

vSphere IaaS 制御プレーン のインストールと構成

Update 3

VMware vSphere 8.0

VMware vCenter 8.0

VMware ESXi 8.0

VMware by Broadcom の Web サイトで最新の技術ドキュメントを確認できます

<https://docs.vmware.com/jp/>

VMware by Broadcom

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

Copyright © 2022-2024 Broadcom. All Rights Reserved. 「Broadcom」という語表現は、Broadcom Inc. およびその子会社のいずれかまたは両方を指します。詳細については、<https://www.broadcom.com> を参照してください。本書に記載されるすべての商標、製品名、サービス マークおよびロゴは、各社に帰属します。

目次

vSphere IaaS 制御プレーンのインストールと構成 7

更新情報 8

1 vSphere IaaS control plane のインストールと構成のワークフロー 10

vSphere クラスタで vSphere IaaS control plane を構成するための前提条件 17

2 vSphere IaaS control plane のストレージ ポリシーの作成 20

3 マルチゾーン スーパーバイザー デプロイ用の vSphere Zones の作成 23

vSphere Zone の管理 24

4 vSphere IaaS control plane のネットワーク 25

スーパーバイザー ネットワーク 25

vSphere IaaS control plane で使用する NSX のインストールと構成 35

vSphere Distributed Switch の作成と構成 37

分散ポート グループの作成 38

vSphere Distributed Switch へのホストの追加 39

NSX Manager のデプロイと構成 41

NSX Manager ノードのデプロイによるクラスタの形成 42

ライセンスの追加 44

コンピュート マネージャの追加 44

トランスポート ゾーン の作成 46

ホストのトンネル エンドポイント IP アドレス用の IP アドレス プールの作成 46

Edge ノード用の IP アドレス プールの作成 47

ホスト アップリンク プロファイルの作成 48

Edge アップリンク プロファイルの作成 48

トランスポート ノード プロファイルの作成 49

クラスタ上の NSX の構成 50

NSX Edge トランスポートノードの設定とデプロイ 50

NSX Edge クラスタの作成 53

Tier-0 アップリンク セグメントの作成 53

Tier-0 ゲートウェイの作成 54

NSX と NSX Advanced Load Balancer のインストールと構成 56

NSX Advanced Load Balancer で使用する スーパーバイザー の vSphere Distributed Switch の作成 58

NSX Manager のデプロイと構成 59

NSX Manager ノードのデプロイによるクラスタの形成 61

ライセンスの追加	63
コンピューターマネージャの追加	63
トランスポートゾーンの作成	64
ホストのトンネルエンドポイントIPアドレス用のIPアドレスプールの作成	65
Edgeノード用のIPアドレスプールの作成	66
ESXiホストアップリンクプロファイルの作成	67
NSX Edgeアップリンクプロファイルの作成	68
トランスポートノードプロファイルの作成	68
NSX Edgeクラスタプロファイルの作成	69
クラスタ上のNSXの構成	70
NSX Edgeトランスポートノードの作成	70
NSX Edgeクラスタの作成	73
Tier-0ゲートウェイの作成	73
Edge Tier-0ゲートウェイへのNSXルートマップの構成	75
Tier-1ゲートウェイの作成	77
Tier-0アップリンクセグメントとオーバーレイセグメントの作成	77
NSXを使用したvSphere IaaS control plane用NSX Advanced Load Balancerのインストールと構成	78
ローカルコンテンツライブラリへのNSX Advanced Load Balancer OVAのインポート	78
NSX Advanced Load Balancer Controllerのデプロイ	79
NSX Advanced Load Balancer Controllerの構成	82
サービスエンジングループの構成	85
NSX Advanced Load Balancerの使用に関する制限事項	89
NSX Advanced Load Balancerのインストールと構成	89
NSX Advanced Load Balancerで使用するスーパーバイザーのvSphere Distributed Switchの作成	90
ローカルコンテンツライブラリへのNSX Advanced Load Balancer OVAのインポート	92
NSX Advanced Load Balancerコントローラのデプロイ	93
コントローラクラスタのデプロイ	95
コントローラのパワーオン	95
コントローラの構成	96
ライセンスの追加	100
コントローラへの証明書の割り当て	100
サービスエンジングループの構成	102
固定ルートの構成	103
仮想IPネットワークの構成	103
NSX Advanced Load Balancerのテスト	105
HAProxyロードバランサのインストールと構成	105
HAProxyロードバランサで使用するスーパーバイザーのvSphere Distributed Switchの作成	105
HAProxyロードバランサ制御プレーン仮想マシンのデプロイ	107
HAProxyロードバランサのカスタマイズ	109

- 5 3 ゾーン スーパーバイザー のデプロイ 112**
 - VDS ネットワーク スタックを使用する 3 ゾーン スーパーバイザー のデプロイ 112
 - NSX ネットワークを使用する 3 ゾーン スーパーバイザー のデプロイ 122
- 6 1 ゾーン スーパーバイザー のデプロイ 129**
 - VDS ネットワーク スタックを使用する 1 ゾーン スーパーバイザー のデプロイ 129
 - NSX ネットワークを使用する 1 ゾーン スーパーバイザー のデプロイ 139
- 7 NSX ネットワークで使用されるロード バランサの確認 145**
- 8 スーパーバイザー 構成のエクスポート 146**
- 9 JSON 構成ファイルのインポートによる スーパーバイザー のデプロイ 148**
- 10 スーパーバイザー へのライセンスの割り当て 151**
- 11 vSphere IaaS control plane クラスタへの接続 153**
 - vSphere 向け Kubernetes CLI Tools のダウンロードとインストール 153
 - vSphere IaaS control plane クラスタでのセキュア ログインの構成 155
 - vCenter Single Sign-On ユーザーとして スーパーバイザー に接続する 156
 - 開発者に対する Tanzu Kubernetes クラスタへのアクセス権の付与 158
- 12 スーパーバイザー の構成と管理 160**
 - スーパーバイザー API エンドポイントに安全に接続するための VIP 証明書の置き換え 161
 - スーパーバイザー の Tanzu Kubernetes Grid と Tanzu Mission Control の統合 162
 - Tanzu Kubernetes Grid クラスタのデフォルト CNI の設定 164
 - スーパーバイザー の制御プレーン サイズの変更 166
 - VDS ネットワークが構成されている スーパーバイザー のロード バランサ設定の変更 167
 - VDS ネットワークが構成されている スーパーバイザー へのワークロード ネットワークの追加 169
 - スーパーバイザー の管理ネットワーク設定の変更 171
 - VDS ネットワークが構成されている スーパーバイザー のワークロード ネットワーク設定の変更 172
 - NSX が構成されている スーパーバイザー のワークロード ネットワーク設定の変更 173
 - vSphere IaaS control plane での HTTP プロキシ設定の構成 175
 - vSphere Client を使用した スーパーバイザー での HTTP プロキシ設定の構成 176
 - クラスタ管理 API と DCLI を使用した スーパーバイザー への HTTP プロキシの構成 177
 - Tanzu Mission Control 向けの スーパーバイザー および TKG クラスタでの HTTP プロキシ設定の構成 178
 - TKG サービス クラスタで使用する外部 ID プロバイダの構成 179
 - スーパーバイザー への外部 IDP の登録 187
 - スーパーバイザー のストレージ設定の変更 191
 - カスタム可観測プラットフォームへの スーパーバイザー メトリックのストリーミング 193

スーパーバイザー 制御プレーンの DNS 名の変更 197

外部監視システムへの スーパーバイザー ログの転送 198

13 既存の構成のクローン作成による スーパーバイザー のデプロイ 204

14 スーパーバイザー の有効化のトラブルシューティング 206

有効化または更新中のスーパーバイザー制御プレーン仮想マシンの健全性ステータス エラーの解決 206

リモート rsyslog に対する スーパーバイザー 制御プレーンのログ ストリーミング 210

ワークロード管理有効化クラスタの互換性エラーのトラブルシューティング 212

ワークロード管理のログ ファイルのテール 214

15 ネットワークのトラブルシューティング 215

NSX Manager による vCenter Server の登録 215

NSX アプライアンスのパスワードを変更できない 216

障害が発生したワークフローと不安定な NSX Edge のトラブルシューティング 216

NSX のトラブルシューティングのためのサポート バンドルの収集 216

NSX のログ ファイルの収集 217

NSX の管理証明書、サムプリント、または IP アドレスが変更された場合の WCP サービスの再起動 218

NSX Advanced Load Balancer のトラブルシューティングのためのサポート バンドルの収集 218

NSX Advanced Load Balancer 構成が適用されない 219

ESXi ホストをメンテナンス モードに切り替えることができない 220

IP アドレスの問題のトラブルシューティング 220

トラフィック エラーに関する問題のトラブルシューティング 222

NSX のバックアップとリストアによって発生した問題のトラブルシューティング 222

NSX のバックアップとリストア後の古い Tier-1 セグメント 223

ホスト トランスポート ノードのトラフィックに必須の Distributed Switch 224

16 vSphere IaaS control plane のトラブルシューティング 225

ストレージのベスト プラクティスとトラブルシューティング 225

vSAN 以外のデータストアで制御プレーン仮想マシンの非アフィニティ ルールを使用する 225

vSphere から削除されたストレージ ポリシーが引き続き Kubernetes ストレージ クラスとして表示される 226

vSAN Direct と外部ストレージの併用 227

ネットワーク トポロジのアップグレードのトラブルシューティング 229

Edge ロード バランサのキャパシティ不足によるアップグレード事前チェックの失敗 229

アップグレード中にスキップされる スーパーバイザー ワークロードの名前空間 229

アップグレード中にスキップされるロード バランサ サービス 230

vSphere IaaS control plane ワークロード ドメインのシャットダウンと起動 230

スーパーバイザー でのサポート バンドルの収集 230

vSphere IaaS 制御プレーンのインストールと構成

『vSphere IaaS 制御プレーンのインストールと構成』では、vSphere Client を使用した vSphere IaaS control plane (旧称 vSphere with Tanzu) の構成と管理について説明します。

vSphere IaaS 制御プレーンのインストールと構成では、既存の vSphere クラスタで vSphere IaaS control plane を有効にし、名前空間を作成および管理する手順について説明します。この情報には、kubectl を使用した Kubernetes 制御プレーンとのセッション確立についてのガイドラインも含まれています。

対象読者

vSphere IaaS 制御プレーンのインストールと構成は、vSphere で vSphere IaaS control plane を有効にし、名前空間を構成して DevOps チームに提供する vSphere 管理者を対象としています。vSphere IaaS control plane を使用する vSphere 管理者には、コンテナおよび Kubernetes に関する基本的な知識が必要です。

更新情報

『vSphere IaaS 制御プレーンのインストールと構成』は、製品のリリースごとに、または必要に応じて更新されません。

『vSphere IaaS 制御プレーンのインストールと構成』の更新履歴については、次の表をご確認ください。

リビジョン	説明
2024年6月25日	vSphere 8.0 Update 3 リリースの一般的な更新と機能強化。
2024年3月18日	トピック「 スーパーバイザー API エンドポイントに安全に接続するための VIP 証明書の置き換え 」を更新し、証明書チェーン全体のインポートに関する注記を追加しました。
2024年2月29日	<ul style="list-style-type: none">■ コントローラの初期構成中にカスタム クラウドを作成する手順を追加しました。コントローラの構成を参照してください。■ スーパーバイザー のデプロイ中にクラウドを選択する手順を追加しました。VDS ネットワーク スタックを使用する 3 ゾーン スーパーバイザー のデプロイと VDS ネットワーク スタックを使用する 1 ゾーン スーパーバイザー のデプロイを参照してください。■ スーパーバイザー で FQDN ログインを構成する手順を追加しました。VDS ネットワーク スタックを使用する 3 ゾーン スーパーバイザー のデプロイ、VDS ネットワーク スタックを使用する 1 ゾーン スーパーバイザー のデプロイ、およびスーパーバイザー の管理ネットワーク設定の変更を参照してください。■ NSX オーバーレイ セグメントを作成する手順を追加しました。Tier-0 アップリンク セグメントとオーバーレイ セグメントの作成を参照してください。
2024年1月24日	<ul style="list-style-type: none">■ 「NSX Advanced Load Balancer Controller の NSX Manager への登録」を更新し、DNS と NTP の設定に関する注記を追加しました。■ プライベート認証局 (CA) 署名付き証明書が指定されている場合に、スーパーバイザー のデプロイが完了せず NSX Advanced Load Balancer 構成が適用されないときに実行が必要な手順の内容を追加しました。NSX Advanced Load Balancer 構成が適用されないを参照してください。
2023年12月23日	<ul style="list-style-type: none">■ VDS ネットワークが構成されている スーパーバイザー でのロード バランサ設定の変更に関するコンテンツを追加しました。VDS ネットワークが構成されている スーパーバイザー のロード バランサ設定の変更を参照してください。■ VDS ネットワークが構成されている スーパーバイザー のワークロード ネットワーク設定の変更に関するコンテンツを更新しました。VDS ネットワークが構成されている スーパーバイザー のワークロード ネットワーク設定の変更を参照してください。
2023年12月13日	ESXi ホストをトランスポート ノードとして準備するためのリファレンスを追加しました。 ホスト トランスポート ノードのライフックに必須の Distributed Switch を参照してください。
2023年11月21日	スーパーバイザー クラスタではマルチ NSX がサポートされていないことを示すドキュメントを更新しました。 コンピューターマネージャの追加 を参照してください。
2023年9月29日	<ul style="list-style-type: none">■ 「vSphere IaaS control plane での HTTP プロキシ設定の構成」の更新。■ HAProxy ロード バランサをカスタマイズする際の要件を更新しました。HAProxy ロード バランサのカスタマイズを参照してください。
2023年9月21日	NSX による NSX Advanced Load Balancer のインストールと構成の情報を使用して、ネットワークに関するセクションを更新しました。 NSX と NSX Advanced Load Balancer のインストールと構成 を参照してください。

リビジョン	説明
2023 年 6 月 30 日	スーパーバイザー のインストールに関するトピックと「 スーパーバイザー の制御プレーン サイズの変更 」にスーパーバイザー 制御プレーンのサイズを追加しました。
2023 年 6 月 23 日	コンテンツ ライブラリを作成および編集するためのリンクを更新しました。 ローカル コンテンツ ライブラリへの NSX Advanced Load Balancer OVA のインポート を参照してください。
2023 年 6 月 15 日	HTTP プロキシのみを使用してスーパーバイザー を Tanzu Mission Control に登録できるという注記を追加しました。 vSphere IaaS control plane での HTTP プロキシ設定の構成 を参照してください。
2023 年 5 月 15 日	スーパーバイザー または 1 ゾーン スーパーバイザー 内の名前空間に使用されるストレージ ポリシーでは使用ドメインを有効にしないという注記を追加しました。 2 章 vSphere IaaS control plane のストレージ ポリシーの作成 を参照してください。
2023 年 5 月 12 日	vSphere IaaS control plane 環境を vSphere 8.0 より前のバージョンからアップグレードして vSphere Zone を使用する場合は、新しい 3 ゾーン スーパーバイザー を作成する必要があるという注記を追加しました。 5 章 3 ゾーン スーパーバイザー のデプロイ を参照してください。
2023 年 4 月 26 日	「 vSphere 名前空間の構成と管理 」を『vSphere IaaS 制御プレーンのサービスとワークロード』に移動しました。
2023 年 4 月 18 日	NSX Advanced Load Balancer のインストールと構成 セクションを更新して、NSX Advanced Load Balancer バージョン 22.1.3 のサポートを追加しました。

vSphere IaaS control plane のイン ストールと構成のワークフロー

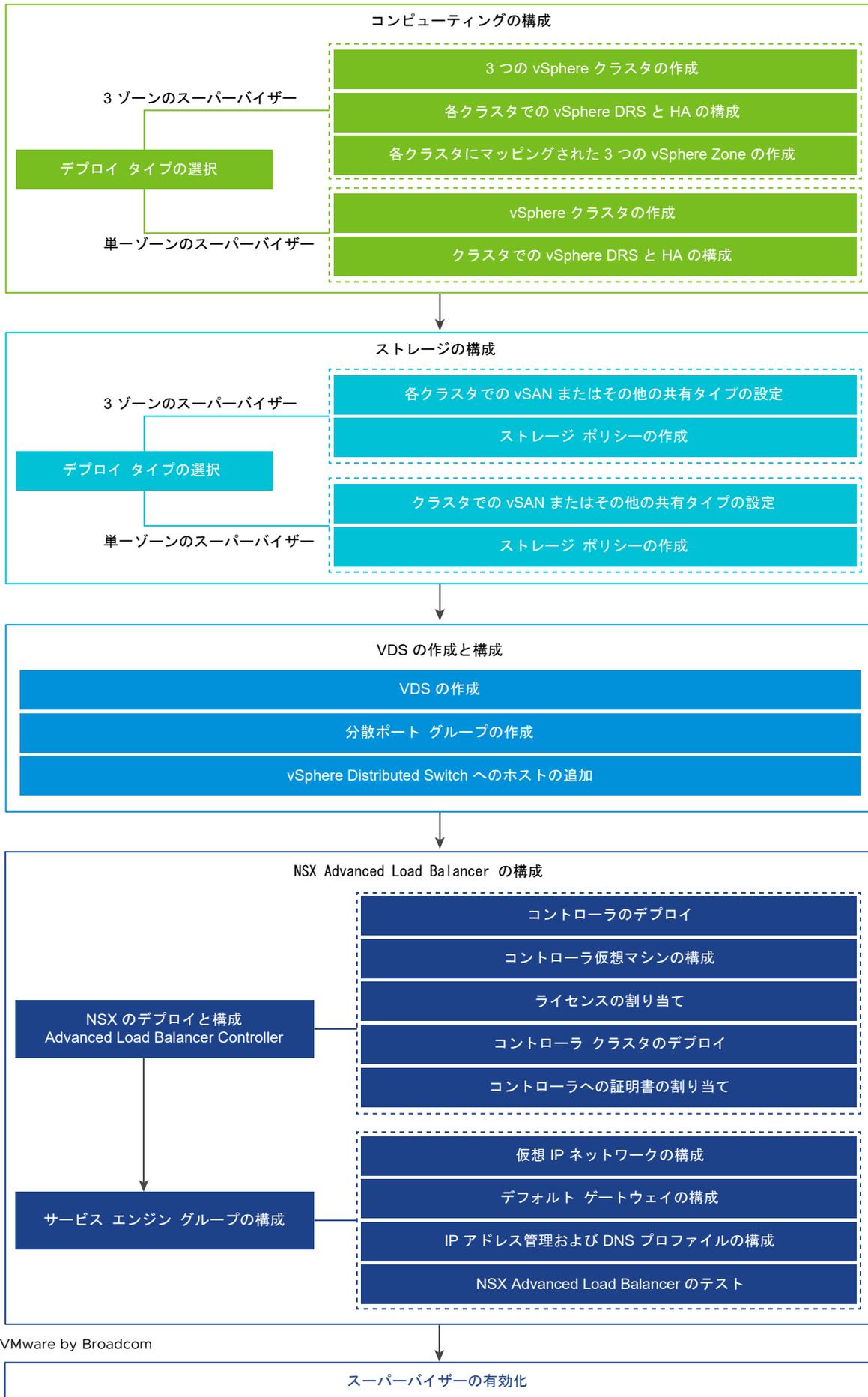
1

vSphere クラスタを、vSphere で Kubernetes ワークロードを実行するためのプラットフォームに変更するためのワークフローを確認します。

VDS ネットワークと NSX Advanced Load Balancer を使用して スーパーバイザー をデプロイするためのワークフロー

vSphere 管理者は、NSX Advanced Load Balancer による VDS ネットワークに基づくネットワーク スタックを使用して、スーパーバイザー をデプロイできます。

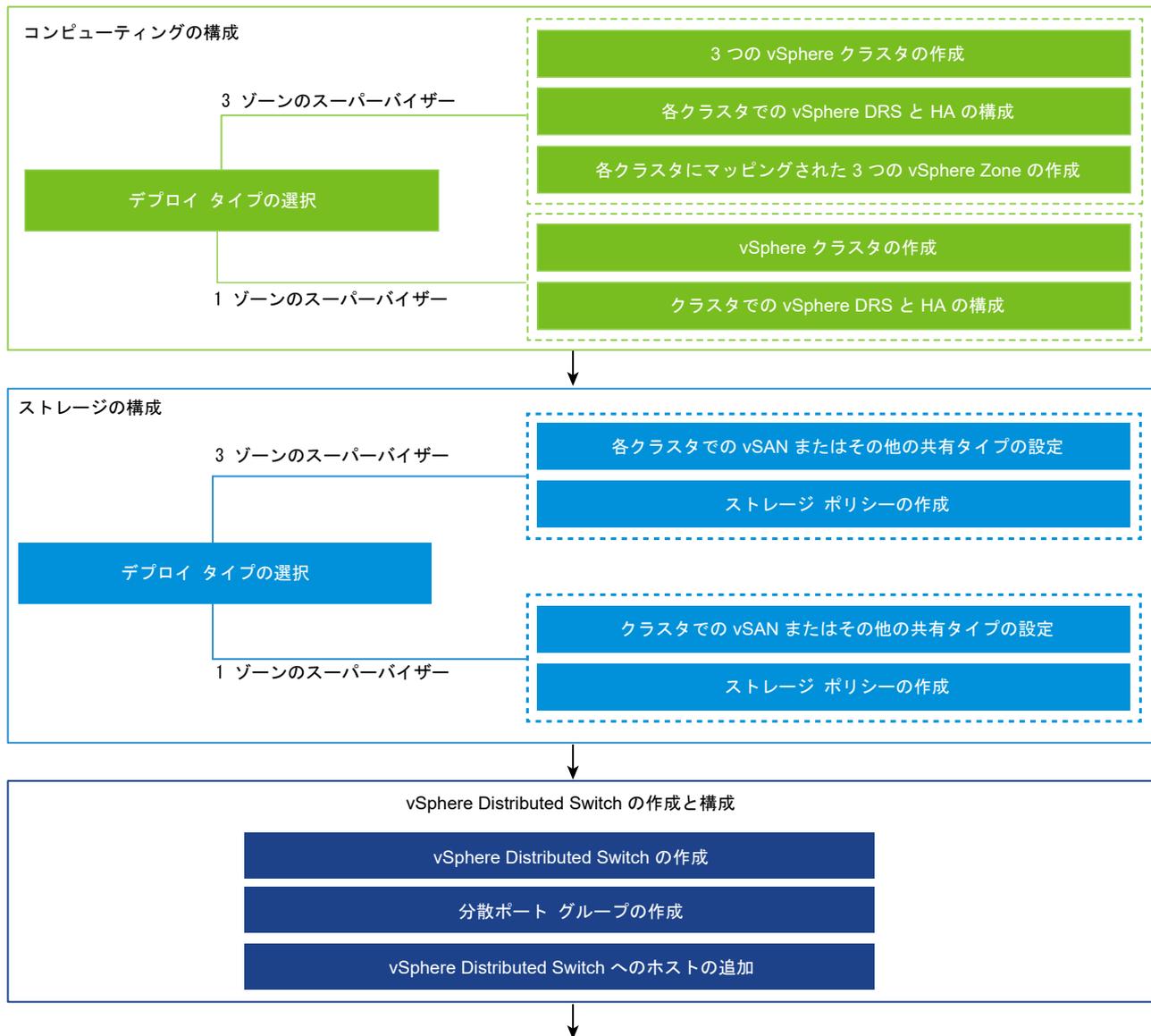
図 1-1. NSX Advanced Load Balancer を使用してスーパーバイザーをデプロイするためのワークフロー

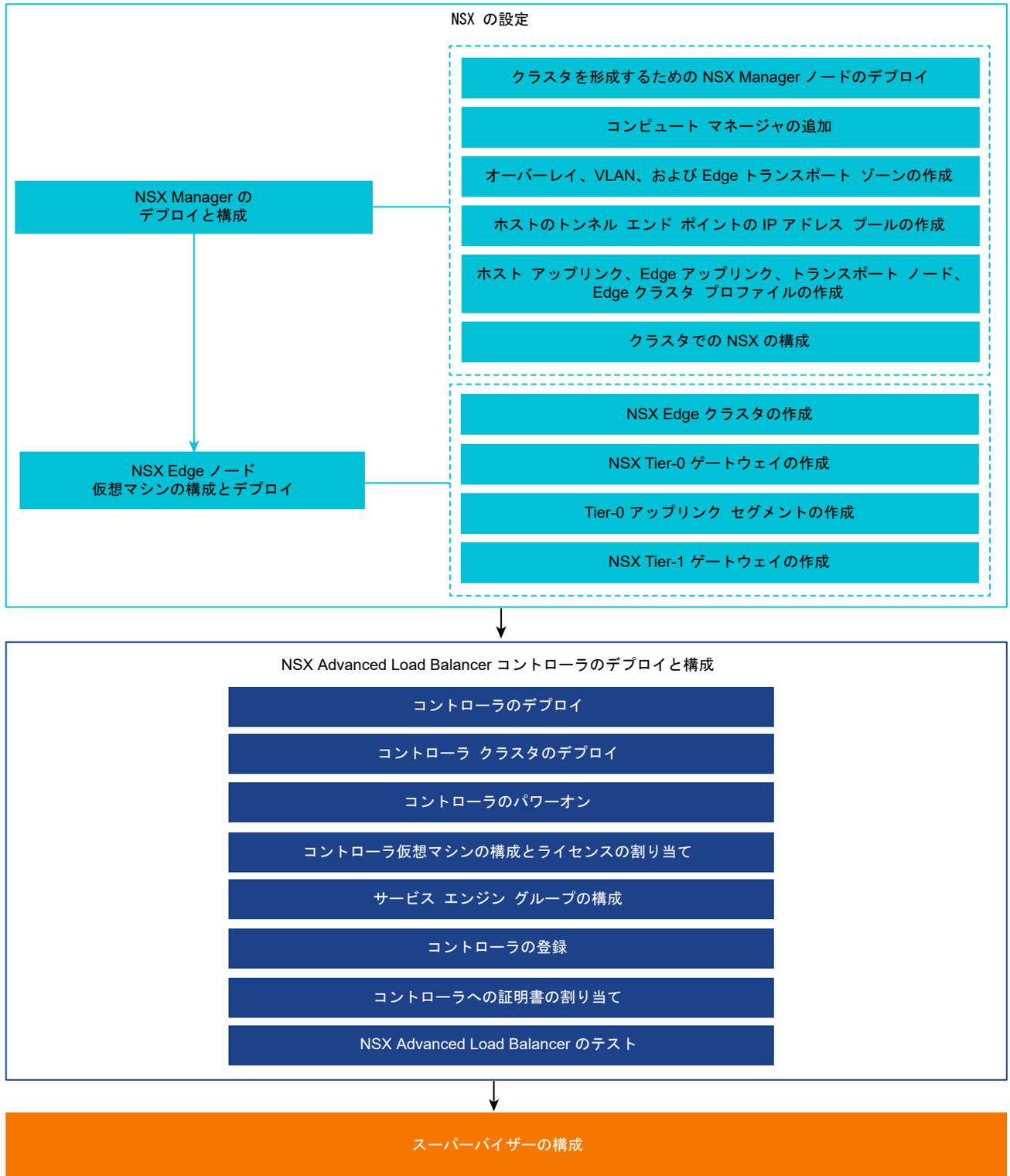


NSX ネットワークと NSX Advanced Load Balancer Controller を使用する スーパーバイザー のワークフロー

vSphere 管理者は、NSX ネットワーク スタックと NSX Advanced Load Balancer Controller を使用して、スーパーバイザー をデプロイできます。

図 1-2. NSX ネットワークと NSX Advanced Load Balancer Controller を使用してスーパーバイザーをデプロイするためのワークフロー

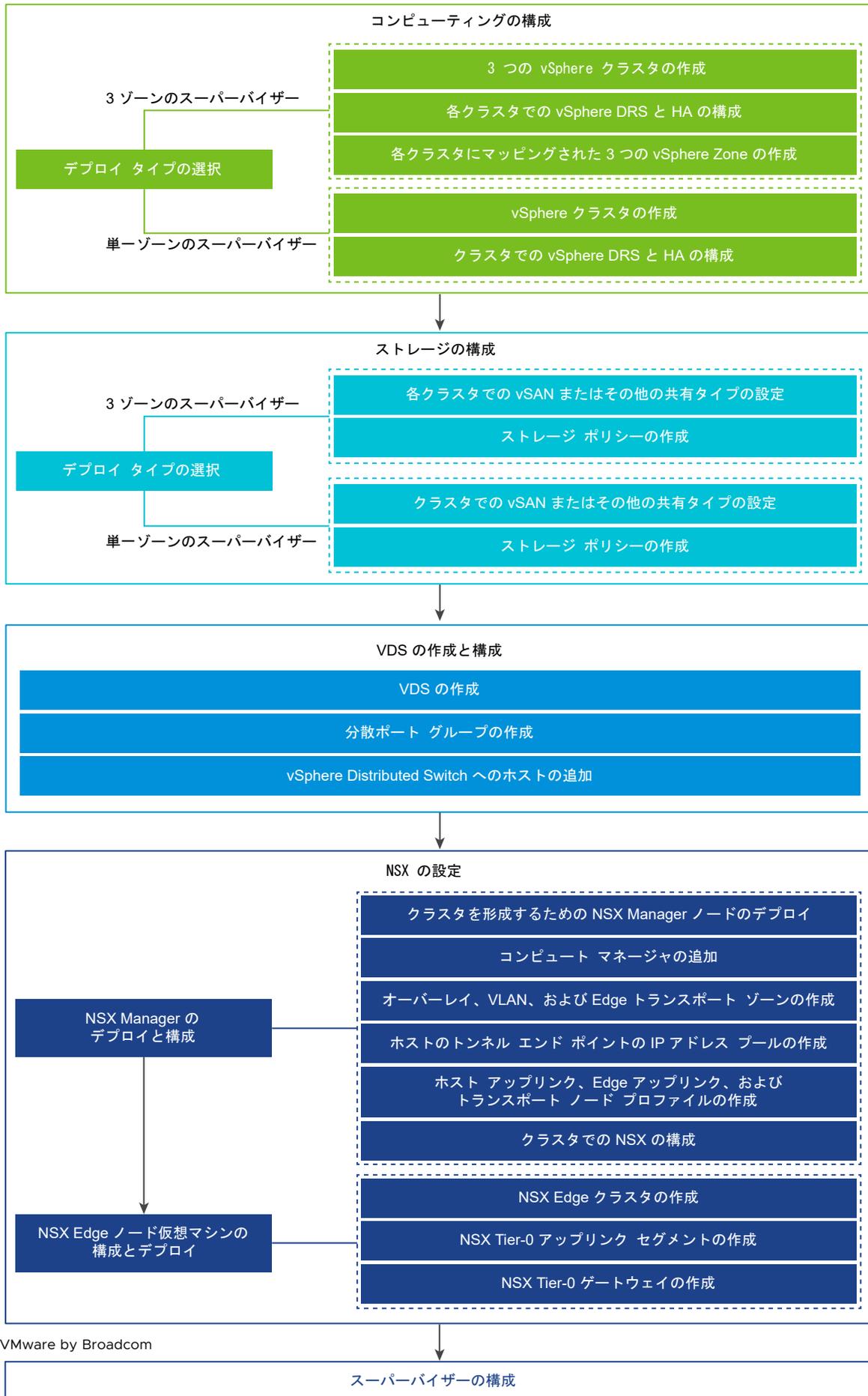




NSX ネットワークを使用して スーパーバイザー をデプロイするためのワークフロー

vSphere 管理者は、NSX に基づくネットワーク スタックを使用して、スーパーバイザー をデプロイできます。

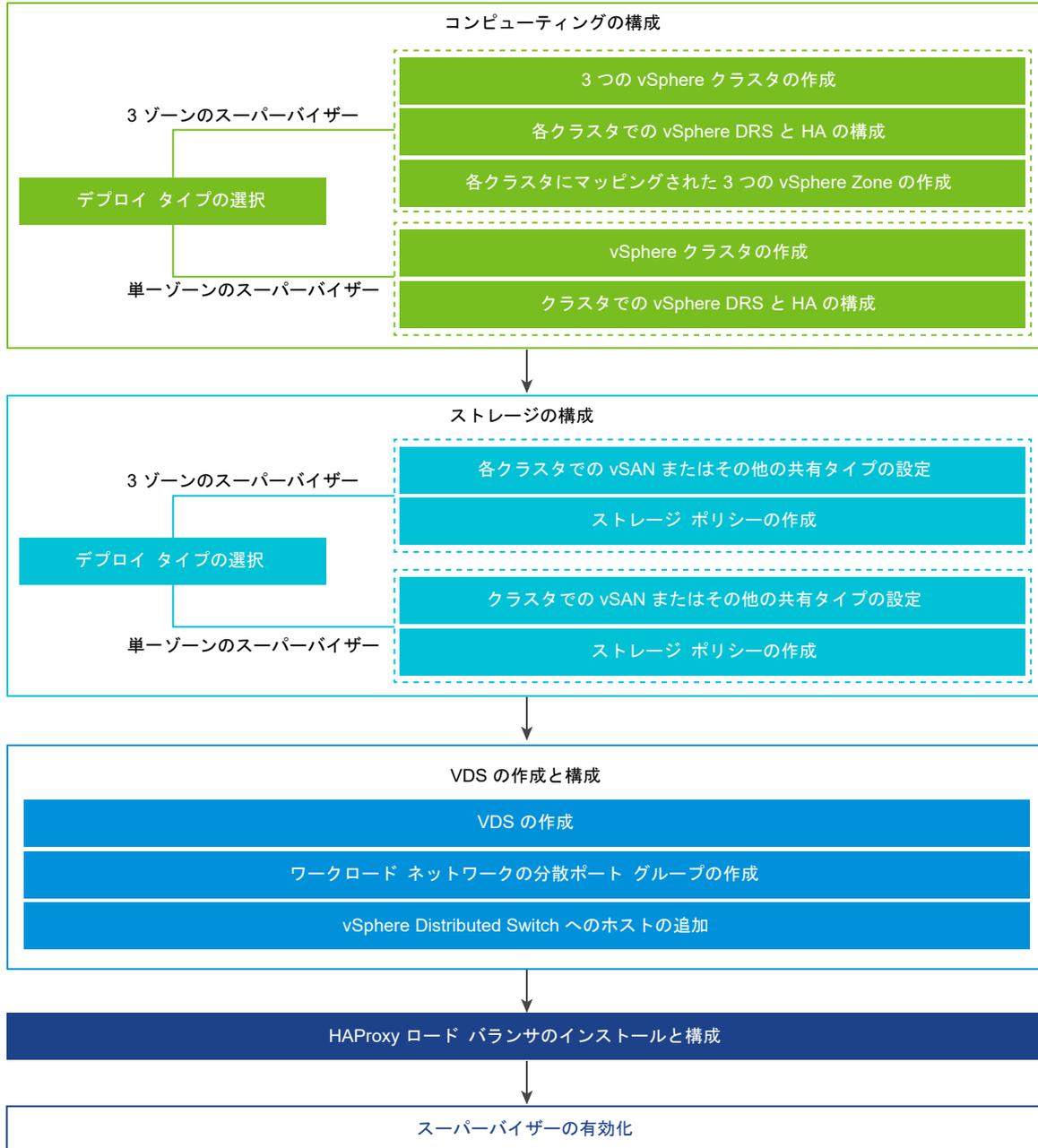
図 1-3. NSX をネットワーク スタックとして使用してスーパーバイザーをデプロイするためのワークフロー



VDS ネットワークと HAProxy ロード バランサを使用して スーパーバイザー をデプロイするためのワークフロー

vSphere 管理者は、VDS および HAProxy ロード バランサに基づくネットワーク スタックを使用して、スーパーバイザー をデプロイできます。

図 1-4. VDS ネットワークと HAProxy を使用してスーパーバイザーをデプロイするためのワークフロー



次のトピックを参照してください。

- [vSphere クラスタで vSphere IaaS control plane を構成するための前提条件](#)

vSphere クラスタで vSphere IaaS control plane を構成するための前提条件

vSphere 環境で vSphere IaaS control plane を有効にするための前提条件を確認してください。vSphere でコンテナベースのワークロードをネイティブに実行するには、vSphere 管理者が vSphere クラスタをスーパーバイザーとして有効にします。スーパーバイザーの Kubernetes レイヤーでは、vSphere ポッド、プロビジョニング Tanzu Kubernetes クラスタ、および仮想マシンをデプロイすることによって vSphere 上で Kubernetes ワークロードを実行できます。

vSphere クラスタの作成と構成

スーパーバイザーは、vSphere Zone に関連付けられている 1 つまたは 3 つの vSphere クラスタで実行できます。各 vSphere Zone は 1 つの vSphere クラスタにマッピングされ、1 つまたは 3 つのゾーンにスーパーバイザーをデプロイできます。3 ゾーンスーパーバイザーは、Kubernetes ワークロードを実行するために、より多くのリソースを提供します。また、vSphere クラスタレベルで高可用性を実現し、クラスタ障害からワークロードを保護します。1 ゾーンスーパーバイザーには、vSphere HA によって提供されるホストレベルの高可用性があり、1 つのクラスタのリソースのみを使用して Kubernetes ワークロードを実行します。

注： 1 つの vSphere Zone にスーパーバイザーをデプロイすると、スーパーバイザーを 3 ゾーンのデプロイに拡張できなくなります。

スーパーバイザーをデプロイする各 vSphere クラスタは、次の要件を満たす必要があります。

- 2 台以上の ESXi ホストが含まれる vSphere クラスタを作成、構成します。vSAN を使用している場合は、クラスタに少なくとも 3 台のホストが必要です。最適なパフォーマンスを得るには、4 台必要です。[クラスタの作成と構成](#)を参照してください。
- クラスタに vSAN などの共有ストレージを構成します。vSphere HA や DRS を使用するため、およびパーシステント コンテナ ボリュームを格納するためには、共有ストレージが必要です。[vSAN クラスタの作成](#)を参照してください。
- vSphere HA のクラスタを有効にします。[vSphere HA クラスタの作成と使用](#)を参照してください。
- 完全自動化モードで vSphere DRS のクラスタを有効にします。[DRS クラスタの作成](#)を参照してください。
- ユーザー アカウントに vSphere クラスタに対するクラスタ全体の構成の変更権限があって、ユーザーがスーパーバイザーをデプロイできることを確認します。
- 3 ゾーンスーパーバイザーをデプロイするには、3 つの vSphere ゾーンを作成します。[3 章 マルチゾーンスーパーバイザー デプロイ用の vSphere Zones の作成](#)を参照してください。
- スーパーバイザーで vSphere Lifecycle Manager イメージを使用する場合は、[ワークロード管理] を有効にする vSphere クラスタを vSphere Lifecycle Manager イメージを使用するように切り替えてから、[ワークロード管理] を有効にします。vSphere Lifecycle Manager ベースラインまたは vSphere Lifecycle Manager イメージのいずれかを使用して、スーパーバイザーのライフサイクルを管理できます。ただし、vSphere Lifecycle Manager ベースラインを使用するスーパーバイザーを、vSphere Lifecycle Manager イメージを使用するスーパーバイザーに変換することはできません。そのため、[ワークロード管理] を有効にする前に、vSphere クラスタを vSphere Lifecycle Manager イメージを使用するように切り替える必要があります。

ストレージ ポリシーの作成

スーパーバイザー をデプロイする前に、スーパーバイザー 制御プレーン仮想マシンのデータストア配置を決定するストレージ ポリシーを作成する必要があります。スーパーバイザー で vSphere ポッド がサポートされる場合は、コンテナとイメージのストレージ ポリシーも必要です。さまざまなレベルのストレージ サービスに関連付けられたストレージ ポリシーを作成できます。

2 章 vSphere IaaS control plane のストレージ ポリシーの作成 を参照してください。

ネットワーク スタックの選択と構成

スーパーバイザー をデプロイするには、それを使用するようにネットワーク スタックを構成する必要があります。2 つのオプションがあります。NSX と、ロード バランサを使用する vSphere Distributed Switch (vDS) ネットワークです。NSX Advanced Load Balancer または HAProxy ロード バランサを構成できます。

スーパーバイザー に NSX ネットワークを使用するには、次の操作を実行します。

- NSX ネットワークのシステム要件とトポロジを確認します。vSphere IaaS 制御プレーンの概念と計画 の [Requirements for Enabling a Three-Zone Supervisor with NSX](#) および [Requirements for Setting Up a Single-Cluster Supervisor with NSX](#) を参照してください。
- vSphere IaaS control plane で使用する NSX をインストールして構成します。vSphere IaaS control plane で使用する NSX のインストールと構成を参照してください。

スーパーバイザー で vDS ネットワークと NSX Advanced Load Balancer を使用するには、次の操作を実行します。

- NSX Advanced Load Balancer の要件を確認します。『vSphere IaaS 制御プレーンの概念と計画』の [Requirements for a Three-Zone Supervisor with NSX Advanced Load Balancer](#) および [Requirements for Enabling a Single Cluster Supervisor with NSX Advanced Load Balancer](#) を参照してください。
- vSphere Distributed Switch (vDS) を作成し、クラスタ内のすべての ESXi ホストを Distributed Switch に追加して、ワークロード ネットワーク用のポート グループを作成します。NSX Advanced Load Balancer で使用するスーパーバイザー の vSphere Distributed Switch の作成を参照してください。
- NSX Advanced Load Balancer をデプロイして構成します。NSX Advanced Load Balancer コントローラのデプロイを参照してください。

注： vSphere IaaS control plane は、vSphere 7 U2 以降で NSX Advanced Load Balancer をサポートします。

スーパーバイザー に、HAProxy ロード バランシングを使用する vDS ネットワークを使用するには、次の操作を実行します。

- HAProxy ロード バランサを使用する vSphere ネットワークのシステム要件とネットワーク トポロジを確認します。『vSphere IaaS 制御プレーンの概念と計画』の [Requirements for Enabling a Three-Zone Supervisor with HA Proxy Load Balancer](#) および [Requirements for Enabling a Single-Cluster Supervisor with VDS Networking and HAProxy Load Balancer](#) を参照してください。

- vSphere Distributed Switch (VDS) を作成し、クラスタ内のすべての ESXi ホストを Distributed Switch に追加して、ワークロード ネットワーク用のポート グループを作成します。HAProxy ロード バランサで使用する スーパーバイザー の vSphere Distributed Switch の作成を参照してください。
- スーパーバイザー をデプロイする vSphere クラスタのホストに接続されている vDS にルーティング可能な HAProxy ロード バランサ インスタンスをインストールして構成します。HAProxy ロード バランサは、クライアント ネットワークからワークロードへのネットワーク接続をサポートし、Tanzu Kubernetes クラスタ間のトラフィックのロード バランシングを行います。HAProxy ロード バランサのインストールと構成を参照してください。

注： vSphere IaaS control plane は、vSphere 7 U1 以降で HAProxy ロード バランサをサポートします。

vSphere IaaS control plane のストレージポリシーの作成

2

vSphere IaaS control plane を有効にする前に、スーパーバイザー および名前空間で使用するストレージポリシーを作成します。このポリシーは、データストアを表し、スーパーバイザー 制御プレーン仮想マシン、vSphere ポッドの短期ディスク、コンテナ イメージなどのコンポーネントやオブジェクトのストレージ配置を管理します。パーシステント ボリュームおよび仮想マシン コンテンツ ライブラリのストレージ配置にもポリシーが必要になることがあります。Tanzu Kubernetes クラスタを使用する場合は、ストレージポリシーによって、Tanzu Kubernetes クラスタ ノードのデプロイ方法も決定されます。

vSphere ストレージ環境と DevOps のニーズに応じて、さまざまなストレージ クラスのために複数のストレージポリシーを作成することができます。たとえば、vSphere ストレージ環境にブロンズ、シルバー、ゴールドの3つのクラスのデータストアがある場合、すべてのデータストア タイプに対してストレージポリシーを作成できます。

スーパーバイザー を有効にして名前空間を設定すると、多様なオブジェクト、コンポーネント、ワークロードで使用されるさまざまなストレージポリシーを割り当てることができます。

注： スーパーバイザー 用、または1ゾーンスーパーバイザー 内の名前空間用に作成するストレージポリシーは、トポロジに対応する必要はありません。これらのポリシーでは、使用ドメインを有効にしないでください。

3ゾーンスーパーバイザー 内の名前空間用に作成するストレージポリシーは、トポロジに対応し、手順4bで使用ドメインを有効にする必要があります。3ゾーン名前空間を使用すると、トポロジに対応しないストレージポリシーを割り当てることができません。

次の例では、ゴールドとタグ付けされたデータストアのストレージポリシーを作成します。

前提条件

- vSphere IaaS control plane でのストレージポリシーの詳細については、『vSphere IaaS 制御プレーンの概念と計画』の [About Storage Policies](#) を参照してください。
- パーシステント ストレージに vSAN データ パーシステンス プラットフォームを使用し、vSAN Direct または vSAN SNA データストア向けにカスタム ストレージポリシーを作成する必要がある場合は、『vSphere IaaS 制御プレーンのサービスとワークロード』の [Creating Custom Storage Policies for vSAN Data Persistence Platform](#) を参照してください。
- 3ゾーンスーパーバイザー でパーシステント ストレージに使用するトポロジ対応のストレージポリシーを作成する必要がある場合は、『vSphere IaaS 制御プレーンのサービスとワークロード』の [3ゾーンスーパーバイザーでのパーシステント ストレージの使用](#) を参照してください。
- ストレージポリシーで参照するデータストアが、クラスタ内のすべての ESXi ホスト間で共有されることを確認します。VMFS、NFS、vSAN、vVols など、環境内のすべての共有データストアがサポートされます。

- 必要な権限：仮想マシン ストレージ ポリシー.更新および仮想マシン ストレージ ポリシー.表示。

手順

1 データストアにタグを追加します。

- タグ付けするデータストアを右クリックし、[タグとカスタム属性] - [タグの割り当て] の順に選択します。
- [タグの追加] をクリックして、タグのプロパティを指定します。

プロパティ	説明
名前	データストア タグの名前を指定します (Gold など)。
説明	タグの説明を追加します (Datastore for Kubernetes objects など)。
カテゴリ	既存のカテゴリを選択するか、新しいカテゴリを作成します (Storage for Kubernetes など)。

2 vSphere Client で、[仮想マシン ストレージ ポリシーの作成] ウィザードを開きます。

- [メニュー] - [ポリシーおよびプロファイル] の順にクリックします。
- [ポリシーおよびプロファイル] で、[仮想マシン ストレージ ポリシー] をクリックします。
- [仮想マシン ストレージ ポリシーの作成] をクリックします。

3 ポリシーの名前と説明を入力します。

オプション	操作
vCenter Server	vCenter Server インスタンスを選択します。
名前	ストレージ ポリシーの名前 (goldsp など) を入力します。 注： vSphere IaaS control plane によって、名前空間に割り当てたストレージ ポリシーが Kubernetes ストレージ クラスに変換されると、すべての大文字は小文字に変更され、スペースがダッシュ (-) に置き換えられます。混乱を避けるため、仮想マシン ストレージ ポリシー名には小文字を使用し、スペースは含めないでください。
説明	ストレージ ポリシーの説明を入力します。

4 [ポリシー構造] 画面で次のオプションを選択し、[次へ] をクリックします。

- [データストア固有のルール]で、タグベースの配置ルールを有効にします。
- トポロジ対応のポリシーを作成するには、[ストレージ トポロジ] で [使用ドメインの有効化] を選択します。

この手順は、3 ゾーン スーパーバイザー 内の名前空間にあるパーシステント ストレージに対して使用するトポロジ対応のポリシーを作成する場合にのみ必要です。

5 [タグベースの配置] ページで、タグ ルールを作成します。

次の例を使用してオプションを選択します。

オプション	説明
タグ カテゴリ	ドロップダウン メニューから、タグのカテゴリ ([Kubernetes のストレージ] など) を選択します。
使用量オプション	[以下のタグ付けをされたストレージを使用:] を選択します。
Tags	[タグを参照] をクリックし、データストア タグ ([Gold] など) を選択します。

6 [ストレージ トポロジ] を有効にしてある場合は、[使用ドメイン] 画面でストレージ トポロジ タイプを指定します。

オプション	説明
ゾーン	データストアは、1つのゾーン内のすべてのホストで共有されます。

7 [ストレージ互換性] ページでこのポリシーに適合するデータストアのリストを確認します。

この例では、ゴールドとタグ付けされたデータストアのみが表示されます。

8 [確認して完了] ページでポリシーの設定を確認し、[完了] をクリックします。

結果

既存のストレージ ポリシーのリストに、ゴールドとタグ付けされたデータストアの新しいストレージ ポリシーが表示されます。

次のステップ

ストレージ ポリシーを作成した後、vSphere 管理者は次のタスクを実行できます。

- ストレージ ポリシーを スーパーバイザー に割り当てます。スーパーバイザー に設定したストレージ ポリシーにより、制御プレーン仮想マシン、ポッドの短期ディスク、およびコンテナ イメージが、ポリシーによって表されるデータストアに配置されます。
- ストレージ ポリシーを vSphere 名前空間 に割り当てます。名前空間で認識されるストレージ ポリシーにより、名前空間がどのデータストアにアクセスしてパーシステント ボリュームに使用できるかが決まります。ストレージ ポリシーは、名前空間では一致する Kubernetes ストレージ クラスとして表示されます。このストレージ クラスは、この名前空間の Tanzu Kubernetes クラスタにも伝達されます。DevOps エンジニアは、ストレージ クラスをパーシステント ボリュームの要求指定で使用できます。vSphere 名前空間の作成と構成を参照してください。

マルチゾーン スーパーバイザー デプロイ用の vSphere Zones の作成

3

vSphere Zone を作成する方法を確認します。vSphere Zone を使用すると、スーパーバイザー で実行されている Kubernetes ワークロードにクラスタ レベルの高可用性を提供できます。Kubernetes ワークロードにクラスタ レベルの高可用性を提供するには、3 つの vSphere Zones にスーパーバイザー をデプロイします。各 vSphere Zone は、少なくとも 2 台のホストを持つ、1 つの vSphere クラスタにマッピングされます。

前提条件

- 各ゾーンに 3 台以上のホストを持つ 3 つの vSphere クラスタを作成します。vSAN ストレージの場合、クラスタには 4 台のホストが必要です。
- 各クラスタで、vSAN または他の共有ストレージ ソリューションを使用してストレージを構成します。
- 完全自動化モードまたは一部自動化モードで vSphere HA と vSphere DRS を有効にします。
- NSX または vSphere Distributed Switch (vDS) ネットワークを使用して、クラスタのネットワークを構成します。

手順

- 1 vSphere Client で、vCenter Server に移動します。
- 2 [構成] を選択し、[vSphere Zones] を選択します。
- 3 [新規 vSphere Zone の追加] をクリックします。
- 4 ゾーンに **zone1** などの名前を付け、オプションで説明を追加します。
- 5 ゾーンに追加する vSphere クラスタを選択し、[終了] をクリックします。
- 6 手順を繰り返して 3 つの vSphere Zones を作成します。

次のステップ

- ■ スーパーバイザー で使用するネットワーク スタックを構成します。4 章 [vSphere IaaS control plane のネットワーク](#) を参照してください
- 作成した 3 つの vSphere Zones でスーパーバイザー を有効にします。『5 章 3 ゾーン スーパーバイザー のデプロイ』を参照してください。

vSphere Zone に変更を加える必要がある場合は、スーパーバイザー をデプロイする前に実行できます。

vSphere Zone の管理

vSphere Zone を変更する必要がある場合は、Zone にスーパーバイザーをデプロイする前に変更を行う必要があります。Zone に関連付けられているクラスタを変更することも、Zone を削除することもできます。vSphere Zone を削除すると、Zone に関連付けられているクラスタが削除され、次に Zone が vCenter Server から削除されます。

vSphere Zone からのクラスタの削除

vSphere Zone からクラスタを削除するには、ゾーンカード上の 3 つのドット (...) をクリックして [クラスタの削除] を選択します。クラスタが Zone から削除され、別のクラスタを追加できるようになります。

注： vSphere Zone ゾーンでスーパーバイザーがすでに有効になっている場合は、その Zone からクラスタを削除することはできません。

vSphere Zone の削除

vSphere Zone を削除するには、ゾーンカード上の 3 つのドット (...) をクリックして [ゾーンの削除] を選択します。

注： vSphere Zone でスーパーバイザーがすでに有効になっている場合は、その Zone を削除することはできません。

vSphere IaaS control plane のネットワーク

4

スーパーバイザーは、vSphere のネットワーク スタックまたは VMware NSX® を使用して、Kubernetes 制御プレーンの仮想マシン、サービス、およびワークロードへの接続を提供できます。Tanzu Kubernetes Grid によってプロビジョニングされた Tanzu Kubernetes クラスタで使用されるネットワークは、vSphere IaaS control plane インフラストラクチャの基盤であるファブリックと、クラスタのポッド、サービス、および入力方向のネットワークを提供するオープンソース ソフトウェアの組み合わせです。

次のトピックを参照してください。

- [スーパーバイザー ネットワーク](#)
- [vSphere IaaS control plane で使用する NSX のインストールと構成](#)
- [NSX と NSX Advanced Load Balancer のインストールと構成](#)
- [NSX Advanced Load Balancer のインストールと構成](#)
- [HAProxy ロード バランサのインストールと構成](#)

スーパーバイザー ネットワーク

vSphere IaaS control plane 環境の場合、スーパーバイザーは vSphere ネットワーク スタックまたは NSX を使用して、スーパーバイザー 制御プレーンの仮想マシン、サービス、およびワークロードへの接続を提供できます。

スーパーバイザーに vSphere ネットワーク スタックが構成されている場合、スーパーバイザーのすべてのホストは、ワークロードとスーパーバイザー 制御プレーン仮想マシンへの接続を提供する Distributed Switch に接続されます。vSphere ネットワーク スタックを使用するスーパーバイザーには、DevOps ユーザーおよび外部サービスへの接続を提供するために vCenter Server 管理ネットワーク上にロード バランサが必要です。

NSX を使用して構成されるスーパーバイザーは、ソリューションのソフトウェアベースのネットワークと NSX Edge ロード バランサまたは NSX Advanced Load Balancer を使用して、外部サービスと DevOps ユーザーへの接続を提供します。環境が次の条件を満たしている場合は、NSX で NSX Advanced Load Balancer を構成できます。

- NSX のバージョンが 4.1.1 以降である。
- NSX Advanced Load Balancer バージョンが 2.1.4 以降で、Enterprise ライセンスがある。
- 構成する NSX Advanced Load Balancer Controller が NSX に登録されている。
- NSX ロード バランサがスーパーバイザーでまだ構成されていない。

VDS を使用した スーパーバイザー ネットワーク

ネットワーク スタックとしての VDS によってバックアップされている スーパーバイザー では、スーパーバイザー をバックアップしている vSphere クラスタのすべてのホストが同じ VDS に接続されている必要があります。スーパーバイザー は、Kubernetes ワークロードおよび制御プレーン トラフィックのワークロード ネットワークとして分散ポート グループを使用します。ワークロード ネットワークを スーパーバイザー 内の名前空間に割り当てます。

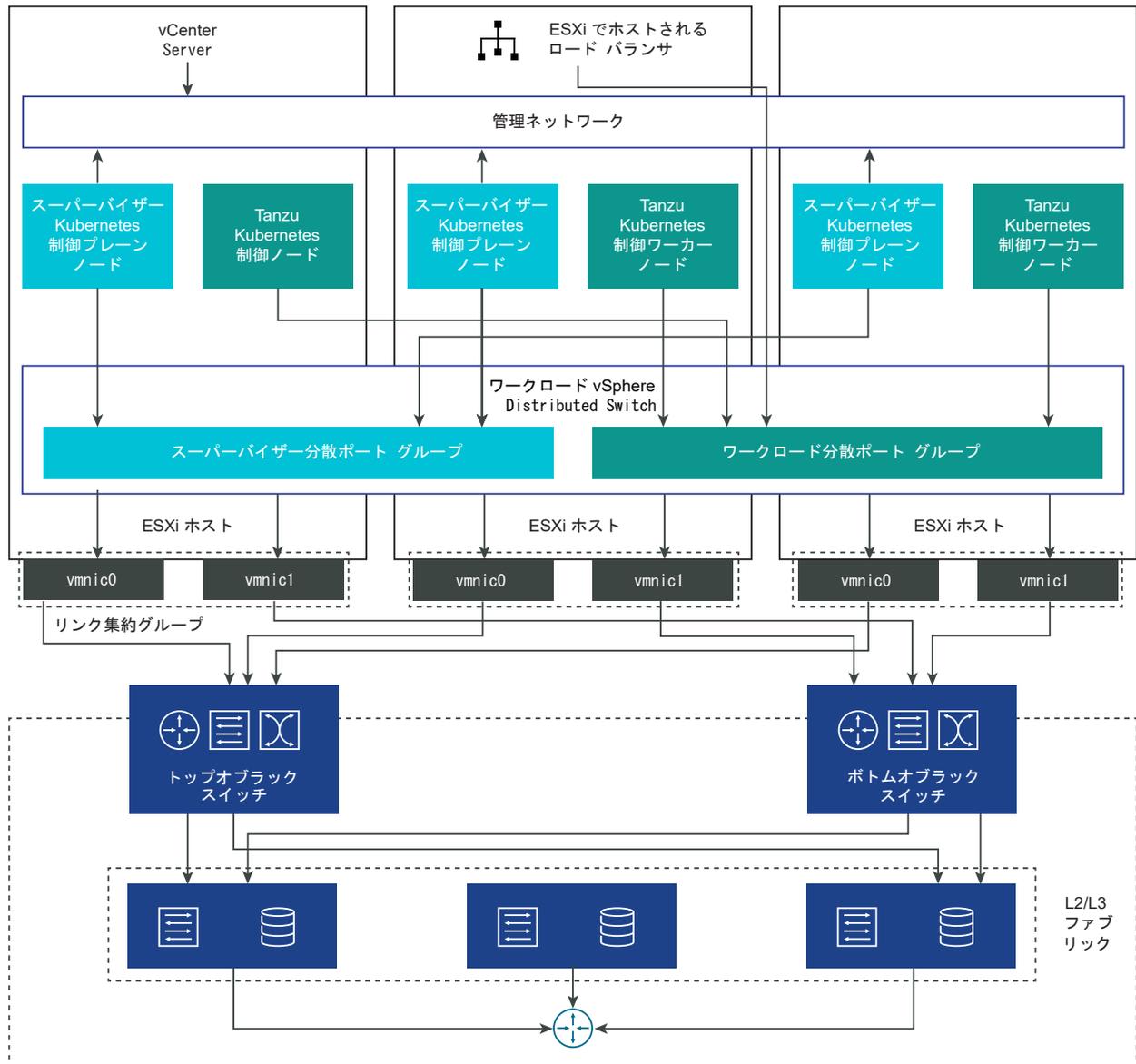
スーパーバイザー に実装するトポロジによっては、1 つ以上の分散ポート グループをワークロード ネットワークとして使用できます。スーパーバイザー 制御プレーン仮想マシンへの接続を提供するネットワークは、プライマリ ワークロード ネットワークと呼ばれます。スーパーバイザー 上のすべての名前空間にこのネットワークを割り当てることも、名前空間ごとに異なるネットワークを使用することもできます。クラスタが配置されている名前空間に割り当てられたワークロード ネットワークに、Tanzu Kubernetes Grid クラスタが接続されます。

VDS によってバックアップされる スーパーバイザー は、DevOps ユーザーと外部サービスへの接続を提供するためにロード バランサを使用します。NSX Advanced Load Balancer または HAProxy ロード バランサを使用できます。

詳細については、[NSX Advanced Load Balancer のインストールと構成](#)および[HAProxy ロード バランサのインストールと構成](#)を参照してください。

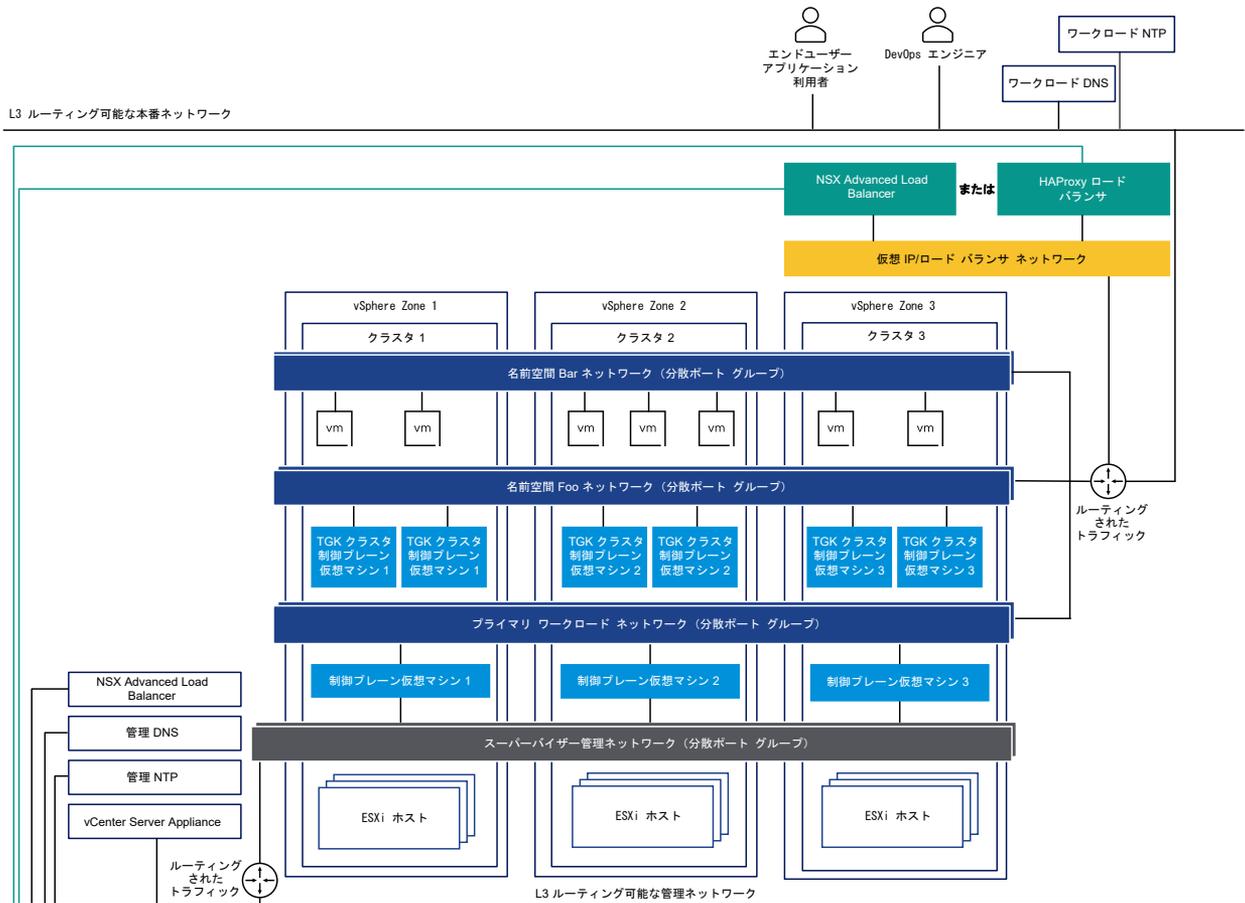
単一クラスタ スーパーバイザー セットアップでは、スーパーバイザー は 1 つの vSphere クラスタのみによってバックアップされます。クラスタのすべてのホストが、VDS に接続されている必要があります。

図 4-1. VDS を使用した単ークラスタ スーパーバイザー ネットワーク



3ゾーンスーパーバイザーでは、スーパーバイザーを3つのvSphereゾーンにデプロイします。それぞれのゾーンは、vSphereクラスタにマッピングされています。これらのvSphereクラスタのすべてのホストは、同じVDSに接続されている必要があります。すべての物理サーバがL2デバイスに接続されている必要があります。名前空間に構成するワークロードネットワークは、3つのvSphereゾーンすべてにまたがります。

