Installieren und Konfigurieren der vSphere IaaS-Steuerungsebene

Update 3
VMware vSphere 8.0
VMware vCenter 8.0
VMware ESXi 8.0

vmware by Broadcom

Die aktuellste technische Dokumentation finden Sie auf der VMware by Broadcom-Website unter:

https://docs.vmware.com/de/

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

Inhalt

Installieren und Konfigurieren der vSphere IaaS-Steuerungsebene

In *Installieren und Konfigurieren der vSphere IaaS-Steuerungsebene* wird beschrieben, wie die vSphere IaaS control plane (zuvor vSphere with Tanzu) mit vSphere Client konfiguriert und verwaltet wird.

Installieren und Konfigurieren der vSphere IaaS-Steuerungsebene enthält Anweisungen zum Aktivieren von vSphere IaaS control plane auf vorhandenen vSphere-Clustern sowie zum Erstellen und Verwalten von Namespaces. Diese Informationen enthalten auch Richtlinien zum Einrichten einer Sitzung mit der Kubernetes-Steuerungsebene über kubectl.

Zielgruppe

Installieren und Konfigurieren der vSphere IaaS-Steuerungsebene ist für vSphere-Administratoren vorgesehen, die vSphere IaaS control plane in vSphere aktivieren, Namespaces konfigurieren und DevOps-Teams bereitstellen möchten. vSphere-Administratoren, die vSphere IaaS control plane verwenden möchten, sollten über Grundkenntnisse in den Bereichen Container und Kubernetes verfügen.

Aktualisierte Informationen

Installieren und Konfigurieren der vSphere IaaS-Steuerungsebene wird mit jeder Produktversion oder bei Bedarf aktualisiert.

Diese Tabelle enthält den Update-Verlauf für die Dokumentation *Installieren und Konfigurieren der vSphere IaaS-Steuerungsebene*.

Revision	Beschreibung
25. Juni 2024	Allgemeine Updates und Verbesserungen für vSphere 8.0 Update 3.
18. MÄR 2024	Das Thema Ersetzen des VIP-Zertifikats zur sicheren Verbindung mit dem Supervisor-API-Endpoint wurde mit einem Hinweis zum Importieren der gesamten Zertifikatskette aktualisiert.
29. FEB 2024	■ Es wurden Schritte zum Erstellen einer benutzerdefinierten Cloud während der Erstkonfiguration des Controllers hinzugefügt. Weitere Informationen hierzu finden Sie unter Konfigurieren des Controllers. ■ Es wurden Schritte zur Auswahl der Cloud bei der Bereitstellung des Supervisors hinzugefügt. Weitere Informationen finden Sie unter Bereitstellen eines Supervisor für drei Zonen mit dem VDS-Netzwerk-Stack und Bereitstellen eines Supervisor für eine Zone mit dem VDS-Netzwerk-Stack. ■ Es wurden Schritte zum Konfigurieren der FQDN-Anmeldung mit dem Supervisor hinzugefügt. Weitere Informationen finden Sie unter Bereitstellen eines Supervisor für drei Zonen mit dem VDS-Netzwerk-Stack, Bereitstellen eines Supervisor für eine Zone mit dem VDS-Netzwerk-Stack und Ändern der Verwaltungsnetzwerkeinstellungen auf einem Supervisor. ■ Ein Schritt zum Erstellen des NSX Overlay-Segments wurde hinzugefügt. Weitere Informationen hierzu finden Sie unter Erstellen eines Tier-0-Uplink-Segments und eines Overlay-Segments.
24. JAN 2024	■ Registrieren Sie die NSX Advanced Load Balancer Controller bei NSX Manager wurde mit einem Hinweis zu DNS- und NTP-Einstellungen aktualisiert. ■ Es wurden Inhalte für Schritte hinzugefügt, die durchgeführt werden müssen, wenn die Supervisor-Bereitstellung nicht abgeschlossen wird und die NSX Advanced Load Balancer-Konfiguration nicht angewendet wird, wenn ein von einer privaten Zertifizierungsstelle (CA) signiertes Zertifikat bereitgestellt wird. Weitere Informationen hierzu finden Sie unter NSX Advanced Load Balancer Konfiguration wird nicht angewendet.
23. DEZ 2023	■ Es wurden Inhalte zum Ändern der Lastausgleichsdiensteinstellungen auf einem mit VDS-Netzwerk konfigurierten Supervisor hinzugefügt. Weitere Informationen finden Sie unter Ändern der Einstellungen für den Lastausgleichsdienst auf einem Supervisor, der mit VDS-Netzwerk konfiguriert ist. ■ Der Inhalt zum Ändern der Einstellungen für das Arbeitslastnetzwerk von Supervisor, die mit dem VDS-Netzwerk konfiguriert sind, wurde aktualisiert. Weitere Informationen finden Sie unter Ändern der Einstellungen für das Arbeitslastnetzwerk auf einem Supervisor, der mit vDS-Netzwerk konfiguriert ist.
13. DEZ 2023	Es wurde eine Referenz zum Vorbereiten von ESXi-Hosts als Transportknoten hinzugefügt. Weitere Informationen finden Sie unter Für den Datenverkehr des Hosttransportknotens erforderlicher VDS.
21. NOV 2023	Die Dokumentation wurde aktualisiert, um darauf hinzuweisen, dass Multi-NSX auf dem Supervisor-Cluster nicht unterstützt wird. Weitere Informationen finden Sie unter Hinzufügen eines Compute Managers.

Revision	Beschreibung
29. SEP 2023	■ Aktualisierungen für Konfigurieren von HTTP-Proxy-Einstellungen in vSphere IaaS control plane ■ Aktualisierte Anforderungen für die Anpassung des HAProxy-Lastausgleichsdiensts. Weitere Informationen hierzu finden Sie unter Anpassen des HAProxy-Lastausgleichdiensts. .
21. SEP 2023	Der Abschnitt „Netzwerk“ wurde mit Informationen zum Installieren und Konfigurieren von NSX Advanced Load Balancer mit NSX aktualisiert. Weitere Informationen finden Sie unter Installieren und Konfigurieren von NSX und NSX Advanced Load Balancer.
30. JUN 2023	Die Größen der Supervisor-Steuerungsebene wurden in den Installationsthemen und Ändern der Größe der Steuerungsebene eines Supervisors der Supervisor hinzugefügt.
23. JUN 2023	Ein Link zum Erstellen und Bearbeiten von Inhaltsbibliotheken wurde aktualisiert. Weitere Informationen finden Sie unter Importieren der NSX Advanced Load Balancer-OVA in eine lokale Inhaltsbibliothek.
15. JUN 2023	Es wurde ein Hinweis hinzugefügt, der besagt, dass Sie nur einen HTTP-Proxy verwenden können, um einenSupervisor mit Tanzu Mission Control zu registrieren. Weitere Informationen finden Sie unter Konfigurieren von HTTP-Proxy-Einstellungen in vSphere IaaS control plane.
15. MAI 2023	Es wurde ein Hinweis hinzugefügt, dass Sie die Verbrauchsdomäne in den Speicherrichtlinien, die für einen Supervisor oder einen Namespace in einem Supervisor mit einer Zone verwendet werden, nicht aktivieren sollten. Weitere Informationen finden Sie unter Kapitel 2 Erstellen von Speicherrichtlinien für vSphere IaaS control plane.
12. MAI 2023	Es wurde ein Hinweis hinzugefügt, dass Sie, wenn Sie für Ihre vSphere IaaS control plane-Umgebung ein Upgrade von einer vSphere-Version vor 8.0 durchgeführt haben und vSphere-Zones verwenden möchten, eine neue Supervisor mit drei Zonen erstellen müssen. Weitere Informationen finden Sie unter Kapitel 5 Bereitstellen eines Supervisor für drei Zonen .
26. APR 2023	Konfiguration und Verwalten von vSphere-Namespaces verschoben in *Dienste und Arbeitslasten der vSphere IaaS-Steuerungsebene*.
18. APR 2023	Der Abschnitt Installieren und Konfigurieren von NSX Advanced Load Balancer wurde aktualisiert und enthält nun Unterstützung für NSX Advanced Load Balancer in der Version 22.1.3.

Workflow zur Installation und Konfiguration von vSphere IaaS control plane

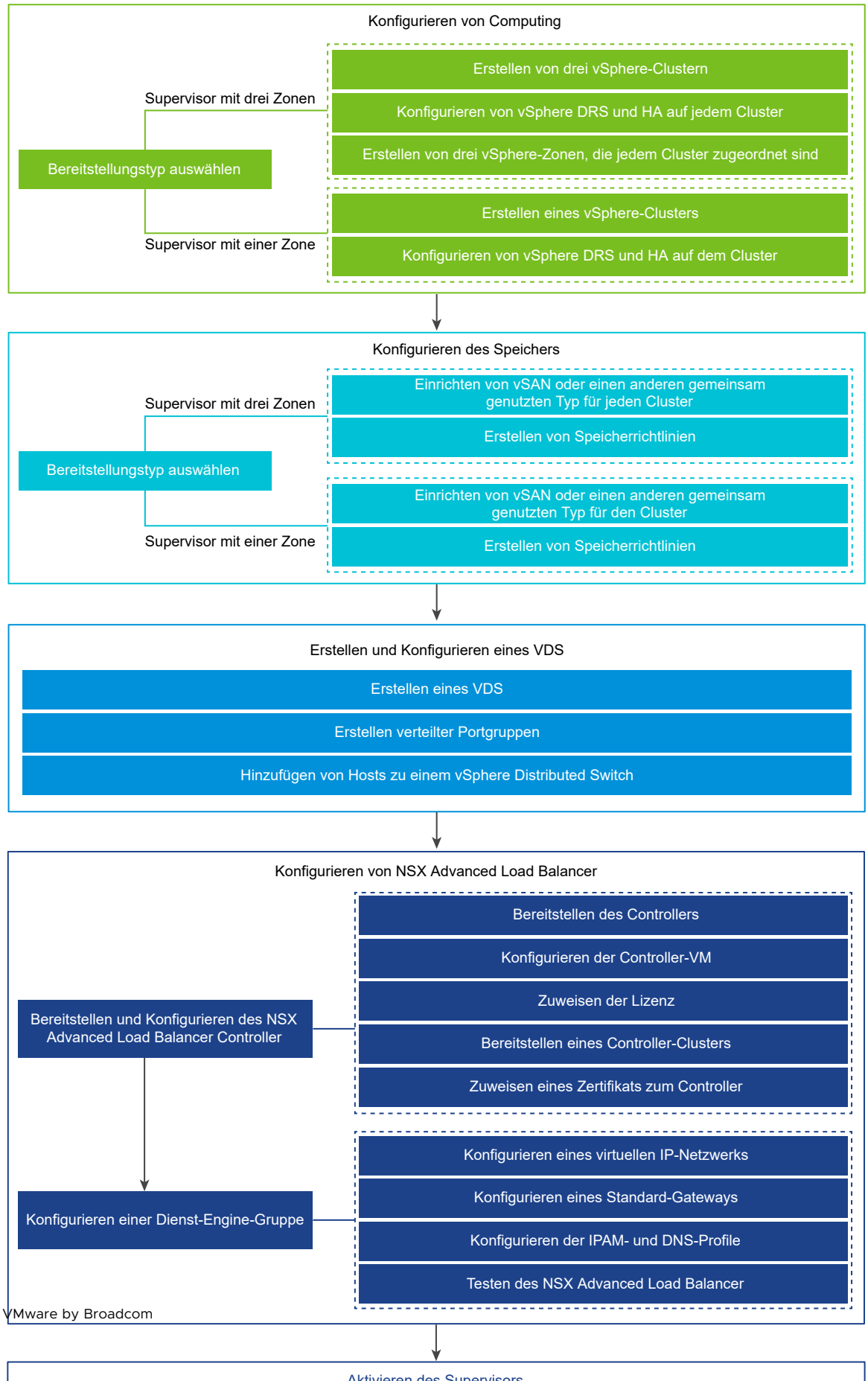
1

Überprüfen Sie die Workflows für die Umwandlung von vSphere-Clustern in eine Plattform zum Ausführen von Kubernetes-Arbeitslasten auf vSphere.

Workflow für die Bereitstellung eines Supervisors mit VDS-Netzwerk und NSX Advanced Load Balancer

Als vSphere-Administrator können Sie einen Supervisor mit dem Netzwerk-Stack basierend auf dem VDS-Netzwerk mit dem NSX Advanced Load Balancer bereitstellen.

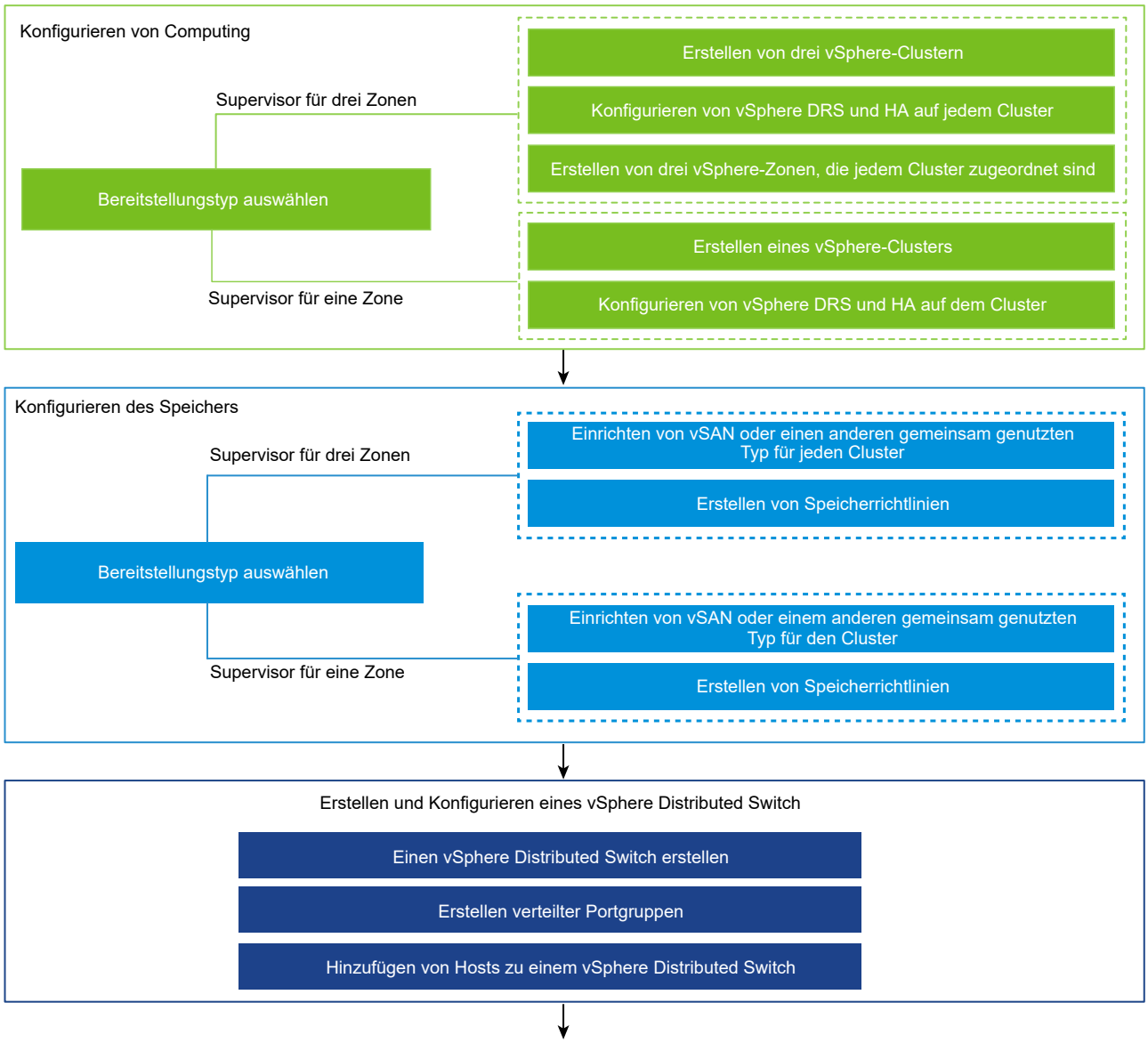
Abbildung 1-1. Workflow für die Bereitstellung eines Supervisors mit NSX Advanced Load Balancer



Workflow für Supervisor mit NSX-Netzwerk und NSX Advanced Load Balancer Controller

Als vSphere-Administrator können Sie einen Supervisor mit dem NSX-Netzwerk-Stack basierend auf NSX Advanced Load Balancer Controller bereitstellen.

Abbildung 1-2. Workflow zum Konfigurieren eines Supervisors mit NSX-Netzwerk und NSX Advanced Load Balancer Controller

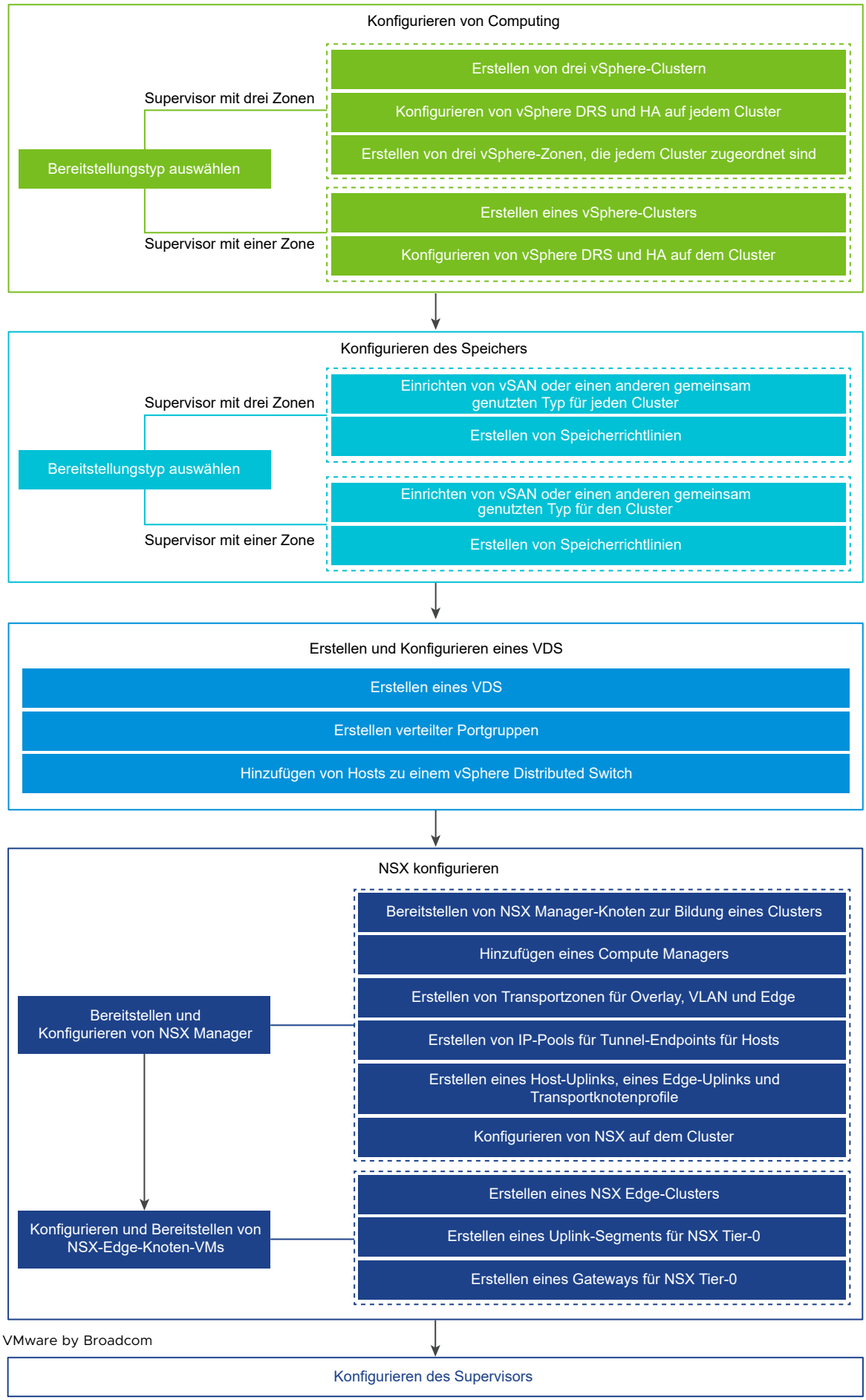



NSX konfigurieren
Bereitstellen und Konfigurieren von NSX Manager
Bereitstellen von NSX Manager-Knoten zur Bildung eines Clusters
Hinzufügen eines Compute Managers
Erstellen von Transportzonen für Overlay, VLAN und Edge
Erstellen von IP-Pools für Tunnel-Endpoints für Hosts
Erstellen eines Host-Uplinks, Edge-Uplinks, Transportknotens und Edge-Clusterprofilen
Konfigurieren von NSX auf dem Cluster
Konfigurieren und Bereitstellen von NSX Edge-Knoten-VMs
Erstellen eines NSX Edge-Clusters
Erstellen eines Gateways für NSX Tier-0
Erstellen eines Tier-0-Uplink-Segments
Erstellen eines Gateways für NSX Tier-1
Bereitstellen und Konfigurieren des NSX Advanced Load Balancer Controller
Bereitstellen des Controllers
Bereitstellen eines Controller-Clusters
Einschalten des Controllers
Konfigurieren der Controller-VM und Zuweisen einer Lizenz
Konfigurieren einer Dienst-Engine-Gruppe
Registrieren des Controllers
Zuweisen eines Zertifikats zum Controller
Testen des NSX Advanced Load Balancer
Konfigurieren des Supervisors

Workflow für die Bereitstellung eines Supervisors mit NSX-Netzwerk

Als vSphere-Administrator können Sie einen Supervisor mit dem Netzwerk-Stack basierend auf NSX bereitstellen.

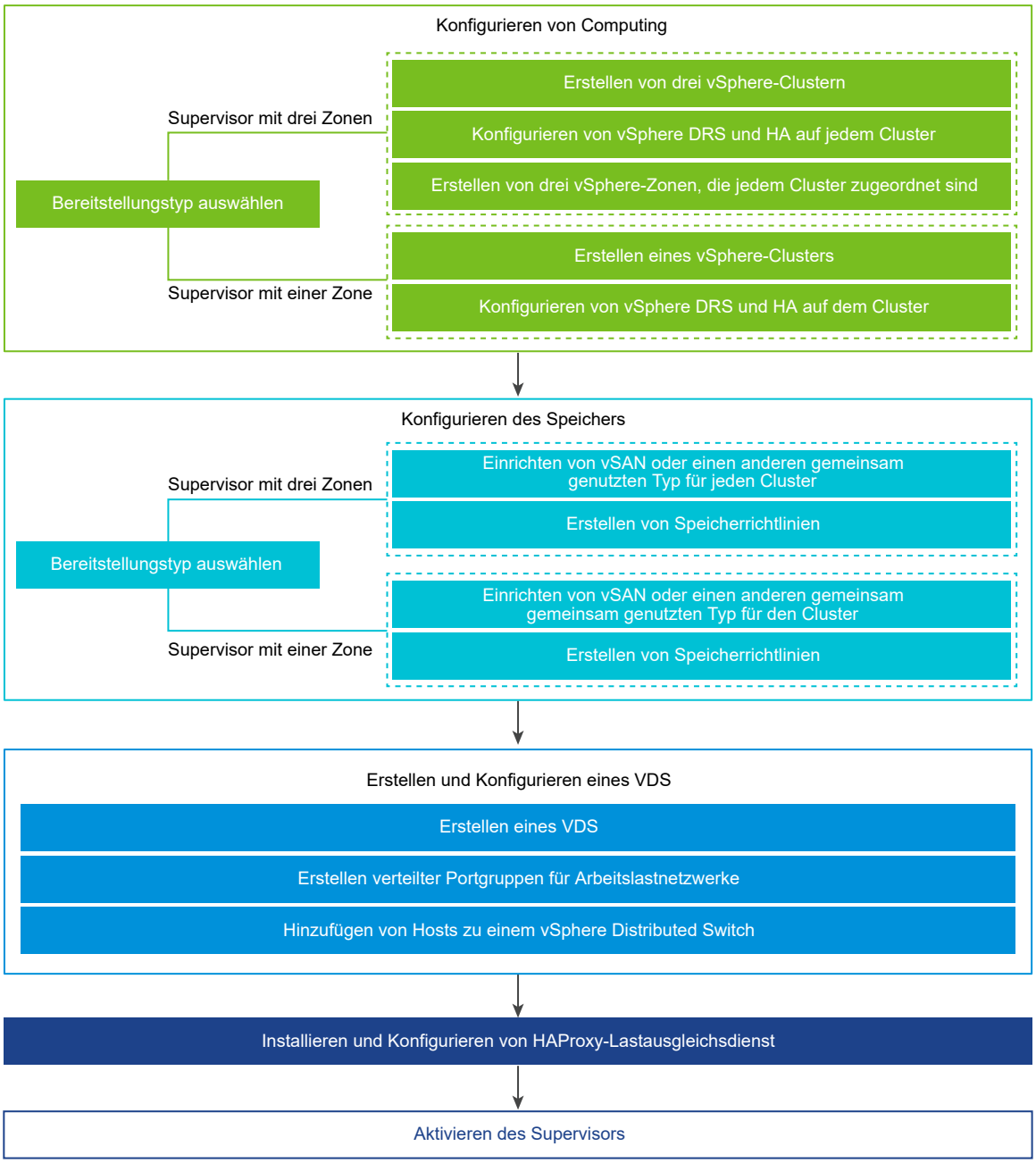
Abbildung 1-3. Workflow für die Bereitstellung eines Supervisors mit NSX als Netzwerk-Stack



Workflow für die Bereitstellung eines Supervisors mit VDS-Netzwerk und HAProxy-Lastausgleichsdienst

Als vSphere-Administrator können Sie einen Supervisor mit dem Netzwerk-Stack basierend auf VDS und dem HAProxy-Lastausgleichsdienst bereitstellen.

Abbildung 1-4. Workflow für die Bereitstellung von Supervisor mit VDS-Netzwerk und HAProxy



Lesen Sie als Nächstes die folgenden Themen:

- Voraussetzungen für die Konfiguration von vSphere IaaS control plane in vSphere-Cluster

Voraussetzungen für die Konfiguration von vSphere IaaS control plane in vSphere-Cluster

Überprüfen Sie die Voraussetzungen für die Aktivierung von vSphere IaaS control plane in Ihrer vSphere-Umgebung. Um containerbasierte Arbeitslasten nativ in vSphere auszuführen, aktivieren Sie als vSphere-Administrator die vSphere-Cluster als Supervisoren. Ein Supervisor verfügt über eine Kubernetes-Schicht, mit der Sie Kubernetes-Arbeitslasten auf vSphere ausführen können, indem Sie vSphere-Pods, Tanzu Kubernetes-Cluster und VMs bereitstellen.

Erstellen und Konfigurieren von vSphere-Clustern

Ein Supervisor kann auf einem oder drei vSphere-Clustern mit vSphere-Zonen ausgeführt werden. Jede vSphere-Zone wird einem vSphere-Cluster zugeordnet, und Sie können einen Supervisor für eine oder drei Zonen bereitstellen. Ein Supervisor mit drei Zonen bietet mehr Ressourcen für die Ausführung Ihrer Kubernetes-Arbeitslasten und verfügt über Hochverfügbarkeit auf vSphere-Clusterebene, die Ihre Arbeitslasten vor Clusterausfall schützt. Ein Supervisor für eine Zone verfügt über eine hochverfügbare Hostebene, die von vSphere HA zur Verfügung gestellt wird, und nutzt die Ressourcen eines einzigen Clusters für die Ausführung Ihrer Kubernetes-Arbeitslasten.

Hinweis Sobald Sie einen Supervisor auf einer vSphere Zone bereitgestellt haben, können Sie den Supervisor nicht mehr auf eine Bereitstellung mit drei Zonen ausweiten.

Jeder vSphere-Cluster, in dem Sie einen Supervisor bereitstellen möchten, muss die folgenden Anforderungen erfüllen:

- Erstellen und konfigurieren Sie einen vSphere-Cluster mit mindestens zwei ESXi-Hosts. Wenn Sie vSAN verwenden, muss der Cluster über mindestens drei oder vier Hosts verfügen, um eine optimale Leistung zu erzielen. Weitere Informationen finden Sie unter Erstellen und Konfigurieren von Clustern.
- Konfigurieren Sie den Cluster mit gemeinsam genutztem Speicher wie vSAN. Der freigegebene Speicher ist für vSphere HA, DRS und zum Speichern persistenter Container-Volumes erforderlich. Weitere Informationen finden Sie unter Erstellen eines vSAN-Clusters.
- Aktivieren des Clusters mit vSphere HA. Weitere Informationen finden Sie unter Erstellen und Verwenden von vSphere HA-Clustern.
- Aktivieren Sie den Cluster mit vSphere DRS im vollautomatischen Modus. Weitere Informationen finden Sie unter Erstellen eines DRS-Clusters.
- Überprüfen Sie, ob Ihr Benutzerkonto im vSphere-Cluster über die Berechtigung **Clusterweite Konfiguration ändern** verfügt, damit Sie den Supervisor bereitstellen können.
- Informationen zum Bereitstellen eines Supervisors für drei Zonen und zum Erstellen von drei vSphere-Zonen finden Sie unter Kapitel 3 Erstellen von vSphere-Zonen für eine Supervisor-Bereitstellung mit mehreren Zonen.

- Wenn Sie vSphere Lifecycle Manager-Images mit dem Supervisor verwenden möchten, wechseln Sie die vSphere Cluster, in denen Sie die **Arbeitslastverwaltung** aktivieren möchten, um vSphere Lifecycle Manager-Images zu verwenden, bevor Sie **Arbeitslastverwaltung** aktivieren. Sie können den Lebenszyklus eines Supervisors entweder mit vSphere Lifecycle Manager-Baselines oder mit vSphere Lifecycle Manager-Images verwalten. Sie können jedoch keinen Supervisor, der vSphere Lifecycle Manager-Baselines verwendet, in einen Supervisor konvertieren, der vSphere Lifecycle Manager-Images verwendet. Daher ist ein Wechsel der vSphere-Cluster zur Verwendung von vSphere Lifecycle Manager-Images erforderlich, bevor Sie **Arbeitslastverwaltung** aktivieren.

Erstellen von Speicherrichtlinien

Vor der Supervisor-Bereitstellung müssen Sie Speicherrichtlinien erstellen, die die Datenspeicherplatzierung der Supervisor-Steuerungsebenen-VMs bestimmen. Wenn der Supervisor vSphere-Pods unterstützt, benötigen Sie auch Speicherrichtlinien für Container und Images. Sie können Speicherrichtlinien erstellen, die verschiedenen Ebenen von Speicherdiensten zugeordnet sind.

Weitere Informationen finden Sie unter Kapitel 2 Erstellen von Speicherrichtlinien für vSphere IaaS control plane.

Auswählen und Konfigurieren des Netzwerk-Stacks

Um einen Supervisor bereitzustellen, müssen Sie den Netzwerk-Stack für die Verwendung mit diesem konfigurieren. Es stehen zwei Optionen zur Verfügung: NSX oder vSphere Distributed Switch (vDS)-Netzwerk mit einem Lastausgleichsdienst. Sie können den NSX Advanced Load Balancer oder den HAProxy-Lastausgleichsdienst konfigurieren.

So verwenden Sie das NSX-Netzwerk für den Supervisor:

- Überprüfen Sie die Systemanforderungen und Topologien für das NSX-Netzwerk. Weitere Informationen finden Sie unter Anforderungen zum Aktivieren eines Supervisors für drei Zonen mit NSX und Anforderungen zum Einrichten eines Supervisors für einen einzelnen Cluster mit NSX in *Konzepte und Planung der vSphere IaaS-Steuerungsebene*.
- Installieren und Konfigurieren von NSX für vSphere IaaS control plane Weitere Informationen hierzu finden Sie unter Installieren und Konfigurieren von NSX für vSphere IaaS control plane.

So verwenden Sie das vDS-Netzwerk mit dem NSX Advanced Load Balancer für den Supervisor:

- Prüfen Sie die NSX Advanced Load Balancer-Anforderungen. Weitere Informationen finden Sie unter Anforderungen für einen Drei-Zonen-Supervisor mit NSX Advanced Load Balancer und Anforderungen für die Aktivierung eines Einzelcluster-Supervisors mit NSX Advanced Load Balancer in *Konzepte und Planung der vSphere IaaS-Steuerungsebene*.
- Erstellen Sie einen vSphere Distributed Switch (vDS) und fügen Sie alle ESXi-Hosts aus dem Cluster zum vDS hinzu und erstellen Sie Portgruppen für Arbeitslastnetzwerke. Weitere Informationen hierzu finden Sie unter Erstellen eines vSphere Distributed Switch für einen Supervisor zwecks Verwendung mit NSX Advanced Load Balancer.

- Stellen Sie den NSX Advanced Load Balancer bereit und konfigurieren Sie ihn. Weitere Informationen hierzu finden Sie unter Bereitstellen des NSX Advanced Load Balancer-Controllers.

Hinweis vSphere IaaS control plane unterstützt den NSX Advanced Load Balancer mit vSphere 7 U2 und höher.

So verwenden Sie das vDS-Netzwerk mit HAProxy-Lastausgleich für den Supervisor:

- Überprüfen Sie die Systemanforderungen und Netzwerktopologien für vSphere-Netzwerke mit einem HAProxy-Lastausgleichsdienst. Weitere Informationen finden Sie unter Anforderungen zum Aktivieren eines Supervisors mit drei Zonen mit HAProxy-Lastausgleichsdienst und Anforderungen zum Aktivieren eines Supervisors mit einem einzelnen Cluster mit VDS-Netzwerk und HAProxy-Lastausgleichsdienst *Konzepte und Planung der vSphere IaaS-Steuerungsebene*.
- Erstellen Sie einen vSphere Distributed Switch (VDS) und fügen Sie alle ESXi-Hosts aus dem Cluster zum vDS hinzu und erstellen Sie Portgruppen für Arbeitslastnetzwerke. Weitere Informationen hierzu finden Sie unter Erstellen eines vSphere Distributed Switch für einen Supervisor für die Verwendung mit dem HAProxy-Lastausgleichsdienst.
- Installieren und konfigurieren Sie die HAProxy-Lastausgleichsdienst-Instanz, die zu dem vDS geroutet werden kann, der von den vSphere-Clustern, in denen Sie den Supervisor bereitstellen, mit den Hosts verbunden ist. Der HAProxy-Lastausgleichsdienst unterstützt die Netzwerkkonnektivität zu Arbeitslasten aus Clientnetzwerken und zum Lastausgleich des Datenverkehrs zwischen Tanzu Kubernetes-Clustern. Weitere Informationen hierzu finden Sie unter Installieren und Konfigurieren des HAProxy-Lastausgleichsdiensts.

Hinweis vSphere IaaS control plane unterstützt den HAProxy-Lastausgleichsdienst mit vSphere 7 U1 und höher.

Erstellen von Speicherrichtlinien für vSphere IaaS control plane

2

Erstellen Sie vor dem Aktivieren von vSphere IaaS control plane Speicherrichtlinien, die im Supervisor und den Namespaces verwendet werden sollen. Die Richtlinien stellen Datenspeicher dar und steuern die Speicherplatzierung von Komponenten und Objekten wie Supervisor-Steuerungsebenen-VMs, flüchtigen vSphere Pod-Festplatten und Container-Images. Möglicherweise benötigen Sie auch Richtlinien für die Speicherplatzierung dauerhafter Volumes und VM-Inhaltsbibliotheken. Falls Sie Tanzu Kubernetes-Cluster verwenden, bestimmen die Speicherrichtlinien auch, wie die Tanzu Kubernetes-Clusterknoten bereitgestellt werden.

Je nach vSphere-Speicherumgebung und den Anforderungen von DevOps können Sie mehrere Speicherrichtlinien für verschiedene Speicherklassen erstellen. Wenn Ihre vSphere-Speicherumgebung beispielsweise über drei Klassen von Datenspeichern (Bronze, Silber und Gold) verfügt, können Sie Speicherrichtlinien für alle Datenspeichertypen erstellen.

Wenn Sie einen Supervisor aktivieren und Namespaces einrichten, können Sie verschiedene Speicherrichtlinien zuweisen, die von verschiedenen Objekten, Komponenten und Arbeitslasten verwendet werden sollen.

Hinweis Speicherrichtlinien, die Sie für einen Supervisor oder für einen Namespace in einem Supervisor mit einer Zone erstellen, müssen nicht topologiefähig sein. Aktivieren Sie die Verbrauchsdomäne für diese Richtlinien nicht.

Speicherrichtlinien, die Sie für einen Namespace in einem Supervisor mit drei Zonen erstellen, müssen topologiefähig sein und die Verbrauchsdomäne in Schritt 4b aktiviert haben. Der Namespace mit drei Zonen verhindert, dass Sie Speicherrichtlinien zuweisen können, die nicht topologiefähig sind.

Im folgenden Beispiel wird die Speicherrichtlinie für den als „Gold“ gekennzeichneten Datenspeicher erstellt.

Voraussetzungen

- Informationen zu Speicherrichtlinien in vSphere IaaS control plane finden Sie unter Informationen zu Speicherrichtlinien in *Konzepte und Planung der vSphere IaaS-Steuerungsebene*.

- Wenn Sie die vSAN Data Persistence-Plattform für dauerhaften Speicher verwenden und benutzerdefinierte Speicherrichtlinien für vSAN Direct- oder vSAN SNA-Datenspeicher erstellen müssen, finden Sie weitere Informationen unter Erstellen von benutzerdefinierten Speicherrichtlinien für die vSAN-Datenpersistenzplattform in *Dienste und Arbeitslasten der vSphere IaaS-Steuerungsebene*.
- Wenn Sie topologiefähige Speicherrichtlinien für persistenten Speicher in einem Supervisor mit drei Zonen erstellen müssen, machen Sie sich mit den Richtlinien unter Verwenden von persistentem Speicher auf einem Supervisor mit drei Zonen in *Dienste und Arbeitslasten der vSphere IaaS-Steuerungsebene* vertraut.
- Stellen Sie sicher, dass der Datenspeicher, auf den in der Speicherrichtlinie verwiesen wird, von allen ESXi-Hosts im Cluster gemeinsam genutzt wird. Alle gemeinsam genutzten Datenspeicher in Ihrer Umgebung werden unterstützt, einschließlich VMFS, NFS, vSAN oder vVols.
- Erforderliche Rechte: **VM-Speicherrichtlinien. Aktualisieren** und **VM-Speicherrichtlinien. Anzeigen**.

Verfahren

1 Fügen Sie Tags zum Datenspeicher hinzu.

   a Klicken Sie mit der rechten Maustaste auf den zu kennzeichnenden Datenspeicher und wählen Sie **Tags und benutzerdefinierte Attribute > Tag zuweisen** aus.

   b Klicken Sie auf **Tag hinzufügen** und geben Sie die Eigenschaften des Tags an.

Eigenschaft	Beschreibung
Name	Geben Sie den Namen des Datenspeicher-Tags an, wie z. B. **`Gold`**.
Beschreibung	Fügen Sie die Beschreibung des Tags hinzu. Beispielsweise **`Datenspeicher für Kubernetes-Objekte`**.
Kategorie	Wählen Sie eine vorhandene Kategorie aus oder erstellen Sie eine neue Kategorie. Beispielsweise **`Speicher für Kubernetes`**.

2 Öffnen Sie im vSphere Client den Assistenten **VM-Speicherrichtlinie erstellen**.

   a Klicken Sie auf **Menü > Richtlinien und Profile**.

   b Klicken Sie unter **Richtlinien und Profile** auf **VM-Speicherrichtlinien**.

   c Klicken Sie auf **VM-Speicherrichtlinie erstellen**.

3 Geben Sie den Richtliniennamen und eine Beschreibung ein.

Option	Aktion
vCenter Server	Wählen Sie die vCenter Server-Instanz aus.
Name	Geben Sie den Namen der Speicherrichtlinie ein, z. B. **`goldsp`**. **Hinweis** Wenn vSphere IaaS control plane zu Namespaces zugewiesene Speicherrichtlinien in Kubernetes-Speicherklassen umwandelt, werden alle Großbuchstaben in Kleinbuchstaben geändert und Leerzeichen durch Bindestriche (-) ersetzt. Verwenden Sie der Eindeutigkeit halber Kleinbuchstaben und keine Leerzeichen in den Namen der VM-Speicherrichtlinien.
Beschreibung	Geben Sie die Beschreibung der Speicherrichtlinie ein.

4 Wählen Sie auf der Seite **Richtlinienstruktur** die folgenden Optionen aus und klicken Sie auf **Weiter**.

a Aktivieren Sie unter **Datenspeicherspezifische Regeln** „Tag-basierte Platzierungsregeln“.

b Zum Erstellen einer topologiefähigen Richtlinie wählen Sie unter **Speichertopologie** die Option **Verbrauchsdomäne aktivieren** aus.

