリックします。

下記画面へ遷移するまで待ちます。



11. VMware HCX の管理画面を閉じます。

12. Webブラウザより、お客さまオンプレミス環境の vCenter Server へログインします。

13. VMware HCX Connector をパワーオフします。

14. VMware HCX Connector を削除します。

☑重要	本項のオンプレミス環境のVMware HCXのアンインストール手順を完了後、引き続き当社作業によるプライベートクラウド環境での削除対応を実施する必要があります。 作業完了後は、当社サポート窓口または担当営業・SEへご連絡ください。

9. Advanced Cross vCenter vMotion による移行

2つのvSphere環境間でのVM移行機能をご提供いたします。

本項では、お客さまvSphere環境を移行元、当社プライベートクラウド環境を移行先として手順を記載いたします。

> 補足 **Advanced Cross vCenter vMotion機能のご提供について**
>
> 本機能はオプションのお申込みなしにご利用いただけます。システム要件等の詳細は
> 下記ヴイエムウェア社の公式ドキュメントをご参照ください。
>
> 参照 『Advanced Cross vCenter vMotion を使用した仮想マシンのインポートまたはクローン作成』
> 『vCenter Server インスタンス間の移行の要件』

9.1. オンプレミス環境のネットワーク情報登録

移行元となるお客さま環境のvCenterおよびESXiが、プライベートクラウド環境と通信(Tier-0ゲートウェイを経由)できるようにする必要があります。そのためNSX-Tにて当社作成済みグループに対し、お客さま環境のvCenterおよびESXiのIPアドレスを登録します。

ネットワーク情報の登録については下記手順をご参照ください。

参照 「6.14.3 Advanced Cross vCenter vMotion の移行元ネットワークの登録」

9.2. プライベートクラウド環境への移行

パワーオン状態の仮想マシンを、お客さまオンプレミス環境からプライベートクラウド環境へ移行します。切り替わりの際に仮想マシンのネットワークが切断されます。

1. **プライベートクラウドのvSphere Client へアクセスし、CustomerAdmins グループのアカウントにてログインします。**

2. **「ホストおよびクラスタ」より仮想マシンの移行先クラスタを右クリックし、「仮想マシンのインポート」を選択します。**

   「仮想マシンのインポート」ウィザードが開きます。

3. **「ソースvCenter Sertver を選択します」画面にて、お客さまオンプレミス環境のvCenter Server情報を入力し、「ログイン」をクリックします。**

   「*vCenter Server*アドレス に正常に接続されました」と表示されます。

4. **「NEXT」をクリックします。**

   仮想マシンの選択画面へ遷移します。

5. **移行対象の仮想マシンにチェックを入れ、「NEXT」をクリックします。**

   移行先リソースの選択画面へ遷移します。

6. **任意の移行先を選択し、「NEXT」をクリックします。**

   ストレージの選択画面へ遷移します。

7. **任意のデータストアを選択し、「NEXT」をクリックします。**

   フォルダ選択画面へ遷移します。

> ☑重要 **エコノミーストレージの利用における制限事項**
>
> エコノミーストレージをお申込み頂いているお客さまにつきましては、下記注意事項をご確認ください。
>
> ・ ゲスト OS のシステム領域としての利用は禁止操作となります
> ・エコノミーストレージに大量データの読込/書込を行った場合、スループット制御によりIO性能の制限が行われます

8. 任意のフォルダを選択し、「NEXT」をクリックします。

ネットワークの選択画面へ遷移します。

9. 「ターゲットネットワーク」を選択し、「NEXT」をクリックします。

設定の確認画面へ遷移します。

10. 設定内容に誤りが無いことを確認し、「FINISH」をクリックします。

Advanced Cross vCenter vMotionが開始されます。

10. コンテナ機能 （vSphere with Tanzu）

本オプションをご利用いただくことで、vSphereクラスタのKubernetes機能 (vSphere with Tanzu)をご提供いたします。この機能により、Kubernetes ワークロードをESXiホストで直接実行し、Kubernetes専用のリソースプール内にコンテナを作成・稼働することが可能になります。

> 重要 **コンテナ機能の提供形態について**
>
> 本オプションはライセンスのみのご提供となります。
>
> 製品仕様や操作方法に関するお問い合わせはお受けできません。

本サービスのコンテナ機能では、以下の機能をご利用いただけます。

項目	機能概要
名前空間	名前空間は、コンテナ展開用のリソースプールです。名前空間を利用することで、本サービス上にコンテナを展開することが可能です。
vSphere Pod (コンテナ)	作成した名前空間上に vSphere Pod を展開し、コンテナを実行させることが可能です。vSphere Pod は、Kubernetes アプリケーションの基本的な実行単位であり、vSphere Pod 単位でコンテナを実行します。
ロードバランサ	本サービスのコンテナ機能は NSX-T と連携し、vSphere Pod で利用可能なロードバランサ機能をご提供いたします。
コンテナレジストリ	本サービス上で動作するプライベートコンテナレジストリ（Harbor）をご提供いたします。Harbor をご利用いただくことで、コンテナイメージの格納・管理が可能です
永続ボリューム	コンテナで使用する永続ボリュームを作成・利用することが可能です。 作成した永続ボリュームは、専用ストレージのデータストア内に格納されます。

ここでは、各機能の代表的な利用方法をご説明いたします。

本ガイドの解説に含まれない機能については、ヴイエムウェア社の公式ドキュメントをご参照ください。

参照 『 vSphere with Tanzu の設定と管理』

> 重要 本サービスでご提供いたしますコンテナ機能は「vSphere Pod」のみとなります。
>
> 「Tanzu Kubernetes Cluster」はご提供いたしませんのでご注意ください。

10.1. 名前空間の構成と管理

コンテナを展開するための名前空間の作成・管理方法をご説明いたします。

10.1.1. 名前空間の作成

新規名前空間の作成手順をご説明いたします。

1. **vSphere Client のメニューより、「ワークロード管理」をクリックします。**

   「ワークロード管理」画面が表示されます。

2. **「名前空間」タブの画面にて、「新規名前空間」をクリックします。**

   「名前空間の作成」画面が表示されます。

3. **クラスタ欄のツリーから、名前空間を作成するクラスタを選択し、「名前」欄に作成する名前空間の名前と、必要に応じて「説明」欄を入力し、「作成」ボタンをクリックします。**

新規名前空間が作成され、作成完了画面が表示されます。

4. 「確認」ボタンをクリックします。

作成完了画面が閉じられ、作成した名前空間の「サマリ」画面が表示されます。

10.1.2. 名前空間の構成

作成した名前空間の設定を行い、ワークロードデプロイの準備を行います。

ここでは、各種設定の手順をご説明いたします。

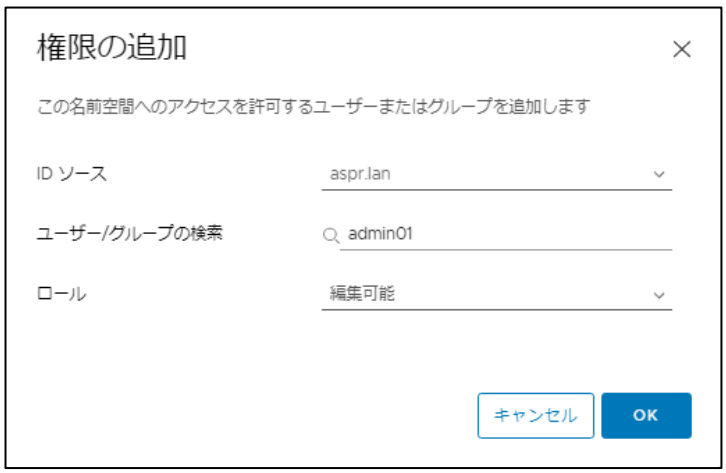
ユーザ権限の設定

名前空間にアクセスできるユーザとその権限を設定します。

1. 名前空間の「サマリ」画面のメニューより、「権限」欄の「権限の追加」ボタンをクリックします。

「権限の追加」画面が表示されます。

2. 権限を付与するユーザとロールを指定し、「OK」ボタンをクリックします。



項目	機能概要
ID ソース	権限を付与するユーザ、またはグループが登録されている ID ソースを指定します。 本サービスでは「aspr.lan」を指定してください。
ユーザー/グループの検索	ユーザ、またはグループを指定します。 文字列を入力し、虫メガネボタンをクリックすることで ID ソースから検索することが可能です。
ロール	割り当てる権限ロールを指定します。 使用可能な権限ロールは以下 2 つのどちらかです。 ・ 表示可能：名前空間内の情報の表示のみを行うことが可能な権限 ・ 編集可能：名前空間内の全ての操作を行うことが可能な権限 コンテナを作成するユーザを設定する場合は、「編集可能」権限をご利用ください。

指定したユーザに、名前空間の権限が付与されます。

「サマリ」画面の「権限」欄に権限を持つユーザが表示されます。

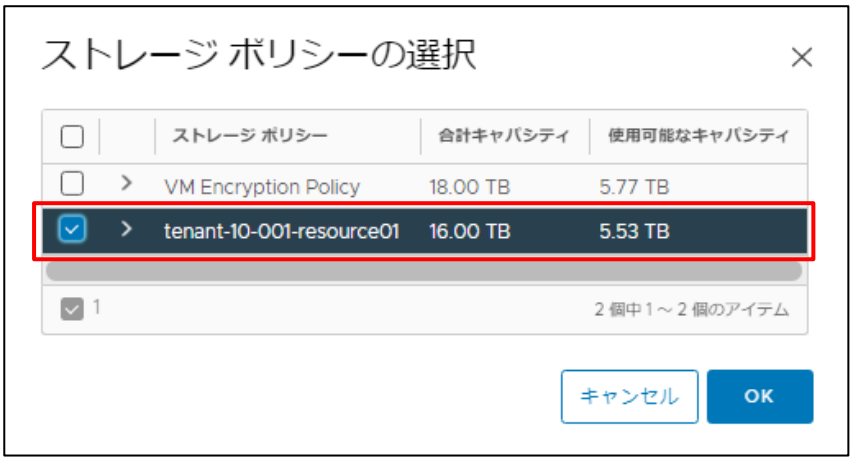
ストレージポリシーの設定

永続ボリュームを作成した際に、データを格納するデータストアをストレージポリシーで指定します。

1. **名前空間の「サマリ」画面のメニューより、「ストレージ」欄の「ストレージの追加」ボタンをクリックします。**

「ストレージポリシーの選択」画面が表示されます。

2. **ストレージポリシーリストから「tenant-XX-YYY-resourceZZ」を選択し、「OK」ボタンをクリックします。**

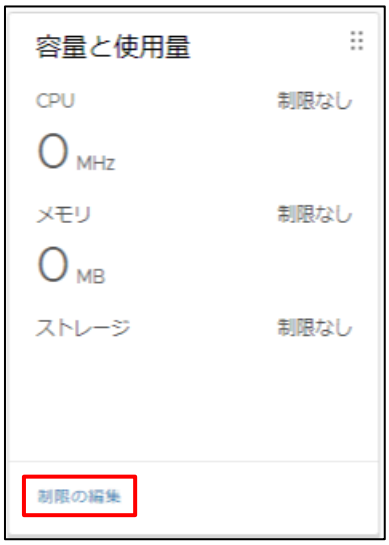


「サマリ」画面の「ストレージ」欄にストレージポリシー設定が表示されます。

リソース制限の設定

名前空間で使用するリソース容量の上限に制限をかけることが可能です。

1. 名前空間の「サマリ」画面のメニューより、「容量と使用量」欄の「制限の編集」ボタンをクリックします。



「容量の制限」画面が表示されます。

2. CPU・メモリ・ストレージの各欄に、使用量の上限とする数値と単位を入力し、「OK」ボタンをクリックします。

「サマリ」画面の「容量と使用量」欄に指定した上限値が表示されます。

補足 **より詳細なリソースの制限について**

名前空間の「設定」タブのメニューから選択できる「リソースの制限」「オブジェクトの制限」では、ここで設定したリソースの制限だけでなく、コンテナの制限や名前空間内のオブジェクトの制限を設定することが可能です。