図 4-2. VDS を使用した 3 ゾーン スーパーバイザー ネットワーク



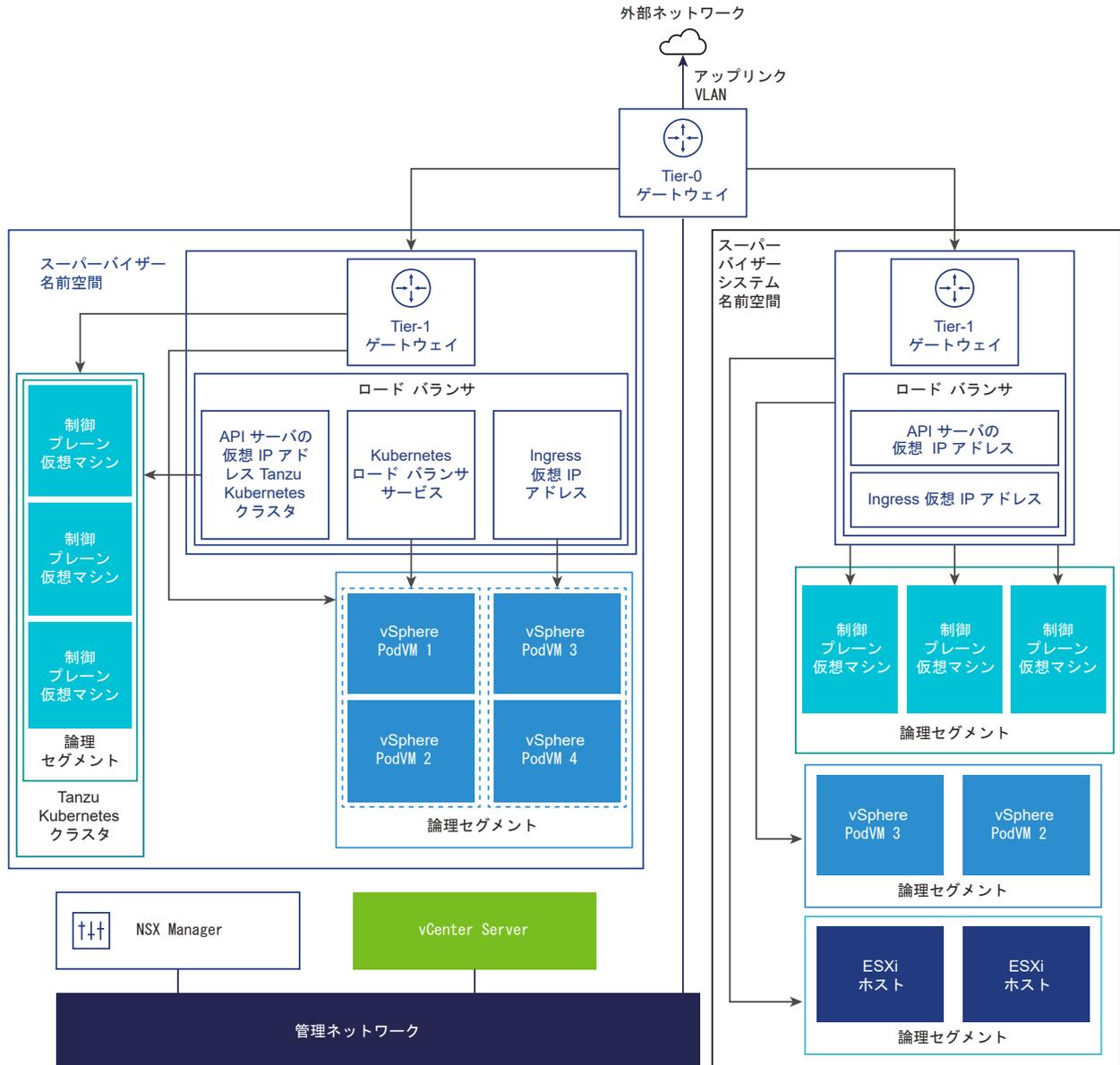
NSX を使用する スーパーバイザー ネットワーク

NSX は、スーパーバイザー 内のオブジェクトおよび外部ネットワークへのネットワーク接続を提供します。クラスターを構成する ESXi ホストへの接続は、標準の vSphere ネットワークによって処理されます。

既存の NSX デプロイを使用するか、NSX の新しいインスタンスをデプロイすることによって、スーパーバイザー ネットワークを手動で構成することもできます。

詳細については、「vSphere IaaS control plane で使用する NSX のインストールと構成」を参照してください。

図 4-3. NSX を使用する スーパーバイザー ネットワーク



- NSX Container Plugin (NCP) は NSX と Kubernetes を統合します。NCP のメイン コンポーネントはコンテナで実行され、NSX Manager および Kubernetes 制御プレーンと通信します。NCP は、コンテナおよびその他のリソースへの変更を監視し、NSX API を呼び出して、コンテナの論理ポート、セグメント、ルーター、セキュリティ グループなどのネットワーク リソースを管理します。

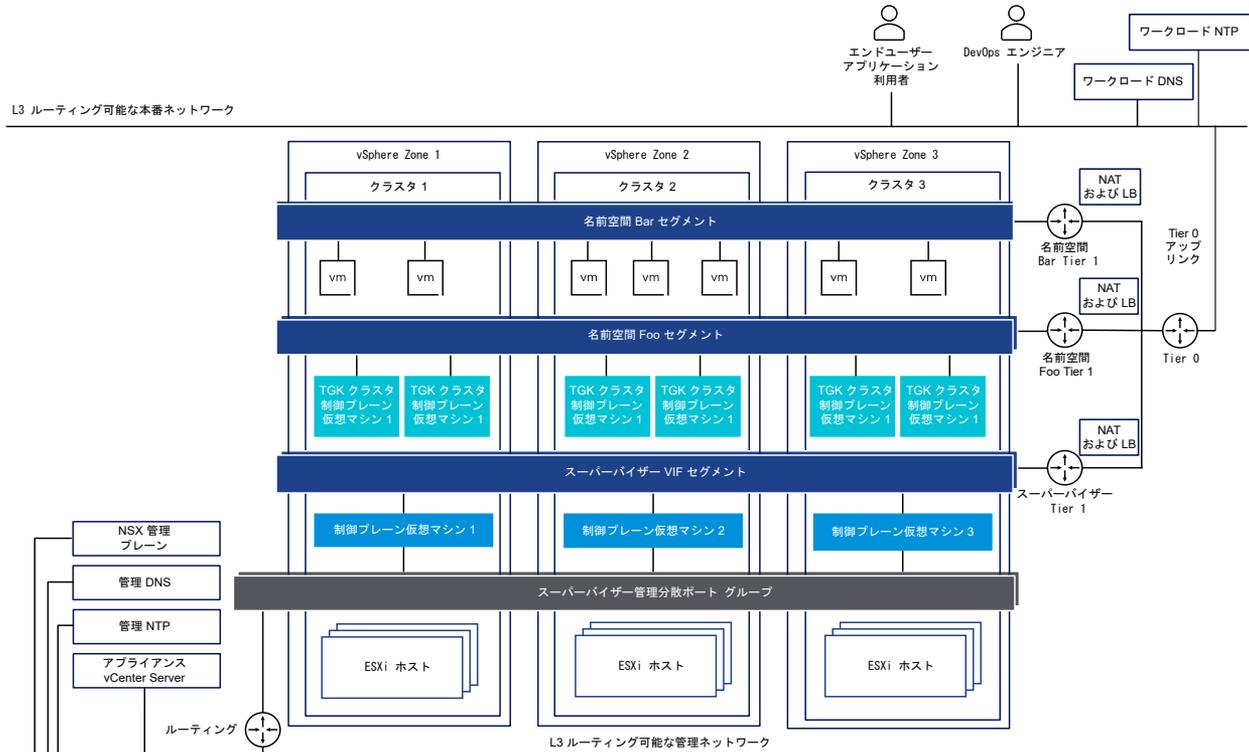
NCP はデフォルトで、システム名前空間用の共有 Tier-1 ゲートウェイを 1 つ作成し、名前空間ごとに Tier-1 ゲートウェイとロード バランサを 1 つずつ作成します。Tier-1 ゲートウェイは、Tier-0 ゲートウェイとデフォルトのセグメントに接続されています。

システム名前空間は、スーパーバイザー クラスタと Tanzu Kubernetes Grid クラスタの機能に不可欠な主要コンポーネントで 사용되는名前空間です。Tier-1 ゲートウェイ、ロード バランサ、SNAT IP を含む共有ネットワーク リソースは、システム名前空間内でグループ化されます。

- NSX Edge は、外部ネットワークから スーパーバイザー オブジェクトへの接続を提供します。NSX Edge クラスタには、スーパーバイザー 制御プレーン仮想マシン上にある Kubernetes API サーバの冗長性を確保するロード バランサや、スーパーバイザー の外部に公開されてアクセスできる必要があるアプリケーションがあります。
- NSX Edge クラスタには Tier-0 ゲートウェイが関連付けられており、外部ネットワークへのルーティングを提供します。アップリンク インターフェイスでは、動的ルーティング プロトコルの BGP またはスタティックルーティングのいずれかが使用されます。
- 各 vSphere 名前空間 には、個別のネットワークのほかに、Tier-1 ゲートウェイ、ロード バランサ サービス、SNAT IP アドレスなど、名前空間内のアプリケーションで共有される一連のネットワーク リソースが含まれています。
- 同じ名前空間内にある vSphere ポッド、通常の仮想マシン、または Tanzu Kubernetes Grid クラスタで実行されるワークロードは、North-South 接続に対して同じ SNAT IP アドレスを共有します。
- vSphere ポッド または Tanzu Kubernetes Grid クラスタで実行されるワークロードには、デフォルトのファイアウォールによって実装される共通の隔離ルールが適用されます。
- Kubernetes 名前空間ごとに個別の SNAT IP アドレスが必要になることはありません。名前空間の間の East-West 接続は、SNAT ではありません。
- 各名前空間のセグメントは、NSX Edge クラスタに関連付けられている、標準モードで機能する VDS に配置されます。このセグメントは、スーパーバイザー にオーバーレイ ネットワークを提供します。
- スーパーバイザー の共有 Tier-1 ゲートウェイ内に、個別のセグメントがあります。各 Tanzu Kubernetes Grid クラスタのセグメントは、名前空間の Tier-1 ゲートウェイ内で定義されています。
- 各 ESXi ホストの Spherelet プロセスは、管理ネットワーク上のインターフェイスを介して vCenter Server と通信します。

ネットワーク スタックとして NSX を使用して構成された 3 ゾーン スーパーバイザー では、ゾーンにマッピングされた 3 つのすべての vSphere クラスタのすべてのホストが、同じ VDS に接続され、同じ NSX オーバーレイ トランスポート ゾーンに参加している必要があります。すべてのホストが同じ L2 物理デバイスに接続されている必要があります。

図 4-4. NSX を使用した 3 ゾーン スーパーバイザー ネットワーク



NSX と NSX Advanced Load Balancer を使用する スーパーバイザー ネットワーク

NSX は、スーパーバイザー 内のオブジェクトおよび外部ネットワークへのネットワーク接続を提供します。NSX を使用して構成される スーパーバイザー では、NSX Edge または NSX Advanced Load Balancer を使用できます。

NSX Advanced Load Balancer のコンポーネントには、NSX Advanced Load Balancer Controller クラスター、サービス エンジン (データ プレーン) 仮想マシン、Avi Kubernetes Operator (AKO) が含まれます。

NSX Advanced Load Balancer Controller は vCenter Server と連携して、Tanzu Kubernetes Grid クラスターのロード バランシングを自動実行します。コントローラは、サービス エンジンのプロビジョニング、サービス エンジン間でのリソースの調整、サービス エンジンのメトリックとログの集計を行います。また、ユーザー操作およびプログラムによる連携のための Web インターフェイス、コマンドライン インターフェイス、および API を提供します。コントローラ仮想マシンをデプロイして構成した後、コントローラ クラスターをデプロイして、HA 用の制御プレーン クラスターを設定できます。

サービス エンジンはデータ プレーン仮想マシンです。サービス エンジンは 1 つ以上の仮想サービスを実行します。サービス エンジンは NSX Advanced Load Balancer Controller によって管理されます。コントローラは、仮想サービスをホストするようにサービス エンジンを提供します。

サービス エンジンには、次の 2 種類のネットワーク インターフェイスがあります。

- 仮想マシンの最初のネットワーク インターフェイス vnic0 は管理ネットワークに接続され、そこから NSX Advanced Load Balancer Controller に接続することができます。

- もう一方のインターフェイス `vnic1 - 8` は、仮想サービスが実行されるワークロード ネットワークに接続されます。

サービス エンジン インターフェイスは、適切な Distributed Switch ポート グループに自動的に接続します。各サービス エンジンは、最大 1,000 個の仮想サービスをサポートできます。

仮想サービスは、Tanzu Kubernetes Grid クラスター ワークロード用のレイヤー 4 およびレイヤー 7 ロード バランシング サービスを提供します。仮想サービスは、1つの仮想 IP アドレスと複数のポートで構成されます。仮想サービスをデプロイすると、コントローラによって ESX サーバが自動的に選択され、サービス エンジンが起動して適切なネットワーク（ポート グループ）に接続します。

最初のサービス エンジンは、最初の仮想サービスが構成された後にのみ作成されます。以降に構成された仮想サービスは、既存のサービス エンジンを使用します。

各仮想サーバは、Tanzu Kubernetes Grid クラスターのロード バランサー タイプの異なる IP アドレスを持つレイヤー 4 ロード バランサーを公開します。各仮想サーバに割り当てられる IP アドレスは、構成時にコントローラに指定する IP アドレス ブロックから選択されます。

Avi Kubernetes Operator (AKO) は Kubernetes リソースを監視し、NSX Advanced Load Balancer Controller と通信して、対応するロード バランシング リソースを要求します。Avi Kubernetes Operator は、有効化プロセスの一環として スーパーバイザー にインストールされます。

詳細については、「[NSX および NSX Advanced Load Balancer のインストールと構成](#)」を参照してください。

図 4-5. NSX と NSX Advanced Load Balancer Controller を使用する スーパーバイザー ネットワーク

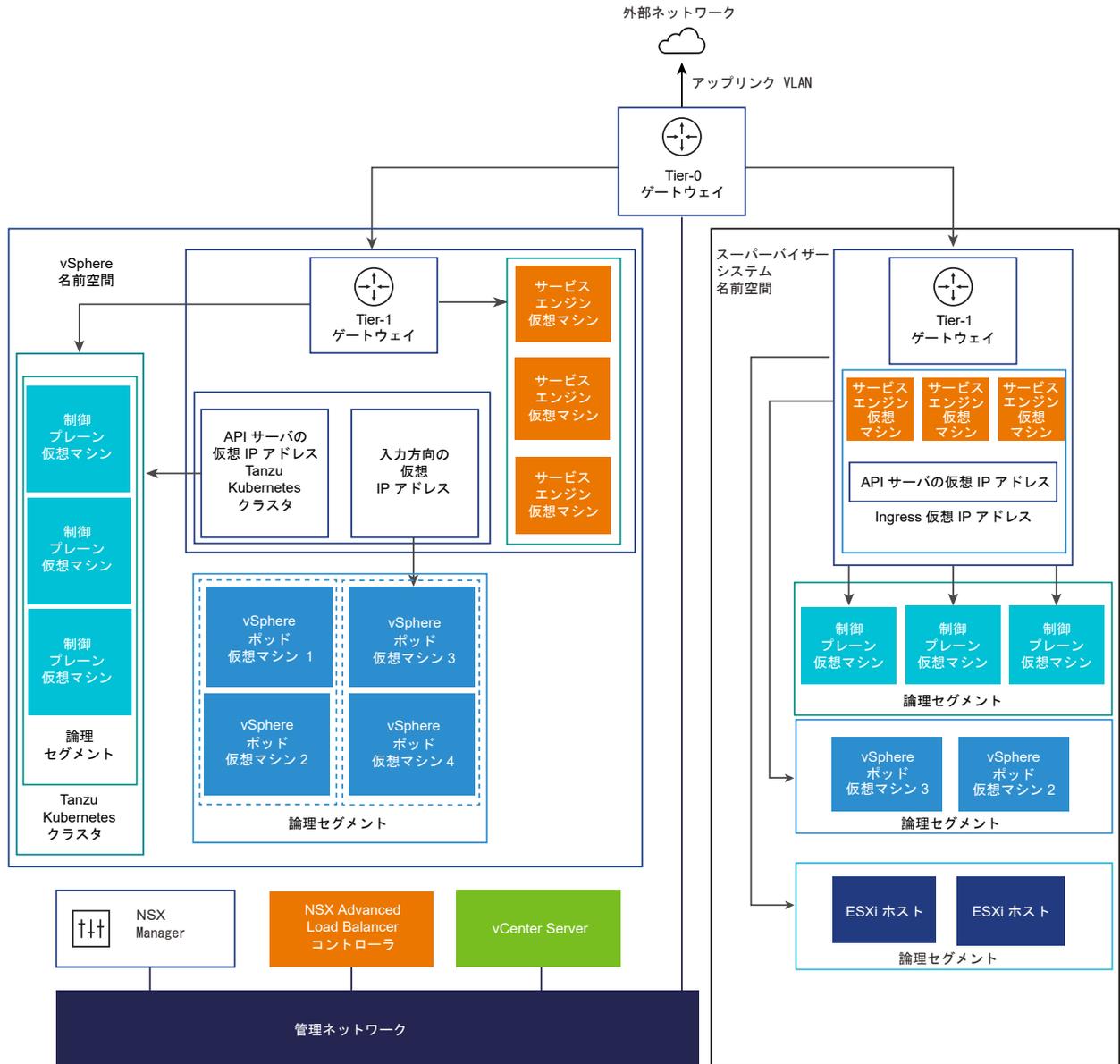
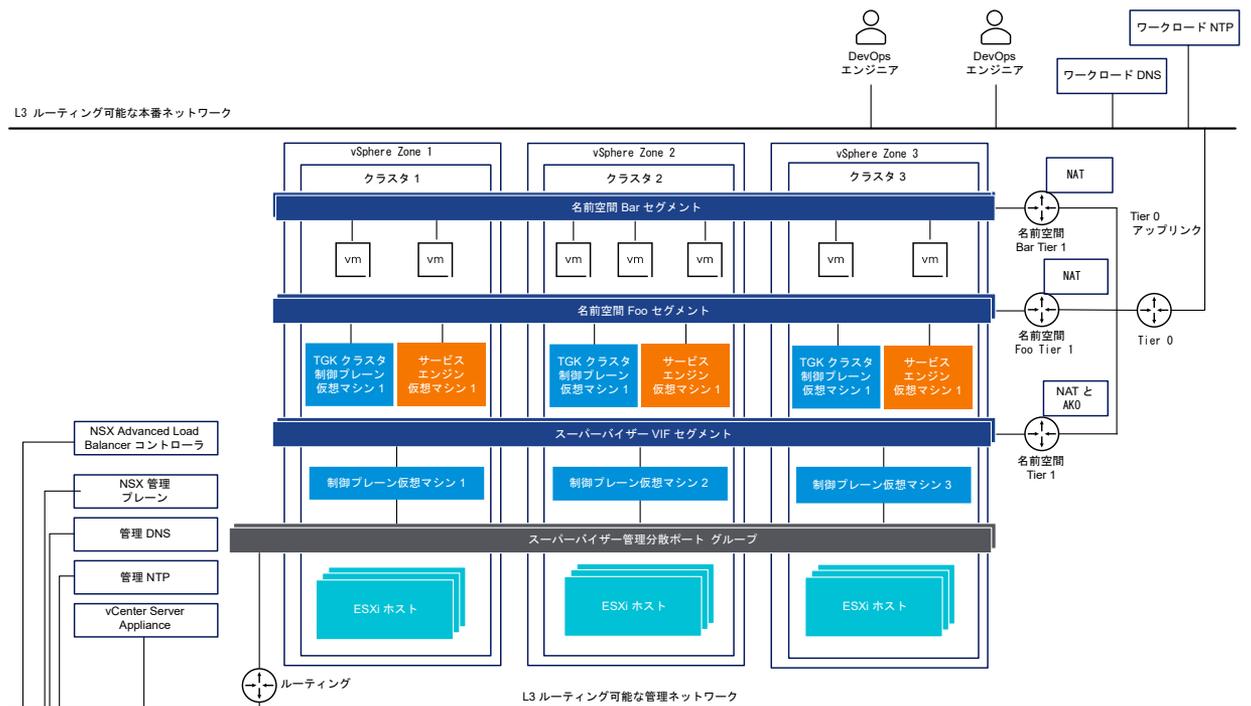


図 4-6. NSX と NSX Advanced Load Balancer Controller を使用した 3 ゾーン スーパーバイザー ネットワーク



重要： NSX のデプロイで NSX Advanced Load Balancer Controller を構成する場合は、次の点を考慮してください。

- vCenter Server 拡張リンク モード デプロイでは NSX Advanced Load Balancer Controller をデプロイできません。単一の vCenter Server のデプロイでのみ NSX Advanced Load Balancer Controller をデプロイできます。複数の vCenter Server がリンクされている場合、NSX Advanced Load Balancer Controller の構成時に使用できるのはそのうちの 1 つのみです。
- 多層の Tier-0 トポロジでは、NSX Advanced Load Balancer Controller を構成できません。NSX 環境が多層の Tier-0 トポロジで設定されている場合、NSX Advanced Load Balancer Controller の構成時に使用できる Tier-0 ゲートウェイは 1 つのみです。

NSX を使用するネットワークの構成方法

スーパーバイザー は、固定型ネットワーク構成を使用します。NSX を使用する スーパーバイザー ネットワークを構成するには次の 2 つの方法があり、いずれの場合でも 1 ゾーン スーパーバイザー 用の同じネットワーク モデルがデプロイされます。

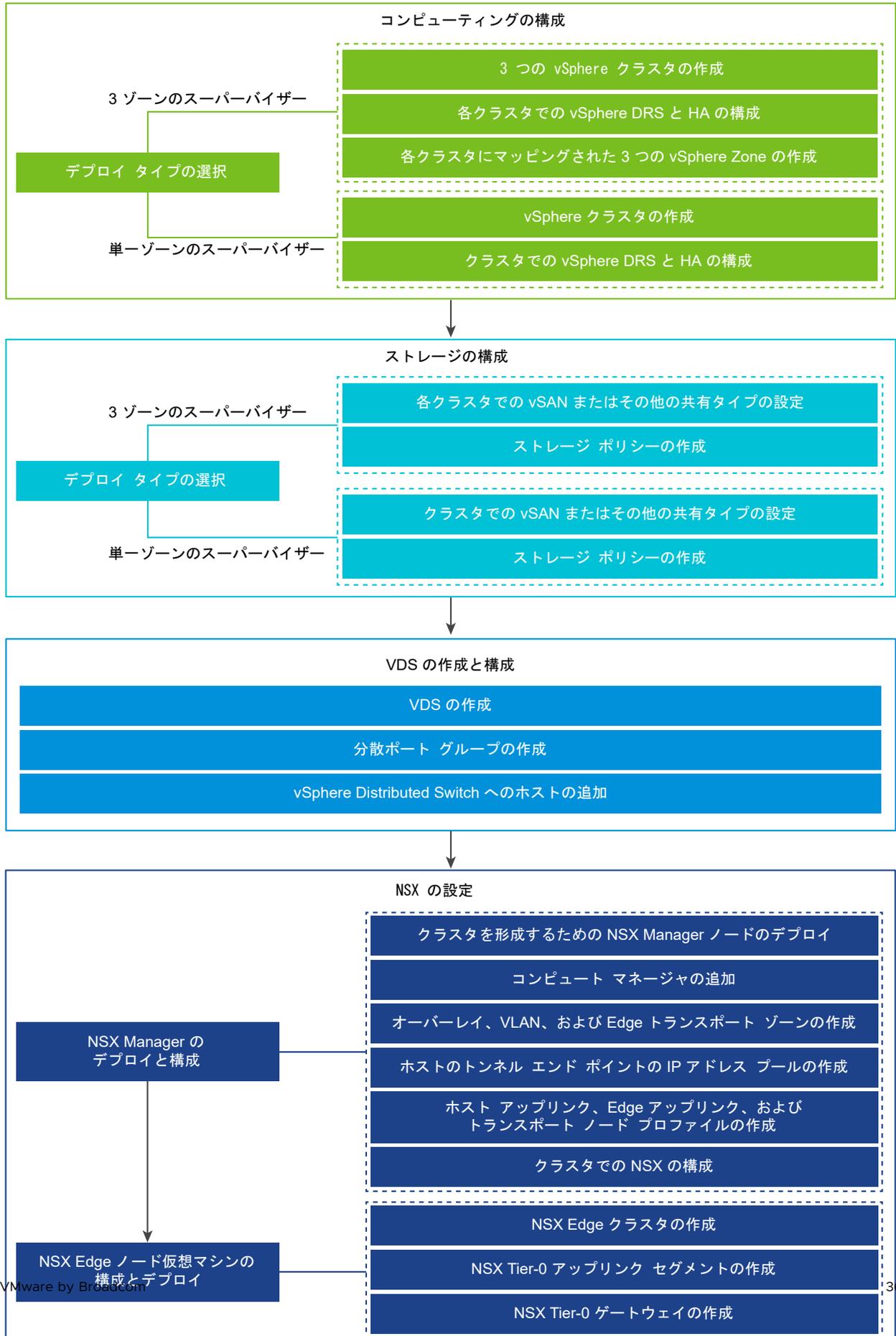
- スーパーバイザー ネットワークを構成する最も簡単な方法は、VMware Cloud Foundation SDDC Manager を使用することです。詳細については、VMware Cloud Foundation SDDC Manager のドキュメントを参照してください。詳細については、『[VMware Cloud Foundation 管理ガイド](#)』を参照してください。

- 既存の NSX デプロイを使用するか、NSX の新しいインスタンスをデプロイすることによって、スーパーバイザー ネットワークを手動で構成することもできます。詳細については、「[vSphere IaaS control plane で使用する NSX のインストールと構成](#)」を参照してください。

vSphere IaaS control plane で使用する NSX のインストールと構成

vSphere IaaS control plane では、スーパーバイザー、vSphere 名前空間、名前空間内で実行されるすべてのオブジェクト（vSphere ポッド、仮想マシン、Tanzu Kubernetes クラスターなど）への接続を有効にするために、特定のネットワーク構成が必要です。vSphere 管理者は、vSphere IaaS control plane で使用する NSX をインストールして構成します。

図 4-7. NSX を使用してスーパーバイザーを構成するためのワークフロー



このセクションでは、新しい NSX インスタンスをデプロイして スーパーバイザー ネットワークを構成する方法について説明しますが、手順は既存の NSX デプロイにも適用できます。また、このセクションでは、スーパーバイザー ワークロード ドメインを設定するときに VMware Cloud Foundation SDDC Manager で行われている処理を理解するための背景も説明します。

前提条件

- 環境が vSphere クラスタを スーパーバイザー として設定するためのシステム要件を満たしていることを確認します。要件の詳細については、『vSphere IaaS 制御プレーンの概念と計画』の「[NSX でのゾーン スーパーバイザーの要件](#)」および「[NSX を使用したクラスタ スーパーバイザーのデプロイの要件](#)」を参照してください。
- Tanzu エディション ライセンスを スーパーバイザー に割り当てます。
- 制御プレーン仮想マシン、ポッドの短期ディスク、コンテナ イメージの配置用のストレージ ポリシーを作成します。
- クラスタの共有ストレージを構成します。vSphere DRS と HA、およびコンテナのパーシステント ボリュームの保存には、共有ストレージが必要です。
- vSphere クラスタで DRS と HA が有効であり、DRS が完全自動化モードに設定されていることを確認します。
- クラスタに関するクラスタ全体の構成の変更権限があることを確認します。

手順

1 vSphere Distributed Switch の作成と構成

スーパーバイザー 内のすべてのホストのネットワーク構成を処理するには、vSphere Distributed Switch を作成し、分散ポート グループを作成してから、ホストをスイッチに関連付けます。

2 NSX Manager のデプロイと構成

vSphere Client を使用して NSX Manager を vSphere クラスタにデプロイし、vSphere IaaS control plane で使用することができます。

3 トランスポート ゾーンの作成

トランスポート ゾーンは、特定のネットワークを使用できるホストおよび仮想マシンを示します。トランスポート ゾーンは、1つ以上のホスト クラスタにまたがることができます。

4 NSX Edge トランスポートノードの設定とデプロイ

NSX Edge 仮想マシン (VM) を NSX ファブリックに追加して、NSX Edge トランスポート ノード仮想マシンとして構成することができます。

vSphere Distributed Switch の作成と構成

スーパーバイザー 内のすべてのホストのネットワーク構成を処理するには、vSphere Distributed Switch を作成し、分散ポート グループを作成してから、ホストをスイッチに関連付けます。

手順

- 1 vSphere Client で、データセンターに移動します。

- 2 ナビゲータでデータセンターを右クリックし、[Distributed Switch] - [新しい Distributed Switch] の順に選択します。
- 3 新しい Distributed Switch の名前を入力します。
例えば、DSwitch です。
- 4 [バージョンの選択] に Distributed Switch のバージョンを入力します。
[8.0] を選択します。
- 5 [設定] にアップリンク ポートの数を入力します。
2 の値を入力します。
- 6 設定内容を確認して、[終了] をクリックします。
- 7 作成した Distributed Switch を右クリックし、[設定] - [設定の編集] の順に選択します。
- 8 [詳細] タブで、MTU (バイト) 値として 1,700 以上の値を入力し、[OK] をクリックします。
オーバーレイ トラフィックを伝送するネットワークでは、MTU サイズを 1,700 以上にする必要があります。
たとえば、9000 です。
NSX では、グローバルのデフォルト MTU 値 1,700 が使用されます。

分散ポート グループの作成

NSX Edge ノードのアップリンク、Edge ノード TEP、管理ネットワーク、および共有ストレージごとに、分散ポートグループを作成します。

デフォルトのポート グループとデフォルトのアップリンクは、vSphere Distributed Switch の作成時に作成されます。管理ポート グループ、vSAN ポート グループ、Edge TEP ポート グループ、および NSX Edge アップリンク ポート グループを作成する必要があります。

前提条件

vSphere Distributed Switch が作成されていることを確認します。

手順

- 1 vSphere Client で、データセンターに移動します。
- 2 ナビゲータで Distributed Switch を右クリックして、[分散ポート グループ] - [新規分散ポート グループ] の順に選択します。
- 3 NSX Edge アップリンクのポート グループを作成します。
例えば、DPortGroup-EDGE-UPLINK です。
- 4 [VLAN タイプ] を VLAN トランクに設定します。
- 5 デフォルトの VLAN トランク範囲 [(0-4094)] を適用します。
- 6 [次へ] をクリックして [終了] をクリックします。
- 7 Distributed Switch を右クリックして、[アクション] メニューから [分散ポート グループ] - [分散ポート グループの管理] の順に選択します。

- 8 [チーミングおよびフェイルオーバー] を選択して、[次へ] をクリックします。
- 9 アクティブ アップリンクとスタンバイ アップリンクを構成します。
例えば、アクティブ アップリンクは Uplink1、スタンバイ アップリンクは Uplink2 です。
- 10 [OK] をクリックして、ポート グループの構成を完了します。
- 11 2 ~ 10 の手順を繰り返して、Edge ノード TEP、管理ネットワーク、および共有ストレージのポート グループを作成します。
たとえば、次のポート グループを作成します。

ポート グループ	名前	VLAN タイプ
Edge ノード TEP	DPortGroup-EDGE-TEP	[VLAN タイプ] を VLAN トランクに設定します。 アクティブ アップリンクを Uplink2、スタンバイ アップリンクを Uplink1 と設定します。 注： Edge ノード TEP に使用される VLAN は、ESXi TEP に使用される VLAN とは異なる必要があります。
マネージメント ツール	DPortGroup-MGMT	[VLAN タイプ] を [VLAN] に設定し、管理ネットワークの VLAN ID を入力します。たとえば、1060 です。
共有ストレージまたは vSAN	DPortGroup-VSAN	[VLAN タイプ] を [VLAN] に設定し、VLAN ID を入力します。たとえば、3082 です。

- 12 次のコンポーネントのポート グループを作成します。
 - [vSphere vMotion]。このポート グループは、スーパーバイザー を更新する場合に必要です。vMotion のデフォルト ポート グループを構成します。
 - [仮想マシンのトラフィック]。仮想マシンのトラフィックを処理するようにデフォルトのポート グループを構成します。

vSphere Distributed Switch へのホストの追加

vSphere Distributed Switch を使用して環境のネットワークを管理するには、スーパーバイザー に属するホストをスイッチに関連付ける必要があります。Distributed Switch にホストの物理 NIC、VMkernel アダプタ、および仮想マシン ネットワーク アダプタを接続してください。

前提条件

- スイッチに接続する物理 NIC に割り当てるための十分なアップリンクが Distributed Switch で使用可能であることを確認します。
- Distributed Switch で使用できる分散ポート グループが 1 つ以上あることを確認します。
- 分散ポート グループのチーミングおよびフェイルオーバー ポリシーで、アクティブなアップリンクが構成されていることを確認します。

手順

- 1 vSphere Client で、[ネットワーク] を選択して Distributed Switch に移動します。
- 2 [アクション] メニューから、[ホストの追加と管理] を選択します。
- 3 [タスクを選択] 画面で、[ホストの追加] を選択し、[次へ] をクリックします。
- 4 [ホストの選択] 画面で、[新規ホスト] をクリックし、データセンター内のホストを選択して [OK] をクリックします。次に [次へ] をクリックします。
- 5 [物理アダプタの管理] 画面で、Distributed Switch の物理 NIC を構成します。
 - a [他のスイッチ上/未要求] リストから、物理 NIC を選択します。

他のスイッチにすでに接続されている物理 NIC を選択した場合、その物理 NIC は現在の Distributed Switch に移行されます。
 - b [アップリンクの割り当て] をクリックします。
 - c アップリンクを選択します。
 - d このアップリンクをクラスタ内のすべてのホストに割り当てるには、[このアップリンクの割り当てを残りのホストに適用します] を選択します。
 - e [OK] をクリックします。

たとえば、Uplink 1 を vmnic0 に割り当て、Uplink 2 を vmnic1 に割り当てます。
- 6 [次へ] をクリックします。
- 7 [VMkernel アダプタの管理] 画面で、VMkernel アダプタを構成します。
 - a VMkernel アダプタを選択し、[ポート グループの割り当て] をクリックします。
 - b 分散ポート グループを選択します。

たとえば、[DPortGroup] です。
 - c このポート グループをクラスタ内のすべてのホストに適用するには、[このポート グループの割り当てを残りのホストに適用します] を選択します。
 - d [OK] をクリックします。
- 8 [次へ] をクリックします。
- 9 (オプション) [仮想マシン ネットワークの移行] 画面で [仮想マシン ネットワークの移行] チェック ボックスをオンにして、仮想マシン ネットワークを構成します。
 - a 仮想マシンのすべてのネットワーク アダプタを分散ポート グループに接続するには、仮想マシンを選択するか、個々のネットワーク アダプタを選択して、そのアダプタのみに接続します。
 - b [ポート グループの割り当て] をクリックします。
 - c リストから分散ポート グループを選択し、[OK] をクリックします。
 - d [次へ] をクリックします。

次のステップ

NSX Manager をデプロイし、構成します。[NSX Manager のデプロイと構成](#)を参照してください。

NSX Manager のデプロイと構成

vSphere Client を使用して NSX Manager を vSphere クラスタにデプロイし、vSphere IaaS control plane で使用することができます。

OVA ファイルを使用して NSX Manager をデプロイするには、この手順を実行します。

ユーザー インターフェイスまたは CLI を使用した NSX Manager のデプロイの詳細については、『NSX インストール ガイド』を参照してください。

前提条件

- 環境がネットワークの要件を満たしていることを確認します。要件の詳細については、『vSphere IaaS 制御プレーンの概念と計画』の [Requirements for a Three-Zone Supervisor with NSX Advanced Load Balancer](#) および [Requirements for Enabling a Single Cluster Supervisor with NSX Advanced Load Balancer](#) を参照してください。
- 必要なポートが開いていることを確認します。ポートとプロトコルの詳細については、『NSX インストール ガイド』を参照してください。

手順

- 1 VMware ダウンロード ポータルで NSX OVA ファイルを見つけます。
ダウンロード URL をコピーするか、OVA ファイルをダウンロードします。
- 2 右クリックして [OVF テンプレートのデプロイ] を選択し、インストール ウィザードを開始します。
- 3 [OVF テンプレートの選択] タブで、OVA のダウンロード URL を入力するか、OVA ファイルに移動します。
- 4 [名前とフォルダの選択] タブで、NSX Manager 仮想マシン (VM) の名前を入力します。
- 5 [コンピューティング リソースの選択] タブで、NSX Manager をデプロイする vSphere クラスタを選択します。
- 6 [次へ] をクリックして、詳細を確認します。
- 7 [構成] タブで、NSX のデプロイ サイズを選択します。
推奨される最小デプロイ サイズは [中] です。
- 8 [ストレージの選択] タブで、デプロイ用の共有ストレージを選択します。
- 9 [仮想ディスク フォーマットの選択] で [シン プロビジョニング] を選択して、シン プロビジョニングを有効にします。
デフォルトでは、仮想ディスクはシック プロビジョニングされます。
- 10 [ネットワークの選択] タブの [ターゲット ネットワーク] で、NSX Manager の管理ポート グループまたはターゲット ネットワークを選択します。
たとえば、DPortGroup-MGMT です。

- 11 [テンプレートのカスタマイズ] タブで、NSX Manager のシステム root、CLI 管理者、および監査パスワードを入力します。パスワードの強度の制限に従ってパスワードを入力する必要があります。
 - 12 文字以上。
 - 小文字が 1 文字以上。
 - 大文字が 1 文字以上。
 - 数字が 1 文字以上。
 - 特殊文字が 1 文字以上。
 - 異なる文字が 5 文字以上。
 - デフォルトのパスワードの複雑性ルールが Linux PAM モジュールによって適用されます。
- 12 デフォルトの IPv4 ゲートウェイ、管理ネットワークの IPv4、管理ネットワークのネットマスク、DNS サーバ、ドメイン検索リスト、および NTP IP アドレスを入力します。
- 13 SSH を有効にして、NSX Manager コマンドラインに root による SSH ログインを許可します。
デフォルトでは、SSH オプションはセキュリティ上の理由から無効になっています。
- 14 カスタム OVF テンプレートの仕様が正確であることを確認し、[終了] をクリックしてインストールを開始します。
- 15 NSX Manager が起動したら、admin として CLI にログインし、`get interface eth0` コマンドを実行して、IP アドレスが想定どおりに適用されていることを確認します。
- 16 `get services` コマンドを入力して、すべてのサービスが実行されていることを確認します。

NSX Manager ノードのデプロイによるクラスタの形成

NSX Manager クラスタは高可用性を提供します。vCenter Server によって管理されている ESXi ホストにのみ、ユーザー インターフェイスを使用して NSX Manager ノードをデプロイできます。NSX Manager クラスタを作成するには、2 台の追加ノードをデプロイして、合計 3 台のノードによるクラスタを形成します。ユーザー インターフェイスから新しいノードをデプロイすると、そのノードは最初にデプロイされたノードに接続してクラスタを形成します。最初にデプロイされたノードのリポジトリのすべての詳細とパスワードは、新しくデプロイされたノードと同期されます。

前提条件

- NSX Manager ノードがインストールされていることを確認します。
- コンピュート マネージャが構成されていることを確認します。
- 必要なポートが開いていることを確認します。
- ESXi ホストにデータストアが構成されていることを確認します。
- IP アドレスとゲートウェイ、DNS サーバの IP アドレス、ドメイン検索リスト、および NTP サーバの IP アドレスが、NSX Manager で使用できるようになっていることを確認します。
- ターゲット仮想マシンのポート グループ ネットワークがあることを確認します。管理仮想マシン ネットワークに NSX アプライアンスを配置します。

手順

- 1 ブラウザから管理者権限で <https://<manager-ip-address>> の NSX Manager にログインします。
- 2 アプライアンスをデプロイするために、[システム] - [アプライアンス] - [NSX アプライアンスの追加] の順に選択します。
- 3 アプライアンスの詳細を入力します。

オプション	説明
ホスト名	ノードに使用するホスト名または FQDN を入力します。
管理 IP アドレス/ネットマスク	ノードに割り当てる IP アドレスを入力します。
管理ゲートウェイ	ノードで使用するゲートウェイ IP アドレスを入力します。
DNS サーバ	ノードで使用する DNS サーバの IP アドレスのリストを入力します。
NTP サーバ	NTP サーバの IP アドレスのリストを入力します。
ノード サイズ	オプションから [中 (6 個の vCPU、24 GB の RAM、300 GB のストレージ)] のフォームファクタを選択します。

- 4 アプライアンスの構成の詳細を入力します。

オプション	説明
コンピューター マネージャ	コンピューター マネージャとして構成した vCenter Server を選択します。
コンピューティング クラスター	ノードが参加するクラスターを選択します。
データストア	ノードのファイル用のデータストアを選択します。
仮想ディスクのフォーマット	[シン プロビジョニング] フォーマットを選択します。
ネットワーク	[ネットワークの選択] をクリックして、ノードの管理ネットワークを選択します。

- 5 アクセスと認証情報の詳細を入力します。

オプション	説明
SSH の有効化	ボタンを切り替えて、新しいノードへの SSH ログインを許可します。
root アクセスの有効化	ボタンを切り替えて、新しいノードへの root アクセスを許可します。

オプション	説明
システムの root 認証情報	<p>新しいノードの root パスワードを設定して確認します。</p> <p>パスワードの強度の制限に従ってパスワードを入力する必要があります。</p> <ul style="list-style-type: none"> ■ 12 文字以上。 ■ 小文字が 1 文字以上。 ■ 大文字が 1 文字以上。 ■ 数字が 1 文字以上。 ■ 特殊文字が 1 文字以上。 ■ 異なる文字が 5 文字以上。 ■ デフォルトのパスワードの複雑性ルールが Linux PAM モジュールによって適用されません。
管理者 CLI 認証情報と監査 CLI 認証情報	<p>root に設定したものと同一パスワードを使用する場合は、[root パスワードと同じ] チェックボックスをオンにします。または、チェックボックスをオフにして、別のパスワードを設定します。</p>

6 [アプライアンスのインストール] をクリックします。

新しいノードがデプロイされます。デプロイ プロセスは [システム] - [アプライアンス] 画面で追跡できます。インストールが完了してクラスタが安定するまでは、ノードを追加しないでください。

7 デプロイ、クラスタの形成、およびリポジトリの同期が完了するまで待機します。

ノードの参加とクラスタの安定化には、10 ~ 15 分程度かかる場合があります。クラスタに他の変更を加える前に、すべてのクラスタ サービス グループの状態が接続中であることを確認します。

8 ノードが起動したら、管理者として CLI にログインし、`get interface eth0` コマンドを実行して、IP アドレスが想定どおりに適用されていることを確認します。

9 クラスタのノードが 2 台のみの場合は、別のアプライアンスを追加します。[システム] - [アプライアンス] - [NSX アプライアンスの追加] の順に選択して、構成手順を繰り返します。

ライセンスの追加

NSX Manager を使用してライセンスを追加します。

前提条件

NSXAdvanced 以上のライセンスを取得します。

手順

- 1 NSX Manager にログインします。
- 2 [システム] - [ライセンス] - [追加] の順に選択します。
- 3 ライセンス キーを入力します。
- 4 [追加] をクリックします。

コンピュート マネージャの追加

コンピュート マネージャは、ホストや仮想マシンなどのリソースを管理するアプリケーションです。NSX に関連付けられている vCenter Server を NSX Manager のコンピュート マネージャとして構成します。

詳細については、『NSX 管理ガイド』を参照してください。

手順

- 1 NSX Manager にログインします。
- 2 [システム] - [ファブリック] - [コンピュート マネージャ] - [追加] の順に選択します。
- 3 コンピュート マネージャの詳細を入力します。

オプション	説明
名前と説明	vCenter Server の名前および説明を入力します。
タイプ	デフォルトのタイプは VMware vCenter です。
マルチ NSX	このオプションは選択解除したままにします。 マルチ NSX オプションを使用すると、同じ vCenter Server を複数の NSX Manager に登録できます。このオプションは、スーパーバイザー および vSphere Lifecycle Manager クラスタではサポートされません。
FQDN または IP アドレス	vCenter Server の FQDN または IP アドレスを入力します。
リバース プロキシの HTTPS ポート	デフォルトのポートは 443 です。別のポートを使用する場合は、すべての NSX Manager アプライアンスでポートが開いていることを確認します。 リバース プロキシ ポートを設定して、NSX にコンピュート マネージャを登録します。
ユーザー名とパスワード	vCenter Server のログイン認証情報を入力します。
SHA-256 サムプリント	vCenter Server SHA-256 サムプリント アルゴリズムの値を入力します。

その他の設定はデフォルトのままにかまいません。

サムプリント値を空白にすると、サーバのサムプリントを使用するように指示されます。サムプリントを受け入れてから NSX が vCenter Server リソースを検出して登録するまで、数秒かかります。

- 4 [信頼の有効化] を選択して、vCenter Server が NSX と通信できるようにします。
- 5 NSX Manager のサムプリント値を指定しなかった場合、システムはサムプリントを識別して表示します。
- 6 [追加] をクリックして、サムプリントを受け入れます。

結果

しばらくすると、コンピュート マネージャが vCenter Server に登録され、接続ステータスが 接続中に変わります。vCenter Server の FQDN または PNID が変更された場合は、NSX Manager に再登録する必要があります。詳細については、『NSX Manager による vCenter Server の登録』を参照してください。

注: vCenter Server が正常に登録されたら、コンピュート マネージャを削除する前に NSX Manager 仮想マシンをパワーオフして削除しないでください。そのようにすると、新しい NSX Manager をデプロイするときに、同じ vCenter Server を再度登録することができなくなります。vCenter Server がすでに別の NSX Manager に登録されていることを示すエラーが表示されます。

コンピュート マネージャ名をクリックすると、詳細の表示、コンピュート マネージャの編集、またはコンピュート マネージャに適用されるタグの管理を行うことができます。

トランスポート ゾーン の作成

トランスポート ゾーンは、特定のネットワークを使用できるホストおよび仮想マシンを示します。トランスポート ゾーンは、1つ以上のホスト クラスタにまたがることができます。

vSphere 管理者は、デフォルトのトランスポート ゾーンを使用するか、次のトランスポート ゾーンを作成します。

- スーパーバイザー 制御プレーンの仮想マシンによって使用されるオーバーレイ トランスポート ゾーン。
- 物理ネットワークへのアップリンクに使用する NSX Edge ノードの VLAN トランスポート ゾーン。

手順

- 1 NSX Manager にログインします。
- 2 [システム] - [ファブリック] - [トランスポート ゾーン] - [追加] の順に選択します。
- 3 トランスポート ゾーンの名前と、必要に応じて説明を入力します。
- 4 トラフィック タイプを選択します。

[オーバーレイ] または [VLAN] を選択できます。

デフォルトでは、次のトランスポート ゾーンがあります。

- 名前が `nsx-vlan-transportzone` の VLAN トランスポート ゾーン。
- 名前が `nsx-overlay-transportzone` のオーバーレイ トランスポート ゾーン。

- 5 (オプション) 1つ以上のアップリンク チーミング ポリシー名を入力します。

トランスポート ゾーンに接続されたセグメントは、これらの名前付きチーミング ポリシーを使用します。一致する名前付きチーミング ポリシーをセグメントが見つけれられない場合は、デフォルトのアップリンク チーミング ポリシーが使用されます。

結果

[トランスポート ゾーン] 画面に新しいトランスポート ゾーンが表示されます。

ホストのトンネル エンドポイント IP アドレス用の IP アドレス プールの作成

ESXi ホストのトンネル エンドポイント (TEP) の IP アドレス プールを作成します。TEP は、オーバーレイ フレームの NSX のカプセル化を開始および終了する ESXi ホストを識別するために、外部 IP ヘッダーで使用されるソース IP アドレスとターゲット IP アドレスです。TEP の IP アドレスには、DHCP を使用するか、手動で設定した IP アドレス プールを使用できます。

手順

- 1 NSX Manager にログインします。
- 2 [ネットワーク] - [IP アドレス プール] - [IP アドレス プールの追加] の順に選択します。

3 次の IP アドレス プールの詳細を入力します。

オプション	説明
名前と説明	IP アドレス プール名と、必要に応じて説明を入力します。 例えば、ESXI-TEP-IP-POOL です。
IP アドレス範囲	IP アドレスの割り当ての範囲を入力します。 たとえば、192.23.213.158 - 192.23.213.160。
ゲートウェイ	ゲートウェイ IP アドレス を入力します。 たとえば、192.23.213.253 です。
CIDR	ネットワーク アドレスを CIDR 表記で入力します。 たとえば、192.23.213.0/24 です。

4 [追加] および [適用] クリックします。

結果

作成した TEP の IP アドレス プールが [IP アドレス プール] 画面に表示されていることを確認します。

Edge ノード用の IP アドレス プールの作成

Edge ノード用の IP アドレス プールを作成します。TEP アドレスはルーティング可能である必要はありません。Edge TEP がホスト TEP と通信できる任意の IP アドレス指定スキームを使用できます。

手順

- 1 NSX Manager にログインします。
- 2 [ネットワーク] - [IP アドレス プール] - [IP アドレス プールの追加] の順に選択します。
- 3 次の IP アドレス プールの詳細を入力します。

オプション	説明
名前と説明	IP アドレス プール名と、必要に応じて説明を入力します。 例えば、EDGE-TEP-IP-POOL です。
IP アドレス範囲	IP アドレスの割り当ての範囲を入力します。 たとえば、192.23.213.1 - 192.23.213.10。。
ゲートウェイ	ゲートウェイ IP アドレス を入力します。 たとえば、192.23.213.253 です。
CIDR	ネットワーク アドレスを CIDR 表記で入力します。 たとえば、192.23.213.0/24 です。

4 [追加] および [適用] クリックします。

結果

作成した IP アドレス プールが [IP アドレス プール] 画面に表示されていることを確認します。

ホスト アップリンク プロファイルの作成

ホスト アップリンク プロファイルは、ESXi ホストから NSX セグメントへのアップリンクのポリシーを定義します。

手順

- 1 NSX Manager にログインします。
- 2 [システム] - [ファブリック] - [プロファイル] - [アップリンク プロファイル] - [追加] の順に選択します。
- 3 アップリンク プロファイルの名前と、オプションでアップリンク プロファイルの説明を入力します。
例えば、ESXI-UPLINK-PROFILE です。
- 4 [チーミング] セクションで、[追加] をクリックして名前付けチーミング ポリシーを追加し、[フェイルオーバーの順序] ポリシーを構成します。
アクティブ アップリンクのリストが指定され、トランスポート ノードの各インターフェイスが1つのアクティブ アップリンクに固定されます。この設定により、複数のアクティブ アップリンクを同時に使用できます。
- 5 アクティブ アップリンクとスタンバイ アップリンクを構成します。
たとえば、uplink-1 をアクティブ アップリンクとして、uplink-2 をスタンバイ アップリンクとして構成します。
- 6 トランスポート VLAN の値を入力します。
アップリンク プロファイルで設定されたトランスポート VLAN がオーバーレイ トラフィックをタグ付けし、VLAN ID はトンネル エンドポイント (TEP) によって使用されます。
たとえば、1060 です。
- 7 MTU 値を入力します。
アップリンク プロファイル MTU のデフォルト値は1,600 です。

注： 値は1,600 以上にする必要がありますが、物理スイッチと vSphere Distributed Switch の MTU 値よりも大きくすることはできません。

Edge アップリンク プロファイルの作成

アップリンク プロファイルを作成し、フェイルオーバーの順序チーミング ポリシーを追加して、Edge 仮想マシンのオーバーレイ トラフィックに対して1つのアップリンクが使用されるようにします。

手順

- 1 NSX Manager にログインします。
- 2 [システム] - [ファブリック] - [プロファイル] - [アップリンク プロファイル] - [追加] の順に選択します。
- 3 アップリンク プロファイルの名前を入力し、オプションでアップリンク プロファイルの説明を追加します。
例えば、EDGE-UPLINK-PROFILE です。

- 4 [チーミング] セクションで、[追加] をクリックして名前付けチーミング ポリシーを追加し、[フェイルオーバー] ポリシーを構成します。

アクティブ アップリンクのリストが表示され、トランスポート ノードの各インターフェイスが1つのアクティブ アップリンクに固定されます。この設定により、複数のアクティブ アップリンクを同時に使用できます。

- 5 アクティブ アップリンクを構成します。

たとえば、uplink-1 をアクティブ アップリンクとして構成します。

- 6 アップリンクを [アップリンク プロファイル] 画面で確認します。

トランスポート ノード プロファイルの作成

トランスポート ノード プロファイルは、プロファイルが添付されている特定のクラスタ内のホストに NSX をどのようにインストールして構成するかを定義します。

前提条件

オーバーレイ トランスポート ゾーンを作成してあることを確認します。

手順

- 1 NSX Manager にログインします。
- 2 [システム] - [ファブリック] - [プロファイル] - [トランスポート ノード プロファイル] - [追加] の順に選択します。
- 3 トランスポート ノード プロファイルの名前と、必要に応じて説明を入力します。
例えば、HOST-TRANSPORT-NODE-PROFILE です。
- 4 [新しいノード スイッチ] セクションで、[タイプ] として VDS を選択します。
- 5 [モード] として Standard を選択します。
- 6 リストから vCenter Server と Distributed Switch の名前を選択します。
たとえば、DSwitch。
- 7 以前に作成したオーバーレイ トランスポート ゾーンを選択します。
例えば、NSX-OVERLAY-TRANSPORTZONE です。
- 8 以前に作成したホスト アップリンク プロファイルを選択します。
例えば、ESXI-UPLINK-PROFILE です。
- 9 [IP アドレスの割り当て] リストから [IP アドレス プールを使用] を選択します。
- 10 以前に作成したホスト TEP プールを選択します。
例えば、ESXI-TEP-IP-POOL です。

- 11 [チーミング ポリシー スイッチ マッピング] で編集アイコンをクリックし、NSX アップリンク プロファイルで定義されているアップリンクを vSphere Distributed Switch アップリンクにマッピングします。

たとえば、uplink-1 (active) を Uplink 1 にマッピングし、uplink-2 (standby) を Uplink 2 にマッピングします。

- 12 [追加] をクリックします。

- 13 作成したプロファイルが [トランスポート ノード プロファイル] 画面に一覧表示されていることを確認します。

クラスタ上の NSX の構成

NSX をインストールしてオーバーレイ TEP を準備するには、トランスポート ノード プロファイルを vSphere クラスタに適用します。

前提条件

トランスポート ノード プロファイルが作成されていることを確認します。

手順

- 1 NSX Manager にログインします。

- 2 [システム] - [ファブリック] - [ノード] - [ホスト トランスポート ノード] の順に選択します。

- 3 [管理元] ドロップダウン メニューから、既存の vCenter Server を選択します。

画面には、使用可能な vSphere クラスタが一覧表示されます。

- 4 NSX を構成するコンピューティング クラスタを選択します。

- 5 [NSX の構成] をクリックします。

- 6 以前に作成したトランスポート ノード プロファイルを選択し、[適用] をクリックします。

例えば、HOST-TRANSPORT-NODE-PROFILE です。

- 7 [ホスト トランスポート ノード] 画面で、NSX の構成状態が Success であること、およびクラスタ内にあるホストの NSX Manager の接続ステータスが Up であることを確認します。

結果

NSX のインストールとオーバーレイ TEP の準備のために、以前に作成したトランスポート ノード プロファイルが vSphere クラスタに適用されます。

NSX Edge トランスポートノードの設定とデプロイ

NSX Edge 仮想マシン (VM) を NSX ファブリックに追加して、NSX Edge トランスポート ノード仮想マシンとして構成することができます。

前提条件

トランスポート ゾーン、Edge アップリンク プロファイル、Edge TEP IP アドレス プールを作成済みであることを確認します。

手順

- 1 NSX Manager にログインします。
- 2 [システム] - [ファブリック] - [ノード] - [Edge トラnsポート ノード] - [Edge 仮想マシンの追加] の順に選択します。
- 3 [名前と説明] に NSX Edge の名前を入力します。
たとえば、nsx-edge-1。
- 4 vCenter Server のホスト名または FQDN を入力します。
たとえば、nsx-edge-1.lab.com です。
- 5 Large フォーム ファクタを選択します。
- 6 [認証情報] に NSX Edge の CLI および root パスワードを入力します。パスワードの強度の制限に従ってパスワードを入力する必要があります。
 - 12 文字以上。
 - 小文字が 1 文字以上。
 - 大文字が 1 文字以上。
 - 数字が 1 文字以上。
 - 特殊文字が 1 文字以上。
 - 異なる文字が 5 文字以上。
 - デフォルトのパスワードの複雑性ルールが Linux PAM モジュールによって適用されます。
- 7 CLI および Root 認証情報に対して [SSH ログインを許可] を有効にします。
- 8 [デプロイの構成] で、次のプロパティを構成します。

オプション	説明
コンピュータ マネージャ	ドロップダウン メニューからコンピュータ マネージャを選択します。 たとえば、vCenter を選択します。
クラスタ	ドロップダウン メニューからクラスタを選択します。 たとえば、Compute-Cluster を選択します。
データストア	リストから共有データストアを選択します。 たとえば、vsanDatastore です。

9 ノードを設定します。

オプション	説明
IP アドレスの割り当て	<p>[固定] を選択します。</p> <p>以下の値を入力します。</p> <ul style="list-style-type: none"> ■ [管理 IP アドレス]: vCenter Server 管理ネットワークと同じ VLAN 上の IP アドレスを入力します。 <p>たとえば、10.197.79.146/24 です。</p> <ul style="list-style-type: none"> ■ [デフォルト ゲートウェイ]: 管理ネットワークのデフォルト ゲートウェイ。 <p>たとえば、10.197.79.253 です。</p>
管理インターフェイス	<p>[インターフェイスの選択] をクリックし、以前に作成したドロップダウン メニューから、管理ネットワークと同じ VLAN 上の vSphere Distributed Switch ポート グループを選択します。</p> <p>たとえば、DPortGroup-MGMT です。</p>

10 [NSX の構成] で [スイッチの追加] をクリックして、スイッチのプロパティを構成します。

11 [Edge スイッチ名] のデフォルト名を使用します。

たとえば、nvds1 です。

12 トランスポート ノードが属するトランスポート ゾーンを選択します。

以前に作成したオーバーレイ トランスポート ゾーンを選択します。

たとえば、nsx-overlay-transportzone です。

13 以前に作成した Edge アップリンク プロファイルを選択します。

例えば、EDGE-UPLINK-PROFILE です。

14 [IP アドレスの割り当て] の [IP アドレス プールを使用] を選択します。

15 以前に作成した Edge TEP の IP アドレス プールを選択します。

例えば、EDGE-TEP-IP-POOL です。

16 [チーミング ポリシー スイッチ マッピング] セクションで、以前に作成した Edge アップリンク プロファイルにアップリンクをマッピングします。

たとえば、Uplink1 の場合は、DPortGroup-EDGE-TEP を選択します。

17 手順 10 ~ 16 を繰り返して、新しいスイッチを追加します。

たとえば、次の値を構成します。

プロパティ	値
Edge スイッチ名	nvds2
トランスポート ゾーン	nsx-vlan-transportzone
Edge アップリンク プロファイル	EDGE-UPLINK-PROFILE
チーミング ポリシー スイッチ マッピング	DPortGroup-EDGE-UPLINK

18 [終了] をクリックします。

19 2 台目の NSX Edge 仮想マシンについて、手順 2 ~ 18 を繰り返します。

20 [Edge トランSPORT ノード] 画面で接続状態を確認します。

NSX Edge クラスタの作成

1 つ以上の NSX Edge が常に使用可能になるようにするには、NSX Edge クラスタを作成します。

手順

1 NSX Manager にログインします。

2 [システム] - [ファブリック] - [ノード] - [Edge クラスタ] - [追加] の順に選択します。

3 NSX Edge クラスタ名を入力します。

例えば、EDGE-CLUSTER です。

4 ドロップダウン メニューからデフォルトの NSX Edge クラスタ プロファイルを選択します。

[nsx-default-edge-high-availability-profile] を選択します。

5 [メンバーのタイプ] ドロップダウン メニューで、[Edge ノード] を選択します。

6 [使用可能] 列で、以前に作成した NSX Edge 仮想マシンを選択し、右矢印をクリックして [選択済み] 列に移動します。

7 たとえば、nsx-edge-1 および nsx-edge-2 などです。

8 [保存] をクリックします。

Tier-0 アップリンク セグメントの作成

Tier-0 アップリンク セグメントは、NSX から物理インフラストラクチャへの North-South 接続を提供します。

前提条件

Tier-0 ゲートウェイが作成されていることを確認します。

手順

1 NSX Manager にログインします。

2 [ネットワーク] - [セグメント] - [セグメントの追加] の順に選択します。

3 セグメントの名前を入力します。

例えば、TIER-0-LS-UPLINK です。

4 以前に作成したトランSPORT ゾーンを選択します。

たとえば、nsx-vlan-transportzone を選択します。

5 [管理者ステータス] を切り替えて有効にします。

6 Tier-0 ゲートウェイの VLAN ID を入力します。

たとえば、1089 です。

7 [保存] をクリックします。

Tier-0 ゲートウェイの作成

Tier-0 ゲートウェイは、物理インフラストラクチャへの NSX 論理ネットワークの North-South 接続を提供する NSX 論理ルーターです。vSphere IaaS control plane は、同じトランスポート ゾーン内の複数の NSX Edge クラスタで複数の Tier-0 ゲートウェイをサポートします。

Tier-0 ゲートウェイには、Tier-1 ゲートウェイとのダウンリンク接続および物理ネットワークとの外部接続があります。

アクティブ/アクティブまたはアクティブ/スタンバイになるように、Tier-0 ゲートウェイの HA (高可用性) モードを構成できます。次のサービスは、アクティブ/スタンバイ モードでのみサポートされます。

- NAT
- ロード バランシング
- ステートフル ファイアウォール
- VPN

NAT ルールまたはロード バランサの VIP が Tier-0 ゲートウェイ外部インターフェイスのサブネットの IP アドレスを使用する場合、Tier-0 ゲートウェイでプロキシ ARP が自動的に有効になります。プロキシ ARP を有効にすると、オーバーレイ セグメント上のホストと VLAN セグメント上のホストは、物理ネットワーク ファブリックに変更を加えることなくネットワーク トラフィックを交換できます。

NSX 3.2 より前では、アクティブ/スタンバイ構成のみ、Tier-0 ゲートウェイでプロキシ ARP がサポートされません。NSX 3.2 以降では、アクティブ/アクティブ構成の Tier-0 ゲートウェイでもプロキシ ARP がサポートされません。

詳細については、NSX 管理ガイドを参照してください。

前提条件

NSX Edge クラスタを作成済みであることを確認します。

手順

- 1 NSX Manager にログインします。
- 2 [ネットワーク] - [Tier-0 ゲートウェイ] の順に選択します。
- 3 [Tier-0 ゲートウェイの追加] をクリックします。
- 4 Tier-0 ゲートウェイの名前を入力します。

例えば、Tier-0_VWT です。

- 5 アクティブ/スタンバイ HA モードを選択します。

アクティブ/スタンバイ モードでは、選択されたアクティブなメンバーがすべてのトラフィックを処理します。アクティブなメンバーに障害が発生した場合は、新しいメンバーが選択されてアクティブになります。

- 6 以前に作成した NSX Edge クラスタを選択します。

たとえば、EDGE-CLUSTER を選択します。

7 [保存] をクリックします。

Tier-0 ゲートウェイが作成されます。

8 [はい] を選択して、構成を続行します。

9 インターフェイスを設定します。

a [インターフェイス] を展開して、[設定] をクリックします。

b [インターフェイスの追加] をクリックします。

c 名前を入力します。

たとえば、TIER-0_VWT-UPLINK1 という名前を入力します。

d [タイプ] で [外部] を選択します。

e Edge 論理ルーター – アップリンク VLAN から IP アドレスを入力します。IP アドレスは、以前に作成した NSX Edge 仮想マシン用に設定した管理 IP アドレスとは異なる必要があります。

たとえば、10.197.154.1/24 です。

f [接続先] で、以前に作成した Tier-0 アップリンク セグメントを選択します。

たとえば、TIER-0-LS-UPLINK。

g リストから NSX Edge ノードを選択します。

たとえば、nsx-edge-1 です。

h [保存] をクリックします。

i 2 つ目のインターフェイスについて、手順 a ~ h を繰り返します。

たとえば、IP アドレス 10.197.154.2/24 で nsx-edge-2 Edge ノードに接続される 2 つ目のアップリンク TIER-0_VWT-UPLINK2 を作成します。

j [閉じる] をクリックします。

10 高可用性を構成するには、[HA VIP 構成] で [設定] をクリックします。

a [HA VIP 構成の追加] をクリックします。

b IP アドレスを入力します。

たとえば、10.197.154.3/24。

c インターフェイスを選択します。

たとえば、TIER-0_VWT-UPLINK1 や TIER-0_VWT-UPLINK2 を選択します。

d [追加]、[適用] の順にクリックします。

11 ルーティングを構成するには、[ルーティング] をクリックします。

a スタティック ルートで [設定] をクリックします。

b [スタティック ルートの追加] をクリックします。

- c 名前を入力します。
たとえば、DEFAULT-STATIC-ROUTE です。
- d ネットワーク IP アドレスとして 0.0.0.0/0 を入力します。
- e ネクスト ホップを設定するには、[ネクスト ホップの設定] をクリックし、次に [ネクスト ホップの追加] をクリックします。
- f ネクスト ホップ ルーターの IP アドレスを入力します。通常、これは NSX Edge 論理ルーター アップリンク VLAN からの管理ネットワーク VLAN のデフォルト ゲートウェイです。
たとえば、10.197.154.253 です。
- g [追加]、[適用]、[保存] の順にクリックします。
- h [閉じる] をクリックします。