Dieser Schritt ist nur erforderlich, wenn Sie topologiefähige Richtlinien erstellen, die für persistenten Speicher auf einem Namespace in einem Supervisor mit drei Zonen verwendet werden sollen.

5 Erstellen Sie auf der Seite **Tag-basierte Platzierung** die Tag-Regeln.

Wählen Sie die Optionen mithilfe des folgenden Beispiels aus.

Option	Beschreibung
Tag-Kategorie	Wählen Sie im Dropdown-Menü die Kategorie des Tags aus, wie z. B. **Speicher für Kubernetes**.
Nutzungsoption	Wählen Sie **Speicher verwenden, die mit folgenden Tags versehen sind** aus.
Tags	Klicken Sie auf **Tags durchsuchen** und wählen Sie das Datenspeicher-Tag aus, wie z. B. **Gold**.

6 Wenn Sie **Speichertopologie** aktiviert haben, geben Sie auf der Seite **Verbrauchsdomäne** den Typ der Speichertopologie an.

Option	Bezeichnung
Zonal	Der Datenspeicher wird von allen Hosts in einer einzelnen Zone gemeinsam genutzt.

7 Überprüfen Sie auf der Seite **Speicherkompatibilität** die Liste der Datenspeicher, die mit dieser Richtlinie übereinstimmen.

In diesem Beispiel wird nur der Datenspeicher angezeigt, der als „Gold“ markiert ist.

8 Überprüfen Sie auf der Seite **Überprüfen und beenden** die Einstellungen der Speicherrichtlinie und klicken Sie auf **Beenden**.

Ergebnisse

Die neue Speicherrichtlinie für den als „Gold“ gekennzeichneten Datenspeicher wird in der Liste der vorhandenen Speicherrichtlinien angezeigt.

Nächste Schritte

Nach dem Erstellen von Speicherrichtlinien kann ein vSphere-Administrator die folgenden Aufgaben durchführen:

- Weisen Sie dem Supervisor die Speicherrichtlinien zu. Mit den im Supervisor konfigurierten Speicherrichtlinien wird sichergestellt, dass die VMs der Steuerungsebene, die flüchtigen Pod-Festplatten und die Container-Images auf den Datenspeichern platziert werden, die von den Richtlinien dargestellt werden.
- Weisen Sie dem vSphere-Namespace die Speicherrichtlinien zu. Mit den für den Namespace sichtbaren Speicherrichtlinien wird festgelegt, auf welche Datenspeicher der Namespace zugreifen und welche Datenspeicher er für dauerhafte Volumes verwenden kann. Die Speicherrichtlinien werden als übereinstimmende Kubernetes-Speicherklassen im Namespace angezeigt. Sie werden auch an den Tanzu Kubernetes-Cluster in diesem Namespace weitergegeben. DevOps-Ingenieure können die Speicherklassen in ihren Anspruchsspezifikationen für dauerhafte Volumes verwenden. Informationen hierzu finden Sie unter Erstellen und Konfigurieren eines vSphere-Namespace.

Erstellen von vSphere-Zonen für eine Supervisor-Bereitstellung mit mehreren Zonen

3

Erfahren Sie, wie Sie vSphere-Zonen erstellen, die Sie verwenden können, um Hochverfügbarkeit auf Clusterebene für Ihre Kubernetes-Arbeitslasten bereitzustellen, die auf einem Supervisor ausgeführt werden. Um Hochverfügbarkeit auf Clusterebene für Ihre Kubernetes-Arbeitslasten bereitzustellen, stellen Sie den Supervisor in drei vSphere-Zonen bereit. Jede vSphere-Zone ist einem vSphere-Cluster zugeordnet, der über mindestens 2 Hosts verfügt.

Voraussetzungen

- Erstellen Sie drei vSphere Cluster mit mindestens 3 Hosts in jeder Zone. Für Speicher mit vSAN muss der Cluster über 4 Hosts verfügen.
- Konfigurieren Sie Speicher mit vSAN oder einer anderen Lösung für gemeinsam genutzten Speicher für jeden Cluster.
- Aktivieren Sie vSphere-HA und vSphere-DRS im voll- oder teilautomatisierten Modus.
- Konfigurieren Sie das Netzwerk mit NSX- oder vSphere Distributed Switch-Netzwerken (vDS) für die Cluster.

Verfahren

1. Navigieren Sie in vSphere Client zu vCenter Server.
2. Wählen Sie **Konfigurieren** und anschließend **vSphere-Zonen**.
3. Klicken Sie auf **Neue vSphere-Zone hinzufügen**.
4. Benennen Sie die Zone, z. B. **`zone1`**, und fügen Sie eine optionale Beschreibung hinzu.
5. Wählen Sie einen vSphere-Cluster aus, den Sie der Zone hinzufügen möchten, und klicken Sie auf **Beenden**.
6. Wiederholen Sie die Schritte zum Erstellen drei vSphere-Zonen.

Nächste Schritte

- - Konfigurieren Sie einen Netzwerk-Stack für die Verwendung mit dem Supervisor. Siehe Kapitel 4 Netzwerk für vSphere IaaS control plane.
  - Aktivieren Sie den Supervisor in den von Ihnen erstellten drei vSphere-Zonen. Siehe Kapitel 5 Bereitstellen eines Supervisor für drei Zonen .

Wenn Sie Änderungen an einer vSphere-Zone vornehmen müssen, können Sie diese vor Bereitstellung des Supervisors durchführen.

Verwalten von vSphere-Zonen

Wenn Sie Änderungen an einer vSphere-Zone vornehmen müssen, müssen Sie dies tun, bevor Sie einen Supervisor in der Zone bereitstellen. Sie können den zugehörigen Cluster ändern oder die Zone löschen. Beim Löschen einer vSphere-Zone wird der zugehörige Cluster entfernt und anschließend die Zone aus vCenter Server gelöscht.

Entfernen eines Clusters aus einer vSphere-Zone

Um einen Cluster aus einer vSphere-Zone zu entfernen, klicken Sie auf die drei Punkte (...) auf der Zonenkarte und wählen Sie **Cluster entfernen** aus. Der Cluster wird aus der Zone entfernt, und Sie können einen anderen hinzufügen.

Hinweis Sie können einen Cluster nicht aus einer vSphere-Zone entfernen, wenn in dieser Zone bereits ein Supervisor aktiviert ist.

Löschen einer vSphere-Zone

Um eine vSphere-Zone zu löschen, klicken Sie auf die drei Punkte (...) auf der Zonenkarte und wählen Sie **Zone löschen** aus.

Hinweis Sie können eine vSphere-Zone nicht löschen, wenn in dieser Zone bereits ein Supervisor aktiviert ist.

Netzwerk für vSphere IaaS control plane

4

Ein Supervisor kann entweder den vSphere-Netzwerk-Stack oder VMware NSX® verwenden, um Kubernetes-Steuerungsebenen-VMs, Diensten und Arbeitslasten Konnektivität bereitzustellen. Das für Tanzu Kubernetes-Cluster verwendete Netzwerk, das vom Tanzu Kubernetes Grid bereitgestellt wird, ist eine Kombination aus dem Fabric, das der vSphere IaaS control plane-Infrastruktur zugrunde liegt, und der Open Source-Software, die Netzwerke für Cluster-Pods, Dienste und Ingress bereitstellt.

Lesen Sie als Nächstes die folgenden Themen:

- Supervisor-Netzwerk
- Installieren und Konfigurieren von NSX für vSphere IaaS control plane
- Installieren und Konfigurieren von NSX und NSX Advanced Load Balancer
- Installieren und Konfigurieren von NSX Advanced Load Balancer
- Installieren und Konfigurieren des HAProxy-Lastausgleichsdiensts

Supervisor-Netzwerk

In einer vSphere IaaS control plane-Umgebung kann ein Supervisor entweder den vSphere-Netzwerk-Stack oder NSX verwenden, um Konnektivität für Supervisor-Steuerungsebenen-VMs, Dienste und Arbeitslasten bereitzustellen.

Wenn ein Supervisor mit dem vSphere-Netzwerk-Stack konfiguriert ist, werden alle Hosts aus dem Supervisor mit einem vDS verbunden, der Arbeitslasten und Supervisor-Steuerungsebenen-VMs Konnektivität bereitstellt. Ein Supervisor, der den vSphere-Netzwerk-Stack verwendet, benötigt einen Lastausgleichsdienst im vCenter Server-Verwaltungsnetzwerk, um DevOps-Benutzern und externen Diensten Konnektivität bereitzustellen.

Ein Supervisor, der mit NSX konfiguriert ist, verwendet die softwarebasierten Netzwerke der Lösung sowie einen NSX Edge-Lastausgleichsdienst oder den NSX Advanced Load Balancer, der externen Diensten und DevOps-Benutzern Konnektivität bereitstellt. Sie können den NSX Advanced Load Balancer auf NSX konfigurieren, wenn Ihre Umgebung die folgenden Bedingungen erfüllt:

- NSX-Version ist 4.1.1 oder höher.
- Die NSX Advanced Load Balancer Version ist 22.1.4 oder höher mit der Enterprise-Lizenz.

- Der NSX Advanced Load Balancer Controller, den Sie konfigurieren möchten, ist auf NSX registriert.
- Ein NSX-Lastausgleichsdienst ist auf dem Supervisor noch nicht konfiguriert.

Supervisor-Netzwerk mit VDS

In einem Supervisor, der von VDS als Netzwerk-Stack gestützt wird, müssen alle Hosts aus den vSphere-Clustern, die den Supervisor unterstützen, mit demselben VDS verbunden sein. Der Supervisor verwendet verteilte Portgruppen als Arbeitslastnetzwerke für Kubernetes-Arbeitslasten und Datenverkehr auf Steuerungsebene. Sie weisen Arbeitslastnetzwerke Namespaces im Supervisor zu.

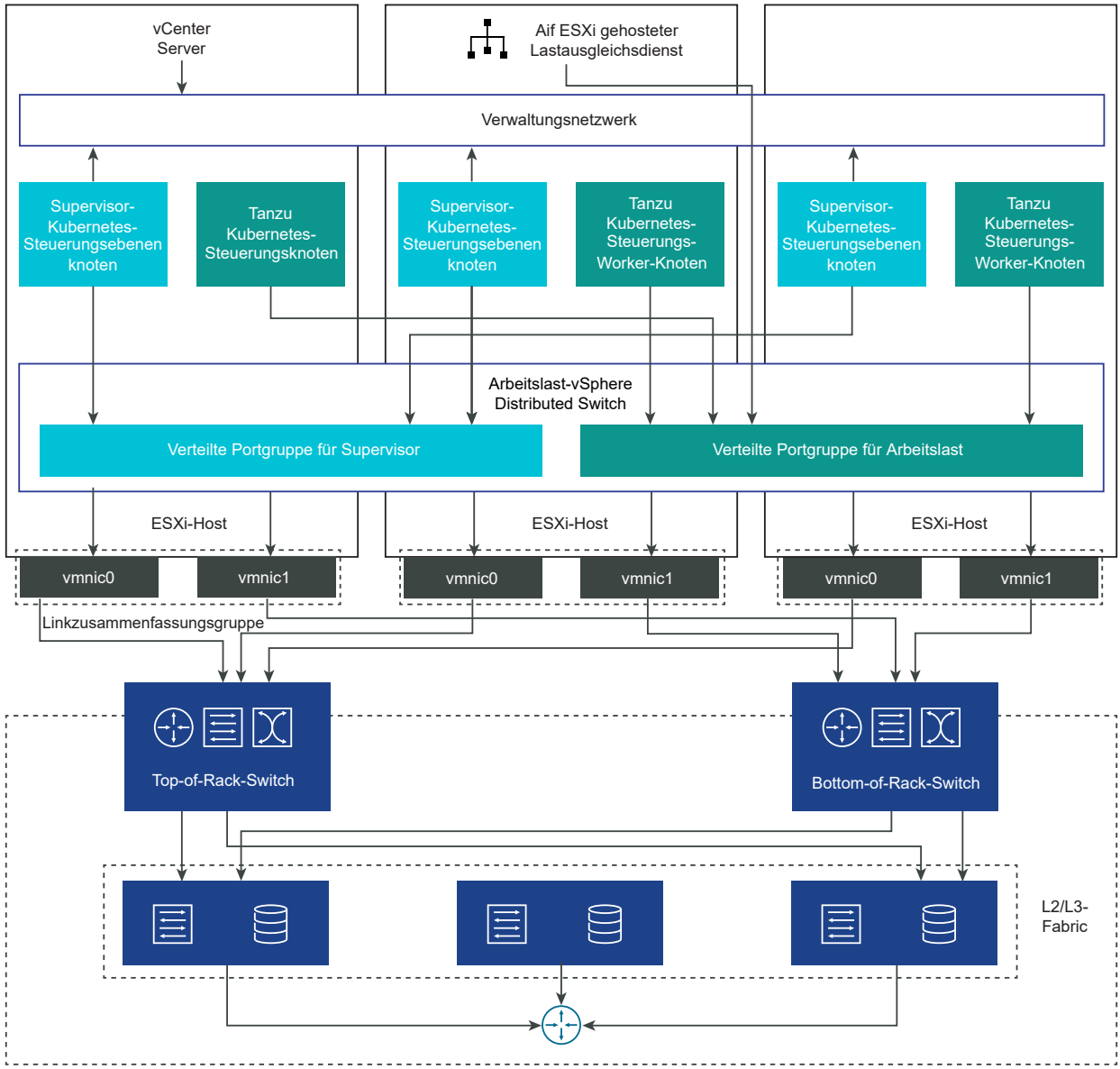
Abhängig von der für den Supervisor implementierten Topologie können Sie eine oder mehrere verteilte Portgruppen als Arbeitslastnetzwerke verwenden. Das Netzwerk, das den Supervisor-Steuerungsebenen-VMs Konnektivität bereitstellt, wird als primäres Arbeitslastnetzwerk bezeichnet. Sie können dieses Netzwerk allen Namespaces auf dem Supervisor zuweisen. Sie können aber auch verschiedene Netzwerke für jeden Namespace verwenden. Die Tanzu Kubernetes Grid-Cluster stellen eine Verbindung zu dem Arbeitslastnetzwerk her, das dem Namespace zugewiesen wird, in dem sich der Cluster befindet.

Ein von einem VDS gestützter Supervisor verwendet einen Lastausgleichsdienst, um DevOps-Benutzern und externen Diensten Konnektivität bereitzustellen. Sie können die -NSX Advanced Load Balancer oder den HAProxy-Lastausgleichsdienst verwenden.

Weitere Informationen finden Sie unter Installieren und Konfigurieren von NSX Advanced Load Balancer und Installieren und Konfigurieren von HAProxy-Lastausgleichsdienst.

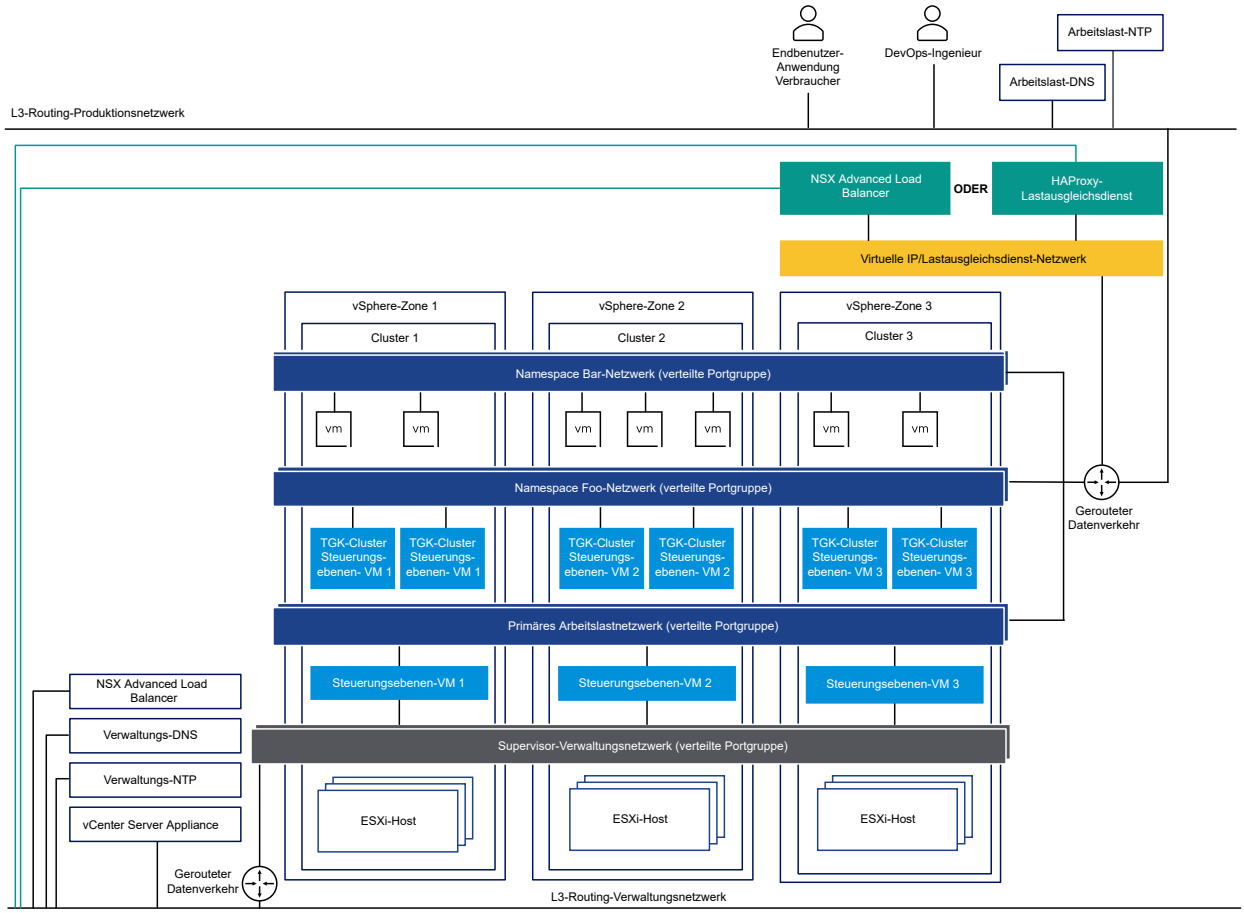
In einer Supervisor-Einrichtung mit einem Cluster wird Supervisor nur von einem vSphere-Cluster gestützt. Alle Hosts aus dem Cluster müssen mit einem VDS verbunden sein.

Abbildung 4-1. Supervisor-Netzwerk mit einem Cluster und VDS



In einem Supervisor für drei Zonen stellen Sie Supervisor auf drei vSphere-Zonen bereit, die jeweils einem vSphere-Cluster zugeordnet sind. Alle Hosts aus diesen vSphere-Clustern müssen mit demselben VDS verbunden sein. Alle physischen Server müssen mit einem L2-Gerät verbunden sein. Arbeitslastnetzwerke, die Sie für den Namespace konfigurieren, erstrecken sich über alle drei vSphere-Zonen.

Abbildung 4-2. Supervisor-Netzwerk für drei Zonen und VDS



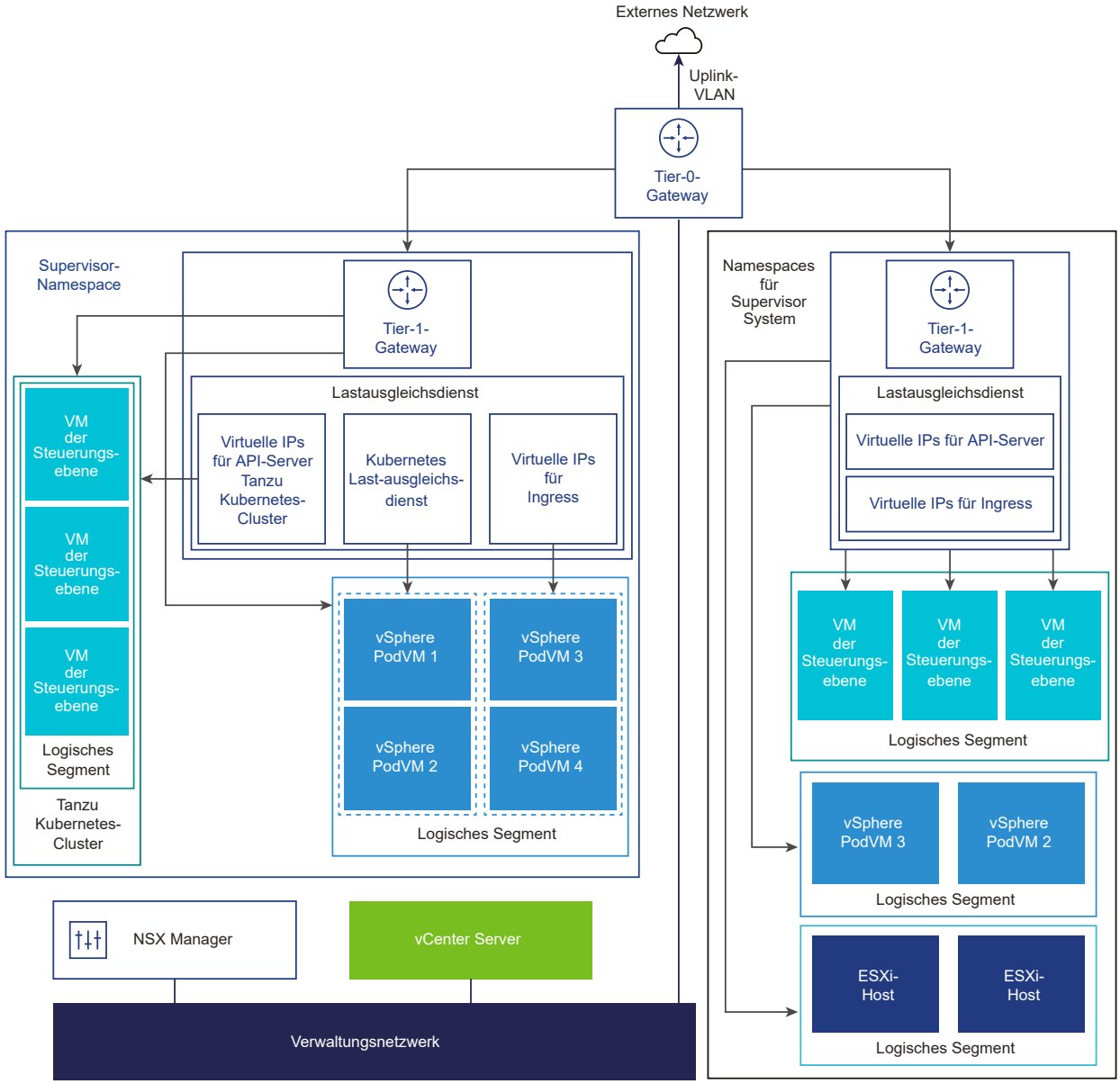
Supervisor-Netzwerk mit NSX

NSX bietet Netzwerkkonnektivität zu den Objekten innerhalb des Supervisors und externen Netzwerken. Die Konnektivität mit den ESXi-Hosts, die den Cluster umfassen, wird von den standardmäßigen vSphere-Netzwerken verarbeitet.

Sie können das Supervisor-Netzwerk auch manuell konfigurieren, indem Sie eine vorhandene NSX-Bereitstellung verwenden oder eine neue NSX-Instanz bereitstellen.

Weitere Informationen finden Sie unter Installieren und Konfigurieren von NSX for vSphere IaaS control plane.

Abbildung 4-3. Supervisor-Netzwerk mit NSX



- NSX Container Plugin (NCP) bietet Integration zwischen NSX und Kubernetes. Die Hauptkomponente von NCP wird in einem Container ausgeführt und kommuniziert mit NSX Manager und mit der Kubernetes-Steuerungsebene. NCP überwacht Änderungen an Containern und anderen Ressourcen und verwaltet Netzwerkressourcen wie logische Ports, Segmente, Router und Sicherheitsgruppen für die Container durch Aufrufen der NSX API.

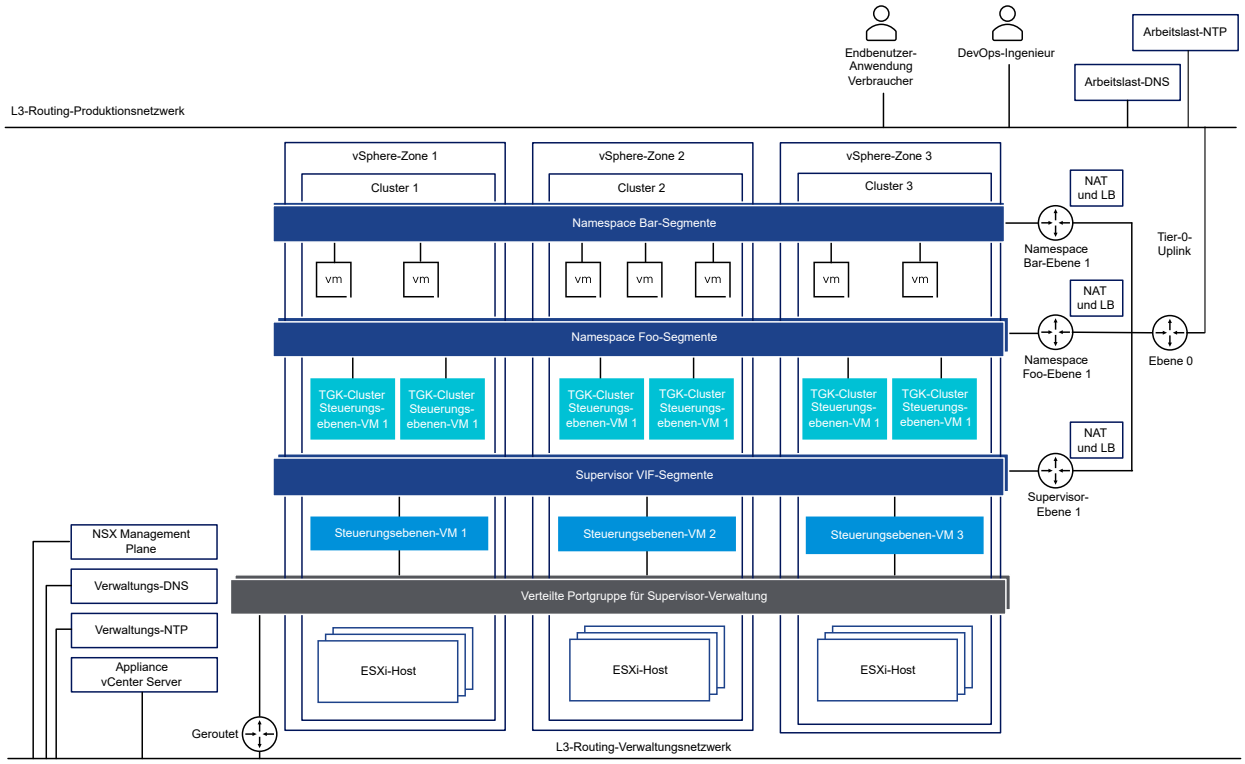
  Das NCP erstellt standardmäßig ein freigegebenes Tier-1-Gateway für System-Namespaces und ein Tier-1-Gateway und einen Lastausgleichsdienst für jeden Namespace. Das Tier-1-Gateway ist mit dem Tier-0-Gateway und einem Standardsegment verbunden.

System-Namespaces sind Namespaces, die von den Kernkomponenten verwendet werden, die für das Funktionieren des Supervisors und der Tanzu Kubernetes Grid-Cluster von wesentlicher Bedeutung sind. Die freigegebenen Netzwerkressourcen, die das Tier-1-Gateway, den Lastausgleichsdienst und die SNAT-IP enthalten, sind in einem System-Namespace gruppiert.

- NSX Edge bietet Konnektivität von externen Netzwerken zu Supervisor-Objekten. Der NSX Edge-Cluster verfügt über einen Lastausgleichsdienst, der Redundanz für die Kubernetes-API-Server auf den Supervisor-Steuerungsebenen-VMs sowie für alle Anwendungen bietet, die veröffentlicht werden müssen und auf die ein Zugriff von außerhalb des Supervisors möglich sein muss.
- Ein Tier-0-Gateway ist mit dem NSX Edge-Cluster verknüpft, um das Routing zum externen Netzwerk bereitzustellen. Die Uplink-Schnittstelle verwendet entweder das dynamische Routing-Protokoll, BGP oder statisches Routing.
- Jeder vSphere-Namespace verfügt über ein separates Netzwerk und eine Reihe von Netzwerkressourcen, die von Anwendungen innerhalb des Namespace gemeinsam genutzt werden, wie z. B. das Tier-1-Gateway, den Lastausgleichsdienst und die SNAT-IP-Adresse.
- Arbeitslasten, die in vSphere-Pods, regulären VMs oder Tanzu Kubernetes Grid-Clustern ausgeführt werden, die sich im selben Namespace befinden, nutzen dieselbe SNAT-IP für die Nord-Süd-Konnektivität.
- Arbeitslasten, die in vSphere-Pods oder Tanzu Kubernetes Grid-Clustern ausgeführt werden, haben dieselbe Isolationsregel, die von der Standard-Firewall implementiert wird.
- Eine eigene SNAT-IP ist nicht für jeden Kubernetes-Namespace erforderlich. Die Ost-West-Konnektivität zwischen Namespaces ist kein SNAT.
- Die Segmente für die einzelnen Namespaces befinden sich auf dem im Standardmodus funktionierenden VDS, der dem NSX Edge-Cluster zugeordnet ist. Das Segment stellt dem Supervisor ein Overlay-Netzwerk zur Verfügung.
- Supervisoren verfügen über getrennte Segmente innerhalb des gemeinsam genutzten Tier-1-Gateways. Für jeden Tanzu Kubernetes Grid-Cluster werden Segmente innerhalb des Tier-1-Gateways des Namespace definiert.
- Die Spherelet-Prozesse auf den einzelnen ESXi-Hosts kommunizieren mit vCenter Server über eine Schnittstelle im Verwaltungsnetzwerk.

In einer Supervisor-Konfiguration für drei Zonen mit NSX als Netzwerk-Stack müssen alle Hosts aus allen drei vSphere-Clustern, die den Zonen zugeordnet sind, mit demselben VDS verbunden sein und an derselben NSX-Overlay-Transportzone teilnehmen. Alle Hosts müssen mit demselben physischen L2-Gerät verbunden sein.

Abbildung 4-4. Supervisor-Netzwerk für drei Zonen mit NSX



Supervisor-Netzwerk mit NSX und NSX Advanced Load Balancer

NSX bietet Netzwerkkonnektivität zu den Objekten innerhalb des Supervisors und externen Netzwerken. Ein mit NSX konfigurierter Supervisor kann den NSX Edge oder den NSX Advanced Load Balancer verwenden.

Zu den Komponenten des NSX Advanced Load Balancer gehören der NSX Advanced Load Balancer Controller-Cluster, Dienst-Engines (Datenebenen-) VMs und der Avi Kubernetes Operator (AKO).

Der NSX Advanced Load Balancer Controller interagiert mit dem vCenter Server, um den Lastausgleich für die Tanzu Kubernetes Grid-Cluster zu automatisieren. Er ist für die Bereitstellung von Dienst-Engines, die Koordination von Ressourcen anhand von Dienst-Engines sowie die Zusammenfassung von Dienst-Engine-Metriken und -Protokollen zuständig. Der Controller bietet eine Web-Schnittstelle, Befehlszeilenschnittstelle und API für den Benutzerbetrieb und die programmgesteuerte Integration. Nachdem Sie die Controller-VM bereitgestellt und konfiguriert haben, können Sie einen Controller-Cluster bereitstellen, um den Steuerungsebenen-Cluster für HA einzurichten.

Die Dienst-Engine ist die virtuelle Maschine der Datenebene. Eine Dienst-Engine führt einen oder mehrere virtuelle Dienste aus. Eine Dienst-Engine wird vom NSX Advanced Load Balancer Controller verwaltet. Der Controller stellt Dienst-Engines für das Hosten virtueller Dienste zur Verfügung.

Die Dienst-Engines verfügen über zwei Arten von Netzwerkschnittstellen:

- Die erste Netzwerkschnittstelle, `vnic0` der VM, wird mit dem Verwaltungsnetzwerk verbunden, wo sie eine Verbindung zum NSX Advanced Load Balancer Controller herstellen kann.
- Die restlichen Schnittstellen, `vnic1 – 8`, verbinden sich mit dem Datennetzwerk, in dem virtuelle Dienste ausgeführt werden.

Die Dienst-Engine-Schnittstellen stellen automatisch eine Verbindung mit den richtigen vDS-Portgruppen her. Jede Dienst-Engine kann bis zu 1.000 virtuelle Dienste unterstützen.

Ein virtueller Dienst stellt Ebene-4- und Ebene-7-Lastausgleichsdienste für Tanzu Kubernetes Grid-Clusterarbeitslasten zur Verfügung. Ein virtueller Dienst ist mit einer virtuellen IP und mehreren Ports konfiguriert. Wenn ein virtueller Dienst bereitgestellt wird, wählt der Controller automatisch einen ESX-Server aus, startet eine Dienst-Engine und verbindet sie mit den richtigen Netzwerken (Portgruppen).

Die erste Dienst-Engine wird erst erstellt, nachdem der erste virtuelle Dienst konfiguriert wurde. Alle nachfolgenden virtuellen Dienste, die konfiguriert werden, verwenden die vorhandene Dienst-Engine.

Jeder virtuelle Server macht einen Load Balancer der Ebene 4 mit einer eindeutigen IP-Adresse des Typs Load Balancer für einen Tanzu Kubernetes Grid verfügbar. Die IP-Adresse, die jedem virtuellen Server zugewiesen ist, wird aus dem IP-Adressblock ausgewählt, der dem Controller bei der Konfiguration zugewiesen wurde.

Der Avi-Kubernetes-Operator (AKO) überwacht Kubernetes-Ressourcen und kommuniziert mit dem NSX Advanced Load Balancer Controller, um die entsprechenden Lastausgleichsressourcen anzufordern. Der Avi-Kubernetes-Operator wird im Rahmen des Aktivierungsprozesses auf den Supervisoren installiert.

Weitere Informationen finden Sie unter Installieren und Konfigurieren von NSX und NSX Advanced Load Balancer.

Abbildung 4-5. Supervisor-Netzwerk mit NSX und NSX Advanced Load Balancer Controller

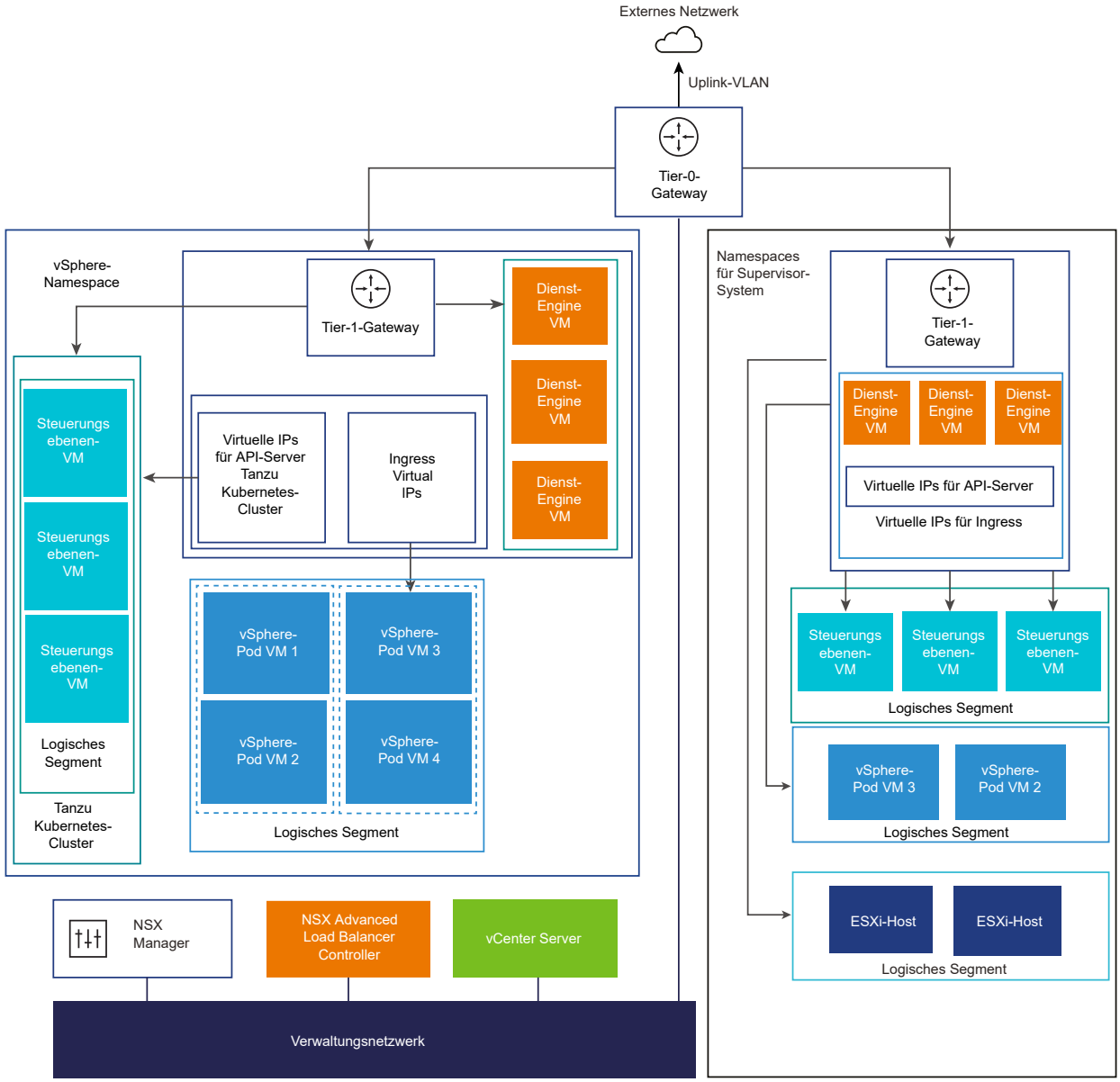
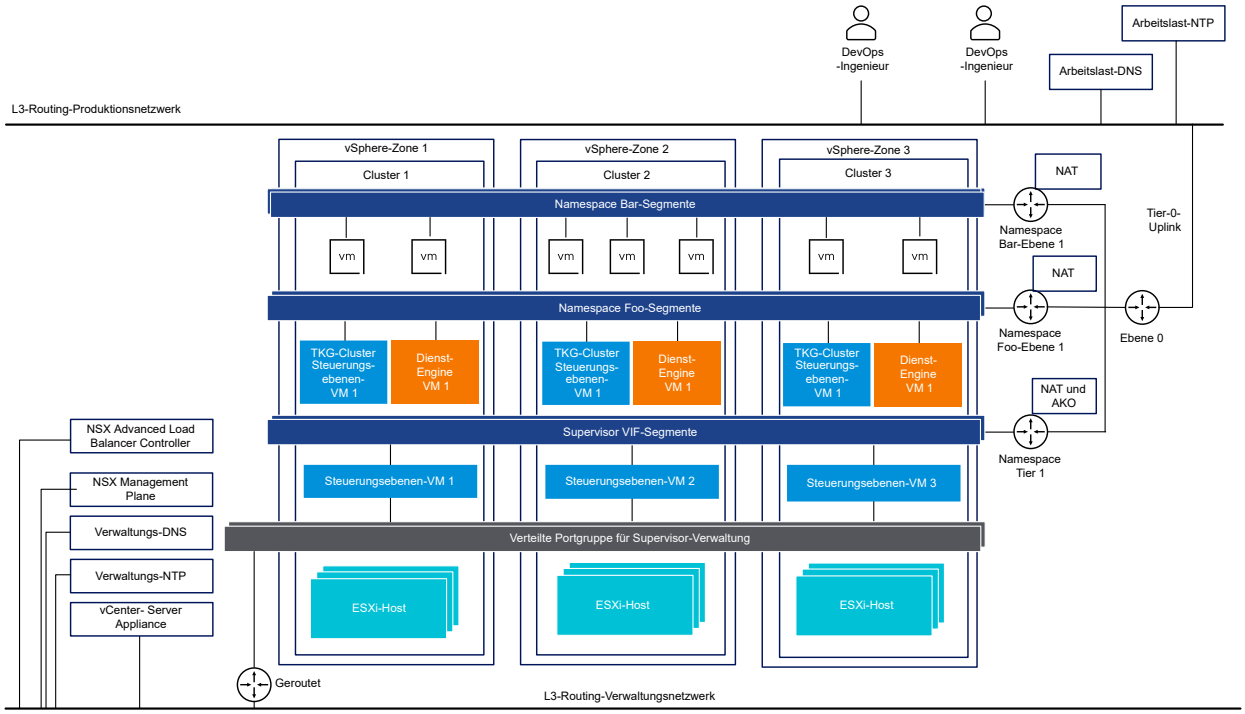


Abbildung 4-6. Supervisor-Netzwerk für drei Zonen mit NSX und NSX Advanced Load Balancer Controller



Wichtig Wenn Sie den NSX Advanced Load Balancer Controller in einer NSX-Bereitstellung konfigurieren, sollten Sie Folgendes berücksichtigen:

- Sie können den NSX Advanced Load Balancer Controller nicht in einer vCenter Server-Bereitstellung im erweiterten verknüpften Modus bereitstellen. Sie können den NSX Advanced Load Balancer Controller nur in einer Bereitstellung mit einem einzelnen vCenter Server bereitstellen. Wenn mehrere vCenter Server verknüpft sind, kann nur einer davon beim Konfigurieren des NSX Advanced Load Balancer Controller verwendet werden.
- Sie können den NSX Advanced Load Balancer Controller nicht in einer mehrschichtigen Tier-0-Topologie konfigurieren. Wenn die NSX-Umgebung mit einer Tier-0-Topologie mit mehreren Ebenen eingerichtet ist, können Sie beim Konfigurieren des NSX Advanced Load Balancer Controller nur ein Tier-0-Gateway verwenden.