設定可能な項目とその説明は、ヴイエムウェア社の公式ドキュメントをご参照ください。

参照 『vSphere 名前空間 での Kubernetes オブジェクトの制限の構成』

Kubernetesイベントの参照

名前空間で発生したイベント履歴の参照手順をご説明いたします。

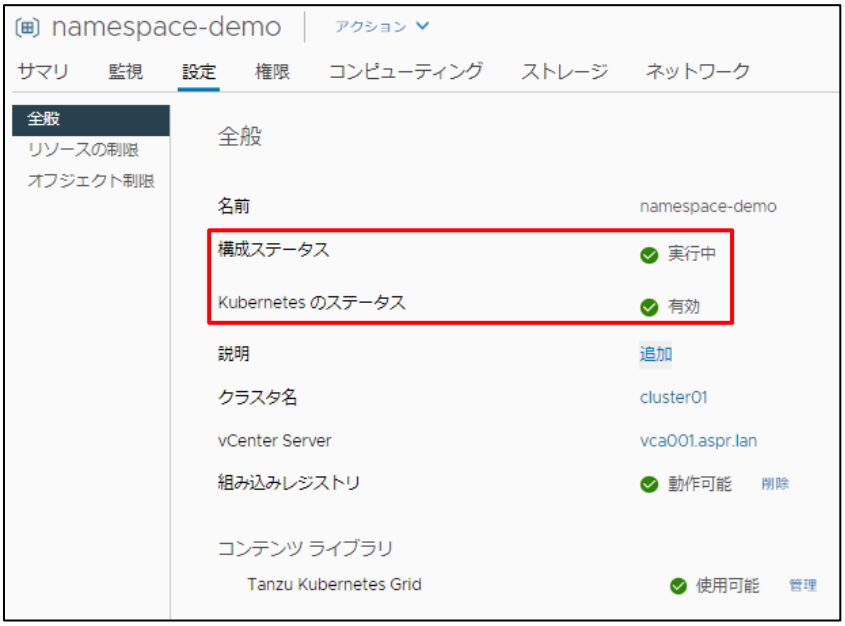
1. 名前空間の「監視」タブのメニューより、「イベント」>「Kubernetes」をクリックします。

「Kubernetesイベント」画面が表示されます。

名前空間のステータスの確認

名前空間、およびKubernetesの稼働ステータス確認の手順をご説明いたします。

1. 名前空間の「設定」タブのメニューより、「全般」をクリックします。



「全般」画面が表示されます。

「構成ステータス」の表記が「実行中」、

「Kubernetesのステータス」の表記が「有効」であることを確認します。

10.2.クライアント端末の準備

コンテナ機能を利用するためには、KubernetesのCLIツールをインストール済みのクライアント端末が必要です。

ここでは、クライアント端末の準備手順をご説明いたします。

10.2.1. クライアント端末の準備

事前準備として、クライアント端末として使用するサーバまたはPCをご用意ください。

クライアント端末の要件は下記の通りです。

項目	機能概要
OS 種別	Windows OS / Linux / Mac OS
通信要件	Kubernetes API エンドポイント への通信 ※Kubernetes API エンドポイントの IP アドレスは『開通通知書』をご参照ください。

10.2.2. CLIツールの導入

クライアント端末へのCLIツールインストール手順をご説明いたします。
ここでは、クライアント端末に Linux を使用した場合の手順をご説明いたします。

CLIツールインストーラのダウンロード

作成済みの名前空間から、CLIツールのインストーラファイルをダウンロードします。

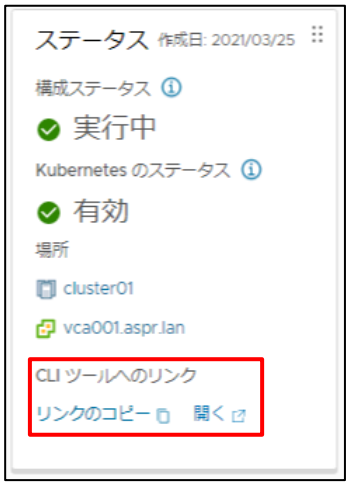
1. **vSphere Client の「三」ボタンより、「ワークロード管理」をクリックします。**

   「ワークロード管理」画面が表示されます。

2. **「名前空間」タブの画面にて、作成済みのいずれかの「名前空間」をクリックします。**

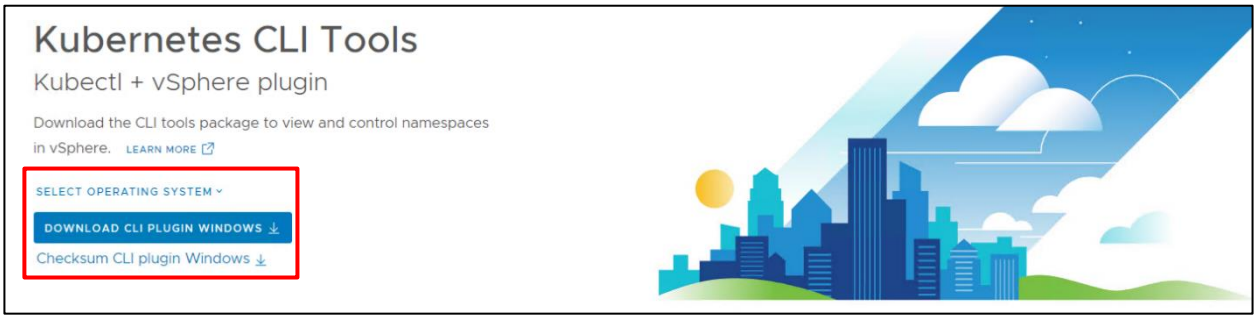
   選択した名前空間の「サマリ」画面が表示されます。

3. 名前空間の「サマリ」画面のメニューより、「ステータス」欄の「CLIツールへのリンク」から「開く」ボタンをクリックします。



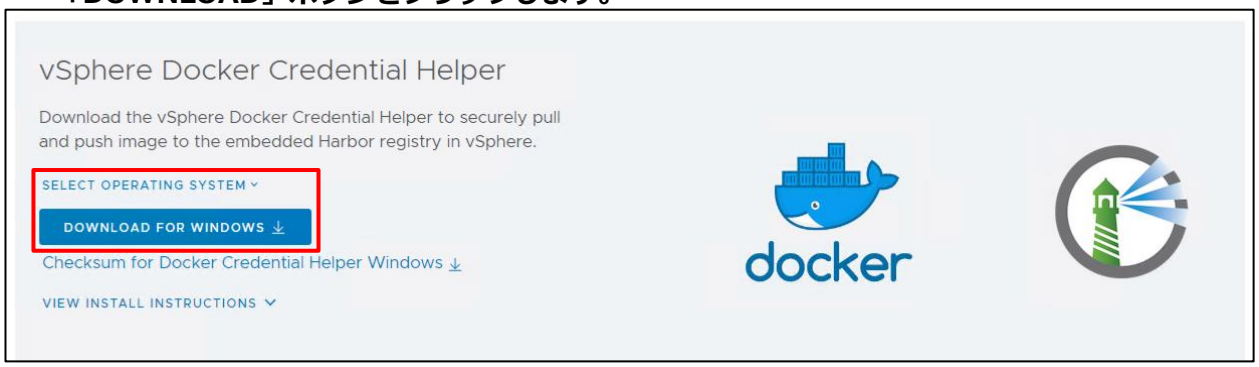
Webブラウザの新規ウィンドウにて、「VMware - Download Kubernetes CLI Tools」のページが開かれます。

4. 「SELECT OPERATIONG SYSTEM」をクリックして利用するOS種別を選択し、「DOWNLOAD CLI PLUGIN」ボタンをクリックします。



「vsphere-plugin.zip」がダウンロードされます。

5. 画面下部の「vSphere Docker Credential Helper」についても同様にOS種別を選択し、「DOWNLOAD」ボタンをクリックします。



「vsphere-docker-credential-helper.zip」がダウンロードされます。

補足 **コマンドによるインストーラの直接ダウンロードについて**

2つのインストーラファイルは、linux の wget コマンドや curl コマンドを用いて直接ダウンロードすることも可能です。

・ vsphere-plugin.zip

```
# wget --no-check-certificate https://<Kubenetes APIエンドポイントIPアドレス>/wcp/plugin/linux-amd64/vsphere-plugin.zip
```

・ vsphere-docker-credential-helper.zip

```
# wget --no-check-certificate https://<Kubenetes APIエンドポイントIPアドレス>/wcp/helper/linux-amd64/vsphere-docker-credential-helper.zip
```

CLIツールのインストール

前項でダウンロードしたインストーラファイルを使用し、クライアント端末にCLIツールをインストールします。

1. **クライアント端末のOSに、「vsphere-plugin.zip」および「vsphere-docker-credential-helper.zip」をアップロードします。**

2. **クライアント端末のOSの任意のディレクトリで、「vsphere-plugin.zip」および「vsphere-docker-credential-helper.zip」を展開します。**

```
# unzip vsphere-plugin.zip
Archive:  vsphere-plugin.zip
   creating: bin/
  inflating: bin/kubectl-vsphere
  inflating: bin/kubectl

# unzip vsphere-docker-credential-helper.zip
Archive:  vsphere-docker-credential-helper.zip
  inflating: bin/docker-credential-vsphere
```

ファイルを展開すると、「bin」ディレクトリ配下に「kubectl」と、スーパーバイザクラスタに接続するためのkubectlプラグイン「kubectl-vsphere」が格納されます。

ここでは実行例として、/root で実行しました。そのため、 /root/bin 配下に各ファイルが展開されています。

3. 「kubectl」の実行準備としてPATHを追加します。

```
# export PATH=$(pwd)/bin:$PATH
# which kubectl
/root/kubectl/bin/kubectl
```

which コマンドの実行結果により、kubectl のPATHが通っていることが確認できました。

Kubernetes APIエンドポイントへのログイン

CLIツールを使用し、Kubernetes APIエンドポイントへのログインテストを行います。

ここでは、Kubernetes APIエンドポイントのIPアドレスが「192.168.200.1」の場合の実行例を記載しています。

ログインに使用するユーザは、名前空間の権限を付与したユーザを使用します。

参照 「10.1.2 名前空間の構成」

1. 以下のコマンドを実行し、kubernetes APIエンドポイントへログインします。

```
# kubectl vsphere login –insecure-skip-tls-verify –server=192.168.200.1

Username: admin01@aspr.lan
Password:
Logged in successfully

You have access to the following contexts:
   192.168.200.1
   namespace-demo01
   namespace-demo02

If the context you wish to use is not in this list, you may need to try
logging in again later, or contact your cluster administrator.

To change context, use `kubectl config use-context <workload name>`
```

ログインが成功し、アクセス可能な名前空間のコンテキストリストが表示されます。

> 補足 **証明書のインストール**
>
> Tanzu Kubernetes クラスタに安全にログインするには、vCenter Server および kubectl 向けの vSphere プラグイン の最新バージョンのルート CA 証明書をダウンロードしてインストールします。
>
> CA証明書のインストール方法は、ヴイエムウェア社の公式ドキュメントをご参照ください。
>
> 参照 『 安全な CLI アクセスのための TLS 証明書のダウンロードとインストール』