12 接続を確認するために、物理アーキテクチャの外部デバイスが、構成したアップリンクに対して ping を実行できることを確認します。

次のステップ

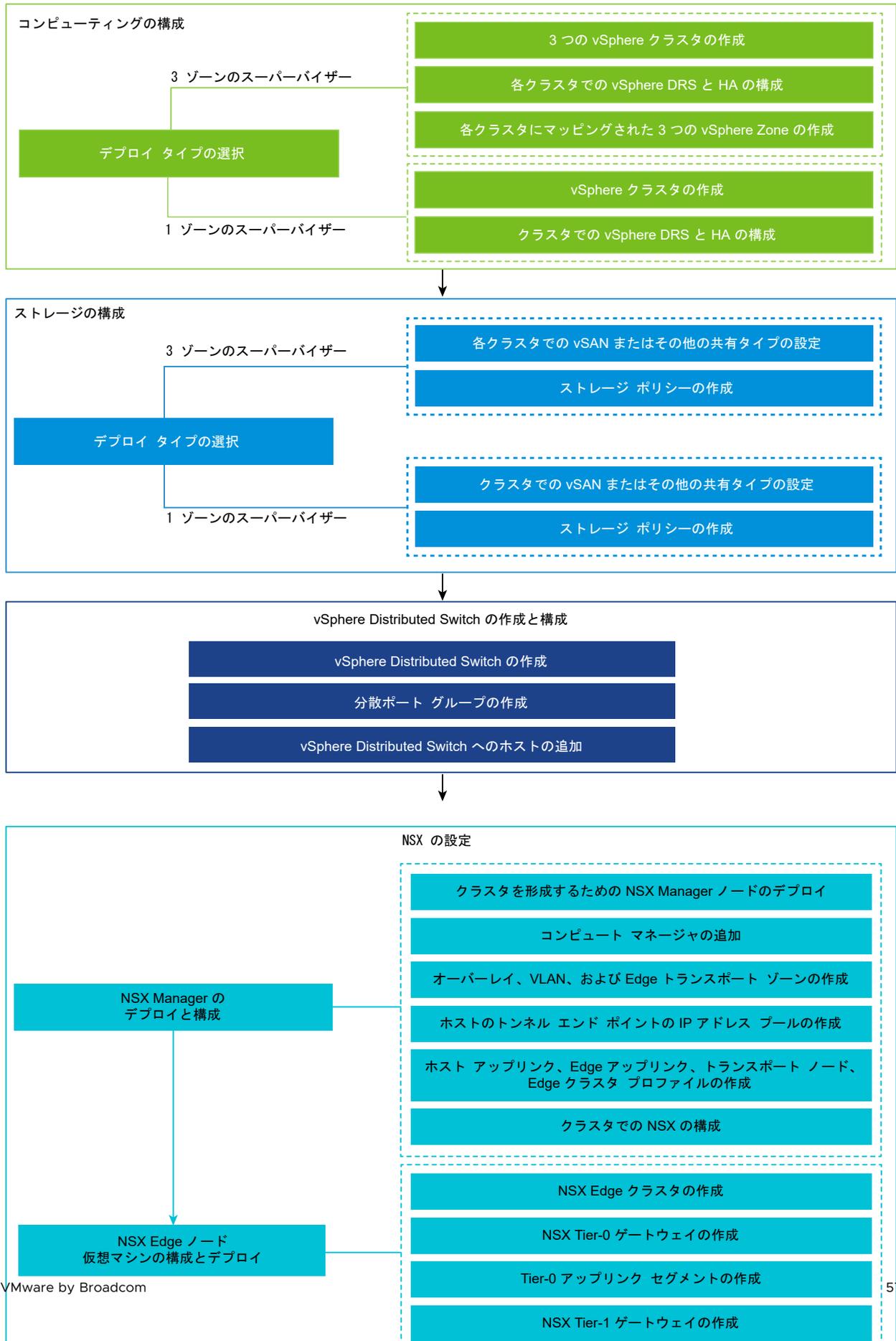
スーパーバイザー を構成します。『[NSX ネットワークを使用する 1 ゾーン スーパーバイザー のデプロイ](#)』を参照してください

NSX と NSX Advanced Load Balancer のインストールと構成

NSX をネットワーク スタックとして使用する スーパーバイザー 環境では、ロード バランシング サービスとして NSX Advanced Load Balancer を使用できます。

このセクションでは、新しい NSX インスタンスと新しい NSX Advanced Load Balancer をデプロイして スーパーバイザー ネットワークを構成する方法について説明します。NSX Advanced Load Balancer のインストールと構成の手順は、既存の NSX デプロイにも適用できます。

図 4-8. NSX と NSX Advanced Load Balancer を使用してスーパーバイザーを構成するためのワークフロー



NSX Advanced Load Balancer で使用する スーパーバイザー の vSphere Distributed Switch の作成

NSX ネットワーク スタックを使用し、NSX Advanced Load Balancer をスーパーバイザー として使用する vSphere クラスタを構成するには、vSphere Distributed Switch を構成する必要があります。Distributed Switch 上でスーパーバイザー のワークロード ネットワークとして構成できるポート グループを作成します。NSX Advanced Load Balancer にサービス エンジン データ インターフェイスを接続するには、分散ポート グループが必要です。分散ポート グループは、アプリケーションの仮想 IP アドレス (VIP) をサービス エンジンに配置するために使用されます。

前提条件

NSX Advanced Load Balancer でスーパーバイザー の vSphere ネットワークを使用するためのシステム要件とネットワーク トポロジを確認します。『vSphere IaaS 制御プレーンの概念と計画』の「[Requirements for Zonal Supervisor with NSX and NSX Advanced Load Balancer](#)」および「[Requirements for Cluster Supervisor Deployment with NSX and NSX Advanced Load Balancer](#)」を参照してください。

手順

- 1 vSphere Client で、データセンターに移動します。
- 2 データセンターを右クリックして、[Distributed Switch] - [新しい Distributed Switch] の順に選択します。
- 3 スイッチの名前 (**wcp_vds_1** など) を入力し、[次へ] をクリックします。
- 4 スイッチのバージョン 8.0 を選択して、[次へ] をクリックします。
- 5 [ポート グループ名] に **プライマリ ワークロード ネットワーク** と入力し、[次へ] をクリックして [終了] をクリックします。

1つのポート グループを持つ新しい Distributed Switch がデータセンターに作成されます。このポート グループは、作成するスーパーバイザー のプライマリ ワークロード ネットワークとして使用できます。プライマリ ワークロード ネットワークは、Kubernetes 制御プレーン仮想マシンのトラフィックを処理します。

- 6 ワークロード ネットワークの分散ポート グループを作成します。

作成するポート グループの数は、スーパーバイザー 用に実装するトポロジによって異なります。隔離されたワークロード ネットワークが1つ含まれるトポロジの場合は、スーパーバイザー のすべての名前空間用のネットワークとして使用する分散ポート グループを1つ作成します。ネットワークが名前空間ごとに隔離されているトポロジの場合は、作成する名前空間と同じ数のポート グループを作成します。

- a 新しく作成した Distributed Switch に移動します。
- b スイッチを右クリックして、[分散ポート グループ] - [新規分散ポート グループ] の順に選択します。
- c ポート グループの名前 (**ワークロード ネットワーク** など) を入力して、[次へ] をクリックします。
- d デフォルトのままにして、[次へ] をクリックし、[終了] をクリックします。

7 データ ネットワークのポート グループを作成します。

- a Distributed Switch を右クリックして、[分散ポート グループ] - [新規分散ポート グループ] を選択します。
- b ポート グループの名前（**データ ネットワーク** など）を入力して、[次へ] をクリックします。
- c [設定の構成] 画面で新規分散ポート グループの全般プロパティを入力し、[次へ] をクリックします。

プロパティ	説明
ポート バインド	この分散ポート グループに接続された仮想マシンにポートを割り当てるときに選択します。 [静的バインド] を選択すると、仮想マシンが分散ポート グループに接続されるときに仮想マシンにポートを割り当てます。
ポートの割り当て	ポート割り当てとして [弾性] を選択します。 デフォルトのポート数は 8 個です。すべてのポートが割り当てられたら、新しい 8 組のポートが作成されます。
ポート数	デフォルト値を保持します。
ネットワーク リソース プール	ドロップダウン メニューで、新しい分散ポート グループをユーザー定義のネットワーク リソース プールに割り当てます。ネットワーク リソース プールを作成していない場合、このメニューは空です。
VLAN	ドロップダウン メニューで VLAN トラフィックのフィルタリングおよびマーキングのタイプを選択します。 <ul style="list-style-type: none"> ■ [なし]：VLAN を使用しません。外部スイッチ タギングを使用している場合は、このオプションを選択します。 ■ [VLAN]：[VLAN ID] テキスト ボックスに、仮想スイッチ タギング用の値を 1～4,094 の範囲で入力します。 ■ [VLAN トランク]：仮想ゲスト タギングを行って、VLAN トラフィックに ID を設定してゲスト OS に送信するには、このオプションを使用します。VLAN トランク 範囲を入力します。コンマ区切りリストを使用して複数の範囲や個々の VLAN を設定できます。たとえば、1702-1705、1848-1849 です。 ■ [プライベート VLAN]：トラフィックと、Distributed Switch で作成されたプライベート VLAN を関連付けます。プライベート VLAN を作成していない場合、このメニューは空です。
詳細	このオプションは選択解除したままにします。

8 [設定の確認] 画面で構成を確認し、[完了] をクリックします。

結果

Distributed Switch が作成され、Distributed Switch の下に分散ポート グループが表示されます。

NSX Manager のデプロイと構成

vSphere Client を使用して、vSphere クラスタに NSX Manager をデプロイします。その後、NSX Manager を構成して使用することにより、NSX 環境を管理できます。

前提条件

- ■ 環境がネットワークの要件を満たしていることを確認します。要件の詳細については、『vSphere IaaS 制御プレーンの概念と計画』の「Requirements for Zonal Supervisor with NSX and NSX Advanced Load Balancer」および「Requirements for Cluster Supervisor Deployment with NSX and NSX Advanced Load Balancer」を参照してください。
- 必要なポートが開いていることを確認します。ポートとプロトコルの詳細については、『NSX インストール ガイド』を参照してください。

手順

- 1 VMware ダウンロード ポータルで NSX OVA ファイルを見つけます。
ダウンロード URL をコピーするか、OVA ファイルをダウンロードします。
- 2 右クリックして [OVF テンプレートのデプロイ] を選択し、インストール ウィザードを開始します。
- 3 [OVF テンプレートの選択] タブで、OVA のダウンロード URL を入力するか、OVA ファイルに移動します。
- 4 [名前とフォルダの選択] タブで、NSX Manager 仮想マシン (VM) の名前を入力します。
- 5 [コンピューティング リソースの選択] タブで、NSX Manager をデプロイする vSphere クラスタを選択します。
- 6 [次へ] をクリックして、詳細を確認します。
- 7 [構成] タブで、NSX のデプロイ サイズを選択します。
- 8 [ストレージの選択] タブで、デプロイ用の共有ストレージを選択します。
- 9 [仮想ディスク フォーマットの選択] で [シン プロビジョニング] を選択して、シン プロビジョニングを有効にします。

デフォルトでは、仮想ディスクはシック プロビジョニングされます。
- 10 [ネットワークの選択] タブの [ターゲット ネットワーク] で、NSX Manager の管理ポート グループまたはターゲット ネットワークを選択します。

たとえば、DPortGroup-MGMT です。
- 11 [テンプレートのカスタマイズ] タブで、NSX Manager のシステム root、CLI 管理者、および監査パスワードを入力します。パスワードの強度の制限に従ってパスワードを入力する必要があります。
 - 12 文字以上。
 - 小文字が 1 文字以上。
 - 大文字が 1 文字以上。
 - 数字が 1 文字以上。
 - 特殊文字が 1 文字以上。
 - 異なる文字が 5 文字以上。
 - デフォルトのパスワードの複雑性ルールが Linux PAM モジュールによって適用されます。

- 12 デフォルトの IPv4 ゲートウェイ、管理ネットワークの IPv4、管理ネットワークのネットマスク、DNS サーバ、ドメイン検索リスト、および NTP IP アドレスを入力します。
- 13 SSH を有効にして、NSX Manager コマンドラインに root による SSH ログインを許可します。
デフォルトでは、SSH オプションはセキュリティ上の理由から無効になっています。
- 14 カスタム OVF テンプレートの仕様が正確であることを確認し、[終了] をクリックしてインストールを開始します。
- 15 NSX Manager が起動したら、admin として CLI にログインし、`get interface eth0` コマンドを実行して、IP アドレスが想定どおりに適用されていることを確認します。
- 16 `get services` コマンドを入力して、すべてのサービスが実行されていることを確認します。

NSX Manager ノードのデプロイによるクラスタの形成

NSX Manager クラスタは高可用性を提供します。vCenter Server によって管理されている ESXi ホストにのみ、ユーザー インターフェイスを使用して NSX Manager ノードをデプロイできます。NSX Manager クラスタを作成するには、2 台の追加ノードをデプロイして、合計 3 台のノードによるクラスタを形成します。ユーザー インターフェイスから新しいノードをデプロイすると、そのノードは最初にデプロイされたノードに接続してクラスタを形成します。最初にデプロイされたノードのリポジトリのすべての詳細とパスワードは、新しくデプロイされたノードと同期されます。

前提条件

- NSX Manager ノードがインストールされていることを確認します。
- コンピュート マネージャが構成されていることを確認します。
- 必要なポートが開いていることを確認します。
- ESXi ホストにデータストアが構成されていることを確認します。
- IP アドレスとゲートウェイ、DNS サーバの IP アドレス、ドメイン検索リスト、および NTP サーバの IP アドレスが、NSX Manager で使用できるようになっていることを確認します。
- ターゲット仮想マシンのポート グループ ネットワークがあることを確認します。管理仮想マシン ネットワークに NSX アプライアンスを配置します。

手順

- 1 ブラウザから管理者権限で `https://<manager-ip-address>` の NSX Manager にログインします。
- 2 アプライアンスをデプロイするために、[システム] - [アプライアンス] - [NSX アプライアンスの追加] の順に選択します。
- 3 アプライアンスの詳細を入力します。

オプション	説明
ホスト名	ノードに使用するホスト名または FQDN を入力します。
管理 IP アドレス/ネットマスク	ノードに割り当てる IP アドレスを入力します。
管理ゲートウェイ	ノードで使用するゲートウェイ IP アドレスを入力します。

オプション	説明
DNS サーバ	ノードで使用する DNS サーバの IP アドレスのリストを入力します。
NTP サーバ	NTP サーバの IP アドレスのリストを入力します
ノード サイズ	オプションから [中 (6 個の vCPU、24 GB の RAM、300 GB のストレージ)] のフォームファクタを選択します。

4 アプライアンスの構成の詳細を入力します

オプション	説明
コンピュート マネージャ	コンピュート マネージャとして構成した vCenter Server を選択します。
コンピューティング クラスタ	ノードが参加するクラスタを選択します。
データストア	ノードのファイル用のデータストアを選択します。
仮想ディスクのフォーマット	[シン プロビジョニング] フォーマットを選択します。
ネットワーク	[ネットワークの選択] をクリックして、ノードの管理ネットワークを選択します。

5 アクセスと認証情報の詳細を入力します。

オプション	説明
SSH の有効化	ボタンを切り替えて、新しいノードへの SSH ログインを許可します。
root アクセスの有効化	ボタンを切り替えて、新しいノードへの root アクセスを許可します。
システムの root 認証情報	新しいノードの root パスワードを設定して確認します。 パスワードの強度の制限に従ってパスワードを入力する必要があります。 <ul style="list-style-type: none"> ■ 12 文字以上。 ■ 小文字が 1 文字以上。 ■ 大文字が 1 文字以上。 ■ 数字が 1 文字以上。 ■ 特殊文字が 1 文字以上。 ■ 異なる文字が 5 文字以上。 ■ デフォルトのパスワードの複雑性ルールが Linux PAM モジュールによって適用されません。
管理者 CLI 認証情報と監査 CLI 認証情報	root に設定したのと同じパスワードを使用する場合は、[root パスワードと同じ] チェックボックスをオンにします。または、チェックボックスをオフにして、別のパスワードを設定します。

6 [アプライアンスのインストール] をクリックします。

新しいノードがデプロイされます。デプロイ プロセスは [システム] - [アプライアンス] 画面で追跡できます。インストールが完了してクラスタが安定するまでは、ノードを追加しないでください。

7 デプロイ、クラスタの形成、およびリポジトリの同期が完了するまで待機します。

ノードの参加とクラスタの安定化には、10 ~ 15 分程度かかる場合があります。クラスタに他の変更を加える前に、すべてのクラスタ サービス グループの状態が接続中であることを確認します。

- 8 ノードが起動したら、管理者として CLI にログインし、`get interface eth0` コマンドを実行して、IP アドレスが想定どおりに適用されていることを確認します。
- 9 クラスタのノードが 2 台のみの場合は、別のアプライアンスを追加します。[システム] - [アプライアンス] - [NSX アプライアンスの追加] の順に選択して、構成手順を繰り返します。

ライセンスの追加

NSX Manager を使用してライセンスを追加します。

前提条件

NSXAdvanced 以上のライセンスを取得します。

手順

- 1 NSX Manager にログインします。
- 2 [システム] - [ライセンス] - [追加] の順に選択します。
- 3 ライセンス キーを入力します。
- 4 [追加] をクリックします。

コンピュート マネージャの追加

コンピュート マネージャは、ホストや仮想マシンなどのリソースを管理するアプリケーションです。NSX に関連付けられている vCenter Server を NSX Manager のコンピュート マネージャとして構成します。

詳細については、『NSX 管理ガイド』を参照してください。

手順

- 1 NSX Manager にログインします。
- 2 [システム] - [ファブリック] - [コンピュート マネージャ] - [追加] の順に選択します。
- 3 コンピュート マネージャの詳細を入力します。

オプション	説明
名前と説明	vCenter Server の名前および説明を入力します。
タイプ	デフォルトのタイプは VMware vCenter です。
マルチ NSX	このオプションは選択解除したままにします。 マルチ NSX オプションを使用すると、同じ vCenter Server を複数の NSX Manager に登録できます。このオプションは、スーパーバイザー および vSphere Lifecycle Manager クラスタではサポートされません。
FQDN または IP アドレス	vCenter Server の FQDN または IP アドレスを入力します。
リバース プロキシの HTTPS ポート	デフォルトのポートは 443 です。別のポートを使用する場合は、すべての NSX Manager アプライアンスでポートが開いていることを確認します。 リバース プロキシ ポートを設定して、NSX にコンピュート マネージャを登録します。

オプション	説明
ユーザー名とパスワード	vCenter Server のログイン認証情報を入力します。
SHA-256 サンプリント	vCenter Server SHA-256 サンプリント アルゴリズムの値を入力します。

その他の設定はデフォルトのままかまいません。

サンプリント値を空白にすると、サーバのサンプリントを使用するように指示されます。サンプリントを受け入れてから NSX が vCenter Server リソースを検出して登録するまで、数秒かかります。

- 4 [信頼の有効化] を選択して、vCenter Server が NSX と通信できるようにします。
- 5 NSX Manager のサンプリント値を指定しなかった場合、システムはサンプリントを識別して表示します。
- 6 [追加] をクリックして、サンプリントを受け入れます。

結果

しばらくすると、コンピュート マネージャが vCenter Server に登録され、接続ステータスが 接続中 に変わります。vCenter Server の FQDN または PNID が変更された場合は、NSX Manager に再登録する必要があります。詳細については、『[NSX Manager による vCenter Server の登録](#)』を参照してください。

注: vCenter Server が正常に登録されたら、コンピュート マネージャを削除する前に NSX Manager 仮想マシンをパワーオフして削除しないでください。そのようにすると、新しい NSX Manager をデプロイするときに、同じ vCenter Server を再度登録することができなくなります。vCenter Server がすでに別の NSX Manager に登録されていることを示すエラーが表示されます。

コンピュート マネージャ名をクリックすると、詳細の表示、コンピュート マネージャの編集、またはコンピュート マネージャに適用されるタグの管理を行うことができます。

トランスポート ゾーンの作成

トランスポート ゾーンは、特定のネットワークを使用できるホストおよび仮想マシンを示します。トランスポート ゾーンは、1 つ以上のホスト クラスタにまたがることができます。

デフォルトのトランスポート ゾーンを使用するか、次のゾーンを作成します。

- NSX Advanced Load Balancer Controller とサービス エンジンの間の管理ネットワーク接続のために、スーパーバイザー 制御プレーン仮想マシンによって使用されるオーバーレイ トランスポート ゾーン。
- 物理ネットワークへのアップリンクに使用する NSX Edge ノードの VLAN トランスポート ゾーン。

手順

- 1 NSX Manager にログインします。
- 2 [システム] - [ファブリック] - [トランスポート ゾーン] - [トランスポート ゾーンの追加 (ADD TRANSPORT ZONE)] の順に選択します。
- 3 トランスポート ゾーンの名前と、必要に応じて説明を入力します。例: **overlayTZ**。

4 [オーバーレイ] トラフィック タイプを選択します。

デフォルトでは、次のトランスポート ゾーンがあります。

- 名前が `nsx-vlan-transportzone` の VLAN トランスポート ゾーン。
- 名前が `nsx-overlay-transportzone` のオーバーレイ トランスポート ゾーン。

5 [[保存]] をクリックします。

6 2 から 5 の手順を繰り返して、名前が `vlanTZ`、トラフィック タイプが [VLAN] のトランスポート ゾーンを作成します。

7 (オプション) 1つ以上のアップリンク チーミング ポリシー名を入力します。

トランスポート ゾーンに接続されたセグメントは、これらの名前付きチーミング ポリシーを使用します。一致する名前付きチーミング ポリシーをセグメントが見つけれられない場合は、デフォルトのアップリンク チーミング ポリシーが使用されます。

結果

作成したトランスポート ゾーンが [トランスポート ゾーン] 画面に表示されます。

ホストのトンネル エンドポイント IP アドレス用の IP アドレス プールの作成

ESXi ホストのトンネル エンドポイント (TEP) の IP アドレス プールを作成します。TEP は、オーバーレイ フレームの NSX のカプセル化を開始および終了する ESXi ホストを識別するために、外部 IP ヘッダーで使用される送信元 IP アドレスと宛先 IP アドレスです。

手順

- 1 NSX Manager にログインします。
- 2 [ネットワーク] - [IP アドレス プール] - [IP アドレス プールの追加] の順に選択します。
- 3 IP アドレス プールの名前、およびオプションで説明を入力します。たとえば、`ESXI-TEP-IP-POOL` です。
- 4 [設定] をクリックします。
- 5 [サブネットの追加 (ADD SUBNET)] ドロップダウン メニューから [IP アドレス範囲] を選択します。
- 6 次の IP アドレス プールの詳細を入力します。

オプション	説明
IP アドレス範囲	IP アドレスの割り当ての範囲を入力します。 たとえば、IPv4 Range - 192.168.12.1-192.168.12.60, IPv6 Range - 2001:800::0001-2001:0fff:ffff:ffff:ffff:ffff:ffff:ffff。
CIDR	ネットワーク アドレスを CIDR 表記で入力します。 たとえば、192.23.213.0/24 です。

7 必要に応じて、次の詳細を入力します。

オプション	説明
説明	IP アドレス範囲の説明を入力します。
ゲートウェイ IP	ゲートウェイ IP アドレスを入力します。 たとえば、192.23.213.253 です。
DNS サーバ	DNS サーバのアドレスを入力します。
DNS サフィックス	DNS サフィックスを入力します。

8 [追加]、[適用] の順にクリックします。

9 [保存] をクリックします。

結果

作成した TEP の IP アドレス プールが [IP アドレス プール] 画面に表示されていることを確認します。

Edge ノード用の IP アドレス プールの作成

Edge ノード用の IP アドレス プールを作成します。TEP アドレスはルーティング可能である必要はありません。Edge TEP がホスト TEP と通信できる任意の IP アドレス指定スキームを使用できます。

手順

1 NSX Manager にログインします。

2 [ネットワーク] - [IP アドレス プール] - [IP アドレス プールの追加] の順に選択します。

3 IP アドレス プールの名前、およびオプションで説明を入力します。例：**EDGE-TEP-IP-POOL**。

4 [設定] をクリックします。

5 次の IP アドレス プールの詳細を入力します。

オプション	説明
IP アドレス範囲	IP アドレスの割り当ての範囲を入力します。 たとえば、IPv4 Range - 192.168.12.1-192.168.12.60, IPv6 Range - 2001:800::0001-2001:0fff:ffff:ffff:ffff:ffff:ffff:ffff。
CIDR	ネットワーク アドレスを CIDR 表記で入力します。 たとえば、192.23.213.0/24 です。

6 必要に応じて、次の詳細を入力します。

オプション	説明
説明	IP アドレス範囲の説明を入力します。
ゲートウェイ IP	ゲートウェイ IP アドレスを入力します。 たとえば、192.23.213.253 です。

オプション	説明
DNS サーバ	DNS サーバのアドレスを入力します。
DNS サフィックス	DNS サフィックスを入力します。

7 [追加]、[適用] の順にクリックします。

8 [保存] をクリックします。

結果

作成した IP アドレス プールが [IP アドレス プール] 画面に表示されていることを確認します。

ESXi ホスト アップリンク プロファイルの作成

ホスト アップリンク プロファイルは、ESXi ホストから NSX セグメントへのアップリンクのポリシーを定義します。

手順

1 NSX Manager にログインします。

2 [システム] - [ファブリック] - [プロファイル] - [アップリンク プロファイル] - [プロファイルの追加 (ADD PROFILE)] の順に選択します。

3 アップリンク プロファイルの名前と、オプションでアップリンク プロファイルの説明を入力します。

例： **ESXI-UPLINK-PROFILE**。

4 [チーミング] セクションで、[追加] をクリックしてチーミング ポリシーの名前を追加し、[FAILOVER_ORDER] ポリシーを構成します。

アクティブ アップリンクのリストが指定され、トランスポート ノードの各インターフェイスが1つのアクティブ アップリンクに固定されます。この設定により、複数のアクティブ アップリンクを同時に使用できます。

5 アクティブ リンクとスタンバイ リンクを構成します。

たとえば、 **uplink-1** をアクティブ アップリンクとして、 **uplink-2** をスタンバイ アップリンクとして構成します。

6 (オプション) トランスポート VLAN の値を入力します。例： **1060**。

アップリンク プロファイルで設定されたトランスポート VLAN がオーバーレイ トラフィックをタグ付けし、VLAN ID はトンネル エンドポイント (TEP) によって使用されます。

7 MTU 値を入力します。値は 1,600 以上にする必要がありますが、物理スイッチと vSphere Distributed Switch の MTU 値よりも大きくすることはできません。

NSX は、グローバルのデフォルト MTU 値 1700 を使用します。

結果

アップリンクを [アップリンク プロファイル] 画面で確認します。

NSX Edge アップリンク プロファイルの作成

アップリンクは、NSX Edge ノードから NSX 論理スイッチへのリンクです。アップリンク プロファイルは、チーミング ポリシー、アクティブ リンク、スタンバイ リンク、トランスポート VLAN ID、MTU 値を設定することによってアップリンクのポリシーを定義します。

アップリンク プロファイルを作成し、フェイルオーバーの順序チーミング ポリシーを追加して、Edge 仮想マシンのオーバーレイ トラフィックに対して 1 つのアップリンクが使用されるようにします。

手順

- 1 NSX Manager にログインします。
- 2 [システム] - [ファブリック] - [プロファイル] - [アップリンク プロファイル] - [プロファイルの追加 (ADD PROFILE)] - [の順に選択します。].
- 3 アップリンク プロファイルの名前と、オプションでアップリンク プロファイルの説明を入力します。

例： **EDGE-UPLINK-PROFILE**。

- 4 [チーミング] セクションで、[追加] をクリックしてチーミング ポリシーの名前を追加し、[FAILOVER_ORDER] ポリシーを構成します。

アクティブ アップリンクのリストが指定され、トランスポート ノードの各インターフェイスが 1 つのアクティブ アップリンクに固定されます。この設定により、複数のアクティブ アップリンクを同時に使用できます。

- 5 アクティブ アップリンクを構成します。

たとえば、 **uplink-1** をアクティブ アップリンクとして構成します。

結果

アップリンクを [アップリンク プロファイル] 画面で確認します。

トランスポート ノード プロファイルの作成

トランスポート ノード プロファイルは、プロファイルが添付されている特定のクラスタ内のホストに NSX をどのようにインストールして構成するかを定義します。ESXi クラスタをトランスポート ノードとして準備する前に、トランスポート ノード プロファイルを作成します。

注： トランスポート ノード プロファイルは、ホストにのみ適用されます。NSX Edge トランスポート ノードには適用できません。

前提条件

- クラスタが使用可能であることを確認します。NSX Manager ノードのデプロイによるクラスタの形成を参照してください。
- オーバーレイ トランスポート ゾーンを作成します。トランスポート ゾーンの作成を参照してください。
- IP アドレス プールを構成します。ホストのトンネル エンドポイント IP アドレス用の IP アドレス プールの作成を参照してください。
- コンピュート マネージャを追加します。コンピュート マネージャの追加を参照してください。

手順

- 1 NSX Manager にログインします。
- 2 [システム] - [ファブリック (Fabric)] - [ホスト] の順に選択します。
- 3 [ホスト] 画面で、[トランスポート ノード プロファイル (Transport Node Profile)] - [トランスポート ノード プロファイルの追加 (ADD TRANSPORT NODE PROFILE)] の順に選択します。
- 4 トランスポート ノード プロファイルを識別する名前を入力します。例：
HOST-TRANSPORT-NODE-PROFILE。
オプションで、トランスポート ノード プロファイルについての説明を追加できます。
- 5 [ホスト スイッチ] フィールドで、[設定] を選択します。
- 6 [ホスト スイッチ (Host Switch)] ウィンドウで、スイッチの詳細を入力します。

オプション	説明
vCenter Server	[vCenter Server] を選択します。
タイプ	ホストで構成されるスイッチ タイプを選択します。[VDS] を選択します。
Distributed Switch	選択した vCenter Server に作成した VDS を選択します。例： wcp_vds_1 。
トランスポート ゾーン	以前に作成したオーバーレイ トランスポート ゾーンを選択します。例： overlayTZ 。
アップリンク プロファイル	以前に作成したホスト アップリンク プロファイルを選択します。例： ESXI-UPLINK-PROFILE 。
IP アドレス タイプ	IPv4 を選択します。
IPv4 の割り当て	[Use IP Pool] を選択します。
IPv4 プール	以前に作成したホスト TEP プールを選択します。例： ESXI-TEP-IP-POOL 。
チーミング ポリシー アップリンク マッピング	[追加] をクリックし、NSX アップリンク プロファイルで定義されているアップリンクを vSphere Distributed Switch アップリンクにマッピングします。たとえば、 uplink-1 を Uplink 1 にマッピングし、 uplink-2 を Uplink 2 にマッピングします。

- 7 [追加]、[適用] の順にクリックします。
- 8 [保存] をクリックして構成を保存します。

結果

作成したプロファイルが [トランスポート ノード プロファイル] 画面に一覧表示されます。

NSX Edge クラスタ プロファイルの作成

NSX Edge トランスポート ノードのポリシーを定義する NSX Edge クラスタ プロファイルを作成します。

前提条件

NSX Edge クラスタが使用可能であることを確認します。

手順

- 1 NSX Manager にログインします。

- 2 [システム] - [ファブリック] - [プロファイル] - [Edge クラスタ プロファイル (Edge Cluster Profiles)] - [プロファイルの追加 (ADD PROFILE)] - [の順に選択します.]
- 3 NSX Edge クラスタ プロファイルの詳細を入力します。
- 4 NSX Edge クラスタ プロファイルの名前を入力します。例 : **Cluster Profile - 1**。
必要に応じて、説明を入力します。
- 5 その他の設定はデフォルトのままにします。
- 6 [追加] をクリックします。

クラスタ上の NSX の構成

NSX をインストールしてオーバーレイ TEP を準備するには、トランスポート ノード プロファイルを vSphere クラスタに適用します。

前提条件

トランスポート ノード プロファイルが作成されていることを確認します。

手順

- 1 NSX Manager にログインします。
- 2 [システム] - [ファブリック] - [ノード] - [ホスト トランスポート ノード] の順に選択します。
- 3 [管理元] ドロップダウン メニューから、既存の vCenter Server を選択します。
画面には、使用可能な vSphere クラスタが一覧表示されます。
- 4 NSX を構成するコンピューティング クラスタを選択します。
- 5 [NSX の構成] をクリックします。
- 6 以前に作成したトランスポート ノード プロファイルを選択し、[適用] をクリックします。
例えば、HOST-TRANSPORT-NODE-PROFILE です。
- 7 [ホスト トランスポート ノード] 画面で、NSX の構成状態が `Success` であること、およびクラスタ内にあるホストの NSX Manager の接続ステータスが `Up` であることを確認します。

結果

NSX のインストールとオーバーレイ TEP の準備のために、以前に作成したトランスポート ノード プロファイルが vSphere クラスタに適用されます。

NSX Edge トランスポート ノードの作成

NSX Edge 仮想マシン (VM) を NSX ファブリックに追加して、NSX Edge トランスポート ノード仮想マシンとして構成することができます。

前提条件

トランスポート ゾーン、Edge アップリンク プロファイル、Edge TEP IP アドレス プールを作成済みであることを確認します。

手順

- 1 NSX Manager にログインします。
- 2 [システム] - [ファブリック] - [ノード] - [Edge トランスポート ノード] - [Edge ノードの追加 (ADD EDGE NODE)] の順に選択します。
- 3 [名前と説明] に NSX Edge ノードの名前を入力します。
たとえば、nsx-edge-1。
- 4 vCenter Server のホスト名または FQDN を入力します。
たとえば、nsx-edge-1.lab.com です。
- 5 NSX Edge 仮想マシン アプライアンスのフォーム ファクタを選択します。
- 6 [認証情報] に NSX Edge の CLI および root パスワードを入力します。パスワードの強度の制限に従ってパスワードを入力する必要があります。
 - 12 文字以上。
 - 小文字が 1 文字以上。
 - 大文字が 1 文字以上。
 - 数字が 1 文字以上。
 - 特殊文字が 1 文字以上。
 - 異なる文字が 5 文字以上。
 - デフォルトのパスワードの複雑性ルールが Linux PAM モジュールによって適用されます。
- 7 CLI および Root 認証情報に対して [SSH ログインを許可] を有効にします。
- 8 [デプロイの構成] で、次のプロパティを構成します。

オプション	説明
コンピュータ マネージャ	ドロップダウン メニューからコンピュータ マネージャを選択します。 たとえば、vCenter を選択します。
クラスタ	ドロップダウン メニューからクラスタを選択します。 たとえば、Compute-Cluster を選択します。
データストア	リストから共有データストアを選択します。 たとえば、vsanDatastore です。

9 ノードを設定します。

オプション	説明
IP アドレスの割り当て	<p>[固定] を選択します。</p> <p>以下の値を入力します。</p> <ul style="list-style-type: none"> ■ [管理 IP アドレス]: vCenter Server 管理ネットワークと同じ VLAN 上の IP アドレスを入力します。 <p>たとえば、10.197.79.146/24 です。</p> <ul style="list-style-type: none"> ■ [デフォルト ゲートウェイ]: 管理ネットワークのデフォルト ゲートウェイ。 <p>たとえば、10.197.79.253 です。</p>
管理インターフェイス	<p>[インターフェイスの選択] をクリックし、以前に作成したドロップダウン メニューから、管理ネットワークと同じ VLAN 上の vSphere Distributed Switch ポート グループを選択します。</p> <p>たとえば、DPortGroup-MGMT です。</p>

10 [NSX の構成] で [スイッチの追加] をクリックして、スイッチのプロパティを構成します。

11 [Edge スイッチ名] のデフォルト名を使用します。

たとえば、nvds1 です。

12 トランスポート ノードが属するトランスポート ゾーンを選択します。

以前に作成したオーバーレイ トランスポート ゾーンを選択します。

たとえば、overlayTZ です。

13 以前に作成した Edge アップリンク プロファイルを選択します。

例えば、EDGE-UPLINK-PROFILE です。

14 [IP アドレスの割り当て] の [IP アドレス プールを使用] を選択します。

15 以前に作成した Edge TEP の IP アドレス プールを選択します。

例えば、EDGE-TEP-IP-POOL です。

16 [チーミング ポリシー スイッチ マッピング] セクションで、以前に作成した Edge アップリンク プロファイルにアップリンクをマッピングします。

たとえば、Uplink1 の場合は、uplink-1 を選択します。

17 手順 10 ~ 16 を繰り返して、新しいスイッチを追加します。

たとえば、次の値を構成します。

プロパティ	値
Edge スイッチ名	nvds2
トランスポート ゾーン	vlanTZ
Edge アップリンク プロファイル	EDGE-UPLINK-PROFILE
チーミング ポリシー スイッチ マッピング	DPortGroup-EDGE-UPLINK

- 18 [終了] をクリックします。
- 19 2 台目の NSX Edge 仮想マシンについて、手順 2 ~ 18 を繰り返します。
- 20 [Edge トランスポート ノード] 画面で接続状態を確認します。

NSX Edge クラスタの作成

1 つ以上の NSX Edge が常に使用可能になるようにするには、NSX Edge クラスタを作成します。

手順

- 1 NSX Manager にログインします。
- 2 [システム] - [ファブリック] - [ノード] - [Edge クラスタ] - [追加] の順に選択します。
- 3 NSX Edge クラスタ名を入力します。
例えば、EDGECLUSTER1 です。
- 4 [保存] をクリックします。
- 5 ドロップダウン メニューから作成済みの NSX Edge クラスタ プロファイルを選択します。例：
Cluster Profile - 1。
- 6 [メンバーのタイプ] ドロップダウン メニューで、[Edge ノード] を選択します。
- 7 [使用可能] 列で、以前に作成した NSX Edge 仮想マシンを選択し、右矢印をクリックして [選択済み] 列に移動します。
- 8 たとえば、nsx-edge-1 および nsx-edge-2 などです。
- 9 [保存] をクリックします。

次のステップ

Tier-0 ゲートウェイの作成

Tier-0 ゲートウェイは、物理インフラストラクチャへの NSX 論理ネットワークの North-South 接続を提供する NSX 論理ルーターです。vSphere IaaS control plane は、同じトランスポート ゾーン内の複数の NSX Edge クラスタで複数の Tier-0 ゲートウェイをサポートします。

エッジ Tier-0 ルータにおける NSX ルート マップの構成の詳細については、<https://docs.vmware.com/jp/VMware-Cloud-Foundation/4.0/vcf-40-doc.zip> にある『VMware Cloud Foundation 運用および管理ガイド』を参照してください。

前提条件

NSX Edge クラスタを作成済みであることを確認します。

手順

- 1 NSX Manager にログインします。
- 2 [ネットワーク] - [Tier-0 ゲートウェイ] の順に選択します。

3 [ゲートウェイを追加] をクリックします。

4 Tier-0 ゲートウェイの名前を入力します。

例えば、ContainerT0 です。

5 アクティブ/スタンバイ HA モードを選択します。

デフォルトのモードは、アクティブ/アクティブです。アクティブ/スタンバイ モードでは、選択されたアクティブなメンバーがすべてのトラフィックを処理します。アクティブなメンバーに障害が発生した場合は、新しいメンバーが選択されてアクティブになります。

6 HA モードがアクティブ/スタンバイの場合は、フェイルオーバー モードを選択します。

オプション	説明
プリエンティブ	優先ノードが機能を停止してリカバリした場合、そのピアが先取りされ、アクティブ ノードになります。ピアの状態はスタンバイに変わります。
非プリエンティブ	優先ノードで障害が発生し、リカバリした場合、ピアがアクティブ ノードかどうか確認します。アクティブな場合、優先ノードがピアを先取りせず、スタンバイ ノードになります。

7 以前に作成した NSX Edge クラスタを選択します。

たとえば、Cluster Profile - 1 を選択します。

8 [保存] をクリックします。

Tier-0 ゲートウェイが作成されます。

9 [はい] を選択して、構成を続行します。

10 インターフェイスを設定します。

a [インターフェイス] を展開して、[設定] をクリックします。

b [インターフェイスの追加] をクリックします。

c 名前を入力します。

たとえば、TIER-0_VWT-UPLINK1 という名前を入力します。

d [タイプ] で [外部] を選択します。

e Edge 論理ルーター - アップリンク VLAN から IP アドレスを入力します。IP アドレスは、以前に作成した NSX Edge 仮想マシン用に設定した管理 IP アドレスとは異なる必要があります。

たとえば、10.197.154.1/24 です。

f [接続先] で、以前に作成した Tier-0 アップリンク セグメントを選択します。

たとえば、TIER-0-LS-UPLINK。

g リストから NSX Edge ノードを選択します。

たとえば、nsx-edge-1 です。

h [保存] をクリックします。

- i 2つ目のインターフェイスについて、手順 a ~ h を繰り返します。
たとえば、IP アドレス 10.197.154.2/24 で nsx-edge-2 Edge ノードに接続される 2 つ目のアップリンク TIER-0_VWT-UPLINK2 を作成します。
 - j [閉じる] をクリックします。
- 11 高可用性を構成するには、[HA VIP 構成] で [設定] をクリックします。
- a [HA VIP 構成の追加] をクリックします。
 - b IP アドレスを入力します。
たとえば、10.197.154.3/24。
 - c インターフェイスを選択します。
たとえば、TIER-0_VWT-UPLINK1 や TIER-0_VWT-UPLINK2 を選択します。
 - d [追加]、[適用] の順にクリックします。
- 12 ルーティングを構成するには、[ルーティング] をクリックします。
- a スタティック ルートで [設定] をクリックします。
 - b [スタティック ルートの追加] をクリックします。
 - c 名前を入力します。
たとえば、DEFAULT-STATIC-ROUTE です。
 - d ネットワーク IP アドレスとして 0.0.0.0/0 を入力します。
 - e ネクスト ホップを設定するには、[ネクスト ホップの設定] をクリックし、次に [ネクスト ホップの追加] をクリックします。
 - f ネクスト ホップ ルーターの IP アドレスを入力します。通常、これは NSX Edge 論理ルーター アップリンク VLAN からの管理ネットワーク VLAN のデフォルト ゲートウェイです。
たとえば、10.197.154.253 です。
 - g [追加]、[適用]、[保存] の順にクリックします。
 - h [閉じる] をクリックします。
- 13 (オプション) BGP を選択して、BGP ローカルおよびピアの詳細を構成します。
- 14 接続を確認するために、物理アーキテクチャの外部デバイスが、構成したアップリンクに対して ping を実行できることを確認します。

Edge Tier-0 ゲートウェイへの NSX ルート マップの構成

vSphere IaaS control plane をデプロイすると、eBGP モードの Edge Tier-0 ゲートウェイに作成されたルート マップに、拒否ルールのみ IP プリフィックスが追加されます。これによって、ToR スイッチにはルートがアドバタイズされなくなります。

Kubernetes ワークロード管理にのみ Edge クラスタを使用している場合は、オプション 1 に従って Tier-1 ルートアドバタイズを無効にします。その他のタスクに Edge クラスタを使用している場合は、オプション 2 に従って新しい許可ルールを作成します。

オプション 1: Tier-0 ゲートウェイを介した Tier-1 接続ネットワークのアドバタイズを無効にする

Tier-1 ゲートウェイに接続されたネットワークは、Tier-0 ゲートウェイから外部ネットワークにアドバタイズされません。

- 1 NSX Manager にログインします。
- 2 [ネットワーク] - [Tier-0 ゲートウェイ] の順に選択します。
- 3 [編集] をクリックします。
- 4 [アドバタイズされた Tier-1 サブネット] セクションで、[接続されたインターフェイスとセグメント] の選択を解除します。
- 5 [適用] をクリックし、[保存] をクリックします。

オプション 2: 新しい許可ルールを作成してルート再配布に適用する

vSphere IaaS control plane をデプロイすると、ルート マップに新しい拒否ルールが追加されます。そのため、IP プリフィックス リストとルート マップを許可する新しい許可ルールをルート マップに追加し、最後のルールとしてルート再配布ルールに適用する必要があります。

- 1 NSX Manager にログインします。
- 2 [ネットワーク] - [Tier-0 ゲートウェイ] の順に選択します。
- 3 新しい IP プリフィックス リストを作成します。
 - a [ルーティング] を展開します。
 - b IP プリフィックス リストの横にある 1 をクリックします。
 - c [IP プリフィックス リストの設定] ダイアログ ボックスで、[IP プリフィックス リストの追加] をクリックします。
 - d **test** などの名前を入力し、[設定] をクリックします。
 - e [プレフィックスの追加] をクリックします。
 - f [ネットワーク] で [すべて] をクリックし、[アクション] で [許可] を選択します。
 - g [適用] をクリックし、[保存] をクリックします。
- 4 手順 3 で作成した IP プリフィックス リストのルート マップを作成します。
 - a ルート マップの横にある [設定] をクリックします。
 - b [ルート マップの追加] をクリックします。
 - c IP プリフィックスを含んだ新しい一致条件を追加します。
 - d 手順 3 で作成した IP プリフィックスと [許可] アクションを選択します。
 - e [適用] をクリックし、[保存] をクリックします。

- 5 編集したルート マップをルート再配布に適用します。
 - a [Tier-0 ゲートウェイ] ページで、[ルート再配布] を展開し、[編集] をクリックします。
 - b [ルート マップ] 列のドロップダウン メニューから、手順 4 で作成したルート マップを選択します。
 - c [適用] をクリックし、[保存] をクリックします。

Tier-1 ゲートウェイの作成

Tier-1 ゲートウェイは通常、North バウンズの Tier-0 ゲートウェイと、South バウンズのセグメントに接続されています。

前提条件

Tier-0 ゲートウェイが作成されていることを確認します。

手順

- 1 NSX Manager にログインします。
- 2 [ネットワーク] - [Tier-1 ゲートウェイ] の順に選択します。
- 3 [Tier-1 ゲートウェイの追加] をクリックします。
- 4 ゲートウェイの名前を入力します。例：**ContainerAviT1**
- 5 この Tier-1 ゲートウェイに接続する Tier-0 ゲートウェイを選択します。例：**ContainerT0**。
- 6 NSX Edge クラスタを選択します。たとえば、**EDGECLUSTER1** を選択します。
- 7 NSX Edge クラスタを選択すると、NSX Edge ノードを選択するトグル オプションが表示されます。
- 8 フェイルオーバー モードを選択するか、デフォルト オプションの [非プリエンプティブ (Non-preemptive)] を受け入れます。
- 9 他の設定では、デフォルトのオプションを受け入れます。
- 10 [保存] をクリックします。
- 11 (オプション) サービス インターフェイス、スタティック ルート、マルチキャストの設定を構成します。デフォルト値を受け入れて問題ありません。

Tier-0 アップリンク セグメントとオーバーレイ セグメントの作成

Tier-0 アップリンク セグメントは、NSX から物理インフラストラクチャへの North-South 接続を提供します。オーバーレイ セグメントは、サービス エンジン管理 NIC に IP アドレスを提供します。

前提条件

Tier-0 ゲートウェイが作成されていることを確認します。

手順

- 1 NSX Manager にログインします。
- 2 [ネットワーク] - [セグメント] - [セグメントの追加] の順に選択します。

- 3 セグメントの名前を入力します。

例えば、TIER-0-LS-UPLINK です。

- 4 以前に作成したトランスポート ゾーンを選択します。

たとえば、vlanTZ を選択します。

- 5 [管理者ステータス] を切り替えて有効にします。

- 6 Tier-0 ゲートウェイの VLAN ID を入力します。

たとえば、1089 です。

- 7 [保存] をクリックします。

- 8 手順 2 ~ 7 を繰り返して、トランスポート ゾーン nsx-overlay-transportzone を持つオーバーレイ セグメント nsxoverlaysegment を作成します。

NSX を使用した vSphere IaaS control plane 用 NSX Advanced Load Balancer のインストールと構成

vSphere IaaS control plane 環境で NSX 4.1.1 以降のバージョンを使用している場合は、NSX Advanced Load Balancer 22.1.4 以降のバージョンをインストールして構成できます。

- 環境が、NSX Advanced Load Balancer を使用して vSphere IaaS control plane を構成するための要件を満たしていることを確認します。『vSphere IaaS 制御プレーンの概念と計画』の「Requirements for Zonal Supervisor with NSX and NSX Advanced Load Balancer」および「Requirements for Cluster Supervisor Deployment with NSX and NSX Advanced Load Balancer」を参照してください。
- NSX をインストールして構成します。
- NSX Advanced Load Balancer OVA をダウンロードします。VMware は、ワークロード管理を有効にする vSphere 環境にデプロイされる NSX Advanced Load Balancer OVA ファイルを提供しています。[VMware Customer Connect](#) ポータルから、vSphere IaaS control plane でサポートされている最新バージョンの OVA ファイルをダウンロードします。

注： このガイドの手順は、vSphere IaaS control plane 8.0 Update 2 でサポートされている NSX Advanced Load Balancer に関連しています。NSX Advanced Load Balancer の以降のバージョンの中に、入手可能な、ユーザー インターフェイス ワークフローが異なるバージョンが含まれている可能性があります。

NSX Advanced Load Balancer の詳細については、[VMware NSX Advanced Load Balancer のドキュメント](#)を参照してください。

ローカル コンテンツ ライブラリへの NSX Advanced Load Balancer OVA のインポート

NSX Advanced Load Balancer OVA イメージを保存するには、ローカル コンテンツ ライブラリを作成して、OVA をインポートします。

ローカル コンテンツ ライブラリを作成するには、ライブラリの構成、OVA ファイルのダウンロード、OVA ファイルのローカル コンテンツ ライブラリへのインポートを行います。詳細については、[コンテンツ ライブラリの使用](#)を参照してください。

前提条件

NSX Advanced Load Balancer OVA がダウンロードされていることを確認します。

ローカル コンテンツ ライブラリを作成します。「[コンテンツ ライブラリの作成と編集](#)」を参照してください。

手順

- 1 vSphere Client を使用して、vCenter Server にログインします。
- 2 [メニュー] - [コンテンツ ライブラリ] の順に選択します。
- 3 [コンテンツ ライブラリ] のリストから、作成したローカル コンテンツ ライブラリの名前のリンクをクリックします。例：[NSX ALB]。
- 4 [アクション] をクリックします。
- 5 [アイテムのインポート] を選択します。
- 6 [ライブラリ アイテムのインポート] ウィンドウで、[ローカル ファイル] を選択します。
- 7 [ファイルのアップロード] をクリックします。
- 8 ダウンロードした OVA ファイルを選択します。
- 9 [インポート] をクリックします。
- 10 画面の下部にある [最近のタスク] ペインを表示します。
- 11 [ライブラリ アイテムのコンテンツの取得] タスクを監視し、正常に [完了] になっていることを確認します。

次のステップ

NSX Advanced Load Balancer コントローラをデプロイします。[NSX Advanced Load Balancer コントローラのデプロイ](#)を参照してください。

NSX Advanced Load Balancer Controller のデプロイ

NSX Advanced Load Balancer Controller 仮想マシンを、vSphere IaaS control plane 環境内の管理ネットワークにデプロイします。

前提条件

- NSX Advanced Load Balancer をデプロイする管理ネットワークがあることを確認します。これは、vSphere Distributed Switch (vDS) または vSphere 標準スイッチ (vSS) のいずれかです。
- データ ネットワーク用の Distributed Switch およびポート グループが作成されていることを確認します。[NSX Advanced Load Balancer で使用する スーパーバイザー の vSphere Distributed Switch の作成](#)を参照してください。
- すべての前提条件を満たしていることを確認します。『vSphere IaaS 制御プレーンの概念と計画』の「[Requirements for Zonal Supervisor with NSX and NSX Advanced Load Balancer](#)」および「[Requirements for Cluster Supervisor Deployment with NSX and NSX Advanced Load Balancer](#)」を参照してください。

手順

- 1 vSphere Client を使用して、vCenter Server にログインします。
- 2 管理コンポーネント用に指定されている vSphere クラスタを選択します。
- 3 **AVI-LB** という名前のリソース プールを作成します。
- 4 リソース プールを右クリックして、[OVF テンプレートのデプロイ] を選択します。
- 5 [ローカル ファイル] を選択し [ファイルのアップロード] をクリックします。
- 6 前提条件としてダウンロードした controller-VERSION.ova ファイルを参照して選択します。
- 7 名前を入力し、コントローラのフォルダを選択します。

オプション	説明
仮想マシン名	avi-controller-1
仮想マシンの場所	[Datacenter]

- 8 コンピューティング リソースとして **AVI-LB** リソース プールを選択します。
- 9 構成の詳細を確認し、[次へ] をクリックします。
- 10 [仮想マシン ストレージ ポリシー] を選択します (**vsanDatastore** など)。
- 11 **network-1** などの管理ネットワークを選択します。
- 12 次のように構成をカスタマイズして、完了したら [次へ] をクリックします。

オプション	説明
管理インターフェイスの IP アドレス	コントローラ仮想マシンの IP アドレスを入力します (10.199.17.51 など)。
管理インターフェイスのサブネット マスク	サブネット マスクを入力します (255.255.255.0 など)。
デフォルト ゲートウェイ	管理ネットワークのデフォルト ゲートウェイを入力します (10.199.17.235 など)。
sysadmin ログイン認証キー	必要に応じて、パブリック キーの内容を貼り付けます。キーは空白のままにしておくこともできます。
Avi Controller のホスト名	コントローラの FQDN または IP アドレスを入力します。

- 13 展開設定を確認します。
- 14 [完了] をクリックして構成を完了します。
- 15 vSphere Client を使用して、[タスク] パネルでコントローラ仮想マシンのプロビジョニングを監視します。
- 16 コントローラ仮想マシンがデプロイされたら、vSphere Client を使用してパワーオンします。

コントローラ クラスタのデプロイ

必要に応じて、3 台のコントローラ ノードからなるクラスタをデプロイできます。HA およびディザスタ リカバリ用に、本番環境内にクラスタを構成することを推奨します。単一ノードの NSX Advanced Load Balancer コントローラを実行している場合は、バックアップとリストア機能を使用する必要があります。

3 ノード クラスタを実行するには、最初のコントローラ仮想マシンをデプロイした後、さらに 2 台のコントローラ仮想マシンをデプロイしてパワーオンします。初期構成ウィザードの実行や、これらのコントローラの管理者パスワードの変更が不要になります。最初のコントローラ仮想マシンの構成が、新しい 2 台のコントローラ仮想マシンに割り当てられます。

手順

- 1 [管理] - [コントローラ] の順に選択します。
- 2 [ノード] を選択します。
- 3 [編集] アイコンをクリックします。
- 4 [コントローラ クラスタ IP アドレス] に固定 IP アドレスを追加します。
この IP アドレスは、管理ネットワークから取得する必要があります。
- 5 [クラスタ ノード] で、新しい 2 台のクラスタ ノードを構成します。

オプション	説明
IP	コントローラ ノードの IP アドレス。
名前	ノードの名前。名前に IP アドレスを指定できます。
パスワード	コントローラ ノードのパスワード。パスワードは空のままにします。
パブリック IP アドレス	コントローラ ノードのパブリック IP アドレス。空のままにします。

- 6 [保存] をクリックします。

注： クラスタをデプロイした後の構成には、コントローラ ノードの IP アドレスではなく、コントローラ クラスタの IP アドレスを使用する必要があります。

コントローラのパワーオン

コントローラ仮想マシンをデプロイしたら、その仮想マシンをパワーオンできます。起動中に、デプロイ時に指定した IP アドレスが仮想マシンに割り当てられます。

パワーオン後、コントローラ仮想マシンの最初の起動プロセスが実行されるまで、最大 10 分かかる場合があります。

前提条件

コントローラをデプロイします。

手順

- 1 vCenter Server で、デプロイした avi-controller-1 仮想マシンを右クリックします。
- 2 [電源] - [パワーオン] の順に選択します。
仮想マシンに、デプロイ時に指定した IP アドレスが割り当てられます。
- 3 仮想マシンがパワーオン状態かどうかを確認するには、ブラウザで IP アドレスにアクセスします。
仮想マシンがオンラインになると、TLS 証明書と接続に関する警告が表示されます。
- 4 [接続はプライベートではありません] という警告で、[詳細を表示] をクリックします。

- 5 表示されるウィンドウで [この Web サイトを閲覧] をクリックします。

ユーザー認証情報を入力するように求められます。

NSX Advanced Load Balancer Controller の構成

NSX Advanced Load Balancer Controller 仮想マシンを vSphere IaaS control plane 環境に構成します。

ロード バランサ制御プレーンを vCenter Server 環境に接続するには、NSX Advanced Load Balancer Controller にデプロイ後の構成パラメータをいくつか指定する必要があります。

前提条件

- 環境が NSX Advanced Load Balancer を構成するためのシステム要件を満たしていることを確認します。『vSphere IaaS 制御プレーンの概念と計画』の「[Requirements for Zonal Supervisor with NSX and NSX Advanced Load Balancer](#)」および「[Requirements for Cluster Supervisor Deployment with NSX and NSX Advanced Load Balancer](#)」を参照してください。
- Enterprise Tier ライセンスを持っていることを確認します。コントローラは評価モードで起動します。評価モードでは、Enterprise Edition ライセンスに相当するすべての機能を使用できます。評価期間が終了する前に、有効な Enterprise Tier ライセンスをコントローラに割り当てる必要があります。

手順

- 1 ブラウザを使用して、NSX Advanced Load Balancer Controller のデプロイ時に指定した IP アドレスに移動します。
- 2 [管理者アカウント] を作成します。

オプション	説明
ユーザー名	初期構成に使用する管理者のユーザー名。このフィールドは編集できません。
パスワード	コントローラ仮想マシンの管理者パスワードを入力します。 パスワードには、数字、特殊文字、大文字、小文字の組み合わせを含む 8 文字以上を指定する必要があります。
パスワードの確認	管理者パスワードを再度入力します。
メール アドレス (オプション)	管理者のメール アドレスを入力します。 本番環境でのパスワード回復用のメール アドレスを指定することを推奨します。

- 3 [システム設定] を構成します。

オプション	説明
パスフレーズ	コントローラ バックアップのパスフレーズを入力します。コントローラ構成は、定期的にローカル ディスクに自動的にバックアップされます。詳細については、 バックアップとリストア を参照してください。 パスフレーズには、数字、特殊文字、大文字、小文字の組み合わせを含む 8 文字以上を指定する必要があります。
パスフレーズの確認	バックアップ パスフレーズを再度入力します。

オプション	説明
DNS リゾルバ	vSphere IaaS control plane 環境で使用している DNS サーバの IP アドレスを入力します。たとえば、10.14.7.12 など。
DNS 検索ドメイン	ドメイン文字列を入力します。

4 ライセンスを割り当てます。

- a [管理] - [ライセンス] を選択します。
- b [設定] を選択します。
- c [Enterprise Tier] を選択し、[保存] をクリックします。
- d ライセンスを追加するには、[コンピュータからアップロード] を選択します。

ライセンス ファイルをアップロードすると、コントローラのライセンス リストに表示されます。開始日や有効期限などのライセンスに関する情報が表示されます。

5 NSX Advanced Load Balancer Controller が NSX Manager と通信できるようにするには、NSX Manager の認証情報を作成します。NSX Advanced Load Balancer Controller ダッシュボードで、[管理] - [ユーザー認証情報 (User Credentials)] の順に選択します。

オプション	説明
名前	認証情報の名前。例： <code>nsxuser</code>
認証情報のタイプ	[NSX-T] を選択します。
ユーザー名	NSX Manager にログインするためのユーザー名を入力します。
パスワード	NSX Manager のパスワードを入力します。

6 NSX Advanced Load Balancer Controller が vCenter Server と通信できるようにするには、vCenter Server の認証情報を作成します。

オプション	説明
名前	認証情報の名前。例： <code>vcuser</code> 。
認証情報のタイプ	[[vCenter]] を選択します。
ユーザー名	vCenter Server にログインするためのユーザー名を入力します。
パスワード	vCenter Server のパスワードを入力します。

7 プレースホルダの IP アドレス管理プロファイルを作成します。

仮想サービスの作成時に仮想 IP アドレスを割り当てるには、IP アドレス管理が必要です。

- a NSX Advanced Load Balancer Controller ダッシュボードで、[テンプレート] - [IPAM/DNS プロファイル] の順に選択します。

[新しい IP アドレス管理/DNS プロファイル] 画面が表示されます。

- b プロファイルの名前を入力します。例：`default-ipam`。

- c [タイプ] を **Avi Vantage IPAM** として選択します。
 - d [保存] をクリックします。
- 8 [NSX Cloud] を構成します。
- a NSX Advanced Load Balancer Controller ダッシュボードで、[インフラストラクチャ] - [クラウド] の順に選択します。
 - b クラウドの名前を入力します。例：**nsx-cloud**
 - c クラウド タイプとして [NSX-T Cloud] を選択します。
 - d [DHCP] を選択します。
 - e サービス エンジンの [オブジェクト名プリフィックス] を入力します。プリフィックス文字列には、文字、数字、アンダースコアのみを使用できます。クラウドが構成されると、このフィールドは変更できなくなります。例：**nsx**
- 9 NSX の認証情報を入力します。
- a NSX Manager の IP アドレスを入力します。
 - b 作成した NSX Manager の認証情報を入力します。例：**nsxuser**。
- 10 管理ネットワークを構成します。管理ネットワークは、NSX Advanced Load Balancer Controller とサービス エンジンの間の通信チャンネルです。

オプション	説明
トランスポート ゾーン	サービス エンジンが配置されるトランスポート ゾーン。 オーバーレイ トランスポート ゾーンを選択します。例： nsx-overlay-transportzone
Tier1 論理ルーター	Tier-1 ゲートウェイを選択します。例： Tier-1_VWT 。
オーバーレイ セグメント	サービス エンジン管理 NIC が IP アドレスを取得する元の管理オーバーレイ セグメント。 例： nsxoverlaysegment 。

- 11 データ ネットワークを構成します。
- [データ ネットワーク] セクションで、[追加] をクリックします。

オプション	説明
トランスポート ゾーン	オーバーレイ トランスポート ゾーンを選択します。例： nsx-overlay-transportzone
論理ルーター	Tier-1 ゲートウェイを入力します。例： Tier-1_VWT 。
オーバーレイ セグメント	オーバーレイ セグメントを選択します。例： nsxoverlaysegment 。

12 vCenter Server 認証情報を入力します。

[vCenter Server] セクションで、[追加] をクリックします。

オプション	説明
名前	作成した認証情報の名前。例： vcuser 。
URL	vCenter Server の IP アドレス。

13 作成した IP アドレス管理プロファイルを追加します。[IPAM プロファイル] で、**default-ipam** を選択します。

仮想サービスの作成時に仮想 IP アドレスを割り当てるには、IP アドレス管理が必要です。

結果

構成が完了すると、NSX Advanced Load Balancer Controller の [ダッシュボード] が表示されます。[インフラストラクチャ] - [クラウド] の順に選択し、[NSX Cloud] の NSX Advanced Load Balancer Controller のステータスが緑であることを確認します。NSX Advanced Load Balancer Controller が vCenter Server 環境内のすべてのポート グループを検出してステータスが緑になるまで、しばらくの間、ステータスが黄色になることがあります。

次のステップ

サービス エンジン グループを構成します。[サービス エンジン グループの構成](#)を参照してください。

サービス エンジン グループの構成

vSphere IaaS control plane は、[Default-Group] をテンプレートとして使用し、スーパーバイザー ごとにサービス エンジン グループを構成します。必要に応じて、グループ内に [Default-Group] サービス エンジンを構成して、vCenter Server 内のサービス エンジン仮想マシンの配置と数を定義することができます。NSX Advanced Load Balancer Controller が Enterprise モードになっている場合は、高可用性を構成することもできます。

手順

- 1 NSX Advanced Load Balancer Controller ダッシュボードで、[インフラストラクチャ] - [クラウド リソース] - [サービス エンジン グループ] の順に選択します。
- 2 [サービス エンジン グループ] ページで、[Default-Group] の編集アイコンをクリックします。

[全般設定] タブが表示されます。

3 [高可用性と配置設定] セクションで、高可用性と仮想サービスの設定を構成します。

a [高可用性モード] を選択します。

デフォルトのオプションは N + M (buffer) です。デフォルト値をそのまま使用することも、次のいずれかのオプションを選択することもできます。

- Active/Standby
- Active/Active

b [サービス エンジンの数] を構成します。これは、サービス エンジン グループ内に作成できるサービス エンジンの最大数です。デフォルトは 10 です。

c [サービス エンジン間の仮想サービスの配置] を構成します。

デフォルトのオプションは [コンパクト] です。次のいずれかのオプションを選択できます。

- [配布済み]。NSX Advanced Load Balancer Controller は、新しくスピンアップされたサービス エンジンに仮想サービスを指定したサービス エンジンの最大数まで配置することで、パフォーマンスを最大化します。
- [コンパクト]。NSX Advanced Load Balancer Controller は、許容される最小限のサービス エンジンにスピンアップし、既存のサービス エンジンに新しい仮想サービスを配置します。新しいサービス エンジンは、すべてのサービス エンジンが使用されている場合にのみ作成されます。

4 その他の設定ではデフォルト値を使用できます。

5 [保存] をクリックします。

結果

AKO は、各 vSphere IaaS control plane クラスタごとに 1 つのサービス エンジン グループを作成します。サービス エンジン グループの構成は、[Default-Group] 構成から取得されます。[Default-Group] の必須の値が構成されると、AKO によって作成されるすべての新しいサービス エンジン グループの設定が同じになります。ただし、[Default-Group] 構成に加えた変更は、作成済みのサービス エンジン グループには反映されません。既存のサービス エンジン グループの構成は、個別に変更する必要があります。

NSX Advanced Load Balancer Controller の NSX Manager への登録

NSX Advanced Load Balancer Controller を NSX Manager に登録します。

前提条件

NSX Advanced Load Balancer Controller がデプロイされ、構成されていることを確認します。

手順

- 1 root ユーザーとして NSX Manager にログインします。
- 2 次のコマンドを実行します。

```
curl -k --location --request PUT 'https://<nsx-mgr-ip>/policy/api/v1/infra/alb-onboarding-workflow' \
--header 'X-Allow-Overwrite: True' \
--header 'Authorization: Basic <base64 encoding of username:password of NSX Mgr>' \
```

```
--header 'Content-Type: application/json' \
--data-raw '{
"owned_by": "LCM",
"cluster_ip": "<nsx-alb-controller-cluster-ip>",
"infra_admin_username" : "username",
"infra_admin_password" : "password"
}'
```

API 呼び出しで DNS 設定と NTP 設定を指定すると、グローバル設定がオーバーライドされます。たとえば、`"dns_servers": ["<dns-servers-ips>"]` および `"ntp_servers": ["<ntp-servers-ips>"]` などです。

NSX Advanced Load Balancer Controller への証明書の割り当て

NSX Advanced Load Balancer Controller は、クライアントに送信する証明書を使用してサイトを認証し、セキュアな通信を確立します。証明書は、NSX Advanced Load Balancer によって自己署名されるか、信頼されている (CA) に送信される証明書署名リクエスト (CSR) として作成され、そこで信頼できる証明書が生成されます。自己署名証明書を作成することも、外部証明書をアップロードすることもできます。

スーパーバイザーを有効にするには、カスタム証明書を指定する必要があります。デフォルトの証明書は使用できません。証明書の詳細については、「[SSL/TLS Certificates](#)」を参照してください。

プライベート認証局 (CA) 署名付き証明書を使用すると、スーパーバイザーのデプロイが完了せず、NSX Advanced Load Balancer 構成が適用されないことがあります。詳細については、『[NSX Advanced Load Balancer 構成が適用されない](#)』を参照してください。