Netzwerkkonfigurationsmethoden mit NSX

Supervisor verwendet eine Opinionated-Netzwerkkonfiguration. Zum Konfigurieren des Supervisor-Netzwerks mit NSX gibt es zwei Methoden, die zur Bereitstellung desselben Netzwerkmodells für einen Supervisor für eine Zone führen:

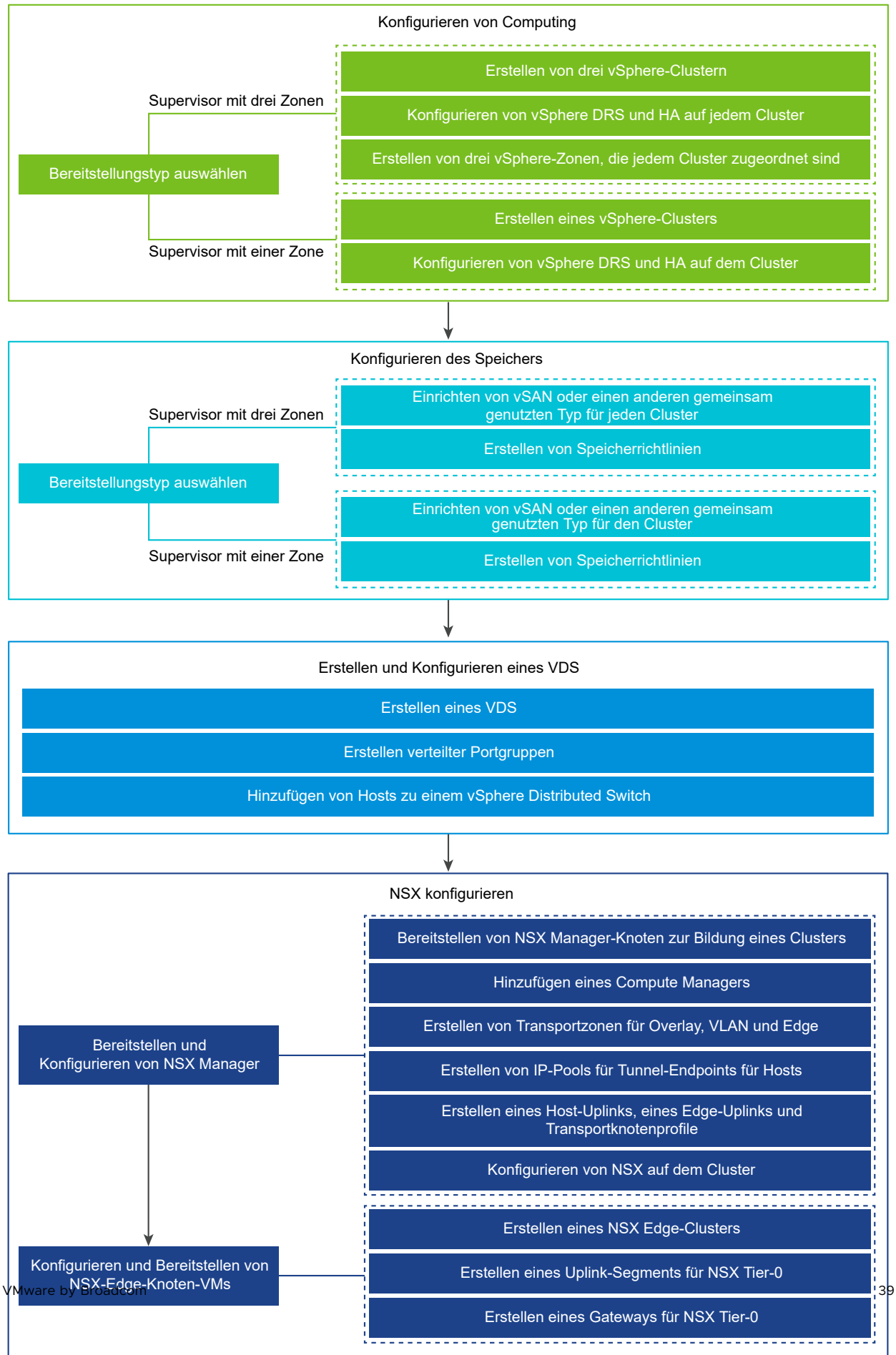
- Die einfachste Möglichkeit zur Konfiguration des Supervisor-Netzwerks besteht darin, VMware Cloud Foundation SDDC Manager zu verwenden. Weitere Informationen finden Sie in der Dokumentation zu VMware Cloud Foundation SDDC Manager. Weitere Informationen finden Sie im Administratorhandbuch für VMware Cloud Foundation.

- Sie können das Supervisor-Netzwerk auch manuell konfigurieren, indem Sie eine vorhandene NSX-Bereitstellung verwenden oder eine neue NSX-Instanz bereitstellen. Weitere Informationen finden Sie unter Installieren und Konfigurieren von NSX for vSphere IaaS control plane.

Installieren und Konfigurieren von NSX für vSphere IaaS control plane

vSphere IaaS control plane erfordert eine bestimmte Netzwerkkonfiguration, um die Konnektivität mit den Supervisoren, vSphere-Namespaces und allen Objekten zu ermöglichen, die in den Namespaces ausgeführt werden, z. B. vSphere-Pods, VMs und Tanzu Kubernetes-Cluster. Als vSphere-Administrator installieren und konfigurieren Sie NSX für vSphere IaaS control plane.

Abbildung 4-7. Workflow zum Konfigurieren eines Supervisors mit NSX



In diesem Abschnitt wird beschrieben, wie das Supervisor-Netzwerk durch Bereitstellen einer neuen NSX-Instanz konfiguriert wird. Die Verfahren gelten jedoch auch für eine vorhandene NSX-Bereitstellung. Darüber hinaus finden Sie in diesem Abschnitt auch Hintergrundinformationen zu den Schritten, die VMware Cloud Foundation SDDC Manager beim Einrichten der Supervisor-Arbeitslastdomäne ausführt.

Voraussetzungen

- Stellen Sie sicher, dass Ihre Umgebung die Systemanforderungen für die Konfiguration eines vSphere-Clusters als Supervisor erfüllt. Informationen zu den Anforderungen finden Sie unter Anforderungen an einen Zonen-Supervisor mit NSX und Anforderungen an die Cluster-Supervisor-Bereitstellung mit NSX in *Konzepte und Planung der vSphere IaaS-Steuerungsebene*.
- Weisen Sie dem Supervisor eine Lizenz der Tanzu Edition zu.
- Erstellen Sie Speicherrichtlinien für die Platzierung von Steuerungsebenen-VMs, flüchtigen Pod-Festplatten und Container-Images.
- Konfigurieren Sie freigegebenen Speicher für den Cluster. Der gemeinsam genutzte Speicher ist für vSphere DRS, HA und die Speicherung persistenter Container-Volumes erforderlich.
- Stellen Sie sicher, dass DRS und HA auf dem vSphere-Cluster aktiviert ist und DRS sich im vollautomatisierten Modus befindet.
- Stellen Sie sicher, dass Sie über das Recht **Clusterweite Konfiguration ändern** auf dem Cluster verfügen.

Verfahren

1. Erstellen und Konfigurieren eines vSphere Distributed Switch

   Um die Netzwerkkonfiguration für alle Hosts im Supervisor zu verarbeiten, erstellen Sie einen vSphere Distributed Switch sowie verteilte Portgruppen und ordnen Sie dem Switch Hosts zu.

2. Bereitstellen und Konfigurieren von NSX Manager

   Mithilfe von vSphere Client können Sie NSX Manager im vSphere-Cluster bereitstellen und gemeinsam mit vSphere IaaS control plane verwenden.

3. Erstellen von Transportzonen

   Transportzonen geben an, welche Hosts und VMs ein bestimmtes Netzwerk verwenden können. Eine Transportzone kann sich über einen oder mehrere Host-Cluster erstrecken.

4. Konfigurieren und Bereitstellen eines NSX Edge-Transportknotens

   Sie können der NSX-Fabric eine NSX Edge-VM hinzufügen und sie dann als NSX Edge-Transportknoten-VM konfigurieren.

Erstellen und Konfigurieren eines vSphere Distributed Switch

Um die Netzwerkkonfiguration für alle Hosts im Supervisor zu verarbeiten, erstellen Sie einen vSphere Distributed Switch sowie verteilte Portgruppen und ordnen Sie dem Switch Hosts zu.

Verfahren

1 Navigieren Sie im vSphere Client zu einem Datencenter.

2 Klicken Sie mit der rechten Maustaste auf das Datencenter im Navigator und wählen Sie **Distributed Switch > Neuer Distributed Switch** aus.

3 Geben Sie einen Namen für den neuen Distributed Switch ein.

Beispiel: `DSwitch`.

4 Geben Sie unter **Version auswählen** eine Version für den Distributed Switch ein.

Wählen Sie **8,0**.

5 Geben Sie unter **Einstellungen konfigurieren** die Anzahl der Uplink-Ports ein.

Geben Sie den Wert `2` ein.

6 Überprüfen Sie die Einstellungen und klicken Sie auf **Fertig stellen**.

7 Klicken Sie mit der rechten Maustaste auf den von Ihnen erstellten Distributed Switch und wählen Sie **Einstellungen > Einstellungen bearbeiten** aus.

8 Geben Sie auf der Registerkarte **Erweitert** einen Wert über 1700 als MTU-Wert (Byte) ein und klicken Sie auf **OK**.

Die MTU-Größe muss für jedes Netzwerk, das Overlay-Datenverkehr überträgt, mindestens 1700 betragen.

Beispiel: `9000`.

NSX verwendet den globalen MTU-Standardwert 1700.

Erstellen verteilter Portgruppen

Erstellen Sie verteilte Portgruppen für jeden NSX Edge-Knoten-Uplink, Edge-Knoten-TEP, das Verwaltungsnetzwerk und den freigegebenen Speicher.

Die Standardportgruppe und die Standard-Uplinks werden beim Erstellen des vSphere Distributed Switch erstellt. Sie müssen die Verwaltungsportgruppe, vSAN-Portgruppe, erstellen. Edge-TEP-Portgruppe und die NSX Edge-Uplink-Portgruppe.

Voraussetzungen

Vergewissern Sie sich, dass Sie einen vSphere Distributed Switch erstellt haben.

Verfahren

1 Navigieren Sie im vSphere Client zu einem Datencenter.

2 Klicken Sie im Navigator mit der rechten Maustaste auf den Distributed Switch und wählen Sie **Verteilte Portgruppe > Neue verteilte Portgruppe** aus.

3 Erstellen Sie eine Portgruppe für den NSX Edge-Uplink.

Beispiel: `DPortGroup-EDGE-UPLINK`.

4 Konfigurieren Sie **VLAN-Typ** als „VLAN-Trunking“.

5 Akzeptieren Sie den standardmäßigen VLAN-Trunk-Bereich **(0-4094)**.

6 Klicken Sie auf **Weiter** und dann auf **Beenden**.

7 Klicken Sie mit der rechten Maustaste auf den Distributed Switch und wählen Sie im Menü **Aktionen** die Option **Verteilte Portgruppe > Verteilte Portgruppen verwalten** aus.

8 Wählen Sie **Teaming und Failover** aus, und klicken Sie auf **Weiter**.

9 Konfigurieren Sie aktive und Standby-Uplinks.

Der aktive Uplink ist beispielsweise `Uplink1`, der Standby-Uplink `Uplink2`.

10 Klicken Sie auf **OK**, um die Konfiguration der Portgruppe abzuschließen.

11 Wiederholen Sie die Schritte 2 bis 10, um Portgruppen für den Edge-Knoten-TEP, das Verwaltungsnetzwerk und den gemeinsam genutzten Speicher zu erstellen.

Erstellen Sie z. B. die folgenden Portgruppen:

Portgruppe	Name	VLAN-Typ
Edge-Knoten-TEP	`DPortGroup-EDGE-TEP`	Konfigurieren Sie **VLAN-Typ** als „VLAN-Trunking“. Konfigurieren Sie den aktiven Uplink als `Uplink2` und den Standby-Uplink als `Uplink1`. **Hinweis** Das für den Edge-Knoten-TEP verwendete VLAN muss sich von dem VLAN unterscheiden, das für den ESXi-TEP verwendet wird.
Verwaltung	`DPortGroup-MGMT`	Konfigurieren Sie **VLAN-Typ** als VLAN und geben Sie die VLAN-ID des Verwaltungsnetzwerks ein. Beispiel: `1060`.
Freigegebener Speicher oder vSAN	`DPortGroup-VSAN`	Konfigurieren Sie **VLAN-Typ** als VLAN und geben Sie die VLAN-ID ein. Beispiel: `3082`.

12 Erstellen Sie Portgruppen für die folgenden Komponenten:

- **vSphere vMotion**. Diese Portgruppe ist für Supervisor-Updates erforderlich. Konfigurieren Sie die Standardportgruppe für vMotion.
- **VM-Datenverkehr**. Konfigurieren Sie die Standardportgruppe für die Verarbeitung des VM-Datenverkehrs.

Hinzufügen von Hosts zu einem vSphere Distributed Switch

Um das Netzwerk Ihrer Umgebung mithilfe des vSphere Distributed Switch zu verwalten, müssen Sie Hosts aus dem Supervisor mit dem Switch verknüpfen. Verbinden Sie physische Netzwerkkarten, VMkernel-Adapter und Netzwerkadapter virtueller Maschinen mit dem Distributed Switch.

Voraussetzungen

- Stellen Sie sicher, dass genügend Uplinks auf dem Distributed Switch zur Verfügung stehen, um sie den physischen Netzwerkkarten zuzuordnen, die Sie mit dem Switch verbinden möchten.
- Vergewissern Sie sich, dass mindestens eine verteilte Portgruppe auf dem Distributed Switch verfügbar ist.
- Stellen Sie sicher, dass die verteilte Portgruppe aktive Uplinks enthält, die in der zugehörigen Teaming- und Failover-Richtlinie konfiguriert sind.

Verfahren

1. Wählen Sie im vSphere Client die Option **Netzwerk** aus und navigieren Sie zum Distributed Switch.
2. Wählen Sie im Menü **Aktionen** die Option **Hosts hinzufügen und verwalten** aus.
3. Wählen Sie auf der Seite **Aufgabe auswählen** die Option **Hosts hinzufügen** aus und klicken Sie auf **Weiter**.
4. Klicken Sie auf der Seite **Hosts auswählen** auf **Neue Hosts**, wählen Sie die gewünschten Hosts in Ihrem Datencenter aus, klicken Sie auf **OK** und anschließend auf **Weiter**.
5. Konfigurieren Sie auf der Seite **Physische Netzwerkadapter verwalten** physische Netzwerkkarten für den Distributed Switch.
   a. Wählen Sie aus der Liste **Auf anderen Switches/nicht beansprucht** eine physische Netzwerkkarte aus.

      Wenn Sie bereits mit anderen Switches verbundene physische Netzwerkkarten auswählen, werden sie zum aktuellen Distributed Switch migriert.

   b. Klicken Sie auf **Uplink zuweisen**.

   c. Auswählen eines Uplinks

   d. Um den Uplink allen Hosts im Cluster zuzuweisen, wählen Sie **Diese Uplink-Zuweisung auf die restlichen Hosts anwenden** aus.

   e. Klicken Sie auf **OK**.

   Weisen Sie beispielsweise `vmnic0` `Uplink 1` und `vmnic1` `Uplink 2` zu.
6. Klicken Sie auf **Weiter**.

7 Konfigurieren Sie auf der Seite **VMkernel-Adapter verwalten** VMkernel-Adapter.
   a Wählen Sie einen VMkernel-Adapter aus und klicken Sie auf **Portgruppe zuweisen**.
   b Wählen Sie eine verteilte Portgruppe aus.

      Beispielsweise **DPortGroup**.
   c Um die Portgruppe auf alle Hosts im Cluster anzuwenden, wählen Sie **Diese Portgruppenzuweisung auf die restlichen Hosts anwenden**.
   d Klicken Sie auf **OK**.
8 Klicken Sie auf **Weiter**.
9 (Optional) Aktivieren Sie auf der Seite **VM-Netzwerk migrieren** das Kontrollkästchen **Netzwerk virtueller Maschinen migrieren**, um ein Netzwerk virtueller Maschinen zu konfigurieren.
   a Um alle Netzwerkadapter einer virtuellen Maschine mit einer verteilten Portgruppe zu verbinden, wählen Sie die virtuelle Maschine aus, oder wählen Sie einen einzelnen Netzwerkadapter aus, um nur diesen Adapter zu verbinden.
   b Klicken Sie auf **Portgruppe zuweisen**.
   c Wählen Sie eine verteilte Portgruppe aus der Liste aus und klicken Sie auf **OK**.
   d Klicken Sie auf **Weiter**.

Nächste Schritte

Stellen Sie NSX Manager bereit und führen Sie die Konfiguration durch. Weitere Informationen hierzu finden Sie unter Bereitstellen und Konfigurieren von NSX Manager

Bereitstellen und Konfigurieren von NSX Manager

Mithilfe von vSphere Client können Sie NSX Manager im vSphere-Cluster bereitstellen und gemeinsam mit vSphere IaaS control plane verwenden.

Um NSX Manager über die OVA-Datei bereitzustellen, führen Sie die in diesem Verfahren angegebenen Schritte aus.

Informationen zum Bereitstellen von NSX Manager über die Benutzeroberfläche oder CLI finden Sie im *Installationshandbuch für NSX*.

Voraussetzungen

- Vergewissern Sie sich, dass Ihre Umgebung die Netzwerkanforderungen erfüllt. Informationen zu den Anforderungen finden Sie unter Anforderungen für einen Drei-Zonen-Supervisor mit NSX Advanced Load Balancer und Anforderungen für die Aktivierung eines Einzelcluster-Supervisors mit NSX Advanced Load Balancer in *Konzepte und Planung der vSphere IaaS-Steuerungsebene*.
- Vergewissern Sie sich, dass die erforderlichen Ports geöffnet sind. Weitere Informationen zu Ports und Protokollen finden Sie im *Installationshandbuch für NSX*.

Verfahren

1 Suchen Sie die OVA-Datei von NSX im VMware-Download-Portal.

   Kopieren Sie entweder die Download-URL oder laden Sie die OVA-Datei herunter.

2 Klicken Sie mit der rechten Maustaste und wählen Sie **OVF-Vorlage bereitstellen** aus, um den Installationsassistenten zu starten.

3 Geben Sie auf der Registerkarte **OVF-Vorlage auswählen** die OVA-Download-URL ein oder navigieren Sie zur OVA-Datei.

4 Geben Sie auf der Registerkarte **Namen und Ordner auswählen** einen Namen für die NSX Manager-VM ein.

5 Wählen Sie auf der Registerkarte **Computing-Ressource auswählen** den vSphere-Cluster aus, in dem der NSX Manager bereitgestellt werden soll.

6 Klicken Sie auf **Weiter**, um die Details zu überprüfen.

7 Wählen Sie auf der Registerkarte **Konfiguration** die NSX-Bereitstellungsgröße aus.

   Die empfohlene Mindestbereitstellungsgröße ist „Mittel“.

8 Wählen Sie auf der Registerkarte **Speicher auswählen** den freigegebenen Speicher für die Bereitstellung aus.

9 Aktivieren Sie Thin Provisioning, indem Sie unter **Format für die virtuelle Festplatte auswählen** die Option **Thin Provision** auswählen.

   Die virtuellen Festplatten werden standardmäßig per Thick Provisioning bereitgestellt.

10 Wählen Sie auf der Registerkarte **Netzwerke auswählen** unter **Zielnetzwerk** die Verwaltungsportgruppe oder das Zielnetzwerk für den NSX Manager aus.

   Beispiel: `DPortGroup-MGMT`.

11 Geben Sie auf der Registerkarte **Vorlage anpassen** das System-Root-, CLI-Administrator- und das Überwachungskennwort für den NSX Manager ein. Ihre Kennwörter müssen den Einschränkungen für die Kennwortsicherheit entsprechen.

   - Mindestens 12 Zeichen.
   - Mindestens ein Kleinbuchstabe.
   - Mindestens ein Großbuchstabe.
   - Mindestens eine Ziffer.
   - Mindestens ein Sonderzeichen.
   - Mindestens fünf verschiedene Zeichen.
   - Standardmäßig werden die Komplexitätsregeln des Kennworts durch das Linux PAM-Modul erzwungen.

12 Geben Sie für das IPv4-Gateway, die IPv4-Adresse des Verwaltungsnetzwerks, die Netzmaske des Verwaltungsnetzwerks, den DNS-Server, die Domänensuchliste und die NTP-IP-Adresse jeweils die Standardwerte ein.

13 Aktivieren Sie SSH und lassen Sie die Root-SSH-Anmeldung bei der NSX Manager-Befehlszeile zu.

   Die SSH-Optionen sind aus Sicherheitsgründen standardmäßig deaktiviert.

14 Stellen Sie sicher, dass Ihre benutzerdefinierte OVF-Vorlagenspezifikation korrekt ist, und klicken Sie auf **Beenden**, um die Installation zu initiieren.

15 Melden Sie sich nach dem Start von NSX Manager als Administrator bei der CLI an und führen Sie den Befehl `get interface eth0` aus, um zu überprüfen, ob die IP-Adresse erwartungsgemäß angewendet wurde.

16 Geben Sie den Befehl `get services` ein, um zu überprüfen, ob alle Dienste ausgeführt werden.

Bereitstellen von NSX Manager-Knoten zur Bildung eines Clusters

Ein NSX Manager-Cluster bietet Hochverfügbarkeit. Sie können NSX Manager-Knoten über die Benutzeroberfläche nur auf ESXi-Hosts bereitstellen, die von vCenter Server verwaltet werden. Um einen NSX Manager-Cluster zu erstellen, stellen Sie zwei zusätzliche Knoten bereit, um einen Cluster mit insgesamt drei Knoten zu bilden. Wenn Sie einen neuen Knoten über die Benutzeroberfläche bereitstellen, stellt der Knoten zur Bildung eines Clusters eine Verbindung zum ersten bereitgestellten Knoten her. Alle Repository-Details und das Kennwort des ersten bereitgestellten Knotens werden mit dem neu bereitgestellten Knoten synchronisiert.

Voraussetzungen

- Vergewissern Sie sich, dass ein NSX Manager-Knoten installiert ist.
- Vergewissern Sie sich, dass ein Compute Manager konfiguriert ist.
- Vergewissern Sie sich, dass die erforderlichen Ports geöffnet sind.
- Vergewissern Sie sich , dass ein Datenspeicher auf dem ESXi-Host konfiguriert ist.
- Vergewissern Sie sich, dass Sie über die IP-Adresse und das IP-Gateway, die DNS-Server-IP-Adressen, die Domänensuchliste und die NTP-Server-IP-Adresse verfügen, die vom NSX Manager verwendet werden sollen.
- Vergewissern Sie sich, dass Sie über ein Portgruppennetzwerk für die Ziel-VM verfügen. Platzieren Sie die NSX-Appliances in einem VM-Verwaltungsnetzwerk.

Verfahren

1 Melden Sie sich in einem Browser unter https://<manager-ip-address> mit Administratorrechten beim NSX Manager an.

2 Wählen Sie zum Bereitstellen einer Appliance **System > Appliances > NSX-Appliance hinzufügen** aus.

3 Geben Sie die Appliance-Details ein.

Option	Beschreibung
Hostname	Geben Sie den Hostnamen oder den FQDN ein, der für den Knoten verwendet werden soll.
Verwaltungs-IP/Netzmaske	Geben Sie eine IP-Adresse ein, die dem Knoten zugewiesen werden soll.
Verwaltungs-Gateway	Geben Sie eine Gateway-IP-Adresse ein, die vom Knoten verwendet werden soll.
DNS-Server	Geben Sie die Liste der DNS-Server-IP-Adressen ein, die vom Knoten verwendet werden sollen.
NTP-Server	Geben Sie die Liste der NTP-Server-IP-Adressen ein.
Knotengröße	Wählen Sie aus den verfügbaren Optionen den Formfaktor **Mittel (6 vCPUs, 24 GB RAM, 300 GB Speicher)**.

4 Geben Sie die Appliance-Konfigurationsdetails ein.

Option	Beschreibung
Compute Manager	Wählen Sie den vCenter Server aus, den Sie als Compute Manager konfiguriert haben.
Computing-Cluster	Wählen Sie den Cluster aus, dem der Knoten beitreten muss.
Datenspeicher	Wählen Sie einen Datenspeicher für die Knotendateien aus.
Format für die virtuelle Festplatte	Wählen Sie das Format **Thin Provision** aus.
Netzwerk	Klicken Sie auf **Netzwerk auswählen**, um das Verwaltungsnetzwerk für den Knoten auszuwählen.

5 Geben Sie die Details für den Zugriff und die Anmeldedaten ein.

Option	Beschreibung
Aktivieren von SSH	Schalten Sie die Umschaltfläche so um, dass eine SSH-Anmeldung beim neuen Knoten zulässig ist.
Zulassen von Root-Zugriff	Schalten Sie die Umschaltfläche so um, dass ein Root-Zugriff auf den neuen Knoten zulässig ist.

Option	Beschreibung
System-Root-Anmeldedaten	Legen Sie das Root-Kennwort für den neuen Knoten fest und bestätigen Sie es. Ihr Kennwort muss den Einschränkungen für die Kennwortsicherheit entsprechen. ■ Mindestens 12 Zeichen. ■ Mindestens ein Kleinbuchstabe. ■ Mindestens ein Großbuchstabe. ■ Mindestens eine Ziffer. ■ Mindestens ein Sonderzeichen. ■ Mindestens fünf verschiedene Zeichen. ■ Standardmäßig werden die Komplexitätsregeln des Kennworts durch das Linux PAM-Modul erzwungen.
Administrator-CLI- und Überwachungs-CLIAnmeldedaten	Aktivieren Sie das Kontrollkästchen **Identisch mit Root-Kennwort**, um dasselbe Kennwort zu verwenden, das Sie für „Root“ konfiguriert haben, oder deaktivieren Sie das Kontrollkästchen und legen Sie ein anderes Kennwort fest.

6 Klicken Sie auf **Appliance installieren**.

Der neue Knoten ist bereitgestellt. Sie können den Bereitstellungsvorgang auf der Seite **System > > Appliances** nachverfolgen. Fügen Sie keine weiteren Knoten hinzu, bis die Installation abgeschlossen und der Cluster stabil ist.

7 Warten Sie, bis die Bereitstellung, die Clusterbildung und die Repository-Synchronisierung abgeschlossen sind.

Der Beitritts- und der Clusterstabilisierungsvorgang können zwischen 10 und 15 Minuten in Anspruch nehmen. Vergewissern Sie sich, dass der Status jeder Clusterdienstgruppe `UP` ist, bevor Sie andere Clusteränderungen vornehmen.

8 Melden Sie sich nach dem Start des Knotens als Administrator bei der CLI an und führen Sie den Befehl `get interface eth0` aus, um zu überprüfen, ob die IP-Adresse erwartungsgemäß angewendet wurde.

9 Wenn Ihr Cluster nur zwei Knoten aufweist, fügen Sie eine weitere Appliance hinzu. Wählen Sie **System > Appliances > NSX-Appliance hinzufügen** aus und wiederholen Sie die Konfigurationsschritte.

Hinzufügen einer Lizenz

Fügen Sie eine Lizenz mithilfe von NSX Manager hinzu.

Voraussetzungen

Rufen Sie eine Advanced- oder höhere NSX-Lizenz ab.

Verfahren

1 Melden Sie sich beim NSX Manager an.

2 Wählen Sie **System > Lizenzen > Hinzufügen** aus.

3 Geben Sie den Lizenzschlüssel ein.

4 Klicken Sie auf **Hinzufügen**.

Hinzufügen eines Compute Managers

Ein Compute Manager ist eine Anwendung, die Ressourcen wie Hosts und virtuelle Maschinen verwaltet. Konfigurieren Sie den vCenter Server, der dem NSX als Compute Manager im NSX Manager zugeordnet ist.

Weitere Informationen finden Sie im *Administratorhandbuch für NSX*.

Verfahren

1 Melden Sie sich beim NSX Manager an.

2 Wählen Sie **System > Fabric > Compute Manager > Hinzufügen** aus.

3 Geben Sie die Details zum Compute Manager ein.

Option	Beschreibung
Name und Beschreibung	Geben Sie den Namen und die Beschreibung von vCenter Server ein.
Typ	Der Standardtyp ist VMware vCenter.
Multi-NSX	Lassen Sie diese Option unausgewählt. Mit der Multi-NSX-Option können Sie denselben vCenter Server bei mehreren NSX-Managern registrieren. Diese Option wird auf Supervisor- und vSphere Lifecycle Manager-Clustern nicht unterstützt.
FQDN oder IP-Adresse	Geben Sie den FQDN oder die IP-Adresse von vCenter Server ein.
HTTPS-Port des Reverse-Proxys	Der Standardport ist 443. Wenn Sie einen anderen Port verwenden, stellen Sie sicher, dass der Port auf allen NSX Manager-Appliances offen ist. Legen Sie den Reverse-Proxy-Port zum Registrieren von Compute Manager in NSX fest.
Benutzername und Kennwort	Geben Sie die vCenter Server-Anmeldedaten ein.
SHA-256-Fingerabdruck	Geben Sie den Wert für den vCenter Server-SHA-256-Fingerabdruckalgorithmus ein.

Sie können die Standardwerte für die anderen Einstellungen beibehalten.

Wenn Sie den Fingerabdruckwert leer lassen, werden Sie aufgefordert, den vom Server bereitgestellten Fingerabdruck zu akzeptieren. Nachdem Sie den Fingerabdruck akzeptiert haben, dauert es einige Sekunden, bis NSX die vCenter-Ressourcen ermittelt und registriert.

4 Wählen Sie **Vertrauensstellung aktivieren** aus, damit vCenter Server mit NSX kommunizieren kann.

5 Wenn Sie keinen Fingerabdruckwert für NSX Manager angeben, identifiziert das System den Fingerabdruck und zeigt ihn an.

6 Klicken Sie auf **Hinzufügen**, um den Fingerabdruck zu akzeptieren.

Ergebnisse

Nach einiger Zeit wird der Compute Manager bei vCenter Server registriert, und der Verbindungsstatus wechselt zu `Aktiv`. Wenn sich der FQDN/die PNID von vCenter Server ändert, müssen Sie sie beim NSX Manager erneut registrieren. Weitere Informationen finden Sie unter vCenter Server bei NSX Manager erneut registrieren.

Hinweis Nachdem vCenter Server erfolgreich registriert wurde, müssen Sie zuerst den Compute Manager löschen, bevor Sie die NSX Manager-VM ausschalten und löschen. Andernfalls können Sie beim Bereitstellen einer neuen NSX Manager-Instanz dieselbe vCenter Server-Instanz nicht wieder registrieren. Sie erhalten eine Fehlermeldung, dass vCenter Server bereits bei einer anderen NSX Manager-Instanz registriert ist.

Sie können auf den Namen des Compute Managers klicken, um die Details anzuzeigen, den Compute Manager zu bearbeiten oder Tags zu verwalten, die auf den Compute Manager angewendet wurden.

Erstellen von Transportzonen

Transportzonen geben an, welche Hosts und VMs ein bestimmtes Netzwerk verwenden können. Eine Transportzone kann sich über einen oder mehrere Host-Cluster erstrecken.

Als vSphere Administrator verwenden Sie die Standardtransportzonen oder erstellen die folgenden Transportzonen:

- Eine Overlay-Transportzone, die von den VMs der Supervisor-Steuerungsebene verwendet wird.
- Eine VLAN-Transportzone für die NSX Edge-Knoten, die für Uplinks mit dem physischen Netzwerk verwendet werden sollen.

Verfahren

1. Melden Sie sich beim NSX Manager an.
2. Wählen Sie **System > Fabric > Transportzonen > Hinzufügen** aus.
3. Geben Sie einen Namen für die Transportzone und optional eine Beschreibung ein.
4. Wählen Sie einen Datenverkehrstyp aus.

   Sie können **Overlay** oder **VLAN** auswählen.

   Die folgenden Transportzonen sind standardmäßig vorhanden:

   - Eine VLAN-Transportzone mit dem Namen `nsx-vlan-transportzone`.
   - Eine Overlay-Transportzone mit dem Namen `nsx-overlay-transportzone`.
5. (Optional) Geben Sie einen oder mehrere Namen für die Uplink-Teaming-Richtlinie ein.

   Die an die Transportzonen angehängten Segmente verwenden diese benannten Teaming-Richtlinien. Wenn die Segmente keine übereinstimmende benannte Teaming-Richtlinie finden, wird die standardmäßige Uplink-Teaming-Richtlinie verwendet.

Ergebnisse

Die neue Transportzone wird auf der Seite **Transportzonen** angezeigt.

Erstellen eines IP-Pools für die IP-Adressen von Hosttunnel-Endpoints

Erstellen Sie IP-Pools für die ESXi-Hosttunnel-Endpoints (TEPs). TEPs sind die Quell- und Ziel-IP-Adressen, die in der externen IP-Kopfzeile verwendet werden, um die ESXi-Hosts zu identifizieren, bei denen die NSX-Kapselung von Frame-Overlays beginnt und endet. Sie können DHCP oder manuell konfigurierte IP-Pools für TEP-IP-Adressen verwenden.

Verfahren

1 Melden Sie sich beim NSX Manager an.

2 Wählen Sie **Netzwerk > IP-Adresspools > IP-Adresspool hinzufügen** aus.

3 Geben Sie die folgenden Details zum IP-Pool ein:

Option	Beschreibung
Name und Beschreibung	Geben Sie den IP-Poolnamen und eine optionale Beschreibung ein. Beispiel: `ESXI-TEP-IP-POOL`.
IP-Bereiche	Geben Sie den IP-Zuteilungsbereich ein. Beispielsweise `192.23.213.158 - 192.23.213.160`
Gateway	Geben Sie die Gateway-IP-Adresse ein. Beispiel: `192.23.213.253`.
CIDR	Geben Sie die Netzwerkadresse in einer CIDR-Notation ein. Beispiel: `192.23.213.0/24`.

4 Klicken Sie auf **Hinzufügen** und **Übernehmen**.

Ergebnisse

Stellen Sie sicher, dass die von Ihnen erstellten TEP-IP-Pools auf der Seite **IP-Pool** angezeigt werden.

Erstellen eines IP-Pools für Edge-Knoten

Erstellen Sie IP-Pools für die Edge-Knoten. Die TEP-Adressen müssen nicht routingfähig sein. Sie können ein beliebiges IP-Adressschema verwenden, mit dem der Edge-TEP mit dem Host-TEP kommunizieren kann.

Verfahren

1 Melden Sie sich beim NSX Manager an.

2 Wählen Sie **Netzwerk > IP-Adresspools > IP-Adresspool hinzufügen** aus.

3 Geben Sie die folgenden Details zum IP-Pool ein:

Option	Beschreibung
Name und Beschreibung	Geben Sie den IP-Poolnamen und eine optionale Beschreibung ein. Beispiel: `EDGE-TEP-IP-POOL`.
IP-Bereiche	Geben Sie den IP-Zuteilungsbereich ein. Beispielsweise `192.23.213.1 - 192.23.213.10`.
Gateway	Geben Sie die Gateway-IP-Adresse ein. Beispiel: `192.23.213.253`.
CIDR	Geben Sie die Netzwerkadresse in einer CIDR-Notation ein. Beispiel: `192.23.213.0/24`.

4 Klicken Sie auf **Hinzufügen** und **Übernehmen**.

Ergebnisse

Stellen Sie sicher, dass die von Ihnen erstellten IP-Pools auf der Seite **IP-Pool** angezeigt werden.

Erstellen eines Host-Uplink-Profils

Ein-Host-Uplink-Profil definiert Richtlinien für die Uplinks von den ESXi-Hosts zu NSX-Segmenten.

Verfahren

1 Melden Sie sich beim NSX Manager an.

2 Wählen Sie **System > Fabric > Profile > Uplink-Profile > Hinzufügen** aus.

3 Geben Sie einen Namen und optional eine Beschreibung für das Uplink-Profil ein.

Beispiel: `ESXI-UPLINK-PROFILE`.

4 Klicken Sie im Abschnitt **Teaming** auf **Hinzufügen**, um eine Teaming-Richtlinie für die Benennung hinzuzufügen, und konfigurieren Sie eine Richtlinie für die **Failover-Reihenfolge**.

Eine Liste der aktiven Uplinks wird angegeben, und jede Schnittstelle auf dem Transportknoten ist an einen aktiven Uplink gebunden. Bei dieser Konfiguration können mehrere aktive Uplinks gleichzeitig verwendet werden.

5 Konfigurieren Sie aktive und Standby-Uplinks.

Sie können z. B. `uplink-1` als aktiven Uplink und `uplink-2` als Standby-Uplink konfigurieren.

6 Geben Sie einen Wert für das Transport-VLAN ein.

Das in den Tags des Uplink-Profils festgelegte Transport-VLAN überlagert den Datenverkehr, und die VLAN-ID wird vom Tunnel-Endpoint (TEP) verwendet.

Beispiel: `1060`.

7 Geben Sie den MTU-Wert ein.

Der Standardwert für die MTU des Uplink-Profils ist 1600.

Hinweis Der Wert muss mindestens 1600 betragen, darf aber nicht höher sein als der MTU-Wert auf den physischen Switches und dem vSphere Distributed Switch.

Erstellen eines Edge-Uplink-Profils

Erstellen Sie ein Uplink-Profil mit der Teaming-Richtlinie für die Failover-Reihenfolge mit einem aktiven Uplink für Overlay-Datenverkehr der Edge-VM.

Verfahren

1 Melden Sie sich beim NSX Manager an.

2 Wählen Sie **System > Fabric > Profile > Uplink-Profile > Hinzufügen** aus.

3 Geben Sie einen Uplink-Profilnamen ein und fügen Sie optional eine Beschreibung für das Uplink-Profil hinzu.

Beispiel: `EDGE-UPLINK-PROFILE`.

4 Klicken Sie im Abschnitt **Teaming** auf **Hinzufügen**, um eine Teaming-Richtlinie für die Benennung hinzuzufügen, und konfigurieren Sie eine **Failover**-Richtlinie.

Eine Liste der aktiven Uplinks wird angezeigt, und jede Schnittstelle auf dem Transportknoten wird an einen aktiven Uplink gebunden. Bei dieser Konfiguration können mehrere aktive Uplinks gleichzeitig verwendet werden.

5 Konfigurieren Sie einen aktiven Uplink.

Konfigurieren Sie z. B. `uplink-1` als aktiven Uplink.

6 Zeigen Sie die Uplinks auf der Seite **Uplink-Profil** an.

Erstellen eines Transportknotenprofils

Ein Transportknotenprofil definiert, wie NSX auf den Hosts in einem bestimmten Cluster, an den das Profil angehängt ist, installiert und konfiguriert ist.

Voraussetzungen

Stellen Sie sicher, dass Sie eine Overlay-Transportzone erstellt haben.

Verfahren

1 Melden Sie sich beim NSX Manager an.

2 Wählen Sie **System > Fabric > Profile > Transportknotenprofile > Hinzufügen** aus.

3 Geben Sie einen Namen für das Transportknotenprofil und optional eine Beschreibung ein.

Beispiel: `HOST-TRANSPORT-NODE-PROFILE`.

4 Wählen Sie im Abschnitt **Switch des neuen Knotens** als **Typ** die Option `VDS` aus.

5 Wählen Sie als **Modus** die Option `Standard` aus.

6 Wählen Sie die Namen für den vCenter Server und den Distributed Switch aus der Liste aus.

Beispielsweise `DSwitch`

7 Wählen Sie die zuvor erstellte Overlay-Transportzone aus.

Beispiel: `NSX-OVERLAY-TRANSPORTZONE`.

8 Wählen Sie das zuvor erstellte Host-Uplink-Profil aus.

Beispiel: `ESXI-UPLINK-PROFILE`.