CLIツールの使い方

CLIツールの仕様は Kubernetes 標準の kubectl に準じます。

kubectl の詳しい使い方については、Kubernetes の公式ドキュメントをご参照ください。

参照 『Kubernetesドキュメント CLIリファレンス』

10.3. Harborレジストリへのイメージアップロード

プライベートコンテナレジストリであるHarborへコンテナイメージ（Docker イメージ）のアップロードを行う手順をご説明いたします。

ここでは、HarborのIPアドレスを「192.168.200.2」、使用する名前空間名を「namespace-demo」とした場合の実行例を記載します。

ログインに使用するユーザは、ログインに使用するユーザは、名前空間の権限を付与したユーザを使用します。

参照 「10.1.2 名前空間の構成」

また、アップロードするイメージファイルは、Docker Hub からダウンロードした centos7 dockerイメージを使用します。

1. **以下のコマンドを実行し、Harborにログインします。**

```
# docker-credential-vsphere login 192.168.200.2
Username: admin01@aspr.lan
Password:
INFO[0010] Fetched username and password
INFO[0010] Fetched auth token
INFO[0010] Saved auth token
```

補足 **Harborレジストリ証明書のインストール**

クライアント端末から Harbor レジストリを使用するためには、Harbor レジストリルートCA証明書をインストールする必要があります。

Harbor レジストリルートCA証明書のインストール方法は、ヴイエムウェア社の公式ドキュメントをご参照ください。

参照 『 組み込みの Harbor レジストリ 証明書のダウンロードとインストール』

2. 以下のコマンドを実行し、Docker Hub から Docker イメージをダウンロードします。

```
# docker pull centos:centos7
centos7: Pulling from library/centos
Digest:
sha256:0f4ec88e21daf75124b8a9e5ca03c37a5e937e0e108a255d890492430789b60e
Status: Image is up to date for centos:centos7
docker.io/library/centos:centos7
```

3. 以下のコマンドを実行し、Harbor へ Docker イメージをアップロードします。

```
# docker tag centos:centos7 192.168.200.2/namespace-demo/centos:centos7
# docker push 192.168.200.2/namespace-demo/centos:centos7
The push refers to repository [192.168.200.2/namespace-demo/centos]
174f56854903: Pushed
centos7: digest:
sha256:e4ca2ed0202e76be184e75fb26d14bf974193579039d5573fb2348664deef76e size: 529
```

4. 以下のコマンドを実行し、Docker イメージの登録状態を確認します。

```
# docker images
REPOSITORY                                  TAG       IMAGE ID       CREATED        SIZE
192.168.200.2/namespace-demo/centos   centos7   8652b9f0cb4c   4 months ago   204MB
centos                                      centos7   8652b9f0cb4c   4 months ago   204MB
```

ローカルと Harbor レジストリに格納されている Dockerイメージが表示されます。

10.4. ワークロードのデプロイ

Harborレジストリのイメージを使用して、ワークロードをデプロイする手順をご説明いたします。

1. デプロイするワークロードの内容を定義するマニフェストファイルをYAML書式で作成します。

下記はYAMLファイルのサンプルです。

```
# vi demo.yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: demo-deployment
spec:
  selector:
    matchLabels:
      app: demo
  replicas: 3
  template:
    metadata:
      labels:
        app: demo-app
    spec:
      containers:
        - name: cent-demo
          image: 192.168.200.2/namespace-demo/centos:centos7
          ports:
            - containerPort: 80
```

マニフェストとYAML書式の仕様は Kubernetes 標準に準拠します。

YAML書式の詳しい説明については、Kubernetes の公式ドキュメントをご参照ください。

参照 『Kubernetesオブジェクトを理解する』

2. 以下のコマンドを実行し、YAMLファイルからコンテナをデプロイします。

```
# kubectl apply -f demo.yaml
```

YAMLファイルの定義に従い、コンテナのデプロイタスクが実行されます。

3. 以下のコマンドを実行し、デプロイしたコンテナの稼働状態を確認します。

```
# kubectl get pods -o wide
# kubectl describe -f demo.yaml
```

11. エコノミーストレージ

専用ストレージとは別の共有ストレージを利用した大容量ボリュームをご提供するオプションです。

11.1.エコノミーストレージについて

本オプションは共有ストレージを複数のお客さまでご利用いただくシェアリング型のサービスとなります。
ストレージ領域は論理的に分割されていますので、割り当てられた領域は専用としてご利用いただけます。

> **重要** **エコノミーストレージの利用における制限事項**
>
> ・ゲストOSのシステム領域としての利用は禁止操作となります
>
> ・エコノミーストレージに大量データの読込/書込を行った場合、スループット制御によりIO性能の制限が行われます

本オプションをご契約いただくことで、エコノミーストレージのストレージボリュームをVMware vCenter Server 上のデータストアとしてご提供いたします。

> **補足** **データストア名**
>
> エコノミーストレージは命名規則に従い「tenant-***XX***-***YYY***-economy***ZZ***」のデータストア名でご提供いたします。具体的なデータストア名は『開通通知書』の記載をご確認ください。

11.2.エコノミーストレージの利用方法

エコノミーストレージのデータストアは、仮想マシンにディスクを追加する際のデータストアとしてご利用ください。

仮想マシンにエコノミーストレージのディスクを追加する手順

1. **vSphere Client の「三」ボタンより、「インベントリ」をクリックします。**

   「インベントリ」画面へ遷移します。

2. **左ペインのツリーより、ハードディスクの追加を行う仮想マシンを右クリックし、メニューから「設定の編集」をクリックします。**

   「設定の編集」画面が表示されます。

3. **「仮想ハードウェア」タブにて、「新規デバイスを追加」ボタンから、「ハードディスク」をクリックします。**

   ハードウェアリストに「新規ハードディスク」が追加されます。

4. **「新規ハードディスク」の「＞」をクリックして展開し、ハードディスクのサイズを入力します。**

5. **「場所」欄のドロップダウンボックスから「参照」ボタンをクリックします。**

   「データストアクラスタまたはデータストアの選択」画面が表示されます。

6. **データストアのリストから、エコノミーストレージデータストアを選択し、「OK」ボタンをクリックします。**

7. **設定内容に誤りがないことを確認し、「OK」ボタンをクリックします。**

   「仮想マシンの再設定」タスクが実行されます。タスクステータスが「完了」になることを確認します。

8. **対象仮想マシンの「サマリ」画面にて「仮想マシンのハードウェア」ウィンドウの「ハードディスク」欄を展開し、「場所」に表示されたデータストア名がエコノミーストレージデータストアであることを確認します。**

11.3.エコノミーストレージの管理

エコノミーストレージの容量管理には、専用ストレージと同様、vRealize Operations Manager のダッシュボードを参照することが可能です。

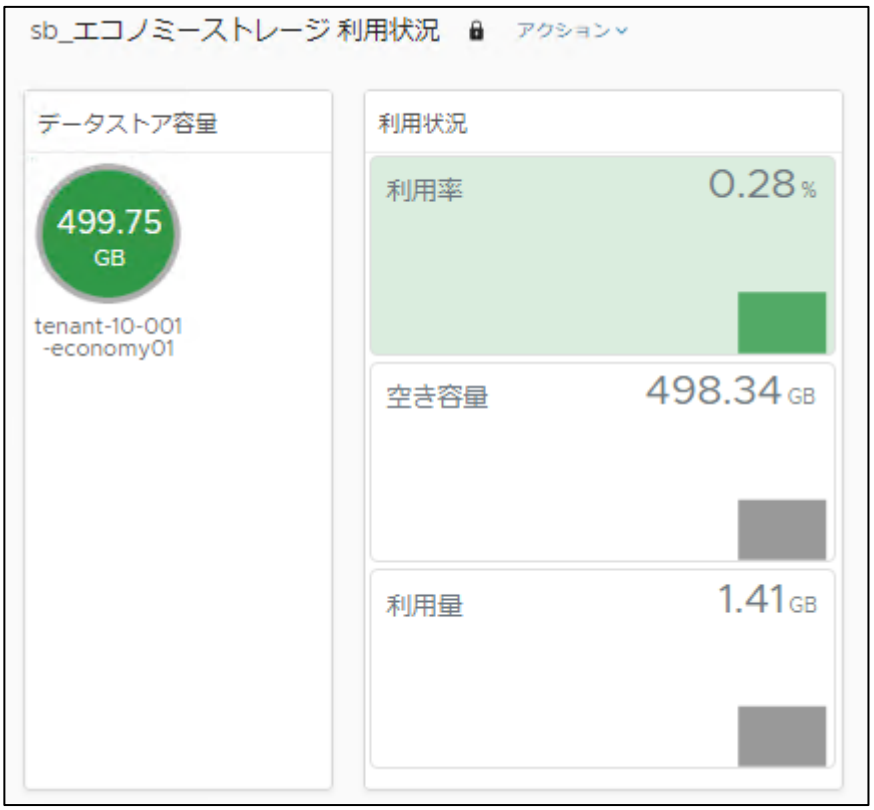
専用ストレージの容量管理とは異なり、データストアとしての使用量/残り容量をそのまま使用状況としてご確認ください。

1. **vRealize Operations Manager の「可視化」より「ダッシュボード」をクリックします。**

   直近で開いていたダッシュボードが表示されます。直近で開いていたダッシュボードが無い場合は「ホーム」の画面が表示されます。

2. **「管理」より一覧から、「sb_エコノミーストレージ 利用状況」をクリックします。**

   「sb_エコノミーストレージ 利用状況」ダッシュボードが表示されます。



ウィジェット	表示内容
データストア容量	エコノミーストレージとしてご利用いただける全体容量
利用状況	下記 3 点の使用状況表示と、直近 30 日の推移のグラフ ・ 利用率：現在のデータストア使用量がデータストア容量に占める割合 ・ 空き容量：未使用のストレージ容量（=データストア容量 - 現在の使用量） ・ 利用量：現在のデータストア使用量

12. 多機能ロードバランサ(Netwiser VE)

多機能ロードバランサ（Netwiser Virtual Edition）は、多機能ロードバランサオプションをご契約の場合に利用できるサービスです。ヴイエムウェア株式会社が提供する NSX ロードバランサ機能とは別に、セイコーソリューションズ株式会社が提供する「Netwiser Virtual Edition」をご利用いただけます。

詳しくは、法人テクニカルサポートWebに掲載されている『ホワイトクラウド_ASPIRE_専用型ロードバランサ_サービスご利用ガイド』をご参照ください。

> **重要** **多機能ロードバランサを冗長構成でお申込の場合の設定について**
>
> 多機能ロードバランサを冗長構成で利用する場合は、下記の追加設定が必要になります。
>
> 参照 「6.17 多機能ロードバランサを冗長構成で利用する場合の準備(オプション)」

13. Cloud One Workload Security

Cloud One Workload Securityは、トレンドマイクロ社が提供する総合サーバセキュリティサービスです。
オプションのCloud One Workload Securityをご契約の場合にご利用いただけます。

Cloud One Workload Security の利用手順は、
『ホワイトクラウド ASPIRE サービスご利用ガイド』の紹介ページをご参照ください。

参照 『ホワイトクラウド ASPIRE サービスご利用ガイド』Cloud One Workload Security

14. アンチウイルスオプション

本サービスでご提供いたしますアンチウイルスオプション製品は、ソフォス株式会社が提供するサーバセキュリティサービスです。
このサービスは、アンチウイルスオプションをご契約の場合にご利用いただけます。

アンチウイルスオプション の利用手順は、
『ホワイトクラウド ASPIRE サービスご利用ガイド』の紹介ページをご参照ください。

参照 『ホワイトクラウド ASPIRE サービスご利用ガイド』アンチウイルス（オプション）

15. Acronis Cyber Backup powered by ASPIRE

Acronis Cyber Protect Cloud は、アクロニス社が提供するデータ保護ソリューションです。

このサービスは、オプションの Acronis Cyber Backup powered by ASPIRE をご契約の場合にご利用いただけます。

Acronis Cyber Backup powered by ASPIRE の利用手順は、

『ホワイトクラウド ASPIRE サービスご利用ガイド』の紹介ページをご参照ください。

参照 『ホワイトクラウド ASPIRE サービスご利用ガイド』Acronis Cyber Backup powered by ASPIRE

補足

参照先手順の読み替えについて

上記参照先手順の一部手順は、『ホワイトクラウド ASPIRE』で提供されるポータルサイトの操作を参照します。

該当する箇所の手順は本サービスにおいては「VMware vCenter Server の操作」になるため、以下のように読み替えを行います。

・ 「リストアを実施する」 > 「リストア先の新規仮想マシンを作成し、ブータブルメディアを挿入する」

OS が入っていない空の仮想マシンを作成する手順は、下記項目を参照してください。

参照 「5.3.1 仮想マシンの作成」

カタログからブータブルメディア ISO イメージを挿入する手順は、下記項目をご参照ください。

参照 「5.4.9 仮想マシンへの ISO イメージのマウント」

16. モニタリングオプション(Mackerel)