前提条件

NSX Advanced Load Balancer が NSX Manager に登録されていることを確認します。

手順

- 1 コントローラ ダッシュボードで、左上隅にあるメニューをクリックして、[テンプレート] - [セキュリティ] の順に選択します。
- 2 [SSL/TLS 証明書] を選択します。
- 3 証明書を作成するには、[作成] をクリックし、[コントローラ証明書] を選択します。
[新しい証明書 (SSL/TLS)] ウィンドウが表示されます。
- 4 証明書の名前を入力します。

- 5 事前に作成された有効な証明書がない場合は、[タイプ] に Self Signed を選択して自己署名証明書を追加します。

- a 次の詳細を入力します。

オプション	説明
共通名	サイトの完全修飾名を指定します。サイトが信頼されていると見なされるには、このエントリがクライアントのブラウザに入力されたホスト名と一致する必要があります。
アルゴリズム	EC (楕円曲線暗号) または RSA を選択します。EC が推奨です。
キーのサイズ	ハンドシェイクに使用する暗号化のレベルを選択します。 <ul style="list-style-type: none"> ■ SECP256R1 は EC 証明書に使用されます。 ■ RSA 証明書には 2048 ビットが推奨です。

- b [サブジェクト代替名 (SAN)] で、[追加] をクリックします。

- c NSX Advanced Load Balancer Controller が単一ノードとしてデプロイされている場合は、クラスタの IP アドレスまたは FQDN、あるいは両方を入力します。IP アドレスまたは FQDN のみが使用されている場合は、これがデプロイ時に指定した NSX Advanced Load Balancer Controller 仮想マシンの IP アドレスと一致する必要があります。

[NSX Advanced Load Balancer Controller のデプロイ](#)を参照してください。NSX Advanced Load Balancer Controller クラスタが 3 ノードのクラスタとしてデプロイされている場合は、クラスタの IP アドレスまたは FQDN を入力します。

- d [保存] をクリックします。

この証明書は、ワークロード管理機能を有効にするよう スーパーバイザー を構成する場合に必要になります。

- 6 作成した自己署名証明書をダウンロードします。

- a [セキュリティ] - [SSL/TLS 証明書] の順に選択します。

証明書が表示されない場合は、ページを更新します。

- b 作成した証明書を選択し、ダウンロード アイコンをクリックします。

- c 表示された [証明書のエクスポート] 画面で、証明書に対して [クリップボードにコピー] をクリックします。キーをコピーしないでください。

- d 後でワークロード管理の有効化の際に使用するためにコピーした証明書を保存します。

- 7 事前に作成された有効な証明書がある場合は、[タイプ] に Import を選択してアップロードします。

- a [証明書] で [ファイルのアップロード] をクリックして、証明書をインポートします。

アップロードする証明書の SAN フィールドには、コントローラのクラスタ IP アドレスまたは FQDN が必要です。

注： 証明書の内容をアップロードまたは貼り付けるのは、必ず 1 回だけにしてください。

- b [キー (PEM) または PKCS12] で [ファイルのアップロード] をクリックして、キーをインポートします。

- c [検証] をクリックして、証明書とキーを検証します。
 - d [保存] をクリックします。
- 8 証明書を変更するには、次の手順を実行します。
- a コントローラ ダッシュボードで、[管理] - [システム設定] の順に選択します。
 - b [編集] をクリックします。
 - c [アクセス] タブを選択します。
 - d [SSL/TLS 証明書] で、既存のデフォルト ポータル証明書を削除します。
 - e ドロップダウンで、新しく作成した証明書またはアップロードした証明書を選択します。
 - f [基本認証] を選択します。
 - g [保存] をクリックします。

NSX Advanced Load Balancer の使用に関する制限事項

vSphere IaaS control plane 環境で NSX Advanced Load Balancer を構成する場合は注意が必要です。

次の場合、Ingress は NSX Advanced Load Balancer から外部 IP アドレスを取得しません。

- Ingress の構成でホスト名が指定されていない場合。
- Ingress がホスト名ではなく defaultBackend 構成オプションを使用して構成されている場合。

デフォルトでは、Kubernetes の Ingress リソースは、外部 IP アドレスを割り当てるために、コントローラ構成でホスト名を定義する必要があります。この処理が必要なのは、NSX Advanced Load Balancer では Kubernetes Ingress に対応して作成される仮想サービスのトラフィックに仮想ホスティングを使用するためです。defaultBackend 構成オプションの詳細については、<https://kubernetes.io/docs/concepts/services-networking/ingress/#default-backend> を参照してください。

Ingress のホスト名が別の名前空間の Ingress と同じ場合、その Ingress は NSX Advanced Load Balancer から外部 IP アドレスを取得しません。デフォルトでは、NSX Advanced Load Balancer は名前空間ごとに一意の VIP を割り当てます。つまり、1つの名前空間内のすべての Ingress が同じ VIP を共有します。そのため、異なる名前空間からの 2つの Ingress には個別の VIP が割り当てられます。ただし、これらの Ingress のホスト名が同じである場合、DNS サーバはホスト名を解決するための IP アドレスを認識できません。

NSX Advanced Load Balancer のインストールと構成

vSphere Distributed Switch (vDS) ネットワークを使用している場合は、vSphere IaaS control plane 環境に NSX Advanced Load Balancer 22.1.4 をインストールして、構成することができます。

- 環境が、NSX Advanced Load Balancer を使用して vSphere IaaS control plane を構成するための要件を満たしていることを確認します。『vSphere IaaS 制御プレーンの概念と計画』の [Requirements for a Three-Zone Supervisor with NSX Advanced Load Balancer](#) および [Requirements for Enabling a Single Cluster Supervisor with NSX Advanced Load Balancer](#) を参照してください。

- NSX Advanced Load Balancer OVA をダウンロードします。VMware は、ワークロード管理を有効にする vSphere 環境にデプロイされる NSX Advanced Load Balancer OVA ファイルを提供しています。
VMware Customer Connect ポータルから、vSphere IaaS control plane でサポートされている最新バージョンの OVA ファイルをダウンロードします。

注： このガイドの手順は、vSphere IaaS control plane 8.0 Update 2 でサポートされている NSX Advanced Load Balancer に関連しています。NSX Advanced Load Balancer の以降のバージョンの中に、入手可能な、ユーザー インターフェイス ワークフローが異なるバージョンが含まれている可能性があります。

NSX Advanced Load Balancer の詳細については、[VMware NSX Advanced Load Balancer のドキュメント](#)を参照してください。

次に参照するドキュメント

手順

- 1 [NSX Advanced Load Balancer で使用する スーパーバイザー の vSphere Distributed Switch の作成](#)
vSphere ネットワーク スタックおよび NSX Advanced Load Balancer を使用する スーパーバイザー として vSphere クラスタを構成するには、vSphere Distributed Switch を作成する必要があります。Distributed Switch 上で スーパーバイザー のワークロード ネットワークとして構成できるポート グループを作成します。NSX Advanced Load Balancer にサービス エンジン データ インターフェイスを接続するには、分散ポート グループが必要です。分散ポート グループは、アプリケーションの仮想 IP アドレス (VIP) をサービス エンジンに配置するために使用されます。
- 2 [ローカル コンテンツ ライブラリへの NSX Advanced Load Balancer OVA のインポート](#)
NSX Advanced Load Balancer OVA イメージを保存するには、ローカル コンテンツ ライブラリを作成して、OVA をインポートします。
- 3 [NSX Advanced Load Balancer コントローラのデプロイ](#)
NSX Advanced Load Balancer コントローラ仮想マシンを、vSphere IaaS control plane 環境内の管理 ネットワークにデプロイします。
- 4 [サービス エンジン グループの構成](#)
vSphere IaaS control plane では、サービス エンジン グループとして [Default-Group] が使用されます。必要に応じて、グループ内に [Default-Group] サービス エンジン構成して、vCenter Server 内のサービス エンジン仮想マシンの配置と数を定義することができます。NSX Advanced Load Balancer Controller が Enterprise モードになっている場合は、高可用性を構成することもできます。vSphere IaaS control plane では、[Default-Group] サービス エンジンのみがサポートされています。他のサービス エンジン グループを作成することはできません。

NSX Advanced Load Balancer で使用する スーパーバイザー の vSphere Distributed Switch の作成

vSphere ネットワーク スタックおよび NSX Advanced Load Balancer を使用する スーパーバイザー として vSphere クラスタを構成するには、vSphere Distributed Switch を作成する必要があります。Distributed Switch 上で スーパーバイザー のワークロード ネットワークとして構成できるポート グループを作成します。NSX Advanced Load Balancer にサービス エンジン データ インターフェイスを接続するには、分散ポート グループ

ループが必要です。分散ポート グループは、アプリケーションの仮想 IP アドレス (VIP) をサービス エンジンに配置するために使用されます。

前提条件

NSX Advanced Load Balancer で スーパーバイザー の vSphere ネットワーク使用するためのシステム要件とネットワーク トポロジを確認します。『vSphere IaaS 制御プレーンの概念と計画』の [Requirements for a Three-Zone Supervisor with NSX Advanced Load Balancer](#) および [Requirements for Enabling a Single Cluster Supervisor with NSX Advanced Load Balancer](#) を参照してください。

手順

- 1 vSphere Client で、データセンターに移動します。
- 2 データセンターを右クリックして、[Distributed Switch] - [新しい Distributed Switch] の順に選択します。
- 3 スイッチの名前 (**ワークロード Distributed Switch** など) を入力して、[次へ] をクリックします。
- 4 スイッチのバージョン 8.0 を選択して、[次へ] をクリックします。
- 5 [ポート グループ名] に **プライマリ ワークロード ネットワーク** と入力し、[次へ] をクリックして [終了] をクリックします。

1つのポート グループを持つ新しい Distributed Switch がデータセンターに作成されます。このポート グループは、作成する スーパーバイザー のプライマリ ワークロード ネットワークとして使用できます。プライマリ ワークロード ネットワークは、Kubernetes 制御プレーン仮想マシンのトラフィックを処理します。

- 6 ワークロード ネットワークの分散ポート グループを作成します。

作成するポート グループの数は、スーパーバイザー 用に実装するトポロジによって異なります。隔離されたワークロード ネットワークが1つ含まれるトポロジの場合は、スーパーバイザー のすべての名前空間用のネットワークとして使用する分散ポート グループを1つ作成します。ネットワークが名前空間ごとに隔離されているトポロジの場合は、作成する名前空間と同じ数のポート グループを作成します。

- a 新しく作成した Distributed Switch に移動します。
- b スイッチを右クリックして、[分散ポート グループ] - [新規分散ポート グループ] の順に選択します。
- c ポート グループの名前 (**ワークロード ネットワーク** など) を入力して、[次へ] をクリックします。
- d デフォルトのままにして、[次へ] をクリックし、[終了] をクリックします。

7 データ ネットワークのポート グループを作成します。

- a Distributed Switch を右クリックして、[分散ポート グループ] - [新規分散ポート グループ] を選択します。
- b ポート グループの名前（**データ ネットワーク** など）を入力して、[次へ] をクリックします。
- c [設定の構成] 画面で新規分散ポート グループの全般プロパティを入力し、[次へ] をクリックします。

プロパティ	説明
ポート バインド	この分散ポート グループに接続された仮想マシンにポートを割り当てるときに選択します。 [静的バインド] を選択すると、仮想マシンが分散ポート グループに接続されるときに仮想マシンにポートを割り当てます。
ポートの割り当て	ポート割り当てとして [弾性] を選択します。 デフォルトのポート数は 8 個です。すべてのポートが割り当てられたら、新しい 8 組のポートが作成されます。
ポート数	デフォルト値を保持します。
ネットワーク リソース プール	ドロップダウン メニューで、新しい分散ポート グループをユーザー定義のネットワーク リソース プールに割り当てます。ネットワーク リソース プールを作成していない場合、このメニューは空です。
VLAN	ドロップダウン メニューで VLAN トラフィックのフィルタリングおよびマーキングのタイプを選択します。 <ul style="list-style-type: none"> ■ [なし]：VLAN を使用しません。外部スイッチ タギングを使用している場合は、このオプションを選択します。 ■ [VLAN]：[VLAN ID] テキスト ボックスに、仮想スイッチ タギング用の値を 1～4,094 の範囲で入力します。 ■ [VLAN トランク]：仮想ゲスト タギングを行って、VLAN トラフィックに ID を設定してゲスト OS に送信するには、このオプションを使用します。VLAN トランク 範囲を入力します。コンマ区切りリストを使用して複数の範囲や個々の VLAN を設定できます。たとえば、1702-1705、1848-1849 です。 ■ [プライベート VLAN]：トラフィックと、Distributed Switch で作成されたプライベート VLAN を関連付けます。プライベート VLAN を作成していない場合、このメニューは空です。
詳細	このオプションは選択解除したままにします。

8 [設定の確認] 画面で構成を確認し、[完了] をクリックします。

結果

Distributed Switch が作成され、Distributed Switch の下に分散ポート グループが表示されます。以上で、作成したポート グループを NSX Advanced Load Balancer の [データ ネットワーク] として使用できます。

ローカル コンテンツ ライブラリへの NSX Advanced Load Balancer OVA のインポート

NSX Advanced Load Balancer OVA イメージを保存するには、ローカル コンテンツ ライブラリを作成して、OVA をインポートします。

ローカル コンテンツ ライブラリを作成するには、ライブラリの構成、OVA ファイルのダウンロード、OVA ファイルのローカル コンテンツ ライブラリへのインポートを行います。詳細については、[コンテンツ ライブラリの使用](#)を参照してください。

前提条件

NSX Advanced Load Balancer OVA がダウンロードされていることを確認します。

ローカル コンテンツ ライブラリを作成します。「[コンテンツ ライブラリの作成と編集](#)」を参照してください。

手順

- 1 vSphere Client を使用して、vCenter Server にログインします。
- 2 [メニュー] - [コンテンツ ライブラリ] の順に選択します。
- 3 [コンテンツ ライブラリ] のリストから、作成したローカル コンテンツ ライブラリの名前のリンクをクリックします。例：[NSX ALB]。
- 4 [アクション] をクリックします。
- 5 [アイテムのインポート] を選択します。
- 6 [ライブラリ アイテムのインポート] ウィンドウで、[ローカル ファイル] を選択します。
- 7 [ファイルのアップロード] をクリックします。
- 8 ダウンロードした OVA ファイルを選択します。
- 9 [インポート] をクリックします。
- 10 画面の下部にある [最近のタスク] ペインを表示します。
- 11 [ライブラリ アイテムのコンテンツの取得] タスクを監視し、正常に [完了] になっていることを確認します。

次のステップ

NSX Advanced Load Balancer コントローラをデプロイします。[NSX Advanced Load Balancer コントローラのデプロイ](#)を参照してください。

NSX Advanced Load Balancer コントローラのデプロイ

NSX Advanced Load Balancer コントローラ仮想マシンを、vSphere IaaS control plane 環境内の管理ネットワークにデプロイします。

前提条件

- NSX Advanced Load Balancer をデプロイする管理ネットワークがあることを確認します。これは、vSphere Distributed Switch (vDS) または vSphere 標準スイッチ (vSS) のいずれかです。
- データ ネットワーク用の Distributed Switch およびポートグループが作成されていることを確認します。[NSX Advanced Load Balancer で使用する スーパーバイザー の vSphere Distributed Switch の作成](#)を参照してください。

- すべての前提条件を満たしていることを確認します。『vSphere IaaS 制御プレーンの概念と計画』の [Requirements for a Three-Zone Supervisor with NSX Advanced Load Balancer](#) および [Requirements for Enabling a Single Cluster Supervisor with NSX Advanced Load Balancer](#) を参照してください。

手順

- 1 vSphere Client を使用して、vCenter Server にログインします。
- 2 管理コンポーネント用に指定されている vSphere クラスタを選択します。
- 3 **AVI-LB** という名前のリソース プールを作成します。
- 4 リソース プールを右クリックして、[OVF テンプレートのデプロイ] を選択します。
- 5 [ローカル ファイル] を選択し [ファイルのアップロード] をクリックします。
- 6 前提条件としてダウンロードした `controller-VERSION.ova` ファイルを参照して選択します。
- 7 名前を入力し、コントローラのフォルダを選択します。

オプション	説明
仮想マシン名	<code>avi-controller-1</code>
仮想マシンの場所	[Datacenter]

- 8 コンピューティング リソースとして **AVI-LB** リソース プールを選択します。
- 9 構成の詳細を確認し、[次へ] をクリックします。
- 10 [仮想マシン ストレージ ポリシー] を選択します (`vsanDatastore` など)。
- 11 `network-1` などの管理ネットワークを選択します。
- 12 次のように構成をカスタマイズして、完了したら [次へ] をクリックします。

オプション	説明
管理インターフェイスの IP アドレス	コントローラ仮想マシンの IP アドレスを入力します (10.199.17.51 など)。
管理インターフェイスのサブネット マスク	サブネット マスクを入力します (255.255.255.0 など)。
デフォルト ゲートウェイ	管理ネットワークのデフォルト ゲートウェイを入力します (10.199.17.235 など)。
sysadmin ログイン認証キー	必要に応じて、パブリック キーの内容を貼り付けます。キーは空白のままにしておくこともできます。
Avi Controller のホスト名	コントローラの FQDN または IP アドレスを入力します。

- 13 展開設定を確認します。
- 14 [完了] をクリックして構成を完了します。
- 15 vSphere Client を使用して、[タスク] パネルでコントローラ仮想マシンのプロビジョニングを監視します。
- 16 コントローラ仮想マシンがデプロイされたら、vSphere Client を使用してパワーオンします。

コントローラ クラスタのデプロイ

必要に応じて、3 台のコントローラ ノードからなるクラスタをデプロイできます。HA およびディザスタ リカバリ用に、本番環境内にクラスタを構成することを推奨します。単一ノードの NSX Advanced Load Balancer コントローラを実行している場合は、バックアップとリストア機能を使用する必要があります。

3 ノード クラスタを実行するには、最初のコントローラ仮想マシンをデプロイした後、さらに 2 台のコントローラ仮想マシンをデプロイしてパワーオンします。初期構成ウィザードの実行や、これらのコントローラの管理者パスワードの変更が不要になります。最初のコントローラ仮想マシンの構成が、新しい 2 台のコントローラ仮想マシンに割り当てられます。

手順

- 1 [管理] - [コントローラ] の順に選択します。
- 2 [ノード] を選択します。
- 3 [編集] アイコンをクリックします。
- 4 [コントローラ クラスタ IP アドレス] に固定 IP アドレスを追加します。
この IP アドレスは、管理ネットワークから取得する必要があります。
- 5 [クラスタ ノード] で、新しい 2 台のクラスタ ノードを構成します。

オプション	説明
IP	コントローラ ノードの IP アドレス。
名前	ノードの名前。名前に IP アドレスを指定できます。
パスワード	コントローラ ノードのパスワード。パスワードは空のままにします。
パブリック IP アドレス	コントローラ ノードのパブリック IP アドレス。空のままにします。

- 6 [保存] をクリックします。

注： クラスタをデプロイした後の構成には、コントローラ ノードの IP アドレスではなく、コントローラ クラスタの IP アドレスを使用する必要があります。

コントローラのパワーオン

コントローラ仮想マシンをデプロイしたら、その仮想マシンをパワーオンできます。起動中に、デプロイ時に指定した IP アドレスが仮想マシンに割り当てられます。

パワーオン後、コントローラ仮想マシンの最初の起動プロセスが実行されるまで、最大 10 分かかる場合があります。

前提条件

コントローラをデプロイします。

手順

- 1 vCenter Server で、デプロイした avi-controller-1 仮想マシンを右クリックします。

2 [電源] - [パワーオン] の順に選択します。

仮想マシンに、デプロイ時に指定した IP アドレスが割り当てられます。

3 仮想マシンがパワーオン状態かどうかを確認するには、ブラウザで IP アドレスにアクセスします。

仮想マシンがオンラインになると、TLS 証明書と接続に関する警告が表示されます。

4 [接続はプライベートではありません] という警告で、[詳細を表示] をクリックします。

5 表示されるウィンドウで [この Web サイトを閲覧] をクリックします。

ユーザー認証情報を入力するように求められます。

コントローラの構成

vSphere IaaS control plane 環境でコントローラ仮想マシンを構成し、クラウドを設定します。

ロード バランサ制御プレーンを vCenter Server 環境に接続するには、コントローラにデプロイ後の構成パラメータをいくつか指定する必要があります。コントローラの初期構成では、最初のコントローラがデプロイされた場所に Default-cloud クラウドが作成されます。ロード バランサが複数の vCenter Server または複数のデータセンターにサービスを提供できるようにするには、vCenter Server とデータセンターの組み合わせごとに VMware vCenter タイプのカスタム クラウドを作成します。詳細については、「[NSX Advanced Load Balancer コンポーネント](#)」を参照してください。

前提条件

- 環境が NSX Advanced Load Balancer を構成するためのシステム要件を満たしていることを確認します。
『vSphere IaaS 制御プレーンの概念と計画』の [Requirements for a Three-Zone Supervisor with NSX Advanced Load Balancer](#) および [Requirements for Enabling a Single Cluster Supervisor with NSX Advanced Load Balancer](#) を参照してください。
- コントローラをデプロイします。

手順

- 1 ブラウザを使用して、コントローラのデプロイ時に指定した IP アドレスに移動します。
- 2 [管理者アカウント] を作成します。

オプション	説明
ユーザー名	初期構成に使用する管理者のユーザー名。このフィールドは編集できません。
パスワード	コントローラ仮想マシンの管理者パスワードを入力します。 パスワードには、数字、特殊文字、大文字、小文字の組み合わせを含む 8 文字以上を指定する必要があります。
パスワードの確認	管理者パスワードを再度入力します。
メール アドレス (オプション)	管理者のメール アドレスを入力します。 本番環境でのパスワード回復用のメール アドレスを指定することを推奨します。

3 [システム設定] を構成します。

オプション	説明
パスフレーズ	コントローラ バックアップのパスフレーズを入力します。コントローラ構成は、定期的にローカル ディスクに自動的にバックアップされます。詳細については、 バックアップとリストア を参照してください。 パスフレーズには、数字、特殊文字、大文字、小文字の組み合わせを含む 8 文字以上を指定する必要があります。
パスフレーズの確認	バックアップ パスフレーズを再度入力します。
DNS リゾルバ	vSphere IaaS control plane 環境で使用している DNS サーバの IP アドレスを入力します。たとえば、10.14.7.12 など。
DNS 検索ドメイン	ドメイン文字列を入力します。

4 (オプション) [E メール/SMTP] 設定を構成します。

オプション	説明
SMTP ソース	[なし]、[ローカル ホスト]、[SMTP サーバ]、[匿名サーバ] のいずれかのオプションを選択します。 デフォルトは [ローカル ホスト] です。
送信元アドレス	メール アドレス。

5 [次へ] をクリックします。

6 マルチテナントを構成します。

- a デフォルトのテナント アクセスを維持します。
- b [以下の後にクラウドをセットアップ] を選択して、[保存] をクリックします。

注： 保存する前に [以下の後にクラウドをセットアップ] オプションを選択しなかった場合は、初期構成ウィザードが終了します。クラウド構成ウィンドウは自動的に起動せず、コントローラのダッシュボードビューに移動します。この場合は、[インフラストラクチャ] - [クラウド] の順に移動して、クラウドを構成します。

7 [VMware vCenter/vSphere ESX] クラウドを構成します。[作成] をクリックし、クラウド タイプとして [VMware vCenter/vSphere ESX] を選択します。

[新規クラウド] 設定画面が表示されます。

8 [全般] 設定を構成します。

オプション	説明
名前	クラウドの名前を入力します。たとえば、 Custom-Cloud とします。
タイプ	クラウド タイプは [VMware vCenter/vSphere ESX] です。

- 9 (オプション) [デフォルトのネットワーク IP アドレス管理] セクションで、[DHCP 有効] を選択します (vSphere ポート グループで DHCP が使用可能な場合)。

サービス エンジン インターフェイスで固定 IP アドレスのみを使用する場合は、このオプションを選択解除したままにします。これは、ネットワークごとに個別に構成できます。

詳細については、『[仮想 IP ネットワークの構成](#)』を参照してください。

- 10 [仮想サービス配置] 設定を構成します。

オプション	説明
仮想サービス配置用の直接接続ネットワークより固定ルートを優先	サービス エンジン仮想マシンからサーバ ネットワークにアクセスする際にデフォルト ゲートウェイを経由するように設定するには、このオプションを選択します。 デフォルトでは、コントローラは NIC をサーバ ネットワークに直接接続します。ユーザーはサービス エンジンにデータ ネットワークにのみ強制的に接続し、ワークロード ネットワークにルーティングする必要があります。
VIP のネットワーク解決にスタティック ルートを使用	このオプションは選択解除したままにします。

- 11 [vCenter Server/vSphere] 認証情報を構成します。

[認証情報の設定] をクリックし、次の詳細を入力します。

オプション	説明
vCenter Server アドレス	vSphere IaaS control plane 環境の vCenter Server のホスト名または IP アドレスを入力します。
ユーザー名	vCenter Server 管理者ユーザー名を入力します (administrator@vsphere.local など)。より少ない権限を使用するには、専用ロールを作成します。詳細については、 VMware ユーザー ロール を参照してください。
パスワード	ユーザー パスワードを入力します。
アクセス権	[読み取り]: サービス エンジン仮想マシンを作成および管理します。 [書き込み]: コントローラでサービス エンジン仮想マシンが作成および管理されます。 [書き込み] を選択する必要があります。

- 12 [データセンター] を設定します。

- [ワークロード管理] を有効にする vSphere [データセンター] を選択します。
- [コンテンツ ライブラリを使用] オプションを選択し、リストからローカル コンテンツ ライブラリを選択します。

- 13 [保存して再起動] を選択し、構成した設定で [VMware vCenter/vSphere ESX] クラウドを作成します。

14 [ネットワーク] 設定を構成します。

オプション	説明
管理ネットワーク	[仮想マシン ネットワーク] を選択します。このネットワーク インターフェイスは、サービス エンジンがコントローラに接続するために使用されます。
サービス エンジン	[テンプレート サービス エンジン グループ] は空のままにします。
管理ネットワーク IP アドレス管理	[DHCP 有効] を選択します。

15 (オプション) [DHCP 有効] を選択しなかった場合のみ、次のネットワーク設定を構成します。

オプション	説明
IP サブネット	管理ネットワークの IP サブネットを入力します。たとえば、10.199.32.0/24 です。 注: DHCP を使用できない場合にのみ、IP サブネットを入力します。
デフォルト ゲートウェイ	管理ネットワークのデフォルト ゲートウェイを入力します (10.199.32.253 など)。 注: DHCP を使用できない場合にのみ、IP サブネットを入力します。
固定 IP アドレス プールの追加	1 つ以上の IP アドレスまたは IP アドレス範囲を入力します。たとえば、10.99.32.62-10.199.32.65 です。 注: DHCP を使用できない場合にのみ、IP サブネットを入力します。

16 IP アドレス管理プロファイルを作成し、[IP アドレス管理/DNS] 設定を構成します。

仮想サービスの作成時に仮想 IP アドレスを割り当てるには、IP アドレス管理が必要です。

- a [IP アドレス管理プロファイル] の [その他のアクション] メニューで、[作成] を選択します。

[新しい IP アドレス管理/DNS プロファイル] 画面が表示されます。

- b [IP アドレス管理プロファイル] を構成します。

オプション	説明
名前	ユーザー定義の文字列 (<code>ipam-profile</code> など)
タイプ	[AVI Vantage の IP アドレス管理] を選択します
VRF での IP アドレスの割り当て	このオプションを選択解除します。
クラウド	ドロップダウン リストから [Custom-Cloud] を選択します。

- c [使用可能なネットワーク] で [追加] をクリックし、構成した仮想 IP ネットワークを選択します。このネットワークはプライマリ ネットワークです。

- d [保存] をクリックします。

17 (オプション) 内部 NTP サーバを使用する場合は、NTP 設定を構成します。

- a [管理] - [設定] - [DNS/NTP] の順に選択します。

- b 既存の NTP サーバがある場合は削除し、使用している DNS サーバの IP アドレスを入力します。たとえば、192.168.100.1 のように入力します。

結果

構成が完了すると、コントローラ [ダッシュボード] が表示されます。[インフラストラクチャ] - [クラウド] の順に選択し、[Custom-Cloud] のコントローラのステータスが緑であることを確認します。コントローラが vCenter Server 環境内のすべてのポート グループを検出してステータスが緑になるまで、しばらくの間、ステータスが黄色になることがあります。

ライセンスの追加

NSX Advanced Load Balancer を構成したら、ライセンスを追加する必要があります。コントローラは評価モードで起動します。評価モードでは、Enterprise Edition ライセンスに相当するすべての機能を使用できます。評価期間が終了する前に、有効な Enterprise Tier ライセンスをコントローラに割り当てる必要があります。

前提条件

Enterprise Tier ライセンスを持っていることを確認します。

手順

- 1 NSX Advanced Load Balancer Controller ダッシュボードで、[管理] - [ライセンス] の順に選択します。
- 2 [設定] を選択します。
- 3 [Enterprise Tier] を選択します。
- 4 [保存] をクリックします。
- 5 ライセンスを追加するには、[コンピュータからアップロード] を選択します。

ライセンス ファイルをアップロードすると、コントローラのライセンス リストに表示されます。開始日や有効期限などのライセンスに関する情報が表示されます。

コントローラへの証明書の割り当て

コントローラは、安全な通信を確立するために証明書をクライアントに送信する必要があります。この証明書には、NSX Advanced Load Balancer Controller クラスタのホスト名または IP アドレスと一致する [Subject Alternative Name (SAN)] が必要です。

コントローラにはデフォルトの自己署名の証明書があります。ただし、この証明書には正しい SAN がありません。正しい SAN を持つ有効な証明書または自己署名証明書に置き換える必要があります。自己署名証明書を作成するか、外部証明書をアップロードします。

証明書の詳細については、[Avi のドキュメント](#)を参照してください。

手順

- 1 コントローラ ダッシュボードで、左上隅にあるメニューをクリックして、[テンプレート] - [セキュリティ] の順に選択します。
- 2 [SSL/TLS 証明書] を選択します。
- 3 証明書を作成するには、[作成] をクリックし、[コントローラ証明書] を選択します。
[新しい証明書 (SSL/TLS)] ウィンドウが表示されます。
- 4 証明書の名前を入力します。

- 5 事前に作成された有効な証明書がない場合は、[タイプ] に Self Signed を選択して自己署名証明書を追加します。

- a 次の詳細を入力します。

オプション	説明
共通名	サイトの完全修飾名を指定します。サイトが信頼されていると見なされるには、このエントリがクライアントのブラウザに入力されたホスト名と一致する必要があります。
アルゴリズム	EC (楕円曲線暗号) または RSA を選択します。EC が推奨です。
キーのサイズ	ハンドシェイクに使用する暗号化のレベルを選択します。 <ul style="list-style-type: none"> ■ SECP256R1 は EC 証明書に使用されます。 ■ RSA 証明書には 2048 ビットが推奨です。

- b [サブジェクト代替名 (SAN)] で、[追加] をクリックします。
- c Avi Controller が単一ノードとしてデプロイされている場合は、クラスタの IP アドレスまたは FQDN、あるいは両方を入力します。IP アドレスまたは FQDN のみが使用されている場合は、これがデプロイ時に指定したコントローラ仮想マシンの IP アドレスと一致する必要があります。

[NSX Advanced Load Balancer コントローラのデプロイ](#)を参照してください。

NSX Advanced Load Balancer Controller クラスタが 3 ノードのクラスタとしてデプロイされている場合は、クラスタの IP アドレスまたは FQDN を入力します。3 コントローラ ノードで構成するクラスタのデプロイの詳細については、[コントローラ クラスタのデプロイ](#)を参照してください。

- d [保存] をクリックします。

この証明書は、ワークロード管理機能を有効にするよう スーパーバイザー を構成する場合に必要になります。

- 6 作成した自己署名証明書をダウンロードします。

- a [セキュリティ] - [SSL/TLS 証明書] の順に選択します。

証明書が表示されない場合は、ページを更新します。

- b 作成した証明書を選択し、ダウンロード アイコンをクリックします。

- c 表示された [証明書のエクスポート] 画面で、証明書に対して [クリップボードにコピー] をクリックします。キーをコピーしないでください。

- d 後でワークロード管理の有効化の際に使用するためにコピーした証明書を保存します。

- 7 事前に作成された有効な証明書がある場合は、[タイプ] に Import を選択してアップロードします。

- a [証明書] で [ファイルのアップロード] をクリックして、証明書をインポートします。

アップロードする証明書の SAN フィールドには、コントローラのクラスタ IP アドレスまたは FQDN が必要です。

注： 証明書の内容をアップロードまたは貼り付けるのは、必ず 1 回だけにしてください。

- b [キー (PEM) または PKCS12] で [ファイルのアップロード] をクリックして、キーをインポートします。

- c [検証] をクリックして、証明書とキーを検証します。
 - d [保存] をクリックします。
- 8 ポータル証明書を変更するには、次の手順を実行します。
- a コントローラ ダッシュボードで、[管理] - [システム設定] の順に選択します。
 - b [編集] をクリックします。
 - c [アクセス] タブを選択します。
 - d [SSL/TLS 証明書] で、既存のデフォルト ポータル証明書を削除します。
 - e ドロップダウンで、新しく作成した証明書またはアップロードした証明書を選択します。
 - f [基本認証] を選択します。
 - g [保存] をクリックします。

サービス エンジン グループの構成

vSphere IaaS control plane では、サービス エンジン グループとして [Default-Group] が使用されます。必要に応じて、グループ内に [Default-Group] サービス エンジンを構成して、vCenter Server 内のサービス エンジン仮想マシンの配置と数を定義することができます。NSX Advanced Load Balancer Controller が Enterprise モードになっている場合は、高可用性を構成することもできます。vSphere IaaS control plane では、[Default-Group] サービス エンジンのみがサポートされています。他のサービス エンジン グループを作成することはできません。

フェイルオーバーの場合に十分なキャパシティをプロビジョニングする方法については、『[Avi ドキュメント](#)』を参照してください。

手順

- 1 [NSX Advanced Load Balancer Controller] ダッシュボードで、[インフラストラクチャ] - [クラウド リソース] - [サービス エンジン グループ] の順に選択します。
- 2 [サービス エンジン グループ] ページで、[Default-Group] の編集アイコンをクリックします。
[全般設定] タブが表示されます。
vSphere IaaS control plane では、[Default-Cloud] のみがサポートされています。
- 3 [配置] セクションで、[高可用性モード] を選択します。
デフォルトのオプションは N + M (buffer) です。デフォルト値をそのまま使用することも、次のいずれかのオプションを選択することもできます。
 - Active/Standby
 - Active/Active
- 4 [サービス エンジン] セクションでは、サービス エンジン グループに十分なキャパシティを構成できます。
[サービス エンジンの数] オプションでは、サービス エンジン グループ内に作成できるサービス エンジンの最大数を定義します。デフォルトは 10 です。

十分なキャパシティを構成するには、[バッファ サービス エンジン] で値を指定します。指定する値は、フェイルオーバーの際に十分なキャパシティを確保するためにデプロイされる仮想マシンの数です。

デフォルトは **1** です。

- 5 [仮想サービス] セクションで、次のオプションを構成します。

オプション	説明
サービス エンジンごとの仮想サービス数	コントローラ クラスターがグループ内の任意のサービス エンジンに配置できる仮想サービスの最大数。 値 1000 を入力します。
サービス エンジン間の仮想サービスの配置	[分散] を選択します。このオプションを選択すると、新しくスピンアップされたサービス エンジンに仮想サービスを指定したサービス エンジンの最大数まで配置することで、パフォーマンスが最大化されます。デフォルトは [コンパクト] です。

- 6 その他の設定ではデフォルト値を使用できます。

- 7 [保存] をクリックします。

固定ルートの構成

デフォルト ゲートウェイを構成すると、サービス エンジンはワークロード ネットワーク上のプール サーバにトラフィックをルーティングできるようになります。データ ネットワーク ゲートウェイの IP アドレスをデフォルト ゲートウェイとして構成する必要があります。サービス エンジンは、データ ネットワークの DHCP からデフォルト ゲートウェイの IP アドレスを取得しません。サービス エンジンがワークロード ネットワークおよびクライアント IP アドレスにトラフィックを適切にルーティングできるように、スタティック ルートを構成する必要があります。

手順

- [NSX Advanced Load Balancer Controller] ダッシュボードで、[インフラストラクチャ] - [クラウド リソース] - [VRF コンテキスト] の順に選択します。
- [作成] をクリックします。
- [全般] 設定で、ルーティング コンテキストの名前を入力します。
- [固定ルート] セクションで、[追加] をクリックします。
- [ゲートウェイ サブネット] に 172.16.10.0/24 と入力します。
- [ネクスト ホップ] に、データ ネットワークのゲートウェイ IP アドレスを入力します。
たとえば、192.168.1.1 です。
- (オプション) [BGP ピアリング] を選択して、BGP ローカルおよびピアの詳細を構成します。
詳細については、[Avi のドキュメント](#)を参照してください。
- [保存] をクリックします。

仮想 IP ネットワークの構成

データ ネットワークの仮想 IP アドレス (VIP) サブネットを構成します。仮想サービスが特定の VIP ネットワークに配置されている場合に使用する VIP 範囲を構成できます。サービス エンジンに対して DHCP を構成できます。

DHCP が使用できない場合は、必要に応じて、該当するネットワーク上のサービス エンジン インターフェイスに割り当てられる IP アドレス プールを構成できます。vSphere IaaS control plane では、単一の VIP ネットワークのみがサポートされています。

手順

- 1 [NSX Advanced Load Balancer コントローラ] ダッシュボードで、[インフラストラクチャ] - [クラウド リソース] - [ネットワーク] の順に選択します。
- 2 リストからクラウドを選択します。
たとえば、[Default-Cloud] を選択します。
- 3 ネットワークの名前を入力します。
たとえば、Data Network など。
- 4 データ ネットワークで DHCP が使用可能な場合は、[DHCP 有効] を選択したままにします。
DHCP を使用できない場合は、このオプションを選択解除します。
- 5 [IPv6 自動構成の有効化] を選択します。
仮想マシンがネットワーク上で実行されていて、タイプが [検出済み] と表示される場合、NSX Advanced Load Balancer Controller はネットワークの CIDR を自動的に検出します。
- 6 NSX Advanced Load Balancer Controller が IP サブネットを自動的に検出する場合は、サブネットの IP アドレス範囲を構成します。
 - a 設定を編集します。
 - b [サブネット プリフィックス] を入力します。
 - c サービス エンジンの IP アドレスに DHCP を使用できる場合は、[VIP と SE に固定 IP アドレスを使用] を選択解除します。
 - d 1 つ以上の IP アドレスまたは IP アドレス範囲を入力します。
たとえば、10.202.35.1-10.202.35.254 など。

注: 0 で終わる IP アドレスを入力できます。たとえば、192.168.0.0 です。表示される警告は無視してください。

 - e [保存] をクリックします。
- 7 コントローラで IP サブネットとそのタイプが検出されない場合は、次の手順を実行します。
 - a [追加] をクリックします。
 - b [サブネット プリフィックス] を入力します。
 - c [追加] をクリックします。
 - d サービス エンジンの IP アドレスに DHCP を使用できる場合は、[VIP と SE に固定 IP アドレスを使用] を選択解除します。

- e [IP アドレス] で、仮想 IP アドレスを提供するネットワークの CIDR を入力します。

たとえば、10.202.35.0/22。

- f 1つ以上の IP アドレスまたは IP アドレス範囲を入力します。

範囲は [IP サブネット] のネットワーク CIDR のサブネットである必要があります。たとえば、10.202.35.1-10.202.35.254 など。

注: 0 で終わる IP アドレスを入力できます。たとえば、192.168.0.0 です。表示される警告は無視してください。

- g [保存] をクリックして、サブネットの構成を保存します。

[ネットワーク] 画面には、タイプが [構成済み] の IP サブネットと IP アドレス プールが一覧表示されます。

- 8 [保存] をクリックして、ネットワーク設定を保存します。

結果

[ネットワーク] 画面には、構成済みのネットワークが一覧表示されます。

例

Primary Workload Network ネットワークには、検出されたネットワークが 10.202.32.0/22 として、構成されたサブネットが 10.202.32.0/22 [254/254] としてそれぞれ表示されます。これは、254 の仮想 IP アドレスが 10.202.32.0/22 からのものであることを示します。サマリ ビューには、IP アドレス範囲 10.202.35.1-10.202.35.254 は一覧表示されません。

NSX Advanced Load Balancer のテスト

NSX Advanced Load Balancer 制御プレーンをデプロイして構成したら、その機能を確認します。

手順

- 1 Avi Controller ダッシュボードで、[インフラストラクチャ] - [クラウド] の順に移動します。

- 2 [デフォルト クラウド] のコントローラのステータスが緑色であることを確認します。

発生する可能性のある問題のトラブルシューティングについては、[NSX Advanced Load Balancer のトラブルシューティングのためのサポート バンドルの収集](#)を参照してください。

HAProxy ロード バランサのインストールと構成

VMware では、vSphere IaaS control plane 環境で使用できるオープン ソースの HAProxy ロード バランサの実装を提供しています。[ワークロード管理] に vSphere Distributed Switch (vDS) ネットワークを使用している場合は、HAProxy ロード バランサをインストールして、構成することができます。

HAProxy ロード バランサで使用する スーパーバイザー の vSphere Distributed Switch の作成

vSphere ネットワーク スタックおよび HAProxy ロード バランサを使用する スーパーバイザー として vSphere クラスタを構成するには、vSphere Distributed Switch にホストを追加する必要があります。

Distributed Switch 上で、スーパーバイザー のワークロード ネットワークとして構成するポート グループを作成する必要があります。

クラスターで実行される Kubernetes ワークロードに指定した隔離のレベルに応じて、スーパーバイザー のさまざまなトポロジから選択できます。

前提条件

- HAProxy ロード バランサでスーパーバイザー の vSphere ネットワークを使用するためのシステム要件を確認します。『vSphere IaaS 制御プレーンの概念と計画』の [Requirements for Enabling a Three-Zone Supervisor with HA Proxy Load Balancer](#) および [Requirements for Enabling a Single-Cluster Supervisor with VDS Networking and HAProxy Load Balancer](#) を参照してください。
- スーパーバイザー で HAProxy を使用してワークロード ネットワークを設定するトポロジを判別します。『vSphere IaaS 制御プレーンの概念と計画』の [HAProxy ロード バランサをデプロイするトポロジ](#) を参照してください。

手順

- 1 vSphere Client で、データセンターに移動します。
- 2 データセンターを右クリックして、[Distributed Switch] - [新しい Distributed Switch] の順に選択します。
- 3 スイッチの名前（**ワークロード Distributed Switch** など）を入力して、[次へ] をクリックします。
- 4 スイッチのバージョン 7.0 を選択して、[次へ] をクリックします。
- 5 [ポート グループ名] に **プライマリ ワークロード ネットワーク** と入力し、[次へ] をクリックして [終了] をクリックします。

1つのポート グループを持つ新しい Distributed Switch がデータセンターに作成されます。このポート グループは、作成するスーパーバイザー のプライマリ ワークロード ネットワークとして使用できます。プライマリ ワークロード ネットワークは、Kubernetes 制御プレーン仮想マシンのトラフィックを処理します。

- 6 ワークロード ネットワークの分散ポート グループを作成します。

作成するポート グループの数は、スーパーバイザー 用に実装するトポロジによって異なります。隔離されたワークロード ネットワークが1つ含まれるトポロジの場合は、スーパーバイザー のすべての名前空間用のネットワークとして使用する分散ポート グループを1つ作成します。ネットワークが名前空間ごとに隔離されているトポロジの場合は、作成する名前空間と同じ数のポート グループを作成します。

- a 新しく作成した Distributed Switch に移動します。
 - b スイッチを右クリックして、[分散ポート グループ] - [新規分散ポート グループ] の順に選択します。
 - c ポート グループの名前（**ワークロード ネットワーク** など）を入力して、[次へ] をクリックします。
 - d デフォルトのままにして、[次へ] をクリックし、[終了] をクリックします。
- 7 スーパーバイザー として構成する vSphere クラスターのホストを Distributed Switch に追加します。
 - a Distributed Switch を右クリックして、[ホストの追加と管理] を選択します。
 - b [ホストの追加] を選択します。

- c [新規ホスト] をクリックし、スーパーバイザーとして構成する vSphere クラスタからホストを選択して [次へ] をクリックします。
- d 各ホストから物理 NIC を選択して、Distributed Switch 上のアップリンクに割り当てます。
- e ウィザードの残りの各画面で [次へ] をクリックし、最後に [終了] をクリックします。

結果

ホストが Distributed Switch に追加されます。以上で、スイッチ上に作成したポート グループをスーパーバイザーのワークロード ネットワークとして使用できます。

HAProxy ロード バランサ制御プレーン仮想マシンのデプロイ

Kubernetes ワークロードに vSphere ネットワーク スタックを使用する場合は、HAProxy 制御プレーン仮想マシンをインストールして、Tanzu Kubernetes クラスタにロード バランシング サービスを提供します。

前提条件

- 環境が HA プロキシをデプロイするためのコンピューティング要件とネットワーク要件を満たしていることを確認します。『vSphere IaaS 制御プレーンの概念と計画』の [Requirements for Enabling a Three-Zone Supervisor with HA Proxy Load Balancer](#) および [Requirements for Enabling a Single-Cluster Supervisor with VDS Networking and HAProxy Load Balancer](#) を参照してください。
- HAProxy ロード バランサをデプロイする vSphere 標準スイッチまたは Distributed Switch 上に管理ネットワークが配置されていることを確認します。スーパーバイザーは管理ネットワーク上の HAProxy ロード バランサと通信します。
- ワークロード ネットワーク用の vSphere Distributed Switch とポート グループを作成します。HAProxy ロード バランサは、ワークロード ネットワーク経由でスーパーバイザー および Tanzu Kubernetes クラスタのノードと通信します。HAProxy ロード バランサで使用するスーパーバイザーの vSphere Distributed Switch の作成を参照してください。ワークロード ネットワークについては、『vSphere IaaS 制御プレーンの概念と計画』のスーパーバイザー クラスタのワークロード ネットワークを参照してください。
- [VMware-HAProxy サイト](#) から最新バージョンの VMware HAProxy OVA ファイルをダウンロードします。
- スーパーバイザーに HAProxy ロード バランサとワークロード ネットワークをデプロイするためのトポロジを選択します。『vSphere IaaS 制御プレーンの概念と計画』の [HAProxy ロード バランサをデプロイするトポロジ](#) を参照してください。

Distributed Switch ネットワークおよび HAProxy と vSphere IaaS control plane の併用方法を示すデモが役立つ場合があります。「[Getting Started Using vSphere with Tanzu](#)」のビデオを確認してください。

手順

- 1 vSphere Client を使用して、vCenter Server にログインします。

2 HAProxy OVA ファイルから新しい仮想マシンを作成します。

オプション	説明
コンテンツ ライブラリ	<p>OVA をローカル コンテンツ ライブラリにインポートした場合：</p> <ul style="list-style-type: none"> ■ [メニュー]-[コンテンツ ライブラリ]の順に選択します。 ■ OVA をインポートしたライブラリを選択します。 ■ vmware-haproxy-vX.X.X テンプレートを 選択します。 ■ 右クリックして、[このテンプレートから仮想マシンを新規作成]を選択します。
ローカル ファイル	<p>OVA ファイルをローカル ホストにダウンロードした場合：</p> <ul style="list-style-type: none"> ■ [ワークロード管理]を有効にする vCenter Server クラスタを選択します。 ■ 右クリックして [OVF テンプレートのデプロイ]を選択します。 ■ [ローカル ファイル]を選択し [ファイルのアップロード]をクリックします。 ■ vmware-haproxy-vX.X.X.ovf ファイルを参照して選択します。

- 3 [仮想マシン名] に **haproxy** などの名前を入力します。
- 4 HAProxy をデプロイする [データセンター] 選択して、[次へ] をクリックします。
- 5 [ワークロード管理] を有効にする vCenter Server クラスタを選択して、[次へ] をクリックします。
- 6 デプロイの詳細を確認して、[次へ] をクリックします。
- 7 使用許諾契約書を承諾して、[次へ] をクリックします。
- 8 デプロイの設定を選択してください。詳細については、『vSphere IaaS 制御プレーンの概念と計画』の [HAProxy ネットワーク トポロジ](#)を参照してください。

構成	説明
デフォルト	管理ネットワーク用と単一ワークロード ネットワーク用の 2 つの NIC を持つアプライアンスをデプロイする場合は、このオプションを選択します。
フロントエンド ネットワーク	3 つの NIC を持つアプライアンスをデプロイする場合は、このオプションを選択します。フロントエンド サブネットは、開発者がクラスタ制御プレーンにアクセスするために使用するネットワークからクラスタ ノードを隔離する場合に使用されます。

- 9 仮想マシンに使用するストレージ ポリシーを選択し、[次へ] をクリックします。

10 ロード バランサに使用するネットワーク インターフェイスを選択し、[次へ] をクリックします。

ソース ネットワーク	ターゲット ネットワーク
管理	仮想マシン ネットワークなどの管理ネットワークを選択します。
ワークロード	[ワークロード管理] 用に構成された Distributed Switch ポートグループを選択します。
フロントエンド	フロントエンド サブネットに構成された Distributed Switch ポートグループを選択します。フロントエンド構成を選択しなかった場合、この設定はインストール中に無視されるため、デフォルトのままにすることができます。

注： ワークロード ネットワークは、管理ネットワークとは別のサブネットに配置してください。『vSphere IaaS 制御プレーンの概念と計画』の [Requirements for Enabling a Three-Zone Supervisor with HA Proxy Load Balancer](#) および [Requirements for Enabling a Single-Cluster Supervisor with VDS Networking and HAProxy Load Balancer](#) を参照してください。

- 11 アプリケーション構成設定をカスタマイズします。 [アプライアンスの設定](#) を参照してください。
- 12 ネットワーク構成の詳細を指定します。 [ネットワークの構成](#) を参照してください。
- 13 ロード バランシングを構成します。 [ロード バランシングの設定](#) を参照してください。
- 14 [次へ] をクリックして、OVA の構成を完了します。
- 15 デプロイ構成の詳細を確認し、[完了] をクリックして OVA をデプロイします。
- 16 [タスク] パネルを使用して、仮想マシンのデプロイを監視します。
- 17 仮想マシンのデプロイが完了したら、パワーオンします。

次のステップ

HAProxy ロード バランサが正常に展開されて、パワーオンされたら、[ワークロード管理] の有効化を続行します。
[12 章 スーパーバイザー の構成と管理](#) を参照してください。

HAProxy ロード バランサのカスタマイズ

構成設定、ネットワーク設定、ロード バランシング設定などを行って、HAProxy 制御プレーン仮想マシンをカスタマイズします。

アプライアンスの設定

次の表に、HAProxy アプライアンス構成のパラメータの一覧と説明を示します。

パラメータ	説明	注釈または例
root パスワード	root ユーザーの初期パスワード (6 ~ 128 文字)。	以降のパスワード変更は、オペレーティング システムで実行する必要があります。
root ログインの許可	root ユーザーに、SSH を使用して仮想マシンにリモートでログインすることを許可するオプション。	root ログインはトラブルシューティングのために必要になることがありますが、root ログインを許可した場合のセキュリティ面の影響を考慮する必要があります。

パラメータ	説明	注釈または例
TLS 認証局 (ca.crt)	自己署名 CA 証明書を使用するには、このフィールドを空白のままにします。 独自の CA 証明書 (ca.crt) を使用するには、証明書の内容をこのフィールドに貼り付けます。 Base64 によるコンテンツのエンコードが必要になる場合があります。 https://www.base64encode.org/	自己署名 CA 証明書を使用している場合は、証明書からパブリック キーとプライベート キーが生成されます。
キー (ca.key)	自己署名証明書を使用している場合は、このフィールドを空白のままにします。 CA 証明書を指定した場合は、このフィールドに証明書のプライベート キーの内容を貼り付けます。	

ネットワークの構成

次の表に、HAProxy ネットワーク構成のパラメータの一覧と説明を示します。

パラメータ	説明	注釈または例
ホスト名	HAProxy 制御プレーン仮想マシンに割り当てるホスト名 (または FQDN)	デフォルト値: haproxy.local
DNS	DNS サーバの IP アドレスのカンマ区切りリスト。	デフォルト値: 1.1.1.1, 1.0.0.1 値の例: 10.8.8.8
管理 IP	管理ネットワーク上の HAProxy 制御プレーン仮想マシンの固定 IP アドレス。	ネットワークのプリフィックス長を含む有効な IPv4 アドレス (例: 192.168.0.2/24)。
管理ゲートウェイ	管理ネットワークのゲートウェイの IP アドレス。	例: 192.168.0.1
ワークロード IP アドレス	ワークロード ネットワーク上の HAProxy 制御プレーン仮想マシンの固定 IP アドレス。 この IP アドレスには、ロード バランサの IP アドレス範囲外のアドレスを指定する必要があります。	ネットワークのプリフィックス長を含む有効な IPv4 アドレス (例: 192.168.10.2/24)。
ワークロード ゲートウェイ	ワークロード ネットワークのゲートウェイの IP アドレス。	例: 192.168.10.1 フロントエンド構成を選択した場合は、ゲートウェイを入力する必要があります。フロントエンドが選択されていても、ゲートウェイが指定されていない場合、デプロイは正常に実行されません。
フロントエンド IP アドレス	フロントエンド ネットワーク上の HAProxy アプライアンスの固定 IP アドレス。 この値は、フロントエンド デプロイ モデルが選択されている場合のみ使用されます。	ネットワークのプリフィックス長を含む有効な IPv4 アドレス (例: 192.168.100.2/24)。
フロントエンド ゲートウェイ	フロントエンド ネットワークのゲートウェイの IP アドレス。 この値は、フロントエンド デプロイ モデルが選択されている場合のみ使用されます。	例: 192.168.100.1

ロード バランシングの設定

次の表に、HAProxy ロード バランサ構成のパラメータの一覧と説明を示します。

パラメータ	説明	例または注釈
ロード バランサの IP アドレス範囲	<p>このフィールドには、CIDR 形式を使用する IPv4 アドレスの範囲を指定します。値には有効な CIDR 範囲を指定する必要があります。指定しなかった場合、インストールは失敗します。</p> <p>HAProxy は、仮想 IP アドレス (VIP) 用の IP アドレスを予約します。割り当てが完了すると、各仮想 IP アドレスが割り当てられ、HAProxy はそのアドレスで要求に回答します。</p> <p>vSphere Client を使用して vCenter Server で [ワークロード管理] を有効にした場合、ここで指定する CIDR 範囲と仮想サーバに割り当てる IP アドレスが重複することはできません。</p> <p>注： ロード バランサの IP アドレス範囲は、管理ネットワークとは異なるサブネットに配置する必要があります。管理ネットワークと同じサブネット上にロード バランサの IP アドレス範囲を設定することはできません。</p>	<p>たとえば、ネットワーク CIDR 192.168.100.0/24 は、ロード バランサに 256 個の仮想 IP アドレスを提供します (各アドレスの範囲は 192.168.100.0 - 192.168.100.255)。</p> <p>たとえば、ネットワーク CIDR 192.168.100.0/25 は、ロード バランサに 128 個の仮想 IP アドレスを提供します (各アドレスの範囲は 192.168.100.0 - 192.168.100.127)。</p>
データプレーン API の管理ポート	ロード バランサの API サービスが待機する HAProxy 仮想マシンのポート。	有効なポート。ポート 22 は SSH 用に予約されています。デフォルト値は 5556 です。
HAProxy のユーザー ID	ロード バランサ API のユーザー名	<p>クライアントがロード バランサの API サービスの認証に使用するユーザー名です。</p> <p>注： このユーザー名は、スーパーバイザーを有効にするときに必要になります。</p>
HAProxy のパスワード	ロード バランサ API のパスワード	<p>クライアントがロード バランサの API サービスの認証に使用するパスワードです。</p> <p>注： このパスワードは、スーパーバイザーを有効にするときに必要になります。</p>

3 ゾーン スーパーバイザー のデプロイ

5

3 つの vSphere Zones でスーパーバイザー をデプロイして、クラスタ レベルの高可用性を実現します。各 vSphere Zone は、vSphere クラスタにマッピングされます。

注: vSphere IaaS control plane 環境を 8.0 よりも前のバージョンの vSphere からアップグレードした場合、Tanzu Kubernetes Grid クラスタなどの環境に vSphere Zones を使用するには、新しい 3 ゾーン スーパーバイザー を作成する必要があります。

次のトピックを参照してください。

- [VDS ネットワーク スタックを使用する 3 ゾーン スーパーバイザー のデプロイ](#)
- [NSX ネットワークを使用する 3 ゾーン スーパーバイザー のデプロイ](#)

VDS ネットワーク スタックを使用する 3 ゾーン スーパーバイザー のデプロイ

3 つの vSphere Zone に VDS ネットワーク スタックを使用する スーパーバイザー をデプロイする方法を確認します。各 vSphere Zone は、1 つの vSphere クラスタにマッピングされます。スーパーバイザー を 3 つの vSphere Zone にデプロイすることで、ワークロードにクラスタ レベルで高可用性を提供できます。VDS ネットワークが構成された スーパーバイザー では、仮想マシン サービスから作成された Tanzu Kubernetes Grid クラスタおよび仮想マシンがサポートされます。vSphere ポッド はサポートされません。

前提条件

- vSphere クラスタを スーパーバイザー として構成するための前提条件を満たすこと。vSphere クラスタで [vSphere IaaS control plane](#) を構成するための前提条件を参照してください。
- 3 つの vSphere Zones を作成します。3 章 [マルチゾーン スーパーバイザー デプロイ用の vSphere Zones の作成](#)を参照してください。

手順

- 1 ホーム メニューから、[ワークロード管理] を選択します。
- 2 スーパーバイザー のライセンス オプションを選択します。
 - 有効な Tanzu エディション ライセンスを所有している場合は、[ライセンスの追加] をクリックして、vSphere のライセンス インベントリにライセンス キーを追加します。

- Tanzu エディション ライセンスをまだ所有していない場合は、VMware からの連絡を受信できるように、連絡先の詳細を入力してから、[開始する] をクリックします。

スーパーバイザー の評価期間は、60 日間です。この期間内に、有効な Tanzu エディション ライセンスをクラスタに割り当てる必要があります。Tanzu エディション ライセンス キーを追加した場合は、スーパーバイザー の設定を完了した後、60 日の評価期間内にそのキーを割り当てることができます。

- 3 [ワークロード管理] 画面で、[開始する] を再度クリックします。
- 4 [vCenter Server とネットワーク] 画面を選択し、vCenter Server デプロイ用にセットアップされているスーパーバイザー システムを選択し、ネットワーク スタックとして [vSphere Distributed Switch (VDS)] を選択して、[次へ] をクリックします。
- 5 [スーパーバイザーの配置] 画面で、[vSphere Zone のデプロイ] を選択して 3 つの vSphere Zones にスーパーバイザー をデプロイします。
 - a 新しいスーパーバイザー の名前を入力します。
 - b スーパーバイザー をデプロイするための vSphere Zones を作成したデータセンターを選択します。
 - c 互換性のある vSphere Zones のリストから、3 つのゾーンを選択します。
 - d [次へ] をクリックします。
- 6 [ストレージ] 画面で、制御プレーン仮想マシンを配置するためのストレージを構成します。

オプション	説明
制御プレーン ノード	制御プレーン仮想マシンを配置するためのストレージ ポリシーを選択します。

7 [ロード バランサ] 画面で、ロード バランサの設定を入力します。

- a ロード バランサの名前を指定します。
- b ロード バランサのタイプを選択します。

[NSX Advanced Load Balancer] と [HAProxy] から選択できます。

- c ロード バランサの設定を構成します。
 - NSX Advanced Load Balancer の場合は次の設定を入力します。

オプション	説明
[名前]	NSX Advanced Load Balancer の名前を入力します。
[NSX Advanced Load Balancer コントローラ エンドポイント]	NSX Advanced Load Balancer Controller の IP アドレス。 デフォルトのポートは 443 です。
[ユーザー名]	NSX Advanced Load Balancer を使用して構成されたユーザー名。このユーザー名は、コントローラへのアクセスに使用します。
[パスワード]	ユーザー名のパスワード。
[サーバ証明書]	コントローラによって使用される証明書。 構成時に割り当てた証明書を指定できます。 詳細については、 コントローラへの証明書の割り当て を参照してください。
[クラウド名]	設定したカスタム クラウドの名前を入力します。クラウド名では大文字と小文字が区別されます。 [Default-Cloud] を使用する場合は、このフィールドを空のままにします。 詳細については、『 コントローラの構成 』を参照してください。

- HAProxy の場合は次の設定を入力します。

オプション	説明
[HAProxy ロード バランサ コントローラ エンドポイント]	HAProxy アプライアンスの管理 IP アドレスである、HAProxy データ プレーン API の IP アドレスとポート。このコンポーネントは、HAProxy サーバを制御し、HAProxy 仮想マシン内で実行されます。
[ユーザー名]	HAProxy OVA ファイルを使用して構成されたユーザー名。この名前は、HAProxy データ プレーン API での認証に使用します。
[パスワード]	ユーザー名のパスワード。
[仮想 IP アドレスの範囲]	Tanzu Kubernetes クラスタによってワークロード ネットワークで使用される IP アドレスの範囲。この IP アドレス範囲は、HAProxy アプライアンスのデプロイ時に構成した CIDR で定義された IP アドレスのリストから取得されます。HAProxy デプロイで構成された範囲の全体を設定できますが、その CIDR のサブセットを設定することで、複数の スーパーバイザー を作成してその CIDR 範囲の IP アドレスを使用することもできま

オプション	説明
	<p>す。この範囲は、このウィザードでワークロード ネットワーク用に定義されている IP アドレス範囲と重複することはできません。また、この範囲は、このワークロード ネットワークの DHCP 範囲とも重複することができません。</p>
[HAProxy 管理 TLS 証明書]	<p>署名済みの PEM 形式の証明書、またはデータ プレーン API によって提供されるサーバ証明書の信頼できるルートである PEM 形式の証明書。</p> <ul style="list-style-type: none"> ■ オプション 1: root アクセスが有効な場合に、HAProxy 仮想マシンに root として SSH 接続し、[サーバ認証局] に /etc/haproxy/ca.crt をコピーします。 \n 形式のエスケープ行を使用しないでください。 ■ オプション 2: HAProxy 仮想マシンを右クリックし、[設定の編集] を選択します。適切なフィールドから CA 証明書をコピーし、https://www.base64decode.org/ などの変換ツールを使用して Base64 から変換します。 ■ オプション 3: 次の PowerCLI スクリプトを実行します。変数 \$vc、\$vc_user、\$vc_password の値を適切な値に置き換えます。 <pre> \$vc = "10.21.32.43" \$vc_user = "administrator@vsphere.local" \$vc_password = "PASSWORD" Connect-VIServer -User \$vc_user -Password \$vc_password -Server \$vc \$VMname = "haproxy-demo" \$AdvancedSettingName = "guestinfo.dataplaneapi.cacert" \$Base64cert = get-vm \$VMname Get- AdvancedSetting -Name \$AdvancedSettingName while ([string]::IsNullOrEmpty(\$Base64cert .Value)) { Write-Host "Waiting for CA Cert Generation... This may take a under 5-10 minutes as the VM needs to boot and generate the CA Cert (if you haven't provided one already)."<!-- \$Base64cert = get-vm \$VMname Get-AdvancedSetting -Name \$AdvancedSettingName Start-sleep -seconds 2 } Write-Host "CA Cert Found... Converting from BASE64" \$cert = [Text.Encoding]::Utf8.GetString([Con vert]::FromBase64String(\$Base64cert. Value)) Write-Host \$cert </pre--> </pre>

8 [管理ネットワーク] 画面で、Kubernetes 制御プレーン仮想マシンに使用されるネットワークのパラメータを構成します。

a [ネットワーク モード] を選択します。

- [DHCP ネットワーク]。このモードでは、制御プレーン仮想マシンの IP アドレス、フローティング IP アドレス、DNS サーバ、DNS、検索ドメイン、NTP サーバなど、管理ネットワークのすべての IP アドレスが DHCP サーバから自動的に取得されます。フローティング IP アドレスを取得するためには、クライアント ID をサポートするように DHCP サーバを構成する必要があります。DHCP モードでは、すべての制御プレーン仮想マシンが安定した DHCP クライアント ID を使用して IP アドレスを取得します。これらのクライアント ID を使用すると、DHCP サーバ上の制御プレーン仮想マシンの IP アドレスに対して固定 IP アドレス割り当てを設定して、IP アドレスが変更されないようにすることができます。制御プレーン仮想マシンの IP アドレスとフローティング IP アドレスの変更はサポートされていません。

DHCP から継承された一部の設定をオーバーライドするには、これらの設定のテキスト フィールドに値を入力します。

オプション	説明
[ネットワーク]	スーパーバイザー の管理トラフィックを処理するネットワークを選択します
[フローティング IP アドレス]	<p>Kubernetes 制御プレーン仮想マシンに接続する 5 つの IP アドレスを予約するための開始点を決定する IP アドレスを、次のように入力します。</p> <ul style="list-style-type: none"> ■ Kubernetes 制御プレーン仮想マシンそれぞれの IP アドレス。 ■ 管理ネットワークへのインターフェイスとして機能するいずれかの Kubernetes 制御プレーン仮想マシンのフローティング IP アドレス。フローティング IP アドレスが割り当てられた制御プレーン仮想マシンは、3 台すべての Kubernetes 制御プレーン仮想マシンの中で主要な仮想マシンとして機能します。フローティング IP アドレスは、Kubernetes クラスタ内の etcd リーダーである制御プレーン ノードに移動されます。これにより、ネットワーク パーティション イベントが発生した場合に、可用性が向上します。 ■ Kubernetes 制御プレーン仮想マシンで障害が発生し、新しい制御プレーン仮想マシンが引き継ぐため起動しているときにバッファとして機能する IP アドレス。
[DNS サーバ]	環境内で使用する DNS サーバのアドレスを入力します。vCenter Server システムが FQDN で登録されている場合は、vSphere 環境で使用する DNS サーバの IP アドレスを入力して、スーパーバイザー で FQDN を解決できるようにする必要があります。
[DNS 検索ドメイン]	DNS が Kubernetes 制御プレーン ノード内で検索するドメイン名 (corp.local など) を入力して、DNS サーバで解決できるようにします。
[NTP サーバ]	環境内で使用する NTP サーバがある場合は、そのアドレスを入力します。