9 Wählen Sie aus der Liste **IP-Zuweisung** die Option **IP-Pool verwenden** aus.

10 Wählen Sie den zuvor erstellten Host-TEP-Pool aus.

Beispiel: `ESXI-TEP-IP-POOL`.

11 Klicken Sie unter **Switch-Zuordnung für Teaming-Richtlinien** auf das Bearbeitungssymbol und ordnen Sie die im NSX-Uplink-Profil definierten Uplinks den vSphere Distributed Switch-Uplinks zu.

Weisen Sie beispielsweise `Uplink 1` `uplink-1 (active)` und `Uplink 2` `uplink-2 (standby)` zu.

12 Klicken Sie auf **Hinzufügen**.

13 Vergewissern Sie sich, dass das von Ihnen erstellte Profil auf der Seite **Transportknotenprofile** aufgelistet ist.

Konfigurieren von NSX im Cluster

Um NSX zu installieren und die Overlay-TEPs vorzubereiten, wenden Sie das Transportknotenprofil auf den vSphere-Cluster an.

Voraussetzungen

Stellen Sie sicher, dass Sie ein Transportknotenprofil erstellt haben.

Verfahren

1 Melden Sie sich beim NSX Manager an.

2 Wählen Sie **System > Fabric > Knoten > Host-Transportknoten** aus.

3 Wählen Sie im Dropdown-Menü **Verwaltet von** eine vorhandene vCenter Server-Instanz aus.

Auf der Seite werden die verfügbaren vSphere-Cluster aufgelistet.

4 Wählen Sie den Computing-Cluster aus, in dem Sie NSX konfigurieren möchten.

5 Klicken Sie auf **NSX konfigurieren**.

6 Wählen Sie das zuvor erstellte Transportknotenprofil aus und klicken Sie auf **Übernehmen**.

Beispiel: `HOST-TRANSPORT-NODE-PROFILE`.

7 Stellen Sie auf der Seite **Host-Transportknoten** sicher, dass der Konfigurationszustand von NSX `Success` und der NSX Manager-Konnektivitätsstatus der Hosts im Cluster `Up` ist.

Ergebnisse

Das zuvor erstellte Transportknotenprofil wird auf den vSphere-Cluster angewendet, um NSX zu installieren und die Overlay-TEPs vorzubereiten.

Konfigurieren und Bereitstellen eines NSX Edge-Transportknotens

Sie können der NSX-Fabric eine NSX Edge-VM hinzufügen und sie dann als NSX Edge-Transportknoten-VM konfigurieren.

Voraussetzungen

Stellen Sie sicher, dass Sie Transportzonen, das Edge-Uplink-Profile und den Edge-TEP-IP-Pool erstellt haben.

Verfahren

1 Melden Sie sich beim NSX Manager an.

2 Wählen Sie **System > Fabric > Knoten > Edge-Transportknoten > Edge-VM hinzufügen** aus.

3 Geben Sie unter **Name und Beschreibung** einen Namen für die NSX Edge ein.

Beispielsweise `nsx-edge-1`

4 Geben Sie den Hostnamen oder den FQDN aus vCenter Server ein.

Beispiel: `nsx-edge-1.lab.com`.

5 Wählen Sie den Formfaktor `Large` aus.

6 Geben Sie unter **Anmeldedaten** das CLI- und das Root-Kennwort für die NSX Edge ein. Ihre Kennwörter müssen den Einschränkungen für die Kennwortsicherheit entsprechen.

- Mindestens 12 Zeichen.
- Mindestens ein Kleinbuchstabe.
- Mindestens ein Großbuchstabe.
- Mindestens eine Ziffer.
- Mindestens ein Sonderzeichen.
- Mindestens fünf verschiedene Zeichen.
- Standardmäßig werden die Komplexitätsregeln des Kennworts durch das Linux PAM-Modul erzwungen.

7 Aktivieren Sie die Option **SSH-Anmeldung zulassen** für die CLI- und die Root-Anmeldedaten.

8 Konfigurieren Sie unter **Bereitstellung konfigurieren** die folgenden Eigenschaften:

Option	Beschreibung
Compute Manager	Wählen Sie im Dropdown-Menü den Compute Manager aus. Wählen Sie z. B. `vCenter` aus.
Cluster	Wählen Sie im Dropdown-Menü den Cluster aus. Wählen Sie z. B. `Compute-Cluster` aus.
Datenspeicher	Wählen Sie den gemeinsam genutzten Datenspeicher aus der Liste aus. Beispiel: `vsanDatastore`.

9 Konfigurieren Sie die Knoteneinstellungen.

Option	Beschreibung
IP-Zuweisung	Wählen Sie „Statisch“ aus. Geben Sie Werte für folgende Elemente ein: ■ **Verwaltungs-IP**: Geben Sie die IP-Adresse im selben VLAN ein, in dem sich das vCenter Server-Verwaltungsnetzwerk befindet. Beispiel: `10.197.79.146/24`. ■ **Standard-Gateway**: Das Standard-Gateway des Verwaltungsnetzwerks. Beispiel: `10.197.79.253`.
Verwaltungsschnittstelle	Klicken Sie auf **Schnittstelle auswählen** und wählen Sie im zuvor von Ihnen erstellten Dropdown-Menü die vSphere Distributed Switch-Portgruppe im selben VLAN aus, in dem sich das Verwaltungsnetzwerk befindet. Beispiel: `DPortGroup-MGMT`.

10 Klicken Sie unter **NSX konfigurieren** auf **Switch hinzufügen**, um die Switch-Eigenschaften zu konfigurieren.

11 Verwenden Sie für **Edge-Switchname** den Standardnamen.

Beispiel: `nvds1`.

12 Wählen Sie die Transportzone aus, zu der der Transportknoten gehört.

Wählen Sie die zuvor erstellten Overlay-Transportzonen aus.

Beispiel: `nsx-overlay-transportzone`.

13 Wählen Sie das zuvor erstellte Edge-Uplink-Profil aus.

Beispiel: `EDGE-UPLINK-PROFILE`.

14 Wählen Sie unter **IP-Zuweisung** die Option **IP-Pool verwenden** aus.

15 Wählen Sie den zuvor erstellten Edge-TEP-IP-Pool aus.

Beispiel: `EDGE-TEP-IP-POOL`.

16 Ordnen Sie im Abschnitt **Switch-Zuordnung für Teaming- Uplinks** den Uplink den zuvor erstellten Edge-Uplink-Profilen zu.

   Wählen Sie beispielsweise für `Uplink1` `DPortGroup-EDGE-TEP` aus.

17 Wiederholen Sie die Schritte 10 – 16, um einen neuen Switch hinzuzufügen.

   Konfigurieren Sie beispielsweise die folgenden Werte:

Eigenschaft	Wert
Name des Edge-Switch	`nvds2`
Transportzone	`nsx-vlan-transportzone`
Edge-Uplink-Profil	`EDGE-UPLINK-PROFILE`
Switch-Zuordnung für Teaming-Richtlinien	`DPortGroup-EDGE-UPLINK`

18 Klicken Sie auf **Beenden**.

19 Wiederholen Sie die Schritte 2 – 18 für eine zweite NSX Edge-VM.

20 Sehen Sie sich auf der Seite **Edge-Transportknoten** den Verbindungsstatus an.

Erstellen eines NSX Edge-Clusters

Um sicherzustellen, dass immer mindestens eine NSX Edge-Instanz verfügbar ist, erstellen Sie einen NSX Edge-Cluster.

Verfahren

1 Melden Sie sich beim NSX Manager an.

2 Wählen Sie **System > Fabric > Knoten > Edge-Cluster > Hinzufügen** aus.

3 Geben Sie den NSX Edge-Clusternamen ein.

   Beispiel: `EDGE-CLUSTER`.

4 Wählen Sie im Dropdown-Menü das standardmäßige NSX Edge-Clusterprofil aus.

   Wählen Sie **nsx-default-edge-high-availability-profile** aus.

5 Wählen Sie im Dropdown-Menü **Mitgliedstyp** den **Edge-Knoten** aus.

6 Wählen Sie in der Spalte **Verfügbar** die zuvor erstellten NSX Edge-VMs aus und klicken Sie auf den Pfeil nach rechts, um sie in die Spalte **Ausgewählt** zu verschieben.

7 Beispiele: `nsx-edge-1` und `nsx-edge-2`.

8 Klicken Sie auf **Speichern**.

Erstellen eines Tier-0-Uplink-Segments

Das Tier-0-Uplink-Segment bietet die Nord-Süd-Konnektivität von NSX zur physischen Infrastruktur.

Voraussetzungen

Vergewissern Sie sich, dass Sie ein Tier-0-Gateway erstellt haben.

Verfahren

1. Melden Sie sich beim NSX Manager an.
2. Wählen Sie **Netzwerk > Segmente > Segment hinzufügen** aus.
3. Geben Sie einen Namen für das Segment ein.

   Beispiel: `TIER-0-LS-UPLINK`.
4. Wählen Sie die zuvor erstellte Transportzone aus.

   Wählen Sie z. B. `nsx-vlan-transportzone` aus.
5. Schalten Sie die Option **Administrativer Status** um, um sie zu aktivieren.
6. Geben Sie eine VLAN-ID des Tier-0-Gateways ein.

   Beispiel: `1089`.
7. Klicken Sie auf **Speichern**.

Erstellen eines Tier-0-Gateways

Das Tier-0-Gateway ist der logische NSX-Router, der der physischen Infrastruktur die Nord-Süd-Konnektivität für das logische NSX-Netzwerk bereitstellt. vSphere IaaS control plane unterstützt mehrere Tier-0-Gateways auf mehreren NSX Edge-Clustern in derselben Transportzone.

Ein Tier-0-Gateway verfügt über Downlink-Verbindungen zu Tier-1-Gateways und externe Verbindungen zu physischen Netzwerken.

Sie können den Hochverfügbarkeitsmodus (HA) eines Tier-0-Gateways als „Aktiv-Aktiv“ oder „Aktiv-Standby“ konfigurieren. Die folgenden Dienste werden nur im „Aktiv-Standby“-Modus unterstützt:

- NAT
- Lastausgleich
- Statusbehaftete Firewall
- VPN

Proxy-ARP wird automatisch auf einem Tier-0-Gateway aktiviert, wenn eine NAT-Regel oder eine Load Balancer-VIP eine IP-Adresse aus dem Subnetz der externen Schnittstelle des Tier-0-Gateways verwendet. Durch die Aktivierung von Proxy-ARP können Hosts in den Overlay-Segmenten und Hosts in einem VLAN-Segment Netzwerkdatenverkehr gemeinsam austauschen, ohne Änderungen am physischen Netzwerk-Fabric vorzunehmen.

Vor NSX 3.2 wird Proxy-ARP auf einem Tier-0-Gateway nur in einer Aktiv/Aktiv-Konfiguration unterstützt. Ab NSX 3.2 wird Proxy-ARP auch auf einem Tier-0-Gateway in einer Aktiv/Aktiv-Konfiguration unterstützt.

Weitere Informationen finden Sie unter *Administratorhandbuch für NSX*.

Voraussetzungen

Stellen Sie sicher, dass Sie einen NSX Edge-Cluster erstellt haben.

Verfahren

1. Melden Sie sich beim NSX Manager an.
2. Wählen Sie **Netzwerk > Tier-0 Gateways** aus.
3. Klicken Sie auf **Tier-0-Gateway hinzufügen**.
4. Geben Sie einen Namen für das Tier-0-Gateway ein.

   Beispiel: `Tier-0_VWT`.
5. Wählen Sie einen Aktiv-Standby-HA-Modus aus.

   Im Aktiv-Standby-Modus verarbeitet das gewählte aktive Mitglied den gesamten Datenverkehr. Wenn das aktive Mitglied ausfällt, wird ein neues Mitglied als aktives Mitglied ausgewählt.
6. Wählen Sie den zuvor erstellten NSX Edge-Cluster aus.

   Wählen Sie z. B. `EDGE-CLUSTER` aus.
7. Klicken Sie auf **Speichern**.

   Das Tier-0-Gateway wird erstellt.
8. Wählen Sie **Ja**, um mit der Konfiguration fortzufahren.
9. Konfigurieren Sie Schnittstellen.
   a. Erweitern Sie **Schnittstellen** und klicken Sie auf **Festlegen**.
   b. Klicken Sie auf **Schnittstelle hinzufügen**.
   c. Geben Sie einen Namen ein.

      Geben Sie z. B. den Namen `TIER-0_VWT-UPLINK1` ein.
   d. Wählen Sie für **Typ** die Option **Extern** aus.
   e. Geben Sie eine IP-Adresse aus dem Uplink-VLAN des logischen Edge-Routers ein. Die IP-Adresse darf nicht mit der Verwaltungs-IP-Adresse identisch sein, die für die zuvor erstellten NSX Edge-VMs konfiguriert wurde.

      Beispiel: `10.197.154.1/24`.
   f. Wählen Sie unter **Verbunden mit** das zuvor erstellte Tier-0-Uplink-Segment aus.

      Beispielsweise `TIER-0-LS-UPLINK`
   g. Wählen Sie einen NSX Edge-Knoten aus der Liste aus.

      Beispiel: `nsx-edge-1`.

h Klicken Sie auf **Speichern**.

i Wiederholen Sie die Schritte a – h für die zweite Schnittstelle.

Erstellen Sie beispielsweise einen zweiten Uplink `TIER-0_VWT-UPLINK2` mit der IP-Adresse `10.197.154.2/24`, der mit dem Edge-Knoten `nsx-edge-2` verbunden ist.

j Klicken Sie auf **Schließen**.

10 Um High Availability zu konfigurieren, klicken Sie unter **HA-VIP-Konfiguration** auf **Festlegen**.

a Klicken Sie auf **HA-VIP-KONFIGURATION HINZUFÜGEN**.

b Geben Sie die IP-Adresse ein.

Beispielsweise `10.197.154.3/24`

c Wählen Sie die Schnittstellen aus.

Beispiel: `TIER-0_WVT-UPLINK1` und `TIER-0_WVT-UPLINK2`

d Klicken Sie auf **Hinzufügen** und **Übernehmen**.

11 Um Routing zu konfigurieren, klicken Sie auf **Routing**.

a Klicken Sie unter „Statische Routen“ auf **Festlegen**.

b Klicken Sie auf **STATISCHE ROUTE HINZUFÜGEN**.

c Geben Sie einen Namen ein.

Beispiel: `DEFAULT-STATIC-ROUTE`.

d Geben Sie als Netzwerk-IP-Adresse `0.0.0.0/0` ein.

e Um die nächsten Hops zu konfigurieren, klicken Sie auf **Nächste Hops festlegen** und **Nächsten Hop hinzufügen**.

f Geben Sie die IP-Adresse des Routers für den nächsten Hop ein. In der Regel handelt es sich hierbei um das Standard-Gateway des VLAN des Verwaltungsnetzwerks aus dem Uplink-VLAN des logischen NSX Edge-Routers.

Beispiel: `10.197.154.253`.

g Klicken Sie auf **Hinzufügen** und **Übernehmen** und **SPEICHERN**.

h Klicken Sie auf **Schließen**.

12 Stellen Sie zum Überprüfen der Konnektivität sicher, dass ein externes Gerät in der physischen Architektur die von Ihnen konfigurierten Uplinks pingen kann.

Nächste Schritte

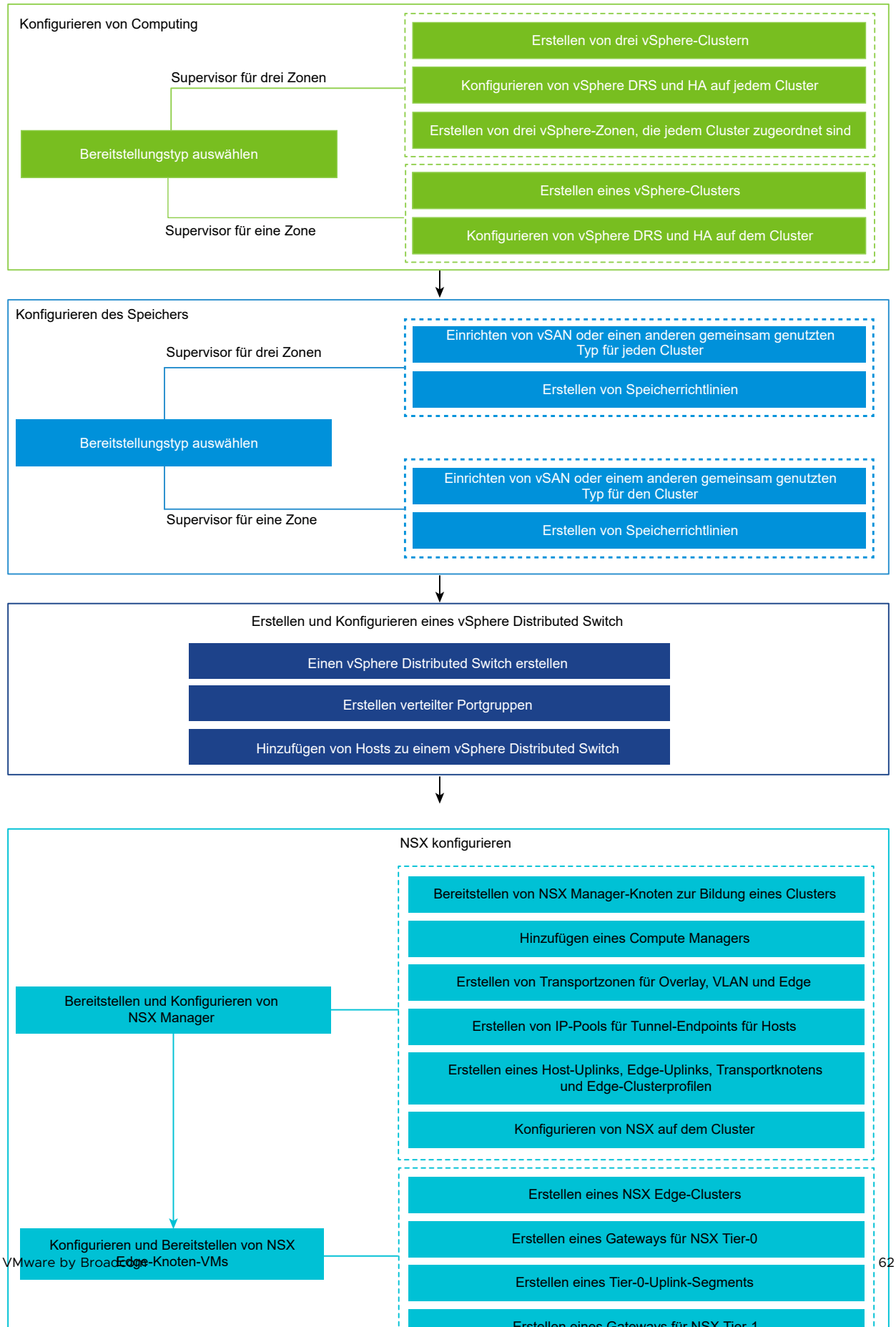
Konfigurieren Sie einen Supervisor. Siehe Bereitstellen einers Supervisors für eine Zone mit NSX-Netzwerk.

Installieren und Konfigurieren von NSX und NSX Advanced Load Balancer

In einer Supervisor-Umgebung, in der NSX als Netzwerk-Stack verwendet wird, können Sie den NSX Advanced Load Balancer für Lastausgleichsdienste verwenden.

In diesem Abschnitt wird beschrieben, wie Sie das Supervisor-Netzwerk konfigurieren, indem Sie eine neue NSX-Instanz und eine neue NSX Advanced Load Balancer bereitstellen. Das Verfahren zum Installieren und Konfigurieren der NSX Advanced Load Balancer gilt auch für eine vorhandene NSX-Bereitstellung.

Abbildung 4-8. Workflow zum Konfigurieren eines Supervisors mit NSX und NSX Advanced Load Balancer



Erstellen eines vSphere Distributed Switch für einen Supervisor zwecks Verwendung mit NSX Advanced Load Balancer

Um einen vSphere-Cluster zu konfigurieren, der den NSX-Netzwerk-Stack und NSX Advanced Load Balancer als Supervisor verwendet, müssen Sie einen vSphere Distributed Switch erstellen. Erstellen Sie Portgruppen auf dem Distributed Switch, den Sie als Arbeitslastnetzwerke für den Supervisor konfigurieren können. Der NSX Advanced Load Balancer benötigt eine verteilte Portgruppe, um die Dienst-Engine-Datenschnittstellen zu verbinden. Die Portgruppe wird verwendet, um die virtuellen Anwendungs-IPs (VIPs) auf den Dienst-Engines zu platzieren.

Voraussetzungen

Überprüfen Sie die Systemanforderungen und Netzwerktopologien für die Verwendung des vSphere-Netzwerks für den Supervisor mit dem NSX Advanced Load Balancer. Siehe Anforderungen für Zonal Supervisor mit NSX und NSX Advanced Load Balancer und Anforderungen für die Cluster Supervisor-Bereitstellung mit NSX und NSX Advanced Load Balancer in *Konzepte und Planung der vSphere IaaS-Steuerungsebene*.

Verfahren

1. Navigieren Sie im vSphere Client zu einem Datencenter.
2. Klicken Sie mit der rechten Maustaste auf das Datencenter und wählen Sie **Distributed Switch > Neuer Distributed Switch** aus.
3. Geben Sie einen Namen für den Switch ein, z. B. **`wcp_vds_1`**, und klicken Sie auf **Weiter**.
4. Wählen Sie Version 8.0 für den Switch aus und klicken Sie auf **Weiter**.
5. Geben Sie unter **Portgruppenname** **`Primäres Arbeitslastnetzwerk`** ein, klicken Sie auf **Weiter** und dann auf **Beenden**.

   Ein neuer Distributed Switch mit einer Portgruppe wird im Datencenter erstellt. Sie können diese Portgruppe als das primäre Arbeitslastnetzwerk für den Supervisor verwenden, den Sie erstellen werden. Das primäre Arbeitslastnetzwerk verarbeitet den Datenverkehr für die Kubernetes-Steuerungsebenen-VMs.
6. Erstellen Sie verteilte Portgruppen für Arbeitslastnetzwerke.

   Wie viele Portgruppen Sie erstellen, hängt von der Topologie ab, die Sie für den Supervisor implementieren möchten. Erstellen Sie für eine Topologie mit einem isolierten Arbeitslastnetzwerk eine verteilte Portgruppe, die Sie als Netzwerk für alle Namespaces auf dem Supervisor verwenden werden. Erstellen Sie für eine Topologie mit isolierten Netzwerken für jeden Namespace dieselbe Anzahl an Portgruppen wie die Anzahl der von Ihnen zu erstellenden Namespaces.
   a. Navigieren Sie zum neu erstellten Distributed Switch.
   b. Klicken Sie mit der rechten Maustaste auf den Switch und wählen Sie **Verteilte Portgruppen > Neue verteilte Portgruppe** aus.

c Geben Sie einen Namen für die Portgruppe ein, z. B. **`Arbeitslastnetzwerk`**, und klicken Sie auf **Weiter**.

d Behalten Sie die Standardeinstellungen bei, klicken Sie auf **Weiter** und dann auf **Beenden**.

7 Erstellen Sie eine Portgruppe für das Datennetzwerk.

a Klicken Sie mit der rechten Maustaste auf den Distributed Switch und wählen Sie **Verteilte Portgruppe > Neue verteilte Portgruppe** aus.

b Geben Sie einen Namen für die Portgruppe ein, z. B. **`Datennetzwerk`**, und klicken Sie auf **Weiter**.

c Geben Sie auf der Seite **Einstellungen konfigurieren** die allgemeinen Eigenschaften für die neue verteilte Portgruppe ein und klicken Sie auf **Weiter**.

Eigenschaft	Beschreibung
Port-Bindung	Wählen Sie aus, wann Ports virtuellen Maschinen zugewiesen werden, die mit dieser verteilten Portgruppe verbunden sind. Wählen Sie **Statische Bindung** aus, um einer virtuellen Maschine einen Port zuzuweisen, wenn die virtuelle Maschine mit der verteilten Portgruppe verbunden wird.
Portzuteilung	Wählen Sie die Portzuteilung **Elastisch** aus. Die Standardanzahl der Ports ist acht. Wenn alle Ports zugewiesen wurden, wird ein neues Set aus acht Ports erstellt.
Anzahl der Ports	Behalten Sie den Standardwert bei.
Netzwerkressourcenpool	Weisen Sie über das Dropdown-Menü die neue verteilte Portgruppe einem benutzerdefinierten Netzwerkressourcenpool zu. Wenn Sie keinen Netzwerkressourcenpool erstellt haben, bleibt dieses Menü leer.
VLAN	Wählen Sie im Dropdown-Menü den Typ des VLAN-Datenverkehrsfilters und der Markierung aus: ■ **Keine**: Verwenden Sie VLAN nicht. Wählen Sie diese Option aus, wenn Sie External Switch Tagging verwenden. ■ **VLAN**: Geben Sie im Textfeld „VLAN-ID“ einen Wert zwischen 1 und 4.094 für Virtual Switch Tagging ein. ■ **VLAN-Trunking**: Verwenden Sie diese Option für das Virtual Guest Tagging und um VLAN-Datenverkehr mit einer ID an das Gastbetriebssystem weiterzuleiten. Geben Sie einen VLAN-Trunk-Bereich ein. Sie können mithilfe einer kommagetrennten Liste mehrere Bereiche oder individuelle VLANs festlegen. Beispiel: `1702-1705, 1848-1849`. ■ **Privates VLAN**: Ordnen Sie den Datenverkehr einem privaten VLAN zu, das auf dem Distributed Switch erstellt wurde. Wenn Sie keine privaten VLANs erstellt haben, bleibt dieses Menü leer.
Erweitert	Lassen Sie diese Option unausgewählt.

8 Überprüfen Sie auf der Seite **Bereit zum Abschließen** die Konfiguration und klicken Sie auf **Beenden**.

Ergebnisse

Der Distributed Switch wird erstellt und verteilte Portgruppen werden unter dem Distributed Switch angezeigt.

Bereitstellen und Konfigurieren von NSX Manager

Verwenden Sie den vSphere Client zum Bereitstellen des NSX Manager im vSphere-Cluster. Sie können dann den NSX Manager konfigurieren und verwenden, um Ihre NSX-Umgebung zu verwalten.

Voraussetzungen

- - Vergewissern Sie sich, dass Ihre Umgebung die Netzwerkanforderungen erfüllt. Siehe Anforderungen für Zonal Supervisor mit NSX und NSX Advanced Load Balancer und Anforderungen für die Cluster Supervisor-Bereitstellung mit NSX und NSX Advanced Load Balancer in *Konzepte und Planung der vSphere IaaS-Steuerungsebene* für Informationen zu den Anforderungen.
- Vergewissern Sie sich, dass die erforderlichen Ports geöffnet sind. Weitere Informationen zu Ports und Protokollen finden Sie im *Installationshandbuch für NSX*.

Verfahren

1. Suchen Sie die OVA-Datei von NSX im VMware-Download-Portal.

   Kopieren Sie entweder die Download-URL oder laden Sie die OVA-Datei herunter.
2. Klicken Sie mit der rechten Maustaste und wählen Sie **OVF-Vorlage bereitstellen** aus, um den Installationsassistenten zu starten.
3. Geben Sie auf der Registerkarte **OVF-Vorlage auswählen** die OVA-Download-URL ein oder navigieren Sie zur OVA-Datei.
4. Geben Sie auf der Registerkarte **Namen und Ordner auswählen** einen Namen für die NSX Manager-VM ein.
5. Wählen Sie auf der Registerkarte **Computing-Ressource auswählen** den vSphere-Cluster aus, in dem der NSX Manager bereitgestellt werden soll.
6. Klicken Sie auf **Weiter**, um die Details zu überprüfen.
7. Wählen Sie auf der Registerkarte **Konfiguration** die NSX-Bereitstellungsgröße aus.
8. Wählen Sie auf der Registerkarte **Speicher auswählen** den freigegebenen Speicher für die Bereitstellung aus.
9. Aktivieren Sie Thin Provisioning, indem Sie unter **Format für die virtuelle Festplatte auswählen** die Option **Thin Provision** auswählen.

   Die virtuellen Festplatten werden standardmäßig per Thick Provisioning bereitgestellt.

10 Wählen Sie auf der Registerkarte **Netzwerke auswählen** unter **Zielnetzwerk** die Verwaltungsportgruppe oder das Zielnetzwerk für den NSX Manager aus.

   Beispiel: `DPortGroup-MGMT`.

11 Geben Sie auf der Registerkarte **Vorlage anpassen** das System-Root-, CLI-Administrator- und das Überwachungskennwort für den NSX Manager ein. Ihre Kennwörter müssen den Einschränkungen für die Kennwortsicherheit entsprechen.

   - Mindestens 12 Zeichen.
   - Mindestens ein Kleinbuchstabe.
   - Mindestens ein Großbuchstabe.
   - Mindestens eine Ziffer.
   - Mindestens ein Sonderzeichen.
   - Mindestens fünf verschiedene Zeichen.
   - Standardmäßig werden die Komplexitätsregeln des Kennworts durch das Linux PAM-Modul erzwungen.

12 Geben Sie für das IPv4-Gateway, die IPv4-Adresse des Verwaltungsnetzwerks, die Netzmaske des Verwaltungsnetzwerks, den DNS-Server, die Domänensuchliste und die NTP-IP-Adresse jeweils die Standardwerte ein.

13 Aktivieren Sie SSH und lassen Sie die Root-SSH-Anmeldung bei der NSX Manager-Befehlszeile zu.

   Die SSH-Optionen sind aus Sicherheitsgründen standardmäßig deaktiviert.

14 Stellen Sie sicher, dass Ihre benutzerdefinierte OVF-Vorlagenspezifikation korrekt ist, und klicken Sie auf **Beenden**, um die Installation zu initiieren.

15 Melden Sie sich nach dem Start von NSX Manager als Administrator bei der CLI an und führen Sie den Befehl `get interface eth0` aus, um zu überprüfen, ob die IP-Adresse erwartungsgemäß angewendet wurde.

16 Geben Sie den Befehl `get services` ein, um zu überprüfen, ob alle Dienste ausgeführt werden.

Bereitstellen von NSX Manager-Knoten zur Bildung eines Clusters

Ein NSX Manager-Cluster bietet Hochverfügbarkeit. Sie können NSX Manager-Knoten über die Benutzeroberfläche nur auf ESXi-Hosts bereitstellen, die von vCenter Server verwaltet werden. Um einen NSX Manager-Cluster zu erstellen, stellen Sie zwei zusätzliche Knoten bereit, um einen Cluster mit insgesamt drei Knoten zu bilden. Wenn Sie einen neuen Knoten über die Benutzeroberfläche bereitstellen, stellt der Knoten zur Bildung eines Clusters eine Verbindung zum ersten bereitgestellten Knoten her. Alle Repository-Details und das Kennwort des ersten bereitgestellten Knotens werden mit dem neu bereitgestellten Knoten synchronisiert.

Voraussetzungen

- Vergewissern Sie sich, dass ein NSX Manager-Knoten installiert ist.
- Vergewissern Sie sich, dass ein Compute Manager konfiguriert ist.
- Vergewissern Sie sich, dass die erforderlichen Ports geöffnet sind.
- Vergewissern Sie sich , dass ein Datenspeicher auf dem ESXi-Host konfiguriert ist.
- Vergewissern Sie sich, dass Sie über die IP-Adresse und das IP-Gateway, die DNS-Server-IP-Adressen, die Domänensuchliste und die NTP-Server-IP-Adresse verfügen, die vom NSX Manager verwendet werden sollen.
- Vergewissern Sie sich, dass Sie über ein Portgruppennetzwerk für die Ziel-VM verfügen. Platzieren Sie die NSX-Appliances in einem VM-Verwaltungsnetzwerk.

Verfahren

1 Melden Sie sich in einem Browser unter https://<manager-ip-address> mit Administratorrechten beim NSX Manager an.

2 Wählen Sie zum Bereitstellen einer Appliance **System > Appliances > NSX-Appliance hinzufügen** aus.

3 Geben Sie die Appliance-Details ein.

Option	Beschreibung
Hostname	Geben Sie den Hostnamen oder den FQDN ein, der für den Knoten verwendet werden soll.
Verwaltungs-IP/Netzmaske	Geben Sie eine IP-Adresse ein, die dem Knoten zugewiesen werden soll.
Verwaltungs-Gateway	Geben Sie eine Gateway-IP-Adresse ein, die vom Knoten verwendet werden soll.
DNS-Server	Geben Sie die Liste der DNS-Server-IP-Adressen ein, die vom Knoten verwendet werden sollen.
NTP-Server	Geben Sie die Liste der NTP-Server-IP-Adressen ein.
Knotengröße	Wählen Sie aus den verfügbaren Optionen den Formfaktor **Mittel (6 vCPUs, 24 GB RAM, 300 GB Speicher)**.

4 Geben Sie die Appliance-Konfigurationsdetails ein.

Option	Beschreibung
Compute Manager	Wählen Sie den vCenter Server aus, den Sie als Compute Manager konfiguriert haben.
Computing-Cluster	Wählen Sie den Cluster aus, dem der Knoten beitreten muss.
Datenspeicher	Wählen Sie einen Datenspeicher für die Knotendateien aus.

Option	Beschreibung
Format für die virtuelle Festplatte	Wählen Sie das Format **Thin Provision** aus.
Netzwerk	Klicken Sie auf **Netzwerk auswählen**, um das Verwaltungsnetzwerk für den Knoten auszuwählen.

5 Geben Sie die Details für den Zugriff und die Anmeldedaten ein.

Option	Beschreibung
Aktivieren von SSH	Schalten Sie die Umschaltfläche so um, dass eine SSH-Anmeldung beim neuen Knoten zulässig ist.
Zulassen von Root-Zugriff	Schalten Sie die Umschaltfläche so um, dass ein Root-Zugriff auf den neuen Knoten zulässig ist.
System-Root-Anmeldedaten	Legen Sie das Root-Kennwort für den neuen Knoten fest und bestätigen Sie es. Ihr Kennwort muss den Einschränkungen für die Kennwortsicherheit entsprechen. ■ Mindestens 12 Zeichen. ■ Mindestens ein Kleinbuchstabe. ■ Mindestens ein Großbuchstabe. ■ Mindestens eine Ziffer. ■ Mindestens ein Sonderzeichen. ■ Mindestens fünf verschiedene Zeichen. ■ Standardmäßig werden die Komplexitätsregeln des Kennworts durch das Linux PAM-Modul erzwungen.
Administrator-CLI- und Überwachungs-CLIAnmeldedaten	Aktivieren Sie das Kontrollkästchen **Identisch mit Root-Kennwort**, um dasselbe Kennwort zu verwenden, das Sie für „Root“ konfiguriert haben, oder deaktivieren Sie das Kontrollkästchen und legen Sie ein anderes Kennwort fest.

6 Klicken Sie auf **Appliance installieren**.

Der neue Knoten ist bereitgestellt. Sie können den Bereitstellungsvorgang auf der Seite **System > > Appliances** nachverfolgen. Fügen Sie keine weiteren Knoten hinzu, bis die Installation abgeschlossen und der Cluster stabil ist.

7 Warten Sie, bis die Bereitstellung, die Clusterbildung und die Repository-Synchronisierung abgeschlossen sind.

Der Beitritts- und der Clusterstabilisierungsvorgang können zwischen 10 und 15 Minuten in Anspruch nehmen. Vergewissern Sie sich, dass der Status jeder Clusterdienstgruppe `UP` ist, bevor Sie andere Clusteränderungen vornehmen.

8 Melden Sie sich nach dem Start des Knotens als Administrator bei der CLI an und führen Sie den Befehl `get interface eth0` aus, um zu überprüfen, ob die IP-Adresse erwartungsgemäß angewendet wurde.

9 Wenn Ihr Cluster nur zwei Knoten aufweist, fügen Sie eine weitere Appliance hinzu. Wählen Sie **System > Appliances > NSX-Appliance hinzufügen** aus und wiederholen Sie die Konfigurationsschritte.

Hinzufügen einer Lizenz

Fügen Sie eine Lizenz mithilfe von NSX Manager hinzu.

Voraussetzungen

Rufen Sie eine Advanced- oder höhere NSX-Lizenz ab.

Verfahren

1 Melden Sie sich beim NSX Manager an.

2 Wählen Sie **System > Lizenzen > Hinzufügen** aus.

3 Geben Sie den Lizenzschlüssel ein.

4 Klicken Sie auf **Hinzufügen**.

Hinzufügen eines Compute Managers

Ein Compute Manager ist eine Anwendung, die Ressourcen wie Hosts und virtuelle Maschinen verwaltet. Konfigurieren Sie den vCenter Server, der dem NSX als Compute Manager im NSX Manager zugeordnet ist.

Weitere Informationen finden Sie im *Administratorhandbuch für NSX*.

Verfahren

1 Melden Sie sich beim NSX Manager an.

2 Wählen Sie **System > Fabric > Compute Manager > Hinzufügen** aus.

3 Geben Sie die Details zum Compute Manager ein.

Option	Beschreibung
Name und Beschreibung	Geben Sie den Namen und die Beschreibung von vCenter Server ein.
Typ	Der Standardtyp ist VMware vCenter.
Multi-NSX	Lassen Sie diese Option unausgewählt. Mit der Multi-NSX-Option können Sie denselben vCenter Server bei mehreren NSX-Managern registrieren. Diese Option wird auf Supervisor- und vSphere Lifecycle Manager-Clustern nicht unterstützt.
FQDN oder IP-Adresse	Geben Sie den FQDN oder die IP-Adresse von vCenter Server ein.
HTTPS-Port des Reverse-Proxys	Der Standardport ist 443. Wenn Sie einen anderen Port verwenden, stellen Sie sicher, dass der Port auf allen NSX Manager-Appliances offen ist. Legen Sie den Reverse-Proxy-Port zum Registrieren von Compute Manager in NSX fest.

Option	Beschreibung
Benutzername und Kennwort	Geben Sie die vCenter Server-Anmeldedaten ein.
SHA-256-Fingerabdruck	Geben Sie den Wert für den vCenter Server-SHA-256-Fingerabdruckalgorithmus ein.

Sie können die Standardwerte für die anderen Einstellungen beibehalten.

Wenn Sie den Fingerabdruckwert leer lassen, werden Sie aufgefordert, den vom Server bereitgestellten Fingerabdruck zu akzeptieren. Nachdem Sie den Fingerabdruck akzeptiert haben, dauert es einige Sekunden, bis NSX die vCenter-Ressourcen ermittelt und registriert.

4 Wählen Sie **Vertrauensstellung aktivieren** aus, damit vCenter Server mit NSX kommunizieren kann.

5 Wenn Sie keinen Fingerabdruckwert für NSX Manager angeben, identifiziert das System den Fingerabdruck und zeigt ihn an.

6 Klicken Sie auf **Hinzufügen**, um den Fingerabdruck zu akzeptieren.

Ergebnisse

Nach einiger Zeit wird der Compute Manager bei vCenter Server registriert, und der Verbindungsstatus wechselt zu `Aktiv`. Wenn sich der FQDN/die PNID von vCenter Server ändert, müssen Sie sie beim NSX Manager erneut registrieren. Weitere Informationen finden Sie unter vCenter Server bei NSX Manager erneut registrieren.

Hinweis Nachdem vCenter Server erfolgreich registriert wurde, müssen Sie zuerst den Compute Manager löschen, bevor Sie die NSX Manager-VM ausschalten und löschen. Andernfalls können Sie beim Bereitstellen einer neuen NSX Manager-Instanz dieselbe vCenter Server-Instanz nicht wieder registrieren. Sie erhalten eine Fehlermeldung, dass vCenter Server bereits bei einer anderen NSX Manager-Instanz registriert ist.

Sie können auf den Namen des Compute Managers klicken, um die Details anzuzeigen, den Compute Manager zu bearbeiten oder Tags zu verwalten, die auf den Compute Manager angewendet wurden.

Erstellen von Transportzonen

Transportzonen geben an, welche Hosts und VMs ein bestimmtes Netzwerk verwenden können. Eine Transportzone kann sich über einen oder mehrere Host-Cluster erstrecken.

Sie verwenden die Standardtransportzonen oder erstellen die folgenden Zonen:

- Eine Overlay-Transportzone, die von den Supervisor Control Plane-VMs für die Verwaltungsnetzwerkkonnektivität zwischen NSX Advanced Load Balancer Controller und den Dienst-Engines verwendet wird.
- Eine VLAN-Transportzone für die NSX Edge-Knoten, die für Uplinks mit dem physischen Netzwerk verwendet werden sollen.

Verfahren

1 Melden Sie sich beim NSX Manager an.

2 Wählen Sie **System > Fabric > Transportzonen > TRANSPORTZONE HINZUFÜGEN**.

3 Geben Sie einen Namen für die Transportzone und optional eine Beschreibung ein. Zum Beispiel: **`overlayTZ`**.

4 Wählen Sie den Datenverkehrstyp **Overlay**.

   Die folgenden Transportzonen sind standardmäßig vorhanden:

   - Eine VLAN-Transportzone mit dem Namen `nsx-vlan-transportzone`.
   - Eine Overlay-Transportzone mit dem Namen `nsx-overlay-transportzone`.