はてな社が提供するSaaS型のサービス、Mackerel (マカレル)を使用して仮想マシン監視およびURL監視(外形監視)を提供するモニタリングサービスです。
このサービスは、モニタリング（Mackerel）をご契約の場合にご利用いただけます。

モニタリングオプション（Mackerel） の利用手順は、
『ホワイトクラウド ASPIRE サービスご利用ガイド』の紹介ページをご参照ください。

参照 『ホワイトクラウド ASPIRE サービスご利用ガイド』モニタリング（Mackerel）

17. Red Hat Cloud Access

Red Hat Cloud Accessは、お客さま保有のRed Hatライセンス（RHELサブスクリプション）を、Red Hat社の認定プロバイダー（当社）のクラウド環境へのライセンス持込みが許容されるライセンス制度です。

Red Hat Cloud Access の利用手順は、
『ホワイトクラウド ASPIRE サービスご利用ガイド』の紹介ページをご参照ください。

参照 『ホワイトクラウド ASPIRE サービスご利用ガイド』Red Hat Cloud Access

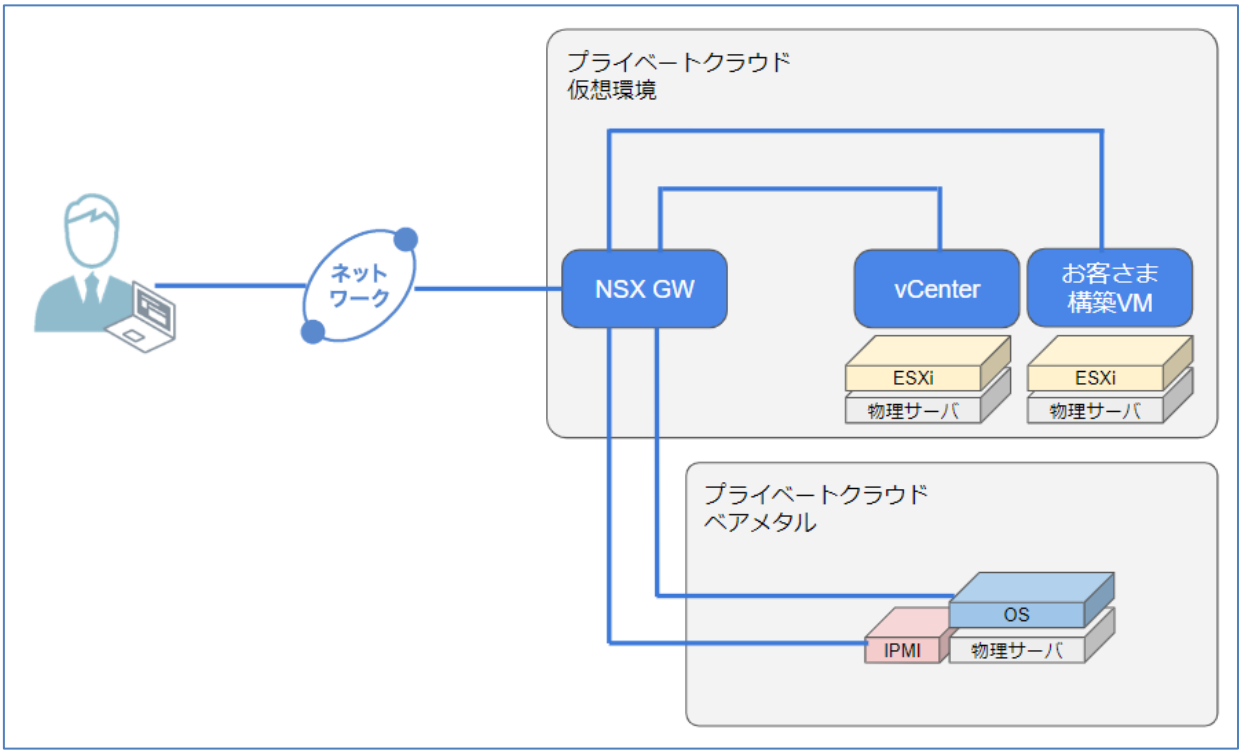
18. ベアメタルサーバの提供機能

当社データセンター内に物理サーバを仮想基盤用ソフトウェアのインストールをせずにご提供いたします。ライセンスの都合上クラウド環境での利用が困難であったソフトウェアを、オンプレミス環境と同様にご利用いただくことが可能です。

18.1. ベアメタルサーバの構成

ベアメタルサーバはプライベートクラウドの仮想基盤のサーバとは別に物理サーバを用意し、プライベートクラウド環境のNSX-T ゲートウェイを介して通信を行います。

サービス概要図



18.2. ベアメタルサーバ管理ツール

ベアメタルサーバでは下記の管理ツールをご提供いたします。

管理ツールの操作方法は後述の操作方法解説ページをご参照ください。

管理ツール	機能概要
Lenovo XClarity Controller(以降、文中は XCC と記載いたします)	ベアメタルサーバに搭載されているサーバ管理用のモジュールで、OS からは独立して動作します。 代表的なものとして下記の機能をご提供いたします。 • リモート コンソール • サーバ 電源操作 • サーバ Firmwareの管理

18.3. ベアメタルサーバで利用可能なASPIRE共通オプション

本サービスでは下記のソフトウェアをオプション機能としてご提供いたします。

各製品の操作方法は前述の操作方法解説ページをご参照ください。

機能	機能概要
Cloud One Workload Security	トレンドマイクロ社が提供するクラウド環境保護ソリューション「Trend Micro Cloud One」のうち、セキュリティ対策製品である「Workload Security」をご利用いただけるサービスです 。
アンチウイルス オプション	ソフォス社が提供する「Central Server Protection」により、ウイルス対策機能をご利用いただけるサービスです。
モニタリング（Mackerel）	はてな社が提供する Mackerel をご利用いただき、OS 監視および外形監視(URL 監視)を行う SaaS 型モニタリングサービスです。

18.4. ベアメタルサーバ管理ツールの通信要件

ベアメタルサーバの管理ツールをご利用いただくには、管理ツールへのアクセス経路が必要になります。

各製品の管理ツールへのアクセスは、NSX-Tにて「tenant_external」または「tenant_overlay」もしくは「tenant_baremetal_os」のグループに登録されているネットワークに制限をしています。

管理ツールを利用するために必要な通信要件は、以下の通りです。

お客さまの端末から管理ツールのIPアドレスへのプロトコル/ポート宛通信が可能となるようご準備ください。「宛先」と対応するIPアドレスについては、『開通通知書』をご参照ください。

管理ツール名称	宛先	プロトコル	ポート
Lenovo XClarity Controller (XCC)	『開通通知書』参照	TCP	443,3900

18.5. ベアメタルサーバ管理のためのソフトウェア要件

管理ツールを利用するためのソフトウェア要件を下記に記載いたします。

Lenovo XClarity Controller (XCC)

XCCを使用するには、サポート対象の Web ブラウザが必要です。
サポートされているブラウザは下記の通りです。

サポートされるブラウザのバージョン

- Chrome 48.0 以上(リモート・コンソールには 55.0 以上)
- Firefox ESR 38.6.0 以上
- Microsoft Edge
- Safari 9.0.2 以上(iOS 7 以上 および OS X)

> **補足**
> ・リモート・コンソール機能は、モバイルデバイスのOSのブラウザからはサポートされていません。
>
> ・サポート対象のブラウザはご利用中のXCCのバージョンによって異なる場合があります。
> ご利用中のXCCのバージョンでサポートされるブラウザはXCC ログイン画面の
> 「サポートされているブラウザー」から確認できます。