- [固定]。管理ネットワークのすべてのネットワーク設定を手動で入力します。

オプション	説明
[ネットワーク]	スーパーバイザー の管理トラフィックを処理するネットワークを選択します
[開始 IP アドレス]	<p>Kubernetes 制御プレーン仮想マシンに接続する 5 つの IP アドレスを予約するための開始点を決定する IP アドレスを、次のように入力します。</p> <ul style="list-style-type: none"> ■ Kubernetes 制御プレーン仮想マシンそれぞれの IP アドレス。 ■ 管理ネットワークへのインターフェイスとして機能するいずれかの Kubernetes 制御プレーン仮想マシンのフローティング IP アドレス。フローティング IP アドレスが割り当てられた制御プレーン仮想マシンは、3 台すべての Kubernetes 制御プレーン仮想マシンの中で主要な仮想マシンとして機能します。フローティング IP アドレスは、Kubernetes クラスタ内の etcd リーダーである制御プレーン ノードに移動されます。これにより、ネットワークパーティション イベントが発生した場合に、可用性が向上します。 ■ Kubernetes 制御プレーン仮想マシンで障害が発生し、新しい制御プレーン仮想マシンが引き継ぐため起動しているときにバッファとして機能する IP アドレス。
[サブネット マスク]	<p>固定 IP 構成にのみ適用されます。管理ネットワークのサブネット マスクを入力します。</p> <p>たとえば、255.255.255.0。</p>
[ゲートウェイ]	管理ネットワークのゲートウェイを入力します。
[DNS サーバ]	<p>環境内で使用する DNS サーバのアドレスを入力します。</p> <p>vCenter Server システムが FQDN で登録されている場合は、vSphere 環境で使用する DNS サーバの IP アドレスを入力して、スーパーバイザー で FQDN を解決できるようにする必要があります。</p>
[DNS 検索ドメイン]	DNS が Kubernetes 制御プレーン ノード内で検索するドメイン名 (corp.local など) を入力して、DNS サーバで解決できるようにします。
[NTP サーバ]	環境内で使用する NTP サーバがある場合は、そのアドレスを入力します。

- b [次へ] をクリックします。

- 9 [ワークロード ネットワーク] 画面で、スーパーバイザー 上で実行されている Kubernetes ワークロードのネットワークトラフィックを処理するネットワークの設定を入力します。

注： ワークロード ネットワークのネットワーク設定に DHCP サーバを使用する場合、スーパーバイザー の構成を完了した後に新しいワークロード ネットワークを作成することはできません。

a ネットワーク モードを選択します。

- [DHCP ネットワーク]。このネットワーク モードでは、ワークロード ネットワークのすべてのネットワーク設定が DHCP を介して取得されます。これらの設定のテキスト フィールドに値を入力して、DHCP から継承された一部の設定をオーバーライドすることもできます。

オプション	説明
[Kubernetes サービスの内部ネットワーク]	Tanzu Kubernetes クラスタおよびクラスタ内で実行されるサービスの IP アドレスの範囲を決定する CIDR 表記を入力します。
[ポート グループ]	スーパーバイザー に対してプライマリ ワークロード ネットワークとして機能するポート グループを選択します。 プライマリ ネットワークは、Kubernetes 制御プレーン仮想マシンのトラフィックと Kubernetes ワークロード ネットワークのトラフィックを処理します。 ネットワーク トポロジによっては、ネットワークとして機能する別のポート グループを後で各名前空間に割り当てることができます。これにより、スーパーバイザー の名前空間の間でレイヤー 2 の隔離が可能になります。名前空間のネットワークとして別のポート グループが割り当てられていない場合は、プライマリ ネットワークが使用されます。Tanzu Kubernetes クラスタで使用されるネットワークは、そのクラスタがデプロイされた名前空間に割り当てられているネットワークのみです。その名前空間にネットワークが明示的に割り当てられていない場合は、プライマリ ネットワークが使用されます。
[ネットワーク名]	ネットワーク名を入力します。
[DNS サーバ]	環境内で使用する DNS サーバがある場合は、その IP アドレスを入力します。 たとえば、 10.142.7.1 のように入力します。 DNS サーバの IP アドレスを入力すると、各制御プレーン仮想マシンにスタティック ルートが追加されます。これは、DNS サーバへのトラフィックがワークロード ネットワークを通過することを意味します。 指定した DNS サーバが管理ネットワークとワークロード ネットワークの間で共有されている場合、制御プレーン仮想マシンの DNS ルックアップは、初期セットアップ後にワークロード ネットワークを介してルーティングされます。
[NTP サーバ]	環境内で使用する NTP サーバがある場合は、そのアドレスを入力します。

- [固定]。ワークロード ネットワーク設定を手動で構成します

オプション	説明
[Kubernetes サービスの内部ネットワーク]	Tanzu Kubernetes クラスタおよびクラスタ内で実行されるサービスの IP アドレスの範囲を決定する CIDR 表記を入力します。
[ポート グループ]	<p>スーパーバイザー に対してプライマリ ワークロード ネットワークとして機能するポート グループを選択します。</p> <p>プライマリ ネットワークは、Kubernetes 制御プレーン仮想マシンのトラフィックと Kubernetes ワークロード トラフィックを処理します。</p> <p>ネットワーク トポロジによっては、ネットワークとして機能する別のポート グループを後で各名前空間に割り当てることができます。これにより、スーパーバイザー の名前空間の間でレイヤー 2 の隔離が可能になります。名前空間のネットワークとして別のポート グループが割り当てられていない場合は、プライマリ ネットワークが使用されます。Tanzu Kubernetes クラスタで使用されるネットワークは、そのクラスタがデプロイされた名前空間に割り当てられているネットワークのみです。その名前空間にネットワークが明示的に割り当てられていない場合は、プライマリ ネットワークが使用されます。</p>
[ネットワーク名]	ネットワーク名を入力します。
[IP アドレス範囲]	<p>Kubernetes 制御プレーン仮想マシンおよびワークロードの IP アドレスを割り当てるために IP アドレス範囲を入力します。</p> <p>このアドレス範囲はスーパーバイザー ノードに接続します。単一のワークロード ネットワークを使用している場合も、Tanzu Kubernetes クラスタ ノードに接続します。</p> <p>HAProxy に [デフォルト] 構成を使用している場合、この IP アドレス範囲がロード バランサの VIP 範囲と重複することはできません。</p>
[サブネット マスク]	サブネット マスク IP アドレスを入力します。
[ゲートウェイ]	プライマリ ネットワークのゲートウェイを入力します。
[NTP サーバ]	環境内で使用する NTP サーバがある場合は、そのアドレスを入力します。
[DNS サーバ]	<p>環境内で使用する DNS サーバがある場合は、その IP アドレスを入力します。</p> <p>たとえば、10.142.7.1 のように入力します。</p>

b [次へ] をクリックします。

- 10 [確認] 画面で、上にスクロールして、これまでに構成したすべての設定を確認し、スーパーバイザー デプロイの詳細設定を行います。

オプション	説明
スーパーバイザー制御プレーンのサイズ	<p>制御プレーン仮想マシンのサイジングを選択します。制御プレーン仮想マシンのサイズによって、スーパーバイザー で実行できるワークロードの数が決まります。以下の中から選択できます。</p> <ul style="list-style-type: none"> ■ 極小 - 2 個の CPU、8 GB のメモリ、32 GB のストレージ ■ 小 - 4 個の CPU、16 GB のメモリ、32 GB のストレージ ■ 中 - 8 個の CPU、16 GB のメモリ、32 GB のストレージ ■ 大 - 16 個の CPU、32 GB のメモリ、32 GB のストレージ <p>注： いったん制御プレーンのサイズを選択した後は、スケールアップのみ可能です。選択したサイズよりも小さなサイズにスケールダウンすることはできません。</p>
API サーバの DNS 名	<p>必要に応じて、スーパーバイザー 制御プレーンの IP アドレスを使用せずにスーパーバイザー 制御プレーンにアクセスするための FQDN を入力します。入力した FQDN は、自動生成された証明書に組み込まれます。スーパーバイザー に対して FQDN を使用することで、ロードバランサ証明書での IP アドレスの指定を省略できます。</p>
設定のエクスポート	<p>入力したスーパーバイザー 構成の値を含む JSON ファイルをエクスポートします。</p> <p>スーパーバイザー を再デプロイする場合、または類似した構成で新しいスーパーバイザー をデプロイする場合は、後でファイルを変更してインポートできます。</p> <p>スーパーバイザー 構成をエクスポートすると、スーパーバイザー を再デプロイするときこのウィザードのすべての構成値を新たに入力する必要がなく、時間を節約できます。</p>

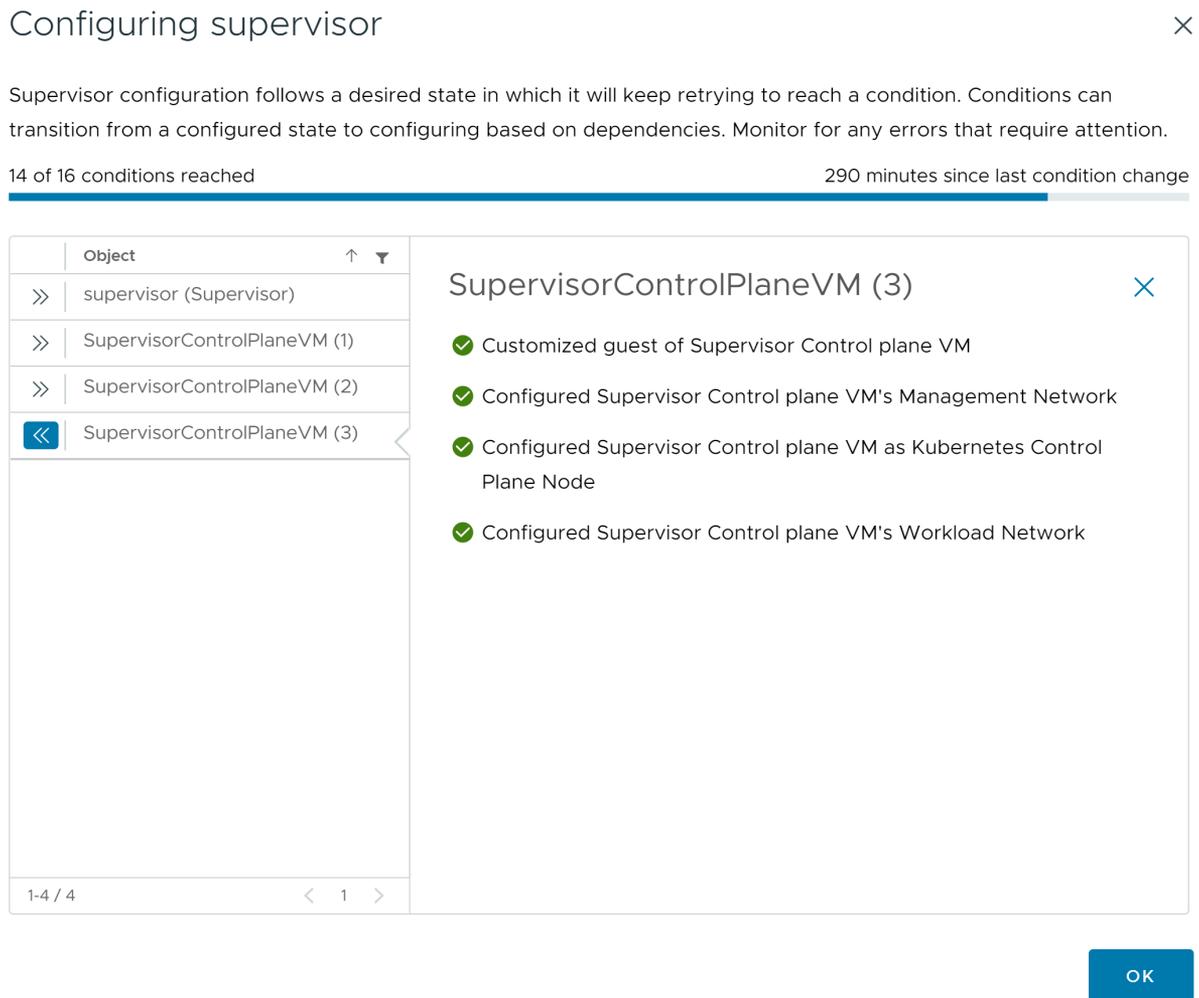
- 11 設定を確認する準備ができたなら、[終了] をクリックします。

スーパーバイザー の有効化により、制御プレーン仮想マシンおよびいくつかのコンポーネントの作成と構成が開始されます。

次のステップ

スーパーバイザー を有効にするためのウィザードを完了したら、有効化プロセスを追跡し、トラブルシューティングを必要とする潜在的な問題を確認できます。[構成ステータス] 列で、スーパーバイザー のステータスの横にある [表示] をクリックします。

図 5-1. スーパーバイザーの有効化ビュー



デプロイ プロセスを完了するには、スーパーバイザー が目的の状態に到達する、つまり、すべての条件が満たされる必要があります。スーパーバイザー が正常に有効になると、ステータスが [設定中] から [実行中] に変わります。スーパーバイザー が [設定中] 状態の間は、各条件を満たしたかどうかが継続的に再確認されます。条件を満たさない場合、成功するまで操作が再試行されます。このため、16 件中 10 件が満たされた場合など、満たした条件の数が増減する可能性があります。たとえば、16 件中 10 件が満たされた後で、16 件中 4 件が満たされるなどです。ごくまれに、目的の状態に到達することを阻止するエラーがある場合、ステータスが [エラー] に変わることがあります。

デプロイ エラーとそのトラブルシューティング方法の詳細については、「[有効化または更新中のスーパーバイザー制御プレーン仮想マシンの健全性ステータス エラーの解決](#)」を参照してください。

ウィザードで入力した構成値を変更してスーパーバイザー を再デプロイする場合は、「[9 章 JSON 構成ファイルのインポートによるスーパーバイザー のデプロイ](#)」を参照してください。

NSX ネットワークを使用する 3 ゾーン スーパーバイザー のデプロイ

NSX を使用する スーパーバイザー を 3 つの vSphere Zone にデプロイする方法を確認します。各 vSphere Zone は、1 つの vSphere クラスタにマッピングされます。スーパーバイザー を 3 つの vSphere Zone にデプロイすることで、ワークロードにクラスタ レベルで高可用性を提供できます。NSX が構成された 3 ゾーン スーパーバイザー では、Tanzu Kubernetes のクラスタおよび仮想マシンのみがサポートされます。vSphere ポッド はサポートされません。

NSX バージョン 4.1.1 以降を構成し、Enterprise ライセンスの NSX Advanced Load Balancer バージョン 22.1.4 以降を NSX にインストール、構成、登録した場合、NSX で使用されるロード バランサは NSX Advanced Load Balancer です。4.1.1 よりも前のバージョンの NSX を構成している場合は、NSX ロード バランサが使用されます。詳細については、『7 章 NSX ネットワークで使用されるロード バランサの確認』を参照してください。

前提条件

- vSphere クラスタを スーパーバイザー として構成するための前提条件を満たすこと。vSphere クラスタで vSphere IaaS control plane を構成するための前提条件を参照してください。
- 3 つの vSphere Zones を作成します。3 章 マルチゾーン スーパーバイザー デプロイ用の vSphere Zones の作成を参照してください。

手順

- 1 ホーム メニューから、[ワークロード管理] を選択します。
- 2 スーパーバイザー のライセンス オプションを選択します。
 - 有効な Tanzu エディション ライセンスを所有している場合は、[ライセンスの追加] をクリックして、vSphere のライセンス インベントリにライセンス キーを追加します。
 - Tanzu エディション ライセンスをまだ所有していない場合は、VMware からの連絡を受信できるように、連絡先の詳細を入力してから、[開始する] をクリックします。

スーパーバイザー の評価期間は、60 日間です。この期間内に、有効な Tanzu エディション ライセンスをクラスタに割り当てる必要があります。Tanzu エディション ライセンス キーを追加した場合は、スーパーバイザー の設定を完了した後、60 日の評価期間内にそのキーを割り当てることができます。
- 3 [ワークロード管理] 画面で、[開始する] を再度クリックします。
- 4 [vCenter Server とネットワーク] 画面で、スーパーバイザー デプロイ用にセットアップされている vCenter Server システムを選択し、ネットワーク スタックとして [NSX] を選択します。
- 5 [次へ] をクリックします。
- 6 [スーパーバイザーの配置] 画面で、[vSphere Zone のデプロイ] を選択して 3 つの vSphere Zones に スーパーバイザー をデプロイします。
 - a 新しい スーパーバイザー の名前を入力します。
 - b スーパーバイザー をデプロイするための vSphere Zones を作成したデータセンターを選択します。

- c 互換性のある vSphere Zones のリストから、3 つのゾーンを選択します。
- d [次へ] をクリックします。

7 スーパーバイザー のストレージ ポリシーを選択します。

オプション	説明
制御プレーン ストレージ ポリシー	制御プレーン仮想マシンを配置するためのストレージ ポリシーを選択します。
短期ディスク ストレージ ポリシー	vSphere ポッドは 3 ゾーン スーパーバイザー ではサポートされていないため、このオプションは無効になっています。
イメージ キャッシュ ストレージ ポリシー	vSphere ポッドは 3 ゾーン スーパーバイザー ではサポートされていないため、このオプションは無効になっています。

8 [次へ] をクリックします。

9 [管理ネットワーク] 画面で、Kubernetes 制御プレーン仮想マシンに使用されるネットワークのパラメータを構成します。

a [ネットワーク モード] を選択します。

- [DHCP ネットワーク]。このモードでは、制御プレーン仮想マシンの IP アドレス、フローティング IP アドレス、DNS サーバ、DNS、検索ドメイン、NTP サーバなど、管理ネットワークのすべての IP アドレスが DHCP サーバから自動的に取得されます。フローティング IP アドレスを取得するためには、クライアント ID をサポートするように DHCP サーバを構成する必要があります。DHCP モードでは、すべての制御プレーン仮想マシンが安定した DHCP クライアント ID を使用して IP アドレスを取得します。これらのクライアント ID を使用すると、DHCP サーバ上の制御プレーン仮想マシンの IP アドレスに対して固定 IP アドレス割り当てを設定して、IP アドレスが変更されないようにすることができます。制御プレーン仮想マシンの IP アドレスとフローティング IP アドレスの変更はサポートされていません。

DHCP から継承された一部の設定をオーバーライドするには、これらの設定のテキスト フィールドに値を入力します。

オプション	説明
[ネットワーク]	スーパーバイザー の管理トラフィックを処理するネットワークを選択します
[フローティング IP アドレス]	<p>Kubernetes 制御プレーン仮想マシンに接続する 5 つの IP アドレスを予約するための開始点を決定する IP アドレスを、次のように入力します。</p> <ul style="list-style-type: none"> ■ Kubernetes 制御プレーン仮想マシンそれぞれの IP アドレス。 ■ 管理ネットワークへのインターフェイスとして機能するいずれかの Kubernetes 制御プレーン仮想マシンのフローティング IP アドレス。フローティング IP アドレスが割り当てられた制御プレーン仮想マシンは、3 台すべての Kubernetes 制御プレーン仮想マシンの中で主要な仮想マシンとして機能します。フローティング IP アドレスは、Kubernetes クラスタ内の etcd リーダーである制御プレーン ノードに移動されます。これにより、ネットワークパーティション イベントが発生した場合に、可用性が向上します。 ■ Kubernetes 制御プレーン仮想マシンで障害が発生し、新しい制御プレーン仮想マシンが引き継ぐため起動しているときにバッファとして機能する IP アドレス。
[DNS サーバ]	環境内で使用する DNS サーバのアドレスを入力します。vCenter Server システムが FQDN で登録されている場合は、vSphere 環境で使用する DNS サーバの IP アドレスを入力して、スーパーバイザー で FQDN を解決できるようにする必要があります。
[DNS 検索ドメイン]	DNS が Kubernetes 制御プレーン ノード内で検索するドメイン名 (corp.local など) を入力して、DNS サーバで解決できるようにします。
[NTP サーバ]	環境内で使用する NTP サーバがある場合は、そのアドレスを入力します。

- [固定]。管理ネットワークのすべてのネットワーク設定を手動で入力します。

オプション	説明
[ネットワーク]	スーパーバイザー の管理トラフィックを処理するネットワークを選択します
[開始 IP アドレス]	<p>Kubernetes 制御プレーン仮想マシンに接続する 5 つの IP アドレスを予約するための開始点を決定する IP アドレスを、次のように入力します。</p> <ul style="list-style-type: none"> ■ Kubernetes 制御プレーン仮想マシンそれぞれの IP アドレス。 ■ 管理ネットワークへのインターフェイスとして機能するいずれかの Kubernetes 制御プレーン仮想マシンのフローティング IP アドレス。フローティング IP アドレスが割り当てられた制御プレーン仮想マシンは、3 台すべての Kubernetes 制御プレーン仮想マシンの中で主要な仮想マシンとして機能します。フローティング IP アドレスは、Kubernetes クラスタ内の etcd リーダーである制御プレーン ノードに移動されます。これにより、ネットワークパーティション イベントが発生した場合に、可用性が向上します。 ■ Kubernetes 制御プレーン仮想マシンで障害が発生し、新しい制御プレーン仮想マシンが引き継ぐため起動しているときにバッファとして機能する IP アドレス。
[サブネット マスク]	<p>固定 IP 構成にのみ適用されます。管理ネットワークのサブネット マスクを入力します。</p> <p>たとえば、255.255.255.0。</p>
[ゲートウェイ]	管理ネットワークのゲートウェイを入力します。
[DNS サーバ]	<p>環境内で使用する DNS サーバのアドレスを入力します。</p> <p>vCenter Server システムが FQDN で登録されている場合は、vSphere 環境で使用する DNS サーバの IP アドレスを入力して、スーパーバイザー で FQDN を解決できるようにする必要があります。</p>
[DNS 検索ドメイン]	DNS が Kubernetes 制御プレーン ノード内で検索するドメイン名 (corp.local など) を入力して、DNS サーバで解決できるようにします。
[NTP サーバ]	環境内で使用する NTP サーバがある場合は、そのアドレスを入力します。

b [次へ] をクリックします。

10 [ワークロード ネットワーク] ペインで、名前空間のネットワークの設定を構成します。

オプション	説明
vSphere Distributed Switch	<p>スーパーバイザー のオーバーレイ ネットワークを処理する vSphere Distributed Switch を選択します。</p> <p>たとえば、DSwitch を選択します。</p>
DNS サーバ	<p>環境内で使用する DNS サーバがある場合は、その IP アドレスを入力します。</p> <p>たとえば、10.142.7.1 です。</p>

オプション	説明
NAT モード	<p>NAT モードは、デフォルトで選択されています。</p> <p>このオプションを選択解除すると、vSphere ポッド、仮想マシン、Tanzu Kubernetes クラスタ ノードの IP アドレスなどのワークロードがいずれも Tier-0 ゲートウェイの外から直接アクセスできるようになります。Egress CIDR を構成する必要はありません。</p> <p>注： NAT モードを選択解除すると、ファイル ボリューム ストレージはサポートされません。</p>
名前空間ネットワーク	1つ以上の IP CIDR を入力してサブネット/セグメントを作成し、ワークロードに IP アドレスを割り当てます。
Ingress CIDR	Kubernetes サービスの Ingress IP アドレス範囲を決定する CIDR 注釈を入力します。この範囲は、タイプがロード バランサで Ingress のサービスに使用されます。
Edge クラスタ	<p>名前空間ネットワークに使用する Tier-0 ゲートウェイを持つ NSX Edge クラスタを選択します。</p> <p>たとえば、EDGE-CLUSTER を選択します。</p>
Tier-0 ゲートウェイ	クラスタの Tier-1 ゲートウェイに関連付ける Tier-0 ゲートウェイを選択します。
サブネット プリフィックス	名前空間セグメント用に予約されるサブネットのサイズを指定する、サブネット プリフィックスを入力します。デフォルトは 28 です。
サービス CIDR	Kubernetes サービスの IP アドレス範囲を決定する CIDR 注釈を入力します。デフォルト値を使用できます。
Egress CIDR	<p>Kubernetes サービスの Egress IP アドレスを決定する CIDR 注釈を入力します。スーパーバイザー 内の名前空間ごとに 1つの Egress IP アドレスのみが割り当てられます。</p> <p>Egress IP アドレスは、特定の名前空間内の Kubernetes ワークロードが NSX の外部と通信するために使用する IP アドレスです。</p>

11 [次へ] をクリックします。

- 12 [確認] 画面で、上にスクロールして、これまでに構成したすべての設定を確認し、スーパーバイザー デプロイの詳細設定を行います。

オプション	説明
スーパーバイザー制御プレーンのサイズ	<p>制御プレーン仮想マシンのサイジングを選択します。制御プレーン仮想マシンのサイズによって、スーパーバイザー で実行できるワークロードの数が決まります。以下の中から選択できます。</p> <ul style="list-style-type: none"> ■ 極小 - 2 個の CPU、8 GB のメモリ、32 GB のストレージ ■ 小 - 4 個の CPU、16 GB のメモリ、32 GB のストレージ ■ 中 - 8 個の CPU、16 GB のメモリ、32 GB のストレージ ■ 大 - 16 個の CPU、32 GB のメモリ、32 GB のストレージ <p>注： いったん制御プレーンのサイズを選択した後は、スケールアップのみ可能です。選択したサイズよりも小さなサイズにスケールダウンすることはできません。</p>
API サーバの DNS 名	<p>必要に応じて、スーパーバイザー 制御プレーンの IP アドレスを使用せずにスーパーバイザー 制御プレーンにアクセスするための FQDN を入力します。入力した FQDN は、自動生成された証明書に組み込まれます。スーパーバイザー に対して FQDN を使用することで、ロードバランサ証明書での IP アドレスの指定を省略できます。</p>
設定のエクスポート	<p>入力したスーパーバイザー 構成の値を含む JSON ファイルをエクスポートします。</p> <p>スーパーバイザー を再デプロイする場合、または類似した構成で新しいスーパーバイザー をデプロイする場合は、後でファイルを変更してインポートできます。</p> <p>スーパーバイザー 構成をエクスポートすると、スーパーバイザー を再デプロイするときこのウィザードのすべての構成値を新たに入力する必要がなく、時間を節約できます。</p>

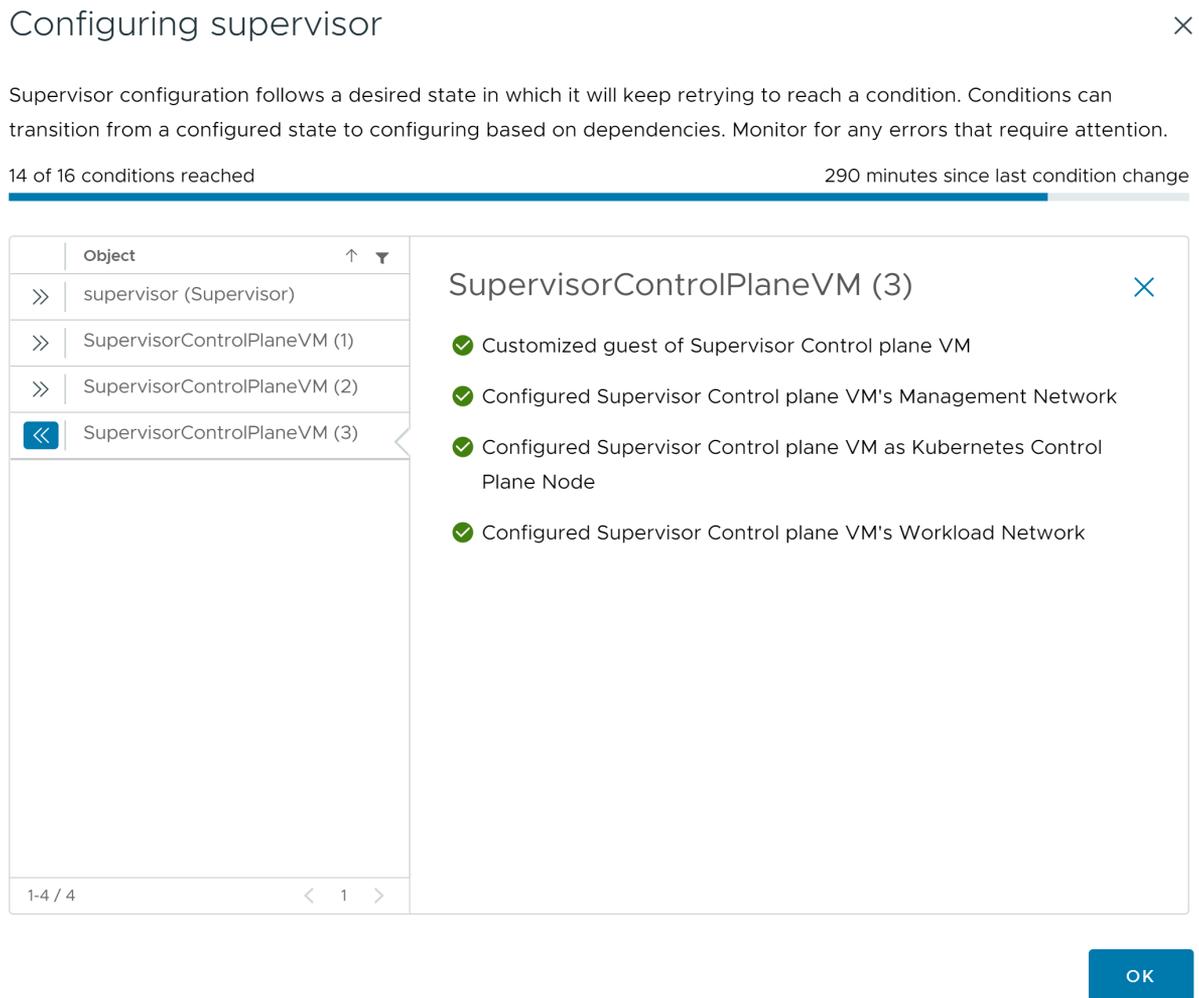
- 13 設定を確認する準備ができたなら、[終了] をクリックします。

スーパーバイザー の有効化により、制御プレーン仮想マシンおよびいくつかのコンポーネントの作成と構成が開始されます。

次のステップ

スーパーバイザー を有効にするためのウィザードを完了したら、有効化プロセスを追跡し、トラブルシューティングを必要とする潜在的な問題を確認できます。[構成ステータス] 列で、スーパーバイザー のステータスの横にある [表示] をクリックします。

図 5-2. スーパーバイザーの有効化ビュー



デプロイ プロセスを完了するには、スーパーバイザー が目的の状態に到達する、つまり、すべての条件が満たされる必要があります。スーパーバイザー が正常に有効になると、ステータスが [設定中] から [実行中] に変わります。スーパーバイザー が [設定中] 状態の間は、各条件を満たしたかどうかが継続的に再確認されます。条件を満たさない場合、成功するまで操作が再試行されます。このため、16 件中 10 件が満たされた場合など、満たした条件の数が増減する可能性があります。たとえば、16 件中 10 件が満たされた後で、16 件中 4 件が満たされるなどです。ごくまれに、目的の状態に到達することを阻止するエラーがある場合、ステータスが [エラー] に変わることがあります。

デプロイ エラーとそのトラブルシューティング方法の詳細については、「[有効化または更新中のスーパーバイザー制御プレーン仮想マシンの健全性ステータス エラーの解決](#)」を参照してください。

ウィザードで入力した構成値を変更してスーパーバイザー を再デプロイする場合は、「[9 章 JSON 構成ファイルのインポートによるスーパーバイザー のデプロイ](#)」を参照してください。

1 ゾーン スーパーバイザー のデプロイ

6

1つの vSphere Zone に自動的にマッピングされる 1つの vSphere クラスタで、スーパーバイザー をデプロイします。1ゾーン スーパーバイザー には、vSphere HA によって提供されるホスト レベルの高可用性があります。

次のトピックを参照してください。

- [VDS ネットワーク スタックを使用する 1 ゾーン スーパーバイザー のデプロイ](#)
- [NSX ネットワークを使用する 1 ゾーン スーパーバイザー のデプロイ](#)

VDS ネットワーク スタックを使用する 1 ゾーン スーパーバイザー のデプロイ

VDS ネットワーク スタック、および HA プロキシ ロード バランサまたは NSX Advanced Load Balancer を使用する 1ゾーン スーパーバイザー をデプロイする方法を確認します。VDS ネットワークを使用するように構成された 1ゾーン スーパーバイザー では、Tanzu Kubernetes Grid を使用して作成された Tanzu Kubernetes クラスタのデプロイがサポートされます。スーパーバイザー サービス によってデプロイされたものと別に vSphere ポッド を実行することはサポートされません。

注： 単一の vSphere クラスタに スーパーバイザー をデプロイすると、1つの vSphere Zone が作成されるため、スーパーバイザー を 3 ゾーンのデプロイに拡張することはできません。1つの vSphere Zone（単一クラスタのデプロイ）または 3つの vSphere Zone に スーパーバイザー をデプロイできます。

前提条件

- vSphere クラスタを スーパーバイザー として構成するための前提条件を満たすこと。[vSphere クラスタで vSphere IaaS control plane を構成するための前提条件](#)を参照してください。

手順

- 1 ホーム メニューから、[ワークロード管理] を選択します。
- 2 スーパーバイザー のライセンス オプションを選択します。
 - 有効な Tanzu エディション ライセンスを所有している場合は、[ライセンスの追加] をクリックして、vSphere のライセンス インベントリにライセンス キーを追加します。
 - Tanzu エディション ライセンスをまだ所有していない場合は、VMware からの連絡を受信できるように、連絡先の詳細を入力してから、[開始する] をクリックします。

スーパーバイザー の評価期間は、60 日間です。この期間内に、有効な Tanzu エディション ライセンスをクラスタに割り当てる必要があります。Tanzu エディション ライセンス キーを追加した場合は、スーパーバイザー の設定を完了した後、60 日の評価期間内にそのキーを割り当てることができます。

- 3 [ワークロード管理] 画面で、[開始する] を再度クリックします。
- 4 [vCenter Server とネットワーク] 画面を選択し、vCenter Server デプロイ用にセットアップされているスーパーバイザー システムを選択し、ネットワーク スタックとして [vSphere Distributed Switch (VDS)] を選択して、[次へ] をクリックします。
- 5 1 ゾーン スーパーバイザー を有効にするには、スーパーバイザー の場所の画面で [クラスタのデプロイ] を選択します。

1 ゾーン スーパーバイザー でワークロード管理を有効にすると、vSphere Zone が自動的に作成され、クラスタがゾーンに割り当てられます。

- 6 互換性のあるクラスタのリストからクラスタを選択します。
- 7 スーパーバイザー の名前を入力します。
- 8 (オプション) vSphere Zone の名前を入力し、[次へ] をクリックします。

vSphere Zone の名前を入力しないと、名前は自動的に割り当てられ、後から変更することはできません。

- 9 [ストレージ] 画面で、制御プレーン仮想マシンを配置するためのストレージを構成します。

オプション	説明
制御プレーン ノード	制御プレーン仮想マシンを配置するためのストレージ ポリシーを選択します。

10 [ロード バランサ] 画面で、ロード バランサの設定を入力します。

- a ロード バランサの名前を指定します。
- b ロード バランサのタイプを選択します。

[NSX Advanced Load Balancer] と [HAProxy] から選択できます。

- c ロード バランサの設定を構成します。
 - NSX Advanced Load Balancer の場合は次の設定を入力します。

オプション	説明
[名前]	NSX Advanced Load Balancer の名前を入力します。
[NSX Advanced Load Balancer コントローラ エンドポイント]	NSX Advanced Load Balancer Controller の IP アドレス。 デフォルトのポートは 443 です。
[ユーザー名]	NSX Advanced Load Balancer を使用して構成されたユーザー名。このユーザー名は、コントローラへのアクセスに使用します。
[パスワード]	ユーザー名のパスワード。
[サーバ証明書]	コントローラによって使用される証明書。 構成時に割り当てた証明書を指定できます。 詳細については、 コントローラへの証明書の割り当て を参照してください。
[クラウド名]	設定したカスタム クラウドの名前を入力します。クラウド名では大文字と小文字が区別されます。 [Default-Cloud] を使用する場合は、このフィールドを空のままにします。 詳細については、『 コントローラの構成 』を参照してください。

- HAProxy の場合は次の設定を入力します。

オプション	説明
[HAProxy ロード バランサ コントローラ エンドポイント]	HAProxy アプライアンスの管理 IP アドレスである、HAProxy データ プレーン API の IP アドレスとポート。このコンポーネントは、HAProxy サーバを制御し、HAProxy 仮想マシン内で実行されます。
[ユーザー名]	HAProxy OVA ファイルを使用して構成されたユーザー名。この名前は、HAProxy データ プレーン API での認証に使用します。
[パスワード]	ユーザー名のパスワード。
[仮想 IP アドレスの範囲]	Tanzu Kubernetes クラスタによってワークロード ネットワークで使用される IP アドレスの範囲。この IP アドレス範囲は、HAProxy アプライアンスのデプロイ時に構成した CIDR で定義された IP アドレスのリストから取得されます。HAProxy デプロイで構成された範囲の全体を設定できますが、その CIDR のサブセットを設定することで、複数の スーパーバイザー を作成してその CIDR 範囲の IP アドレスを使用することもできま

オプション	説明
	<p>す。この範囲は、このウィザードでワークロード ネットワーク用に定義されている IP アドレス範囲と重複することはできません。また、この範囲は、このワークロード ネットワークの DHCP 範囲とも重複することができません。</p>
[HAProxy 管理 TLS 証明書]	<p>署名済みの PEM 形式の証明書、またはデータ プレーン API によって提供されるサーバ証明書の信頼できるルートである PEM 形式の証明書。</p> <ul style="list-style-type: none"> ■ オプション 1: root アクセスが有効な場合に、HAProxy 仮想マシンに root として SSH 接続し、[サーバ認証局] に /etc/haproxy/ca.crt をコピーします。 \n 形式のエスケープ行を使用しないでください。 ■ オプション 2: HAProxy 仮想マシンを右クリックし、[設定の編集] を選択します。適切なフィールドから CA 証明書をコピーし、https://www.base64decode.org/ などの変換ツールを使用して Base64 から変換します。 ■ オプション 3: 次の PowerCLI スクリプトを実行します。変数 \$vc、\$vc_user、\$vc_password の値を適切な値に置き換えます。 <pre> \$vc = "10.21.32.43" \$vc_user = "administrator@vsphere.local" \$vc_password = "PASSWORD" Connect-VIServer -User \$vc_user -Password \$vc_password -Server \$vc \$VMname = "haproxy-demo" \$AdvancedSettingName = "guestinfo.dataplaneapi.cacert" \$Base64cert = get-vm \$VMname Get- AdvancedSetting -Name \$AdvancedSettingName while ([string]::IsNullOrEmpty(\$Base64cert .Value)) { Write-Host "Waiting for CA Cert Generation... This may take a under 5-10 minutes as the VM needs to boot and generate the CA Cert (if you haven't provided one already)."<!-- \$Base64cert = get-vm \$VMname Get-AdvancedSetting -Name \$AdvancedSettingName Start-sleep -seconds 2 } Write-Host "CA Cert Found... Converting from BASE64" \$cert = [Text.Encoding]::Utf8.GetString([Con vert]::FromBase64String(\$Base64cert. Value)) Write-Host \$cert </pre--> </pre>

11 [管理ネットワーク] 画面で、Kubernetes 制御プレーン仮想マシンに使用されるネットワークのパラメータを構成します。

a [ネットワーク モード] を選択します。

- [DHCP ネットワーク]。このモードでは、制御プレーン仮想マシンの IP アドレス、フローティング IP アドレス、DNS サーバ、DNS、検索ドメイン、NTP サーバなど、管理ネットワークのすべての IP アドレスが DHCP サーバから自動的に取得されます。フローティング IP アドレスを取得するためには、クライアント ID をサポートするように DHCP サーバを構成する必要があります。DHCP モードでは、すべての制御プレーン仮想マシンが安定した DHCP クライアント ID を使用して IP アドレスを取得します。これらのクライアント ID を使用すると、DHCP サーバ上の制御プレーン仮想マシンの IP アドレスに対して固定 IP アドレス割り当てを設定して、IP アドレスが変更されないようにすることができます。制御プレーン仮想マシンの IP アドレスとフローティング IP アドレスの変更はサポートされていません。

DHCP から継承された一部の設定をオーバーライドするには、これらの設定のテキスト フィールドに値を入力します。

オプション	説明
[ネットワーク]	スーパーバイザー の管理トラフィックを処理するネットワークを選択します
[フローティング IP アドレス]	<p>Kubernetes 制御プレーン仮想マシンに接続する 5 つの IP アドレスを予約するための開始点を決定する IP アドレスを、次のように入力します。</p> <ul style="list-style-type: none"> ■ Kubernetes 制御プレーン仮想マシンそれぞれの IP アドレス。 ■ 管理ネットワークへのインターフェイスとして機能するいずれかの Kubernetes 制御プレーン仮想マシンのフローティング IP アドレス。フローティング IP アドレスが割り当てられた制御プレーン仮想マシンは、3 台すべての Kubernetes 制御プレーン仮想マシンの中で主要な仮想マシンとして機能します。フローティング IP アドレスは、Kubernetes クラスタ内の etcd リーダーである制御プレーン ノードに移動されます。これにより、ネットワーク パーティション イベントが発生した場合に、可用性が向上します。 ■ Kubernetes 制御プレーン仮想マシンで障害が発生し、新しい制御プレーン仮想マシンが引き継ぐため起動しているときにバッファとして機能する IP アドレス。
[DNS サーバ]	環境内で使用する DNS サーバのアドレスを入力します。vCenter Server システムが FQDN で登録されている場合は、vSphere 環境で使用する DNS サーバの IP アドレスを入力して、スーパーバイザー で FQDN を解決できるようにする必要があります。
[DNS 検索ドメイン]	DNS が Kubernetes 制御プレーン ノード内で検索するドメイン名 (corp.local など) を入力して、DNS サーバで解決できるようにします。
[NTP サーバ]	環境内で使用する NTP サーバがある場合は、そのアドレスを入力します。

- [固定]。管理ネットワークのすべてのネットワーク設定を手動で入力します。

オプション	説明
[ネットワーク]	スーパーバイザー の管理トラフィックを処理するネットワークを選択します
[開始 IP アドレス]	<p>Kubernetes 制御プレーン仮想マシンに連続する 5 つの IP アドレスを予約するための開始点を決定する IP アドレスを、次のように入力します。</p> <ul style="list-style-type: none"> ■ Kubernetes 制御プレーン仮想マシンそれぞれの IP アドレス。 ■ 管理ネットワークへのインターフェイスとして機能するいずれかの Kubernetes 制御プレーン仮想マシンのフローティング IP アドレス。フローティング IP アドレスが割り当てられた制御プレーン仮想マシンは、3 台すべての Kubernetes 制御プレーン仮想マシンの中で主要な仮想マシンとして機能します。フローティング IP アドレスは、Kubernetes クラスタ内の etcd リーダーである制御プレーン ノードに移動されます。これにより、ネットワークパーティション イベントが発生した場合に、可用性が向上します。 ■ Kubernetes 制御プレーン仮想マシンで障害が発生し、新しい制御プレーン仮想マシンが引き継ぐため起動しているときにバッファとして機能する IP アドレス。
[サブネット マスク]	<p>固定 IP 構成にのみ適用されます。管理ネットワークのサブネット マスクを入力します。</p> <p>たとえば、255.255.255.0。</p>
[ゲートウェイ]	管理ネットワークのゲートウェイを入力します。
[DNS サーバ]	<p>環境内で使用する DNS サーバのアドレスを入力します。</p> <p>vCenter Server システムが FQDN で登録されている場合は、vSphere 環境で使用する DNS サーバの IP アドレスを入力して、スーパーバイザー で FQDN を解決できるようにする必要があります。</p>
[DNS 検索ドメイン]	<p>DNS が Kubernetes 制御プレーン ノード内で検索するドメイン名 (corp.local など) を入力して、DNS サーバで解決できるようにします。</p>
[NTP サーバ]	<p>環境内で使用する NTP サーバがある場合は、そのアドレスを入力します。</p>

- b [次へ] をクリックします。

- 12 [ワークロード ネットワーク] 画面で、スーパーバイザー 上で実行されている Kubernetes ワークロードのネットワークトラフィックを処理するネットワークの設定を入力します。

注： ワークロード ネットワークのネットワーク設定に DHCP サーバを使用する場合、スーパーバイザー の構成を完了した後に新しいワークロード ネットワークを作成することはできません。

a ネットワーク モードを選択します。

- [DHCP ネットワーク]。このネットワーク モードでは、ワークロード ネットワークのすべてのネットワーク設定が DHCP を介して取得されます。これらの設定のテキスト フィールドに値を入力して、DHCP から継承された一部の設定をオーバーライドすることもできます。

注： ワークロード ネットワークの DHCP 構成は、Distributed Switch スタックが構成されたスーパーバイザー のスーパーバイザー サービス ではサポートされません。スーパーバイザー サービスを使用するには、固定 IP アドレスを使用してワークロード ネットワークを構成します。ただし、管理ネットワークには DHCP を使用できます。

オプション	説明
[Kubernetes サービスの内部ネットワーク]	Tanzu Kubernetes クラスタおよびクラスタ内で実行されるサービスの IP アドレスの範囲を決定する CIDR 表記を入力します。
[ポート グループ]	スーパーバイザー に対してプライマリ ワークロード ネットワークとして機能するポート グループを選択します。 プライマリ ネットワークは、Kubernetes 制御プレーン仮想マシンのトラフィックと Kubernetes ワークロード トラフィックを処理します。 ネットワーク トポロジによっては、ネットワークとして機能する別のポート グループを後で各名前空間に割り当てることができます。これにより、スーパーバイザー の名前空間の間でレイヤー 2 の隔離が可能になります。名前空間のネットワークとして別のポート グループが割り当てられていない場合は、プライマリ ネットワークが使用されます。Tanzu Kubernetes クラスタで使用されるネットワークは、そのクラスタがデプロイされた名前空間に割り当てられているネットワークのみです。その名前空間にネットワークが明示的に割り当てられていない場合は、プライマリ ネットワークが使用されます。
[ネットワーク名]	ネットワーク名を入力します。
[DNS サーバ]	環境内で使用する DNS サーバがある場合は、その IP アドレスを入力します。 たとえば、 10.142.7.1 のように入力します。 DNS サーバの IP アドレスを入力すると、各制御プレーン仮想マシンにスタティック ルートが追加されます。これは、DNS サーバへのトラフィックがワークロード ネットワークを通過することを意味します。

オプション	説明
	指定した DNS サーバが管理ネットワークとワークロード ネットワークの間で共有されている場合、制御プレーン仮想マシンの DNS ルックアップは、初期セットアップ後にワークロード ネットワークを介してルーティングされます。
[NTP サーバ]	環境内で使用する NTP サーバがある場合は、そのアドレスを入力します。

- [固定]。ワークロード ネットワーク設定を手動で構成します

オプション	説明
[Kubernetes サービスの内部ネットワーク]	Tanzu Kubernetes クラスタおよびクラスタ内で実行されるサービスの IP アドレスの範囲を決定する CIDR 表記を入力します。
[ポート グループ]	スーパーバイザー に対してプライマリ ワークロード ネットワークとして機能するポート グループを選択します。 プライマリ ネットワークは、Kubernetes 制御プレーン仮想マシンのトラフィックと Kubernetes ワークロード トラフィックを処理します。 ネットワーク トポロジによっては、ネットワークとして機能する別のポート グループを後で各名前空間に割り当てることができます。これにより、スーパーバイザー の名前空間の間でレイヤー 2 の隔離が可能になります。名前空間のネットワークとして別のポート グループが割り当てられていない場合は、プライマリ ネットワークが使用されます。Tanzu Kubernetes クラスタで使用されるネットワークは、そのクラスタがデプロイされた名前空間に割り当てられているネットワークのみです。その名前空間にネットワークが明示的に割り当てられていない場合は、プライマリ ネットワークが使用されます。
[ネットワーク名]	ネットワーク名を入力します。
[IP アドレス範囲]	Kubernetes 制御プレーン仮想マシンおよびワークロードの IP アドレスを割り当てるために IP アドレス範囲を入力します。 このアドレス範囲はスーパーバイザー ノードに接続します。単一のワークロード ネットワークを使用している場合も、Tanzu Kubernetes クラスタ ノードに接続します。HAProxy に [デフォルト] 構成を使用している場合、この IP アドレス範囲がロード バランサの VIP 範囲と重複することはできません。
[サブネット マスク]	サブネット マスク IP アドレスを入力します。
[ゲートウェイ]	プライマリ ネットワークのゲートウェイを入力します。
[NTP サーバ]	環境内で使用する NTP サーバがある場合は、そのアドレスを入力します。
[DNS サーバ]	環境内で使用する DNS サーバがある場合は、その IP アドレスを入力します。

オプション	説明
	たとえば、 10.142.7.1 のように入力します。

b [次へ] をクリックします。

- 13 [確認] 画面で、上にスクロールして、これまでに構成したすべての設定を確認し、スーパーバイザー デプロイの詳細設定を行います。

オプション	説明
スーパーバイザー制御プレーンのサイズ	<p>制御プレーン仮想マシンのサイジングを選択します。制御プレーン仮想マシンのサイズによって、スーパーバイザー で実行できるワークロードの数が決まります。以下の中から選択できます。</p> <ul style="list-style-type: none"> ■ 極小 - 2 個の CPU、8 GB のメモリ、32 GB のストレージ ■ 小 - 4 個の CPU、16 GB のメモリ、32 GB のストレージ ■ 中 - 8 個の CPU、16 GB のメモリ、32 GB のストレージ ■ 大 - 16 個の CPU、32 GB のメモリ、32 GB のストレージ <p>注： いったん制御プレーンのサイズを選択した後は、スケールアップのみ可能です。選択したサイズよりも小さなサイズにスケールダウンすることはできません。</p>
API サーバの DNS 名	<p>必要に応じて、スーパーバイザー 制御プレーンの IP アドレスを使用せずにスーパーバイザー 制御プレーンにアクセスするための FQDN を入力します。入力した FQDN は、自動生成された証明書に組み込まれます。スーパーバイザー に対して FQDN を使用することで、ロードバランサ証明書での IP アドレスの指定を省略できます。</p>
設定のエクスポート	<p>入力したスーパーバイザー 構成の値を含む JSON ファイルをエクスポートします。</p> <p>スーパーバイザー を再デプロイする場合、または類似した構成で新しいスーパーバイザー をデプロイする場合は、後でファイルを変更してインポートできます。</p> <p>スーパーバイザー 構成をエクスポートすると、スーパーバイザー を再デプロイするときこのウィザードのすべての構成値を新たに入力する必要がなく、時間を節約できます。</p>

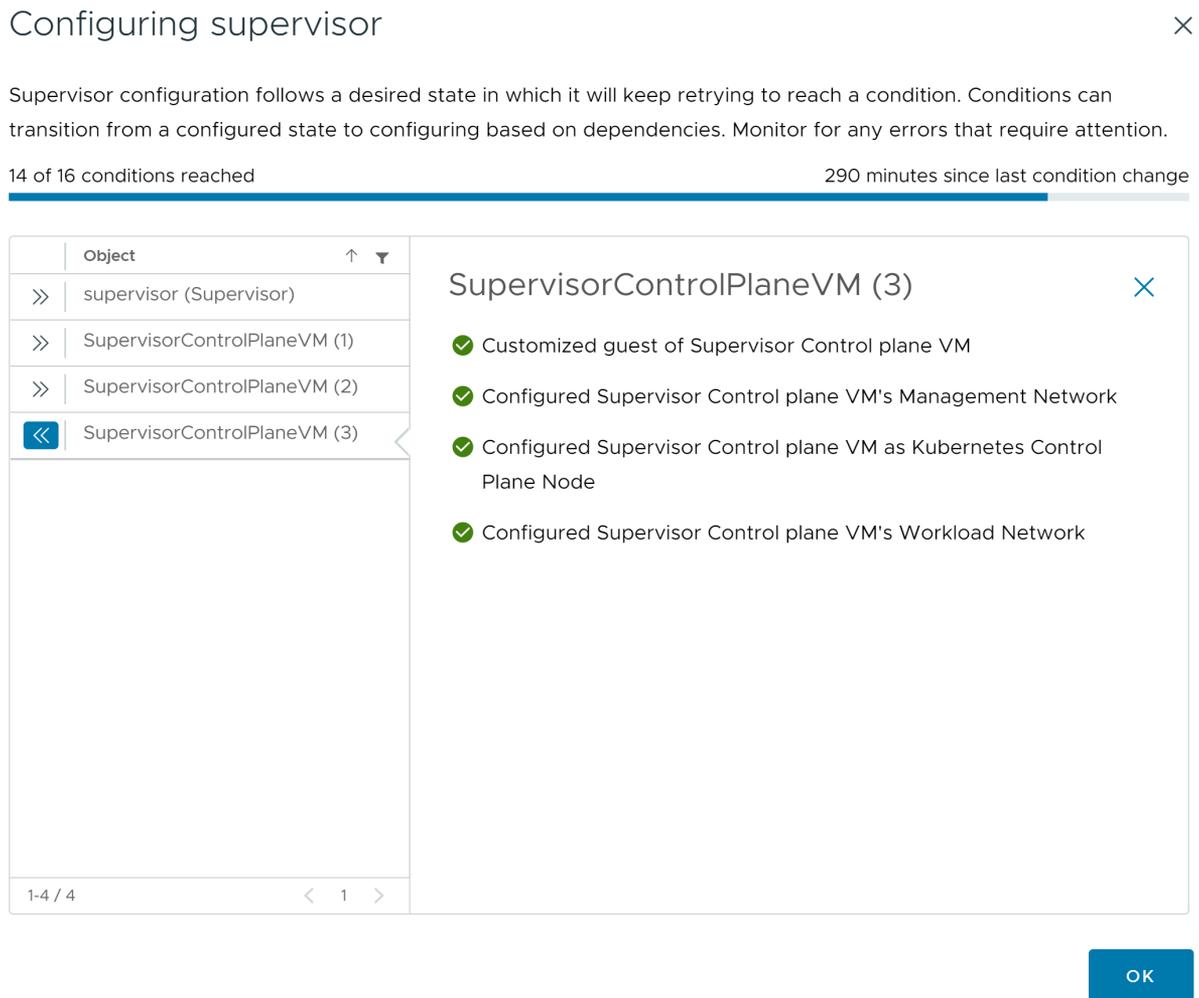
- 14 設定を確認する準備ができたなら、[終了] をクリックします。

スーパーバイザー のデプロイにより、制御プレーン仮想マシンとその他のコンポーネントの作成と構成が開始されます。

次のステップ

スーパーバイザー を有効にするためのウィザードを完了したら、有効化プロセスを追跡し、トラブルシューティングを必要とする潜在的な問題を確認できます。[構成ステータス] 列で、スーパーバイザー のステータスの横にある [表示] をクリックします。

図 6-1. スーパーバイザーの有効化ビュー



デプロイ プロセスを完了するには、スーパーバイザー が目的の状態に到達する、つまり、すべての条件が満たされる必要があります。スーパーバイザー が正常に有効になると、ステータスが [設定中] から [実行中] に変わります。スーパーバイザー が [設定中] 状態の間は、各条件を満たしたかどうかが継続的に再確認されます。条件を満たさない場合、成功するまで操作が再試行されます。このため、16 件中 10 件が満たされた場合など、満たした条件の数が増減する可能性があります。たとえば、16 件中 10 件が満たされた後で、16 件中 4 件が満たされるなどです。ごくまれに、目的の状態に到達することを阻止するエラーがある場合、ステータスが [エラー] に変わることがあります。

デプロイ エラーとそのトラブルシューティング方法の詳細については、「[有効化または更新中のスーパーバイザー制御プレーン仮想マシンの健全性ステータス エラーの解決](#)」を参照してください。

ウィザードで入力した構成値を変更してスーパーバイザー を再デプロイする場合は、「[9 章 JSON 構成ファイルのインポートによるスーパーバイザー のデプロイ](#)」を参照してください。

NSX ネットワークを使用する 1 ゾーン スーパーバイザー のデプロイ

vSphere ゾーンにマッピングされる 1 つの vSphere クラスタに、NSX ネットワークを使用する スーパーバイザー をデプロイする方法について説明します。結果として得られる スーパーバイザー は、vSphere HA によって提供されるホスト レベルの高可用性を備えます。1 ゾーン スーパーバイザー は、すべての Tanzu Kubernetes クラスタ、仮想マシン、vSphere ポッド をサポートします。

NSX バージョン 4.1.1 以降を構成し、Enterprise ライセンスの NSX Advanced Load Balancer バージョン 22.1.4 以降を NSX にインストール、構成、登録した場合、NSX で使用されるロード バランサは NSX Advanced Load Balancer です。4.1.1 よりも前のバージョンの NSX を構成している場合は、NSX ロード バランサが使用されます。詳細については、『7 章 NSX ネットワークで使用されるロード バランサの確認』を参照してください。

注： 単一の vSphere クラスタに スーパーバイザー をデプロイすると、1 つの vSphere Zone が作成されるため、スーパーバイザー を 3 ゾーンのデプロイに拡張することはできません。1 つの vSphere Zone (単一クラスタのデプロイ) または 3 つの vSphere Zone に スーパーバイザー をデプロイできます。

前提条件

環境が vSphere クラスタを スーパーバイザー として構成するための前提条件を満たしていることを確認します。要件の詳細については、[vSphere クラスタで vSphere IaaS control plane を構成するための前提条件](#)を参照してください。

手順

- 1 ホーム メニューから、[ワークロード管理] を選択します。
- 2 スーパーバイザー のライセンス オプションを選択します。
 - 有効な Tanzu エディション ライセンスを所有している場合は、[ライセンスの追加] をクリックして、vSphere のライセンス インベントリにライセンス キーを追加します。
 - Tanzu エディション ライセンスをまだ所有していない場合は、VMware からの連絡を受信できるように、連絡先の詳細を入力してから、[開始する] をクリックします。

スーパーバイザー の評価期間は、60 日間です。この期間内に、有効な Tanzu エディション ライセンスをクラスタに割り当てる必要があります。Tanzu エディション ライセンス キーを追加した場合は、スーパーバイザー の設定を完了した後、60 日の評価期間内にそのキーを割り当てることができます。
- 3 [ワークロード管理] 画面で、[開始する] を再度クリックします。
- 4 [vCenter Server とネットワーク] 画面で、スーパーバイザー デプロイ用にセットアップされている vCenter Server システムを選択し、ネットワーク スタックとして [NSX] を選択します。
- 5 [スーパーバイザーの配置] 画面で、[クラスタのデプロイ] を選択します。
 - a 新しい スーパーバイザー の名前を入力します。
 - b 互換性のある vSphere クラスタを選択します。
 - c 選択したクラスタに自動的に作成される vSphere Zone の名前を入力します。
ゾーンの名前を指定しないと、自動的に生成されます。
 - d [次へ] をクリックします。

6 スーパーバイザー のストレージ ポリシーを選択します。

次のオブジェクトごとに選択したストレージ ポリシーによって、そのオブジェクトがストレージ ポリシーで参照されるデータストアに配置されます。各オブジェクトには、同じストレージ ポリシーを使用することも異なるストレージ ポリシーを使用することもできます。

オプション	説明
制御プレーン ストレージ ポリシー	制御プレーン仮想マシンを配置するためのストレージ ポリシーを選択します。
短期ディスク ストレージ ポリシー	vSphere ボット を配置するためのストレージ ポリシーを選択します。
イメージ キャッシュ ストレージ ポリシー	コンテナ イメージのキャッシュを配置するためのストレージ ポリシーを選択します。

7 [管理ネットワーク] 画面で、Kubernetes 制御プレーン仮想マシンに使用されるネットワークのパラメータを構成します。

a [ネットワーク モード] を選択します。

- [DHCP ネットワーク]。このモードでは、制御プレーン仮想マシンの IP アドレス、DNS サーバ、DNS、検索ドメイン、NTP サーバなど、管理ネットワークのすべての IP アドレスが DHCP から自動的に取得されます。
- [固定]。管理ネットワークのすべてのネットワーク設定を手動で入力します。

b 管理ネットワークの設定を構成します。

DHCP ネットワーク モードを選択した場合に、DHCP から取得した設定をオーバーライドするには、[追加設定] をクリックして新しい値を入力します。固定ネットワーク モードを選択した場合は、管理ネットワーク設定の値を手動で入力します。

オプション	説明
ネットワーク	VMkernel アダプタが管理トラフィック用に構成されているネットワークを選択します。
開始制御 IP アドレス	Kubernetes 制御プレーン仮想マシンに連続する 5 つの IP アドレスを予約するための開始点を決定する IP アドレスを、次のように入力します。 <ul style="list-style-type: none"> ■ Kubernetes 制御プレーン仮想マシンそれぞれの IP アドレス。 ■ 管理ネットワークへのインターフェイスとして機能するいずれかの Kubernetes 制御プレーン仮想マシンのフローティング IP アドレス。フローティング IP アドレスが割り当てられた制御プレーン仮想マシンは、3 台すべての Kubernetes 制御プレーン仮想マシンの中で主要な仮想マシンとして機能します。フローティング IP アドレスは、この Kubernetes クラスタ内の etcd リーダーであり スーパーバイザー でもある制御プレーン ノードに移動されます。これにより、ネットワーク パーティション イベントが発生した場合に、可用性が向上します。 ■ Kubernetes 制御プレーン仮想マシンで障害が発生し、新しい制御プレーン仮想マシンが引き継ぐため起動しているときにバッファとして機能する IP アドレス。
サブネット マスク	固定 IP 構成にのみ適用されます。管理ネットワークのサブネット マスクを入力します。たとえば、255.255.255.0。
DNS サーバ	環境内で使用する DNS サーバのアドレスを入力します。vCenter Server システムが FQDN で登録されている場合は、vSphere 環境で使用する DNS サーバの IP アドレスを入力して、スーパーバイザー で FQDN を解決できるようにする必要があります。
DNS 検索ドメイン	DNS が Kubernetes 制御プレーン ノード内で検索するドメイン名 (corp.local など) を入力して、DNS サーバで解決できるようにします。
NTP	環境内で使用する NTP サーバがある場合は、そのアドレスを入力します。

8 [ワークロード ネットワーク] ペインで、名前空間のネットワークの設定を構成します。

オプション	説明
vSphere Distributed Switch	スーパーバイザー のオーバーレイ ネットワークを処理する vSphere Distributed Switch を選択します。 たとえば、DSwitch を選択します。
DNS サーバ	環境内で使用する DNS サーバがある場合は、その IP アドレスを入力します。 たとえば、10.142.7.1 です。

オプション	説明
NAT モード	<p>NAT モードは、デフォルトで選択されています。</p> <p>このオプションを選択解除すると、vSphere ポッド、仮想マシン、Tanzu Kubernetes クラスタ ノードの IP アドレスなどのワークロードがいずれも Tier-0 ゲートウェイの外から直接アクセスできるようになります。Egress CIDR を構成する必要はありません。</p> <p>注： NAT モードを選択解除すると、ファイル ボリューム ストレージはサポートされません。</p>
名前空間ネットワーク	1つ以上の IP CIDR を入力してサブネット/セグメントを作成し、ワークロードに IP アドレスを割り当てます。
Ingress CIDR	Kubernetes サービスの Ingress IP アドレス範囲を決定する CIDR 注釈を入力します。この範囲は、タイプがロード バランサで Ingress のサービスに使用されます。
Edge クラスタ	<p>名前空間ネットワークに使用する Tier-0 ゲートウェイを持つ NSX Edge クラスタを選択します。</p> <p>たとえば、EDGE-CLUSTER を選択します。</p>
Tier-0 ゲートウェイ	クラスタの Tier-1 ゲートウェイに関連付ける Tier-0 ゲートウェイを選択します。
サブネット プリフィックス	名前空間セグメント用に予約されるサブネットのサイズを指定する、サブネット プリフィックスを入力します。デフォルトは 28 です。
サービス CIDR	Kubernetes サービスの IP アドレス範囲を決定する CIDR 注釈を入力します。デフォルト値を使用できます。
Egress CIDR	<p>Kubernetes サービスの Egress IP アドレスを決定する CIDR 注釈を入力します。スーパーバイザー 内の名前空間ごとに 1つの Egress IP アドレスのみが割り当てられます。</p> <p>Egress IP アドレスは、特定の名前空間内の Kubernetes ワークロードが NSX の外部と通信するために使用する IP アドレスです。</p>