5 Klicken Sie auf **SPEICHERN**.

6 Wiederholen Sie die Schritte 2 bis 5, um eine Transportzone mit dem Namen **`vlanTZ`** und dem Datenverkehrstyp **VLAN** zu erstellen.

7 (Optional) Geben Sie einen oder mehrere Namen für die Uplink-Teaming-Richtlinie ein.

   Die an die Transportzonen angehängten Segmente verwenden diese benannten Teaming-Richtlinien. Wenn die Segmente keine übereinstimmende benannte Teaming-Richtlinie finden, wird die standardmäßige Uplink-Teaming-Richtlinie verwendet.

Ergebnisse

Die von Ihnen erstellten Transportzonen werden auf der Seite **Transportzonen** angezeigt.

Erstellen eines IP-Pools für die IP-Adressen von Hosttunnel-Endpoints

Erstellen Sie IP-Pools für die ESXi-Hosttunnel-Endpoints (TEPs). TEPs sind die Quell- und Ziel-IP-Adressen, die in der externen IP-Kopfzeile verwendet werden, um die ESXi-Hosts zu identifizieren, bei denen die NSX-Kapselung von Overlay-Frames beginnt und endet.

Verfahren

1 Melden Sie sich beim NSX Manager an.

2 Wählen Sie **Netzwerk > IP-Adresspools > IP-ADRESSENPOOL HINZUFÜGEN** aus.

3 Geben Sie einen Namen und optional eine Beschreibung für den IP-Adresspool ein. Beispiel: `ESXI-TEP-IP-POOL`.

4 Klicken Sie auf **Festlegen**.

5 Wählen Sie **IP-Bereiche** aus dem Dropdown-Menü **SUBNETZ FESTLEGEN** aus.

6 Geben Sie die folgenden Details zum IP-Adressen-Pool ein:

Option	Beschreibung
IP-Bereiche	Geben Sie den IP-Zuteilungsbereich ein. Beispielsweise `IPv4 Range - 192.168.12.1-192.168.12.60, IPv6 Range - 2001:800::0001-2001:0fff:ffff:ffff:ffff:ffff:ffff:ffff`
CIDR	Geben Sie die Netzwerkadresse in einer CIDR-Notation ein. Beispiel: `192.23.213.0/24`.

7 Geben Sie optional die folgenden Details ein.

Option	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für den IP-Bereich ein.
Gateway-IP	Geben Sie die Gateway-IP-Adresse ein. Beispiel: `192.23.213.253`.
DNS-Server	Geben Sie die Adresse des DNS-Servers ein.
DNS-Suffix	Geben Sie das DNS-Suffix ein.

8 Klicken Sie auf **HINZUFÜGEN** und **ÜBERNEHMEN**.

9 Klicken Sie auf **SPEICHERN**.

Ergebnisse

Stellen Sie sicher, dass die von Ihnen erstellten TEP-IP-Pools auf der Seite IP-Pool angezeigt werden.

Erstellen eines IP-Pools für Edge-Knoten

Erstellen Sie IP-Pools für die Edge-Knoten. Die TEP-Adressen müssen nicht routingfähig sein. Sie können ein beliebiges IP-Adressschema verwenden, mit dem der Edge-TEP mit dem Host-TEP kommunizieren kann.

Verfahren

1 Melden Sie sich beim NSX Manager an.

2 Wählen Sie **Netzwerk > IP-Adresspools > IP-ADRESSENPOOL HINZUFÜGEN** aus.

3 Geben Sie einen Namen und optional eine Beschreibung für den IP-Adresspool ein. Zum Beispiel: **`EDGE-TEP-IP-POOL`**.

4 Klicken Sie auf **Festlegen**.

5 Geben Sie die folgenden Details zum IP-Adressen-Pool ein:

Option	Beschreibung
IP-Bereiche	Geben Sie den IP-Zuteilungsbereich ein. Beispielsweise `IPv4 Range - 192.168.12.1-192.168.12.60, IPv6 Range - 2001:800::0001-2001:0fff:ffff:ffff:ffff:ffff:ffff:ffff`
CIDR	Geben Sie die Netzwerkadresse in einer CIDR-Notation ein. Beispiel: `192.23.213.0/24`.

6 Geben Sie optional die folgenden Details ein.

Option	Beschreibung
Beschreibung	Geben Sie eine Beschreibung für den IP-Bereich ein.
Gateway-IP	Geben Sie die Gateway-IP-Adresse ein. Beispiel: `192.23.213.253`.
DNS-Server	Geben Sie die Adresse des DNS-Servers ein.
DNS-Suffix	Geben Sie das DNS-Suffix ein.

7 Klicken Sie auf **HINZUFÜGEN** und **ÜBERNEHMEN**.

8 Klicken Sie auf **SPEICHERN**.

Ergebnisse

Stellen Sie sicher, dass die von Ihnen erstellten IP-Pools auf der Seite IP-Pool angezeigt werden.

Erstellen eines ESXi Host-Uplink-Profils

Ein Host-Uplink-Profil definiert Richtlinien für die Uplinks von den ESXi-Hosts zu NSX-Segmenten.

Verfahren

1 Melden Sie sich beim NSX Manager an.

2 Wählen Sie **System > Fabric > Profile > Uplink-Profile > PROFIL HINZUFÜGEN**.

3 Geben Sie einen Namen und optional eine Beschreibung für das Uplink-Profil ein.

Zum Beispiel: **`ESXI-UPLINK-PROFIL`**.

4 Klicken Sie im Abschnitt **Teaming** auf **HINZUFÜGEN**, um eine Teaming-Richtlinie für die Benennung hinzuzufügen, und konfigurieren Sie eine **FAILOVER_ORDER**-Richtlinie.

Eine Liste der aktiven Uplinks wird angegeben, und jede Schnittstelle auf dem Transportknoten ist an einen aktiven Uplink gebunden. Bei dieser Konfiguration können mehrere aktive Uplinks gleichzeitig verwendet werden.

5 Konfigurieren Sie aktive und Standby-Links.

Sie können z. B. **`uplink-1`** als aktiven Uplink und **`uplink-2`** als Standby-Uplink konfigurieren.

6 (Optional) Geben Sie einen Wert für das Transport-VLAN ein. Zum Beispiel: **1060**.

   Das in den Tags des Uplink-Profils festgelegte Transport-VLAN überlagert den Datenverkehr, und die VLAN-ID wird vom Tunnel-Endpoint (TEP) verwendet.

7 Geben Sie den MTU-Wert ein. Der Wert muss mindestens 1600 betragen, darf aber nicht höher sein als der MTU-Wert auf den physischen Switches und dem vSphere Distributed Switch.

   NSX verwendet den globalen MTU-Standardwert 1700.

Ergebnisse

Zeigen Sie den Uplink auf der Seite **Uplink-Profil** an.

Erstellen eines NSX Edge-Uplink-Profils

Ein Uplink ist ein Link von den NSX Edge-Knoten zu den logischen NSX-Switches. Ein Uplink-Profil definiert Richtlinien für die Uplinks, indem Gruppierungsrichtlinien, aktive und Standby-Links, Transport-VLAN-ID und MTU-Wert festgelegt werden.

Erstellen Sie ein Uplink-Profil mit der Teaming-Richtlinie für die Failover-Reihenfolge mit einem aktiven Uplink für Overlay-Datenverkehr der Edge-VM.

Verfahren

1 Melden Sie sich beim NSX Manager an.

2 Wählen Sie **System > Fabric > Profile > Uplink-Profile > PROFIL HINZUFÜGEN > .**.

3 Geben Sie einen Namen und optional eine Beschreibung für das Uplink-Profil ein.

   Zum Beispiel: **EDGE-UPLINK-PROFIL**.

4 Klicken Sie im Abschnitt **Teaming** auf **HINZUFÜGEN**, um eine Teaming-Richtlinie für die Benennung hinzuzufügen, und konfigurieren Sie eine **FAILOVER_ORDER**-Richtlinie.

   Eine Liste der aktiven Uplinks wird angegeben, und jede Schnittstelle auf dem Transportknoten ist an einen aktiven Uplink gebunden. Bei dieser Konfiguration können mehrere aktive Uplinks gleichzeitig verwendet werden.

5 Konfigurieren Sie einen aktiven Uplink.

   Konfigurieren Sie z. B. **uplink-1** als aktiven Uplink.

Ergebnisse

Zeigen Sie den Uplink auf der Seite **Uplink-Profil** an.

Erstellen eines Transportknotenprofils

Ein Transportknotenprofil definiert, wie NSX auf den Hosts in einem bestimmten Cluster, an den das Profil angehängt ist, installiert und konfiguriert ist. Erstellen Sie ein Transportknotenprofil, bevor Sie ESXi-Cluster als Transportknoten vorbereiten.

Hinweis Transportknotenprofile gelten nur für Hosts. Sie können nicht auf NSX-Edge-Transportknoten angewendet werden.

Voraussetzungen

- Stellen Sie sicher, dass ein Cluster verfügbar ist. Weitere Informationen finden Sie unter Bereitstellen von NSX Manager-Knoten zur Bildung eines Clusters.
- Erstellen Sie eine Overlay-Transportzone. Weitere Informationen finden Sie unter Erstellen von Transportzonen.
- Konfigurieren Sie einen IP-Pool. Weitere Informationen finden Sie unter Erstellen eines IP-Pools für die IP-Adressen von Hosttunnel-Endpoints.
- Fügen Sie einen Compute Manager hinzu. Weitere Informationen finden Sie unter Hinzufügen eines Compute Managers.

Verfahren

1. Melden Sie sich beim NSX Manager an.
2. Wählen Sie **System > Fabric > Hosts** aus.
3. Wählen Sie auf der Seite **Hosts** die Option **Transportknotenprofil > TRANSPORTKNOTENPROFIL HINZUFÜGEN** aus.
4. Geben Sie einen Namen für das Transportknotenprofil ein. Zum Beispiel: **`HOST-TRANSPORTKNOTENPROFIL`**.

   Sie können optional die Beschreibung über das Transportknotenprofil hinzufügen.
5. Wählen Sie im Feld **Host-Switch** die Option **Festlegen** aus.
6. Geben Sie im Fenster **Host-Switch** die Switch-Details ein.

Option	Beschreibung
vCenter	Aktivieren Sie den vCenter Server.
Typ	Wählen Sie den Switch-Typ aus, der auf dem Host konfiguriert wird. Wählen Sie **VDS** aus.
vDS	Wählen Sie einen VDS aus, der unter dem ausgewählten vCenter Server erstellt wird. Zum Beispiel: **`wcp_vds_1`**.
Transportzonen	Wählen Sie die zuvor erstellte Overlay-Transportzone aus. Zum Beispiel: **`overlayTZ`**.
Uplink-Profil	Wählen Sie das zuvor erstellte Host-Uplink-Profil aus. Zum Beispiel: **`ESXI-UPLINK-PROFIL`**.

Option	Beschreibung
IP-Adresstyp	Wählen Sie **`Ipv4`** aus.
IPv4-Zuweisung	Wählen Sie **`IP-Pool verwenden`** aus.
IPv4-Pool	Wählen Sie den zuvor erstellten Host-TEP-Pool aus. Zum Beispiel: **`ESXI-TEP-IP-POOL`**.
Uplink-Zuordnung für Teaming-Richtlinie	Klicken Sie auf **Hinzufügen** und ordnen Sie die im NSX-Uplink-Profil definierten Uplinks den vSphere Distributed Switch Uplinks zu. Ordnen Sie beispielsweise **`uplink-1 Uplink 1`** und **`uplink-2 Uplink 2`** zu.

7 Klicken Sie auf **HINZUFÜGEN** und **ÜBERNEHMEN**.

8 Klicken Sie auf **SPEICHERN**, um die Konfiguration zu speichern.

Ergebnisse

Das von Ihnen erstellte Profil ist auf der Seite **Transportknotenprofile** aufgelistet.

Erstellen eines NSX Edge-Clusterprofils

Erstellen Sie ein NSX Edge-Clusterprofil, das die Richtlinien für den NSX Edge-Transportknoten definiert.

Voraussetzungen

Stellen Sie sicher, dass der NSX Edge-Cluster verfügbar ist.

Verfahren

1 Melden Sie sich beim NSX Manager an.

2 Wählen Sie **System > Fabric > Profile > Edge-Clusterprofile > PROFIL HINZUFÜGEN > .**.

3 Geben Sie die NSX Edge-Cluster-Profildetails ein.

4 Geben Sie einen Profilnamen für den NSX Edge-Cluster ein. Zum Beispiel: **`Clusterprofil – 1`**.

   Geben Sie optional eine Beschreibung ein.

5 Behalten Sie die Standardwerte für die anderen Einstellungen bei.

6 Klicken Sie auf **Hinzufügen**.

Konfigurieren von NSX im Cluster

Um NSX zu installieren und die Overlay-TEPs vorzubereiten, wenden Sie das Transportknotenprofil auf den vSphere-Cluster an.

Voraussetzungen

Stellen Sie sicher, dass Sie ein Transportknotenprofil erstellt haben.

Verfahren

1 Melden Sie sich beim NSX Manager an.

2 Wählen Sie **System > Fabric > Knoten > Host-Transportknoten** aus.

3 Wählen Sie im Dropdown-Menü **Verwaltet von** eine vorhandene vCenter Server-Instanz aus.

Auf der Seite werden die verfügbaren vSphere-Cluster aufgelistet.

4 Wählen Sie den Computing-Cluster aus, in dem Sie NSX konfigurieren möchten.

5 Klicken Sie auf **NSX konfigurieren**.

6 Wählen Sie das zuvor erstellte Transportknotenprofil aus und klicken Sie auf **Übernehmen**.

Beispiel: `HOST-TRANSPORT-NODE-PROFILE`.

7 Stellen Sie auf der Seite **Host-Transportknoten** sicher, dass der Konfigurationszustand von NSX `Success` und der NSX Manager-Konnektivitätsstatus der Hosts im Cluster `Up` ist.

Ergebnisse

Das zuvor erstellte Transportknotenprofil wird auf den vSphere-Cluster angewendet, um NSX zu installieren und die Overlay-TEPs vorzubereiten.

Erstellen eines NSX Edge-Transportknotens

Sie können der NSX-Fabric eine NSX Edge-VM hinzufügen und sie dann als NSX Edge-Transportknoten-VM konfigurieren.

Voraussetzungen

Stellen Sie sicher, dass Sie Transportzonen, das Edge-Uplink-Profile und den Edge-TEP-IP-Pool erstellt haben.

Verfahren

1 Melden Sie sich beim NSX Manager an.

2 Wählen Sie **System > Fabric > Knoten > Edge-Transportknoten > EDGE-KNOTEN HINZUFÜGEN** aus.

3 Geben Sie unter **Name und Beschreibung** einen Namen für den NSX Edge-Knoten ein.

Beispielsweise `nsx-edge-1`

4 Geben Sie den Hostnamen oder den FQDN aus vCenter Server ein.

Beispiel: `nsx-edge-1.lab.com`.

5 Wählen Sie den Formfaktor für die NSX Edge-VM-Appliance aus.

6 Geben Sie unter **Anmeldedaten** das CLI- und das Root-Kennwort für die NSX Edge ein. Ihre Kennwörter müssen den Einschränkungen für die Kennwortsicherheit entsprechen.

- Mindestens 12 Zeichen.

- Mindestens ein Kleinbuchstabe.
- Mindestens ein Großbuchstabe.
- Mindestens eine Ziffer.
- Mindestens ein Sonderzeichen.
- Mindestens fünf verschiedene Zeichen.
- Standardmäßig werden die Komplexitätsregeln des Kennworts durch das Linux PAM-Modul erzwungen.

7 Aktivieren Sie die Option **SSH-Anmeldung zulassen** für die CLI- und die Root-Anmeldedaten.

8 Konfigurieren Sie unter **Bereitstellung konfigurieren** die folgenden Eigenschaften:

Option	Beschreibung
Compute Manager	Wählen Sie im Dropdown-Menü den Compute Manager aus. Wählen Sie z. B. `vCenter` aus.
Cluster	Wählen Sie im Dropdown-Menü den Cluster aus. Wählen Sie z. B. `Compute-Cluster` aus.
Datenspeicher	Wählen Sie den gemeinsam genutzten Datenspeicher aus der Liste aus. Beispiel: `vsanDatastore`.

9 Konfigurieren Sie die Knoteneinstellungen.

Option	Beschreibung
IP-Zuweisung	Wählen Sie „Statisch“ aus. Geben Sie Werte für folgende Elemente ein: ■ **Verwaltungs-IP**: Geben Sie die IP-Adresse im selben VLAN ein, in dem sich das vCenter Server-Verwaltungsnetzwerk befindet. Beispiel: `10.197.79.146/24`. ■ **Standard-Gateway**: Das Standard-Gateway des Verwaltungsnetzwerks. Beispiel: `10.197.79.253`.
Verwaltungsschnittstelle	Klicken Sie auf **Schnittstelle auswählen** und wählen Sie im zuvor von Ihnen erstellten Dropdown-Menü die vSphere Distributed Switch-Portgruppe im selben VLAN aus, in dem sich das Verwaltungsnetzwerk befindet. Beispiel: `DPortGroup-MGMT`.

10 Klicken Sie unter **NSX konfigurieren** auf **Switch hinzufügen**, um die Switch-Eigenschaften zu konfigurieren.

11 Verwenden Sie für **Edge-Switchname** den Standardnamen.

Beispiel: `nvds1`.

12 Wählen Sie die Transportzone aus, zu der der Transportknoten gehört.

Wählen Sie die zuvor erstellten Overlay-Transportzonen aus.

Beispiel: `overlayTZ`.

13 Wählen Sie das zuvor erstellte Edge-Uplink-Profil aus.

Beispiel: `EDGE-UPLINK-PROFILE`.

14 Wählen Sie unter **IP-Zuweisung** die Option **IP-Pool verwenden** aus.

15 Wählen Sie den zuvor erstellten Edge-TEP-IP-Pool aus.

Beispiel: `EDGE-TEP-IP-POOL`.

16 Ordnen Sie im Abschnitt **Switch-Zuordnung für Teaming- Uplinks** den Uplink den zuvor erstellten Edge-Uplink-Profilen zu.

Wählen Sie beispielsweise für `Uplink1` `uplink-1` aus.

17 Wiederholen Sie die Schritte 10 – 16, um einen neuen Switch hinzuzufügen.

Konfigurieren Sie beispielsweise die folgenden Werte:

Eigenschaft	Wert
Name des Edge-Switch	`nvds2`
Transportzone	`vlanTZ`
Edge-Uplink-Profil	`EDGE-UPLINK-PROFILE`
Switch-Zuordnung für Teaming-Richtlinien	`DPortGroup-EDGE-UPLINK`

18 Klicken Sie auf **Beenden**.

19 Wiederholen Sie die Schritte 2 – 18 für eine zweite NSX Edge-VM.

20 Sehen Sie sich auf der Seite **Edge-Transportknoten** den Verbindungsstatus an.

Erstellen eines NSX Edge-Clusters

Um sicherzustellen, dass immer mindestens eine NSX Edge-Instanz verfügbar ist, erstellen Sie einen NSX Edge-Cluster.

Verfahren

1 Melden Sie sich beim NSX Manager an.

2 Wählen Sie **System > Fabric > Knoten > Edge-Cluster > Hinzufügen** aus.

3 Geben Sie den NSX Edge-Clusternamen ein.

Beispiel: `EDGECLUSTER1`.

4 Klicken Sie auf **SPEICHERN**.

5 Wählen Sie das NSX Edge-Clusterprofil, das Sie erstellt haben, im Dropdown-Menü aus. Zum Beispiel: **`Clusterprofil – 1`**.

6 Wählen Sie im Dropdown-Menü **Mitgliedstyp** den **Edge-Knoten** aus.

7 Wählen Sie in der Spalte **Verfügbar** die zuvor erstellten NSX Edge-VMs aus und klicken Sie auf den Pfeil nach rechts, um sie in die Spalte **Ausgewählt** zu verschieben.

8 Beispiele: `nsx-edge-1` und `nsx-edge-2`.

9 Klicken Sie auf **Speichern**.

Nächste Schritte

Erstellen eines Tier-0-Gateways

Das Tier-0-Gateway ist der logische NSX-Router, der der physischen Infrastruktur die Nord-Süd-Konnektivität für das logische NSX-Netzwerk bereitstellt. vSphere IaaS control plane unterstützt mehrere Tier-0-Gateways auf mehreren NSX Edge-Clustern in derselben Transportzone.

Weitere Informationen zum Konfigurieren von NSX-Route Maps auf dem Edge-Tier-0-Router finden Sie im *Betriebs- und Administratorhandbuch für VMware Cloud Foundation* auf https://docs.vmware.com/de/VMware-Cloud-Foundation/4.0/vcf-40-doc.zip.

Voraussetzungen

Stellen Sie sicher, dass Sie einen NSX Edge-Cluster erstellt haben.

Verfahren

1 Melden Sie sich beim NSX Manager an.

2 Wählen Sie **Netzwerk > Tier-0 Gateways** aus.

3 Klicken Sie auf **GATEWAY HINZUFÜGEN**.

4 Geben Sie einen Namen für das Tier-0-Gateway ein.

Beispiel: `ContainerT0`.

5 Wählen Sie einen Aktiv-Standby-HA-Modus aus.

Der Standardmodus lautet „Aktiv/Aktiv“. Im Aktiv-Standby-Modus verarbeitet das gewählte aktive Mitglied den gesamten Datenverkehr. Wenn das aktive Mitglied ausfällt, wird ein neues Mitglied als aktives Mitglied ausgewählt.

6 Wenn der HA-Modus Aktiv/Standby lautet, wählen Sie einen Failover-Modus aus.

Option	Beschreibung
Vorbeugend	Wenn der bevorzugte Knoten fehlschlägt und wiederhergestellt wird, hat er Vorrang vor seinem Peer und wird zum aktiven Knoten. Der Peer ändert seinen Zustand in Standby.
Nicht vorbeugend	Wenn der bevorzugte Knoten fehlschlägt und wiederhergestellt wird, erfolgt eine Überprüfung, ob der zugehörige Peer der aktive Knoten ist. Ist dies der Fall, hat der bevorzugte Knoten keinen Vorrang vor seinem Peer, und er ist der Standby-Knoten.

7 Wählen Sie den zuvor erstellten NSX Edge-Cluster aus.

   Wählen Sie z. B. `Cluster Profile - 1` aus.

8 Klicken Sie auf **Speichern**.

   Das Tier-0-Gateway wird erstellt.

9 Wählen Sie **Ja**, um mit der Konfiguration fortzufahren.

10 Konfigurieren Sie Schnittstellen.

   a Erweitern Sie **Schnittstellen** und klicken Sie auf **Festlegen**.

   b Klicken Sie auf **Schnittstelle hinzufügen**.

   c Geben Sie einen Namen ein.

      Geben Sie z. B. den Namen `TIER-0_VWT-UPLINK1` ein.

   d Wählen Sie für **Typ** die Option **Extern** aus.

   e Geben Sie eine IP-Adresse aus dem Uplink-VLAN des logischen Edge-Routers ein. Die IP-Adresse darf nicht mit der Verwaltungs-IP-Adresse identisch sein, die für die zuvor erstellten NSX Edge-VMs konfiguriert wurde.

      Beispiel: `10.197.154.1/24`.

   f Wählen Sie unter **Verbunden mit** das zuvor erstellte Tier-0-Uplink-Segment aus.

      Beispielsweise `TIER-0-LS-UPLINK`

   g Wählen Sie einen NSX Edge-Knoten aus der Liste aus.

      Beispiel: `nsx-edge-1`.

   h Klicken Sie auf **Speichern**.

   i Wiederholen Sie die Schritte a – h für die zweite Schnittstelle.

      Erstellen Sie beispielsweise einen zweiten Uplink `TIER-0_VWT-UPLINK2` mit der IP-Adresse `10.197.154.2/24`, der mit dem Edge-Knoten `nsx-edge-2` verbunden ist.

   j Klicken Sie auf **Schließen**.

11 Um High Availability zu konfigurieren, klicken Sie unter **HA-VIP-Konfiguration** auf **Festlegen**.

   a Klicken Sie auf **HA-VIP-KONFIGURATION HINZUFÜGEN**.

   b Geben Sie die IP-Adresse ein.

      Beispielsweise `10.197.154.3/24`

   c Wählen Sie die Schnittstellen aus.

      Beispiel: `TIER-0_WVT-UPLINK1` und `TIER-0_WVT-UPLINK2`

   d Klicken Sie auf **Hinzufügen** und **Übernehmen**.

12 Um Routing zu konfigurieren, klicken Sie auf **Routing**.

   a Klicken Sie unter „Statische Routen“ auf **Festlegen**.

   b Klicken Sie auf **STATISCHE ROUTE HINZUFÜGEN**.

   c Geben Sie einen Namen ein.

      Beispiel: `DEFAULT-STATIC-ROUTE`.

   d Geben Sie als Netzwerk-IP-Adresse `0.0.0.0/0` ein.

   e Um die nächsten Hops zu konfigurieren, klicken Sie auf **Nächste Hops festlegen** und **Nächsten Hop hinzufügen**.

   f Geben Sie die IP-Adresse des Routers für den nächsten Hop ein. In der Regel handelt es sich hierbei um das Standard-Gateway des VLAN des Verwaltungsnetzwerks aus dem Uplink-VLAN des logischen NSX Edge-Routers.

      Beispiel: `10.197.154.253`.

   g Klicken Sie auf **Hinzufügen** und **Übernehmen** und **SPEICHERN**.

   h Klicken Sie auf **Schließen**.

13 (Optional) Wählen Sie BGP aus, um lokale BGP- und Peer-Details zu konfigurieren.

14 Stellen Sie zum Überprüfen der Konnektivität sicher, dass ein externes Gerät in der physischen Architektur die von Ihnen konfigurierten Uplinks pingen kann.

Konfigurieren von NSX Route Maps auf dem Edge-Tier-0-Gateway

Wenn Sie vSphere IaaS control plane bereitstellen, enthalten die auf dem Edge-Tier-0-Gateway im eBGP-Modus erstellten Route Maps einen IP-Präfix mit nur einer Verweigerungsregel. Dadurch wird verhindert, dass Routen für die ToR-Switches angekündigt werden.

Wenn Sie den Edge-Cluster nur für das Kubernetes-Arbeitslastverwaltung verwenden, folgen Sie Option 1 und deaktivieren Sie Tier-1-Routenankündigungen. Wenn Sie den Edge-Cluster für zusätzliche Aufgaben verwenden, befolgen Sie Option 2 und erstellen Sie eine neue Zulassungsregel.

Option 1: Deaktivieren von Ankündigungen verbundener Tier-1-Netzwerke über Tier-0-Gateway

Netzwerke, die mit dem Tier-1-Gateway verbunden sind, werden vom Tier-0-Gateway für externe Netzwerke nicht angekündigt.

1 Melden Sie sich beim NSX Manager an.

2 Wählen Sie **Netzwerk > Tier-0 Gateways** aus.

3 Klicken Sie auf **Bearbeiten**.

4 Deaktivieren Sie im Bereich „Angekündigte Tier-1-Subnetze“ die Option **Verbundene Schnittstellen und Segmente**.

5 Klicken Sie auf **Anwenden** und dann auf **Speichern**.

Option 2: Erstellen einer neuen Zulassungsregel und Anwenden der Regel auf die Route Redistribution

Wenn Sie vSphere IaaS control plane bereitstellen, wird eine neue Verweigerungsregel an die Route Map angehängt. Daher müssen Sie der Route Map eine neue Genehmigungsregel hinzufügen, um jede IP-Präfixliste und Route Map zuzulassen und sie als letzte Regel auf die Route-Neuverteilungsregel anzuwenden.

1 Melden Sie sich beim NSX Manager an.

2 Wählen Sie **Netzwerk > Tier-0 Gateways** aus.

3 Erstellen Sie eine neue IP-Präfixliste.

   a Erweitern Sie **Routing**.

   b Klicken Sie neben „IP-Präfix-Listen“ auf „1“.

   c Klicken Sie im Dialogfeld „IP-Präfixliste festlegen“ auf **IP-Präfixliste hinzufügen**.

   d Geben Sie einen Namen ein, z. B. **`test`** und klicken Sie auf **Festlegen**.

   e Klicken Sie auf **Präfix hinzufügen**.

   f Klicken Sie unter „Netzwerk“ auf **Beliebig** und wählen Sie unter „Aktion“ die Option **Zulassen** aus.

   g Klicken Sie auf **Anwenden** und dann auf **Speichern**.

4 Erstellen Sie eine Route Map für die in Schritt 3 erstellte IP-Präfixliste.

   a Klicken Sie neben „Route Map“ auf **Festlegen**.

   b Klicken Sie auf **Route Map hinzufügen**.

   c Fügen Sie neue Übereinstimmungskriterien mit IP-Präfix hinzu.

   d Wählen Sie das in Schritt 3 erstellte IP-Präfix und die Aktion **Zulassen** aus.

   e Klicken Sie auf **Anwenden** und dann auf **Speichern**.

5 Wenden Sie die bearbeitete Route Map auf die Neuverteilung der Route an.

   a Erweitern Sie auf der Seite **Tier-0-Gateways** die Option **Route-Neuverteilung** und klicken Sie auf „Bearbeiten“.

   b Wählen Sie im Dropdown-Menü in der Spalte „Route Map“ die in Schritt 4 erstellte Route Map aus.

   c Klicken Sie auf **Anwenden** und dann auf **Speichern**.

Erstellen Sie ein Tier-1-Gateway

Ein Tier-1-Gateway ist in der Regel mit einem Tier-0-Gateway in Süd-Nord-Richtung oder mit Segmenten in Nord-Süd-Richtung verbunden.

Voraussetzungen

Vergewissern Sie sich, dass Sie ein Tier-0-Gateway erstellt haben.

Verfahren

1. Melden Sie sich beim NSX Manager an.
2. Wählen Sie **Netzwerk > Tier-1-Gateways** aus.
3. Klicken Sie auf **TIER-1-GATEWAY HINZUFÜGEN**.
4. Geben Sie einen Namen für das Gateway ein. Zum Beispiel: **`ContainerAviT1`**
5. Wählen Sie ein Tier-0-Gateway aus, das mit diesem Tier-1-Gateway verbunden werden soll. Zum Beispiel: **`ContainerT0`**.
6. Wählen Sie den NSX Edge-Cluster aus. Wählen Sie z. B. **`EDGECLUSTER1`** aus.
7. Nachdem Sie einen NSX Edge-Cluster ausgewählt haben, bietet Ihnen ein Umschalter die Möglichkeit, NSX Edge-Knoten auszuwählen.
8. Wählen Sie einen Failover-Modus aus oder akzeptieren Sie die Standardoption **Nicht präemptiv**.
9. Übernehmen Sie die Standardoptionen für die verbleibenden Einstellungen.
10. Klicken Sie auf **SPEICHERN**.
11. (Optional) Konfigurieren Sie Dienstschnittstellen, statische Routen und Multicast-Einstellungen. Sie können die Voreinstellung übernehmen.

Erstellen eines Tier-0-Uplink-Segments und eines Overlay-Segments

Das Tier-0-Uplink-Segment bietet die Nord-Süd-Konnektivität von NSX zur physischen Infrastruktur. Das Overlay-Segment stellt der Service Engine Management-Netzwerkkarte die IP-Adresse zur Verfügung.

Voraussetzungen

Vergewissern Sie sich, dass Sie ein Tier-0-Gateway erstellt haben.

Verfahren

1. Melden Sie sich beim NSX Manager an.
2. Wählen Sie **Netzwerk > Segmente > SEGMENT HINZUFÜGEN** aus.
3. Geben Sie einen Namen für das Segment ein.

   Beispiel: `TIER-0-LS-UPLINK`.
4. Wählen Sie die zuvor erstellte Transportzone aus.

   Wählen Sie z. B. `vlanTZ` aus.
5. Schalten Sie die Option **Administrativer Status** um, um sie zu aktivieren.

6 Geben Sie eine VLAN-ID des Tier-0-Gateways ein.

   Beispiel: `1089`.

7 Klicken Sie auf **Speichern**.

8 Wiederholen Sie die Schritte 2 bis 7, um ein Overlay-Segment, `nsxoverlaysegment` mit Transportzone, `nsx-overlay-transportzone` zu erstellen.

Installieren und Konfigurieren von NSX Advanced Load Balancer für vSphere IaaS control plane mit NSX

Wenn Sie NSX 4.1.1 oder höhere Versionen in Ihrer vSphere IaaS control plane-Umgebung verwenden, können Sie die NSX Advanced Load Balancer 22.1.4 oder höher installieren und konfigurieren.

- Stellen Sie sicher, dass Ihre Umgebung die Anforderungen zum Konfigurieren von vSphere IaaS control plane mit dem NSX Advanced Load Balancer erfüllt. Siehe Anforderungen für Zonal Supervisor mit NSX und NSX Advanced Load Balancer und Anforderungen für die Cluster Supervisor-Bereitstellung mit NSX und NSX Advanced Load Balancer in *Konzepte und Planung der vSphere IaaS-Steuerungsebene*.
- Installieren und Konfigurieren von. NSX.
- Laden Sie die NSX Advanced Load Balancer-OVA herunter. VMware stellt eine NSX Advanced Load Balancer-OVA-Datei zur Verfügung, die Sie in Ihrer vSphere-Umgebung bereitstellen, in der Sie die Arbeitslastverwaltung aktivieren. Laden Sie die neueste Version der OVA-Datei, die mit vSphere IaaS control plane unterstützt wird, über das VMware Customer Connect-Portal herunter.

Hinweis Die Verfahren in diesem Handbuch gelten für den NSX Advanced Load Balancer, der von vSphere IaaS control plane 8.0 Update 2 unterstützt wird. Möglicherweise sind höhere Versionen von NSX Advanced Load Balancer verfügbar, in denen die Workflows der Benutzeroberfläche unterschiedlich sein können.

Weitere Informationen zum NSX Advanced Load Balancer finden Sie in der Dokumentation zu VMware NSX Advanced Load Balancer.

Importieren der NSX Advanced Load Balancer-OVA in eine lokale Inhaltsbibliothek

Um das NSX Advanced Load Balancer OVA-Image zu speichern, erstellen Sie eine lokale Inhaltsbibliothek und importieren Sie die OVA in diese Bibliothek.

Das Erstellen einer lokalen Inhaltsbibliothek umfasst das Konfigurieren der Bibliothek, das Herunterladen der OVA-Dateien und das Importieren in die lokale Inhaltsbibliothek. Weitere Informationen finden Sie unter Verwenden von Inhaltsbibliotheken .

Voraussetzungen

Stellen Sie sicher, dass Sie die NSX Advanced Load Balancer-OVA heruntergeladen haben.

Erstellen Sie eine lokale Inhaltsbibliothek. Siehe Erstellen und Bearbeiten einer Inhaltsbibliothek.

Verfahren

1. Melden Sie sich über vSphere Client bei vCenter Server an.
2. Wählen Sie **Menü > Inhaltsbibliotheken** aus.
3. Klicken Sie in der Liste der **Inhaltsbibliotheken** auf den Link für den Namen der von Ihnen erstellten lokalen Inhaltsbibliothek. Beispiel: **NSX ALB**.
4. Klicken Sie auf **Aktionen**.
5. Wählen Sie **Element importieren** aus.
6. Wählen Sie im Fenster **Bibliothekselement importieren** die Option **Lokale Datei** aus.
7. Klicken Sie auf **Dateien hochladen**.
8. Wählen Sie die heruntergeladene OVA-Datei aus.
9. Klicken Sie auf **Import**.
10. Zeigen Sie den Bereich **Aktuelle Aufgaben** am unteren Rand der Seite an.
11. Überwachen Sie die Aufgabe **Inhalt eines Bibliothekselements abrufen** und stellen Sie sicher, dass sie erfolgreich **abgeschlossen** wurde.

Nächste Schritte

Stellen Sie den NSX Advanced Load Balancer-Controller bereit. Weitere Informationen hierzu finden Sie unter Bereitstellen des NSX Advanced Load Balancer-Controllers.

Bereitstellen der NSX Advanced Load Balancer Controller

Stellen Sie die NSX Advanced Load Balancer Controller-VM im Verwaltungsnetzwerk in Ihrer vSphere IaaS control plane-Umgebung bereit.

Voraussetzungen

- Stellen Sie sicher, dass Sie über ein Verwaltungsnetzwerk verfügen, auf dem der NSX Advanced Load Balancer bereitgestellt werden soll. Dabei kann es sich um einen vSphere Distributed Switch (vDS) oder einen vSphere Standard Switch (vSS) handeln.
- Stellen Sie sicher, dass Sie einen vDS-Switch und eine Portgruppe für das Datennetzwerk erstellt haben. Weitere Informationen hierzu finden Sie unter Erstellen eines vSphere Distributed Switch für einen Supervisor zwecks Verwendung mit NSX Advanced Load Balancer.
- Stellen Sie sicher, dass die Voraussetzungen erfüllt sind. Siehe Anforderungen für Zonal Supervisor mit NSX und NSX Advanced Load Balancer und Anforderungen für die Cluster Supervisor-Bereitstellung mit NSX und NSX Advanced Load Balancer in *Konzepte und Planung der vSphere IaaS-Steuerungsebene*.

Verfahren

1 Melden Sie sich über vSphere Client bei vCenter Server an.

2 Wählen Sie den vSphere-Cluster aus, der für Verwaltungskomponenten vorgesehen ist.

3 Erstellen Sie einen Ressourcenpool namens **`AVI-LB`**.

4 Klicken Sie mit der rechten Maustaste auf den Ressourcenpool und wählen Sie **OVF-Vorlage bereitstellen** aus.

5 Wählen Sie **Lokale Datei** aus und klicken Sie auf **Dateien hochladen**.

6 Navigieren Sie zur Datei `controller-`*`VERSION`*`.ova`, die Sie als erforderliche Datei heruntergeladen haben, und wählen Sie sie aus.

7 Geben Sie einen Namen ein und wählen Sie einen Ordner für den Controller aus.

Option	Bezeichnung
Name der virtuellen Maschine	**`avi-controller-1`**
Speicherort für die virtuelle Maschine	**Datencenter**

8 Wählen Sie den **`AVI-LB`**-Ressourcenpool als Computing-Ressource aus.

9 Überprüfen Sie die Konfigurationsdetails und klicken Sie auf **Weiter**.

10 Wählen Sie eine **VM-Speicherrichtlinie** aus, wie z. B. **`vsanDatastore`**.

11 Wählen Sie das Verwaltungsnetzwerk aus, z. B. **`network-1`**.

12 Passen Sie die Konfiguration wie folgt an und klicken Sie abschließend auf **Weiter**.

Option	Bezeichnung
IP-Adresse für die Verwaltungsschnittstelle	Geben Sie die IP-Adresse für die Controller-VM ein, z. B. **`10.199.17.51`**.
Subnetzmaske der Verwaltungsschnittstelle	Geben Sie die Subnetzmaske ein, wie z. B. **`255.255.255.0`**.
Standard-Gateway	Geben Sie das Standard-Gateway für das Verwaltungsnetzwerk ein, z. B. **`10.199.17.235`**.
Authentifizierungsschlüssel für die sysadmin-Anmeldung	Fügen Sie optional den Inhalt eines öffentlichen Schlüssels ein. Sie können den Schlüssel leer lassen.
Hostname von Avi Controller	Geben Sie den FQDN oder die IP-Adresse des Controllers ein.

13 Überprüfen Sie die Bereitstellungseinstellungen.

14 Klicken Sie auf **Fertig stellen**, um die Konfiguration abzuschließen.

15 Verwenden Sie vSphere Client, um die Bereitstellung der Controller-VM im Bereich **Aufgaben** zu überwachen.

16 Verwenden Sie den vSphere Client, um die Controller-VM nach der Bereitstellung einzuschalten.

Bereitstellen eines Controller-Clusters

Optional können Sie einen Cluster mit drei Controller-Knoten bereitstellen. Die Konfiguration eines Clusters wird in Produktionsumgebungen für HA und Notfallwiederherstellung empfohlen. Wenn Sie einen Einzelknoten-NSX Advanced Load Balancer-Controller ausführen, müssen Sie die Sicherungs- und Wiederherstellungsfunktion verwenden.

Um einen Cluster mit drei Knoten auszuführen, stellen Sie nach der Bereitstellung der ersten Controller-VM zwei weitere Controller-VMs bereit und schalten Sie sie ein. Sie dürfen nicht den Erstkonfigurationsassistenten ausführen oder das Administratorkennwort für diese Controller ändern. Die Konfiguration der ersten Controller-VM wird den beiden neuen Controller-VMs zugewiesen.

Verfahren

1 Wechseln Sie zu **Verwaltung > Controller**.

2 Wählen Sie **Knoten** aus.

3 Klicken Sie auf das Symbol „Bearbeiten“.

4 Fügen Sie eine statische IP als **Controller-Cluster-IP** hinzu.

Diese IP-Adresse muss aus dem Verwaltungsnetzwerk stammen.