19. ベアメタルサーバ用初期設定

本章では、ベアメタルサーバ向けに当社にて実施している設定についてご説明いたします。

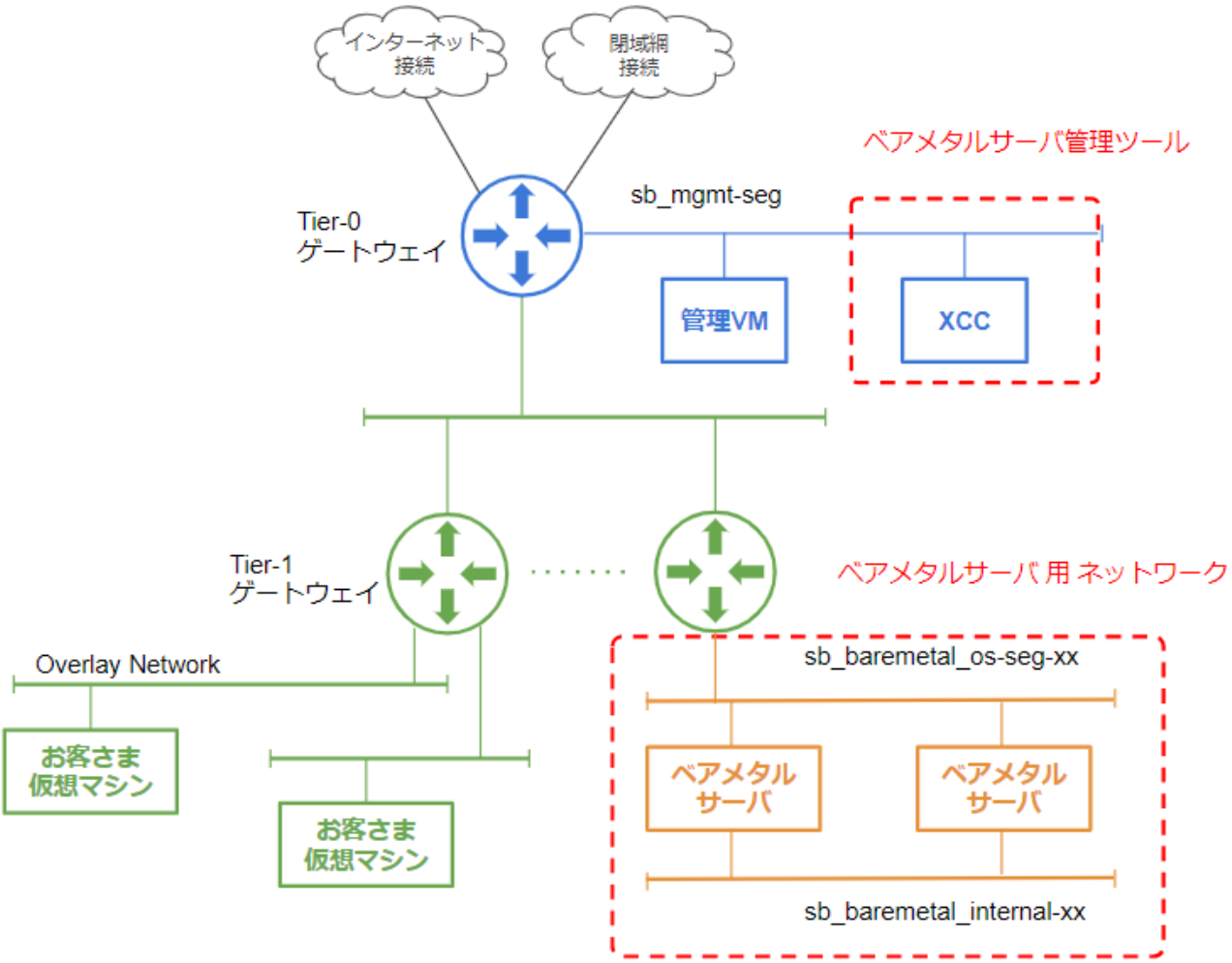
19.1. ベアメタルサーバ用 NSX-T設定

ベアメタルサーバをご契約後、当社にてNSX-Tにベアメタルサーバ向けの設定を実施いたします。

19.1.1. NSX-T の構成(ベアメタル)

プライベートクラウドの NSX-T とベアメタルサーバのネットワーク接続についてご説明いたします。

ベアメタルサーバは『ヒアリング シート』に記載頂いたTier-1 ゲートウェイ配下のVLAN ネットワークに接続されます。



ベアメタルサーバ開通時にNSX-Tに以下設定を追加いたします。各設定の詳細内容は、「19.1.2 Tier-1 ゲートウェイ」以降の各項目にて記載いたします。

内容	説明
Tier-1 ゲートウェイ	『ヒアリング シート』に記載頂いた Tier-1 ゲートウェイにベアメタルサーバ用 ネットワークのインターフェイスを作成します。 ベアメタルサーバは作成したインターフェイスから外部ネットワークとの通信を行います。 ベアメタルサーバ用 ネットワークのインターフェイスの削除や、対象の Tier-1 ゲートウェイの削除は禁止操作となります。
セグメント	ベアメタルサーバ用 ネットワークの VLAN セグメントを作成します。これらの設定の変更や削除は禁止操作となります。
グループ	ゲートウェイ ファイア ウォールで利用するベアメタルサーバ用のグループの定義を作成します。 作成されたグループにはベアメタルサーバが外部と通信する際に設定が必要な定義も含まれております。
ゲートウェイ ファイアウォール	ベアメタルサーバ開通時点ではベアメタルサーバおよび XCC への通信を制限するためのルールを Tier-0 ゲートウェイおよびアップリンク向けに設定しています。これらの設定の変更や削除は禁止操作となります。

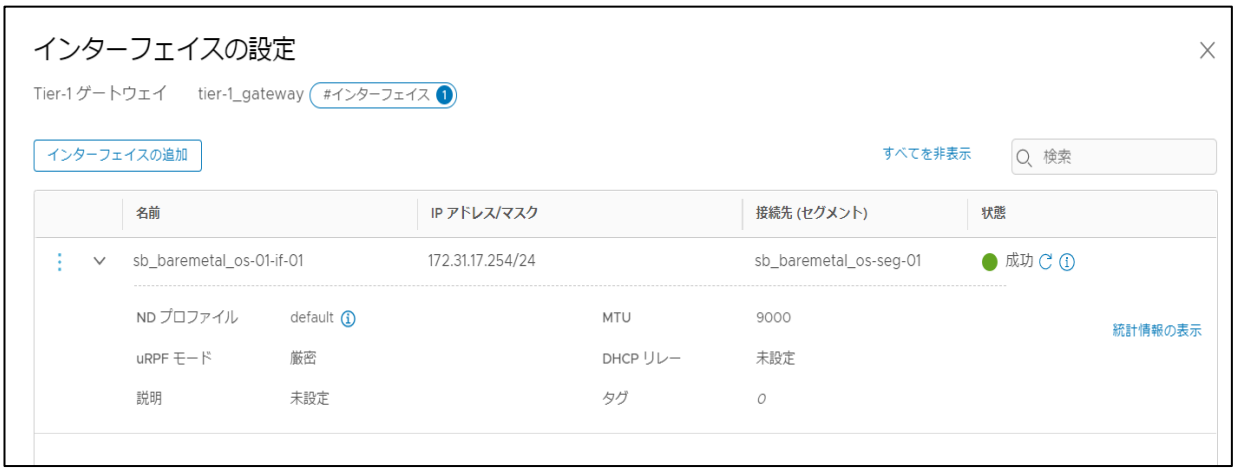
19.1.2. Tier-1 ゲートウェイ(ベアメタル)

Tier-1 ゲートウェイにベアメタルサーバ用 ネットワークのインターフェイスを作成します。

ベアメタルサーバは作成したインターフェイスから外部ネットワークとの通信を行います。

名前	説明
sb_baremetal_os-***XX***-if-***YY***	ベアメタルサーバ OS の外部通信用のインターフェイス※1

※1：接続しているネットワーク数により、複数存在する場合があります。



補足 Tier-1 ゲートウェイで「接続されているすべてのセグメントおよびサービス ポート」のルートアドバタイズを有効にしない場合、同一Tier-1ゲートウェイ配下のネットワーク以外との通信はできません。

重要 インターフェイスやインターフェイスを作成しているTier-1 ゲートウェイは削除しないようにご注意ください。削除されるとベアメタルサーバとの通信が出来なくなります。

19.1.3. セグメント(ベアメタル)

ベアメタルサーバが接続する VLAN セグメントを作成します。

名前	説明
sb_baremetal_os-seg-***XX***	ベアメタルサーバ上の OS 用セグメント※1

※1：接続しているネットワーク数により、複数存在する場合があります。

重要 当社管理セグメントの変更や削除は禁止操作となります。

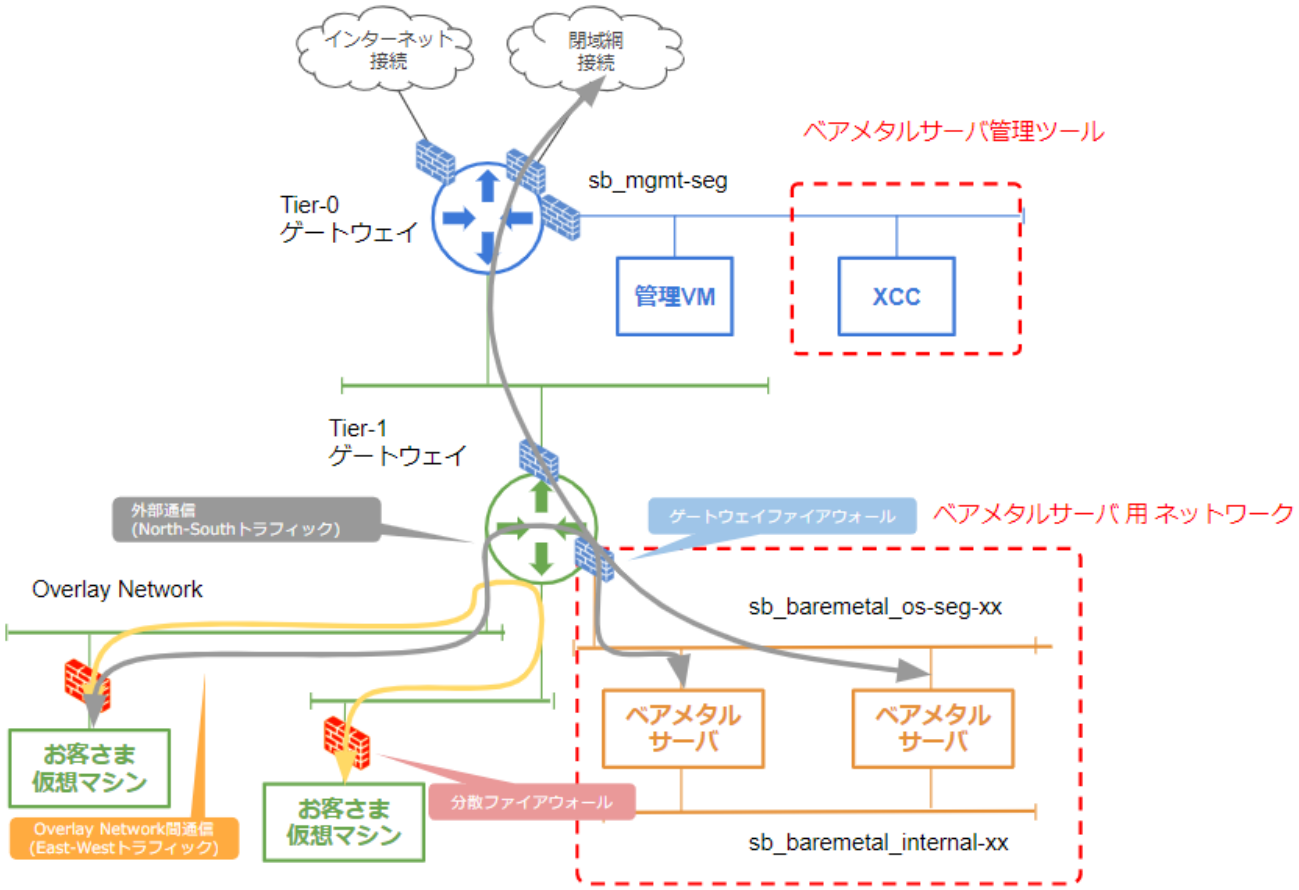
19.1.4. グループ(ベアメタル)

グループ定義はゲートウェイ ファイアウォールの設定で利用されます。

グループ名	お客さま操作 〇：許可 ×：禁止	説明
sb_baremetal_bmc	×	ベアメタルサーバ管理ツールが使用するグループ定義です。これらのグループに対する変更や削除は禁止操作となります。
tenant_baremetal_os	〇	ベアメタルサーバを外部ネットワークと通信させる際に利用します。 このグループに登録することで、外部ネットワークとの通信が双方向で許可されます。 また、同時に管理ツールとの通信がゲートウェイ ファイアウォールで許可されます。

19.1.5. ゲートウェイ ファイアウォール(ベアメタル)

外部ネットワークからベアメタル管理ツールやベアメタルサーバへのアクセスを制限するためのゲートウェイ ファイアウォールのポリシーを設定済みです。



> **補足**
>
> 同一Tier-1 ゲートウェイに接続されているOverlay Networkとベアメタルサーバ用ネットワークの通信では、Overlay Network同士と異なり接続しているTier-1 ゲートウェイのゲートウェイ ファイアウォールのルールが適用されます。
>
> 例として上記構成の場合Overlay Network間通信にはゲートウェイ ファイアウォールルールが適用されませんが、外部通信にはゲートウェイ ファイアウォールルールが適用されます。

19.2. Lenovo XClarity Controller (XCC)設定

ベアメタルサーバをご契約後、お客さまへの提供開始時のXCCの状態をご説明いたします。

19.2.1. Lenovo XClarity Controller (XCC)管理用設定

XCCには以下 当社管理用の設定を実施します。

XCC 設定箇所	設定内容
イベント - アラート受信者 - Syslog	当社管理用の syslog 設定 補足 お客さまにて新規のSyslog設定を追加頂くことは可能です
BMC 構成 - ユーザー/LDAP - LDAP	当社管理サーバとの LDAP 連携設定
BMC 構成 - ユーザ/LDAP - ローカル・ユーザー	当社管理用ユーザの作成 お客さまユーザの作成
BMC 構成 - ネットワーク - イーサネット構成	XCC のホスト名、ネットワーク関連の設定
BMC 構成 - ネットワーク - Ethnet Over USB	Ethnet Over USB の無効化
BMC 構成 - ネットワーク - SNMP セットアップ	当社管理用の SNMP 設定
BMC 構成 - ネットワーク - サービスの有効化とポートの割り当て	IPMI over LAN の無効化
時刻	NTP サーバの設定
ホーム - システム情報および設定	システム名の設定

重要 当社設定内容の変更や削除は禁止操作となります。

19.2.2. Lenovo XClarity Controller (XCC) その他の設定

XCCには管理用設定以外に以下の設定を実施します。

これらの設定はお客さまにて変更頂いて問題ございません。

XCC 設定箇所	設定内容
BMC 構成 - ユーザー/LDAP - 共通設定	パスワード有効期限の無効化 パスワード失効の警告期間の無効化

19.2.3. UEFI Setup設定

UEFI Setupより各HBAに対し以下SAN環境用の設定をします。

UEFI Setup 設定箇所	設定内容
UEFI Setup - System Settings - Storage	各 HBA に以下の設定 ・ Adapter Settings - Data Rate を 32Gb/s で指定 ・ Boot Settings - Adapter Driver を有効化