- 9 [確認] 画面で、上にスクロールして、これまでに構成したすべての設定を確認し、スーパーバイザー デプロイの詳細設定を行います。

オプション	説明
スーパーバイザー制御プレーンのサイズ	<p>制御プレーン仮想マシンのサイジングを選択します。制御プレーン仮想マシンのサイズによって、スーパーバイザー で実行できるワークロードの数が決まります。以下の中から選択できます。</p> <ul style="list-style-type: none"> ■ 極小 - 2 個の CPU、8 GB のメモリ、32 GB のストレージ ■ 小 - 4 個の CPU、16 GB のメモリ、32 GB のストレージ ■ 中 - 8 個の CPU、16 GB のメモリ、32 GB のストレージ ■ 大 - 16 個の CPU、32 GB のメモリ、32 GB のストレージ <p>注： いったん制御プレーンのサイズを選択した後は、スケールアップのみ可能です。選択したサイズよりも小さなサイズにスケールダウンすることはできません。</p>
API サーバの DNS 名	<p>必要に応じて、スーパーバイザー 制御プレーンの IP アドレスを使用せずにスーパーバイザー 制御プレーンにアクセスするための FQDN を入力します。入力した FQDN は、自動生成された証明書に組み込まれます。スーパーバイザー に対して FQDN を使用することで、ロードバランサ証明書での IP アドレスの指定を省略できます。</p>
設定のエクスポート	<p>入力したスーパーバイザー 構成の値を含む JSON ファイルをエクスポートします。</p> <p>スーパーバイザー を再デプロイする場合、または類似した構成で新しいスーパーバイザー をデプロイする場合は、後でファイルを変更してインポートできます。</p> <p>スーパーバイザー 構成をエクスポートすると、スーパーバイザー を再デプロイするときこのウィザードのすべての構成値を新たに入力する必要がなく、時間を節約できます。</p>

- 10 設定を確認する準備ができたなら、[終了] をクリックします。

スーパーバイザー のデプロイにより、制御プレーン仮想マシンとその他のコンポーネントの作成と構成が開始されます。

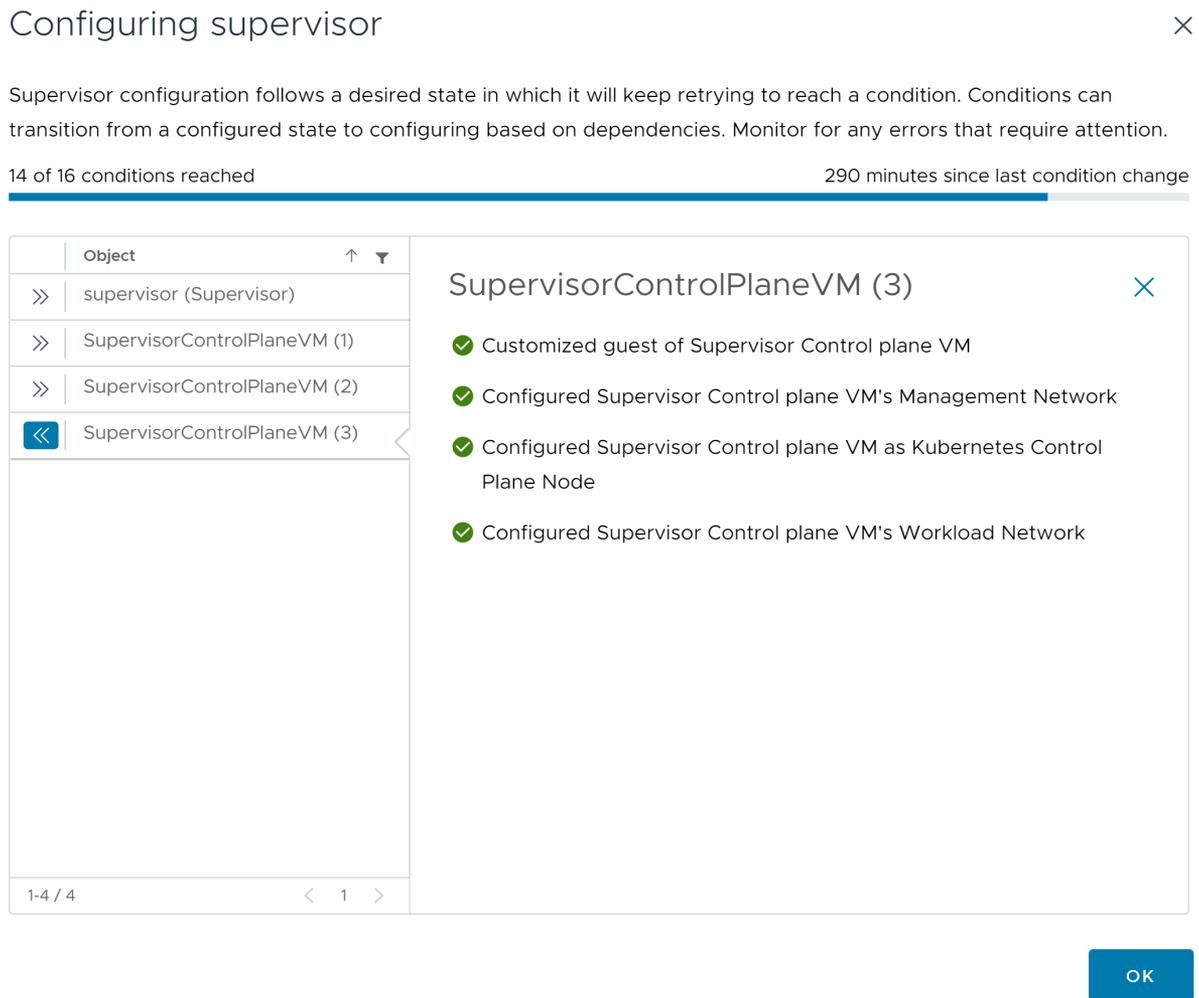
- 11 [スーパーバイザー] タブで、スーパーバイザー のデプロイ プロセスを追跡します。

- a [構成ステータス] 列で、スーパーバイザー のステータスの横にある [表示] をクリックします。
- b 各オブジェクトの構成ステータスを表示し、トラブルシューティングの対象となる潜在的な問題があれば追跡します。

次のステップ

スーパーバイザー を有効にするためのウィザードを完了したら、有効化プロセスを追跡し、トラブルシューティングを必要とする潜在的な問題を確認できます。[構成ステータス] 列で、スーパーバイザー のステータスの横にある [表示] をクリックします。

図 6-2. スーパーバイザーの有効化ビュー



デプロイ プロセスを完了するには、スーパーバイザー が目的の状態に到達する、つまり、すべての条件が満たされる必要があります。スーパーバイザー が正常に有効になると、ステータスが [設定中] から [実行中] に変わります。スーパーバイザー が [設定中] 状態の間は、各条件を満たしたかどうかが継続的に再確認されます。条件を満たさない場合、成功するまで操作が再試行されます。このため、16 件中 10 件が満たされた場合など、満たした条件の数が増減する可能性があります。たとえば、16 件中 10 件が満たされた後で、16 件中 4 件が満たされるなどです。ごくまれに、目的の状態に到達することを阻止するエラーがある場合、ステータスが [エラー] に変わることがあります。

デプロイ エラーとそのトラブルシューティング方法の詳細については、「[有効化または更新中のスーパーバイザー制御プレーン仮想マシンの健全性ステータス エラーの解決](#)」を参照してください。

ウィザードで入力した構成値を変更してスーパーバイザー を再デプロイする場合は、「[9 章 JSON 構成ファイルのインポートによるスーパーバイザー のデプロイ](#)」を参照してください。

NSX ネットワークで使用されるロード バランサの確認

7

NSX ネットワークで構成された スーパーバイザー では、NSX ロード バランサまたは NSX Advanced Load Balancer を使用できます。

NSX バージョン 4.1.1 以降を構成して、NSX Advanced Load Balancer バージョン 22.1.4 以降をインストール、構成して NSX の Enterprise ライセンスに登録している場合、NSX で使用されるロード バランサは NSX Advanced Load Balancer になります。4.1.1 よりも前のバージョンの NSX を構成している場合は、NSX ロード バランサが使用されます。

NSX で構成されているロード バランサを確認するには、次のコマンドを実行します。

```
kubectl get gateways.networking.x-k8s.io <gateway> -n <gateway_namespace> -oyaml
```

ゲートウェイファイナライザー `gateway.ako.vmware.com` または入力方向ファイナライザー `ingress.ako.vmware.com/finalizer` が仕様に含まれている場合は、NSX Advanced Load Balancer が構成されています。

スーパーバイザー 構成のエクスポート

8

既存のスーパーバイザーの構成をエクスポートする方法を確認します。この構成は後でスーパーバイザー アクティベーション ウィザードでインポートして、同じ構成で新しいスーパーバイザー インスタンスをデプロイできます。スーパーバイザーは、JSON 構成ファイルとしてエクスポートされます。これは、必要に応じて変更して、新しいスーパーバイザー インスタンスのデプロイに使用できます。

スーパーバイザー 構成をエクスポートすると、以下のことが可能になります。

- スーパーバイザー 構成の保持。以前のすべてのスーパーバイザー 構成をエクスポートし、必要に応じて再利用できます。
- より効率的なトラブルシューティング。スーパーバイザー のアクティベーションに失敗した場合は、スーパーバイザー 構成を JSON ファイル内で直接調整し、プロセスを再開できます。JSON ファイル内で設定を直接変更してからインポートできるため、迅速なトラブルシューティングが可能になります。
- 管理の合理化。エクスポートしたスーパーバイザー 構成を他の管理者と共有すれば、同様の設定で新しいスーパーバイザー を設定できます。
- 一貫性のある形式。エクスポートしたスーパーバイザー 構成は、サポート対象のデプロイ タイプに適用できる標準化された形式に準拠します。

スーパーバイザー のアクティベーション ワークフロー中に、スーパーバイザー 構成をエクスポートすることもできます。詳細については、[5 章 3 ゾーン スーパーバイザー のデプロイ](#) と [6 章 1 ゾーン スーパーバイザー のデプロイ](#) を参照してください。

前提条件

スーパーバイザー をデプロイします。

手順

- 1 [ワークロード管理] - [スーパーバイザー] - [スーパーバイザー] の順に移動します。
- 2 スーパーバイザー を選択し、[構成のエクスポート] を選択します。

結果

構成がエクスポートされ、wcp-config.zip という名前の ZIP ファイルで、ブラウザのデフォルトのダウンロードフォルダにローカルに保存されます。wcp-config.zip ファイル内には、以下のものが含まれます。

- wcp-config.json という名前のスーパーバイザー 構成を含む JSON ファイル。各構成設定には、JSON ファイル内での対応する名前と場所が含まれています。この JSON ファイルは、階層データ構造に準拠します。

- `wcp-config-schema.json` という名前の有効な JSON スキーマ ファイル。このファイルには、スーパーバイザー のすべてのエクスポート可能な設定の概要が、タイプ、JSON ファイル内での場所、その設定が必須かどうかも含めて記載されています。このスキーマ ファイルを使用して生成できるサンプル構成 JSON ファイルは、手動で入力可能で、新しいアクティベーション ワークフローにポピュレートできます。

次のステップ

,

必要に応じて JSON 構成を編集し、それを使用して新しいスーパーバイザー をデプロイします。9 章 [JSON 構成ファイルのインポートによるスーパーバイザー のデプロイ](#) を参照してください。

JSON 構成ファイルのインポートによるスーパーバイザーのデプロイ

9

以前のスーパーバイザー デプロイからエクスポートした JSON 構成ファイルをインポートすることによってスーパーバイザー アクティベーション ウィザードのすべての構成値を自動的にポピュレートする方法を確認します。スーパーバイザー のデプロイが失敗してトラブルシューティングを行うときや、同様の構成で新しいスーパーバイザー をデプロイするときは、JSON ファイルをウィザードにインポートする前にファイル内の構成値を直接変更できます。これにより、アクティベーション ウィザードのすべての値を手動で入力する時間を節約でき、変更が必要な領域を絞り込むことができます。

スーパーバイザー の構成は、次の 2 つの方法でエクスポートできます。

- スーパーバイザー のデプロイ中（ウィザードの [設定の確認] ページ）。詳細については、[5 章 3 ゾーン スーパーバイザー のデプロイ](#) と [6 章 1 ゾーン スーパーバイザー のデプロイ](#) を参照してください。
- デプロイ済みのスーパーバイザー の構成をエクスポートします。[8 章 スーパーバイザー 構成のエクスポート](#) を参照してください。

前提条件

- vSphere クラスタをスーパーバイザー として構成するための前提条件を満たすこと。[vSphere クラスタで vSphere IaaS control plane を構成するための前提条件](#)を参照してください。
- 既存のスーパーバイザー デプロイからエクスポートした JSON 構成ファイルがあることを確認します。ファイルのデフォルトの名前は、wcp-config.json です。

手順

- 1 次のいずれかの方法で、スーパーバイザー のデプロイを開始します。
 - スーパーバイザー がまだ正常にデプロイされていない場合は、[ワークロード管理] 画面で [開始する] をクリックします。
 - 環境に追加のスーパーバイザー をデプロイする場合は、[ワークロード管理] - [スーパーバイザー] - [スーパーバイザー] - [スーパーバイザーの追加] の順に選択します。
- 2 右上隅で、[構成のインポート] を選択します。

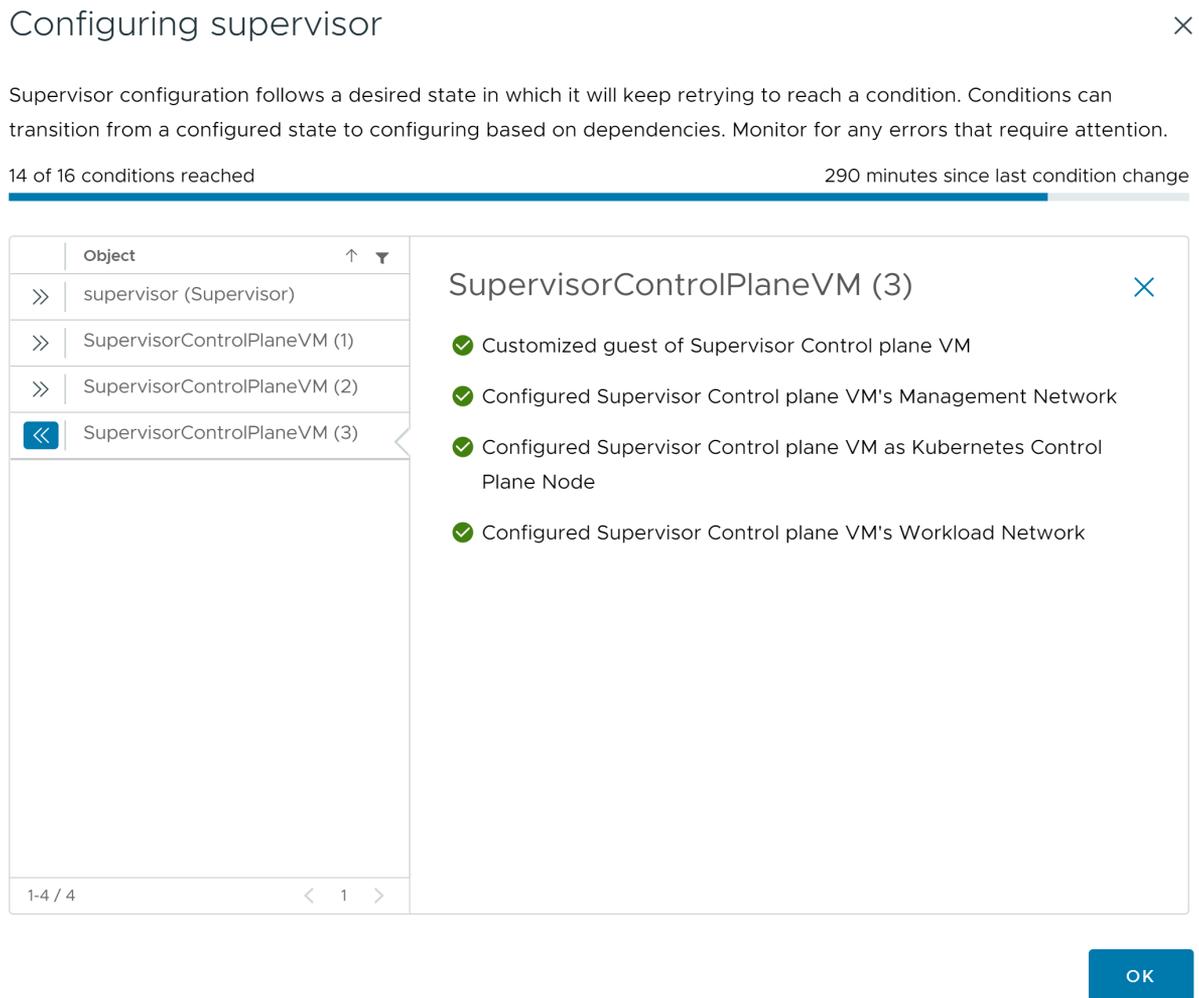
vSphere Client が JSON ファイルの値を検証します。アップロードされたファイルが無効な JSON や破損した JSON の場合、エラーが表示されます。同様に、JSON ファイルに仕様バージョンがない場合、または仕様バージョンが現在クライアントでサポートされているバージョンを超えている場合も、エラーが表示されます。したがって、構成ファイルをインポートする前には、必要な設定のみを編集する必要があります。ファイルが破損している場合は、JSON スキーマを使用して空のスーパーバイザー 構成を生成し、そこに必要な値を入力します。

- 3 [スーパーバイザー構成のアップロード] ダイアログで、[アップロード] をクリックし、以前にエクスポートした JSON 構成ファイルを選択します。
- 4 [インポート] をクリックします。
JSON 構成ファイルに記録されている値がスーパーバイザー のアクティベーション ウィザードにポピュレートされます。ロード バランサのパスワードなど、特定の設定は手動での入力が必要になります。
- 5 ウィザードで [次へ] をクリックし、必要に応じて値を入力します。
- 6 [確認] 画面で、上にスクロールして、これまでに構成したすべての設定を確認し、必要に応じて最終的な変更を加えます。
- 7 設定を確認する準備ができたなら、[終了] をクリックします。
スーパーバイザー のアクティベーションにより、制御プレーン仮想マシンとその他のコンポーネントの作成と構成が開始されます。

次のステップ

スーパーバイザー を有効にするためのウィザードを完了したら、有効化プロセスを追跡し、トラブルシューティングを必要とする潜在的な問題を確認できます。[構成ステータス] 列で、スーパーバイザー のステータスの横にある [表示] をクリックします。

図 9-1. スーパーバイザーの有効化ビュー



デプロイ プロセスを完了するには、スーパーバイザー が目的の状態に到達する、つまり、すべての条件が満たされる必要があります。スーパーバイザー が正常に有効になると、ステータスが [設定中] から [実行中] に変わります。スーパーバイザー が [設定中] 状態の間は、各条件を満たしたかどうかが継続的に再確認されます。条件を満たさない場合、成功するまで操作が再試行されます。このため、16 件中 10 件が満たされた場合など、満たした条件の数が増減する可能性があります。たとえば、16 件中 10 件が満たされた後で、16 件中 4 件が満たされるなどです。ごくまれに、目的の状態に到達することを阻止するエラーがある場合、ステータスが [エラー] に変わることがあります。

デプロイ エラーとそのトラブルシューティング方法の詳細については、「[有効化または更新中のスーパーバイザー制御プレーン仮想マシンの健全性ステータス エラーの解決](#)」を参照してください。

スーパーバイザー へのライセンスの割り当て

10

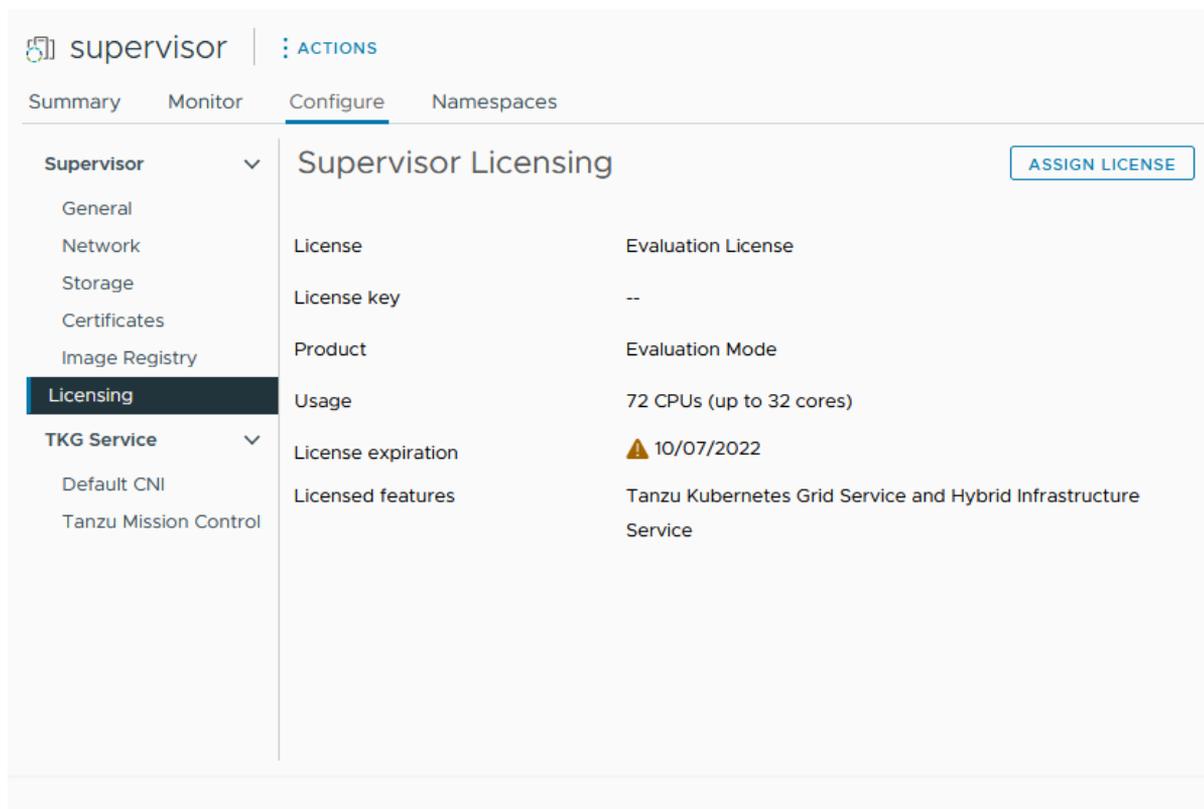
スーパーバイザー を評価モードで使用している場合は、60 日の評価期間が終了する前に、クラスタにソリューション ライセンス（VVF または VCF）または Tanzu エディション ライセンスを割り当てる必要があります。

Tanzu ライセンスの仕組みについては、「[vSphere laaS control plane のライセンス](#)」を参照してください。

手順

- 1 vSphere Client で、[ワークロード管理] に移動します。
- 2 [スーパーバイザー] を選択し、リストからスーパーバイザー を選択します。
- 3 [構成] - [ライセンス] の順に選択します。

図 10-1. スーパーバイザー UI へのライセンスの割り当て



- 4 [ライセンスの割り当て] をクリックします。

- 5 [ライセンスの割り当て] ダイアログで、[新規ライセンス] をクリックします。
- 6 有効なライセンス キーを入力し、[OK] をクリックします。

vSphere IaaS control plane クラスタへの接続

11

Tanzu Kubernetes クラスタ、vSphere ポッド、仮想マシンをプロビジョニングするには、スーパーバイザーに接続します。プロビジョニングが完了すると、さまざまな方法を使用して Tanzu Kubernetes Grid クラスタに接続し、ロールと目的に基づいて認証を行うことができます。

次のトピックを参照してください。

- vSphere 向け Kubernetes CLI Tools のダウンロードとインストール
- vSphere IaaS control plane クラスタでのセキュア ログインの構成
- vCenter Single Sign-On ユーザーとしてスーパーバイザーに接続する
- 開発者に対する Tanzu Kubernetes クラスタへのアクセス権の付与

vSphere 向け Kubernetes CLI Tools のダウンロードとインストール

vSphere 向け Kubernetes CLI Tools を使用してスーパーバイザー 制御プレーンにログインし、権限を持っている vSphere 名前空間にアクセスして、vSphere ポッド、Tanzu Kubernetes Grid クラスタ、仮想マシンをデプロイおよび管理できます。

Kubernetes CLI Tools のダウンロード パッケージには、標準のオープンソース kubectl と kubectl 向けの vSphere プラグインの 2 つの実行可能ファイルが含まれています。kubectl CLI は、プラグイン可能なアーキテクチャを備えています。kubectl 向けの vSphere プラグインでは、kubectl で使用できるコマンドが拡張されているため、vCenter Single Sign-On の認証情報によってスーパーバイザー および Tanzu Kubernetes Grid クラスタに接続できます。

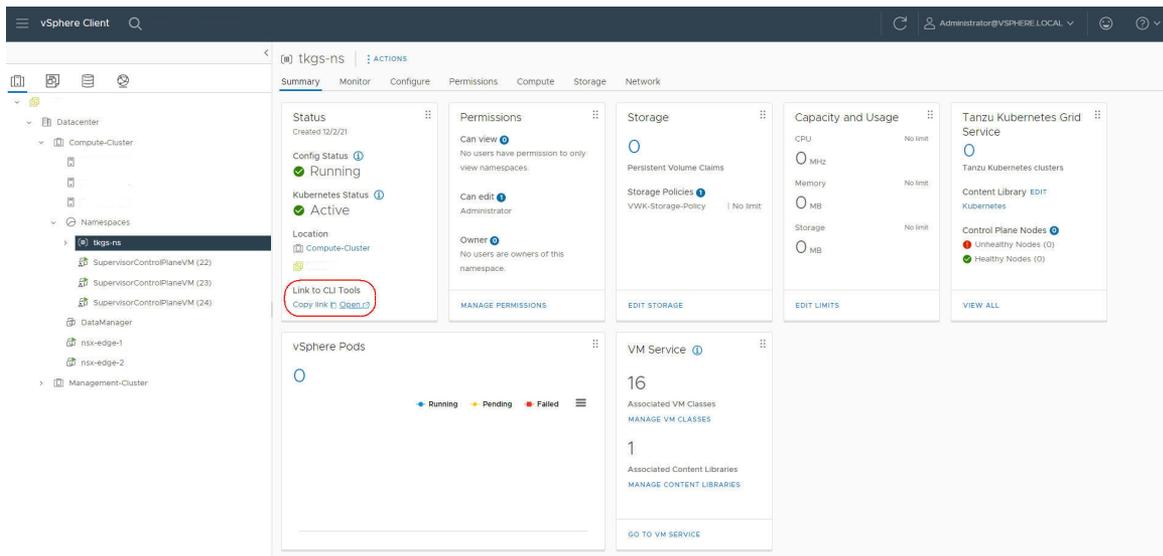
注： ベスト プラクティスとして、vSphere 名前空間 のアップデートを実行し、スーパーバイザー をアップグレードした後で、kubectl 向けの vSphere プラグイン をアップデートしてください。『vSphere IaaS 制御プレーンのメンテナンス』の [Update the vSphere Plugin for kubectl](#) を参照してください。

手順

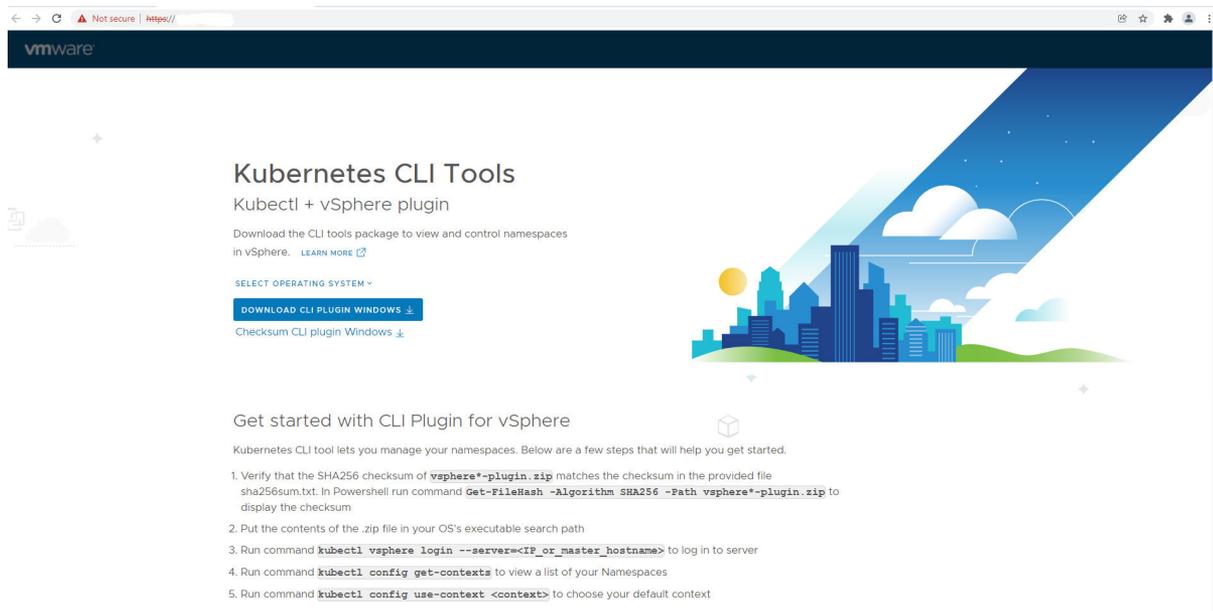
- 1 スーパーバイザー 制御プレーンの IP アドレスまたは FQDN を取得します。これは、vSphere 向け Kubernetes CLI Tools のダウンロード URL でもあります。

vSphere 環境へのアクセス権がない DevOps エンジニアの場合は、次の手順を実行するように vSphere 管理者に依頼することが考えられます。

- a vSphere Client で、[ワークロード管理] - [名前空間] の順に移動して、vSphere 名前空間 を選択します。
- b [サマリ] タブを選択し、[ステータス] ペインを特定します。
- c [CLI ツールへのリンク] で、[開く] または [リンクのコピー] をクリックします。



- 2 ブラウザで、[Kubernetes CLI Tools] のダウンロード URL を開きます。



- 3 オペレーティング システムを選択します。

- 4 `vsphere-plugin.zip` ファイルをダウンロードします。
- 5 この ZIP ファイルのコンテンツを作業ディレクトリに解凍します。
`vsphere-plugin.zip` パッケージには、`kubectl` と `kubectl` 向けの vSphere プラグイン の 2 つの実行可能ファイルが含まれています。`kubectl` は標準の Kubernetes CLI です。`kubectl-vsphere` は、vCenter Single Sign-On の認証情報を使用してスーパーバイザー および Tanzu Kubernetes クラスタで認証を行う際に役立つ `kubectl` 向けの vSphere プラグイン です。
- 6 両方の実行ファイルの場所をシステムの PATH 変数に追加します。
- 7 `kubectl` CLI のインストールを確認するには、シェル、ターミナル、またはコマンド プロンプトのセッションを開始し、`kubectl` コマンドを実行します。
`kubectl` のバナー メッセージと、CLI のコマンドライン オプションのリストが表示されます。
- 8 `kubectl` 向けの vSphere プラグイン のインストールを確認するには、`kubectl vsphere` コマンドを実行します。
`kubectl` 向けの vSphere プラグイン のバナー メッセージと、プラグインのコマンドライン オプションのリストが表示されます。

次のステップ

[vSphere IaaS control plane クラスタでのセキュア ログインの構成](#)。

vSphere IaaS control plane クラスタでのセキュア ログインの構成

スーパーバイザー や Tanzu Kubernetes Grid クラスタに安全にログインするには、適切な TLS 証明書を使用して `kubectl` 向けの vSphere プラグイン を構成し、プラグインの最新バージョンが実行されるようにします。

スーパーバイザー CA 証明書

vSphere IaaS control plane は、`kubectl` 向けの vSphere プラグイン コマンド `kubectl vsphere login ...` を使用することにより、クラスタ アクセスのための vCenter Single Sign-On をサポートします。このユーティリティをインストールして使用するには、[vSphere 向け Kubernetes CLI Tools のダウンロードとインストール](#) を参照してください。

`kubectl` 向けの vSphere プラグイン では、デフォルトで安全なログインが行われ、信頼されている証明書が必要とされます。デフォルトは、vCenter Server ルート CA によって署名された証明書です。プラグインは `--insecure-skip-tls-verify` フラグをサポートしていますが、これはセキュリティ上の理由から推奨されません。

`kubectl` 向けの vSphere プラグイン を使用してスーパーバイザー および Tanzu Kubernetes Grid クラスタに安全にログインするには、次の 2 つのオプションがあります。

オプション	方法
各クライアント マシンに vCenter Server 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。	VMware ナレッジベースの記事 Web ブラウザで証明書に関する警告表示を出さないようにするために vCenter Server のルート証明書をダウンロードしてインストールする方法を参照してください。
スーパーバイザー で使用される VIP 証明書を、各クライアント マシンが信頼する CA によって署名された証明書に置き換えます。	スーパーバイザー API エンドポイントに安全に接続するための VIP 証明書の置き換えを参照してください

注： vCenter Single Sign-On、vCenter Server 証明書の管理とローテーション、認証のトラブルシューティングなど、vSphere 認証の詳細については、[vSphere Authentication](#) のドキュメントを参照してください。vSphere IaaS control plane の証明書の詳細については、VMware ナレッジベースの記事 [KB89324](#) を参照してください。

Tanzu Kubernetes Grid クラスタ CA 証明書

kubectl CLI を使用して Tanzu Kubernetes クラスタ API サーバと安全に接続するには、Tanzu Kubernetes クラスタ CA 証明書をダウンロードします。

kubectl 向けの vSphere プラグイン の最新バージョンを使用している場合、Tanzu Kubernetes Grid クラスタに初めてログインすると、プラグインによって kubeconfig ファイルに Tanzu Kubernetes クラスタ CA 証明書が登録されます。この証明書は `TANZU-KUBERNETES-NAME-ca` という名前の Kubernetes シークレットに格納されます。プラグインは、この証明書を使用して、対応するクラスタの CA データストアの CA 情報をポピュレートします。

vSphere IaaS control plane をアップデートする場合は、プラグインの最新バージョンに更新してください。『vSphere IaaS 制御プレーンのメンテナンス』の [Update the vSphere Plugin for kubectl](#) を参照してください。

vCenter Single Sign-On ユーザーとして スーパーバイザー に接続する

vSphere ポッド、Tanzu Kubernetes Grid クラスタ、または仮想マシンをプロビジョニングするには、kubectl 向けの vSphere プラグイン を使用して スーパーバイザー に接続し、vCenter Single Sign-On 認証情報によって認証します。

スーパーバイザー にログインすると、kubectl 向けの vSphere プラグイン によって スーパーバイザー のコンテキストが生成されます。Kubernetes では、構成コンテキストには スーパーバイザー、vSphere 名前空間、ユーザーが含まれます。クラスタのコンテキストは `.kube/config` ファイルで確認できます。このファイルは、通常、kubeconfig ファイルと呼ばれます。

注： 既存の kubeconfig ファイルがある場合は、そのファイルに各 スーパーバイザー コンテキストが追加されます。kubectl 向けの vSphere プラグイン は、kubectl 自体が使用する KUBECONFIG 環境変数に従います。必須ではありませんが、`kubectl vsphere login ...` を実行する前にこの変数を設定することで、(情報が現在の kubeconfig ファイルに追加されるのではなく) 新しいファイルに書き込まれるようにすることができます。

前提条件

- vCenter Single Sign-On 認証情報は、vSphere 管理者から取得します。

- vSphere 管理者から スーパーバイザー の制御プレーンの IP アドレスを取得します。スーパーバイザー 制御プレーンの IP アドレスは、各 vSphere 名前空間 のユーザー インターフェイスにある、vSphere Client の [ワークロード管理] でリンクされます。
- 制御プレーンの IP アドレスではなく FQDN を使用してログインするには、スーパーバイザー を有効にするときに構成された FQDN を取得します。
- 権限を持つ vSphere 名前空間 の名前を取得します。
- vSphere 名前空間 での編集権限があることを確認します。
- [vSphere 向け Kubernetes CLI Tools のダウンロードとインストール](#)。
- 署名を付与する認証局 (CA) を Trust Root としてインストールするか、または証明書を Trust Root として直接追加することにより、Kubernetes 制御プレーンによって提供される証明書がシステムで信頼されることを確認します。[vSphere IaaS control plane クラスタでのセキュア ログインの構成](#)を参照してください。

手順

- 1 ログインのコマンド構文とオプションを表示するには、次のコマンドを実行します。

```
kubectl vsphere login --help
```

- 2 スーパーバイザー に接続するには、次のコマンドを実行します。

```
kubectl vsphere login --server=<KUBERNETES-CONTROL-PLANE-IP-ADDRESS> --vsphere-username <VCENTER-SSO-USER>
```

FQDN を使用してログインすることもできます。

```
kubectl vsphere login --server <KUBERNETES-CONTROL-PLANE-FQDN> --vsphere-username <VCENTER-SSO-USER>
```

例：

```
kubectl vsphere login --server=10.92.42.13 --vsphere-username administrator@example.com
```

```
kubectl vsphere login --server wonderland.acme.com --vsphere-username administrator@example.com
```

この操作により、Kubernetes API への認証に使用する JSON Web トークン (JWT) を含む設定ファイルが作成されます。

- 3 認証するには、ユーザーのパスワードを入力します。

スーパーバイザー に接続すると、アクセス可能な設定コンテキストが表示されます。例：

```
You have access to the following contexts:
tanzu-ns-1
tkg-cluster-1
tkg-cluster-2
```

- 4 アクセスする権限のある設定コンテキストの詳細を表示するには、次の `kubectl` コマンドを実行します。

```
kubectl config get-contexts
```

CLI に、使用可能な各コンテキストの詳細が表示されます。

- 5 コンテキストを切り替えるには、次のコマンドを使用します。

```
kubectl config use-context <example-context-name>
```

次のステップ

vCenter Single Sign-On ユーザーとして Tanzu Kubernetes Grid クラスタに接続します。詳細については、『vSphere IaaS 制御プレーンでの TKG サービスの使用』の [vCenter Single Sign-On ユーザーとしての TKG クラスタへの接続](#) を参照してください。

開発者に対する Tanzu Kubernetes クラスタへのアクセス権の付与

開発者は、Kubernetes が対象としているユーザーです。Tanzu Kubernetes クラスタをプロビジョニングすると、vCenter Single Sign-On 認証を使用して開発者にアクセス権を付与することができます。

開発者向けの認証

クラスタ管理者は、開発者などの他のユーザーにクラスタへのアクセス権を付与できます。開発者は、ユーザー アカウントを使用して直接、またはサービス アカウントを使用して間接的に、クラスタにポッドをデプロイできます。詳細については、『vSphere IaaS 制御プレーンでの TKG サービスの使用』の [Grant Developers SSO Access to Workload Clusters](#) を参照してください。

- ユーザー アカウント認証の場合、Tanzu Kubernetes クラスタは vCenter Single Sign-On のユーザーとグループをサポートします。ユーザーまたはグループは、vCenter Server のローカルであるか、サポートされているディレクトリ サーバから同期されます。
- サービス アカウント認証の場合は、サービス トークンを使用できます。詳細については、Kubernetes のドキュメントを参照してください。

クラスタへの開発者ユーザーの追加

開発者にクラスタ アクセスを許可するには：

- 1 ユーザーまたはグループの Role または ClusterRole を定義し、クラスタに適用します。詳細については、Kubernetes のドキュメントを参照してください。
- 2 ユーザーまたはグループの RoleBinding または ClusterRoleBinding を作成し、クラスタに適用します。次の例を参照してください。

RoleBinding の例

vCenter Single Sign-On のユーザーまたはグループにアクセス権を付与するには、RoleBinding のサブジェクトに `name` パラメータの値として次のいずれかを含める必要があります。

表 11-1. サポートされているユーザーおよびグループのフィールド

フィールド	説明
<code>sso:USER-NAME@DOMAIN</code>	たとえば、 <code>sso:joe@vsphere.local</code> などのローカル ユーザー名です。
<code>sso:GROUP-NAME@DOMAIN</code>	たとえば、 <code>sso:devs@ldap.example.com</code> などの vCenter Server と統合されたディレクトリ サーバのグループ名です。

次の RoleBinding の例では、Joe という vCenter Single Sign-On ローカル ユーザーが、edit というデフォルトの ClusterRole にバインドされます。このロールにより、名前空間（この例では default 名前空間）内のほとんどのオブジェクトに対する読み取り/書き込みアクセスが許可されます。

```
kind: RoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: rolebinding-cluster-user-joe
  namespace: default
roleRef:
  kind: ClusterRole
  name: edit
  apiGroup: rbac.authorization.k8s.io
subjects:
- kind: User
  name: sso:joe@vsphere.local
  apiGroup: rbac.authorization.k8s.io
```

スーパーバイザー の構成と管理

12

vSphere 管理者は、vSphere クラスタをスーパーバイザーとして有効にします。スーパーバイザーを作成する際に、ネットワークソリューションとして vSphere ネットワーク スタックを使用するのか、あるいは VMware NSX® (NSX) を使用するのかを選択できます。NSX を使用して構成されたクラスタでは、vSphere ポッドと、VMware Tanzu™ Kubernetes Grid™ を介して作成された Tanzu Kubernetes クラスタの実行がサポートされます。vSphere ネットワーク スタックが構成されたスーパーバイザーでは、Tanzu Kubernetes クラスタのみがサポートされます。

スーパーバイザーを有効にした後で、vSphere Client を使用したクラスタの管理と監視が可能になります。

次のトピックを参照してください。

- [スーパーバイザー API エンドポイントに安全に接続するための VIP 証明書の置き換え](#)
- [スーパーバイザーの Tanzu Kubernetes Grid と Tanzu Mission Control の統合](#)
- [Tanzu Kubernetes Grid クラスタのデフォルト CNI の設定](#)
- [スーパーバイザーの制御プレーンサイズの変更](#)
- [VDS ネットワークが構成されているスーパーバイザーのロード バランサ設定の変更](#)
- [VDS ネットワークが構成されているスーパーバイザーへのワークロード ネットワークの追加](#)
- [スーパーバイザーの管理ネットワーク設定の変更](#)
- [VDS ネットワークが構成されているスーパーバイザーのワークロード ネットワーク設定の変更](#)
- [NSX が構成されているスーパーバイザーのワークロード ネットワーク設定の変更](#)
- [vSphere IaaS control plane での HTTP プロキシ設定の構成](#)
- [TKG サービス クラスタで使用する外部 ID プロバイダの構成](#)
- [スーパーバイザーへの外部 IDP の登録](#)
- [スーパーバイザーのストレージ設定の変更](#)
- [カスタム可観測プラットフォームへのスーパーバイザー メトリックのストリーミング](#)
- [スーパーバイザー 制御プレーンの DNS 名のリストの変更](#)
- [外部監視システムへのスーパーバイザー ログの転送](#)

スーパーバイザー API エンドポイントに安全に接続するための VIP 証明書の置き換え

vSphere 管理者は、仮想 IP アドレス (VIP) の証明書を置き換えて、ホストがすでに信頼している CA で署名された証明書を使用して、スーパーバイザー API エンドポイントに安全に接続することができます。証明書は、ログイン時と以降のスーパーバイザーの操作の両方で、DevOps エンジニアに対して Kubernetes 制御プレーンを認証します。

前提条件

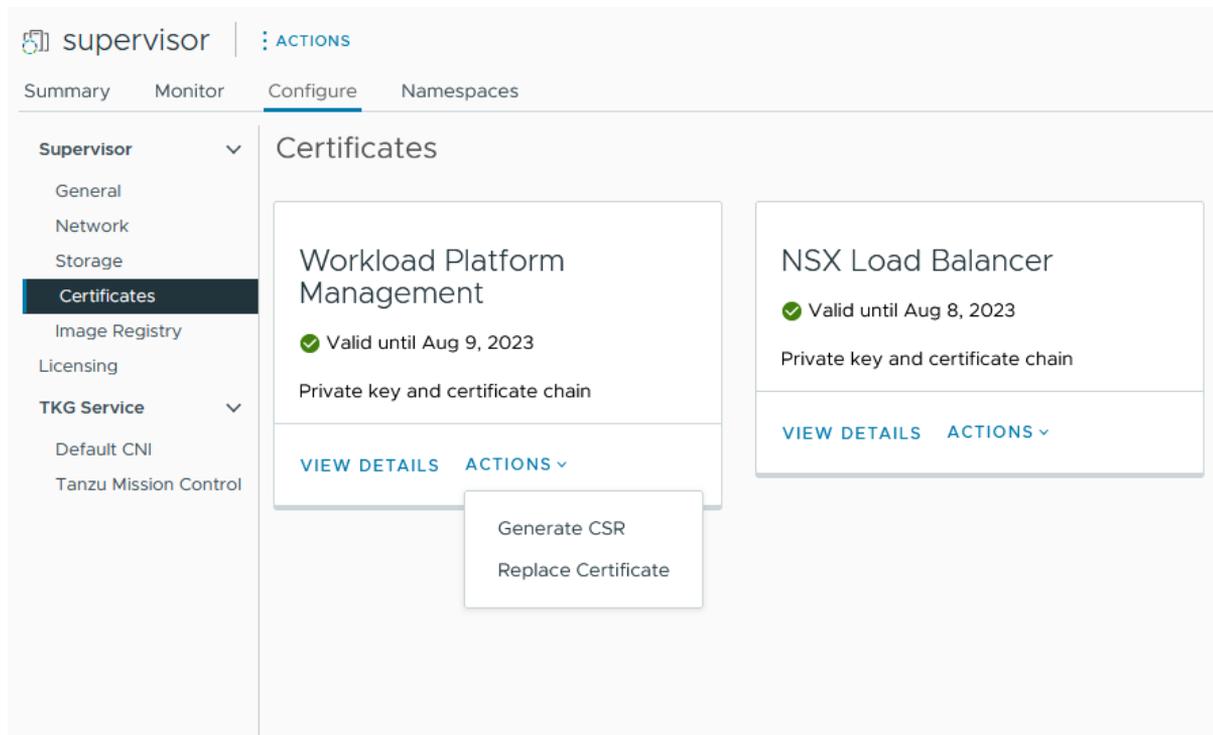
CSR に署名できる認証局 (CA) へのアクセス権があることを確認します。DevOps エンジニアの場合、認証局 (CA) を信頼できるルートとしてシステムにインストールする必要があります。

スーパーバイザー 証明書の詳細については、[スーパーバイザー CA 証明書](#)を参照してください。

手順

- 1 vSphere Client で、[ワークロード管理] に移動します。
- 2 [スーパーバイザー] を選択し、リストからスーパーバイザーを選択します。
- 3 [構成] をクリックし、[証明書] を選択します。
- 4 [ワークロード管理プラットフォーム] ペインで、[アクション] - [CSR の生成] の順に選択します。

図 12-1. スーパーバイザーのデフォルトの証明書の置換



- 5 証明書の詳細を入力します。

注： ID プロバイダ サービスを使用する場合は、証明書チェーン全体も含める必要があります。ただし、標準の HTTPS トラフィックにはチェーンは必要ありません。

- 6 CSR が生成されたら、[コピー] をクリックします。
- 7 認証局 (CA) を使用して証明書に署名します。
- 8 [ワークロード管理プラットフォーム] ペインで、[アクション] - [証明書の置き換え] の順に選択します。
- 9 署名付き証明書ファイルをアップロードし、[証明書の置き換え] をクリックします。
- 10 Kubernetes 制御プレーンの IP アドレスで証明書を検証します。

たとえば、vSphere 向け Kubernetes CLI Tools のダウンロード画面を開き、ブラウザを使用して証明書が正常に置き換えられたことを確認できます。Linux または UNIX システムでは、`echo | openssl s_client -connect https://ip:6443` も使用できます。

スーパーバイザー の Tanzu Kubernetes Grid と Tanzu Mission Control の統合

スーパーバイザー で実行される Tanzu Kubernetes Grid と Tanzu Mission Control を統合できます。統合により、Tanzu Mission Control を使用した Tanzu Kubernetes クラスタのプロビジョニングと管理が可能になります。

Tanzu Mission Control の詳細については、[Tanzu Kubernetes クラスタのライフサイクルの管理](#)を参照してください。デモを見るには、[Tanzu Mission Control Integrated with Tanzu Kubernetes Grid Service](#) のビデオを確認してください。

スーパーバイザー の Tanzu Mission Control 名前空間の表示

vSphere IaaS control plane v7.0.1 U1 以降には Tanzu Mission Control 用の vSphere 名前空間 が付属しています。この名前空間は、Tanzu Mission Control エージェントをインストールするスーパーバイザー 上に存在します。エージェントをインストールすると、Tanzu Mission Control の Web インターフェイスを使用して Tanzu Kubernetes Grid クラスタをプロビジョニングおよび管理できるようになります。

- 1 kubectl 向けの vSphere プラグイン を使用して、スーパーバイザー での認証を行います。[vCenter Single Sign-On ユーザーとしてスーパーバイザー に接続する](#)を参照してください。
- 2 次のように、コンテキストをスーパーバイザー に切り替えます。

```
kubectl config use-context 10.199.95.59
```

- 3 次のコマンドを実行して、名前空間を一覧表示します。

```
kubectl get ns
```

- 4 Tanzu Mission Control に提供される vSphere 名前空間 は `svc-tmc-cXX` として識別されます (XX は数字)。

- 5 この名前空間に Tanzu Mission Control エージェントをインストールします。スーパーバイザー への [Tanzu Mission Control エージェントのインストール](#) を参照してください。

スーパーバイザー への Tanzu Mission Control エージェントのインストール

Tanzu Kubernetes Grid を Tanzu Mission Control と統合するには、スーパーバイザー にエージェントをインストールします。

注： 次の手順では、スーパーバイザー バージョン 1.21.0 以降を使用する vSphere 7.0 U3 以降が必要です。

- 1 Tanzu Mission Control Web インターフェイスを使用して、スーパーバイザー を Tanzu Mission Control に登録します。[管理クラスタの Tanzu Mission Control への登録](#) を参照してください。
- 2 Tanzu Mission Control Web インターフェイスを使用して、[管理] - [管理クラスタ] に移動して、登録 URL を取得します。
- 3 vSphere IaaS control plane 環境で、Tanzu Mission Control で必要となるポート（通常は 443）用のファイアウォール ポートを開きます。[クラスタ エージェント拡張機能によって確立される送信接続](#) を参照してください。
- 4 vSphere Client を使用して、vSphere IaaS control plane 環境にログインします。
- 5 [ワークロード管理] を選択し、スーパーバイザー を選択します。
- 6 [構成] を選択し、[TKG サービス] - [Tanzu Mission Control] の順に選択します。
- 7 [登録 URL] フィールドで登録 URL を指定します。
- 8 [登録] をクリックします。

The screenshot shows the vSphere Client interface for configuring Tanzu Mission Control. The breadcrumb path is 'compute-cluster' > 'ACTIONS'. The 'Configure' tab is selected, and the left sidebar shows 'Namespaces' > 'TKG Service' > 'Tanzu Mission Control' selected. The main content area is titled 'Tanzu Mission Control Registration' and contains the instruction: 'Add a URL token here to automatically connect all of your Tanzu Kubernetes clusters to Tanzu Mission Control.' Below this is a 'Registration URL' field with an information icon, containing the URL: `https://myorg.tmc.cloud.vmware.com/installer?id=121f2verylongstring23e&source=registration`. At the bottom right, there are 'REGISTER' and 'CANCEL' buttons.

Tanzu Mission Control エージェントのアンインストール

スーパーバイザーから Tanzu Mission Control エージェントをアンインストールするには、「[vSphere IaaS control plane](#) におけるスーパーバイザー クラスタからのクラスタ エージェントの手動削除」を参照してください。

Tanzu Kubernetes Grid クラスタのデフォルト CNI の設定

vSphere 管理者は、Tanzu Kubernetes クラスタのデフォルトのコンテナ ネットワーク インターフェイス (CNI) を設定できます。

デフォルトの CNI

Tanzu Kubernetes Grid は、Tanzu Kubernetes Grid クラスタについて、[Antrea](#) と [Calico](#) の 2 つの CNI オプションをサポートしています。

システムで定義されているデフォルトの CNI は Antrea です。デフォルトの CNI 設定の詳細については、vSphere IaaS 制御プレーンでの TKG サービスの使用を参照してください。

デフォルトの CNI は、vSphere Client を使用して変更できます。デフォルトの CNI を設定するには、次の手順を実行します。

注意： デフォルトの CNI の変更は、グローバルに行われます。新しく設定されたデフォルトは、サービスによって作成されたすべての新規クラスタに適用されます。既存のクラスタは変更されません。

- 1 vSphere Client を使用して、vSphere IaaS control plane 環境にログインします。
- 2 [ワークロード管理]、[スーパーバイザー] の順に選択します。
- 3 リストから スーパーバイザー インスタンスを選択します。
- 4 [構成] を選択し、[TKG サービス] - [デフォルトの CNI] の順に選択します。
- 5 新規のクラスタに対してデフォルトの CNI を選択します。
- 6 [更新] をクリックします。

次の図は、デフォルトの CNI が選択されている様子を示しています。

The screenshot shows the Supervisor web interface. The top navigation bar includes 'supervisor' and 'ACTIONS'. Below it are tabs for 'Summary', 'Monitor', 'Configure', and 'Namespaces'. The left sidebar lists various configuration categories: 'Supervisor' (General, Network, Storage, Certificates, Image Registry, Licensing), 'TKG Service' (Default CNI, Tanzu Mission Control). The main content area is titled 'Default Tanzu Kubernetes cluster Container Network Plugin (CNI)'. It contains a yellow warning box stating: 'The setting applies globally to all new clusters. Existing clusters are unchanged.' Below this, there are two radio button options: 'Antrea' (marked as 'default') and 'Calico' (which is selected). Each option has a brief description. At the bottom of the configuration area are 'UPDATE' and 'CANCEL' buttons.

次の図は、CNI の選択が Antrea から Calico に変更された様子を示しています。

supervisor | : ACTIONS

Summary Monitor **Configure** Namespaces

Supervisor

- General
- Network
- Storage
- Certificates
- Image Registry
- Licensing

TKG Service

- Default CNI**
- Tanzu Mission Control

Default Tanzu Kubernetes cluster Container Network Plugin (CNI)

Your Tanzu Kubernetes clusters require a CNI for container networks. Below are the two supported offerings you can choose between as the default CNI for new clusters.

✓ The Tanzu Kubernetes Grid Service configuration was successfully updated!

Antrea **default**

Antrea is a network solution for Kubernetes clusters. Antrea uses Open vSwitch as the networking data plane which supports both Linux and Windows.

Calico

Calico is a network solution for Kubernetes clusters. It uses native Linux kernel performance.

UPDATE

スーパーバイザー の制御プレーン サイズの変更

vSphere IaaS control plane 環境にある スーパーバイザー の Kubernetes 制御プレーン仮想マシンのサイズを変更する方法を確認します。

前提条件

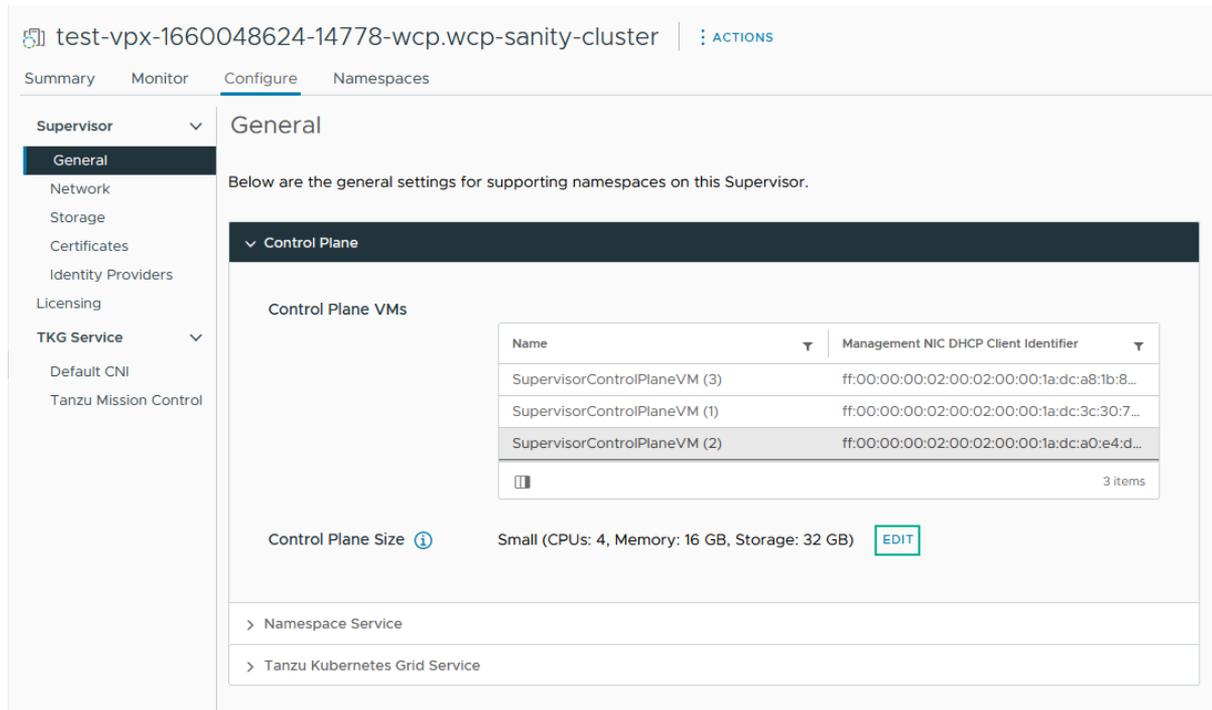
- クラスタに関するクラスタ全体の構成の変更権限があることを確認します。

手順

- 1 vSphere Client で、[ワークロード管理] に移動します。
- 2 [スーパーバイザー] で、[スーパーバイザー] を選択します。
- 3 [構成]、[全般] の順に選択します。

- 4 [制御プレーンのサイズ] を拡張します。

図 12-2. スーパーバイザー制御プレーンの設定



- 5 [編集] をクリックし、ドロップダウンメニューから制御プレーンの新しいサイズを選択します。

オプション	説明
極小	2 個の CPU、8 GB のメモリ、32 GB のストレージ
小	4 個の CPU、16 GB のメモリ、32 GB のストレージ
中	8 個の CPU、16 GB のメモリ、32 GB のストレージ
大	16 個の CPU、32 GB のメモリ、32 GB のストレージ

注： 制御プレーンのサイズを選択した後は、スケールダウンできません。たとえば、スーパーバイザーのアクティベーション中に [極小] オプションをすでに設定していた場合は、スケールアップのみが可能です。

- 6 [保存] をクリックします。

制御プレーンのサイズは、スケールアップのみが可能です。

VDS ネットワークが構成されているスーパーバイザーのロードバランサ設定の変更

スーパーバイザーの VDS ネットワークスタックで構成されたロードバランサの設定を変更する方法を確認します。ユーザー名やパスワードなどの設定の変更、新しい IP アドレス範囲の追加、ロードバランサで使用される証明書の更新を行うことができます。

前提条件

- クラスタに関するクラスタ全体の構成の変更権限があることを確認します。

手順

- 1 vSphere Client で、[ワークロード管理] に移動します。
- 2 [スーパーバイザー] で、[スーパーバイザー]、[構成] の順に選択します。
- 3 [ネットワーク] を選択し、[ワークロード ネットワーク] を展開します。

The screenshot shows the configuration page for a Load Balancer in the Supervisor interface. The left sidebar shows the navigation menu with 'Network' selected under 'Supervisor Services'. The main content area is titled 'Load Balancer' and contains the following configuration details:

- Name:** lb-1
- Load Balancer:** HAProxy
- Type:** (with an information icon)
- HAProxy Load Balancer Controller Endpoint:** 10.168.191.36:5556
- Username:** wcp (with an information icon and an 'EDIT' link)
- Password:** (with an information icon and an 'EDIT' link)
- Virtual IP Ranges:** (with an information icon and an 'Add' link) 192.168.0.1 - 192.168.1.0
- HAProxy Management:** (with an information icon and an 'EDIT' link) Certificate text: -----BEGIN CERTIFICATE----- MIIDqDCCApCgAwIBAgICHtoWdQYJKoZIhvcNAQELBQAwdTELMAkGA1UEBhMCVWxvTFFcZdGRxNzANRzANVRAhMR17Nd2Fv

オプション	説明
設定	説明
ユーザー名	スーパーバイザー がロード バランサ エンドポイントでの認証に使用するユーザー名を編集します。
パスワード	スーパーバイザー がロード バランサ エンドポイントでの認証に使用するパスワードを変更します。
仮想 IP アドレスの範囲	ロード バランサに対して最初に構成した仮想 IP CIDR 範囲のサブセットである IP アドレス範囲を追加します。 注: 新しい IP アドレス範囲の追加のみが可能です。既存の IP アドレス範囲を削除または変更することはできません。
TLS 証明書	スーパーバイザー とロード バランサの間のセキュアな接続を確保するために使用する TLS 証明書を変更します。

VDS ネットワークが構成されている スーパーバイザー へのワークロード ネットワークの追加

スーパーバイザー に vSphere ネットワーク スタックが構成されている場合は、ワークロード ネットワークを作成して名前空間に割り当てることにより、Kubernetes ワークロードに対するレイヤー 2 の隔離を実現できます。ワークロード ネットワークでは、名前空間内の Tanzu Kubernetes Grid クラスタに接続できます。また、ワークロード ネットワークは、スーパーバイザー 内のホストに接続されているスイッチの分散ポート グループによってバックアップされます。

スーパーバイザー に実装できるトポロジの詳細については、『vSphere IaaS 制御プレーンの概念と計画』の [vSphere ネットワークと NSX Advanced Load Balancer を使用したスーパーバイザーのトポロジ](#) または [HAProxy ロード バランサをデプロイするトポロジ](#) を参照してください。

注： ワークロード ネットワークのネットワーク設定を割り当てる DHCP サーバをスーパーバイザー に構成している場合には、スーパーバイザー の構成後に新しいワークロード ネットワークを作成することはできません。

前提条件

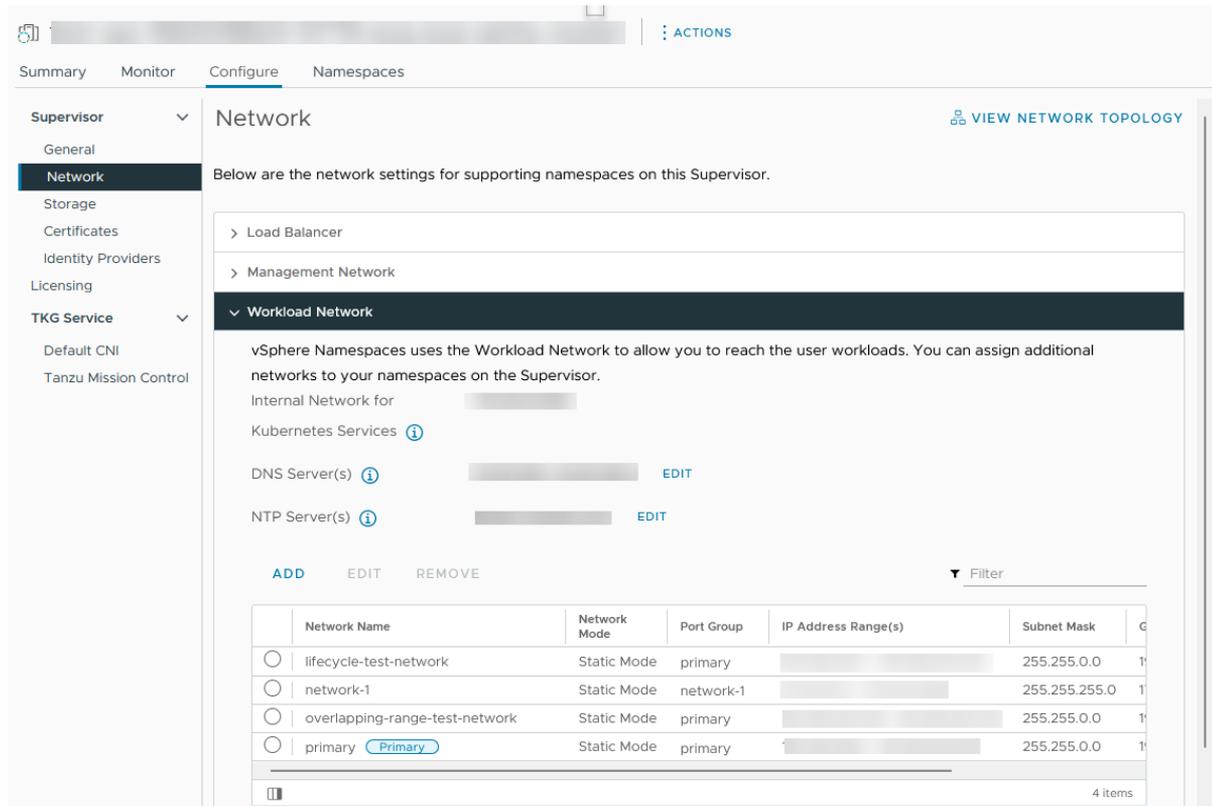
- ワークロード ネットワークをバックアップする分散ポート グループを作成します。
- ワークロード ネットワークに割り当てる IP アドレス範囲が、環境内で使用可能なすべてのスーパーバイザー 内で一意であることを確認します。

手順

- 1 vSphere Client で、[ワークロード管理] に移動します。
- 2 [スーパーバイザー] で、[スーパーバイザー] を選択します。

3 [構成]、[ネットワーク]の順に選択します。

図 12-3. スーパーバイザー ワークロード ネットワークの追加



4 [ワークロード ネットワーク] を選択して、[追加] をクリックします。

オプション	説明
ポート グループ	このワークロード ネットワークに関連付ける分散ポート グループを選択します。スーパーバイザー ネットワーク用に構成された vSphere Distributed Switch (VDS) には、選択元となるポート グループが含まれています。
ネットワーク名	名前空間に割り当てられるときにワークロード ネットワークを識別するネットワーク名。この値は、選択したポート グループの名前から自動的に入力されますが、必要に応じて変更できます。
IP アドレス範囲	Tanzu Kubernetes Grid クラスター ノードに割り当てる IP アドレス範囲を入力します。IP アドレス範囲は、サブネット マスクによって示されるサブネットに含まれている必要があります。 注： ワークロード ネットワークごとに一意の IP アドレス範囲を使用する必要があります。複数のネットワークに同じ IP アドレス範囲を構成しないでください。
サブネット マスク	ポート グループのネットワークのサブネット マスクの IP アドレスを入力します。
ゲートウェイ	ポート グループ上のネットワークのデフォルト ゲートウェイを入力します。ゲートウェイは、サブネット マスクによって示されるサブネットに含まれている必要があります。 注： HAProxy ロードバランサーに割り当てられたゲートウェイは使用しないでください。