5 Konfigurieren Sie in **Clusterknoten** die beiden neuen Clusterknoten.

Option	Beschreibung
IP	IP-Adresse des Controller-Knotens.
Name	Name des Knotens. Als Name kann die IP-Adresse verwendet werden.
Kennwort	Kennwort des Controller-Knotens. Lassen Sie das Kennwort leer.
Öffentliche IP	Die öffentliche IP-Adresse des Controller-Knotens. Lassen Sie dieses Feld leer.

6 Klicken Sie auf **Speichern**.

Hinweis Sobald Sie einen Cluster bereitgestellt haben, müssen Sie die IP des Controller-Clusters für jede weitere Konfiguration verwenden, nicht die IP des Controller-Knotens.

Einschalten des Controllers

Nachdem Sie die Controller-VM bereitgestellt haben, können Sie sie einschalten. Während des Startvorgangs wird der VM die während der Bereitstellung angegebene IP-Adresse zugewiesen.

Nach dem Einschalten kann der erste Startvorgang der Controller-VM bis zu 10 Minuten dauern.

Voraussetzungen

Stellen Sie den Controller bereit.

Verfahren

1 Klicken Sie im vCenter Server mit der rechten Maustaste auf die bereitgestellte `avi-controller-1`-VM.

2 Wählen Sie **Power > Einschalten**.

Der VM wird die IP-Adresse zugewiesen, die Sie während der Bereitstellung angegeben haben.

3 Um zu überprüfen, ob die VM eingeschaltet wurde, greifen Sie in einem Browser auf die IP-Adresse zu.

Wenn die VM online geschaltet wird, werden Warnungen zum TLS-Zertifikat und zur Verbindung angezeigt.

4 Klicken Sie in der Warnung **Diese Verbindung ist nicht privat** auf **Details anzeigen**.

5 Klicken Sie in dem daraufhin eingeblendeten Fenster auf **Diese Website besuchen**.

Sie werden zur Eingabe von Benutzeranmeldedaten aufgefordert.

Konfigurieren des NSX Advanced Load Balancer Controller

Konfigurieren Sie die NSX Advanced Load Balancer Controller-VM für Ihre vSphere IaaS control plane-Umgebung.

Um die Steuerungsebene des Lastausgleichsdiensts mit der vCenter Server-Umgebung zu verbinden, benötigt der NSX Advanced Load Balancer Controller mehrere Konfigurationsparameter nach der Bereitstellung.

Voraussetzungen

- Stellen Sie sicher, dass Ihre Umgebung die Systemanforderungen für die Konfiguration des NSX Advanced Load Balancer erfüllt. Siehe Anforderungen für Zonal Supervisor mit NSX und NSX Advanced Load Balancer und Anforderungen für die Cluster Supervisor-Bereitstellung mit NSX und NSX Advanced Load Balancer in *Konzepte und Planung der vSphere IaaS-Steuerungsebene*.
- Stellen Sie sicher, dass Sie über die Enterprise Tier-Lizenz verfügen. Der Controller wird im Testmodus gestartet, der über alle Funktionen verfügt, die einer verfügbaren Enterprise Edition-Lizenz entsprechen. Sie müssen dem Controller eine gültige Enterprise Tier-Lizenz zuweisen, bevor der Testzeitraum abläuft.

Verfahren

1 Navigieren Sie mithilfe eines Browsers zu der IP-Adresse, die Sie bei der Bereitstellung des NSX Advanced Load Balancer Controller festgelegt haben.

2 Erstellen Sie ein **Administratorkonto**.

Option	Beschreibung
Benutzername	Der Benutzername des Administrators für die anfängliche Konfiguration. Sie können dieses Feld nicht bearbeiten.
Kennwort	Geben Sie ein Administratorkennwort für die Controller-VM ein. Das Kennwort muss mindestens 8 Zeichen lang sein und eine Kombination aus numerischen Zeichen, Sonderzeichen, Großbuchstaben und Kleinbuchstaben enthalten.
Kennwort bestätigen	Geben Sie das Administratorkennwort erneut ein.
E-Mail-Adresse (optional)	Geben Sie eine Administrator-E-Mail-Adresse ein. Es wird empfohlen, eine E-Mail-Adresse für die Kennwortwiederherstellung in einer Produktionsumgebung anzugeben.

3 Konfigurieren Sie die **Systemeinstellungen**.

Option	Beschreibung
Passphrase	Geben Sie eine Passphrase für die Controller-Sicherung ein. Die Controller-Konfiguration wird in regelmäßigen Abständen automatisch auf der lokalen Festplatte gespeichert. Weitere Informationen finden Sie unter Sichern und Wiederherstellen. Die Passphrase muss mindestens 8 Zeichen lang sein und eine Kombination aus numerischen Zeichen, Sonderzeichen, Großbuchstaben und Kleinbuchstaben enthalten.
Passphrase bestätigen	Geben Sie die Sicherungs-Passphrase erneut ein.
DNS-Auflösung	Geben Sie eine IP-Adresse für den DNS-Server ein, den Sie in der vSphere IaaS control plane-Umgebung verwenden. Beispielsweise `10.14.7.12`.
DNS-Suchdomäne	Geben Sie eine Domänenzeichenfolge ein.

4 Weisen Sie eine Lizenz zu.

a Wählen Sie **Administration > Lizenzierung** aus.

b Wählen Sie **Einstellungen**.

c Wählen Sie **Enterprise-Ebene** aus und klicken Sie auf **SPEICHERN**.

d Klicken Sie auf **Hochladen von Computer**, um die Lizenz hinzuzufügen.

Nachdem die Lizenzdatei hochgeladen wurde, wird sie in der Liste der Controller-Lizenzen angezeigt. Das System zeigt die Informationen zur Lizenz an, einschließlich des Start- und Ablaufdatums.

5 Damit der NSX Advanced Load Balancer Controller mit NSX Manager kommunizieren kann, erstellen Sie NSX Manager-Anmeldedaten. Wählen Sie im NSX Advanced Load Balancer Controller-Dashboard **Administration > Benutzeranmeldedaten** aus.

Option	Beschreibung
Name	Name für die Anmeldedaten . Zum Beispiel: **`nsxuser`**
Anmeldedatentyp	Wählen Sie **NSX-T** aus.
Benutzername	Geben Sie den Benutzernamen ein, der zur Anmeldung bei NSX Manager verwendet werden soll.
Kennwort	Geben Sie das Kennwort für den NSX Manager ein.

6 Damit der NSX Advanced Load Balancer Controller mit vCenter Server kommunizieren kann, erstellen Sie vCenter Server-Anmeldedaten.

Option	Beschreibung
Name	Name für die Anmeldedaten . Zum Beispiel: **`vcuser`**.
Anmeldedatentyp	Wählen Sie **vCenter** aus.
Benutzername	Geben Sie den Benutzernamen ein, der zur Anmeldung bei vCenter Server verwendet werden soll.
Kennwort	Geben Sie das Kennwort für den vCenter Server ein.

7 Erstellen Sie ein Platzhalter-IPAM-Profil.

IPAM ist erforderlich, um virtuelle IP-Adressen beim Erstellen virtueller Dienst zuzuteilen.

a Wählen Sie im Dashboard NSX Advanced Load Balancer Controller **Vorlagen > IPAM/ DNS-Profile** aus.

Die Seite **NEUES IPAM/DNS-PROFIL** wird angezeigt.

b Geben Sie einen Namen für das Profil ein. Zum Beispiel: **`default-ipam`**.

c Wählen Sie für den **Typ** die Option **`Avi Vantage IPAM`** aus.

d Klicken Sie auf **Speichern**.

8 Konfigurieren Sie **NSX Cloud**.

a Wählen Sie im Dashboard NSX Advanced Load Balancer Controller **Infrastruktur > Clouds** aus.

b Geben Sie einen Namen für die Cloud ein. Zum Beispiel: **`nsx-cloud`**

c Wählen Sie **NSX-T Cloud** als Cloud-Typ aus.

d Wählen Sie **DHCP** aus.

e Geben Sie ein **Objekt-Namenspräfix** für die Dienst-Engines ein. Die Präfixzeichenfolge darf nur Buchstaben, Zahlen und Unterstriche enthalten. Dieses Feld kann nach der Konfiguration der Cloud nicht mehr geändert werden. Zum Beispiel: **`nsx`**

9 Geben Sie die Anmeldedaten für die NSX ein.

a Geben Sie die IP-Adresse des NSX Managers ein.

b Geben Sie die NSX Manager-Anmeldedaten ein, die Sie erstellt haben. Zum Beispiel: **`nsxuser`**.

10 Konfigurieren Sie das Verwaltungsnetzwerk. Das Verwaltungsnetzwerk ist der Kommunikationskanal zwischen dem NSX Advanced Load Balancer Controller und den Dienst-Engines.

Option	Beschreibung
Transportzone	Die Transportzone, in der die Dienst-Engine platziert wird. Wählen Sie die Overlay-Transportzone aus. Beispiel: **`nsx-overlay-transportzone`**.
Tier 1 Logischer Router	Wählen Sie das Tier-1-Gateway. Zum Beispiel: **`Tier-1_VWT`**.
Overlay-Segment	Das Management-Overlay-Segment, von dem die Verwaltungs-Netzwerkkarte der Dienst-Engine die IP-Adresse erhält. Zum Beispiel: **`nsxoverlaysegment`**.

11 Konfigurieren Sie das Datennetzwerk.

Klicken Sie im Abschnitt **Datennetzwerk** auf **HINZUFÜGEN**.

Option	Beschreibung
Transportzone	Wählen Sie die Overlay-Transportzone aus. Beispiel: **`nsx-overlay-transportzone`**.
Logischer Router	Geben Sie das Tier-1-Gateway ein. Zum Beispiel: **`Tier-1_VWT`**.
Overlay-Segment	Wählen Sie das Overlay-Segment aus. Zum Beispiel: **`nsxoverlaysegment`**.

12 Geben Sie die Anmeldedaten für vCenter Server ein.

Klicken Sie im Abschnitt **vCenter Server** auf **HINZUFÜGEN**.

Option	Beschreibung
Name	Name der zuvor von Ihnen erstellten Anmeldedaten. Zum Beispiel: **`vcuser`**.
URL	Die IP-Adresse des vCenter Server.

13 Fügen Sie das zuvor von Ihnen erstellte IPAM-Profil hinzu. Wählen Sie in **IPAM-Profil** **`default-ipam`** aus.

IPAM ist erforderlich, um virtuelle IP-Adressen beim Erstellen virtueller Dienst zuzuteilen.

Ergebnisse

Nachdem Sie die Konfiguration abgeschlossen haben, sehen Sie das NSX Advanced Load Balancer Controller-**Dashboard**. Wählen Sie **Infrastruktur > Clouds** aus und stellen Sie sicher, dass der Status des NSX Advanced Load Balancer Controller für **NSX Cloud** grün ist. Manchmal kann der Status für einige Zeit gelb sein, bis der NSX Advanced Load Balancer Controlleralle Portgruppen in der vCenter Server-Umgebung erkannt hat und grün wird.

Nächste Schritte

Konfigurieren einer Dienst-Engine-Gruppe. Weitere Informationen finden Sie unter Konfigurieren einer Dienst-Engine-Gruppe.

Konfigurieren einer Dienst-Engine-Gruppe

vSphere IaaS control plane verwendet die **Standardgruppe** als Vorlage zum Konfigurieren einer Dienst-Engine-Gruppe pro Supervisor. Optional können Sie die **Standardgruppe**-Dienst-Engines in einer Gruppe konfigurieren, die die Platzierung und Anzahl der Dienst-Engine-VMs innerhalb von vCenter definiert. Sie können auch Hochverfügbarkeit konfigurieren, wenn sich der NSX Advanced Load Balancer Controller im Enterprise-Modus befindet.

Verfahren

1. Wählen Sie im NSX Advanced Load Balancer Controller-Dashboard **Infrastruktur > Cloud-Ressourcen > Dienst-Engine-Gruppe** aus.
2. Klicken Sie auf der Seite **Dienst-Engine-Gruppe** auf das Bearbeitungssymbol in der **Standardgruppe**.

   Die Registerkarte **Allgemeine Einstellungen** wird angezeigt.

3 Konfigurieren Sie im Abschnitt **Hochverfügbarkeits- und Platzierungseinstellungen** die Einstellungen für Hochverfügbarkeit und virtuelle Dienste.

   a Wählen Sie den **Hochverfügbarkeitsmodus** aus.

   Die Standardoption ist `N + M (buffer)`. Sie können den Standardwert beibehalten oder eine der folgenden Optionen auswählen:

   - `Active/Standy`
   - `Active/Active`

   b Konfigurieren Sie die **Anzahl der Dienst-Engines**. Dies ist die maximale Anzahl von Dienst-Engines, die innerhalb einer Dienstmodulgruppe erstellt werden können. Der Standardwert ist **`10`**.

   c Konfigurieren Sie **Platzierung virtueller Dienste über Dienst-Engines hinweg**.

   Die Standardoption ist **Kompakt**. Sie können eine der folgenden Optionen auswählen:

   - **Verteilt**. Der NSX Advanced Load Balancer Controller maximiert die Leistung, indem virtuelle Dienste auf neu hochgefahrenen Dienst-Engines platziert werden, bis die angegebene maximale Anzahl von Dienst-Engines erreicht ist.
   - **Kompakt**. Die NSX Advanced Load Balancer Controller startet die kleinstmögliche Dienst-Engine und platziert den neuen virtuellen Dienst auf einer bestehenden Dienst-Engine. Eine neue Dienst-Engine wird nur erstellt, wenn alle Dienst-Engines verwendet werden.

4 Sie können die Standardwerte für die anderen Einstellungen beibehalten.

5 Klicken Sie auf **Speichern**.

Ergebnisse

Der AKO erstellt eine Dienst-Engine-Gruppe für jeden vSphere IaaS control plane-Cluster. Die Konfiguration der Dienst-Engine-Gruppe wird von der Konfiguration **Standardgruppe** abgeleitet. Sobald die **Standardgruppe** mit den erforderlichen Werten konfiguriert ist, werden alle von der AKO erstellten neuen Dienst-Engine-Gruppe dieselben Einstellungen aufweisen. Änderungen an der Konfiguration der **Standardgruppe** werden jedoch nicht in einer bereits erstellten Dienst-Engine-Gruppe widergespiegelt. Sie müssen die Konfiguration für eine vorhandene Dienst-Engine-Gruppe separat ändern.

Registrieren Sie die NSX Advanced Load Balancer Controller bei NSX Manager

Registrieren Sie die NSX Advanced Load Balancer Controller bei NSX Manager.

Voraussetzungen

Stellen Sie sicher, dass Sie den NSX Advanced Load Balancer Controller bereitgestellt haben.

Verfahren

1 Melden Sie sich als Root-Benutzer bei NSX Manager an.

2 Führen Sie folgende Befehle aus:

```
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"
}'
```

Wenn Sie DNS- und NTP-Einstellungen im API-Aufruf angeben, werden die globalen Einstellungen überschrieben. Beispiele: `"dns_servers": ["<dns-servers-ips>"]` und `"ntp_servers": ["<ntp-servers-ips>"]`.

Zuweisen eines Zertifikats zum NSX Advanced Load Balancer Controller

Der NSX Advanced Load Balancer Controller verwendet Zertifikate, die er an Clients sendet, um Sites zu authentifizieren und eine sichere Kommunikation herzustellen. Zertifikate können entweder vom NSX Advanced Load Balancer selbstsigniert oder als Zertifikatsignieranforderung (Certificate Signing Request, CSR) erstellt werden, die an eine vertrauenswürdige Zertifizierungsstelle (CA) gesendet wird, die dann ein vertrauenswürdiges Zertifikat generiert. Sie können ein selbstsigniertes Zertifikat erstellen oder ein externes Zertifikat hochladen.

Sie müssen ein benutzerdefiniertes Zertifikat bereitstellen, um Supervisor zu aktivieren. Sie können das Standardzertifikat nicht verwenden. Weitere Informationen zu Zertifikaten finden Sie unter SSL-/TLS-Zertifikate.

Wenn Sie ein von einer privaten Zertifizierungsstelle (CA) signiertes Zertifikat verwenden, wird die Supervisor-Bereitstellung möglicherweise nicht abgeschlossen und die NSX Advanced Load Balancer-Konfiguration möglicherweise nicht angewendet. Weitere Informationen finden Sie unter NSX Advanced Load Balancer Konfiguration wird nicht angewendet.

Voraussetzungen

Stellen Sie sicher, dass die NSX Advanced Load Balancer beim NSX Manager registriert ist.

Verfahren

1 Klicken Sie im Controller-Dashboard auf das Menü in der oberen linken Ecke und wählen Sie **Vorlagen > Sicherheit** aus.

2 Wählen Sie **SSL/TLS-Zertifikat** aus.

3 Zum Erstellen eines Zertifikats klicken Sie auf **Erstellen** und wählen Sie **Controller-Zertifikat** aus.

Das Fenster **Neues Zertifikat (SSL/TLS)** wird geöffnet.

4 Geben Sie einen Namen für das Zertifikat ein.

5 Wenn kein vorab erstelltes gültiges Zertifikat vorhanden ist, fügen Sie ein selbstsigniertes Zertifikat hinzu, indem Sie für **Typ** die Option `Self Signed` auswählen.

a Geben Sie die folgenden Details ein:

Option	Beschreibung
Allgemeiner Name	Geben Sie den vollqualifizierten Namen der Site an. Damit die Site als vertrauenswürdig eingestuft wird, muss dieser Eintrag mit dem Hostnamen übereinstimmen, den der Client im Browser eingegeben hat.
Algorithmus	Wählen Sie EC (Elliptic Curve Cryptography) oder RSA aus. EC wird empfohlen.
Schlüssellänge	Wählen Sie die Verschlüsselungsebene aus, die für Handshakes verwendet werden soll: ■ `SECP256R1` wird für EC-Zertifikate verwendet. ■ 2048 Bit wird für RSA-Zertifikate empfohlen.

b Klicken Sie in **Subject Alternate Name (SAN)** auf **Hinzufügen**.

c Geben Sie die IP-Adresse und/oder den FQDN des Clusters ein, wenn der NSX Advanced Load Balancer Controller als einzelner Knoten bereitgestellt wird. Wenn nur die IP-Adresse oder der FQDN verwendet wird, muss sie mit der IP-Adresse der NSX Advanced Load Balancer Controller-VM übereinstimmen, die Sie während der Bereitstellung angeben.

Weitere Informationen finden Sie unter Bereitstellen der NSX Advanced Load Balancer Controller. Geben Sie die Cluster-IP oder den FQDN des NSX Advanced Load Balancer Controller-Clusters ein, wenn dieser als Cluster mit drei Knoten bereitgestellt wird.

d Klicken Sie auf **Speichern**.

Sie benötigen dieses Zertifikat, wenn Sie den Supervisor zum Aktivieren der Arbeitslastverwaltungsfunktion konfigurieren.

6 Laden Sie das selbstsignierte Zertifikat herunter, das Sie erstellen.

a Klicken Sie auf **Sicherheit > SSL/TLS-Zertifikate**.

Wenn das Zertifikat nicht angezeigt wird, aktualisieren Sie die Seite.

b Wählen Sie das erstellte Zertifikat aus und klicken Sie auf das Download-Symbol.

c Klicken Sie auf der Seite **Zertifikat exportieren** für das Zertifikat auf **In Zwischenablage kopieren**. Kopieren Sie nicht den Schlüssel.

d Speichern Sie das kopierte Zertifikat für die spätere Verwendung, wenn Sie die Arbeitslastverwaltung aktivieren.

7 Wenn ein vorab erstelltes gültiges Zertifikat vorhanden ist, laden Sie es hoch, indem Sie für **Typ** die Option `Import` auswählen.

   a Klicken Sie unter **Zertifikat** auf **Datei hochladen** und importieren Sie das Zertifikat.

   Das SAN-Feld des Zertifikats, das Sie hochladen, muss über die IP-Adresse oder den FQDN des Controllers verfügen.

   Hinweis Stellen Sie sicher, dass Sie den Inhalt des Zertifikats nur einmal hochladen oder einfügen.

   b Klicken Sie in **Schlüssel (PEM) oder PKCS12** auf **Datei hochladen** und importieren Sie den Schlüssel.

   c Klicken Sie **Validieren**, um das Zertifikat und den Schlüssel zu validieren.

   d Klicken Sie auf **Speichern**.

8 Um das Zertifikat zu ändern, führen Sie die folgenden Schritte aus.

   a Wählen Sie im Controller-Dashboard **Verwaltung > Systemeinstellungen** aus.

   b Klicken Sie auf **Bearbeiten**.

   c Wählen Sie die Registerkarte **Zugriff**.

   d Entfernen Sie aus dem **SSL/TLS-Zertifikat** die vorhandenen Standardportalzertifikate.

   e Wählen Sie im Dropdown-Menü das neu erstellte oder hochgeladene Zertifikat aus.

   f Wählen Sie **Standardauthentifizierung** aus.

   g Klicken Sie auf **SPEICHERN**.

Einschränkungen bei der Verwendung des NSX Advanced Load Balancer

Es ist wichtig, dass Sie beim Konfigurieren des NSX Advanced Load Balancer in Ihrer vSphere IaaS control plane-Umgebung die Einschränkungen beachten.

Ein Ingress erhält in den folgenden Fällen keine externe IP vom NSX Advanced Load Balancer:

- Wenn in der Ingress-Konfiguration kein Hostname angegeben ist.
- Wenn der Ingress mit der Konfigurationsoption `defaultBackend` anstatt mit dem Hostnamens konfiguriert ist.

Standardmäßig muss eine Ingress-Ressource in Kubernetes den Hostnamen in der Controller-Konfiguration definieren und ihr eine externe IP-Adresse zuweisen. Dies ist erforderlich, da der NSX Advanced Load Balancer für den Datenverkehr in den virtuellen Diensten, die entsprechend der Kubernetes-Ingresses erstellt werden, virtuelles Hosting verwendet. Weitere Informationen zur Konfigurationsoption `defaultBackend` finden Sie unter https://kubernetes.io/docs/concepts/services-networking/ingress/#default-backend.

Wenn ein Ingress denselben Hostnamen wie ein Ingress in einem anderen Namespace hat, erhält er keine externe IP vom NSX Advanced Load Balancer. Standardmäßig weist der NSX Advanced Load Balancer für jeden Namespace eine eindeutige VIP zu. Dies bedeutet, dass alle Ingresses in einem einzelnen Namespace dieselbe VIP verwenden. Folglich werden zwei Ingresses aus verschiedenen Namespaces unterschiedliche VIPs zugewiesen. Wenn sie jedoch denselben Hostnamen aufweisen, weiß der DNS-Server nicht, in welche IP-Adresse der Hostname aufgelöst werden soll.

Installieren und Konfigurieren von NSX Advanced Load Balancer

Wenn Sie ein vSphere Distributed Switch (vDS)-Netzwerk verwenden, können Sie den NSX Advanced Load Balancer 22.1.4 in Ihrer vSphere IaaS control plane-Umgebung installieren und konfigurieren.

- Stellen Sie sicher, dass Ihre Umgebung die Anforderungen zum Konfigurieren von vSphere IaaS control plane mit dem NSX Advanced Load Balancer erfüllt. Weitere Informationen finden Sie unter Anforderungen für einen Drei-Zonen-Supervisor mit NSX Advanced Load Balancer und Anforderungen für die Aktivierung eines Einzelcluster-Supervisors mit NSX Advanced Load Balancer in *Konzepte und Planung der vSphere IaaS-Steuerungsebene*.
- Laden Sie die NSX Advanced Load Balancer-OVA herunter. VMware stellt eine NSX Advanced Load Balancer-OVA-Datei zur Verfügung, die Sie in Ihrer vSphere-Umgebung bereitstellen, in der Sie die Arbeitslastverwaltung aktivieren. Laden Sie die neueste Version der OVA-Datei, die mit vSphere IaaS control plane unterstützt wird, über das VMware Customer Connect-Portal herunter.

Hinweis Die Verfahren in diesem Handbuch gelten für den NSX Advanced Load Balancer, der von vSphere IaaS control plane 8.0 Update 2 unterstützt wird. Möglicherweise sind höhere Versionen von NSX Advanced Load Balancer verfügbar, in denen die Workflows der Benutzeroberfläche unterschiedlich sein können.

Weitere Informationen zum NSX Advanced Load Balancer finden Sie in der Dokumentation zu VMware NSX Advanced Load Balancer.

Weitere Themen zum Lesen

Verfahren

1. Erstellen eines vSphere Distributed Switch für einen Supervisor zwecks Verwendung mit NSX Advanced Load Balancer

   Zum Konfigurieren eines vSphere-Clusters als Supervisor, der den vSphere-Netzwerk-Stack und den NSX Advanced Load Balancer verwendet, müssen Sie einen vSphere Distributed Switch erstellen. Erstellen Sie Portgruppen auf dem Distributed Switch, den Sie als Arbeitslastnetzwerke für den Supervisor konfigurieren können. Der NSX Advanced Load Balancer benötigt eine verteilte Portgruppe, um die Dienst-Engine-Datenschnittstellen zu verbinden. Die Portgruppe wird verwendet, um die virtuellen Anwendungs-IPs (VIPs) auf den Dienst-Engines zu platzieren.

2. Importieren der NSX Advanced Load Balancer-OVA in eine lokale Inhaltsbibliothek

   Um das NSX Advanced Load Balancer OVA-Image zu speichern, erstellen Sie eine lokale Inhaltsbibliothek und importieren Sie die OVA in diese Bibliothek.

3. Bereitstellen des NSX Advanced Load Balancer-Controllers

   Stellen Sie die NSX Advanced Load Balancer-Controller-VM im Verwaltungsnetzwerk in Ihrer vSphere IaaS control plane-Umgebung bereit.

4. Konfigurieren einer Dienst-Engine-Gruppe

   vSphere IaaS control plane verwendet die Dienst-Engine-Gruppe **Standardgruppe**. Optional können Sie die **Standardgruppe**-Dienst-Engines in einer Gruppe konfigurieren, die die Platzierung und Anzahl der Dienst-Engine-VMs innerhalb von vCenter definiert. Sie können auch Hochverfügbarkeit konfigurieren, wenn sich der NSX Advanced Load Balancer-Controller im Enterprise-Modus befindet. vSphere IaaS control plane unterstützt lediglich die Dienst-Engine **Standardgruppe**. Andere Dienstmodulgruppen können nicht erstellt werden.

Erstellen eines vSphere Distributed Switch für einen Supervisor zwecks Verwendung mit NSX Advanced Load Balancer

Zum Konfigurieren eines vSphere-Clusters als Supervisor, der den vSphere-Netzwerk-Stack und den NSX Advanced Load Balancer verwendet, müssen Sie einen vSphere Distributed Switch erstellen. Erstellen Sie Portgruppen auf dem Distributed Switch, den Sie als Arbeitslastnetzwerke für den Supervisor konfigurieren können. Der NSX Advanced Load Balancer benötigt eine verteilte Portgruppe, um die Dienst-Engine-Datenschnittstellen zu verbinden. Die Portgruppe wird verwendet, um die virtuellen Anwendungs-IPs (VIPs) auf den Dienst-Engines zu platzieren.

Voraussetzungen

Überprüfen Sie die Systemanforderungen und Netzwerktopologien für die Verwendung des vSphere-Netzwerks für den Supervisor mit dem NSX Advanced Load Balancer. Weitere Informationen finden Sie unter Anforderungen für einen Drei-Zonen-Supervisor mit NSX

Advanced Load Balancer und Anforderungen für die Aktivierung eines Einzelcluster-Supervisors mit NSX Advanced Load Balancer in *Konzepte und Planung der vSphere IaaS-Steuerungsebene*.

Verfahren

1 Navigieren Sie im vSphere Client zu einem Datencenter.

2 Klicken Sie mit der rechten Maustaste auf das Datencenter und wählen Sie **Distributed Switch > Neuer Distributed Switch** aus.

3 Geben Sie einen Namen für den Switch ein, z. B. **`Distributed Switch für Arbeitslast`** und klicken Sie auf **Weiter**.

4 Wählen Sie Version 8.0 für den Switch aus und klicken Sie auf **Weiter**.

5 Geben Sie unter **Portgruppenname** **`Primäres Arbeitslastnetzwerk`** ein, klicken Sie auf **Weiter** und dann auf **Beenden**.

   Ein neuer Distributed Switch mit einer Portgruppe wird im Datencenter erstellt. Sie können diese Portgruppe als das primäre Arbeitslastnetzwerk für den Supervisor verwenden, den Sie erstellen werden. Das primäre Arbeitslastnetzwerk verarbeitet den Datenverkehr für die Kubernetes-Steuerungsebenen-VMs.

6 Erstellen Sie verteilte Portgruppen für Arbeitslastnetzwerke.

   Wie viele Portgruppen Sie erstellen, hängt von der Topologie ab, die Sie für den Supervisor implementieren möchten. Erstellen Sie für eine Topologie mit einem isolierten Arbeitslastnetzwerk eine verteilte Portgruppe, die Sie als Netzwerk für alle Namespaces auf dem Supervisor verwenden werden. Erstellen Sie für eine Topologie mit isolierten Netzwerken für jeden Namespace dieselbe Anzahl an Portgruppen wie die Anzahl der von Ihnen zu erstellenden Namespaces.

   a Navigieren Sie zum neu erstellten Distributed Switch.

   b Klicken Sie mit der rechten Maustaste auf den Switch und wählen Sie **Verteilte Portgruppen > Neue verteilte Portgruppe** aus.

   c Geben Sie einen Namen für die Portgruppe ein, z. B. **`Arbeitslastnetzwerk`**, und klicken Sie auf **Weiter**.

   d Behalten Sie die Standardeinstellungen bei, klicken Sie auf **Weiter** und dann auf **Beenden**.

7 Erstellen Sie eine Portgruppe für das Datennetzwerk.

a Klicken Sie mit der rechten Maustaste auf den Distributed Switch und wählen Sie **Verteilte Portgruppe > Neue verteilte Portgruppe** aus.

b Geben Sie einen Namen für die Portgruppe ein, z. B. **`Datennetzwerk`**, und klicken Sie auf **Weiter**.

c Geben Sie auf der Seite **Einstellungen konfigurieren** die allgemeinen Eigenschaften für die neue verteilte Portgruppe ein und klicken Sie auf **Weiter**.

Eigenschaft	Beschreibung
Port-Bindung	Wählen Sie aus, wann Ports virtuellen Maschinen zugewiesen werden, die mit dieser verteilten Portgruppe verbunden sind. Wählen Sie **Statische Bindung** aus, um einer virtuellen Maschine einen Port zuzuweisen, wenn die virtuelle Maschine mit der verteilten Portgruppe verbunden wird.
Portzuteilung	Wählen Sie die Portzuteilung **Elastisch** aus. Die Standardanzahl der Ports ist acht. Wenn alle Ports zugewiesen wurden, wird ein neues Set aus acht Ports erstellt.
Anzahl der Ports	Behalten Sie den Standardwert bei.
Netzwerkressourcenpool	Weisen Sie über das Dropdown-Menü die neue verteilte Portgruppe einem benutzerdefinierten Netzwerkressourcenpool zu. Wenn Sie keinen Netzwerkressourcenpool erstellt haben, bleibt dieses Menü leer.
VLAN	Wählen Sie im Dropdown-Menü den Typ des VLAN-Datenverkehrsfilters und der Markierung aus: ■ **Keine**: Verwenden Sie VLAN nicht. Wählen Sie diese Option aus, wenn Sie External Switch Tagging verwenden. ■ **VLAN**: Geben Sie im Textfeld „VLAN-ID“ einen Wert zwischen 1 und 4.094 für Virtual Switch Tagging ein. ■ **VLAN-Trunking**: Verwenden Sie diese Option für das Virtual Guest Tagging und um VLAN-Datenverkehr mit einer ID an das Gastbetriebssystem weiterzuleiten. Geben Sie einen VLAN-Trunk-Bereich ein. Sie können mithilfe einer kommagetrennten Liste mehrere Bereiche oder individuelle VLANs festlegen. Beispiel: `1702-1705, 1848-1849`. ■ **Privates VLAN**: Ordnen Sie den Datenverkehr einem privaten VLAN zu, das auf dem Distributed Switch erstellt wurde. Wenn Sie keine privaten VLANs erstellt haben, bleibt dieses Menü leer.
Erweitert	Lassen Sie diese Option unausgewählt.

8 Überprüfen Sie auf der Seite **Bereit zum Abschließen** die Konfiguration und klicken Sie auf **Beenden**.

Ergebnisse

Der Distributed Switch wird erstellt, und verteilte Portgruppen werden unter dem Distributed Switch angezeigt. Sie können jetzt diese Portgruppe, die Sie erstellt haben, als **Datennetzwerk** für den NSX Advanced Load Balancer verwenden.

Importieren der NSX Advanced Load Balancer-OVA in eine lokale Inhaltsbibliothek

Um das NSX Advanced Load Balancer OVA-Image zu speichern, erstellen Sie eine lokale Inhaltsbibliothek und importieren Sie die OVA in diese Bibliothek.

Das Erstellen einer lokalen Inhaltsbibliothek umfasst das Konfigurieren der Bibliothek, das Herunterladen der OVA-Dateien und das Importieren in die lokale Inhaltsbibliothek. Weitere Informationen finden Sie unter Verwenden von Inhaltsbibliotheken .

Voraussetzungen

Stellen Sie sicher, dass Sie die NSX Advanced Load Balancer-OVA heruntergeladen haben.

Erstellen Sie eine lokale Inhaltsbibliothek. Siehe Erstellen und Bearbeiten einer Inhaltsbibliothek.

Verfahren

1. Melden Sie sich über vSphere Client bei vCenter Server an.
2. Wählen Sie **Menü > Inhaltsbibliotheken** aus.
3. Klicken Sie in der Liste der **Inhaltsbibliotheken** auf den Link für den Namen der von Ihnen erstellten lokalen Inhaltsbibliothek. Beispiel: **NSX ALB**.
4. Klicken Sie auf **Aktionen**.
5. Wählen Sie **Element importieren** aus.
6. Wählen Sie im Fenster **Bibliothekselement importieren** die Option **Lokale Datei** aus.
7. Klicken Sie auf **Dateien hochladen**.
8. Wählen Sie die heruntergeladene OVA-Datei aus.
9. Klicken Sie auf **Import**.
10. Zeigen Sie den Bereich **Aktuelle Aufgaben** am unteren Rand der Seite an.
11. Überwachen Sie die Aufgabe **Inhalt eines Bibliothekselements abrufen** und stellen Sie sicher, dass sie erfolgreich **abgeschlossen** wurde.

Nächste Schritte

Stellen Sie den NSX Advanced Load Balancer-Controller bereit. Weitere Informationen hierzu finden Sie unter Bereitstellen des NSX Advanced Load Balancer-Controllers.

Bereitstellen des NSX Advanced Load Balancer-Controllers

Stellen Sie die NSX Advanced Load Balancer-Controller-VM im Verwaltungsnetzwerk in Ihrer vSphere IaaS control plane-Umgebung bereit.

Voraussetzungen

- Stellen Sie sicher, dass Sie über ein Verwaltungsnetzwerk verfügen, auf dem der NSX Advanced Load Balancer bereitgestellt werden soll. Dabei kann es sich um einen vSphere Distributed Switch (vDS) oder einen vSphere Standard Switch (vSS) handeln.
- Stellen Sie sicher, dass Sie einen vDS-Switch und eine Portgruppe für das Datennetzwerk erstellt haben. Weitere Informationen hierzu finden Sie unter Erstellen eines vSphere Distributed Switch für einen Supervisor zwecks Verwendung mit NSX Advanced Load Balancer.
- Stellen Sie sicher, dass die Voraussetzungen erfüllt sind. Weitere Informationen finden Sie unter Anforderungen für einen Drei-Zonen-Supervisor mit NSX Advanced Load Balancer und Anforderungen für die Aktivierung eines Einzelcluster-Supervisors mit NSX Advanced Load Balancer in *Konzepte und Planung der vSphere IaaS-Steuerungsebene*.

Verfahren

1. Melden Sie sich beim vCenter Server mit dem vSphere Client an.
2. Wählen Sie den vSphere-Cluster aus, der für Verwaltungskomponenten vorgesehen ist.
3. Erstellen Sie einen Ressourcenpool namens **`AVI-LB`**.
4. Klicken Sie mit der rechten Maustaste auf den Ressourcenpool und wählen Sie **OVF-Vorlage bereitstellen** aus.
5. Wählen Sie **Lokale Datei** aus und klicken Sie auf **Dateien hochladen**.
6. Navigieren Sie zur Datei `controller-`*`VERSION`*`.ova`, die Sie als erforderliche Datei heruntergeladen haben, und wählen Sie sie aus.
7. Geben Sie einen Namen ein und wählen Sie einen Ordner für den Controller aus.

Option	Bezeichnung
Name der virtuellen Maschine	**`avi-controller-1`**
Speicherort für die virtuelle Maschine	Datencenter

8. Wählen Sie den **`AVI-LB`**-Ressourcenpool als Computing-Ressource aus.
9. Überprüfen Sie die Konfigurationsdetails und klicken Sie auf **Weiter**.
10. Wählen Sie eine **VM-Speicherrichtlinie** aus, wie z. B. **`vsanDatastore`**.
11. Wählen Sie das Verwaltungsnetzwerk aus, z. B. **`network-1`**.

12 Passen Sie die Konfiguration wie folgt an und klicken Sie abschließend auf **Weiter**.

Option	Bezeichnung
IP-Adresse für die Verwaltungsschnittstelle	Geben Sie die IP-Adresse für die Controller-VM ein, z. B. `10.199.17.51`.
Subnetzmaske der Verwaltungsschnittstelle	Geben Sie die Subnetzmaske ein, wie z. B. `255.255.255.0`.
Standard-Gateway	Geben Sie das Standard-Gateway für das Verwaltungsnetzwerk ein, z. B. `10.199.17.235`.
Authentifizierungsschlüssel für die sysadmin-Anmeldung	Fügen Sie optional den Inhalt eines öffentlichen Schlüssels ein. Sie können den Schlüssel leer lassen.
Hostname von Avi Controller	Geben Sie den FQDN oder die IP-Adresse des Controllers ein.

13 Überprüfen Sie die Bereitstellungseinstellungen.

14 Klicken Sie auf **Fertig stellen**, um die Konfiguration abzuschließen.

15 Verwenden Sie vSphere Client, um die Bereitstellung der Controller-VM im Bereich **Aufgaben** zu überwachen.

16 Verwenden Sie den vSphere Client, um die Controller-VM nach der Bereitstellung einzuschalten.

Bereitstellen eines Controller-Clusters

Optional können Sie einen Cluster mit drei Controller-Knoten bereitstellen. Die Konfiguration eines Clusters wird in Produktionsumgebungen für HA und Notfallwiederherstellung empfohlen. Wenn Sie einen Einzelknoten-NSX Advanced Load Balancer-Controller ausführen, müssen Sie die Sicherungs- und Wiederherstellungsfunktion verwenden.

Um einen Cluster mit drei Knoten auszuführen, stellen Sie nach der Bereitstellung der ersten Controller-VM zwei weitere Controller-VMs bereit und schalten Sie sie ein. Sie dürfen nicht den Erstkonfigurationsassistenten ausführen oder das Administratorkennwort für diese Controller ändern. Die Konfiguration der ersten Controller-VM wird den beiden neuen Controller-VMs zugewiesen.

Verfahren

1 Wechseln Sie zu **Verwaltung > Controller**.

2 Wählen Sie **Knoten** aus.

3 Klicken Sie auf das Symbol „Bearbeiten“.

4 Fügen Sie eine statische IP als **Controller-Cluster-IP** hinzu.

   Diese IP-Adresse muss aus dem Verwaltungsnetzwerk stammen.

5 Konfigurieren Sie in **Clusterknoten** die beiden neuen Clusterknoten.

Option	Beschreibung
IP	IP-Adresse des Controller-Knotens.
Name	Name des Knotens. Als Name kann die IP-Adresse verwendet werden.
Kennwort	Kennwort des Controller-Knotens. Lassen Sie das Kennwort leer.
Öffentliche IP	Die öffentliche IP-Adresse des Controller-Knotens. Lassen Sie dieses Feld leer.

6 Klicken Sie auf **Speichern**.

Hinweis Sobald Sie einen Cluster bereitgestellt haben, müssen Sie die IP des Controller-Clusters für jede weitere Konfiguration verwenden, nicht die IP des Controller-Knotens.

Einschalten des Controllers

Nachdem Sie die Controller-VM bereitgestellt haben, können Sie sie einschalten. Während des Startvorgangs wird der VM die während der Bereitstellung angegebene IP-Adresse zugewiesen.

Nach dem Einschalten kann der erste Startvorgang der Controller-VM bis zu 10 Minuten dauern.

Voraussetzungen

Stellen Sie den Controller bereit.