重要 当社設定内容の変更や削除は禁止操作となります。

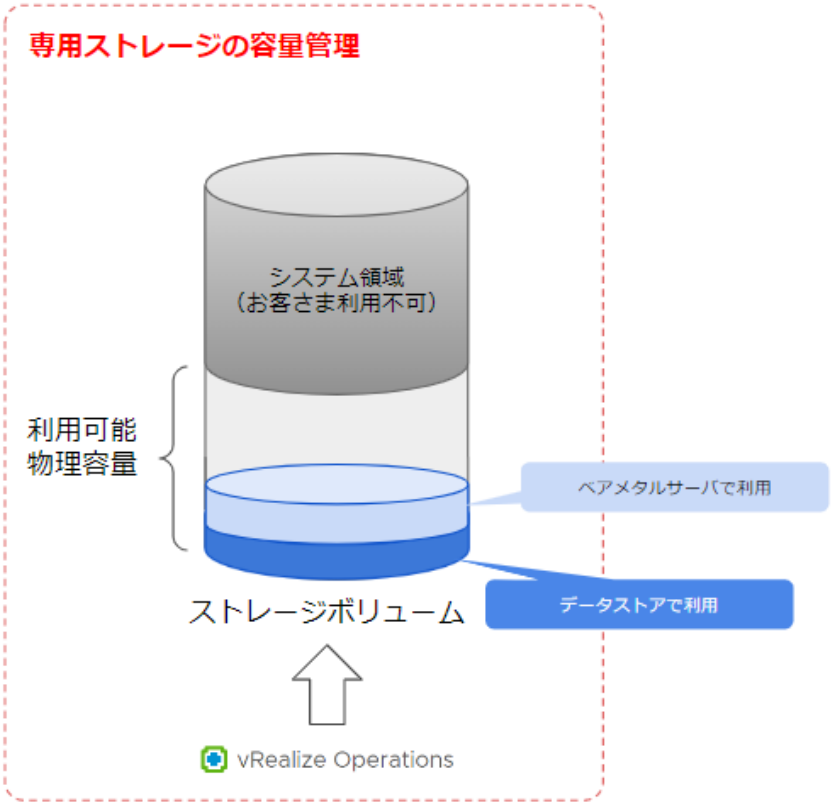
20. 専用ストレージの容量管理について(ベアメタル)

本章では、ベアメタルサーバの専用ストレージの容量管理についてご説明いたします。

> **重要** 本章は、専用ストレージの利用にあたっての重要事項となります。

ベアメタルサーバの容量管理の考え方

ベアメタルサーバで利用するボリュームは専用ストレージの領域から切り出し割り当てます。専用ストレージの容量はデータストアの利用領域と共用しますのでご留意ください。



データストアの容量管理と同様下記の特性・注意事項がありますのでご留意ください

- ベアメタルサーバ OS 上の Disk 使用量と実際の物理容量の使用量は異なります
- 実際の物理容量使用量は、重複排除・圧縮により軽量化されます
- 重複排除・圧縮率は、格納されたデータの内容により異なります
- 専用ストレージの容量管理は、OS 上ではなく vRealize Operations Manager をご利用ください

ベアメタルサーバ用ボリュームの専用ストレージ利用状況の確認方法

専用ストレージの利用状況は、ベアメタルサーバ用VolumeもvRealize Operations Manager のダッシュボード機能にて確認することが可能です。

ボリュームは『ヒアリング シート』に記載頂いたボリューム名で作成しています。

参照「7.6 カスタムダッシュボードによる専用ストレージの容量管理」

21. VMware NSX-T DataCenter の操作(ベアメタル)

本章ではベアメタルサーバ向けのNSX-Tの操作についてご説明いたします。

21.1. 当社作成済みグループの編集(ベアメタル)

ベアメタルサーバご契約時に作成しているグループの編集についてご説明いたします。

ベアメタルサーバご契約時に「tenant_baremetal_os」という名前のグループを当社にて作成しており、お客さまにてメンバーの設定をいただくことで可能です。

下記のような操作を行う場合は、本項の手順を参照し作成済みグループへのIPアドレスの追加を行う必要があります。

- ベアメタルサーバと外部ネットワーク、管理ツールをアクセス可能にする

「tenant_baremetal_os」へのIPアドレスの追加手順は下記をご参照ください。

参照 「6.14.1 外部ネットワークへアクセス可能な Overlay Network の追加」

当社にて作成済みのベアメタルサーバ用グループの一覧と用途について下記をご参照ください。

参照 「19.1.4 グループ(ベアメタル)」

22. Lenovo XClarity Controller(XCC)の操作

ベアメタルサーバサービスにてご提供するサーバについて、各種操作方法について記載いたします。本手順はXCC バージョン V7.80における操作例となりますので、バージョンが異なる際はメーカーマニュアルをご参照ください。

☑重要

本書に記載されていない操作について

本書に記載されていない操作については、当社によるサーバの運用管理に影響を与える可能性があるため、お客さま責任のもと実施してください。

メーカーマニュアルについて

本サービスではLenovo社のThinkSystem SR650を提供します。詳細はメーカサイトにてご確認ください。

ガイドとマニュアル

https://datacentersupport.lenovo.com/jp/ja/products/servers/thinksystem/sr650/7x06/document-userguide

Intel Xeon SP (第 1 世代、第 2 世代) を搭載した Lenovo XClarity Controller

https://sysmgt.lenovofiles.com/help/index.jsp?topic=%2Fcom.lenovo.systems.management.xcc.doc%2Fproduct_page.html&lang=ja

Firmware

https://datacentersupport.lenovo.com/jp/ja

22.1.ユーザの管理

お客さまユーザは、サーバのローカルユーザのみ作成可能です。オプション開通時には最も強い権限を持ったユーザを『開通通知書』にてご連絡します。お客さまにて適切なユーザ作成および権限設定が完了しましたら、本ユーザは削除いただいて問題ありません。

> **重要**
> 当社管理用ユーザが参照でき、一覧に表示されますがこちらのユーザの操作は実施しないでください。
> 当社の管理用ユーザ名は「sb_」で始まるものになります。

22.1.1. ユーザ管理画面の表示

1. **Webブラウザにてベアメタルサーバの管理GUI（以降、XCCと記載いたします）へアクセスします。URLは『開通通知書』をご確認ください。**
   XCCのログイン画面が表示されます。

2. **『開通通知書』に記載されたユーザ名、パスワードにてログインします。**
   XCCのホーム画面が表示されます。

3. **左ペインより「BMC構成」>「ユーザー/LDAP」を選択します。**

4. **右ペインより「ローカル・ユーザー」タブを選択します。**
   ローカルユーザの一覧が表示されます。

22.1.2. ユーザの作成

1. **『22.1.1 ユーザ管理画面の表示』に記載の手順を実施します。**

2. **右ペインの「ローカル・ユーザー」画面にて「+」アイコンをクリックします。**
   「ユーザ資格情報と権限」の設定画面が表示されます。

3. **「ユーザー名」、「パスワード」、「権限レベル」および必要に応じて各種オプションを設定し、「適用」をクリックします。**

   「新規ユーザーが正常に作成されました。これにともない初回ログイン時にパスワードを変更する必要があります。」と表示され、ユーザが追加されます。

4. **作成したユーザにてXCCにログインできることを確認します。**

22.1.3. ユーザの削除

1. **『22.1.1 ユーザ管理画面の表示』に記載の手順を実施します。**

2. **右ペインの「ローカル・ユーザー」画面にて、削除対象ユーザのごみ箱アイコンをクリックします。**

   「<ユーザ名>を削除してもよろしいですか？」と表示されます。

3. **「OK」をクリックします。**

   「ユーザーが正常に削除されました」と表示され、ユーザが削除されます。

22.2. ログの管理

ベアメタルサーバの各種ログはXCC、または後述のSyslogを設定し参照することができます。

22.2.1. Syslogの設定

1. **WebブラウザにてXCCへアクセスします。URLは『開通通知書』をご確認ください。**

   XCCのログイン画面が表示されます。

2. **お客さまにて作成済みのユーザまたは『開通通知書』に記載されたユーザ名、パスワードにてログインします。**

   XCCのホーム画面が表示されます。

3. **左ペインより「イベント」を選択し、右ペインの「アラート受信者」タブを開きます。**

4. **「メール/Syslog受信者」欄にて「+作成」アイコンをクリックします。**

   「メール受信者を作成」、「Syslog受信者を作成」の選択肢が表示されます。

5. **「Syslog受信者を作成」を選択し、お客さま環境のSyslogサーバの情報を入力し、「適用」をクリックします。**

   「メール/Syslog受信者」欄に新規Syslogサーバが表示されます。

6. **「メール/Syslog受信者」欄にて、新規登録したSyslogサーバの「」アイコンをクリックし「OK」をクリックします。**

   Syslogサーバに対して試験用のログが送信されます。

22.2.2. XCCからのログ確認

1. **WebブラウザにてXCCへアクセスします。URLは『開通通知書』をご確認ください。**

   XCCのログイン画面が表示されます。

2. **お客さまにて作成済みのユーザまたは『開通通知書』に記載されたユーザ名、パスワードにてログインします。**

   XCCのホーム画面が表示されます。

3. **左ペインより「イベント」を選択し、右ペインから参照したいログのタブを開きます。**

   対象のログが表示されます。

22.2.3. ログのエクスポート

1. **WebブラウザにてXCCへアクセスします。URLは『開通通知書』をご確認ください。**

   XCCのログイン画面が表示されます。

2. **お客さまにて作成済みのユーザまたは『開通通知書』に記載されたユーザ名、パスワードにてログインします。**

   XCCのホーム画面が表示されます。

3. **画面上部の「エクスポート」をクリックし、エクスポートするログにチェックを入れ「エクスポート」ボタンをクリックします。**

   「エクスポートしています」と表示されます。

4. **ファイルのダウンロードが実行されます。**

   ダウンロード先や、ダウンロード確認が表示されるかはブラウザの設定に依存します

> **補足** 2023年02月時点ではHTML形式でのエクスポートは正常にファイルが生成されない不具合があります。そのため、Excel形式でのエクスポートをご利用ください。

22.3. Lenovo XClarity Controller(XCC)構成のバックアップおよびリストア

サーバの設定を変更した際は、お客さまにてバックアップの取得をお願いいたします。

重要 **サーバ故障時における注意事項**

サーバの修理対応により、下記の２点が発生する可能性があります。

① サーバ設定がリセットされる

② サーバのFirmwareバージョンが修理前と異なる

サーバ修理にて交換されるパーツによっては、各種Firmwareが初期化される場合があります。

またこの作業において、お客さまが故障直前にご利用いただいていたFirmwareバージョンを復旧できる場合と、メーカ都合によりバージョンの異なるFirmwareに設定される場合とがあります。

前者の場合は①に該当し、お客さまにて取得いただいたBMC構成のバックアップファイルにより、設定の復旧が可能です。

後者の場合、異なったBMCバージョン間でのリストアはメーカーサポート外となるため

バックアップファイルによるリストアが実施できません。お客さまのお手元にバックアップファイルとは別に設定情報を保管してください。

22.3.1. Lenovo XClarity Controller(XCC)構成のバックアップ

以下の手順にて、XCCのバックアップを取得します。サーバ管理GUI上で管理されるパラメータは、BMC構成のバックアップに含まれます。

重要 **注意事項**

異なったBMCバージョン間でのリストアはメーカーサポート外となります。

BMCのバージョンアップを実施された場合は、併せてBMC構成のバックアップを取得してください。

1. **Webブラウザにて XCCへアクセスします。URLは『開通通知書』をご確認ください。**

   XCCのログイン画面が表示されます。

2. **お客さまにて作成済みのユーザまたは『開通通知書』に記載されたユーザ名、パスワードにてログインします。**

   XCCのホーム画面が表示されます。

3. **左ペインより「BMC構成」>「バックアップおよびリストア」を選択します。**

4. **右ペインより「BMC 構成のバックアップ」を開きます。**

5. **リストア時に必要となる「パスワード」を設定し、「バックアップを開始」をクリックします。**

   「バックアップを処理中です」とポップアップが表示されます。正常に取得できた場合は、バックアップ取得時間と併せて、「直近のバックアップが正常に完了しました」と表示されます。