5 [追加] をクリックします。

次のステップ

新しく作成したワークロード ネットワークを vSphere 名前空間 に割り当てます。

スーパーバイザー の管理ネットワーク設定の変更

vSphere IaaS control plane 環境で スーパーバイザー 管理ネットワークの DNS および NTP 設定を更新する方法について説明します。

前提条件

- クラスタに関するクラスタ全体の構成の変更権限があることを確認します。

手順

- 1 vSphere Client で、[ワークロード管理] を選択します。
- 2 [スーパーバイザー] で、[スーパーバイザー]、[構成] の順に選択します。
- 3 [ネットワーク] を選択し、[管理ネットワーク] を展開します。

図 12-4. スーパーバイザー管理ネットワークの設定の更新

The screenshot shows the vSphere Client interface for a Supervisor named 'test-vpx-1660048624-14778-wcp.wcp-sanity-cluster'. The 'Configure' tab is active, and the 'Network' section is selected in the left-hand navigation menu. The main content area displays the 'Management Network' settings for supporting namespaces on this Supervisor. The settings are as follows:

Setting	Value	Action
Network Mode	DHCP	
Network	VM Network	
Floating IP	10.78.162.199	
DNS Server(s)	Acquired via DHCP	EDIT
DNS Search Domain(s)	Acquired via DHCP	EDIT
NTP Server(s)	time1.vmware.com	EDIT

4 DNS および NTP 設定を編集します。

オプション	説明
DNS サーバ	環境内で使用する DNS サーバのアドレスを入力します。vCenter Server システムが FQDN で登録されている場合は、vSphere 環境で使用する DNS サーバの IP アドレスを入力して、スーパーバイザーで FQDN を解決できるようにする必要があります。
DNS 検索ドメイン	DNS が Kubernetes 制御プレーン ノード内で検索するドメイン名 (corp.local など) を入力して、DNS サーバで解決できるようにします。
NTP サーバ	環境内で使用する NTP サーバがある場合は、そのアドレスを入力します。

VDS ネットワークが構成されている スーパーバイザー のワークロード ネットワーク設定の変更

VDS ネットワーク スタックが構成されている スーパーバイザー のワークロード ネットワークについて、その NTP および DNS サーバ設定を変更する方法を確認します。ワークロード ネットワーク用に構成する DNS サーバは、Kubernetes ワークロードに公開される外部 DNS サーバであり、スーパーバイザー の外部でホストされるデフォルトのドメイン名を解決します。

前提条件

- クラスタに関するクラスタ全体の構成の変更権限があることを確認します。

手順

- 1 vSphere Client で、[ワークロード管理] を選択します。
- 2 [スーパーバイザー] で、[スーパーバイザー]、[構成] の順に選択します。
- 3 [ネットワーク] を選択し、[ワークロード ネットワーク] を展開します。



注： vSphere 名前空間 に割り当て済みのワークロード ネットワークは削除できません。ワークロード ネットワークを削除する必要がある場合は、そのネットワークに接続されているすべての vSphere 名前空間 を削除する必要があります。また、プライマリ ワークロード ネットワークは、編集も削除もできません。

4 DNS サーバ設定を編集します。

vCenter Server などの vSphere 管理コンポーネントのドメイン名を解決できる DNS サーバのアドレスを入力します。

たとえば、**10.142.7.1** のように入力します。

DNS サーバの IP アドレスを入力すると、各制御プレーン仮想マシンにスタティック ルートが追加されます。これは、DNS サーバへのトラフィックがワークロード ネットワークを通過することを意味します。

指定した DNS サーバが管理ネットワークとワークロード ネットワークの間で共有されている場合、制御プレーン仮想マシンの DNS ルックアップは、初期セットアップ後にワークロード ネットワークを介してルーティングされます。

- 5 必要に応じて NTP 設定を編集します。
- 6 ワークロード ネットワーク設定を編集します。
 - a ワークロード ネットワークを選択し、[編集] をクリックします。
 - b [IP アドレス範囲] の横にある [追加] をクリックし、そのネットワーク上のワークロードに使用する新しい IP アドレス範囲を追加します。

この IP アドレス範囲は、サブネット マスクによって示されるサブネットに含まれている必要があります。

注： 追加する IP アドレス範囲は、ロード バランサのフロントエンド ネットワーク構成の仮想 IP アドレスと重複しないようにする必要があります。

NSX が構成されている スーパーバイザー のワークロード ネットワーク設定の変更

ネットワーク スタックとして NSX 用に構成された スーパーバイザー の DNS サーバ、名前空間ネットワーク、入力方向と出力方向のネットワーク設定を変更する方法について説明します。

前提条件

- クラスタに関するクラスタ全体の構成の変更権限があることを確認します。

手順

- 1 vSphere Client で、[ワークロード管理] に移動します。
- 2 [スーパーバイザー] で、[スーパーバイザー]、[構成] の順に選択します。

- 3 [ネットワーク] を選択し、[ワークロード ネットワーク] を展開します。

図 12-5. スーパーバイザー ワークロード ネットワークの設定の更新

The screenshot displays the vSphere Supervisor configuration interface. The left sidebar shows the navigation menu with 'Network' selected under the 'Supervisor' section. The main content area is titled 'Network' and includes a 'VIEW NETWORK TOPOLOGY' link. Below the title, it states: 'Below are the network settings for supporting namespaces on this Supervisor.' The 'Workload Network' section is expanded, showing the following settings:

Setting	Value	Action
vSphere Distributed Switch	dc-dvs	
Edge Cluster	edge-cluster-0	
DNS Server(s)	[Redacted]	EDIT
Services CIDR	[Redacted]	
Tier-0 Gateway	60970e9d-d22c-40a9-83c8-6e81efaf3eb0	
NAT Mode	Enabled	
Namespace Network	[Redacted]	EDIT
Namespace subnet prefix	/28	
Ingress	[Redacted]	EDIT
Egress	[Redacted]	EDIT

4 必要に応じてネットワーク設定を変更します。

オプション	説明
DNS サーバ	<p>vCenter Server などの vSphere 管理コンポーネントのドメイン名を解決できる DNS サーバのアドレスを入力します。</p> <p>たとえば、10.142.7.1 です。</p> <p>DNS サーバの IP アドレスを入力すると、各制御プレーン仮想マシンにスタティック ルートが追加されます。これは、DNS サーバへのトラフィックがワークロード ネットワークを通過することを意味します。</p> <p>指定した DNS サーバが管理ネットワークとワークロード ネットワークの間で共有されている場合、制御プレーン仮想マシンの DNS ルックアップは、初期セットアップ後にワークロード ネットワークを介してルーティングされます。</p>
名前空間ネットワーク	<p>スーパーバイザー の名前空間セグメントに接続された Kubernetes ワークロードの IP アドレス範囲を変更する CIDR 注釈を入力します。NAT モードが構成されていない場合、この IP アドレス CIDR 範囲は、ルーティング可能な IP アドレスでなければなりません。</p>
入力方向	<p>Kubernetes サービスの入力方向 IP アドレス範囲を変更する CIDR 注釈を入力します。この範囲は、タイプがロード バランサで入力方向のサービスに使用されます。Tanzu Kubernetes Grid クラスタの場合、ServiceType ロードバランサを介してサービスを公開すると、この IP CIDR ブロックから IP アドレスも取得されます。</p> <p>注: 入力方向とワークロードのネットワーク フィールドに CIDR を追加することのみが可能です。既存のフィールドを編集または削除することはできません。</p>
出力方向	<p>スーパーバイザー から出て外部サービスにアクセスするトラフィック用の SNAT（送信元ネットワーク アドレス変換）の IP アドレスを割り当てるための CIDR 注釈を入力します。スーパーバイザー 内の名前空間ごとに 1 つの出力方向 IP アドレスのみが割り当てられます。出力方向 IP アドレスは、特定の名前空間内の vSphere ポッド が NSX の外部と通信するために使用する IP アドレスです。</p>

vSphere IaaS control plane での HTTP プロキシ設定の構成

スーパーバイザー および TKG クラスタに HTTP プロキシ設定を構成する方法と、スーパーバイザー および TKG クラスタを Tanzu Mission Control に登録するときにプロキシを構成するためのワークフローを確認します。

スーパーバイザー に対するプロキシの構成には、vSphere Client、クラスタ管理 API、または DCLI コマンドを使用できます。コンテナ トラフィック、またはスーパーバイザー の外部のネットワークからのイメージ プルを処理する必要がある場合は、プロキシを使用します。Tanzu Mission Control で管理クラスタとして登録するオンプレミススーパーバイザー の場合は、イメージ プルとコンテナ トラフィックに HTTP プロキシを使用できます。

新規作成された vSphere 7.0 Update 3 以降のスーパーバイザー でのプロキシ設定の構成

vSphere 7.0 Update 3 以降の環境で新規作成されたスーパーバイザー の場合、HTTP プロキシ設定は vCenter Server から継承されます。vCenter Server で HTTP プロキシ設定を構成する前または後にスーパーバイザー を作成したかに関係なく、設定はクラスタによって継承されます。

vCenter Server で HTTP プロキシ設定を構成する方法については、[DNS、IP アドレス、およびプロキシの設定](#)を参照してください。

また、vSphere Client、クラスタ管理 API または DCLI を使用して、個々の スーパーバイザー で継承された HTTP プロキシの構成をオーバーライドすることもできます。

vCenter Server プロキシ設定の継承は、新しく作成された vSphere 7.0.3 スーパーバイザー のデフォルト構成であるため、スーパーバイザー がプロキシを必要とせず、vCenter Server が引き続きプロキシを必要とする場合は、クラスタ管理 API または DCLI を使用して HTTP プロキシ設定を継承しないことも可能です。

vSphere 7.0 Update 3 以降にアップグレードされた スーパーバイザー でのプロキシ設定の構成

スーパーバイザー を vSphere 7.0 Update 3 以降にアップグレードした場合、vCenter Server の HTTP プロキシ設定は自動的に継承されません。この場合は、vSphere Client、`vcenter/namespaces-management/clusters` API、または DCLI コマンド ラインを使用して スーパーバイザー のプロキシ設定を構成します。

vSphere IaaS control plane での TKG クラスタへの HTTP プロキシの構成

次のいずれかの方法を使用して、vSphere IaaS control plane で Tanzu Kubernetes クラスタにプロキシを構成します。

- 個々の TKG クラスタにプロキシ設定を構成します。Tanzu Kubernetes Grid サービス v1alpha2 API を使用して Tanzu Kubernetes クラスタをプロビジョニングするための構成パラメータを参照してください。構成 YAML の例については、Tanzu Kubernetes Grid サービス v1alpha2 API を使用してカスタム Tanzu Kubernetes クラスタをプロビジョニングするためのサンプル YAML を参照してください。
- すべての TKG クラスタに適用されるグローバル プロキシ構成を作成します。Tanzu Kubernetes Grid サービス v1alpha2 API の構成パラメータを参照してください。

注： Tanzu Mission Control を使用して TKG クラスタを管理する場合は、vSphere IaaS control plane のクラスタ YAML ファイルを使用してプロキシ設定を構成する必要はありません。TKG クラスタをワークロード クラスタとして Tanzu Mission Control に追加するときにプロキシ設定を構成できます。

vSphere Client を使用した スーパーバイザー での HTTP プロキシ設定の構成

vSphere Client を使用して スーパーバイザー に HTTP プロキシ設定を構成する方法について確認します。個々の スーパーバイザー で vCenter Server から継承されたプロキシ設定をオーバーライドすることも、プロキシ設定をまったく使用しないようにすることもできます。

前提条件

- クラスタに関するクラスタ全体の構成の変更権限があることを確認します。

手順

- 1 vSphere Client で、[ワークロード管理] に移動します。
- 2 [スーパーバイザー] で、[スーパーバイザー]、[構成] の順に選択します。
- 3 [ネットワーク] を選択し、[プロキシ構成] を展開して、[編集] をクリックします。

4 スーパーバイザーで [プロキシ設定の構成] を選択し、プロキシ設定を入力します。

オプション	説明
TLS 証明書	プロキシの証明書を検証するために使用されるプロキシ TLS ルート CA バンドル。バンドルをプレーン テキストで入力します。
ホストと IP アドレスがプロキシから除外されました	プロキシ サーバを必要とせず、直接アクセスできる IPv4 アドレス、FQDN、またはドメイン名のカンマ区切りリスト。
HTTPS 構成	URL、ポート、ユーザー名、パスワードなどの HTTPS 設定。
HTTP 構成	URL、ポート、ユーザー名、パスワードなどの HTTP 設定。

5 [OK] をクリックします。

結果

このスーパーバイザーで構成したプロキシ設定により、vCenter Server から継承された設定がオーバーライドされます。

クラスタ管理 API と DCLI を使用したスーパーバイザーへの HTTP プロキシの構成

vcenter/namespace-management/clusters API または DCLI を使用してスーパーバイザー プロキシ設定を構成できます。

この API には、スーパーバイザーでプロキシを構成するオプションが 3 つあります。

API 設定	新しく作成された vSphere 7.0.3 以降のスーパーバイザー	vSphere 7.0.3 以降にアップグレードされたスーパーバイザー
VC_INHERITED	これは新しいスーパーバイザーのデフォルト設定です。API を使用してスーパーバイザーのプロキシ設定を構成する必要はありません。vCenter Server の管理インターフェイスを使用してプロキシ設定を構成するだけで済みます。	この設定を使用して、HTTP プロキシの構成を vSphere 7.0.3 以降にアップグレードされたスーパーバイザーにプッシュします。
CLUSTER_CONFIGURED	この設定を使用して、次のいずれかの場合に、vCenter Server から継承された HTTP プロキシ構成をオーバーライドします。 <ul style="list-style-type: none"> ■ スーパーバイザーは vCenter Server と異なるサブネット上にあり、別のプロキシサーバが必要になる。 ■ プロキシサーバはカスタム CA バンドルを使用している。 	次のいずれかの場合、この設定を使用して、vSphere 7.0.3 以降にアップグレードされた個々のスーパーバイザーに HTTP プロキシを構成します。 <ul style="list-style-type: none"> ■ スーパーバイザーは vCenter Server と異なるサブネット上にあり、別のプロキシサーバが必要になるため、vCenter Server プロキシは使用できない。 ■ プロキシサーバはカスタム CA バンドルを使用している。
NONE	スーパーバイザーがインターネットに直接接続されている一方で、vCenter Server がプロキシを必要としている場合は、この設定を使用します。NONE の設定を使用すると、vCenter Server のプロキシ設定がスーパーバイザーによって継承されなくなります。	

HTTP プロキシを スーパーバイザー に設定するか、既存の設定を変更するには、vCenter Server との SSH セッションで次のコマンドを使用します。

```
vc_address=<IP address>
cluster_id=domain-c<number>
session_id=$(curl -ksX POST --user '<SSO user name>:<password>' https://$vc_address/api/session | xargs -t)
curl -k -X PATCH -H "vmware-api-session-id: $session_id" -H "Content-Type: application/json" -d '{ "cluster_proxy_config": { "proxy_settings_source": "CLUSTER_CONFIGURED", "http_proxy_config": "<proxy_url>" } }' https://$vc_address/api/vcenter/namespace-management/clusters/$cluster_id
```

クラスタ ID 全体の中で渡す必要があるのは domain_c<number> だけです。たとえば、クラスタ ID が ClusterComputeResource:domain-c50:5bbb510f-759f-4e43-96bd-97fd703b4edb の場合は、そこから domain-c50 を取得します。

VC_INHERITED または NONE の設定を使用する場合は、コマンド内で "http_proxy_config:<proxy_url>" を省略します。

カスタム CA バンドルを使用するには、TSL CA 証明書をプレーン テキストで指定して、コマンドに "tlsRootCaBundle": "<TLS_certificate>" を追加します。

HTTPS プロキシ設定には、次のコマンドを使用します。

```
curl -k -X PATCH -H "vmware-api-session-id: $session_id" -H "Content-Type: application/json" -d '{ "cluster_proxy_config": { "proxy_settings_source": "CLUSTER_CONFIGURED", "https_proxy_config": "<proxy_url>" } }' https://$vc_address/api/vcenter/namespace-management/clusters/$cluster_id
```

DCLI を使用した スーパーバイザー での HTTP プロキシ設定の構成

次の DCLI コマンドを使用すると、CLUSTER_CONFIGURED 設定を使用して スーパーバイザー に HTTP プロキシ設定を構成することができます。

```
<dcli> namespacemanagement clusters update --cluster domain-c57 --cluster-proxy-config-http-proxy-config <proxy URL> --cluster-proxy-config-https-proxy-config <proxy URL> --cluster-proxy-config-proxy-settings-source CLUSTER_CONFIGURED
```

Tanzu Mission Control 向けの スーパーバイザー および TKG クラスタでの HTTP プロキシ設定の構成

Tanzu Mission Control に管理クラスタとして登録する スーパーバイザー で HTTP プロキシを構成するには、次の手順を実行します。

- 1 vSphere で、vCenter Server から HTTP プロキシ設定を継承するか、vSphere Client、[名前空間管理クラスタの API](#)、または DCLI コマンド ラインを使用して個々の スーパーバイザー のプロキシ設定を構成して、スーパーバイザー で HTTP プロキシを構成します。

- 2 Tanzu Mission Control では、vSphere IaaS control plane でスーパーバイザーに構成したプロキシ設定を使用して、プロキシ構成オブジェクトを作成します。「[Create a Proxy Configuration Object for a Tanzu Kubernetes Grid Service Cluster](#)」を参照してください。
- 3 Tanzu Mission Control で、スーパーバイザーを管理クラスタとして登録する場合は、このプロキシ構成オブジェクトを使用します。「[Register a Management Cluster with Tanzu Mission Control](#)」および「[Complete the Registration of a Supervisor Cluster](#)」を参照してください。

Tanzu Mission Control でワークロード クラスタとしてプロビジョニングまたは追加する TKG クラスタに HTTP プロキシを構成するには、次の手順を実行します。

- 1 Tanzu Kubernetes クラスタで使用するプロキシ設定を使用して、プロキシ構成オブジェクトを作成します。「[Create a Proxy Configuration Object for a Tanzu Kubernetes Grid Service Cluster](#)」を参照してください。
- 2 Tanzu Kubernetes クラスタをワークロード クラスタとしてプロビジョニングまたは追加する場合は、このプロキシ構成オブジェクトを使用します。「[Provision a Cluster](#)」および「[Add a Workload Cluster into Tanzu Mission Control Management](#)」を参照してください。

TKG サービス クラスタで使用する外部 ID プロバイダの構成

Okta など、任意の OIDC 準拠 ID プロバイダ (IDP) を使用してスーパーバイザーを構成できます。統合を完了するには、IDP にスーパーバイザーのコールバック URL を構成します。

サポートされている外部 OIDC プロバイダ

任意の [OIDC 準拠 ID プロバイダ](#) を使用してスーパーバイザーを構成できます。次の表に、一般的なものと、構成手順へのリンクを示します。

外部 ID プロバイダ	構成
Okta	Okta を使用した OIDC 構成の例 Configure Okta as an OIDC provider for Pinniped も参照してください。
Workspace ONE	Configure Workspace ONE Access as an OIDC provider for Pinniped
Dex	Configure Dex as an OIDC provider for Pinniped
GitLab	Configure GitLab as an OIDC provider for Pinniped
Google OAuth	Using Google OAuth 2

スーパーバイザーのコールバック URL を使用した ID プロバイダの構成

スーパーバイザーは、外部 ID プロバイダに対する OAuth 2.0 クライアントとして機能します。スーパーバイザーコールバック URL は、外部 ID プロバイダの構成に使用されるリダイレクト URL です。コールバック URL は、<https://SUPERVISOR-VIP/wcp/pinniped/callback> という形式になります。

注： ID プロバイダの登録を実行する際、コールバック URL が構成中の OIDC プロバイダで「リダイレクト URL」と呼ばれることがあります。

スーパーバイザーの TKG で使用する外部 ID プロバイダを構成する場合、外部プロバイダに、vCenter Server で利用可能な [コールバック URL] を [ワークロード管理] - [スーパーバイザー] - [構成] - [ID プロバイダ] 画面で入力します。

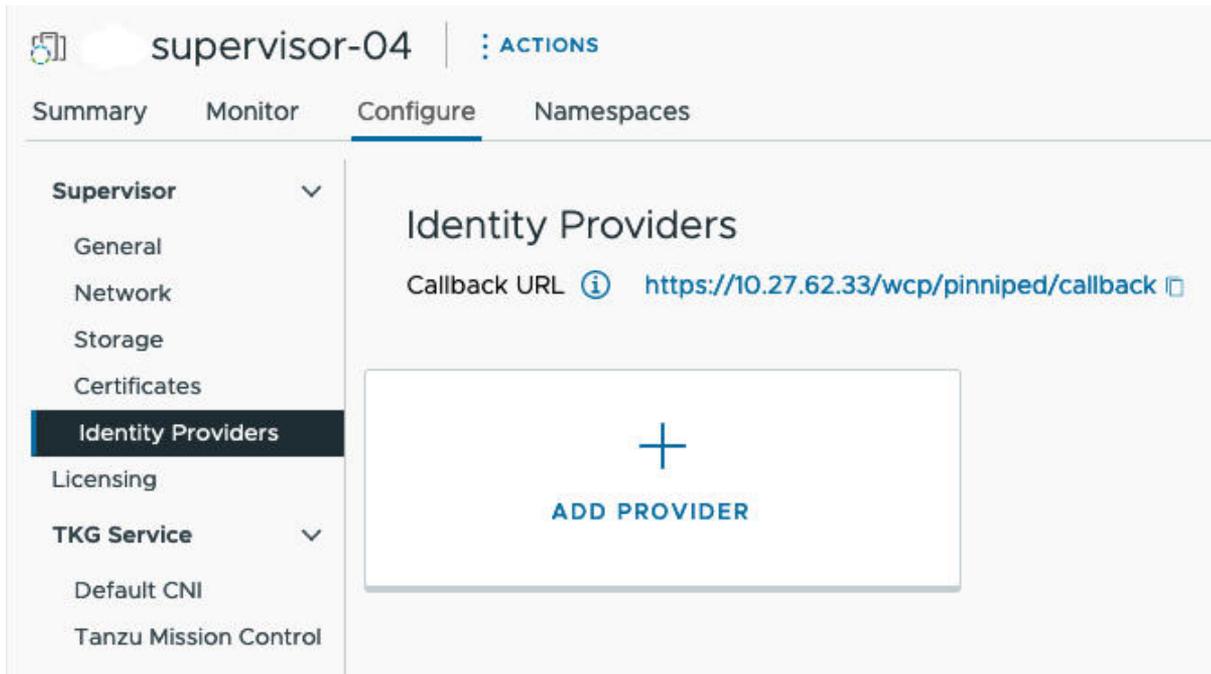
Okta を使用した OIDC 構成の例

Okta では、ユーザーは OpenID Connect プロトコルを使用してアプリケーションにログインできます。スーパーバイザーで Tanzu Kubernetes Grid の外部 ID プロバイダとして Okta を構成する場合、スーパーバイザーと Tanzu Kubernetes Grid クラスタの Pinniped ポッドが vSphere 名前空間 およびワークロード クラスタの両方へのユーザー アクセスを制御します。

- 1 Okta と vCenter Server 間の OIDC 接続を作成する必要がある ID プロバイダのコールバック URL をコピーします。

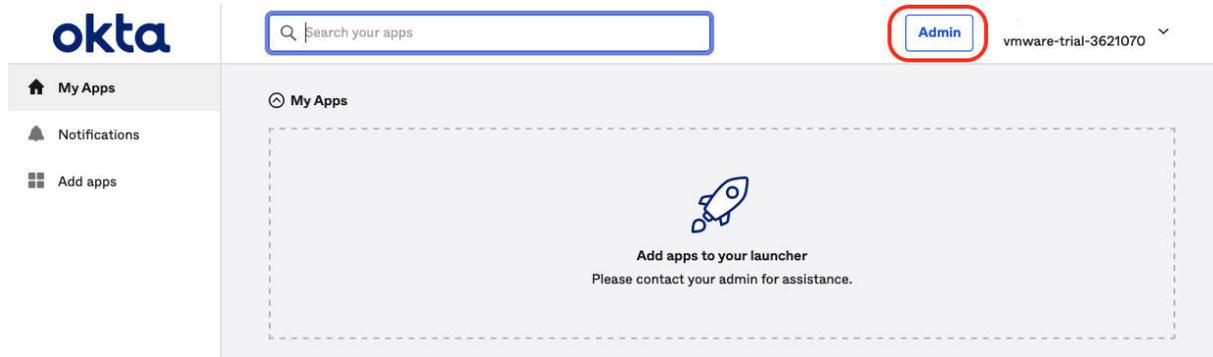
vSphere Client を使用して、ID プロバイダ コールバック URL を [ワークロード管理] - [スーパーバイザー] - [構成] - [ID プロバイダ] で取得します。この URL を一時的な場所にコピーします。

図 12-6. ID プロバイダ コールバック URL



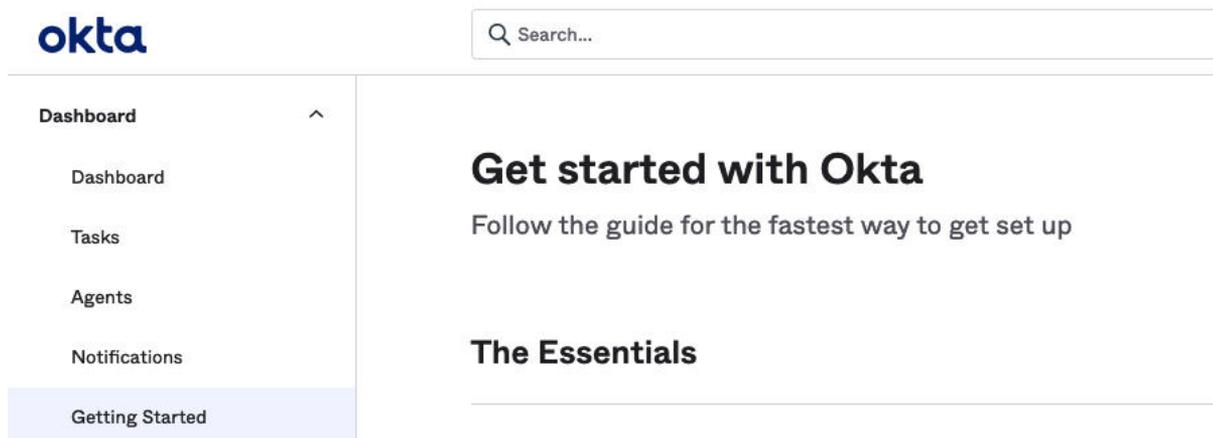
- 2 組織の Okta アカウントにログインするか、<https://www.okta.com/> で評価版アカウントを作成します。[管理] ボタンをクリックして Okta 管理コンソールを開きます。

図 12-7. Okta 管理コンソール



- 3 管理コンソールの [はじめに] ページから、[アプリケーション] - [アプリケーション] に移動します。

図 12-8. Okta の開始



- 4 [アプリケーション統合の作成] オプションを選択します。

図 12-9. Okta アプリケーション統合の作成

Applications



- 5 新しいアプリケーション統合を作成します。
 - ログイン方法を [OIDC - OpenID Connect] に設定します
 - アプリケーション タイプを [Web アプリケーション] に設定します

図 12-10. Okta サインオン方法とアプリケーション タイプ

Create a new app integration X

Sign-in method

[Learn More](#)

- OIDC - OpenID Connect**
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.
- SAML 2.0**
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.
- SWA - Secure Web Authentication**
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.
- API Services**
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

Application type

What kind of application are you trying to integrate with Okta?

Specifying an application type customizes your experience and provides the best configuration, SDK, and sample recommendations.

- Web Application**
Server-side applications where authentication and tokens are handled on the server (for example, Go, Java, ASP.Net, Node.js, PHP)
- Single-Page Application**
Single-page web applications that run in the browser where the client receives tokens (for example, Javascript, Angular, React, Vue)
- Native Application**
Desktop or mobile applications that run natively on a device and redirect users to a non-HTTP callback (for example, iOS, Android, React Native)

Cancel

Next

6 Okta の Web アプリケーション統合の詳細を構成します。

- ユーザー定義文字列である [アプリケーション統合名] を指定します。
- [付与タイプ] を指定します：[認可コード] を選択し、[リフレッシュ トークン] も選択します。
- リダイレクト URI にログインします：スーパーバイザー からコピーした (手順 1 を参照) ID プロバイダ コールバック URL (<https://10.27.62.33/wcp/pinnipend/callback> など) を入力します。
- リダイレクト URI からログアウトします：スーパーバイザー からコピーした (手順 1 を参照) ID プロバイダ コールバック URL (<https://10.27.62.33/wcp/pinnipend/callback> など) を入力します。

図 12-11. Okta Web アプリケーション統合の詳細

☰+ New Web App Integration

General Settings

App integration name

Logo (Optional)

Grant type [Learn More](#)

Client acting on behalf of itself

Client Credentials

Client acting on behalf of a user

Authorization Code

Interaction Code

Refresh Token

Implicit (hybrid)

Sign-in redirect URIs Allow wildcard * in sign-in URI redirect.

Okta sends the authentication response and ID token for the user's sign-in request to these URIs

[Learn More](#)

Sign-out redirect URIs (Optional)

After your application contacts Okta to close the user session, Okta redirects the user to one of these URIs.

[Learn More](#)

7 ユーザー アクセス コントロールを構成します。

[割り当て] - [制限付きアクセス] セクションで、Tanzu Kubernetes Grid クラスタにアクセス可能な組織に存在する Okta ユーザーを任意で制御できます。例では、組織内で定義されているすべてのユーザーがアクセスできます。

図 12-12. Okta アクセス コントロール

Trusted Origins

Base URIs (Optional)

Required if you plan to self-host the Okta Sign-In Widget. With a Trusted Origin set, the Sign-In Widget can make calls to the authentication API from this domain.

[Learn More](#) 



+ Add URI

Assignments

Controlled access

Select whether to assign the app integration to everyone in your org, only selected group(s), or skip assignment until after app creation.

- Allow everyone in your organization to access
- Limit access to selected groups
- Skip group assignment for now

Enable immediate access (Recommended)

Recommended if you want to grant access to everyone without pre-assigning your app to users and use Okta only for authentication.

- Enable immediate access with **Federation Broker Mode**



To ensure optimal app performance at scale, Okta End User Dashboard and provisioning features are disabled. [Learn more about Federation Broker Mode.](#)

Save

Cancel

- 8 [保存] をクリックし、返される [クライアント ID] および [クライアント シークレット] をコピーします。

Okta 構成を保存すると、管理コンソールで [クライアント ID] と [クライアント シークレット] が提供されます。両方のデータをコピーします。これらは スーパーバイザー を外部 ID プロバイダで構成するために必要です。

図 12-13. OIDC クライアント ID およびシークレット

← Back to Applications

My Tanzu K8s Clusters

Active ▾

View Logs

General
Sign On
Assignments
Okta API Scopes

Client Credentials Edit

Client ID Ooa23oi848qxutr3V697

Public identifier for the client that is required for all OAuth flows.

Client authentication

Client secret
 Public key / Private key

CLIENT SECRETS

Generate new secret

Creation date	Secret		Status
Sep 2, 2022		Active ▾

9 OpenID Connect ID トークンを構成します。

[サインオン] タブをクリックします。[OpenID Connect ID トークン] セクションで [編集] リンクをクリックし、[グループ要求タイプ] フィルタを入力し、設定を [保存] します。

たとえば、要求名「グループ」をすべてのグループと一致させるには、[グループ] - [正規表現に一致] - [*] の順に選択します。

図 12-14. OpenID Connect ID トークン

OpenID Connect ID Token Cancel

Issuer:

Audience:

Claims: Claims for this token include all user attributes on the app profile.

Groups claim type:

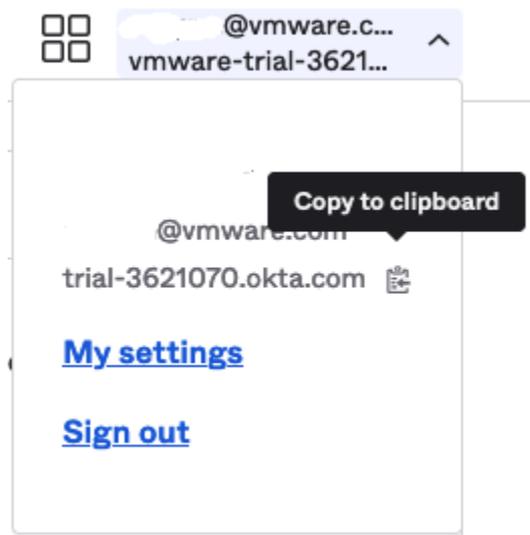
Groups claim filter ?:
[Using Groups Claim](#)

10 [発行者 URL] をコピーします。

スーパーバイザー を構成するには、[クライアント ID] および [クライアント シークレット] に加えて、[発行者 URL] が必要です。

Okta 管理コンソールから [発行者 URL] をコピーします。

図 12-15. Okta 発行者 URL



スーパーバイザー への外部 IDP の登録

Tanzu CLI を使用してスーパーバイザー 上の Tanzu Kubernetes Grid 2.0 クラスタに接続するには、OIDC プロバイダをスーパーバイザー に登録します。

前提条件

外部 OIDC プロバイダをスーパーバイザー に登録する前に、次の前提条件を満たしている必要があります。

- ワークロード管理を有効にして、スーパーバイザー インスタンスをデプロイします。「[スーパーバイザーでの TKG 2.0 クラスタの実行](#)」を参照してください。
- 外部 [OpenID Connect ID プロバイダ](#) をスーパーバイザー コールバック URL で構成します。[TKG サービス クラスタで使用する外部 ID プロバイダの構成](#)を参照してください。
- クライアント ID、クライアント シークレット、および発行者 URL を外部 IDP から取得します。[TKG サービス クラスタで使用する外部 ID プロバイダの構成](#)を参照してください。

スーパーバイザー への外部 IDP の登録

スーパーバイザー は、ポッドとして Pinniped Supervisor コンポーネントと Pinniped Concierge コンポーネントを実行します。Tanzu Kubernetes Grid クラスタは、ポッドとして Pinniped Concierge コンポーネントのみを実行します。これらのコンポーネントとその相互作用の詳細については、[Pinniped 認証サービスのドキュメント](#)を参照してください。

外部 ID プロバイダをスーパーバイザー に登録すると、スーパーバイザー 上の Pinniped Supervisor ポッドと Pinniped Concierge ポッド、Tanzu Kubernetes Grid クラスタ上の Pinniped Concierge ポッドが更新されます。その Tanzu Kubernetes Grid インスタンスで実行されているすべてのスーパーバイザー クラスタは自動的に同じ外部 ID プロバイダで構成されます。

外部 OIDC プロバイダをスーパーバイザー に登録するには、次の手順を実行します。

- 1 vSphere Client を使用して、vCenter Server にログインします。
- 2 [ワークロード管理] - [スーパーバイザー] - [構成] - [ID プロバイダ] の順に選択します。
- 3 プラス記号をクリックして登録プロセスを開始します。
- 4 プロバイダを構成します。[OIDC プロバイダの構成](#)を参照してください。

図 12-16. OIDC プロバイダの構成

Add Provider

- 1 **Provider Configuration**
- 2 OAuth 2.0 Client Details
- 3 Additional Settings
- 4 Review and Confirm

Provider Configuration

Provider Name ⓘ okta

Issuer URL ⓘ https://trial-3621070.okta.com

Username Claim (optional) ⓘ email

Groups Claim (optional) ⓘ groups

- 5 OAuth 2.0 クライアントの詳細を構成します。OAuth 2.0 クライアントの詳細を参照してください。

図 12-17. OAuth 2.0 クライアントの詳細

Add Provider

- 1 Provider Configuration
- 2 **OAuth 2.0 Client Details**
- 3 Additional Settings
- 4 Review and Confirm

OAuth 2.0 Client Details

Client ID ⓘ Ooa23o0aei0TXYuG3697

Client Secret ⓘ ⓘ

- 6 追加の設定を構成します。その他の設定を参照してください。
- 7 プロバイダ設定を確認します。

図 12-18. プロバイダ設定の確認

Add Provider

- 1 Provider Configuration
- 2 OAuth 2.0 Client Details
- 3 Additional Settings
- 4 Review and Confirm

Review and Confirm ×

Provider Configuration

Provider Name ⓘ okta

Issuer URL ⓘ https://trial-3621070.okta.com

Username Claim ⓘ email

Groups Claim ⓘ groups

OAuth 2.0 Client Details

Client ID ⓘ Ooa23oOaelOTXYuG3697

Client Secret ⓘ

Additional Settings

Additional Scopes ⓘ --

Certificate Authority Data ⓘ --

Additional Authorize Parameters ⓘ --

CANCEL
BACK
FINISH

8 [終了] をクリックして、OIDC プロバイダの登録を完了します。

OIDC プロバイダの構成

外部 OIDC プロバイダをスーパーバイザーに登録する場合は、次のプロバイダ構成の詳細を参照してください。

表 12-1. OIDC プロバイダの構成

フィールド	重要度	説明
プロバイダ名	必須	外部 ID プロバイダのユーザー定義名。
発行者 URL	必須	<p>トークンを発行する ID プロバイダの URL。OIDC 検出 URL は、発行者 URL から取得されます。</p> <p>たとえば、Okta の発行者 URL は https://trial-4359939-admin.okta.com のように表示され、管理コンソールから取得できます。</p>

表 12-1. OIDC プロバイダの構成 (続き)

フィールド	重要度	説明
ユーザー名の要求	オプション	<p>指定されたユーザーのユーザー名を取得する際に検査を行う、アップストリーム ID プロバイダの ID トークンまたはユーザー情報エンドポイントからの要求。このフィールドを空のままにすると、アップストリーム発行者の URL が「サブ」要求と連結され、Kubernetes で使用されるユーザー名が生成されます。</p> <p>このフィールドは、認証の判断を行うために、Pinniped がアップストリーム ID トークンの何を認認する必要があるかを指定します。指定しない場合、ユーザー ID は <code>https://IDP-ISSUER?sub=UUID</code> の形式になります。</p>
グループの要求	オプション	<p>指定されたユーザーのグループを取得する際に検査を行う、アップストリーム ID プロバイダの ID トークンまたはユーザー情報エンドポイントからの要求。このフィールドを空のままにすると、アップストリーム ID プロバイダのグループは使用されません。</p> <p>[グループの要求] フィールドでは、ユーザー ID を認認するためにアップストリーム ID トークンから確認する内容が Pinniped に指示されます。</p>

OAuth 2.0 クライアントの詳細

外部 OIDC プロバイダをスーパーバイザーに登録する場合は、次のプロバイダ OAuth 2.0 クライアントの詳細を参照してください。

表 12-2. OAuth 2.0 クライアントの詳細

OAuth 2.0 クライアントの詳細	重要度	説明
クライアント ID	必須	外部 IDP のクライアント ID
クライアント シークレット	必須	外部 IDP のクライアント シークレット

その他の設定

外部 OIDC プロバイダをスーパーバイザーに登録する場合は、次の追加設定を参照してください。

表 12-3. その他の設定

設定	重要度	説明
追加の範囲	オプション	トークンで要求される追加の範囲
認証局データ	オプション	セキュアな外部 IDP 接続のための TLS 証明 局データ
追加の認証パラメータ	オプション	OAuth2 認証要求中の追加パラメータ

スーパーバイザー のストレージ設定の変更

スーパーバイザー に割り当てられたストレージ ポリシーに基づいて、制御プレーンの仮想マシン、vSphere ポッドの短期ディスク、コンテナ イメージ キャッシュなどのオブジェクトが vSphere ストレージ環境のデータストア内に配置されます。vSphere 管理者は、通常、スーパーバイザー を有効にするときにストレージ ポリシーを設定します。最初のスーパーバイザー の設定後にストレージ ポリシーの割り当てを変更する必要がある場合は、このタスクを実行します。このタスクを使用して、TKG クラスタの ReadWriteMany パーシステント ポリリュームのファイル ポリリューム サポートを有効または無効にすることもできます。

一般的に、ストレージ設定に加えた変更は、スーパーバイザー 内の新しいオブジェクトにのみ適用されます。この手順を使用して TKG クラスタでファイル ポリリュームのサポートを有効にする場合は、既存のクラスタに対して実行できます。

前提条件

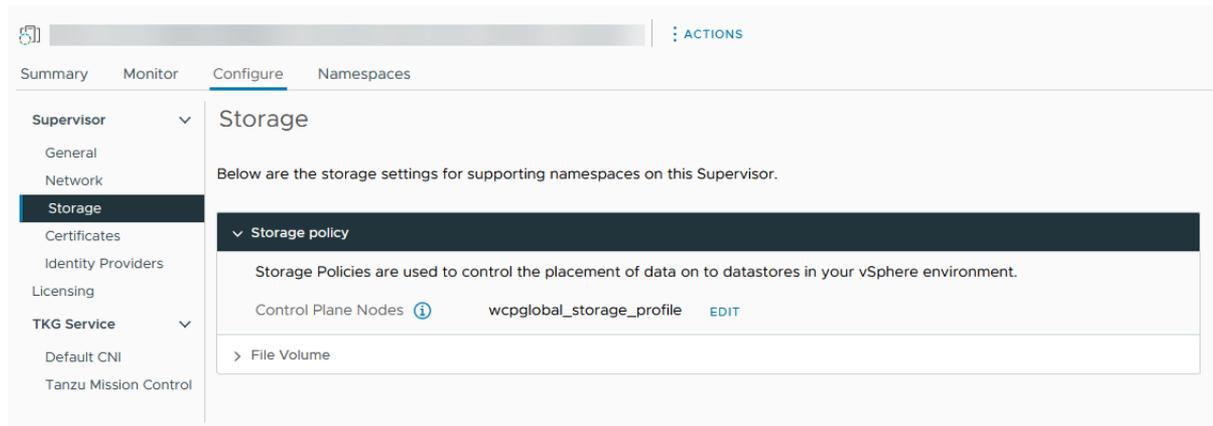
ReadWriteMany モードのパーシステント ポリリュームで TKG クラスタに対するファイル ポリリューム サポートを有効にする場合は、『vSphere IaaS 制御プレーンのサービスとワークロード』ドキュメントの「[vSphere IaaS control plane での ReadWriteMany パーシステント ポリリュームの作成](#)」に記載されている前提条件に従ってください。

手順

- 1 vSphere Client で、[ワークロード管理] に移動します。
- 2 [スーパーバイザー] タブをクリックし、編集する スーパーバイザー をリストから選択します。

- 3 [構成] タブをクリックし、[ストレージ] をクリックします。

図 12-19. スーパーバイザー ストレージ設定の更新



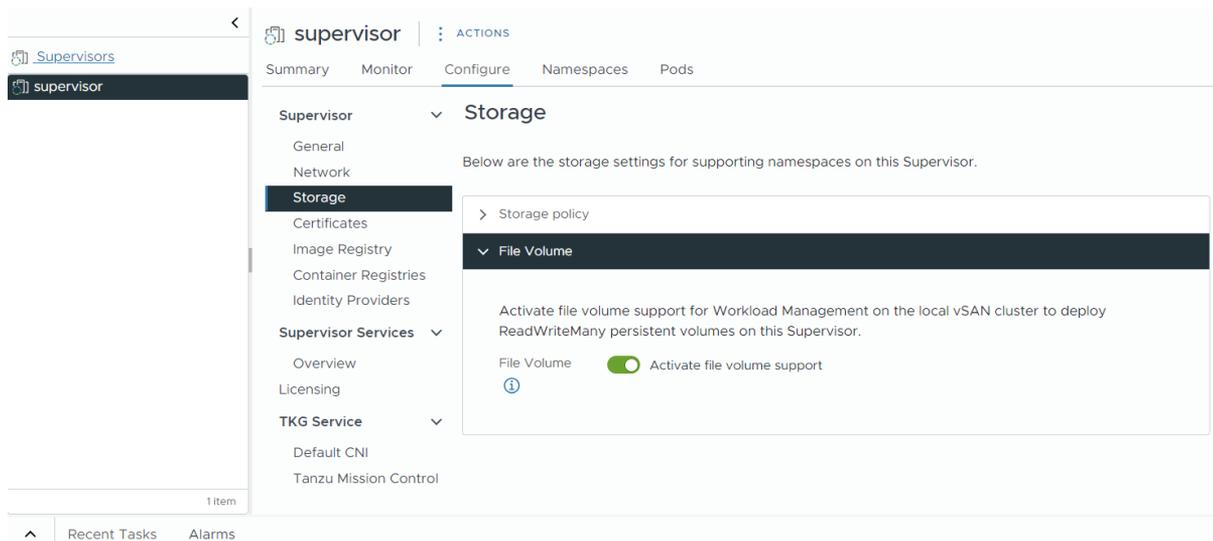
- 4 制御プレーン仮想マシンに対するストレージ ポリシーの割り当てを変更します。

vSphere ポッド がサポートされている環境では、短期仮想ディスクおよびコンテナ イメージ キャッシュのストレージ ポリシーを変更することもできます。

オプション	説明
制御プレーン ノード	制御プレーン仮想マシンを配置するためのストレージ ポリシーを選択します。
ポッドの短期ディスク	vSphere ポッド を配置するためのストレージ ポリシーを選択します。
コンテナ イメージ キャッシュ	コンテナ イメージのキャッシュを配置するためのストレージ ポリシーを選択します。

- 5 ReadWriteMany パーシステント ボリュームをデプロイするために、ファイル ボリューム サポートを有効にします。

このオプションは、環境が vSAN ファイル サービスで構成されている場合にのみ使用できます。「vSAN ファイル サービスの有効化」を参照してください。



カスタム可観測プラットフォームへの スーパーバイザー メトリックのストリーミング

Telegraf によって収集された スーパーバイザー メトリックをカスタム可観測プラットフォームにストリーミングする方法について説明します。スーパーバイザー では Telegraf がデフォルトで有効になっており、Kubernetes API サーバ、仮想マシン サービス、Tanzu Kubernetes Grid などの スーパーバイザー コンポーネントから Prometheus 形式でメトリックが収集されます。vSphere 管理者は、VMware Aria Operations for Applications や Grafana などの可観測プラットフォームを構成して、収集された スーパーバイザー メトリックを表示したり分析したりすることができます。

Telegraf は、さまざまなシステム、データ ベース、IoT からメトリックを収集して送信することを目的としたサーバベースのエージェントです。Telegraf の接続先となるエンドポイントは、各 スーパーバイザー コンポーネントで公開されます。次に、Telegraf は収集されたメトリックを任意の可観測プラットフォームに送信します。スーパーバイザー メトリックは、可観測プラットフォームとして Telegraf がサポートする出力プラグインを構成することで集計、分析できます。サポートされている出力プラグインについては、[Telegraf のドキュメント](#)を参照してください。

Telegraf が接続してメトリックを収集するエンドポイントは、各種のコンポーネント、たとえば、Kubernetes API サーバ、etcd、kubelet、Kubernetes コントローラ マネージャ、Kubernetes スケジューラ、Tanzu Kubernetes Grid、仮想マシン サービス、仮想マシン イメージ サービス、NSX Container Plug-in (NCP)、コンテナ ストレージ インターフェイス (CSI)、証明書マネージャ、NSX、各種ホスト メトリック (CPU、メモリ、ストレージなど) によって公開されます。

Telegraf ポッドと構成の表示

Telegraf は、スーパーバイザー の `vmware-system-monitoring` システム名前空間で実行されます。Telegraf ポッドと ConfigMap を表示するには、次の手順を実行します。

- 1 vCenter Single Sign-On 管理者アカウントで スーパーバイザー 制御プレーンにログインします。

```
kubectl vsphere login --server <control plane IP> --vsphere-username
administrator@vsphere.local
```

- 2 次のコマンドを使用して、Telegraf ポッドを表示します。

```
kubectl -n vmware-system-monitoring get pods
```

結果のポッドは次のとおりです。

```
telegraf-csqs1
telegraf-dkwtk
telegraf-l4nxk
```

- 3 次のコマンドを使用して、Telegraf ConfigMaps を表示します。

```
kubectl -n vmware-system-monitoring get cm
```

結果の ConfigMap は次のとおりです。

```
default-telegraf-config
kube-rbac-proxy-config
kube-root-ca.crt
telegraf-config
```

default-telegraf-config ConfigMap はデフォルトの Telegraf 構成を保持しており、読み取り専用です。ファイルが破損した場合、またはデフォルトにリストアする場合に備えて、telegraf-config で構成をリストアするためのフォールバック オプションとして使用できます。編集できる ConfigMap は telegraf-config のみで、Telegraf エージェントに対して、どのコンポーネントから、どのプラットフォームにメトリックを送信するかを定義します。

4 telegraf-config ConfigMap を表示します。

```
kubectl -n vmware-system-monitoring get cm telegraf-config -o yaml
```

Telegraf がメトリックを収集する スーパーバイザー コンポーネントのすべてのエンドポイントと、メトリック自体のタイプは、telegraf-config ConfigMap の inputs セクションで定義します。たとえば、次の入力では、Kubernetes API サーバをエンドポイントとして定義します。

```
[[inputs.prometheus]]
  # APIServer
  ## An array of urls to scrape metrics from.
  alias = "kube_apiserver_metrics"
  urls = ["https://127.0.0.1:6443/metrics"]
  bearer_token = "/run/secrets/kubernetes.io/serviceaccount/token"
  # Dropping metrics as a part of short term solution to vStats integration 1MB metrics
  payload_limit
  # Dropped Metrics:
  # apiserver_request_duration_seconds
  namepass = ["apiserver_request_total", "apiserver_current_inflight_requests",
"apiserver_current_inqueue_requests", "etcd_object_counts",
"apiserver_admission_webhook_admission_duration_seconds", "etcd_request_duration_seconds"]
  # "apiserver_request_duration_seconds" has _massive_ cardinality, temporarily turned
off. If histogram, maybe filter the highest ones?
  # Similarly, maybe filters to _only_ allow error code related metrics through?
  ## Optional TLS Config
  tls_ca = "/run/secrets/kubernetes.io/serviceaccount/ca.crt"
```

alias プロパティは、収集されるメトリックの送信元コンポーネントを示します。namepass プロパティは、どのコンポーネント メトリックが公開され、それぞれ Telegraf エージェントによって収集されるかを指定します。

telegraf-config ConfigMap にはさまざまなメトリックが最初から含まれていますが、別途メトリックを定義することもできます。[「Metrics For Kubernetes System Components」](#) および [「Kubernetes Metrics Reference」](#) を参照してください。

Telegraf への Observability プラットフォームの構成

telegraf-config の outputs セクションで、Telegraf が収集したメトリックをストリーミングする場所を構成します。outputs.file、outputs.wavefront、outputs.prometheus_client、outputs-https など、いくつかのオプションがあります。outputs-https セクションでは、スーパーバイザー メトリックの集約と監視に使用可能な可観測プラットフォームを構成できます。メトリックを複数のプラットフォームに送信するように Telegraf を構成できます。telegraf-config ConfigMap を編集し、スーパーバイザー メトリックを表示するための可観測プラットフォームを構成するには、次の手順を実行します。

- 1 vCenter Single Sign-On 管理者アカウントでスーパーバイザー 制御プレーンにログインします。

```
kubectl vsphere login --server <control plane IP> --vsphere-username
administrator@vsphere.local
```

- 2 telegraf-config ConfigMap をローカル kubectl フォルダに保存します。

```
kubectl get cm telegraf-config -n vmware-system-monitoring -o
jsonpath="{.data['telegraf\.conf']}">telegraf.conf
```

以前のバージョンのファイルにリストアできるように、telegraf-config ConfigMap は変更前にバージョン管理システムに保存しておいてください。デフォルトの構成にリストアする場合は、default-telegraf-config ConfigMap の値を使用できます。

- 3 VIM などのテキスト エディタを使用して、選択した可観測プラットフォームの接続設定を含む outputs.http セクションを追加します。

```
vim telegraf.conf
```

次のセクションのコメントを直接解除して適宜、値を編集するか、または必要に応じて新しい outputs.http セクションを追加できます。

```
#[[outputs.http]]
# alias = "prometheus_http_output"
# url = "<PROMETHEUS_ENDPOINT>"
# insecure_skip_verify = <PROMETHEUS_SKIP_INSECURE_VERIFY>
# data_format = "prometheusremotewrite"
# username = "<PROMETHEUS_USERNAME>"
# password = "<PROMETHEUS_PASSWORD>"
# <DEFAULT_HEADERS>
```

たとえば、Grafana の outputs.http 構成は次のようになります。

```
[[outputs.http]]
url = "http://<grafana-host>:<grafana-metrics-port>/<prom-metrics-push-path>"
data_format = "influx"
[outputs.http.headers]
Authorization = "Bearer <grafana-bearer-token>"
```

ダッシュボードの構成と Telegraf からのメトリックの取り込みについて詳しくは、「[Stream metrics from Telegraf to Grafana](#)」を参照してください。

次に、VMware Aria Operations for Applications(旧 Wavefront)の例を示します。

```
[[outputs.wavefront]]
  url = "http://<wavefront-proxy-host>:<wavefront-proxy-port>"
```

Aria Operations for Applications にメトリックを取り込む方法として推奨される方法は、プロキシを介して行う方法です。詳細については、「[Wavefront Proxies](#)」を参照してください。

- 4 スーパーバイザー 上の既存の telegraf-config ファイルを、ローカル フォルダで編集したファイルに置き換えます。

```
kubectl create cm --from-file telegraf.conf -n vmware-system-monitoring telegraf-config --dry-run=client -o yaml | kubectl replace -f -
```

- 5 新しい構成が正常に保存されているかどうかを確認します。

- 新しい telegraf-config ConfigMap を表示します。

```
kubectl -n vmware-system-monitoring get cm telegraf-config -o yaml
```

- すべての Telegraf ポッドが実行中であるかどうかを確認します。

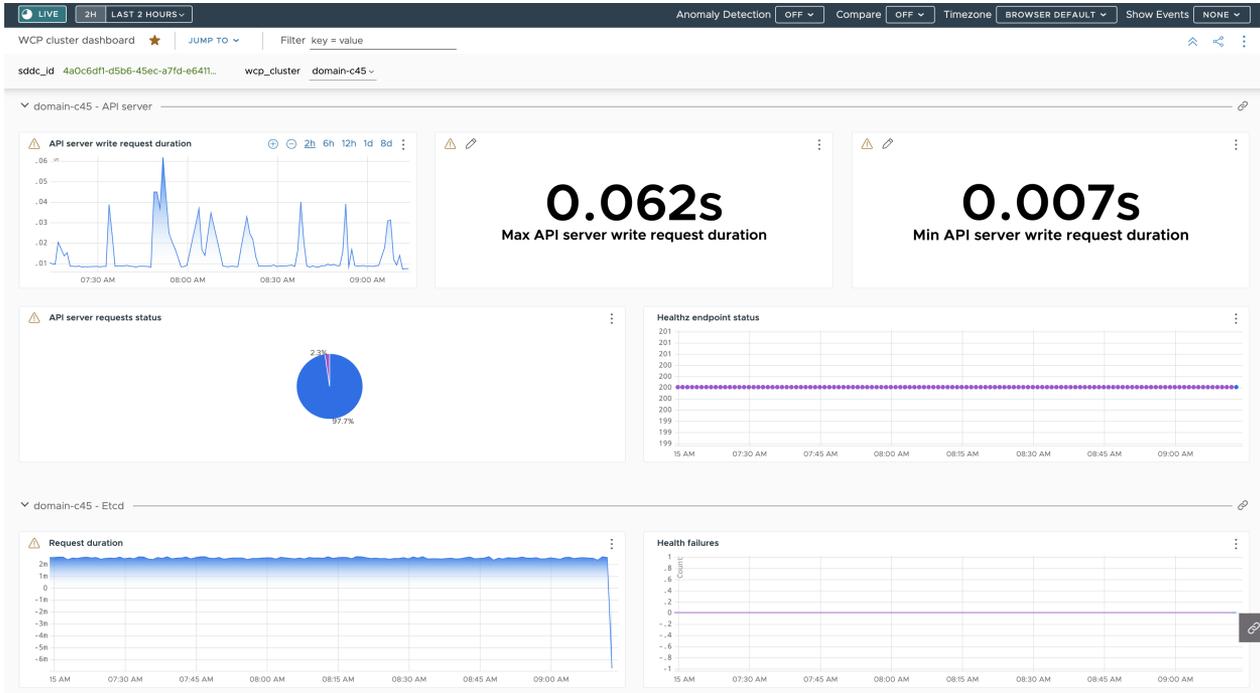
```
kubectl -n vmware-system-monitoring get pods
```

- 実行されていない Telegraf ポッドがある場合は、そのポッドの Telegraf ログを確認してトラブルシューティングを行います。

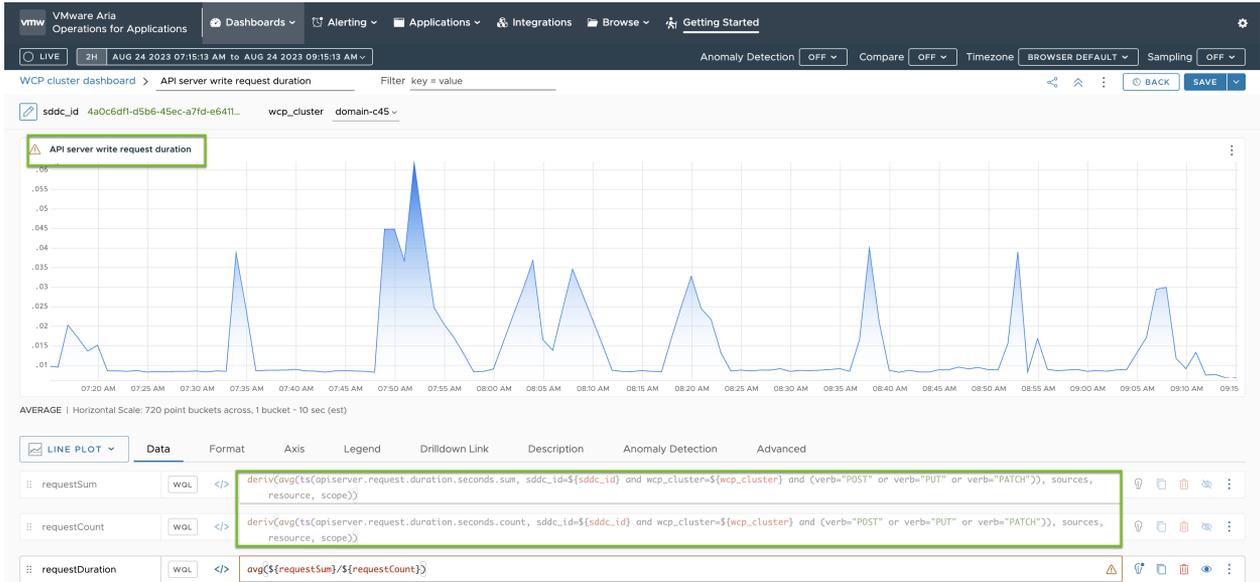
```
kubectl -n vmware-system-monitoring logs <telegraf-pod>
```

Operations for Applications ダッシュボードの例

以下のダッシュボードには、Telegraf を介して API サーバおよび etcd から受信した スーパーバイザー メトリックのサマリが表示されています。



緑色で示されているように、API サーバ書き込み要求時間のメトリックは、telegraf-config ConfigMap に指定されたメトリックに基づきます。



スーパーバイザー 制御プレーンの DNS 名のリストの変更

スーパーバイザー 制御プレーンにアクセスするための FQDN のリストを変更する方法について確認します。スーパーバイザー を有効にするときにスーパーバイザー FQDN のリストを指定して、そのリストを後で更新できます。スーパーバイザー を有効にするときにスーパーバイザー FQDN のリストを指定しなかった場合は、そのリストを設定することもできます。

手順

- ◆ 次の DCLI コマンドを使用して、スーパーバイザー 制御プレーンの FQDN のリストを更新します。

```
dcli com vmware vcenter namespacemanagement clusters update --cluster <cluster_ID> --
master-dns-name <FQDN_1> --master-dns-name <FQDN_2>
```

- 新しい FQDN をリストに追加するには、既存の名前を引数として渡し、新しい FQDN も追加します。
- リストから FQDN を削除するには、削除する FQDN を省略し、保持する残りの FQDN を渡して update コマンドを呼び出します。

3 ゾーンのスーパーバイザー の場合は、スーパーバイザー の一部であるクラスタの ID を渡すことができます。次の例では、クラスタ domain-c50 で実行されているスーパーバイザー はすでに FQDN supervisor.acme.com で構成されています。スーパーバイザー の DNS 名のリストに新しい supervisor.vmware.com FQDN を追加しています。

```
dcli com vmware vcenter namespacemanagement clusters update --cluster domain-c50 --master-
dns-name supervisor.acme.com --master-dns-name supervisor.vmware.com
```

次のステップ

- スーパーバイザー に安全に接続するための仮想 IP アドレス証明書は、自動的に新しい FQDN には更新されません。そのため、手動で更新する必要があります。「[スーパーバイザー API エンドポイントに安全に接続するための VIP 証明書の置き換え](#)」を参照してください。
- 仮想 IP アドレス証明書を更新してスーパーバイザー に接続したら、新しく追加した FQDN を使用してスーパーバイザー 制御プレーンにログインします。『[vCenter Single Sign-On ユーザーとしてスーパーバイザーに接続する](#)』を参照してください

外部監視システムへの スーパーバイザー ログの転送

Fluent Bit を使用して、スーパーバイザー 制御プレーン ログを Grafana Loki や Elastic Search などの外部監視システムに転送するように構成する方法を確認します。

スーパーバイザー 制御プレーン ログは、[Fluent Bit](#) を使用して、vCenter Server アプライアンスに構成された Syslog サーバに自動的に転送されます。Fluent Bit は、オープンソースで軽量のログおよびメトリック プロセッサかつフォワーダであり、さまざまなログ データ タイプ、フィルタリング、およびログ タグの機能強化をサポートする構成を提供します。

スーパーバイザー のアクティベーションまたはアップグレード中も、ブートストラップ ログは rsyslog によって、vCenter Server アプライアンスに構成されている Syslog サーバに転送されます。スーパーバイザー 制御プレーン仮想マシンが実行中になると、[Fluent Bit](#) がスーパーバイザー 制御プレーン ログのデフォルトのログ フォワーダになります。

vSphere 管理者は、Fluent Bit を使用して以下のことができます。

- スーパーバイザー 制御プレーン ログとシステム ジャーナル ログを、Loki、Elastic Search、Grafana などの主要な外部ログ監視プラットフォームや、Fluent Bit でサポートされているその他のプラットフォームに転送します。

- k8s API を使用して、スーパーバイザー 制御プレーンのログ転送構成を更新またはリセットします。

Fluent Bit は、スーパーバイザー 制御プレーン ノードで DaemonSet として実行されます。vmware-system-logging 名前空間で fluentbit-config-custom ConfigMap が公開されます。vSphere 管理者はそれを編集し、ログ サーバを定義して、外部プラットフォームへのログ転送を構成できます。

```
inputs-custom.conf: |
  [INPUT]
    Name          tail
    Alias         audit_apiserver_tail
    Tag           audit.apiserver.*
    Path          /var/log/vmware/audit/kube-apiserver.log
    DB            /var/log/vmware/fluentbit/flb_audit_apiserver.db
    Buffer_Max_Size 12MBb
    Mem_Buf_Limit 32MB
    Skip_Long_Lines On
    Refresh_Interval 10

filters-custom.conf: |
  [FILTER]
    Name          record_modifier
    Alias         audit_apiserver_modifier
    Match         audit.apiserver.*
    Record        hostname ${NODE_NAME}
    Record        appname audit-kube-apiserver
    Record        filename kube-apiserver.log

outputs-custom.conf: |
  [OUTPUT]
    Name          syslog
    Alias         audit_apiserver_output_syslog
    Match         audit.apiserver.*
    Host          <syslog-server-host>
    Port          <syslog-server-port>
    Mode          tcp
    Syslog_Format rfc5424
    Syslog_Message_key log
    Syslog_Hostname_key hostname
    Syslog_Appname_key appname
    Syslog_Msgid_key filename
```

Fluent Bit ログ転送のカスタマイズ

次の手順に従って、Fluent Bit ログ転送構成をカスタマイズします。

- 1 vCenter Single Sign-On 管理者として、スーパーバイザー 制御プレーンにログインします。

```
> kubectl vsphere login --server=<supervisor-cluster-vip> -u administrator@vsphere.local
> kubectl config use-context <supervisor-cluster-vip>
```

- 2 fluentbit-config-custom ConfigMap の outputs-custom.conf セクションで、Syslog 出力を更新または追加します。これにより、すべての制御プレーン仮想マシン システム ログが外部サーバに転送されるようになります。

```
[OUTPUT]
  Name          syslog
  Alias         syslog_system
  Match         system*
  Host          <syslog-server-host>
  Port         <syslog-server-port>
  Mode         tcp
  Syslog_Format rfc5424
  Syslog_Message_key log
  Syslog_Hostname_key hostname
  Syslog_Appname_key appname
  Syslog_Msgid_key filename
  # add the following if the mode is TLS
  Tls          on
  Tls.verify   off
  Tls.ca_file  /etc/ssl/certs/vmca.pem
```

- 3 変更を fluentbit-config-custom ConfigMap に適用します。

```
> kubectl -n vmware-system-logging edit cm fluentbit-config-custom

# use the below command if the change is stored in outputs-custom.conf file
> kubectl -n vmware-system-logging create configmap fluentbit-config-custom --from-file=filters-custom.conf --from-file=inputs-custom.conf --from-file=outputs-custom.conf -o yaml --from-file=parsers-custom.conf --dry-run | kubectl replace -f -
```