Verfahren

1 Klicken Sie im vCenter Server mit der rechten Maustaste auf die bereitgestellte `avi-controller-1`-VM.

2 Wählen Sie **Power > Einschalten**.

Der VM wird die IP-Adresse zugewiesen, die Sie während der Bereitstellung angegeben haben.

3 Um zu überprüfen, ob die VM eingeschaltet wurde, greifen Sie in einem Browser auf die IP-Adresse zu.

Wenn die VM online geschaltet wird, werden Warnungen zum TLS-Zertifikat und zur Verbindung angezeigt.

4 Klicken Sie in der Warnung **Diese Verbindung ist nicht privat** auf **Details anzeigen**.

5 Klicken Sie in dem daraufhin eingeblendeten Fenster auf **Diese Website besuchen**.

Sie werden zur Eingabe von Benutzeranmeldedaten aufgefordert.

Konfigurieren des Controllers

Konfigurieren Sie die Controller-VM für Ihre vSphere IaaS control plane-Umgebung und richten Sie eine Cloud ein.

Um die Steuerungsebene des Lastausgleichsdiensts mit der vCenter Server-Umgebung zu verbinden, benötigt der Controller mehrere Konfigurationsparameter nach der Bereitstellung. Während der Erstkonfiguration des Controllers wird eine Cloud vom Typ Standard-Cloud erstellt, in der der erste Controller bereitgestellt wird. Damit der Lastausgleichsdienst mehrere vCenter Server oder mehrere Datencenter bedienen kann, können Sie benutzerdefinierte Clouds vom Typ VMware vCenter für jede Kombination aus vCenter und Datencenter erstellen. Weitere Informationen finden Sie unter NSX Advanced Load Balancer-Komponenten.

Voraussetzungen

- Stellen Sie sicher, dass Ihre Umgebung die Systemanforderungen für die Konfiguration des NSX Advanced Load Balancer erfüllt. Weitere Informationen finden Sie unter Anforderungen für einen Drei-Zonen-Supervisor mit NSX Advanced Load Balancer und Anforderungen für die Aktivierung eines Einzelcluster-Supervisors mit NSX Advanced Load Balancer in *Konzepte und Planung der vSphere IaaS-Steuerungsebene*.
- Stellen Sie den Controller bereit.

Verfahren

1. Navigieren Sie mithilfe eines Browsers zu der IP-Adresse, die Sie bei der Bereitstellung des Controllers festgelegt haben.
2. Erstellen Sie ein **Administratorkonto**.

Option	Beschreibung
Benutzername	Der Benutzername des Administrators für die anfängliche Konfiguration. Sie können dieses Feld nicht bearbeiten.
Kennwort	Geben Sie ein Administratorkennwort für die Controller-VM ein. Das Kennwort muss mindestens 8 Zeichen lang sein und eine Kombination aus numerischen Zeichen, Sonderzeichen, Großbuchstaben und Kleinbuchstaben enthalten.
Kennwort bestätigen	Geben Sie das Administratorkennwort erneut ein.
E-Mail-Adresse (optional)	Geben Sie eine Administrator-E-Mail-Adresse ein. Es wird empfohlen, eine E-Mail-Adresse für die Kennwortwiederherstellung in einer Produktionsumgebung anzugeben.

3. Konfigurieren Sie die **Systemeinstellungen**.

Option	Beschreibung
Passphrase	Geben Sie eine Passphrase für die Controller-Sicherung ein. Die Controller-Konfiguration wird in regelmäßigen Abständen automatisch auf der lokalen Festplatte gespeichert. Weitere Informationen finden Sie unter Sichern und Wiederherstellen. Die Passphrase muss mindestens 8 Zeichen lang sein und eine Kombination aus numerischen Zeichen, Sonderzeichen, Großbuchstaben und Kleinbuchstaben enthalten.
Passphrase bestätigen	Geben Sie die Sicherungs-Passphrase erneut ein.

Option	Beschreibung
DNS-Auflösung	Geben Sie eine IP-Adresse für den DNS-Server ein, den Sie in der vSphere IaaS control plane-Umgebung verwenden. Beispielsweise `10.14.7.12`.
DNS-Suchdomäne	Geben Sie eine Domänenzeichenfolge ein.

4 (Optional) Konfigurieren Sie die Einstellungen für **E-Mail/SMTP**.

Option	Beschreibung
SMTP-Quelle	Wählen Sie eine der folgenden Optionen aus: **Keine**, **Lokaler Host**, **SMTP-Server** oder **Anonymer Server**. Standard ist **Lokaler Host**.
Von Adresse	E-Mail-Adresse.

5 Klicken Sie auf **Weiter**.

6 Konfigurieren Sie die Einstellungen für mehrere Mandanten.

a Behalten Sie die Standardeinstellung für den Mandantenzugriff bei.

b Wählen Sie **Cloud nach einrichten** aus und klicken Sie auf **Speichern**.

> **Hinweis** Wenn Sie vor dem Speichern die Option **Cloud nach einrichten** nicht ausgewählt haben, wird der Assistent für die Erstkonfiguration beendet. Das Cloud-Konfigurationsfenster wird nicht automatisch gestartet, und Sie werden zu einer Dashboard-Ansicht auf dem Controller geleitet. Navigieren Sie in diesem Fall zu **Infrastruktur > Clouds** und konfigurieren Sie die Cloud.

7 Konfigurieren Sie die **VMware vCenter/vSphere ESX**-Cloud. Klicken Sie auf **Erstellen** und wählen Sie **VMware vCenter/vSphere ESX** als Cloud-Typ aus.

Die Einstellungsseite für **NEUE CLOUD** wird angezeigt.

8 Konfigurieren Sie die Einstellungen **Allgemein**.

Option	Beschreibung
Name	Geben Sie einen Namen für die Cloud ein. Beispiel: **`Benutzerdefinierte Cloud`**.
Typ	Der Cloud-Typ ist **VMware vCenter/vSphere ESX**.

9 (Optional) Wählen Sie im Abschnitt **Standard-Netzwerk-IP-Adressenverwaltung** die Option **DHCP aktiviert** aus, wenn DHCP auf den vSphere-Portgruppen verfügbar ist.

Lassen Sie die Option deaktiviert, wenn die Dienst-Engine-Schnittstellen nur statische IP-Adressen verwenden sollen. Sie können sie für jedes Netzwerk einzeln konfigurieren.

Weitere Informationen finden Sie unter Konfigurieren eines virtuellen IP-Netzwerks.

10 Konfigurieren Sie die **Einstellungen für die Platzierung von virtuellen Diensten**.

Option	Beschreibung
Bevorzugen von statischen Routen im Vergleich zum direkt verbundenen Netzwerk für die Platzierung virtueller Dienste	Wählen Sie diese Option aus, um zu erzwingen, dass die Dienst-Engine-VM auf das Servernetzwerk zugreift, indem sie über das Standard-Gateway geroutet wird. Standardmäßig verbindet der Controller eine Netzwerkkarte direkt mit dem Servernetzwerk. Sie müssen erzwingen, dass die Dienst-Engine ausschließlich eine Verbindung zum Datennetzwerk herstellt und Daten an das Arbeitslastnetzwerk weiterleitet.
Verwenden von statischen Routen für die Netzwerkauflösung der VIP	Lassen Sie diese Option unausgewählt.

11 Konfigurieren Sie die Anmeldedaten für **vCenter/vSphere**.

Klicken Sie auf **Anmeldedaten festlegen** und geben Sie die folgenden Details an:

Option	Bezeichnung
vCenter-Adresse	Geben Sie den vCenter Server-Hostnamen oder die IP-Adresse für die vSphere IaaS control plane-Umgebung ein.
Benutzername	Geben Sie den Benutzernamen des vCenter-Administrators ein, z. B. administrator@vsphere.local. Um niedrigerstufige Berechtigungen zu verwenden, erstellen Sie eine dedizierte Rolle. Nähere Angaben finden Sie unter VMware-Benutzerrolle.
Kennwort	Geben Sie das Benutzerkennwort ein.
Zugriffsberechtigungen	**Lesen**: Sie erstellen und verwalten die Dienst-Engine-VMs. **Schreien**: Der Controller erstellt und verwaltet die Dienst-Engine-VMs. Sie müssen „Schreiben“ auswählen.

12 Konfigurieren Sie die Einstellungen für **Data Center**.

a Wählen Sie das vSphere **Datencenter**, in dem Sie die **Arbeitslastverwaltung** aktivieren möchten.

b Wählen Sie die Option **Inhaltsbibliothek verwenden** aus und wählen Sie die lokale Inhaltsbibliothek aus der Liste aus.

13 Wählen Sie **SPEICHERN UND NEU STARTEN** aus, um die **VMware vCenter/vSphere ESX**-Cloud mit den von Ihnen konfigurierten Einstellungen zu erstellen.

14 Konfigurieren Sie die Einstellungen für das **Netzwerk**.

Option	Beschreibung
Verwaltungsnetzwerk	Wählen Sie das VM-Netzwerk aus. Diese Netzwerkschnittstelle wird von den Dienst-Engines für die Verbindung mit dem Controller verwendet.
Dienst-Engine	Lassen Sie die **Vorlagen-Dienst-Engine-Gruppe** leer.
IP-Adressenverwaltung für das Verwaltungsnetzwerk	Wählen Sie **DHCP aktiviert** aus.

15 (Optional) Konfigurieren Sie die folgenden Netzwerkeinstellungen nur, wenn Sie **DHCP aktiviert** nicht auswählen.

Option	Beschreibung
IP-Subnetz	Geben Sie das IP-Subnetz für das Verwaltungsnetzwerk ein. Beispiel: `10.199.32.0/24`. **Hinweis** Geben Sie ein IP-Subnetz nur dann ein, wenn DHCP nicht verfügbar ist.
Standard-Gateway	Geben Sie das Standard-Gateway für das Verwaltungsnetzwerk ein, z. B. `10.199.32.253`. **Hinweis** Geben Sie ein IP-Subnetz nur dann ein, wenn DHCP nicht verfügbar ist.
Hinzufügen eines statischen IP-Adresspools	Geben Sie eine oder mehrere IP-Adressen oder einen IP-Adressbereich ein. Beispiel: `10.99.32.62-10.199.32.65`. **Hinweis** Geben Sie ein IP-Subnetz nur dann ein, wenn DHCP nicht verfügbar ist.

16 Erstellen Sie ein IPAM-Profil und konfigurieren Sie die Einstellungen für **IPAM/DNS**.

IPAM ist erforderlich, um virtuelle IP-Adressen beim Erstellen virtueller Dienst zuzuteilen.

a Wählen Sie im Menü „Weitere Aktionen“ von **IPAM-Profil** die Option **Erstellen** aus.

Die Seite **NEUES IPAM/DNS-PROFIL** wird angezeigt.

b Konfigurieren Sie das **IPAM-Profil**.

Option	Bezeichnung
Name	Benutzerdefinierte Zeichenfolge, z. B. **`ipam-profile`**
Typ	Wählen Sie **AVI Vantage IPAM** aus
IP in VRF zuteilen	Deaktivieren Sie diese Option.
Cloud	Wählen Sie in der Dropdown-Liste **Benutzerdefinierte Cloud** aus.

c Klicken Sie in **Nutzbares Netzwerk** auf **Hinzufügen** und wählen Sie das virtuelle IP-Netzwerk aus, das Sie konfiguriert haben. Dieses Netzwerk ist das primäre Netzwerk.

d Klicken Sie auf **SPEICHERN**.

17 (Optional) Konfigurieren Sie NTP-Einstellungen, wenn Sie einen internen NTP-Server verwenden möchten.

a Klicken Sie auf **Verwaltung > Einstellungen > DNS/NTP**.

b Löschen Sie vorhandene NTP-Server, sofern vorhanden, und geben Sie die IP-Adresse für den DNS-Server ein, den Sie verwenden. Beispiel: `192.168.100.1`.

Ergebnisse

Nachdem Sie die Konfiguration abgeschlossen haben, sehen Sie das Controller-**Dashboard**. Wählen Sie **Infrastruktur > Clouds** aus und stellen Sie sicher, dass der Status des Controllers für **Benutzerdefinierte Cloud** grün ist. Manchmal kann der Status für einige Zeit gelb sein, bis der Controller alle Portgruppen in der vCenter Server-Umgebung erkannt hat und grün wird.

Hinzufügen einer Lizenz

Nachdem Sie den NSX Advanced Load Balancer konfiguriert haben, müssen Sie ihm eine Lizenz hinzufügen. Der Controller wird im Testmodus gestartet, der über alle Funktionen verfügt, die einer verfügbaren Enterprise Edition-Lizenz entsprechen. Sie müssen dem Controller eine gültige Enterprise Tier-Lizenz zuweisen, bevor der Testzeitraum abläuft.

Voraussetzungen

Stellen Sie sicher, dass Sie über die Enterprise Tier-Lizenz verfügen.

Verfahren

1. Wählen Sie im Controller-Dashboard für NSX Advanced Load Balancer die Option **Verwaltung > Lizenzierung** aus.
2. Wählen Sie **Einstellungen**.
3. Wählen Sie **Enterprise Tier**.
4. Klicken Sie auf **SPEICHERN**.
5. Klicken Sie auf **Hochladen von Computer**, um die Lizenz hinzuzufügen.

   Nachdem die Lizenzdatei hochgeladen wurde, wird sie in der Liste der Controller-Lizenzen angezeigt. Das System zeigt die Informationen zur Lizenz an, einschließlich des Start- und Ablaufdatums.

Zuweisen eines Zertifikats zum Controller

Der Controller muss ein Zertifikat an Clients senden, um eine sichere Kommunikation herstellen zu können. Dieses Zertifikat muss einen **Subject Alternative Name (SAN)** (alternativer Antragstellername) aufweisen, der mit dem Hostnamen oder der IP-Adresse des NSX Advanced Load Balancer-Controller-Clusters übereinstimmt.

Der Controller verfügt über ein selbstsigniertes Standardzertifikat. Dieses Zertifikat verfügt jedoch nicht über das richtige SAN. Sie müssen es durch ein gültiges oder selbstsigniertes Zertifikat mit dem richtigen SAN ersetzen. Sie erstellen ein selbstsigniertes Zertifikat oder laden ein externes Zertifikat hoch.

Weitere Informationen zu Zertifikaten finden Sie in der Avi-Dokumentation.

Verfahren

1. Klicken Sie im Controller-Dashboard auf das Menü in der oberen linken Ecke und wählen Sie **Vorlagen > Sicherheit** aus.

2 Wählen Sie **SSL/TLS-Zertifikat** aus.

3 Zum Erstellen eines Zertifikats klicken Sie auf **Erstellen** und wählen Sie **Controller-Zertifikat** aus.

   Das Fenster **Neues Zertifikat (SSL/TLS)** wird geöffnet.

4 Geben Sie einen Namen für das Zertifikat ein.

5 Wenn kein vorab erstelltes gültiges Zertifikat vorhanden ist, fügen Sie ein selbstsigniertes Zertifikat hinzu, indem Sie für **Typ** die Option `Self Signed` auswählen.

   a Geben Sie die folgenden Details ein:

Option	Beschreibung
Allgemeiner Name	Geben Sie den vollqualifizierten Namen der Site an. Damit die Site als vertrauenswürdig eingestuft wird, muss dieser Eintrag mit dem Hostnamen übereinstimmen, den der Client im Browser eingegeben hat.
Algorithmus	Wählen Sie EC (Elliptic Curve Cryptography) oder RSA aus. EC wird empfohlen.
Schlüssellänge	Wählen Sie die Verschlüsselungsebene aus, die für Handshakes verwendet werden soll: ■ `SECP256R1` wird für EC-Zertifikate verwendet. ■ 2048 Bit wird für RSA-Zertifikate empfohlen.

   b Klicken Sie in **Subject Alternate Name (SAN)** auf **Hinzufügen**.

   c Geben Sie die IP-Adresse und/oder den FQDN des Clusters ein, wenn der Avi Controller als einzelner Knoten bereitgestellt wird. Wenn nur die IP-Adresse oder der FQDN verwendet wird, muss sie mit der IP-Adresse der Controller-VM übereinstimmen, die Sie während der Bereitstellung angeben.

      Weitere Informationen finden Sie unter Bereitstellen des NSX Advanced Load Balancer-Controllers.

      Geben Sie die Cluster-IP oder den FQDN des NSX Advanced Load Balancer-Controller-Clusters ein, wenn dieser als Cluster mit drei Knoten bereitgestellt wird. Informationen zum Bereitstellen eines Clusters mit drei Controller-Knoten finden Sie unter Bereitstellen eines Controller-Clusters.

   d Klicken Sie auf **Speichern**.

   Sie benötigen dieses Zertifikat, wenn Sie den Supervisor zum Aktivieren der Arbeitslastverwaltungsfunktion konfigurieren.

6 Laden Sie das selbstsignierte Zertifikat herunter, das Sie erstellen.

   a Klicken Sie auf **Sicherheit > SSL/TLS-Zertifikate**.

      Wenn das Zertifikat nicht angezeigt wird, aktualisieren Sie die Seite.

   b Wählen Sie das erstellte Zertifikat aus und klicken Sie auf das Download-Symbol.

c Klicken Sie auf der Seite **Zertifikat exportieren** für das Zertifikat auf **In Zwischenablage kopieren**. Kopieren Sie nicht den Schlüssel.

d Speichern Sie das kopierte Zertifikat für die spätere Verwendung, wenn Sie die Arbeitslastverwaltung aktivieren.

7 Wenn ein vorab erstelltes gültiges Zertifikat vorhanden ist, laden Sie es hoch, indem Sie für **Typ** die Option `Import` auswählen.

a Klicken Sie unter **Zertifikat** auf **Datei hochladen** und importieren Sie das Zertifikat.

Das SAN-Feld des Zertifikats, das Sie hochladen, muss über die IP-Adresse oder den FQDN des Controllers verfügen.

Hinweis Stellen Sie sicher, dass Sie den Inhalt des Zertifikats nur einmal hochladen oder einfügen.

b Klicken Sie in **Schlüssel (PEM) oder PKCS12** auf **Datei hochladen** und importieren Sie den Schlüssel.

c Klicken Sie **Validieren**, um das Zertifikat und den Schlüssel zu validieren.

d Klicken Sie auf **Speichern**.

8 Um das Portalzertifikat zu ändern, führen Sie die folgenden Schritte aus.

a Wählen Sie im Controller-Dashboard **Verwaltung > Systemeinstellungen** aus.

b Klicken Sie auf **Bearbeiten**.

c Wählen Sie die Registerkarte **Zugriff**.

d Entfernen Sie aus dem **SSL/TLS-Zertifikat** die vorhandenen Standardportalzertifikate.

e Wählen Sie im Dropdown-Menü das neu erstellte oder hochgeladene Zertifikat aus.

f Wählen Sie **Standardauthentifizierung** aus.

g Klicken Sie auf **SPEICHERN**.

Konfigurieren einer Dienst-Engine-Gruppe

vSphere IaaS control plane verwendet die Dienst-Engine-Gruppe **Standardgruppe**. Optional können Sie die **Standardgruppe**-Dienst-Engines in einer Gruppe konfigurieren, die die Platzierung und Anzahl der Dienst-Engine-VMs innerhalb von vCenter definiert. Sie können auch Hochverfügbarkeit konfigurieren, wenn sich der NSX Advanced Load Balancer-Controller im Enterprise-Modus befindet. vSphere IaaS control plane unterstützt lediglich die Dienst-Engine **Standardgruppe**. Andere Dienstmodulgruppen können nicht erstellt werden.

Informationen dazu, wie Sie bei einem Failover Überkapazitäten bereitstellen können, finden Sie in der Avi-Dokumentation.

Verfahren

1 Wählen Sie im NSX Advanced Load Balancer-Controller-Dashboard **Infrastruktur > Cloud-Ressourcen > Dienst-Engine-Gruppe** aus.

2 Klicken Sie auf der Seite **Dienst-Engine-Gruppe** auf das Bearbeitungssymbol in der **Standardgruppe**.

Die Registerkarte **Allgemeine Einstellungen** wird angezeigt.

vSphere IaaS control plane unterstützt lediglich die **Standardgruppe**.

3 Wählen Sie im Abschnitt **Platzierung** den **Hochverfügbarkeitsmodus** aus.

Die Standardoption ist `N + M (buffer)`. Sie können den Standardwert beibehalten oder eine der folgenden Optionen auswählen:

- `Active/Standy`
- `Active/Active`

4 Im Abschnitt **Dienst-Engine** können Sie Überkapazitäten für die Dienst-Engine-Gruppe konfigurieren.

Die Option **Anzahl der Dienst-Engines** definiert die maximale Anzahl an Dienst-Engines, die innerhalb einer Dienst-Engine-Gruppe erstellt werden können. Der Standardwert ist **10**.

Legen Sie zum Konfigurieren von Überkapazitäten einen Wert in den **Buffer Service Engines** fest. Der von Ihnen angegebenen Wert ist die Anzahl der VMs, die bereitgestellt werden, um im Fall eines Failovers Überkapazitäten zu gewährleisten.

Der Standardwert ist **1**.

5 Konfigurieren Sie im Abschnitt **Virtueller Dienst** die folgenden Optionen.

Option	Beschreibung
Virtuelle Dienste pro Dienstmodul	Die maximale Anzahl virtueller Dienste, die der Controller-Cluster auf einer der Dienst-Engines in der Gruppe platzieren kann. Geben Sie den Wert **1000** ein.
Platzierung virtueller Dienste über Dienst-Engines hinweg	Wählen Sie **Verteilt** aus. Wenn Sie diese Option auswählen, wird die Leistung maximiert, indem virtuelle Dienste auf neu hochgefahrenen Dienst-Engines platziert werden, bis die angegebene maximale Anzahl von Dienst-Engines erreicht ist. Der Standardwert ist **Kompakt**.

6 Sie können die Standardwerte für die anderen Einstellungen beibehalten.

7 Klicken Sie auf **Speichern**.

Konfigurieren von statischen Routen

Ein Standard-Gateway ermöglicht es der Dienst-Engine, Datenverkehr an die Pool-Server im Arbeitslastnetzwerk weiterzuleiten. Sie müssen die Gateway-IP des Datennetzwerks als Standard-Gateway konfigurieren. Die Dienst-Engines erhalten nicht die Standard-Gateway-IP von DHCP in den Datennetzwerken. Sie müssen statische Routen konfigurieren, damit die

Dienst-Engines den Datenverkehr ordnungsgemäß an die Arbeitslastnetzwerke und die Client-IP weiterleiten können.

Verfahren

1 Wählen Sie im NSX Advanced Load Balancer-Controller-Dashboard **Infrastruktur > Cloud-Ressourcen > VRF-Kontext** aus.

2 Klicken Sie auf **Erstellen**.

3 Geben Sie in **Allgemeine Einstellungen** einen Namen für den Routing-Kontext ein.

4 Klicken Sie im Abschnitt **Statische Route** auf **HINZUFÜGEN**.

5 Geben Sie in **Gateway-Subnetz** `172.16.10.0/24` ein.

6 Geben Sie unter **Nächster Hop** die Gateway-IP-Adresse für das Datennetzwerk ein.

   Beispiel: `192.168.1.1`.

7 (Optional) Wählen Sie **BGP-Peering** aus, um lokale BGP- und Peer-Details zu konfigurieren.

   Weitere Informationen finden Sie in der Avi-Dokumentation.

8 Klicken Sie auf **Speichern**.

Konfigurieren eines virtuellen IP-Netzwerks

Konfigurieren Sie ein virtuelles IP-Subnetz (VIP) für das Datennetzwerk. Sie können den VIP-Bereich konfigurieren, der verwendet werden soll, wenn ein virtueller Dienst im bestimmten VIP-Netzwerk platziert wird. Sie können DHCP für die Dienstmodule konfigurieren. Wenn DHCP nicht verfügbar ist, können Sie optional einen Pool von IP-Adressen konfigurieren, die der Service Engine-Schnittstelle in diesem Netzwerk zugewiesen werden. vSphere IaaS control plane unterstützt nur ein einziges VIP-Netzwerk.

Verfahren

1 Wählen Sie im NSX Advanced Load Balancer-Controller-Dashboard **Infrastruktur > Cloud-Ressourcen > Netzwerke** aus.

2 Wählen Sie die Cloud aus der Liste aus.

   Wählen Sie beispielsweise **Standard-Cloud** aus.

3 Geben Sie einen Namen für das Netzwerk ein.

   Beispiel: `Data Nework`.

4 Lassen Sie **DHCP aktiviert** ausgewählt, wenn DHCP im Datennetzwerk verfügbar ist.

   Deaktivieren Sie diese Option, wenn DHCP nicht verfügbar ist.

5 Wählen Sie **Automatische Konfiguration von IPv6 aktivieren** aus.

   Der NSX Advanced Load Balancer-Controller erkennt das Netzwerk-CIDR automatisch, wenn eine VM im Netzwerk ausgeführt und mit dem Typ **Erkannt** angezeigt wird.

6 Wenn der NSX Advanced Load Balancer-Controller das IP-Subnetz automatisch erkennt, konfigurieren Sie den IP-Bereich für das Subnetz.

   a Bearbeiten Sie die Einstellungen.

   b Geben Sie ein **Subnetz-Präfix** ein.

   c Wenn DHCP für die IP-Adresse der Dienst-Engine verfügbar ist, deaktivieren Sie **Statische IP-Adresse für VIPs und SE verwenden**.

   d Geben Sie eine oder mehrere IP-Adressen oder IP-Adressbereiche ein.

   Beispielsweise `10.202.35.1-10.202.35.254`.

   Hinweis Sie können eine IP-Adresse eingeben, die mit `0` endet. Wie beispielsweise `192.168.0.0`, und ignorieren Sie alle eingeblendeten Warnungen.

   e Klicken Sie auf **Speichern**.

7 Wenn der Controller ein IP-Subnetz und dessen Typ nicht findet, führen Sie die folgenden Schritte aus:

   a Klicken Sie auf **Hinzufügen**.

   b Geben Sie ein **Subnetz-Präfix** ein.

   c Klicken Sie auf **Hinzufügen**.

   d Wenn DHCP für die IP-Adresse der Dienst-Engine verfügbar ist, deaktivieren Sie **Statische IP-Adresse für VIPs und SE verwenden**.

   e Geben Sie in **IP-Adresse** den CIDR des Netzwerks ein, das die virtuellen IP-Adressen liefert.

   Beispielsweise `10.202.35.0/22`

   f Geben Sie eine oder mehrere IP-Adressen oder IP-Adressbereiche ein.

   Der Bereich muss eine Teilmenge des Netzwerk-CIDR im **IP-Subnetz sein**. Beispielsweise `10.202.35.1-10.202.35.254`.

   Hinweis Sie können eine IP-Adresse eingeben, die mit `0` endet. Wie beispielsweise `192.168.0.0`, und ignorieren Sie alle eingeblendeten Warnungen.

   g Klicken Sie auf **Speichern**, um die Subnetzkonfiguration zu speichern.

   Auf der Seite **Netzwerk** sind das IP-Subnetz mit dem Typ **Konfiguriert** sowie ein IP-Adressenpool aufgeführt.

8 Klicken Sie auf **Speichern**, um die Netzwerkeinstellungen zu speichern.

Ergebnisse

Auf der Seite **Netzwerk** werden die konfigurierten Netzwerke aufgeführt.

Beispiel

Das `Primary Workload Network`-Netzwerk zeigt das gefundene Netzwerk als `10.202.32.0/22` und konfigurierte Subnetze als `10.202.32.0/22 [254/254]` an. Dies weist darauf hin, dass 254 virtuelle IP-Adressen von `10.202.32.0/22` stammen. Beachten Sie, dass der IP-Bereich in der Übersichtsansicht nicht als `10.202.35.1-10.202.35.254` aufgeführt ist.

Testen Sie den NSX Advanced Load Balancer

Überprüfen Sie nach der Bereitstellung und Konfiguration der NSX Advanced Load Balancer-Steuerungsebene deren Funktionalität.

Verfahren

1. Wechseln Sie im Avi Controller-Dashboard zu **Infrastructure > Clouds**.
2. Stellen Sie sicher, dass der Status des Controllers für **Default-Cloud** grün ist.

   Informationen zur Fehlerbehebung bei möglicherweise auftretenden Problemen finden Sie unter Erfassen von Support-Paketen für die NSX Advanced Load Balancer-Fehlerbehebung.

Installieren und Konfigurieren des HAProxy-Lastausgleichsdiensts

VMware stellt eine Implementierung des Open-Source-HAProxy-Lastausgleichsdiensts bereit, den Sie in Ihrer vSphere IaaS control plane-Umgebung verwenden können. Wenn Sie vSphere Distributed Switch (vDS)-Netzwerke für **Arbeitslastverwaltung** verwenden, können Sie den HAProxy-Lastausgleichsdienst installieren und konfigurieren.

Erstellen eines vSphere Distributed Switch für einen Supervisor für die Verwendung mit dem HAProxy-Lastausgleichsdienst

Zum Konfigurieren eines vSphere-Clusters als Supervisor, der den vSphere-Netzwerk-Stack und den HAProxy-Lastausgleichsdienst verwendet, müssen Sie die Hosts einem vSphere Distributed Switch hinzufügen. Sie müssen Portgruppen auf dem Distributed Switch erstellen, den Sie als Arbeitslastnetzwerke für den Supervisor konfigurieren.

Sie können je nach der Isolationsstufe, die Sie für die im Cluster ausgeführten Kubernetes-Arbeitslasten bereitstellen möchten, zwischen verschiedenen Topologien für den Supervisor auswählen.

Voraussetzungen

- Überprüfen Sie die Systemanforderungen für die Verwendung des vSphere-Netzwerks für den Supervisor mit dem HAProxy-Lastausgleichsdienst. Weitere Informationen finden Sie unter Anforderungen zum Aktivieren eines Supervisors mit drei Zonen mit HAProxy-Lastausgleichsdienst und Anforderungen zum Aktivieren eines Supervisors mit einem einzelnen Cluster mit VDS-Netzwerk und HAProxy-Lastausgleichsdienst *Konzepte und Planung der vSphere IaaS-Steuerungsebene*.

- Ermitteln Sie die Topologie für die Einrichtung von Arbeitslastnetzwerken mit HAProxy auf dem Supervisor. Weitere Informationen finden Sie unter Topologien für die Bereitstellung des HAProxy-Lastausgleichsdiensts in *Konzepte und Planung der vSphere IaaS-Steuerungsebene*.

Verfahren

1 Navigieren Sie im vSphere Client zu einem Datencenter.

2 Klicken Sie mit der rechten Maustaste auf das Datencenter und wählen Sie **Distributed Switch > Neuer Distributed Switch** aus.

3 Geben Sie einen Namen für den Switch ein, z. B. **`Distributed Switch für Arbeitslast`** und klicken Sie auf **Weiter**.

4 Wählen Sie Version 7.0 für den Switch aus und klicken Sie auf **Weiter**.

5 Geben Sie unter **Portgruppenname** **`Primäres Arbeitslastnetzwerk`** ein, klicken Sie auf **Weiter** und dann auf **Beenden**.

   Ein neuer Distributed Switch mit einer Portgruppe wird im Datencenter erstellt. Sie können diese Portgruppe als das primäre Arbeitslastnetzwerk für den Supervisor verwenden, den Sie erstellen werden. Das primäre Arbeitslastnetzwerk verarbeitet den Datenverkehr für die Kubernetes-Steuerungsebenen-VMs.

6 Erstellen Sie verteilte Portgruppen für Arbeitslastnetzwerke.

   Wie viele Portgruppen Sie erstellen, hängt von der Topologie ab, die Sie für den Supervisor implementieren möchten. Erstellen Sie für eine Topologie mit einem isolierten Arbeitslastnetzwerk eine verteilte Portgruppe, die Sie als Netzwerk für alle Namespaces auf dem Supervisor verwenden werden. Erstellen Sie für eine Topologie mit isolierten Netzwerken für jeden Namespace dieselbe Anzahl an Portgruppen wie die Anzahl der von Ihnen zu erstellenden Namespaces.

   a Navigieren Sie zum neu erstellten Distributed Switch.

   b Klicken Sie mit der rechten Maustaste auf den Switch und wählen Sie **Verteilte Portgruppen > Neue verteilte Portgruppe** aus.

   c Geben Sie einen Namen für die Portgruppe ein, z. B. **`Arbeitslastnetzwerk`**, und klicken Sie auf **Weiter**.

   d Behalten Sie die Standardeinstellungen bei, klicken Sie auf **Weiter** und dann auf **Beenden**.

7 Fügen Sie Hosts aus den vSphere-Clustern hinzu, die Sie als Supervisor für den Distributed Switch konfigurieren werden.

   a Klicken Sie mit der rechten Maustaste auf den Distributed Switch und wählen Sie **Hosts hinzufügen und verwalten** aus.

   b Wählen Sie **Hosts hinzufügen** aus.

   c Klicken Sie auf **Neue Hosts**, wählen Sie die Hosts aus dem vSphere-Cluster aus, den Sie als Supervisor konfigurieren werden, und klicken Sie auf **Weiter**.

d Wählen Sie eine physische Netzwerkkarte für jeden Host aus und weisen Sie ihr einen Uplink auf dem Distributed Switch zu.

e Klicken Sie in den verbleibenden Bildschirmen des Assistenten auf **Weiter** und dann auf **Beenden**.

Ergebnisse

Die Hosts werden dem Distributed Switch hinzugefügt. Sie können jetzt die Portgruppen, die Sie auf dem Switch erstellt haben, als Arbeitslastnetzwerke für den Supervisor verwenden.

Bereitstellen der Steuerungsebenen-VM des HAProxy-Lastausgleichdiensts

Wenn Sie den vSphere-Netzwerk-Stack für Kubernetes-Arbeitslasten verwenden möchten, installieren Sie die HAProxy-Steuerungsebenen-VM, um Lastausgleichsdienste für Tanzu Kubernetes bereitzustellen.

Voraussetzungen

- Stellen Sie sicher, dass Ihre Umgebung die Computing- und Netzwerkanforderungen für die Bereitstellung des HA-Proxys erfüllt. Weitere Informationen finden Sie unter Anforderungen zum Aktivieren eines Supervisors mit drei Zonen mit HAProxy-Lastausgleichsdienst und Anforderungen zum Aktivieren eines Supervisors mit einem einzelnen Cluster mit VDS-Netzwerk und HAProxy-Lastausgleichsdienst *Konzepte und Planung der vSphere IaaS-Steuerungsebene*.
- Stellen Sie sicher, dass sie über ein Verwaltungsnetzwerk auf einem vSphere Standard- oder Distributed Switch verfügen, auf dem der HAProxy-Lastausgleichsdienst bereitgestellt werden soll. Der Supervisor kommuniziert mit dem HAProxy-Lastausgleichsdienst in diesem Verwaltungsnetzwerk.
- Erstellen Sie einen vSphere Distributed Switch und Portgruppen für Arbeitslastnetzwerke. Der HAProxy-Lastausgleichsdienst kommuniziert mit Supervisor- und Tanzu Kubernetes-Clusterknoten über die Arbeitslastnetzwerke. Weitere Informationen finden Sie unter Erstellen eines vSphere Distributed Switch für einen Supervisor für die Verwendung mit dem HAProxy-Lastausgleichsdienst. Informationen zu Arbeitslastnetzwerken finden Sie unter Arbeitslastnetzwerke im Supervisor-Cluster in *Konzepte und Planung der vSphere IaaS-Steuerungsebene*.
- Laden Sie die neueste Version der VMware HAProxy-OVA-Datei von der VMware-HAProxy-Site herunter.
- Wählen Sie eine Topologie für die Bereitstellung des HAProxy-Lastausgleichsdiensts und der Arbeitslastnetzwerke auf dem Supervisor aus. Weitere Informationen finden Sie unter Topologien für die Bereitstellung des HAProxy-Lastausgleichsdiensts in *Konzepte und Planung der vSphere IaaS-Steuerungsebene*.

Es kann hilfreich sein, sich eine Demonstration der Verwendung von vSphere IaaS control plane mit vDS-Netzwerk und HAProxy anzusehen. Sehen Sie sich das Video Erste Schritte bei der Verwendung von vSphere with Tanzu an.

Verfahren

1 Melden Sie sich über vSphere Client bei vCenter Server an.

2 Erstellen Sie eine neue VM aus der HAProxy-OVA-Datei.

Option	Beschreibung
Inhaltsbibliothek	Wenn Sie die OVA in eine lokale Inhaltsbibliothek importiert haben: ■ Wechseln Sie zu **Menü > Inhaltsbibliothek**. ■ Wählen Sie die Bibliothek, in der Sie die OVA importiert haben. ■ Wählen Sie die Vorlage `vmware-haproxy-vX.X.X` aus. ■ Klicken Sie mit der rechten Maustaste und wählen Sie **Neue VM über diese Vorlage** aus.
Lokale Datei	Wenn Sie die OVA-Datei auf Ihren lokalen Host heruntergeladen haben: ■ Wählen Sie den vCenter-Cluster aus, in dem Sie **Arbeitslastverwaltung** aktivieren werden. ■ Klicken Sie mit der rechten Maustaste und wählen Sie **OVF-Vorlage bereitstellen**. ■ Wählen Sie **Lokale Datei** aus und klicken Sie auf **Dateien hochladen**. ■ Navigieren Sie zur Datei `vmware-haproxy-vX.X.X.ova` und wählen Sie sie aus.

3 Geben Sie einen **Namen der virtuellen Maschine** ein, z. B. **`haproxy`**.

4 Wählen Sie das **Datencenter** aus, in dem Sie HAProxy einsetzen, und klicken Sie auf **Weiter**.

5 Wählen Sie den vCenter-Cluster aus, in dem Sie **Arbeitslastverwaltung** aktivieren möchten, und klicken Sie auf **Weiter**.

6 Überprüfen und bestätigen Sie die Bereitstellungsdetails und klicken Sie auf **Weiter**.

7 Akzeptieren Sie die Lizenzvereinbarungen und klicken Sie auf **Weiter**.

8 Wählen Sie eine Bereitstellungskonfiguration. Weitere Informationen finden Sie unter HAProxy-Netzwerktopologie in *Konzepte und Planung der vSphere IaaS-Steuerungsebene* .

Konfiguration	Beschreibung
Standard	Wählen Sie diese Option aus, um die Appliance mit 2 Netzwerkkarten bereitzustellen: ein Verwaltungsnetzwerk und ein einzelnes Arbeitslastnetzwerk.
Frontend-Netzwerk	Wählen Sie diese Option aus, um die Appliance mit 3 Netzwerkkarten bereitzustellen. Das Subnetz „Frontend“ wird verwendet, um Clusterknoten aus dem Netzwerk zu isolieren, das von Entwicklern für den Zugriff auf die Cluster-Steuerungsebene verwendet wird.

9 Wählen Sie die Speicherrichtlinie, die für die VM verwendet werden soll, und klicken Sie auf **Weiter**.

10 Wählen Sie die Netzwerkschnittstellen, die für den Lastausgleichsdienst verwendet werden sollen, und klicken Sie auf **Weiter**.

Quellnetzwerk	Zielnetzwerk
Verwaltung	Wählen Sie das Verwaltungsnetzwerk aus, wie z. B. **`VM-Netzwerk`**.
Arbeitslast	Wählen Sie die für **Arbeitslastverwaltung** konfigurierte vDS-Portgruppe aus.
Frontend	Wählen Sie die für das Frontend-Subnetz konfigurierte vDS-Portgruppe aus. Wenn Sie die Konfiguration „Frontend“ nicht auswählt haben, wird diese Einstellung während der Installation ignoriert; Sie können somit die Standardeinstellung lassen.

Hinweis Das Arbeitslastnetzwerk muss sich in einem anderen Subnetz als das Verwaltungsnetzwerk befinden. Weitere Informationen finden Sie unter Anforderungen zum Aktivieren eines Drei-Zonen-Supervisors mit HA-Proxy-Lastausgleichsdienst und Anforderungen zum Aktivieren eines Supervisors mit VDS-Netzwerk und HAProxy-Lastausgleichsdienst *Konzepte und Planung der vSphere IaaS-Steuerungsebene*.

11 Passen Sie die Konfigurationseinstellungen der Anwendung an. Weitere Informationen finden Sie unter Appliance-Konfigurationseinstellungen.

12 Geben Sie die Netzwerkkonfigurationsdetails an. Weitere Informationen hierzu finden Sie unter Netzwerkkonfiguration.

13 Konfigurieren Sie den Lastausgleichsdienst. Weitere Informationen hierzu finden Sie unter Einstellungen zum Lastausgleich.

14 Klicken Sie auf **Weiter**, um die Konfiguration der OVA abzuschließen.

15 Überprüfen Sie die Konfigurationsdetails für die Bereitstellung und klicken Sie auf **Beenden**, um die OVA bereitzustellen.

16 Überwachen Sie die Bereitstellung der VM mithilfe des Fensterbereichs **Aufgaben**.