6. **「バックアップ・ファイルのダウンロード」をクリックします。**

   拡張子.bak のファイルがダウンロードされます。

22.3.2. Lenovo XClarity Controller(XCC)構成のリストア

事前に取得したXCC構成のバックアップファイルを利用し、設定のリストアを実施します。

1. **WebブラウザにてXCCへアクセスします。URLは『開通通知書』をご確認ください。**

   XCCのログイン画面が表示されます。

2. **お客さまにて作成済みのユーザまたは『開通通知書』に記載されたユーザ名、パスワードにてログインします。**

   XCCのホーム画面が表示されます。

3. **左ペインより「BMC構成」>「バックアップおよびリストア」を選択します。**

4. **右ペインより「構成ファイルからの BMC の復元」を開きます。**

5. **「参照」をクリックし、事前に取得したバックアップファイルを選択し、バックアップ取得時に指定したパスワードを入力します。**

6. **「次へ」をクリックします。**

7. **「復元を開始」をクリックします。**

   「復元を処理中です」と表示されますので、「復元が完了しました」と表示されるまで待ちます。

22.4. 仮想メディアからの起動

OSのインストールメディアファイルを利用した仮想メディアからの起動手順について記載いたします。起動後のOSインストール手順に関してはメーカーマニュアルをご参照ください。

1. **WebブラウザにてXCCへアクセスします。URLは『開通通知書』をご確認ください。**
   XCCのログイン画面が表示されます。

2. **お客さまにて作成済みのユーザまたは『開通通知書』に記載されたユーザ名、パスワードにてログインします。**
   XCCのホーム画面が表示されます。

3. **左ペインにて「リモート・コンソール」を選択します。**

4. **「リモート・コンソール・プレビュー」の画面をクリックし、続けて「リモート・コンソールの起動」をクリックします。**
   新規のブラウザタブが開き、コンソール画面が表示されます。ポップアップがブロックされた場合はポップアップを許可します。

5. **「メディア」タブをクリックします。**
   「仮想メディアをマウントする」画面が表示されます。

6. **「ローカル・メディア・ファイルのマウント」欄にて「アクティブにする」をクリックします。**
   仮想メディアが有効になり「参照」が選択できるようになります。

7. **「参照」をクリックし、ローカルのメディアファイルを選択します。**

8. **「すべてのローカル・メディアのマウント」タブをクリックします。**
   画面上部に「合計１の仮想メディアをマウント済み」と表示されます。

9. **「次回起動時にブートする仮想メディアを選択」を開き、「-マウント済みメディアを１つ選択-」をクリックし、マウントしたイメージを選択します。**

10. **「後で手動で再起動」をクリックし、「今すぐサーバーを再起動」を選択します。**

11. **「OK」をクリックします。**
    「今すぐサーバーを再起動してメディア<メディア名>からブートしますか？」と表示されます。

12. 「適用」をクリックします。

「今すぐサーバーを再起動 コマンドが送信されました。」と表示されます。

13. 「閉じる」をクリックします。

マウントしたメディアからの起動を待ちます。

14. インストールするOSのマニュアルを参照し、初期インストールを実施します。

15. OSのマニュアルを参照し、ネットワーク、ストレージのパスに対して冗長化の設定を実施します。

> **重要** **注意事項**
>
> ベアメタルサーバが接続されるイーサネットおよびファイバーチャネルの物理スイッチは、2台で冗長構成を組んでいます。ベアメタルサーバにて稼働するシステムの対障害性を考慮し、必ずOS上にて、パスの冗長化設定を実施してください。

22.5.OS上でのボリュームの認識方法

Windows Server 2019を例に、ボリュームのシリアル番号およびLUNの識別方法を記載いたします。開通後のボリュームサイズ変更やボリューム削除のお申込みの際は対象ボリュームのシリアル番号またはLUNをお知らせください。

> **補足** OS 上の操作に関しましては当社サポート外となりますので、OS 毎の確認方法につきましてはお客さまにてご確認ください。

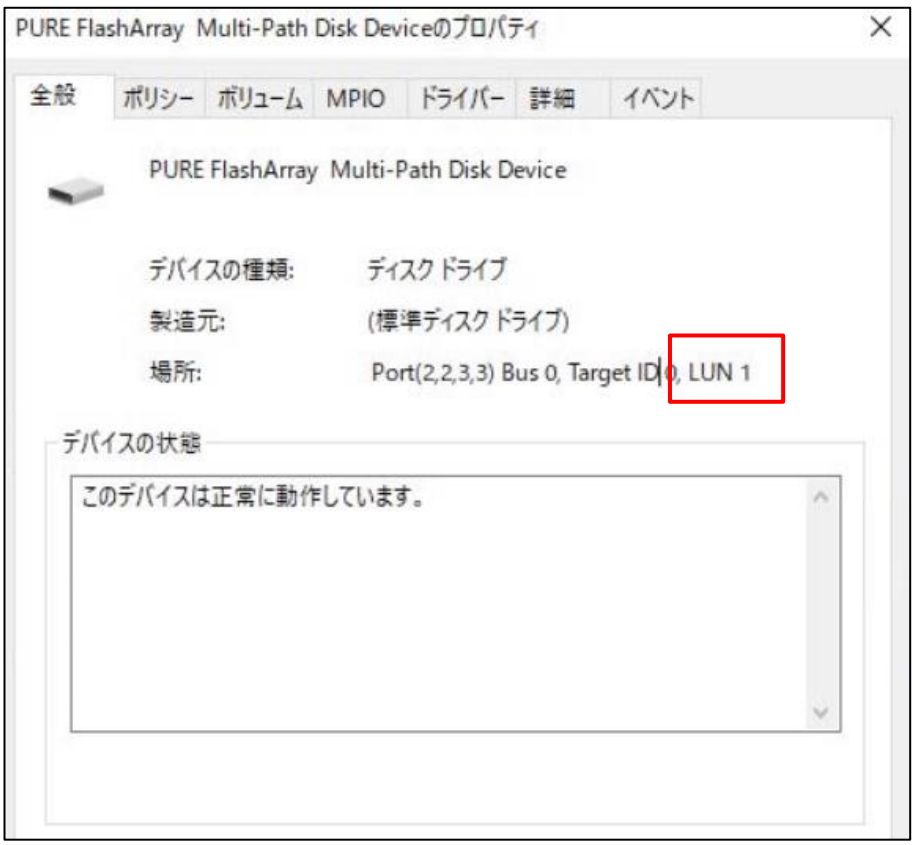
1. **ベアメタルサーバにインストールしたOSにログインします。**

2. **「ディスクの管理」を起動します。**

3. **対象のボリュームを右クリックし、「プロパティ」を開きます。**

4. **「全般」タブから「場所」を確認します。**

   『開通通知書』にてお伝えした「LUN」が確認できます。

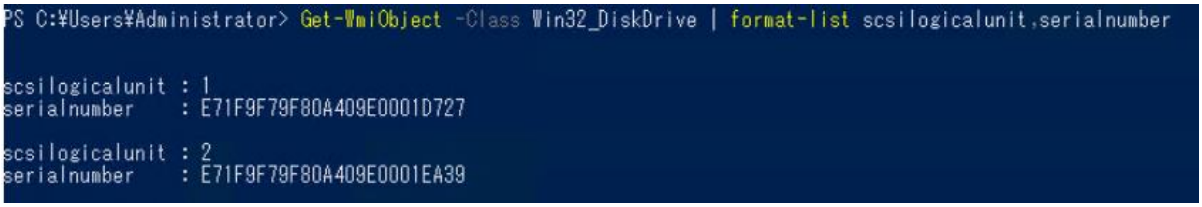


5. 「Windows Power Shell」 を起動します。

コンソール画面が表示されます。

6. コマンド「Get-WmiObject -Class Win32_DiskDrive | format-list scsilogicalunit,serialnumber」を実行します。

「scsilogicalunit」が、先に確認した「LUN」に該当します。OS上のどのディスクに対して、「LUN」と「シリアル番号」がマッピングされているかを確認できます。



22.6. サーバの電源操作

ベアメタルサーバの電源操作についてご説明いたします。サーバの電源操作に関してはOS上の操作を基本とし、XCCからの電源操作はFirmwareのバージョンアップやOS上の操作を受け付けない場合等、必要な場合にのみ実施することを推奨します。

1. **WebブラウザにてXCCへアクセスします。URLは『開通通知書』をご確認ください。**

   Lenovo XClarity Controllerのログイン画面が表示されます。

2. **お客さまにて作成済みのユーザまたは『開通通知書』に記載されたユーザ名、パスワードにてログインします。**

   Lenovo XClarity Controllerのホーム画面が表示されます。

3. **ホーム画面の「クイック操作」欄にて、「電源操作」をクリックします。**

   電源操作メニューの一覧が表示されます。

4. **操作メニュー一覧より、再起動やシャットダウン等の実施したい操作を選択します。**

22.7. Firmwareのバージョンアップ

Firmwareのバージョンアップについては、メーカーマニュアル、ご利用いただくOSとの互換性、および対象Firmwareのリリースノートをご参照のうえ、実施してください。

Firmwareについてサポート期間は定められておりませんが、メーカによる推奨バージョンは常に最新版となっておりますので、定期的なアップデートの実施を推奨します。

各種Firmwareのバージョン確認方法を以下に記載いたします。

1. **WebブラウザにてXCCへアクセスします。URLは『開通通知書』をご確認ください。**

   Lenovo XClarity Controllerのログイン画面が表示されます。

2. **お客さまにて作成済みのユーザまたは『開通通知書』に記載されたユーザ名、パスワードにてログインします。**

   Lenovo XClarity Controllerのホーム画面が表示されます。

3. **左ペインより「システム一覧」を選択します。**

   右ペインにシステムデバイスの一覧が表示されます。各デバイスの詳細や「システム・ファームウェア」欄より各種Firmwareのバージョンが確認できます。

23. ライセンスオプションサービス利用手順(ベアメタル)

本項では、ベアメタルサーバでライセンスオプションサービスをお申し込みいただいている場合の利用について手順をご説明いたします。

> **重要** ライセンスオプションサービスを利用したOSの利用には、ライセンス認証またはソフトウェアアップデートのためのインターネット接続が必要です。

23.1. Microsoft SPLA ライセンス を利用する際の Windows Serverについて(ベアメタル)

Microsoft SPLA ライセンスのお申し込みにより提供される Windows Server についてご説明いたします。

ベアメタルサーバ用 Windows設定

ベアメタルサーバでSPLAライセンスを利用する際は当社にてWindows OSのインストールを実施いたします。OSはインストール時のパラメータ設定とライセンス認証のみ実施した状態で提供いたします。

設定項目	設定
インストールする言語	日本語(日本)
時刻と通貨の形式	日本語(日本)
キーボードまたは入力方式	Microsoft IME
キーボードの種類	日本語キーボード(106/109 キー)
初期パスワード	『開通通知書』をご確認ください

> **補足**
> ・ Server Core のインストールオプションは提供しておりません。
> ・ Disk は単一のパーティションでインストールを実施します。

ベアメタルサーバ用 Windows設定(Windows Server 2016のみ)

Windows Server 2016はインストール直後のOS標準のドライバではNICが認識されないため、当社にてNICのドライバのみインストールを実施いたします。