- 4 Fluent Bit ポッドを監視して構成の変更を自動的に適用し、Syslog サーバのスーパーバイザー ログを照会します。更新した構成が再ロードされた後に Fluentbit DaemonSet でエラーが発生する場合は、fluentbit-config-custom ConfigMap で構成を修復またはリセットして、Fluentbit DaemonSet が健全に動作するようにします。

```
> kubectl -n vmware-system-logging get pod
> kubectl -n vmware-system-logging logs <fluentbit-pod-name>
```

Kubernetes API サーバ監査ログの Grafana Loki サーバへの転送

次の手順に従って、外部 Grafana Loki サーバへのログ転送を構成します。

- 1 vCenter Single Sign-On 管理者として、スーパーバイザー 制御プレーンにログインします。

```
> kubectl vsphere login --server=<supervisor-cluster-vip> -u administrator@vsphere.local
> kubectl config use-context <supervisor-cluster-vip>
```

- 2 fluentbit-config-custom ConfigMap の outputs-custom.conf セクションで、Loki 出力を更新または追加します。これにより、すべての制御プレーン仮想マシン システム ログが Loki ログ サーバに転送されるようになります。

```
[OUTPUT]
  Name loki
  Alias system_output_loki
  Match system*
  Host <loki-server-host>
  Port <loki-server-port>
  Labels $hostname,$appname,$filename,$procid,$labels
```

- 3 変更を fluentbit-config-custom ConfigMap に適用します。

```
> kubectl -n vmware-system-logging edit cm fluentbit-config-custom

# use the below command if the change is stored in outputs-custom.conf file
> kubectl -n vmware-system-logging create configmap fluentbit-config-custom --from-file=filters-custom.conf --from-file=inputs-custom.conf --from-file=outputs-custom.conf -o yaml --from-file=parsers-custom.conf --dry-run | kubectl replace -f -
```

- 4 Fluent Bit ポッドを監視して構成の変更を自動的に適用し、Syslog サーバのスーパーバイザー ログを照会します。更新した構成が再ロードされた後に Fluentbit DaemonSet でエラーが発生する場合は、fluentbit-config-custom ConfigMap で構成を修復またはリセットして、Fluentbit DaemonSet が健全に動作するようにします。

```
> kubectl -n vmware-system-logging get pod
> kubectl -n vmware-system-logging logs <fluentbit-pod-name>
```

Elastic Search へのログの転送

次の手順に従って、外部 Elastic Search サーバへのログ転送を構成します。

- 1 vCenter Single Sign-On 管理者として、スーパーバイザー 制御プレーンにログインします。

```
> kubectl vsphere login --server=<supervisor-cluster-vip> -u administrator@vsphere.local
> kubectl config use-context <supervisor-cluster-vip>
```

- 2 fluentbit-config-custom ConfigMap の outputs-custom.conf セクションで、Elastic Search 出力を更新または追加します。これにより、すべての制御プレーン仮想マシン システム ログが Elastic Search ログ サーバに転送されるようになります。

```
[OUTPUT]
  Name es
  Alias system_output_es
  Match system*
  Host <es-server-host>
  Port <es-server-port>
  Index supervisor
  Type controlplanevm
```

3 変更を fluentbit-config-custom ConfigMap に適用します。

```
> kubectl -n vmware-system-logging edit cm fluentbit-config-custom

# use the below command if the change is stored in outputs-custom.conf file
> kubectl -n vmware-system-logging create configmap fluentbit-config-custom --from-
file=filters-custom.conf --from-file=inputs-custom.conf --from-file=outputs-custom.conf -o
yaml --from-file=parsers-custom.conf --dry-run | kubectl replace -f -
```

4

5 Fluent Bit ポッドを監視して構成の変更を自動的に適用し、Syslog サーバの スーパーバイザー ログを照会します。

```
> kubectl -n vmware-system-logging get pod
> kubectl -n vmware-system-logging logs <fluentbit-pod-name>
```

Kubernetes API 監査ログの Syslog サーバへの転送

次の手順に従って、Kubernetes API 監査ログの外部 Syslog サーバへの転送を構成します。

1 kubectl-plugin-vsphere および authproxy 入力を fluentbit-config ConfigMap に追加します。

```
[INPUT]
  Name          tail
  Tag           auth.kubectl-plugin.*
  Path          /var/log/containers/audit/kubectl-plugin-vsphere*.log
  DB            /var/log/vmware/fluentbit/flb_auth_kubectl-plugin.db
  Skip_Long_Lines Off
  Refresh_Interval 10

[INPUT]
  Name          tail
  Tag           auth.authproxy.*
  Path          /var/log/containers/audit/wcp-authproxy*.log
  DB            /var/log/vmware/fluentbit/flb_auth_authproxy.db
  Skip_Long_Lines Off
  Refresh_Interval 10
```

2 kubectl-plugin-vsphere および authproxy フィルタを fluentbit-config ConfigMap に追加します。

```
[FILTER]
  Name          kubernetes
  Match         auth.*
  Kube_URL      https://localhost:6443
  Tls.verify    Off
  K8S-Logging.Parser On
  K8S-Logging.Exclude On

[FILTER]
  Name          record_modifier
```

```

Match          auth.*
Operation      lift
Nested_under   kubernetes

[FILTER]
Name           modify
Match          auth.*
Rename         container_name appname
Rename         host hostname
Rename         pod_name procid

```

- 3 Syslog サーバへの kubectl-plugin-vsphere 出力を fluentbit-config ConfigMap に追加します。

```

[OUTPUT]
Name           syslog
Match          auth.*
Host           <syslog-server-host>
Port           <syslog-server-port>
Mode           tcp
Syslog_Format  rfc5424
Syslog_Message_key log
Syslog_Hostname_key hostname
Syslog_Appname_key appname
Syslog_Msgid_key filename

```

- 4 上記のファイルを vmware-system-logging 名前空間の fluentbit-config ConfigMap にインストールします。

```

> k -n vmware-system-logging edit cm fluentbit-config
> k -n vmware-system-logging rollout restart ds fluentbit
> k -n vmware-system-logging rollout status ds fluentbit

```

既存の構成のクローン作成による スーパーバイザー のデプロイ

13

既存のスーパーバイザー インスタンスから構成のクローンを作成して、スーパーバイザー をデプロイする方法について説明します。すでにデプロイ済みのスーパーバイザー と同様の設定を使用して新しいスーパーバイザー インスタンスをデプロイする場合は、スーパーバイザー のクローンを作成します。

前提条件

- vSphere クラスタをスーパーバイザー として構成するための前提条件を満たすこと。vSphere クラスタで vSphere IaaS control plane を構成するための前提条件を参照してください。
- スーパーバイザー をデプロイします。

手順

1 [ワークロード管理] - [スーパーバイザー] - [スーパーバイザー] の順に移動します。

2 クローンの作成元となるスーパーバイザー を選択し、[構成のクローン作成] を選択します。

選択したスーパーバイザー の値が事前に入力された状態でスーパーバイザー アクティベーション ウィザードが開きます。

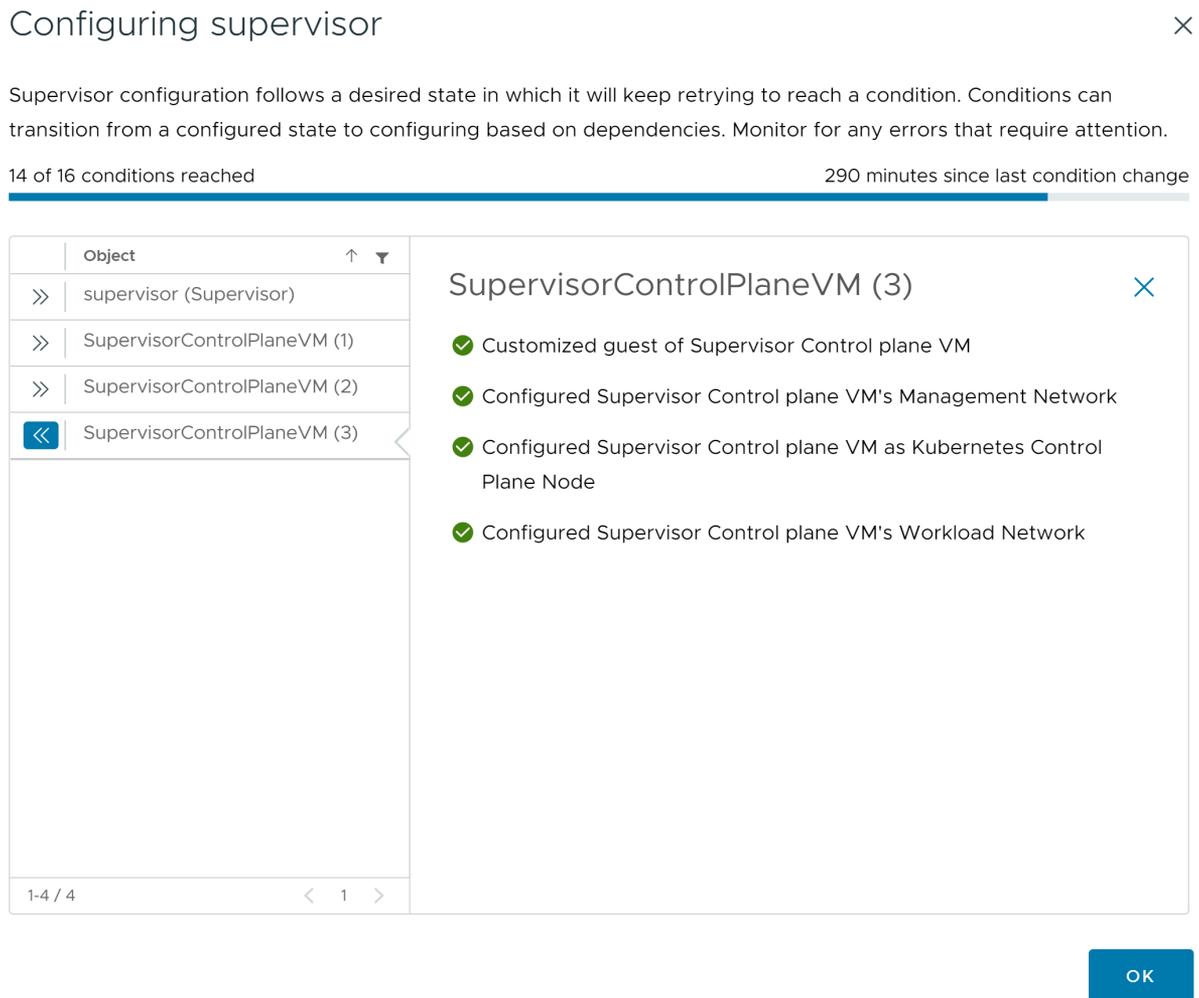
3 必要に応じて値を変更して、ウィザードを実行します。

ウィザードの値の詳細については、「5章3ゾーン スーパーバイザー のデプロイ」および「6章1ゾーン スーパーバイザー のデプロイ」を参照してください。

次のステップ

スーパーバイザー を有効にするためのウィザードを完了したら、有効化プロセスを追跡し、トラブルシューティングを必要とする潜在的な問題を確認できます。[構成ステータス] 列で、スーパーバイザー のステータスの横にある[表示] をクリックします。

図 13-1. スーパーバイザーの有効化ビュー



デプロイ プロセスを完了するには、スーパーバイザー が目的の状態に到達する、つまり、16 個の条件すべてが満たされる必要があります。スーパーバイザー が正常に有効になると、ステータスが [設定中] から [実行中] に変わります。スーパーバイザー が [設定中] 状態の間は、16 個の各条件を満たしたかどうかが継続的に再確認されます。条件を満たさない場合、成功するまで操作が再試行されます。このため、16 件中 10 件が満たされた場合など、満たした条件の数が増減する可能性があります。たとえば、16 件中 10 件が満たされた後で、16 件中 4 件が満たされるなどです。ごくまれに、目的の状態に到達することを阻止するエラーがある場合、ステータスが [エラー] に変わることがあります。

デプロイ エラーとそのトラブルシューティング方法の詳細については、「[有効化または更新中のスーパーバイザー制御プレーン仮想マシンの健全性ステータス エラーの解決](#)」を参照してください。

スーパーバイザーの有効化のトラブルシューティング

14

目的の状態を達成し、16 のすべての有効化条件が満たされるように、スーパーバイザーの有効化をトラブルシューティングする方法を確認してください。

次のトピックを参照してください。

- [有効化または更新中のスーパーバイザー制御プレーン仮想マシンの健全性ステータス エラーの解決](#)
- [リモート rsyslog に対するスーパーバイザー制御プレーンのログ ストリーミング](#)
- [ワークロード管理有効化クラスタの互換性エラーのトラブルシューティング](#)
- [ワークロード管理のログ ファイルのテール](#)

有効化または更新中のスーパーバイザー制御プレーン仮想マシンの健全性ステータス エラーの解決

スーパーバイザーを有効にするか、スーパーバイザー Kubernetes バージョンを更新するか、既存のスーパーバイザーの設定を編集すると、指定したすべての設定が検証され、構成が完了するまでスーパーバイザーに適用されます。健全性チェックは、入力したパラメータに対して実行されます。これにより、構成内のエラーが検出されて、スーパーバイザーの健全性ステータスがエラーになることがあります。これらの健全性ステータス エラーを解決して、スーパーバイザーを構成または更新できるようにする必要があります。

表 14-1. vCenter Server 接続エラー

エラー メッセージ	原因	解決方法
制御プレーン仮想マシン <仮想マシン名> に構成された管理 DNS サーバで vCenter Server プライマリ ネットワーク識別子 <FQDN> を解決できません。管理 DNS サーバ <サーバ名> で <ネットワーク名> が解決できることを検証してください。	<ul style="list-style-type: none"> ■ 1 台以上の管理 DNS サーバにアクセスできません。 ■ 1 つの管理 DNS が静的に提供されています。 ■ 管理 DNS サーバには、vCenter Server PNID のホスト名ルックアップ機能がありません。 ■ vCenter Server PNID が固定 IP アドレスではなく、ドメイン名です。 	<ul style="list-style-type: none"> ■ vCenter Server PNID のホスト エントリを管理 DNS サーバに追加します。 ■ 構成された DNS サーバが正しいことを確認します。
制御プレーン仮想マシン <仮想マシン名> の管理ネットワーク上の DHCP を介して取得した DNS サーバで vCenter Server プライマリ ネットワーク識別子 <ネットワーク名> を解決できません。管理 DNS サーバで <ネットワーク名> を解決できることを検証してください。	<ul style="list-style-type: none"> ■ DHCP サーバによって提供される管理 DNS サーバ (1 台以上) にアクセスできません。 ■ 管理 DNS サーバが静的に提供されています。 ■ 管理 DNS サーバには、vCenter Server PNID のホスト名ルックアップ機能がありません。 ■ 管理 DNS サーバには、vCenter Server PNID のホスト名ルックアップ機能がありません。 ■ vCenter Server PNID が固定 IP アドレスではなく、ドメイン名です。 	<ul style="list-style-type: none"> ■ 構成された DHCP サーバによって提供される管理 DNS サーバに、vCenter Server PNID のホスト エントリを追加します。 ■ DHCP サーバによって提供される DNS サーバが正しいことを確認します。
管理 DNS サーバが構成されていないため、制御プレーン仮想マシン <仮想マシン名> でホスト <ホスト名> を解決できません。	<ul style="list-style-type: none"> ■ vCenter Server PNID が固定 IP アドレスではなく、ドメイン名です。 ■ DNS サーバが構成されていません。 	管理 DNS サーバを構成します。
制御プレーン仮想マシン <仮想マシン名> でホスト <ホスト名> を解決できません。ホスト名の末尾のトップ レベル ドメインが「.local」であるため、管理 DNS 検索ドメインに「local」を含める必要があります。	vCenter Server PNID にはトップ レベル ドメイン (TLD) として、 .local が含まれていますが、構成された検索ドメインには local が含まれていません。	管理 DNS 検索ドメインに local を追加します。

表 14-1. vCenter Server 接続エラー (続き)

エラー メッセージ	原因	解決方法
制御プレーン仮想マシン <仮想マシン名> から管理 DNS サーバ <サーバ名> に接続できません。接続は、ワークロード ネットワークを使用して試行されました。	<ul style="list-style-type: none"> ■ 管理 DNS サーバを vCenter Server に接続できません。 ■ 指定した <code>worker_dns</code> の値には、指定した管理 DNS の値が完全に含まれていません。つまり、スーパーバイザー は固定トラフィックをこれらの IP アドレスに送信するためのネットワーク インターフェイスを 1 つ選択する必要があるため、トラフィックはワークロード ネットワークを介してルーティングされます。 	<ul style="list-style-type: none"> ■ ワークロード ネットワークを調べて、構成された管理 DNS サーバにルーティングできることを確認します。 ■ 競合する IP アドレスがないため、ワークロード ネットワーク上の DNS サーバと他のサーバ間で代替ルーティングがトリガされる可能性がないことを確認します。 ■ 構成された DNS サーバが実際には DNS サーバであり、その DNS ポートがポート 53 でホストされていることを確認します。 ■ ワークロード DNS サーバが、制御プレーン仮想マシンの IP アドレス (ワークロード ネットワークによって提供される IP アドレス) からの接続を許可するように構成されていることを確認します。 ■ 管理 DNS サーバのアドレスに誤りがないことを確認します。 ■ 検索ドメインに、不要な「~」が含まれていないことを確認します。これは、ホスト名の誤った解決の原因になる可能性があります。
制御プレーン仮想マシン <仮想マシン名> から管理 DNS サーバ <サーバ名> に接続できません。	DNS サーバに接続できません。	<ul style="list-style-type: none"> ■ 管理ネットワークを調べて、管理 DNS サーバのルートが存在することを確認します。 ■ 競合する IP アドレスがないため、DNS サーバと他のサーバ間で代替ルーティングがトリガされる可能性がないことを確認します。 ■ 構成された DNS サーバが実際には DNS サーバであり、その DNS ポートがポート 53 でホストされていることを確認します。 ■ 管理 DNS サーバが、制御プレーン仮想マシンの IP アドレスからの接続を許可するように構成されていることを確認します。 ■ 管理 DNS サーバのアドレスに誤りがないことを確認します。 ■ 検索ドメインに、不要な「~」が含まれていないことを確認します。これは、ホスト名の誤った解決の原因になる可能性があります。

表 14-1. vCenter Server 接続エラー (続き)

エラー メッセージ	原因	解決方法
制御プレーン仮想マシン <仮想マシン名> から <コンポーネント名> <コンポーネントアドレス> に接続できません。エラー: エラーメッセージ テキスト	<ul style="list-style-type: none"> ■ 一般的なネットワーク障害が発生しました。 ■ vCenter Server への実際の接続中にエラーが発生しました。 	<ul style="list-style-type: none"> ■ vCenter Server、HAProxy、NSX Manager、NSX Advanced Load Balancer などの構成済みコンポーネントのホスト名または IP アドレスが正しいことを検証します。 ■ 管理ネットワーク上の競合する IP アドレス、ファイアウォール ルールなどの外部ネットワーク設定を検証します。
制御プレーン仮想マシン <仮想マシン名> が vCenter Server <vCenter Server 名> 証明書を検証できません。vCenter Server 証明書は無効です。	vCenter Server から提供された証明書が無効な形式であるため、信頼できません。	<ul style="list-style-type: none"> ■ wcpssc を再起動して、制御プレーン仮想マシンの信頼されたルートバンドルの最新の vCenter Server ルート証明書を含む最新バンドルであることを確認します。 ■ vCenter Server 証明書が実際に有効な証明書であることを確認します。
制御プレーン仮想マシン <仮想マシン名> は vCenter Server <vCenter Server 名> 証明書を信頼していません。	<ul style="list-style-type: none"> ■ vCenter Server によって提示される vmca.pem 証明書は、制御プレーン仮想マシンに構成されているものとは異なります。 ■ vCenter Server アプライアンスの信頼されたルート証明書が置き換えられましたが、wcpssc は再起動しませんでした。 	<ul style="list-style-type: none"> ■ wcpssc を再起動して、制御プレーン仮想マシンの信頼されたルートバンドルの最新の vCenter Server 証明書のルートを含む最新バンドルであることを確認します。

表 14-2. NSX Manager 接続エラー

制御プレーン仮想マシン <仮想マシン名> が NSX サーバ <NSX サーバ名> の証明書を検証できませんでした。サーバ <NSX-T アドレス> から返されたサムプリントが、vCenter Server <vCenter Server 名> に登録された、想定されるクライアント証明書サムプリントと一致しません。	スーパーバイザーに登録された SSL サンプルが、NSX Manager によって提示された証明書の SHA-1 ハッシュと一致しません。	<ul style="list-style-type: none"> ■ NSX と vCenter Server インスタンス間にある NSX Manager で信頼を再度有効にします。 ■ vCenter Server で wcpssc を再起動します。
制御プレーン仮想マシン <仮想マシン名> から <コンポーネント名> <コンポーネントアドレス> に接続できません。エラー: エラーメッセージ テキスト	一般的なネットワーク障害が発生しました。	<ul style="list-style-type: none"> ■ NSX Manager の管理ネットワークで、競合する IP アドレス、ファイアウォールルールなどの外部ネットワーク設定を検証します。 ■ NSX 拡張機能の NSX Manager の IP アドレスが正しいことを確認します。 ■ NSX Manager が実行されていることを確認します。

表 14-3. ロード バランサ エラー

制御プレーン仮想マシン <仮想マシン名> は、ロード バランサの (<ロード バランサ>-<ロード バランサ エンドポイント>) 証明書を信頼していません。	ロード バランサが提示する証明書は、制御プレーン仮想マシンに構成されている証明書とは異なります。	ロード バランサに正しい管理 TLS 証明書が構成されていることを確認します。
制御プレーン仮想マシン <仮想マシン名> がロード バランサの (<ロード バランサ>-<ロード バランサ エンドポイント>) 証明書を検証できませんでした。証明書が無効です。	ロード バランサが提示する証明書の形式が無効であるか、有効期限が切れています。	構成されたロード バランサのサーバ証明書を修正します。
制御プレーン仮想マシン <仮想マシン名> が、ユーザー名 <ユーザー名> と指定のパスワードを使用してロード バランサ (<ロード バランサ>-<ロード バランサ エンドポイント>) に対して認証できませんでした。	ロード バランサのユーザー名またはパスワードが正しくありません。	ロード バランサに構成されたユーザー名とパスワードが正しいかどうかを確認します。
制御プレーン仮想マシン <仮想マシン名> からロード バランサ (<ロード バランサ>-<ロード バランサ エンドポイント>) に接続する際に HTTP エラーが発生しました。	制御プレーン仮想マシンはロード バランサ エンドポイントに接続できますが、エンドポイントが正常な (200) HTTP 応答を返しません	ロード バランサが健全な状態であり、要求を受け入れていることを確認します。
制御プレーン仮想マシン <仮想マシン名> から <ロード バランサ> (<ロード バランサ エンドポイント>) に接続できません。エラー: <エラー テキスト>	<ul style="list-style-type: none"> ■ 一般的なネットワーク障害が発生しました。 ■ 通常は、ロード バランサが機能していないか、ファイアウォールの一部によって接続がブロックされています。 	<ul style="list-style-type: none"> ■ ロード バランサ エンドポイントにアクセスできることを検証します ■ ファイアウォールがロード バランサへの接続をブロックしていないことを検証します。

リモート rsyslog に対する スーパーバイザー 制御プレーンのログ ストリーミング

重要なログ データの損失を防ぐため、スーパーバイザー 制御プレーン仮想マシンからリモート rsyslog レシーバに対するログ ストリーミングの構成方法をチェックします。

スーパーバイザー 制御プレーン仮想マシンのコンポーネントで生成されたログは、仮想マシンのファイル システムにローカルに保存されます。大量のログが溜まると、ログが急速にローテーションされ、さまざまな問題の根本原因の特定に役立つ貴重なメッセージが失われます。vCenter Server と スーパーバイザー 制御プレーン仮想マシンでは、リモート rsyslog レシーバに対するローカル ログのストリーミングをサポートしています。この機能は、次のサービスとコンポーネントのログのキャプチャに便利です。

- vCenter Server : ワークロード制御プレーン サービス、ESX Agent Manager サービス、認証局サービス、vCenter Server で実行しているその他のサービス。
- スーパーバイザー 制御プレーン コンポーネントと スーパーバイザー の組み込みサービス (仮想マシン サービスおよび Tanzu Kubernetes Grid など)。

ローカル ログ データを収集して、それがリモートの rsyslog レシーバにストリーミングされるように、vCenter Server アプライアンスを構成できます。この構成を vCenter Server に適用すると、vCenter Server 内で実行している rsyslog センダーは、その vCenter Server システム内のサービスで生成されたログの送信を開始します。

スーパーバイザー は、vCenter Server と同じメカニズムでローカル ログをオフロードして構成管理のオーバーヘッドを軽減します。ワークロード制御プレーン サービスは、定期的にログをポーリングして、vCenter Server rsyslog 構成を監視します。ワークロード制御プレーン サービスは、リモート vCenter Server rsyslog 構成が空でないことを検出すると、すべてのスーパーバイザー の各制御プレーン仮想マシンにこの構成を伝達します。その場合、大量の rsyslog メッセージトラフィックが生成される場合があります、リモート rsyslog レシーバが過剰負荷になるおそれがあります。そのため、レシーバ マシンには、大量の rsyslog メッセージを保存できる十分なストレージ容量が必要です。

vCenter Server から rsyslog 構成を削除すると、vCenter Server からの rsyslog メッセージが停止します。ワークロード制御プレーン サービスは変更を検出すると、それをすべてのスーパーバイザー の各制御プレーン仮想マシンに伝達し、最終的に、制御プレーン仮想マシンのストリームも停止します。

構成手順

スーパーバイザー 制御プレーン仮想マシンの rsyslog ストリーミングは、次の手順に従って構成してください。

- 1 次のようなマシンをプロビジョニングして、rsyslog レシーバを構成します。
 - rsyslog サービスをレシーバ モードで実行する。rsyslog ドキュメントの[ハイ パフォーマンスで大量のメッセージを受信するの例](#)を参照してください。
 - 大量のログ データを保存できる十分なストレージ容量がある。
 - vCenter Server とスーパーバイザー 制御プレーン仮想マシンからデータを受信するためのネットワーク接続がある。
- 2 <https://<vcenter server address>:5480> の vCenter Server アプライアンス管理インターフェイスに root としてログインします。
- 3 vCenter Server アプライアンス管理インターフェイスから rsyslog レシーバにストリーミングするように vCenter Server を構成します。[vCenter Server のログ ファイルをリモート Syslog サーバへ転送](#)を参照してください。

vCenter Server の rsyslog 構成がスーパーバイザー 制御プレーン仮想マシンに適用されるまでに数分かかる場合があります。vCenter Server アプライアンス上のワークロード制御プレーン サービスは、5 分ごとにアプライアンス構成をポーリングして、使用可能なすべてのスーパーバイザー にそれを伝達します。伝達の完了に必要な時間は、環境内のスーパーバイザー の数によって異なります。スーパーバイザー 上の一部の制御プレーン仮想マシンが健全でない場合、または他の操作を実行している場合、ワークロード制御プレーン サービスは rsyslog 構成が適用されるまでこの動作を繰り返します。

制御プレーン仮想マシン コンポーネントのログの検査

スーパーバイザー 制御プレーン仮想マシンの rsyslog は、ログ メッセージのソース コンポーネントを示すタグをログ メッセージに組み込みます。

ログタグ	説明
vns-control-plane-pods <pod_name>/<instance_number>.log	制御プレーン仮想マシンの Kubernetes ポッドから送信されたログ。 例： vns-control-plane-pods etcd/0.log または vns-control-plane-pods nsx-ncp/573.log
vns-control-plane-vmc	制御プレーン仮想マシンから得られた初期構成ログ。
vns-control-plane-bootstrap	Kubernetes ノードの制御プレーンのデプロイから得られたブートストラップ ログ。
vns-control-plane-upgrade-logs	制御プレーン ノードのパッチとマイナー バージョンのアップグレードから得られたログ。
vns-control-plane-svchost-logs	制御プレーン仮想マシンのシステム レベルのサービス ホストまたはエージェントのログ。
vns-control-plane-update-controller	制御プレーンの目的の状態のシンクロナイザとリアライザのログ。
vns-control-plane-compact-etcd-logs	制御プレーンの etcd サービス ストレージ圧縮を維持するためのログ。

ワークロード管理有効化クラスタの互換性エラーのトラブルシューティング

vSphere クラスタにワークロード管理を有効にするための互換性がないことをシステムが示す場合は、次のトラブルシューティングのヒントを参照してください。

問題

ワークロード管理を有効にしようとしたときに、vCenter Server クラスタに互換性がないことが [ワークロード管理] 画面に示されます。

原因

これには複数の原因があります。まず、環境がワークロード管理を有効にするための最小要件を満たしていることを確認します。

- 有効なライセンス : Kubernetes のアドオンを含む VMware vSphere 7 Enterprise Plus
- 少なくとも 2 台の ESXi ホスト
- 完全に自動化された DRS
- vSphere HA
- vSphere Distributed Switch 7.0
- 十分なストレージ容量

環境がこれらの前提条件を満たしているが、ターゲットの vCenter Server クラスタに互換性がない場合は、VMware Datacenter CLI (DCLI) を使用して問題を特定します。

解決方法

- 1 vCenter Server に SSH 接続します。
- 2 root ユーザーとしてログインします。
- 3 `dcli` コマンドを実行して、VMware Datacenter CLI のヘルプを一覧表示します。
- 4 次の DCLI コマンドを実行して、使用可能な vCenter Server クラスタを一覧表示します。

```
dcli com vmware vcenter cluster list
```

例：

```
dcli +username VI-ADMIN-USER-NAME +password VI-ADMIN-PASSWORD com vmware vcenter cluster list
```

結果の例：

```
|-----|-----|-----|-----|
|drs_enabled|cluster |name          |ha_enabled|
|-----|-----|-----|-----|
|True       |domain-d7|vSAN Cluster|True      |
|-----|-----|-----|-----|
```

- 5 次の DCLI コマンドを実行して、vCenter Server クラスタの互換性を確認します。

```
dcli com vmware vcenter namespacemanagement clustercompatibility list
```

例：

```
dcli +username VI-ADMIN-USER-NAME +password VI-ADMIN-PASSWORD com vmware vcenter namespacemanagement clustercompatibility list
```

次の結果の例は、互換性のある NSX VDS スイッチが環境にないことを示しています。

```
|-----|-----|-----|-----|
|-----|
|cluster |compatible|
incompatibility_reasons |
|-----|-----|-----|-----|
|-----|
|domain-d7|False      |Failed to list all distributed switches in vCenter 2b1c1fa5-
e9d4-45d7-824c-fa4176da96b8.|
|          |          |Cluster domain-d7 is missing compatible NSX
VDS.      |
|-----|-----|-----|-----|
|-----|
```

- 6 必要に応じて追加の DCLI コマンドを実行して、その他の互換性の問題を特定します。非互換の一般的な理由には、NSX エラーのほかに、DNS や NTP 接続の問題があります。

- 7 さらにトラブルシューティングを行うには、次の手順を実行します。
 - a `wcpsvc.log` ファイルをテールします。ワークロード管理のログ ファイルのテールを参照してください。
 - b [ワークロード管理] 画面に移動し [有効化] をクリックします。

ワークロード管理のログ ファイルのテール

ワークロード管理のログ ファイルをテールすると、有効化の問題や スーパーバイザー のデプロイ エラーのトラブルシューティングに役立ちます。

解決方法

- 1 vCenter Server Appliance への SSH 接続を確立します。
- 2 `root` ユーザーとしてログインします。
- 3 `shell` コマンドを実行します。

次のメッセージが表示されます。

```
Shell access is granted to root
root@localhost [ ~ ]#
```

- 4 次の コマンドを実行して、ログをテールします。

```
tail -f /var/log/vmware/wcp/wcpsvc.log
```

ネットワークのトラブルシューティング

15

スーパーバイザーを有効にしたときに発生する可能性のあるネットワークおよびロード バランサの問題をトラブルシューティングできます。

次のトピックを参照してください。

- NSX Manager による vCenter Server の登録
- NSX Advanced Load Balancer のトラブルシューティングのためのサポート バンドルの収集
- ホスト トランスポート ノードのトラフィックに必須の Distributed Switch

NSX Manager による vCenter Server の登録

状況に応じて、vCenter Server OIDC を NSX Manager に再登録する必要があります。たとえば、vCenter Server の FQDN/PNID が変更された場合などです。

手順

- 1 SSH [Secure SHell] を介して vCenter Server アプライアンスに接続します。
- 2 shell コマンドを実行します。
- 3 vCenter Server サムプリントを取得するには、次のコマンドを実行します。

```
- openssl s_client -connect vcenterserver-FQDN:443 </dev/null 2>/dev/null | openssl x509  
-fingerprint -sha256 -noout -in /dev/stdin
```

サムプリントが表示されます。たとえば、

```
08:77:43:29:E4:D1:6F:29:96:78:5F:BF:D6:45:21:F4:0E:3B:2A:68:05:99:C3:A4:89:8F:F2:0B  
:EA:3A:BE:9D。
```

- 4 SHA256 サムプリントをコピーし、コロンを削除します。

```
08774329E4D16F2996785FBFD64521F40E3B2A680599C3A4898FF20BEA3ABE9D
```

- 5 vCenter Server の OIDC を更新するには、次のコマンドを実行します。

```
curl --location --request POST 'https://<NSX-T_ADDRESS>/api/v1/trust-management/oidc-uris'  
\ --header 'Content-Type: application/json' \  
\ --header 'Authorization: Basic <AUTH_CODE>' \  
\ --data-raw '{
```

```
"oidc_type": "vcenter",
  "oidc_uri": "https://<VC_ADDRESS>/openidconnect/vsphere.local/.well-known/openid-configuration",
  "thumbprint": "<VC_THUMBPRINT>"
}'
```

NSX アプライアンスのパスワードを変更できない

root、admin、または audit ユーザーの NSX アプライアンス パスワードを変更できない場合があります。

問題

root、admin、または audit ユーザーの NSX アプライアンス パスワードを、vSphere Client を介して変更すると失敗することがあります。

原因

NSX Manager のインストール時は、3 つのロールすべてに対して 1 つのパスワードのみが受け入れられます。このパスワードを後で変更すると失敗することがあります。

解決方法

- ◆ NSX API を使用してパスワードを変更します。

詳細については、<https://kb.vmware.com/s/article/70691> と『NSX 管理ガイド』を参照してください。

障害が発生したワークフローと不安定な NSX Edge のトラブルシューティング

ワークフローで障害が発生している場合や NSX Edge が不安定になっている場合は、トラブルシューティング手順を実行することで対処できます。

問題

vSphere Client で分散ポート グループ設定を変更すると、ワークフローで障害が発生し、NSX Edge が不安定になることがあります。

原因

クラスタ設定の NSX Edge クラスタの設定中に作成されたオーバーレイおよびアップリンクの分散ポート グループを削除または変更することは、設計上許可されていません。

解決方法

NSX Edge の VLAN または IP アドレス プール設定を変更する必要がある場合は、まず NSX の要素と vSphere IaaS control plane の設定をクラスタから削除する必要があります。

NSX の要素の削除については、『NSX インストール ガイド』を参照してください。

NSX のトラブルシューティングのためのサポート バンドルの収集

トラブルシューティングのために登録済みのクラスタおよびファブリック ノードのサポート バンドルを収集して、そのバンドルをマシンにダウンロードするか、ファイル サーバにアップロードすることができます。

バンドルをマシンにダウンロードする場合は、マニフェスト ファイルと各ノードのサポート バンドルで構成される単一のアーカイブ ファイルが取得されます。バンドルをファイル サーバにアップロードする場合は、マニフェスト ファイルと個々のバンドルがファイル サーバに個別にアップロードされます。

手順

- 1 ブラウザから、管理者権限で NSX Manager にログインします。
- 2 [システム] - [サポート バンドル] の順に選択します。
- 3 ターゲット ノードを選択します。
選択可能なノードのタイプは、[管理ノード]、[Edge]、[ホスト]、および [Public Cloud Gateway] です。
- 4 (オプション) ログの有効期間を日数で指定します。指定した日数を経過したログは除外されます。
- 5 (オプション) コア ファイルおよび監査ログを含めるか除外するかを示すスイッチを切り替えます。

注： コア ファイルと監査ログには、パスワードや暗号化キーなどの機密情報が含まれている場合があります。

- 6 (オプション) バンドルをファイル サーバにアップロードするには、このチェック ボックスを選択します。
- 7 [バンドル収集の開始] をクリックして、サポート バンドルの収集を開始します。
各ノードのログ ファイルの数によって、サポート バンドルの収集にかかる時間が決まります。
- 8 収集プロセスのステータスを監視します。
[ステータス] タブに、サポート バンドルの収集の進行状況が表示されます。
- 9 バンドルをファイル サーバに送信するオプションを設定しなかった場合は、[ダウンロード] をクリックしてバンドルをダウンロードします。

NSX のログ ファイルの収集

エラーの検出やトラブルシューティングのために、vSphere IaaS control plane および NSX コンポーネントのログを収集することができます。ログ ファイルは VMware サポートによって要求される場合があります。

手順

- 1 vSphere Client を使用して、vCenter Server にログインします。
- 2 以下のログ ファイルを収集します。

ログ ファイル	説明
<code>/var/log/vmware/wcp/wcpsvc.log</code>	vSphere IaaS control plane の有効化に関する情報が含まれています。
<code>/var/log/vmware/wcp/nsxd.log</code>	NSX コンポーネントの構成に関する情報が含まれています。

- 3 NSX Manager にログインします。
- 4 特定の vSphere IaaS control plane の操作が失敗したときに NSX Manager が返すエラーに関する情報については、`/var/log/proton/nsxapi.log` を収集します。

NSX の管理証明書、サムプリント、または IP アドレスが変更された場合の WCP サービスの再起動

vSphere IaaS control plane のインストール後に NSX の管理証明書、サムプリント、または IP アドレスが変更された場合は、WCP サービスを再起動する必要があります。

NSX 証明書が変更された場合の vSphere IaaS control plane サービスの再起動

現在、vSphere IaaS control plane では、NSX の証明書かサムプリント、または NSX の IP アドレスが変更された場合、変更を反映するには WCP サービスを再起動する必要があります。どちらかが変更され、サービスを再起動しなかった場合、vSphere IaaS control plane と NSX 間の通信が失敗し、NCP が CrashLoopBackoff ステージに切り替わったり、スーパーバイザー リソースがデプロイ不可になったりするなど、特定の症状が発生する可能性があります。

WCP サービスを再起動するには、`vmon-cli` を使用します。

- 1 vCenter Server に SSH 接続し、root ユーザーとしてログインします。
- 2 `shell` コマンドを実行します。
- 3 `vmon-cli -h` コマンドを実行して、使用する構文とオプションを表示します。
- 4 `vmon-cli -l` コマンドを実行して、wcp プロセスを表示します。
リストの一番下に wcp サービスが表示されます。
- 5 `vmon-cli --restart wcp` コマンドを実行し、wcp サービスを再起動します。
Completed Restart service request というメッセージが表示されます。
- 6 `vmon-cli -s wcp` コマンドを実行し、wcp サービスが開始されていることを確認します。

例：

```
root@localhost [ ~ ]# vmon-cli -s wcp
Name: wcp
Starttype: AUTOMATIC
RunState: STARTED
RunAsUser: root
CurrentRunStateDuration(ms): 22158
HealthState: HEALTHY
FailStop: N/A
MainProcessId: 34372
```

NSX Advanced Load Balancer のトラブルシューティングのためのサポートバンドルの収集

NSX Advanced Load Balancer の問題のトラブルシューティングを行うには、サポートバンドルを収集します。サポートバンドルは VMware のサポートによって要求される場合があります。

サポートバンドルを生成すると、ダウンロードできるデバッグログ用の単一のファイルが取得されます。

手順

- 1 NSX Advanced Load Balancer Controller ダッシュボードで、左上隅のメニューをクリックし、[管理] を選択します。
- 2 [管理] セクションで、[システム] を選択します。
- 3 [システム] 画面で、[Tech Support] を選択します。
- 4 診断バンドルを生成するには、[Tech Support の生成] をクリックします。
- 5 [Tech Support の生成] ウィンドウで、[デバッグ ログ] タイプを選択し、[生成] をクリックします。
- 6 バンドルが生成されたら、[ダウンロード] アイコンをクリックしてマシンにダウンロードします。

ログ収集の詳細については、<https://avinetworks.com/docs/21.1/collecting-tech-support-logs/> を参照してください。

NSX Advanced Load Balancer 構成が適用されない

スーパーバイザー をデプロイしてもデプロイが完了せず、NSX Advanced Load Balancer 構成が適用されません。

問題

プライベート認証局 (CA) の署名付き証明書を指定した場合に、NSX Advanced Load Balancer の構成が適用されません。

スーパーバイザー で実行されているいずれかの NCP ポッドのログ ファイルに、Unable to find certificate chain というエラー メッセージが記録される可能性があります。

- 1 スーパーバイザー 仮想マシンにログインします。
- 2 コマンド `kubectl get pods -A` を使用して、すべてのポッドを一覧表示します。
- 3 スーパーバイザー 上のすべての NCP ポッドからログを取得します。

```
kubectl -n vmware-system-nsx logs nsx-ncp-<id> | grep -i alb
```

原因

Java SDK は、NCP と NSX Advanced Load Balancer Controller の間で通信を確立するために使用されます。このエラーは、NSX トラスト ストアが Java 証明書トラスト ストアと同期していない場合に発生します。

解決方法

- 1 NSX Advanced Load Balancer からルート CA 証明書をエクスポートし、NSX Manager に保存します。
- 2 root ユーザーとして NSX Manager にログインします。
- 3 すべての NSX Manager ノードで、以下のコマンドを順番に実行します。

```
keytool -importcert -alias startssl -keystore /usr/lib/jvm/jre/lib/security/cacerts
-storepass changeit -file <ca-file-path>
```

パスが見つからない場合は、`keytool -importcert -alias startssl -keystore /usr/java/jre/lib/security/cacerts -storepass changeit -file <ca-file-path>` を実行します。

```
sudo cp <ca-file-path> /usr/local/share/ca-certificates/
sudo update-ca-certificates
service proton restart
```

注： 同じ手順を実行して、中間 CA 証明書を割り当てることができます。

4 スーパーバイザー デプロイが完了するまで待つか、デプロイが実行されない場合は再デプロイします。

ESXi ホストをメンテナンス モードに切り替えることができない

アップグレードを実行する場合は、ESXi ホストをメンテナンス モードに切り替えます。

問題

ESXi ホストをメンテナンス モードに切り替えることができないため、ESXi と NSX のアップグレードに影響する可能性があります。

原因

この問題は、ESXi ホストでサービス エンジンがパワーオン状態の場合に発生する可能性があります。

解決方法

- ◆ ESXi ホストをメンテナンス モードに切り替えられるように、サービス エンジンをパワーオフします。

IP アドレスの問題のトラブルシューティング

外部 IP アドレス割り当ての問題が発生した場合は、以下に示すトラブルシューティングのヒントに従ってください。

次の理由により、IP アドレスの問題が発生することがあります。

- ゲートウェイや Ingress などの Kubernetes リソースが AKO から外部 IP アドレスを取得しない。
- Kubernetes リソースに割り当てられている外部 IP アドレスにアクセスできない。
- 外部 IP アドレスが誤って割り当てられている。

Kubernetes リソースが AKO から外部 IP アドレスを取得しない

このエラーは、AKO が NSX Advanced Load Balancer Controller で対応する仮想サービスを作成できない場合に発生します。

AKO ポッドが実行されているかどうかを確認します。ポッドが実行されている場合は、AKO コンテナ ログでエラーを確認します。

Kubernetes リソースに割り当てられている外部 IP アドレスにアクセスできない

この問題は、次の原因で発生する場合があります。

- 外部 IP アドレスをすぐには使用できないが、作成から数分以内にトラフィックの受け入れが開始される。この問題は、仮想サービスの配置に対して新しいサービス エンジンの作成がトリガされた場合に発生します。
- 対応する仮想サービスでエラーが表示されるため、外部 IP アドレスを使用できない。

プール内にサーバがない場合に仮想サービスがエラーを示したり、赤色で表示されたりすることがあります。この問題は、Kubernetes ゲートウェイまたは Ingress リソースがエンドポイント オブジェクトを参照していない場合に発生する可能性があります。

エンドポイントを表示するには、`kubectl get endpoints -n <service_namespace>` コマンドを実行し、セレクタ ラベルの問題を修正します。

健全性モニターにプール サーバの健全性が赤色で表示される場合は、プールがエラー状態になる可能性があります。

この問題を解決するには、次のいずれかの手順を実行します。

- プール サーバまたは Kubernetes ポッドが構成されたポートで待機しているかどうかを確認します。
- サービス エンジンの入力方向または出力方向のトラフィックをブロックしているドロップ ルールが NSX DFW ファイアウォールにないことを確認します。
- サービス エンジンの入力方向または出力方向のトラフィックをブロックしているネットワーク ポリシーが Kubernetes 環境にないことを確認します。

サービス エンジンの問題は、次のとおりです。

1 サービス エンジンの作成に失敗します。

次の理由により、サービス エンジンの作成に失敗することがあります。

- リソース不足のライセンスが NSX Advanced Load Balancer Controller で使用されている。
- サービス エンジン グループで作成されたサービス エンジンの数が上限に達した。
- サービス エンジン データ NIC が IP アドレスの取得に失敗した。

2 サービス エンジンの作成に失敗し、「Insufficient licensable resources available」というエラーメッセージが表示される。

このエラーは、十分なリソースを持つライセンスがサービス エンジンの作成に使用されなかった場合に発生します。

より多くのリソースが割り当てられているライセンスを取得して、NSX Advanced Load Balancer Controller に割り当てます。

3 サービス エンジンの作成に失敗し、「Reached configuration maximum limit」というエラーメッセージが表示される。

このエラーは、サービス エンジン グループで作成されたサービス エンジンの数が上限に達した場合に発生します。

このエラーを解決するには、次の手順を実行します。

- a NSX Advanced Load Balancer Controller ダッシュボードで、[インフラストラクチャ] - [クラウドリソース] - [サービス エンジン グループ] の順に選択します。
 - b IP トラフィックの障害が発生している スーパーバイザー と同じ名前のサービス エンジン グループを検索し、[編集] アイコンをクリックします。
 - c [サービス エンジンの数] に対して大きい値を構成します。
- 4 サービス エンジン データ NIC が IP アドレスの取得に失敗した。

このエラーは、次のいずれかの理由で DHCP IP プールが枯渇した場合に発生する可能性があります。

- 大規模デプロイ用に作成されたサービス エンジンの数が多すぎる。
- サービス エンジンが NSX Advanced Load Balancer ユーザー インターフェイスまたは vSphere Client から直接削除された。このような削除により、DHCP アドレスが DHCP プールから解放されず、リース割り当てエラーが発生します。

外部 IP アドレスが誤って割り当てられている

このエラーは、異なる名前空間内の 2 つの Ingress が同じホスト名を共有している場合に発生します。構成をチェックして、異なる名前空間の 2 つの Ingress に同じ名前が指定されていないことを確認します。

トラフィック エラーに関する問題のトラブルシューティング

NSX Advanced Load Balancer の構成後にトラフィック エラーが発生します。

問題

LB タイプのサービスのエンドポイントが別の名前空間にある場合にトラフィック エラーが発生することがあります。

原因

NSX Advanced Load Balancer が構成された vSphere IaaS control plane 環境では、名前空間に専用の Tier-1 ゲートウェイがあり、各 Tier-1 ゲートウェイには同じ CIDR を持つサービス エンジン セグメントがあります。NSX Advanced Load Balancer サービスとエンドポイントが別々の名前空間にある場合は、トラフィック エラーが発生することがあります。このエラーは、NSX Advanced Load Balancer が外部 IP アドレスをサービスに割り当て、外部 IP アドレスへのトラフィックが失敗するために発生します。

解決方法

- ◆ North-South トラフィックを許可するには、NSX Advanced Load Balancer サービス名前空間の SNAT IP アドレスからの入力を許可する分散ファイアウォール ルールを作成します。

NSX のバックアップとリストアによって発生した問題のトラブルシューティング

NSX のバックアップとリストアにより、NSX Advanced Load Balancer によって提供されるすべての外部 IP アドレスでトラフィック エラーが発生する可能性があります。

問題

NSX のバックアップとリストアを実行すると、トラフィック エラーが発生する可能性があります。

原因

このエラーは、リストア後にサービス エンジン NIC が復帰せず、その結果、IP プールが停止状態と表示されるために発生します。

解決方法

1 NSX Advanced Load Balancer Controller ダッシュボードで、[インフラストラクチャ] - [クラウド] の順に選択します。

2 クラウドを選択して変更を加えずに保存し、ステータスが緑色になるまで待機します。

3 すべての仮想サービスを無効にします。

NSX Advanced Load Balancer Controller がすべてのサービス エンジンから古い NIC を削除するまで待機します。

4 すべての仮想サービスを有効にします。

仮想サービスのステータスが緑色で表示されます。

トラフィック エラーが解決しない場合は、NSX Manager でスタティック ルートを再構成します。

NSX のバックアップとリストア後の古い Tier-1 セグメント

NSX のバックアップとリストアでは古い Tier-1 セグメントをリストアできます。

問題

NSX のバックアップとリストア手順の後、サービス エンジン NIC を持つ古い Tier-1 セグメントがクリーンアップされません。

原因

NSX のバックアップ後に名前空間が削除されると、リストア操作により、NSX Advanced Load Balancer Controller サービス エンジン NIC に関連付けられている古い Tier-1 セグメントがリストアされます。

解決方法

1 NSX Manager にログインします。

2 [ネットワーク] - [セグメント] の順に選択します。

3 削除した名前空間に関連付けられている古いセグメントを検索します。

4 [ポート/インターフェイス] セクションから古いサービス エンジン NIC を削除します。

ホスト トランスポート ノードのトラフィックに必須の Distributed Switch

vSphere IaaS control plane では、ホスト トランスポート ノードのトラフィックに vSphere 8.0 Virtual Distributed Switch (VDS) を使用する必要があります。vSphere IaaS control plane のホスト トランスポート ノードのトラフィックには、NSX VDS (N-VDS) を使用できません。

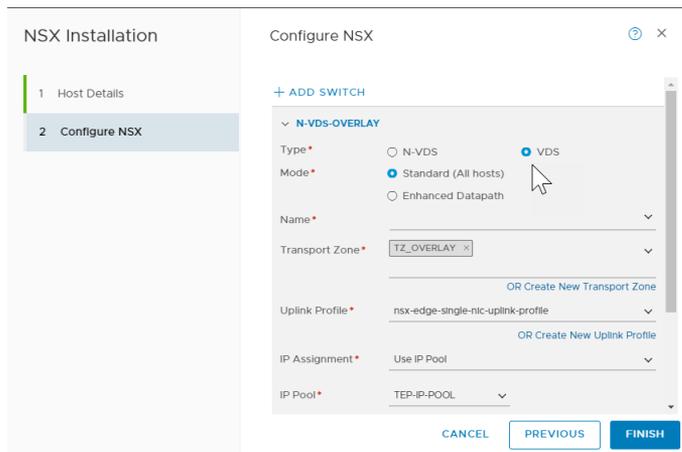
Distributed Switch は必須

vSphere IaaS control plane では、同一の Distributed Switch 上にある vSphere トラフィックと NSX トラフィックの両方をサポートする統合 Distributed Switch が必要です。vSphere および NSX の以前のリリースでは、vSphere トラフィック用に 1 台の Distributed Switch (または VSS) と、NSX トラフィック用に 1 台の N-VDS があります。この構成は、vSphere IaaS control plane ではサポートされていません。N-VDS を使用してワークロード管理を有効にすると、vCenter Server クラスタに互換性がないことが報告されます。詳細については、『ワークロード管理有効化クラスタの互換性エラーのトラブルシューティング』を参照してください。

統合 Distributed Switch を使用するには、vCenter Server を使用して vSphere 8.0 Distributed Switch を作成し、ESXi ホストをトランスポート ノードとして準備する際に NSX でこの Distributed Switch を指定します。vCenter Server 側への VDS-DSwitch の配置のみでは不十分です。[トランスポート ノード プロファイルの作成](#)のトピックに記載されているとおり、VDS-DSwitch 8.0 は次のように NSX トランスポート ノード プロファイルを使用して構成する必要があります。

ESXi ホストをトランスポート ノードとして準備する方法の詳細については、<https://kb.vmware.com/s/article/95820> および NSX ドキュメントの「トランスポート ノードとしての ESXi ホストの準備」を参照してください。

図 15-1. NSX の VDS 構成



以前のバージョンから vSphere 8.0 および NSX 4.x にアップグレードした場合は、各 ESXi トランスポート ノードから N-VDS をアンインストールして、各ホストを Distributed Switch で再構成する必要があります。ガイドランスについては、VMware グローバル サポート サービスにお問い合わせください。

vSphere IaaS control plane のトラブルシューティング

16

vSphere IaaS control plane のインフラストラクチャでは、以下のトラブルシューティング手法とベスト プラクティスを使用します。

次のトピックを参照してください。

- ストレージのベスト プラクティスとトラブルシューティング
- ネットワーク トポロジのアップグレードのトラブルシューティング
- vSphere IaaS control plane ワークロード ドメインのシャットダウンと起動
- スーパーバイザー でのサポート バンドルの収集

ストレージのベスト プラクティスとトラブルシューティング

vSphere IaaS control plane のストレージ環境で、ベスト プラクティスとトラブルシューティング手法を使用できます。

vSAN 以外のデータストアで制御プレーン仮想マシンの非アフィニティ ルールを使用する

vSphere IaaS control plane でクラスタ内の vSAN 以外のデータストアを使用する場合は、可用性を確保するために、3 つの制御プレーン仮想マシンを異なるデータストアに配置します。

制御プレーン仮想マシンはシステムで管理されているため、手動で移行することはできません。データストア クラスタと Storage DRS を組み合わせて使用して制御プレーン仮想マシンを再分散し、それらを別々のデータストアに配置します。

手順

- 1 vSphere Client で、データストア クラスタを作成します。
 - a データセンターに移動します。
 - b データセンター オブジェクトを右クリックし、[新規データストア クラスタ] を選択します。
 - c データストア クラスタに名前を付け、[Storage DRS をオンにする] が有効であることを確認します。
 - d クラスタの自動化レベルを [自動化なし (手動モード)] に設定します。
 - e Storage DRS ランタイム設定はデフォルトのままにします。
 - f vSphere IaaS control plane で有効になっている ESXi クラスタを選択します。

- g データストア クラスタに追加するすべての共有データストアを選択します。
- h [終了] をクリックします。

2 制御プレーン仮想マシンの Storage DRS ルールを定義します。

- a データストア クラスタに移動します。
- b [構成] タブをクリックし、[設定] の [ルール] をクリックします。
- c [追加] アイコンをクリックして、ルールの名前を入力します。
- d [ルールの有効化] が有効であることを確認します。
- e [ルール タイプ] を [仮想マシンの非アフィニティ] に設定します。
- f [追加] アイコンをクリックして、3 つのスーパーバイザー制御プレーン仮想マシンを選択します。
- g [OK] をクリックして設定を終了します。

3 仮想マシン オーバーライドを作成します。

- a データストア クラスタに移動します。
- b [構成] タブをクリックし、[設定] の [仮想マシンのオーバーライド] をクリックします。
- c [追加] アイコンをクリックして、3 つの制御プレーン仮想マシンを選択します。
- d Storage DRS の自動化レベルを有効にするには、[オーバーライド] チェック ボックスを選択し、値を [完全自動化] に設定します。
- e [終了] をクリックします。

結果

このタスクにより、制御プレーン仮想マシンの Storage DRS のみが有効になり、仮想マシンが再分散されて異なるデータストアに配置されます。

Storage vMotion が実行されたら、SDRS ルールおよびオーバーライドを削除し、Storage DRS を無効にして、データストア クラスタを削除することができます。

vSphere から削除されたストレージ ポリシーが引き続き Kubernetes ストレージ クラスとして表示される

vSphere Client を使用して VMware vCenter または スーパーバイザー 内の名前空間からストレージ ポリシーを削除すると、それに一致するストレージ クラスは Kubernetes 環境に残りますが、使用できません。

問題

`kubect1 get sc` コマンドを実行すると、出力には名前空間で使用できるストレージ クラスとして引き続き表示されます。ただし、そのストレージ クラスは使用できません。たとえば、新しいパーシステント ボリュームの要求に対してそのストレージ クラスを使用すると失敗します。

ストレージ クラスがすでに Kubernetes 環境で使用されている場合は、その環境で予期しない動作が発生する可能性があります。

解決方法

- 1 名前空間にあるストレージ クラスを確認するには、
`kubectl describe namespace namespace_name` コマンドを実行します。

一致するストレージ ポリシーが削除されている場合、このコマンドの出力にストレージ クラスは表示されません。
- 2 ストレージ クラスがすでにデプロイ環境で使用されている場合は、そのストレージ クラスをリストアします。
 - a vSphere Client を使用して、削除したポリシーと同じ名前の新しいストレージ ポリシーを作成します。

たとえば、*Gold* ポリシーを削除した場合は、新しいポリシーに *Gold* という名前を付けます。vSphere IaaS 制御プレーンのインストールと構成の [Create Storage Policies for vSphere with Tanzu](#) を参照してください。
 - b ポリシーを名前空間に割り当てます。

vSphere IaaS 制御プレーンのサービスとワークロードの [名前空間のストレージ設定の変更](#) を参照してください。

ポリシーを名前空間に割り当てると、vSphere IaaS control plane によって古いストレージ クラスが削除され、一致するストレージ クラスが同じ名前で作成されます。

vSAN Direct と外部ストレージの併用

vSphere IaaS control plane 環境で vSAN Direct を使用している場合に、外部共有ストレージを使用して管理内部仮想マシンおよびその他のメタデータを格納できます。

問題

同種の vSAN Direct クラスタをデプロイする場合は、スーパーバイザー制御プレーン仮想マシンおよびその他のメタデータを格納するために、クラスタ内の各 ESXi ホストにレプリケートされた vSAN データストアを作成する必要があります。vSAN データストアは容量を使用するほか、各ホストで追加の I/O コントローラが必要となります。また、vSAN Direct をサポートできるハードウェア構成が制限されます。

vSAN データストアを構成する代わりに、外部共有ストレージを使用して管理内部仮想マシンおよびその他のメタデータを格納できます。

解決方法

- 1 クラスタ内の ESXi ホストに vSAN または vSAN Direct がデプロイされている場合は、構成からホストをクリアします。
 - a vSAN または vSAN Direct に割り当てられているディスクを削除します。『VMware vSAN の管理』の [vSAN からのディスク グループまたはデバイスの削除](#) を参照してください。
 - b (オプション) スクリプトを使用して、ホスト上のディスクに vSAN Direct 用のタグを付けます。 [スクリプトを使用した vSAN Direct のストレージ デバイスのタグ付け](#) を参照してください。
- 2 VMware Cloud Foundation を使用して、外部ストレージを含むワークロード ドメインを作成します。

NFS、vVols、ファイバ チャネルなどのストレージ オプションのいずれかを選択してください。選択できるオプションは 1 つだけです。

詳細については、VMware Cloud Foundation のドキュメントの「ワークロード ドメインの操作」を参照してください。

この手順により、vCenter Server と指定した ESXi ホストを含むワークロード ドメインがデプロイされます。外部ストレージがすべてのホストにマウントされ、デフォルトのクラスタに追加されます。

3 vSAN を有効にします。

vSAN 用のディスクが要求されないことを確認します。

詳細については、『VMware vSAN の管理』の既存のクラスタで vSAN を有効にするを参照してください。

この手順により、vSAN ネットワークを使用する 0 バイトの vSAN データストアが作成されます。ローカルディスクは vSAN に使用されません。

4 ホスト上のローカル ディスクを vSAN Direct 用に要求します。

詳細については、『vSphere IaaS 制御プレーンのサービスとワークロード』の vSAN Direct データストアの作成を参照してください。

要求されるデバイスごとに、vSAN Direct は個別のデータストアを作成します。

5 vSAN Direct のストレージ ポリシーを作成します。

詳細については、『vSphere IaaS 制御プレーンのサービスとワークロード』の vSAN Direct ストレージ ポリシーの作成を参照してください。

6 スーパーバイザーを有効にします。

詳細については、『vSphere IaaS 制御プレーンのインストールと構成』ドキュメントを参照してください。

例

この例では、セットアップに外部 NFS ストレージと vSAN Direct データストアが含まれています。制御プレーン仮想マシンと vSphere ポッド は外部 NFS ストレージで実行されています。パーシステント ボリュームの要求は vSAN Direct で実行されます。

The screenshot shows the vSphere Client interface with the 'Datastores' tab selected for the cluster 'sample-1-0'. The table below displays the configured datastores:

Name	Status	Type	Datastore Cl...	Capacity	Free
nfs0-1	✓ Normal	NFS 3		295.17 GB	263.03 GB
vSANDirect	✓ Normal	vSAN Direct		199.75 GB	197.34 GB

ネットワーク トポロジのアップグレードのトラブルシューティング

vSphere IaaS control plane バージョン 7.0 Update 1c をインストールするか、スーパーバイザー をバージョン 7.0 Update 1 からバージョン 7.0 Update 1c にアップグレードすると、ネットワーク トポロジは単一の Tier-1 ゲートウェイ トポロジから、スーパーバイザー 内の名前空間ごとに 1 つの Tier-1 ゲートウェイがあるトポロジにアップグレードされます。

アップグレード中に発生する可能性のある問題のトラブルシューティングを行うことができます。

Edge ロード バランサのキャパシティ不足によるアップグレード事前チェックの失敗

アップグレードの事前チェックが失敗し、エラー メッセージに、ロード バランサのキャパシティが不足していることが示されます。

問題

アップグレードの事前チェック プロセスが失敗し、ロード バランサのキャパシティがスーパーバイザー で必要なキャパシティよりも少ないことを示すエラー メッセージが表示されます。

解決方法

この問題を解決するには次のいずれかの手順を実行します。

- エラー メッセージ内の [強制アップグレード] ボタンをクリックしてアップグレードを強制実行するか、vCenter Server コマンド ラインで `--ignore-precheck-warnings true` フラグを使用します。

注： このソリューションは、Edge クラスタが既存の名前空間ワークロードをサポートできる場合のみ推奨されます。この条件に当てはまらない場合は、アップグレード中にこれらのワークロードがスキップされることがあります。

- 未使用のワークロードを削除します。
- Edge ノードをクラスタに追加します。

アップグレード中にスキップされるスーパーバイザー ワークロードの名前空間

スーパーバイザー のアップグレード中に、アップグレードされない名前空間ワークロードがあります。

問題

スーパーバイザー のアップグレードは成功しますが、一部の名前空間ワークロードはアップグレード中にスキップされます。Kubernetes リソースはリソースが不足していることを示し、新たに作成された Tier-1 ゲートウェイは ERROR 状態になります。

原因

ワークロードをサポートするためのロード バランサのキャパシティが不足しています。

解決方法

この問題を解決するには次のいずれかの手順を実行します。

- 未使用のワークロードを削除し、NCP を再起動して、アップグレードを再度実行します。
- Edge ノードをクラスタに追加して、Tier-1 ゲートウェイへの再割り当てをトリガします。NCP を再起動して、アップグレードを再実行します。

アップグレード中にスキップされるロード バランサ サービス

スーパーバイザー のアップグレード中に、アップグレードされないロード バランサ サービスがあります。

問題

スーパーバイザー のアップグレードは成功しますが、一部の Kubernetes ロード バランサ サービスはアップグレード中にスキップされます。

原因

スーパーバイザー のワークロードおよび関連付けられた Tanzu Kubernetes クラスタ内の Kubernetes ロード バランサ タイプのサービスの数が、NSX Edge 仮想サーバの制限を超えています。

解決方法

未使用のワークロードを削除し、NCP を再起動して、アップグレードを再度実行します。

vSphere IaaS control plane ワークロード ドメインのシャットダウンと起動

データ損失を回避し、vSphere IaaS control plane 環境のコンポーネントおよびワークロードを運用可能な状態に維持するには、コンポーネントのシャットダウンまたは起動時に、特定の順序で実行する必要があります。

通常は、vSphere IaaS control plane 環境にパッチの適用、アップグレード、またはリストアを実行した後に、シャットダウンおよび起動の操作を実行します。

Tanzu Kubernetes Grid によってプロビジョニングされた Tanzu Kubernetes クラスタを含む vSphere IaaS control plane ソリューションは、vSphere Software-Defined Data Center (SDDC) の一部です。したがって、vSphere IaaS control plane 環境をシャットダウンして起動する場合は、vSphere インフラストラクチャ スタック全体を考慮する必要があります。vSphere IaaS control plane を含む vSphere SDDC のシャットダウンと起動については、次に示す検証済みの一連の手順を参照してください。

- [vSphere IaaS control plane を含む vSphere SDDC のシャットダウン手順](#)
- [vSphere IaaS control plane を含む vSphere SDDC の起動手順](#)

スーパーバイザー でのサポート バンドルの収集

スーパーバイザー でのサポート バンドルの収集方法を確認します。スーパーバイザー がエラーまたは構成状態であっても、サポート バンドルの収集は可能です。

前提条件

- ユーザー アカウントには、グローバル診断権限が必要です。

手順

- 1 vSphere Client を使用して、vSphere IaaS control plane 環境にログインします。
- 2 [メニュー] - [ワークロー管理] の順に選択します。
- 3 [スーパーバイザー] タブを選択します。
- 4 ターゲット スーパーバイザー を選択します。
- 5 [ログのエクスポート] をクリックします。

結果

サポート バンドルを収集したら、ナレッジベースの記事「Secure FTP ポータル経由での VMware への診断情報のアップロード」(<http://kb.vmware.com/kb/2069559>) を参照してください。