インストールドライバ	バージョン(2023/02 時点)
Intel Network Windows Driver	27.3.6

23.2. RHELサブスクリプションライセンスの利用(ベアメタル)

RHELサブスクリプションライセンスのお申し込みにより、コンテンツライブラリ上にRHEL ISOが提供されます。

本項では、インストールしたRHELにてRHUIサーバを利用する手順についてご説明いたします。

重要

- RHELのライセンスオプションをお申し込みのお客さまのみ、ISOをコンテンツライブラリ上に提供します。
- アップデート提供サーバ（RHUIサーバ）へのアクセス（yumコマンドの使用）は、当社が提供するインターネット接続からのアクセスに限定しています。
- アップデート提供サーバ（RHUIサーバ）をご契約頂いたサーバ以外で利用するのは禁止事項となります。
- 東日本サイトのRHUIサーバ宛には、宛先IPアドレス（118.103.99.11）およびhttps（443/TCP）通信の許可が必要です。FQDNは「eastrhui.aspire.gcf.whitecloud.jp」です。
- 西日本サイトのRHUIサーバ宛には、宛先IPアドレス（221.110.171.251）およびhttps（443/TCP）通信の許可が必要です。FQDNは「westrhui.aspire.gcf.whitecloud.jp」です。
- 当社が提供するISOより上位のバージョンを利用する場合は、お客さまがアップデートする必要があります。

  例）7.5 へアップデートする場合

  yum update redhat-release-server-7.5.8.el7 kernel-3.10.0-862.3.3.el7

  バージョンはお客さまにて事前に確認の上、適切なバージョンを指定してください。
- ベアメタルサーバ用にお客さま保有のRed Hatライセンス（RHELサブスクリプション）の持込む場合「Red Hat Cloud Access」の利用は不要です。
- ベアメタルサーバでRHUIを利用する場合は対象のサーバハードウェアがRedHatでサポートされている必要があります。

  本手順はインストール直後の状態からの設定例となります。rpmのダウンロード先などはお客さま環境に合わせて読みかえてください。
- RHUIサーバの提供パッケージは、RHEL6,RHEL7では「Base」、「Optional」、「RH Common」、「Extras」、「RHSCL」リポジトリの標準パッケージ、RHEL8では[BaseOS] [AppStream] [CodeReady Linux Builder] リポジトリの標準パッケージが対象となります。

  それ以外のパッケージ(「Debug」、「Source」など)は当社提供対象外となります。

1. 対象のベアメタルサーバにroot権限を持つユーザでログインします。

2. 以下のコマンドを実行します。

以下RHEL8環境の/rootで作業を実施した場合の例となります。OSのバージョンにより表示が異なる場合があります。

 # curl --connect-timeout 10 -kv https://<RHUI サーバ FQDN>/ (RHUI サーバアクセス確認)
< HTTP/1.1 200 OK (このメッセージが含まれることを確認)

 # curl -k -O https://<RHUIサーバ FQDN>/pub/tmp/RPM-GPG-KEY-rhui-custom (GPGキーのダウンロード)
 # ls -ls /root/（GPGキーのダウンロード確認）
RPM-GPG-KEY-rhui-custom (GPGキーファイルが含まれることを確認)

 # curl -k -O https:// <RHUI サーバ FQDN>/pub/tmp/<クライアントパッケージ名>
(クライアントパッケージのダウンロード)

▼クライアントパッケージ名
・RHEL6：rhel-6-rhui-client-config-4.2-1.noarch.rpm
・RHEL7：rhel-7-rhui-client-config-4.2-1.noarch.rpm
・RHEL8：rhel-8-rhui-client-config-4.2-1.noarch.rpm

 # ls -ls /root/（クライアントパッケージのダウンロード確認）
rhel-8-rhui-client-config-4.2-1.noarch.rpm (クライアントパッケージが含まれることをを確認)

 # rpm -Kv ./<クライアントパッケージ名>（GPG キー インポート前の状態確認）
Header V4 RSA/SHA256 Signature, key ID 9b7ce762: NOKEY
V4 RSA/SHA256 Signature, key ID 9b7ce762: NOKEY
(Signature が含まれる行で NOKEY が表示されることを確認する)

 # install -m 644 ./RPM-GPG-KEY-rhui-custom /etc/pki/rpm-gpg/（GPGキーのインストール）
 # rpm --import /etc/pki/rpm-gpg/RPM-GPG-KEY-rhui-custom（GPG キーのインポート）
正常に完了した場合、特にメッセージは表示されません

 # rpm -Kv ./ <クライアントパッケージ名>（GPG キー インポート後の状態確認）
Header V4 RSA/SHA256 Signature, key ID 9b7ce762: OK
V4 RSA/SHA256 Signature, key ID 9b7ce762: OK
(Signature が含まれる行が OK に変わっていることを確認する)

 # yum repolist （yum で利用できるリポジトリが無いことを確認）
No repositories available (このメッセージが表示されることを確認)

 # yum install -y ./<クライアントパッケージ名> ; echo $? （クライアントパッケージのインストール）
<snip>
Installed:
  rhel-8-rhui-client-config-4.2-1.noarch

Complete!
0
(クライアントパッケージがインストールされ、戻り値が 0(正常終了)で表示されることを確認)

 # ls /etc/yum.repos.d/（クライアントパッケージのインストール確認）
rh-cloud.repo
(rh-cloud.repo が含まれることを確認)

 # cat /etc/yum.repos.d/rh-cloud.repo（クライアントパッケージのインストール確認）
[rhui-codeready-builder-for-rhel-8-x86_64-rhui-rpms]
[rhui-custom-rhel-8-rhui-client-config]
[rhui-rhel-8-for-x86_64-appstream-rhui-rpms]
[rhui-rhel-8-for-x86_64-baseos-rhui-rpms]
(RHEL8 の場合上記が含まれることを確認)

 # yum repolist（利用できるリポジトリ確認）
rhui-codeready-builder-for-rhel-8-x86_64-rhui-rpms
rhui-custom-rhel-8-rhui-client-config
rhui-rhel-8-for-x86_64-appstream-rhui-rpms
rhui-rhel-8-for-x86_64-baseos-rhui-rpms
(RHEL8 の場合上記が含まれることを確認)

 # yum clean all && yum repolist -v（yum キャッシュ削除とリポジトリ詳細確認）
<snip>
rhui-codeready-builder-for-rhel-8-x86_64-rhui-rpms
<snip>
Repo-pkgs　　：6,104
(Custom 以外のリポジトリでパッケージの数が参照できることを確認)

以上でRHUIの利用準備が完了します。

24. 用語集

本書の説明に使われている用語を解説します。（五十音順・アルファベット順）

用語	意味
オブジェクト	クラスタや仮想マシン、ストレージ、ネットワークなど、vSphere 環境で管理される何らかの実体を意味します。
オンプレミス環境	お客さまの管理する設備内に設置されたサーバやソフトウェアなどの情報システムのことを指します。
お客さま	本サービスの各種管理ツールを利用し、プライベートクラウド環境を管理する方のことを指します。
クラスタ	複数のコンピュータをまとめて 1 つのコンピュートシステムとしたものを指します。vSphere 環境においては、ESXi サーバをまとめてクラスタとし、その上で仮想マシンを稼働させます。
ゲスト OS	仮想マシン上で稼働する OS（オペレーティングシステム）です。
コンテナ	Docker イメージを元に作成される仮想環境の実行部分です。
コンテナレジストリ	コンテナレジストリとは、コンテナエンジンが扱うコンテナイメージファイルを保管する場所であり、またレジストリにおいてコンテナイメージのバージョン管理や配布を行えるツールです
テナント	本サービスのご契約によりお客さま専用に提供される vSphere 環境の契約ごとの管理単位です。
ペイン （左ペイン/右ペイン）	ウィンドウ内の分割されたエリアを指します。
メトリック	vRealize Operations Manager にて収集されたデータの各要素をメトリックと呼びます。
ワークロード	コンピューティングリソースと、コード（アプリケーションやバックエンドプロセスなど）の集まりです。本サービスではコンテナ機能を利用する際の vSphere ポッドとそれを構成するコンテナによるアプリケーションを指します。
仮想マシン	仮想化されたハードウェアのセット。仮想 CPU、仮想メモリ、仮想ディスク、仮想デバイスなどから構成された vCenter Server 上のオブジェクト
開通通知書	本サービスの開通後、お客さまの利用にあたり必要なアカウントやネットワーク情報が記載された通知書が発行されます。
名前空間	Kubernetes において、複数のユーザの間でクラスタリソースを分割する方法であり、その定義したオブジェクトです。
Firmware	サーバハードウェアを制御するためのソフトウェアでハードウェア上に組み込まれています。
DNAT	NAT とは Network Address Translation の略称で、IP アドレスの変換を行う仕組みです。送信先アドレスを変換するものを DNAT と呼びます。

用語	意味
Docker イメージ	アプリケーションの起動に必要なアプリケーション本体・ライブラリ・設定ファイルをひとまとめにし、コンテナエンジン上で実行できるパッケージにしたものです。
GPG キー	RPM パッケージの検証目的で使用する公開鍵です。
ISO イメージ	CD/DVD などのメディアに格納される形式で保存されたファイルフォーマットです。
Kubernetes	コンテナ化したアプリケーションのデプロイ、スケーリング、および管理を行うための、オープンソースのコンテナオーケストレーションシステムです。
OVF／OVA ファイル	異なる環境でも仮想マシンのイメージを相互にやり取りできるファイルフォーマットです。
RHUI サーバ	RPM パッケージが格納されているアップデート提供サーバです。
SNAT	NAT とは Network Address Translation の略称で、IP アドレスの変換を行う仕組みです。送信元アドレスを変換するものを SNAT と呼びます。
vMotion	VMware vCenter Server により提供されるライブマイグレーション機能です。仮想マシンを停止することなく ESXi ホストを変更することが可能です。
vSphere ポッド	1 つ以上の Linux コンテナを実行する占有量の小さい仮想マシンです。

25. 改訂履歴

日付	バージョン	改訂箇所
2021/04/01	1.0	初版作成
2021/05/26	1.01	全体的な文言修正、および説明項目の追加
2022/01/21	1.02	・提供テンプレートとして RHEL8 を追加 「5.5.5 RHEL サブスクリプションライセンスの利用」 ・Advanced Cross vCenter vMotion の利用方法を記載 「9 Advanced Cross vCenter vMotion による移行」 ・VMware 社製品の不具合情報を記載 「6.6.1　NAT の設定」 「6.10.1　分散ファイアウォールの設定」 「6.11.1　ゲートウェイ ファイアウォールの設定」 「6.15　証明書の操作」 「6.16　NSX ロードバランサの操作(オプション)」 ・ヘッダ修正
2022/07/11	1.03	・補足事項を追記 「15. Acronis Cyber Backup powered by ASPIRE」 ・新規オプション項目を追記 「16. モニタリングオプション(Mackerel)」 「17. Red Hat Cloud Access」

日付	バージョン	改訂箇所
2023/04/06	1.04	・全体的な文言修正、および説明項目の追加 ・vCenter の 7.0u3c バージョンアップに伴い UI の変更があった部分の修正 「1.5 プライベートクラウド管理のためのソフトウェア要件」 「5.1vSphere Client の利用について」 「5.2vSphere Client の基本操作」 「5.3 仮想マシンの管理操作」 「5.4 コンテンツライブラリの操作方法」 「5.5 ライセンスオプションサービス利用手順」 「5.6vSphere Client のそのほかの操作」 「6.4Overlay Network に関する操作」 「11.2 エコノミーストレージの利用方法」 ・vRealize Operations Manager 8.10.0 バージョンアップに伴い UI の変更があった部分の修正 「7 vRealize Operations Manager の操作」 ・ベアメタルサーバ向けの内容を追加 「18 ベアメタルサーバの提供機能」～ 「23 ライセンスオプションサービス利用手順(ベアメタル)」 ・ヴイエムウェア社製品の不具合情報を記載 「6.6.1 NAT の設定」 「6.13.2 グループの設定」 「仮想サーバの作成」
2023/09/01	1.05	Acronis Cyber Backup powered by ASPIRE の提供サービスが「Acronis Cyber Backup」から「Acronis Cyber Protect Cloud」へ変更されたことに伴い、サービス名表記を更新