17 Wenn die Bereitstellung der VM abgeschlossen ist, schalten Sie sie ein.

Nächste Schritte

Sobald der HAProxy-Lastausgleichsdienst erfolgreich bereitgestellt ist und eingeschaltet wurde, fahren Sie mit der Aktivierung der **Arbeitslastverwaltung** fort. Weitere Informationen hierzu finden Sie unter Kapitel 12 Konfigurieren und Verwalten eines Supervisors.

Anpassen des HAProxy-Lastausgleichdiensts

Passen Sie die VM der HAProxy-Steuerungsebene an, einschließlich Konfigurationseinstellungen, Netzwerkeinstellungen und Lastausgleichseinstellungen.

Appliance-Konfigurationseinstellungen

In der Tabelle sind die Parameter für die Konfiguration der HAProxy-Appliance aufgelistet und beschrieben.

Parameter	Beschreibung	Anmerkung oder Beispiel
Root-Kennwort	Anfängliches Kennwort für den-root-Benutzer (6-128 Zeichen).	Im Betriebssystem müssen nachfolgende Kennwortänderungen durchgeführt werden.
Root-Anmeldung zulassen	Option, mit der sich der Root-Benutzer über SSH bei der VM anmelden kann.	Für die Fehlerbehebung ist möglicherweise eine Root-Anmeldung erforderlich. Beachten Sie dabei jedoch die damit verbundenen Auswirkungen auf die Sicherheit.
TLS-Zertifizierungsstelle (ca.crt)	Wenn Sie das selbstsignierte CA-Zertifikat verwenden möchten, lassen Sie dieses Feld leer. Um Ihr eigenes CA-Zertifikat (ca.crt) zu verwenden, fügen Sie den Inhalt in dieses Feld ein. Möglicherweise müssen Sie den Inhalt mit Base64 kodieren. https://www.base64encode.org/	Wenn Sie das selbstsignierte CA-Zertifikat verwenden, werden die öffentlichen und privaten Schlüssel aus dem Zertifikat generiert.
Schlüssel (ca.key)	Wenn Sie das selbstsignierte Zertifikat verwenden, lassen Sie dieses Feld leer. Wenn Sie ein CA-Zertifikat angegeben haben, müssen Sie die Inhalte des privaten Schlüssels des Zertifikats in dieses Feld einfügen.	

Netzwerkkonfiguration

In der Tabelle sind die Parameter für die HAProxy-Netzwerkkonfiguration aufgelistet und beschrieben.

Parameter	Beschreibung	Anmerkung oder Beispiel
Hostname	Der Hostname (oder FQDN), der der VM der HAProxy-Steuerungsebene zugeordnet werden soll	Standardwert: `haproxy.local`
DNS	Eine durch Kommas getrennte Liste der IP-Adressen des DNS-Servers.	Standardwerte: `1.1.1.1, 1.0.0.1` Beispielwert: `10.8.8.8`
IP-Verwaltung	Die statische IP-Adresse der VM der HAProxy-Steuerungsebene auf dem Verwaltungsnetzwerk.	Eine gültige IPv4-Adresse mit der Präfixlänge des Netzwerks, beispielsweise: `192.168.0.2/24`.
Verwaltungs-Gateway	Die IP-Adresse des Gateways für das Verwaltungsnetzwerk.	Beispiel: `192.168.0.1`

Parameter	Beschreibung	Anmerkung oder Beispiel
Arbeitslast-IP	Die statische IP-Adresse der VM der HAProxy-Steuerungsebene auf dem Arbeitslastnetzwerk. Diese IP-Adresse muss sich außerhalb des IP-Adressbereichs des Lastausgleichsdiensts befinden.	Eine gültige IPv4-Adresse mit der Präfixlänge des Netzwerks, beispielsweise: `192.168.10.2/24`.
Arbeitslast-Gateway	Die IP-Adresse des Gateways für das Arbeitslastnetzwerk.	Beispiel: `192.168.10.1` Wenn Sie die Konfiguration „Frontend“ auswählen, müssen Sie ein Gateway eingeben. Die Bereitstellung wird nicht erfolgreich ausgeführt, wenn „Frontend“ ausgewählt ist und kein Gateway angegeben wird.
Frontend-IP	Die statische IP-Adresse der HAProxy-Appliance im Frontend-Netzwerk. Dieser Wert wird nur verwendet, wenn das Bereitstellungsmodell „Frontend“ ausgewählt ist.	Eine gültige IPv4-Adresse mit der Präfixlänge des Netzwerks, zum Beispiel: `192.168.100.2/24`
Frontend-Gateway	Die IP-Adresse des Gateways für das Netzwerk „Frontend“. Dieser Wert wird nur verwendet, wenn das Bereitstellungsmodell „Frontend“ ausgewählt ist.	Beispiel: `192.168.100.1`

Einstellungen zum Lastausgleich

In der Tabelle werden die Parameter für die Konfiguration des HAProxy-Lastausgleichsdiensts aufgelistet.

Parameter	Beschreibung	Beispiel oder Anmerkung
IP-Bereich(e) des Lastausgleichsdiensts	In diesem Feld geben Sie einen Bereich von IPv4-Adressen an, der das CIDR-Format verwendet. Der Wert muss ein gültiger CIDR-Bereich sein, oder die Installation schlägt fehl. HAProxy reserviert die IP-Adressen für virtuelle IPs (VIPs). Nach der Zuweisung wird jede VIP-Adresse zugeteilt, und der HAProxy antwortet auf Anfragen an diese Adresse. Der hier angegebene CIDR-Bereich darf sich nicht mit den IPs überschneiden, die Sie für die virtuellen Server zuweisen, wenn Sie **Arbeitslastverwaltung** im vCenter Server mithilfe des vSphere Client aktivieren. **Hinweis** Der IP-Bereich des Lastausgleichsdiensts muss sich auf einem anderen Subnetz als das Verwaltungsnetzwerk befinden. Er wird nicht unterstützt, wenn sich der IP-Bereich des Lastausgleichsdiensts im selben Subnetz wie das Verwaltungsnetzwerk befindet.	So gibt der Netzwerk-CIDR `192.168.100.0/24` beispielsweise dem Lastausgleichsdienst 256 virtuelle IP-Adressen im Bereich `192.168.100.0 - 192.168.100.255`. So gibt der Netzwerk-CIDR `192.168.100.0/25` beispielsweise dem Lastausgleichsdienst 128 virtuelle IP-Adressen im Bereich `192.168.100.0 - 192.168.100.127`.
Verwaltungsport der Datenebenen-API	Der Port auf der HAProxy-VM, den der API-Dienst des Lastausgleichsdiensts abhört.	Ein gültiger Port. Port 22 ist für SSH reserviert. Der Standardwert ist `5556`.
HAProxy-Benutzerkennung	Benutzername für Lastausgleichsdienst-API	Dies ist der Benutzername, mit dem sich die Clients beim API-Dienst des Lastausgleichsdiensts authentifizieren können. **Hinweis** Sie benötigen diesen Benutzernamen zur Aktivierung des Supervisor.
Kennwort für HAProxy	Kennwort für Lastausgleichsdienst-API	Dies ist das Kennwort, mit dem sich die Clients beim API-Dienst des Lastausgleichsdiensts authentifizieren können. **Hinweis** Sie benötigen dieses Kennwort zur Aktivierung des Supervisor.

Bereitstellen eines Supervisor für drei Zonen

5

Stellen Sie einen Supervisor für drei vSphere-Zonen bereit, um Hochverfügbarkeit auf Clusterebene bereitzustellen. Jede vSphere-Zone wird einem vSphere-Cluster zugeordnet.

Hinweis Wenn Sie Ihre vSphere IaaS control plane-Umgebung von einer vSphere-Version vor 8.0 aktualisiert haben und vSphere Zonen für Ihre Bereitstellungen wie Tanzu Kubernetes Grid-Cluster verwenden möchten, müssen Sie einen neuen Supervisor mit drei Zonen erstellen.

Lesen Sie als Nächstes die folgenden Themen:

- Bereitstellen eines Supervisor für drei Zonen mit dem VDS-Netzwerk-Stack
- Bereitstellen eines Supervisors für drei Zonen mit dem NSX-Netzwerk

Bereitstellen eines Supervisor für drei Zonen mit dem VDS-Netzwerk-Stack

Erfahren Sie, wie Sie einen Supervisor mit dem VDS-Netzwerk-Stack auf drei vSphere-Zonen bereitstellen. Jede vSphere-Zone wird einem vSphere-Cluster zugeordnet. Durch die Bereitstellung des Supervisor auf drei vSphere-Zonen stellen Sie Hochverfügbarkeit für Ihre Arbeitslasten auf Clusterebene bereit. Ein Supervisor, der mit VDS-Netzwerk konfiguriert ist, unterstützt Tanzu Kubernetes Grid-Cluster und VMs, die über den VM-Dienst erstellt wurden. Er unterstützt nicht vSphere-Pods.

Voraussetzungen

- Erfüllen Sie die Voraussetzungen zum Konfigurieren von vSphere-Clustern als Supervisor. Weitere Informationen hierzu finden Sie unter Voraussetzungen für die Konfiguration von vSphere IaaS control plane in vSphere-Cluster.
- Erstellen Sie drei vSphere-Zonen. Weitere Informationen hierzu finden Sie unter Kapitel 3 Erstellen von vSphere-Zonen für eine Supervisor-Bereitstellung mit mehreren Zonen.

Verfahren

1 Wählen Sie im Startmenü die Option **Arbeitslastverwaltung** aus.

2 Wählen Sie eine Lizenzierungsoption für den Supervisor aus.

   - Wenn Sie über eine gültige Tanzu Edition-Lizenz verfügen, klicken Sie auf **Lizenz hinzufügen**, um den Lizenzschlüssel der Lizenzbestandsliste von vSphere hinzuzufügen.
   - Wenn Sie noch keine Tanzu Edition-Lizenz haben, geben Sie die Kontaktdetails ein, damit Sie Mitteilungen von VMware empfangen können, und klicken Sie auf **Erste Schritte**.

   Der Testzeitraum eines Supervisors beträgt 60 Tage. Innerhalb dieses Zeitraums müssen Sie dem Cluster eine gültige Tanzu Edition-Lizenz zuweisen. Wenn Sie einen Tanzu Edition-Lizenzschlüssel hinzugefügt haben, können Sie diesen Schlüssel innerhalb des 60-Tage-Testzeitraums zuweisen, sobald Sie die Einrichtung des Supervisors abgeschlossen haben.

3 Klicken Sie auf dem Bildschirm **Arbeitslastverwaltung** erneut auf **Erste Schritte**.

4 Wählen Sie die Seite **vCenter Server und Netzwerk** aus, wählen Sie das vCenter Server-System aus, das für die Supervisor-Bereitstellung eingerichtet ist, wählen Sie **vSphere Distributed Switch (VDS)** als Netzwerk-Stack aus und klicken Sie auf **Weiter**.

5 Wählen Sie auf der Seite **Supervisor-Standort** die Option **vSphere-Zonenbereitstellung** aus, um einen Supervisor auf drei vSphere-Zonen bereitzustellen.

   a Geben Sie einen Namen für den neuen Supervisor ein.

   b Wählen Sie das Datencenter aus, in dem Sie die vSphere-Zonen für die Bereitstellung von Supervisor erstellt haben.

   c Wählen Sie aus der Liste der kompatiblen vSphere-Zonen drei Zonen aus.

   d Klicken Sie auf **Weiter**.

6 Konfigurieren Sie auf der Seite **Speicher** den Speicher für die Platzierung von Steuerungsebenen-VMs.

Option	Bezeichnung
Steuerungsebenenknoten	Wählen Sie die Speicherrichtlinie für die Platzierung der Control Plane-VMs aus.

7 Konfigurieren Sie auf dem Bildschirm **Lastausgleichsdienst** die Einstellungen eines Lastenausgleichs.

a Geben Sie einen Namen für den Lastausgleichsdienst ein.

b Wählen Sie den Typ des Lastausgleichsdiensts aus.

Sie können zwischen **NSX Advanced Load Balancer** und **HAProxy** auswählen.

c Konfigurieren Sie die Einstellungen für den Lastausgleichsdienst

- Geben Sie die folgenden Einstellungen für den NSX Advanced Load Balancer ein:

Option	Beschreibung
Name	Geben Sie einen Namen für die NSX Advanced Load Balancer-VM ein.
Controller-Endpoint von NSX Advanced Load Balancer	Die IP-Adresse des NSX Advanced Load Balancer-Controllers. Der Standardport ist `443`.
Benutzername	Der Benutzername, der für den NSX Advanced Load Balancer konfiguriert ist. Sie verwenden diesen Benutzernamen für den Zugriff auf den Controller.
Kennwort	Das Kennwort für den Benutzernamen.
Serverzertifikat	Das vom Controller verwendete Zertifikat. Sie können das Zertifikat bereitstellen, das Sie während der Konfiguration zugewiesen haben. Weitere Informationen finden Sie unter Zuweisen eines Zertifikats zum Controller.
Cloud-Name	Geben Sie den Namen der von Ihnen eingerichteten benutzerdefinierten Cloud ein. Beachten Sie, dass beim Cloud-Namen die Groß-/Kleinschreibung beachtet wird. Um **Standard-Cloud** zu verwenden, lassen Sie dieses Feld leer. Weitere Informationen finden Sie unter Konfigurieren des Controllers.

- Geben Sie die folgenden Einstellungen für HAProxy ein:

Option	Beschreibung
Controller-Endpoint des HAProxy-Lastausgleichsdiensts	Die IP-Adresse und der Port der HAProxy-Datenebenen-API, wobei es sich um die Verwaltungs-IP-Adresse der HAProxy-Appliance handelt. Diese Komponente steuert den HAProxy-Server und wird in der HAProxy-VM ausgeführt.
Benutzername	Der Benutzername, der in der HAProxy-OVA-Datei konfiguriert ist. Sie verwenden diesen Namen für die Authentifizierung bei der HAProxy-Datenebenen-API.
Kennwort	Das Kennwort für den Benutzernamen.

Option	Beschreibung
Bereiche für virtuelle IPs	Bereich von IP-Adressen, die im Arbeitslastnetzwerk von Tanzu Kubernetes-Clustern verwendet werden. Dieser IP-Bereich stammt aus der Liste der IPs, die in dem CIDR definiert wurden, den Sie während der Bereitstellung der HAProxy-Appliance konfiguriert haben. Sie können den gesamten in der HAProxy-Bereitstellung konfigurierten Bereich festlegen, Sie können aber auch einen Teilbereich dieses CIDR festlegen, wenn Sie mehrere Supervisoren erstellen und IPs aus diesem CIDR-Bereich verwenden möchten. Dieser Bereich darf sich nicht mit dem für das Arbeitslastnetzwerk in diesem Assistenten definierten IP-Bereich überschneiden. Der Bereich darf sich außerdem nicht mit DHCP-Bereichen in diesem Arbeitslastnetzwerk überschneiden.
TLS-Zertifikat der HAProxy-Verwaltung	Das Zertifikat im PEM-Format, das signiert ist oder das ein vertrauenswürdiger Root des Serverzertifikats ist, das von der Datenebenen-API präsentiert wird. ■ Option 1: Wenn der Root-Zugriff aktiviert ist, melden Sie sich über SSH bei der HAProxy-VM als Root an und kopieren Sie `/etc/haproxy/ca.crt` in die **Zertifizierungsstelle für den Server**. Verwenden Sie keine Escapezeilen im `\n`-Format. ■ Option 2: Klicken Sie mit der rechten Maustaste auf die HAProxy-VM und wählen Sie **Einstellungen bearbeiten** aus. Kopieren Sie das CA-Zertifikat aus dem entsprechenden Feld und konvertieren Sie es aus Base64 mithilfe eines Konvertierungstools, wie z. B. https://www.base64decode.org/. ■ Option 3: Führen Sie das folgende PowerCLI-Skript aus. Ersetzen Sie die Variablen `$vc`, `$vc_user` und `$vc_password` durch entsprechende Werte. `$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`

Option	Beschreibung
	`` 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 ```

8 Konfigurieren Sie auf dem Bildschirm **Verwaltungsnetzwerk** die Parameter für das Netzwerk, das für die VMs der Kubernetes-Steuerungsebene verwendet wird.

a Wählen Sie einen **Netzwerkmodus** aus.

- **DHCP-Netzwerk**. In diesem Modus werden alle IP-Adressen für das Verwaltungsnetzwerk, wie IP-Adressen von Steuerungsebenen-VMs, eine Floating-IP-Adresse, DNS-Server, DNS, Suchdomänen und NTP-Server, automatisch von einem DHCP-Server erfasst. Zum Abrufen von Floating-IP-Adressen muss der DHCP-Server so konfiguriert werden, dass Clientbezeichner unterstützt werden. Im DHCP-Modus verwenden alle Steuerungsebenen-VMs stabile DHCP-Clientbezeichner zum Erfassen von IP-Adressen. Diese Clientbezeichner können verwendet werden, um eine Zuweisung statischer IP-Adressen für die IPs der Steuerungsebenen-VMs auf dem DHCP-Server einzurichten und dadurch sicherzustellen, dass sich diese nicht ändern. Ein Ändern der IP-Adressen von Steuerungsebenen-VMs und Floating-IP-Adressen wird nicht unterstützt.

  Sie können einige der von DHCP übernommenen Einstellungen überschreiben, indem Sie Werte in die Textfelder für diese Einstellungen eingeben.

Option	Beschreibung
Netzwerk	Wählen Sie das Netzwerk aus, das den Verwaltungsdatenverkehr für Supervisor verarbeiten wird.
Floating IP-Adresse	Geben Sie eine IP-Adresse ein, die den Startpunkt für die Reservierung von fünf aufeinanderfolgenden IP-Adressen für die Kubernetes-Steuerungsebenen-VMs wie folgt festlegt: ■ Eine IP-Adresse für jede der Kubernetes-Steuerungsebenen-VMs. ■ Eine Floating-IP-Adresse für eine der Kubernetes-Steuerungsebenen-VMs als Schnittstelle zum Verwaltungsnetzwerk. Die Steuerungsebenen-VM mit der zugewiesenen Floating-IP-Adresse fungiert als führende VM für alle drei Kubernetes-Steuerungsebenen-VMs. Die Floating IP-Adresse wird zum Knoten der Steuerungsebene verschoben, der als etcd-Leader im Kubernetes-Cluster fungiert. Dadurch wird die Verfügbarkeit im Falle eines Netzwerkpartitionsereignisses verbessert. ■ Eine IP-Adresse, die als Puffer dienen soll, falls eine Kubernetes-Steuerungsebenen-VM ausfällt und eine neue Steuerungsebenen-VM als Ersatz bereitgestellt wird.

Option	Beschreibung
DNS-Server	Geben Sie die Adressen der DNS-Server ein, die Sie in Ihrer Umgebung verwenden. Wenn das vCenter Server-System mit einem FQDN registriert ist, müssen Sie die IP-Adressen der DNS-Server eingeben, die Sie mit der vSphere-Umgebung verwenden, damit der FQDN im Supervisor aufgelöst werden kann.
DNS-Suchdomänen	Geben Sie Domänennamen ein, die von DNS innerhalb der Kubernetes Control Plane-Knoten durchsucht werden, z. B. `corp.local`, damit der DNS-Server sie auflösen kann.
NTP-Server	Geben Sie die Adressen der NTP-Server ein, die Sie in Ihrer Umgebung verwenden (sofern vorhanden).

- **Statisch**. Geben Sie alle Netzwerkeinstellungen für das Verwaltungsnetzwerk manuell ein.

Option	Beschreibung
Netzwerk	Wählen Sie das Netzwerk aus, das den Verwaltungsdatenverkehr für Supervisor verarbeiten wird.
IP-Startadresse	Geben Sie eine IP-Adresse ein, die den Startpunkt für die Reservierung von fünf aufeinanderfolgenden IP-Adressen für die Kubernetes-Steuerungsebenen-VMs wie folgt festlegt: ■ Eine IP-Adresse für jede der Kubernetes-Steuerungsebenen-VMs. ■ Eine Floating-IP-Adresse für eine der Kubernetes-Steuerungsebenen-VMs als Schnittstelle zum Verwaltungsnetzwerk. Die Steuerungsebenen-VM mit der zugewiesenen Floating-IP-Adresse fungiert als führende VM für alle drei Kubernetes-Steuerungsebenen-VMs. Die Floating IP-Adresse wird zum Knoten der Steuerungsebene verschoben, der als etcd-Leader im Kubernetes-Cluster fungiert. Dadurch wird die Verfügbarkeit im Falle eines Netzwerkpartitionsereignisses verbessert. ■ Eine IP-Adresse, die als Puffer dienen soll, falls eine Kubernetes-Steuerungsebenen-VM ausfällt und eine neue Steuerungsebenen-VM als Ersatz bereitgestellt wird.
Subnetzmaske	Gilt nur für die Konfiguration statischer IP-Adressen. Geben Sie die Subnetzmaske für das Verwaltungsnetzwerk ein. Beispielsweise `255.255.255.0`

Option	Beschreibung
Gateway	Geben Sie ein Gateway für das Verwaltungsnetzwerk ein.
DNS-Server	Geben Sie die Adressen der DNS-Server ein, die Sie in Ihrer Umgebung verwenden. Wenn das vCenter Server-System mit einem FQDN registriert ist, müssen Sie die IP-Adressen der DNS-Server eingeben, die Sie mit der vSphere-Umgebung verwenden, damit der FQDN im Supervisor aufgelöst werden kann.
DNS-Suchdomänen	Geben Sie Domänennamen ein, die von DNS innerhalb der Kubernetes Control Plane-Knoten durchsucht werden, z. B. `corp.local`, damit der DNS-Server sie auflösen kann.
NTP-Server	Geben Sie die Adressen der NTP-Server ein, die Sie in Ihrer Umgebung verwenden (sofern vorhanden).

b Klicken Sie auf **Weiter**.

9 Geben Sie auf der Seite **Arbeitslastnetzwerk** die Einstellungen für das Netzwerk ein, das den Netzwerkdatenverkehr für im Supervisor ausgeführte Kubernetes-Arbeitslasten verarbeitet.

Hinweis Wenn Sie die Verwendung eines DHCP-Servers zur Bereitstellung der Netzwerkeinstellungen für Arbeitslastnetzwerke aktivieren, können Sie keine neuen Arbeitslastnetzwerke erstellen, nachdem Sie die Supervisor-Konfiguration abgeschlossen haben.

a Wählen Sie einen Netzwerkmodus aus.

- **DHCP-Netzwerk**. In diesem Netzwerkmodus werden alle Netzwerkeinstellungen für Arbeitslastnetzwerke über DHCP abgerufen. Sie können auch einige der von DHCP übernommenen Einstellungen überschreiben, indem Sie Werte in die Textfelder für diese Einstellungen eingeben:

Option	Beschreibung
Internes Netzwerk für Kubernetes-Dienste	Geben Sie eine CIDR-Notation ein, welche den IP-Adressenbereich für Tanzu Kubernetes-Cluster und -Dienste festlegt, die innerhalb der Cluster ausgeführt werden.
Portgruppe	Wählen Sie die Portgruppe aus, die als primäres Arbeitslastnetzwerk für den Supervisor dienen soll. Das primäre Netzwerk verarbeitet den Datenverkehr für die Kubernetes-Steuerungsebenen-VMs und den Kubernetes-Arbeitslast-Datenverkehr. Je nach Ihrer Netzwerktopologie können Sie zu einem späteren Zeitpunkt eine andere Portgruppe als Netzwerk für jeden Namespace zuweisen. Auf diese Weise können Sie Schicht-2-Isolierung zwischen den Namespaces im Supervisor bereitstellen. Namespaces, denen keine andere Portgruppe als ihr Netzwerk zugewiesen ist, verwenden das primäre Netzwerk. Tanzu Kubernetes-Cluster verwenden nur das Netzwerk, das dem Namespace zugewiesen ist, in dem sie bereitgestellt werden, oder sie verwenden das primäre Netzwerk, wenn diesem Namespace kein explizites Netzwerk zugewiesen ist.
Netzwerkname	Geben Sie den Netzwerknamen ein.
DNS-Server	Geben Sie, sofern vorhanden, die IP-Adressen der DNS-Server ein, die Sie in Ihrer Umgebung verwenden. Beispiel: `10.142.7.1`. Wenn Sie die IP-Adresse des DNS-Servers eingeben, wird jeder Steuerungsebenen-VM eine statische Route hinzugefügt. Dadurch wird angegeben, dass der Datenverkehr zu den DNS-Servern über das Arbeitslastnetzwerk fließt.

Option	Beschreibung
	Wenn die von Ihnen angegebenen DNS-Server vom Verwaltungsnetzwerk und vom Arbeitslastnetzwerk gemeinsam genutzt werden, werden die DNS-Lookups auf den Steuerungsebenen-VMs nach der ersten Einrichtung über das Arbeitslastnetzwerk geleitet.
NTP-Server	Geben Sie, sofern vorhanden, die Adresse des NTP-Servers ein, den Sie in Ihrer Umgebung verwenden.

- **Statisch**. Konfigurieren Sie die Arbeitslastnetzwerkeinstellungen manuell

Option	Beschreibung
Internes Netzwerk für Kubernetes-Dienste	Geben Sie eine CIDR-Notation ein, welche den IP-Adressenbereich für Tanzu Kubernetes-Cluster und -Dienste festlegt, die innerhalb der Cluster ausgeführt werden.
Portgruppe	Wählen Sie die Portgruppe aus, die als primäres Arbeitslastnetzwerk für den Supervisor dienen soll. Das primäre Netzwerk verarbeitet den Datenverkehr für die Kubernetes-Steuerungsebenen-VMs und den Kubernetes-Arbeitslast-Datenverkehr. Je nach Ihrer Netzwerktopologie können Sie zu einem späteren Zeitpunkt eine andere Portgruppe als Netzwerk für jeden Namespace zuweisen. Auf diese Weise können Sie Schicht-2-Isolierung zwischen den Namespaces im Supervisor bereitstellen. Namespaces, denen keine andere Portgruppe als ihr Netzwerk zugewiesen ist, verwenden das primäre Netzwerk. Tanzu Kubernetes-Cluster verwenden nur das Netzwerk, das dem Namespace zugewiesen ist, in dem sie bereitgestellt werden, oder sie verwenden das primäre Netzwerk, wenn diesem Namespace kein explizites Netzwerk zugewiesen ist.
Netzwerkname	Geben Sie den Netzwerknamen ein.
IP-Adressbereiche	Geben Sie einen IP-Bereich für die Zuteilung der IP-Adresse von Kubernetes-Steuerungsebenen-VMs und -Arbeitslasten ein. Dieser Adressbereich verbindet die Supervisor-Knoten und verbindet im Falle eines einzelnen Arbeitslastnetzwerks auch die Clusterknoten von Tanzu Kubernetes. Dieser IP-Bereich darf sich nicht mit dem VIP-Bereich des Lastausgleichsdiensts überschneiden, wenn die Konfiguration **Standard** für HAProxy verwendet wird.
Subnetzmaske	Geben Sie die IP-Adresse der Subnetzmaske ein.

Option	Beschreibung
Gateway	Geben Sie das Gateway für das primäre Netzwerk ein.
NTP-Server	Geben Sie, sofern vorhanden, die Adresse des NTP-Servers ein, den Sie in Ihrer Umgebung verwenden.
DNS-Server	Geben Sie, sofern vorhanden, die IP-Adressen der DNS-Server ein, die Sie in Ihrer Umgebung verwenden. Beispiel: `10.142.7.1`.

b Klicken Sie auf **Weiter**.

10 Scrollen Sie auf der Seite **Überprüfen und bestätigen** nach oben und überprüfen Sie alle bisher konfigurierten Einstellungen und legen Sie erweiterte Einstellungen für die Supervisor-Bereitstellung fest.

Option	Beschreibung
Größe der Supervisor-Steuerungsebene	Wählen Sie die Dimensionierung für die Steuerungsebenen-VMs aus. Die Größe der Steuerungsebenen-VMs bestimmt die Menge der Arbeitslasten, die Sie auf dem Supervisor ausführen können. Sie können wählen zwischen: ■ Sehr klein – 2 CPUs, 8 GB Arbeitsspeicher, 32 GB Speicher ■ Klein – 4 CPUs, 16 GB Arbeitsspeicher, 32 GB Speicher ■ Mittel – 8 CPUs, 16 GB Arbeitsspeicher, 32 GB Speicher ■ Groß – 16 CPUs, 32 GB Arbeitsspeicher, 32 GB Speicher **Hinweis** Sobald Sie eine Größe der Steuerungsebene ausgewählt haben, können Sie nur noch vertikal hochskalieren. Sie können nicht auf eine kleinere Größe herunterskalieren.
DNS-Namen des API-Servers	Geben Sie optional die FQDNs ein, die für den Zugriff auf die Supervisor-Steuerungsebene verwendet werden sollen, anstatt die IP-Adresse der Supervisor-Steuerungsebene zu verwenden. Die von Ihnen eingegebenen FQDNs werden in ein automatisch generiertes Zertifikat eingebettet. Wenn Sie FQDNs für Supervisor verwenden, können Sie die Angabe eines IP-Sands im Zertifikat des Lastausgleichsdiensts auslassen.
Konfiguration exportieren	Exportieren Sie eine JSON-Datei, die die Werte der eingegebenen Supervisor-Konfiguration enthält. Sie können die Datei später ändern und importieren, wenn Sie die Supervisor erneut bereitstellen möchten oder wenn Sie eine neue Supervisor mit ähnlicher Konfiguration bereitstellen möchten. Wenn Sie die Supervisor Konfiguration exportieren, sparen Sie im Falle einer erneuten Bereitstellung von Supervisor zeitsparend alle Konfigurationswerte in diesen Assistenten.

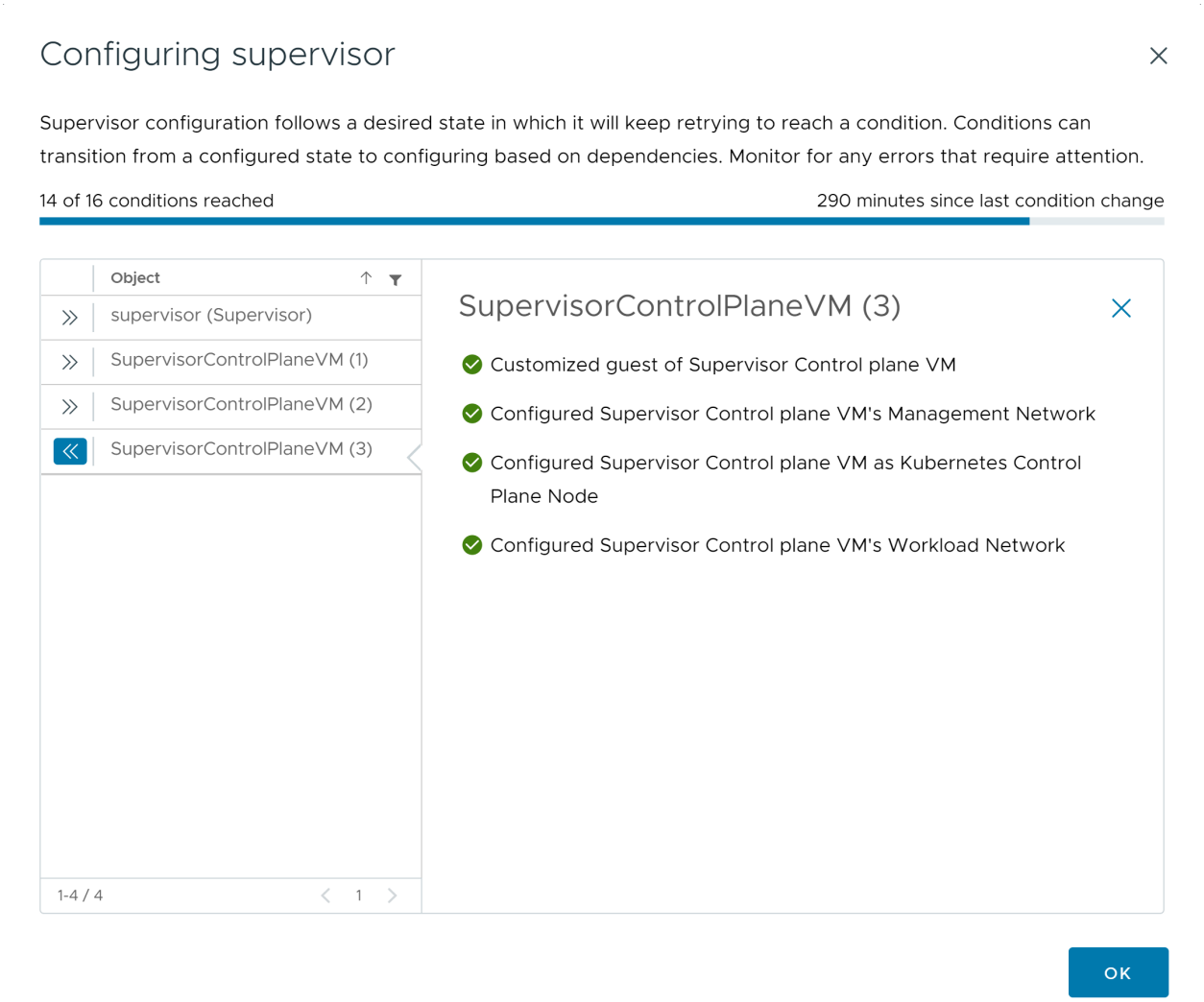
11 Klicken Sie auf **Beenden**, wenn Sie mit der Überprüfung der Einstellungen fertig sind.

Die Aktivierung von Supervisor initiiert die Erstellung und Konfiguration der Steuerungsebenen-VMs und anderer Komponenten.

Nächste Schritte

Sobald der Assistent zum Aktivieren eines Supervisors fertig ist, können Sie den Aktivierungsprozess verfolgen und nach potenzielle Problemen Ausschau halten, die eine Fehlerbehebung erfordern. Klicken Sie in der Spalte **Konfigurationsstatus** neben dem Status des Supervisors auf **Anzeigen**.

Abbildung 5-1. Supervisor-Aktivierungsansicht



Damit der Bereitstellungsvorgang abgeschlossen werden kann, muss der Supervisor den gewünschten Zustand erreichen. Demnach müssen alle 16 Bedingungen erfüllt sein. Wenn ein Supervisor erfolgreich aktiviert wurde, ändert sich sein Status von „Konfigurieren“ zu „Wird ausgeführt“. Während sich der Supervisor im Status „Konfigurieren“ befindet, wird kontinuierlich und wiederholt überprüft, ob die einzelnen Bedingungen erfüllt sind. Wenn eine Bedingung nicht erfüllt wird, wird der Vorgang wiederholt, bis er erfolgreich ist. Aus diesem Grund kann sich die

Anzahl der erreichten Bedingungen ändern. Beispiel: *10 von 16 Bedingungen wurden erfüllt*, dann *4 von 16 Bedingungen wurden erfüllt* usw. In sehr seltenen Fällen kann sich der Status in „Fehler“ ändern, wenn Fehler vorliegen, aufgrund derer der gewünschte Status nicht erreicht werden kann.

Weitere Informationen zu Bereitstellungsfehlern und zur Fehlerbehebung finden Sie unter Beheben von Fehlerzuständen auf den VMs einer Supervisor-Steuerungsebene während der Aktivierung oder Aktualisierung.

Falls Sie versuchen möchten, die Supervisor erneut bereitzustellen, indem Sie die Konfigurationswerte ändern, die Sie im Assistenten eingegeben haben, überprüfen Sie Kapitel 9 Bereitstellen eines Supervisor durch Importieren einer JSON-Konfigurationsdatei.

Bereitstellen eines Supervisors für drei Zonen mit dem NSX-Netzwerk

Erfahren Sie, wie Sie einen Supervisor mit NSX auf drei vSphere-Zonen bereitstellen. Jede vSphere-Zone wird einem vSphere-Cluster zugeordnet. Durch die Bereitstellung des Supervisor auf drei vSphere-Zonen stellen Sie Hochverfügbarkeit für Ihre Arbeitslasten auf Clusterebene bereit. Ein mit NSX konfigurierter Supervisor für drei Zonen unterstützt nur Tanzu Kubernetes-Cluster und -VMs, jedoch nicht vSphere-Pods.

Wenn Sie NSX Version 4.1.1 oder höher konfiguriert haben und NSX Advanced Load Balancer Version 22.1.4 oder höher mit Enterprise-Lizenz für NSXinstalliert, konfiguriert und registriert haben, ist der Lastausgleichsdienst, der mit NSX verwendet wird, NSX Advanced Load Balancer. Wenn Sie Versionen von NSX vor 4.1.1 konfiguriert haben, wird der NSX-Lastausgleichsdienst verwendet. Weitere Informationen finden Sie unter Kapitel 7 Überprüfen des mit dem NSX-Netzwerk verwendeten Lastausgleichsdiensts.

Voraussetzungen

- Erfüllen Sie die Voraussetzungen zum Konfigurieren von vSphere-Clustern als Supervisor. Weitere Informationen hierzu finden Sie unter Voraussetzungen für die Konfiguration von vSphere IaaS control plane in vSphere-Cluster.
- Erstellen Sie drei vSphere-Zonen. Weitere Informationen hierzu finden Sie unter Kapitel 3 Erstellen von vSphere-Zonen für eine Supervisor-Bereitstellung mit mehreren Zonen.

Verfahren

1. Wählen Sie im Startmenü die Option **Arbeitslastverwaltung** aus.
2. Wählen Sie eine Lizenzierungsoption für den Supervisor aus.
   - Wenn Sie über eine gültige Tanzu Edition-Lizenz verfügen, klicken Sie auf **Lizenz hinzufügen**, um den Lizenzschlüssel der Lizenzbestandsliste von vSphere hinzuzufügen.
   - Wenn Sie noch keine Tanzu Edition-Lizenz haben, geben Sie die Kontaktdetails ein, damit Sie Mitteilungen von VMware empfangen können, und klicken Sie auf **Erste Schritte**.

Der Testzeitraum eines Supervisors beträgt 60 Tage. Innerhalb dieses Zeitraums müssen Sie dem Cluster eine gültige Tanzu Edition-Lizenz zuweisen. Wenn Sie einen Tanzu Edition-Lizenzschlüssel hinzugefügt haben, können Sie diesen Schlüssel innerhalb des 60-Tage-Testzeitraums zuweisen, sobald Sie die Einrichtung des Supervisors abgeschlossen haben.

3 Klicken Sie auf dem Bildschirm **Arbeitslastverwaltung** erneut auf **Erste Schritte**.

4 Wählen Sie auf der Seite **vCenter-Server und -Netzwerk** das vCenter Server-System aus, das für die Supervisor-Bereitstellung eingerichtet ist, und wählen Sie **NSX** als Netzwerk-Stack aus.

5 Klicken Sie auf **Weiter**.

6 Wählen Sie auf der Seite **Supervisor-Standort** die Option **vSphere-Zonenbereitstellung** aus, um einen Supervisor auf drei vSphere-Zonen bereitzustellen.

   a Geben Sie einen Namen für den neuen Supervisor ein.

   b Wählen Sie das Datencenter aus, in dem Sie die vSphere-Zonen für die Bereitstellung von Supervisor erstellt haben.

   c Wählen Sie aus der Liste der kompatiblen vSphere-Zonen drei Zonen aus.

   d Klicken Sie auf **Weiter**.

7 Wählen Sie Speicherrichtlinien für den Supervisor aus.

Option	Bezeichnung
Speicherrichtlinie für Steuerungsebene	Wählen Sie die Speicherrichtlinie für die Platzierung der Control Plane-VMs aus.
Speicherrichtlinie für flüchtige Festplatten	Diese Option ist deaktiviert, da vSphere-Pods mit einem 3-Zonen-Supervisor nicht unterstützt wird.
Speicherrichtlinie für Image-Cache	Diese Option ist deaktiviert, da vSphere-Pods mit einem 3-Zonen-Supervisor nicht unterstützt wird.

8 Klicken Sie auf **Weiter**.

9 Konfigurieren Sie auf dem Bildschirm **Verwaltungsnetzwerk** die Parameter für das Netzwerk, das für die VMs der Kubernetes-Steuerungsebene verwendet wird.

a Wählen Sie einen **Netzwerkmodus** aus.

- **DHCP-Netzwerk**. In diesem Modus werden alle IP-Adressen für das Verwaltungsnetzwerk, wie IP-Adressen von Steuerungsebenen-VMs, eine Floating-IP-Adresse, DNS-Server, DNS, Suchdomänen und NTP-Server, automatisch von einem DHCP-Server erfasst. Zum Abrufen von Floating-IP-Adressen muss der DHCP-Server so konfiguriert werden, dass Clientbezeichner unterstützt werden. Im DHCP-Modus verwenden alle Steuerungsebenen-VMs stabile DHCP-Clientbezeichner zum Erfassen von IP-Adressen. Diese Clientbezeichner können verwendet werden, um eine Zuweisung statischer IP-Adressen für die IPs der Steuerungsebenen-VMs auf dem DHCP-Server einzurichten und dadurch sicherzustellen, dass sich diese nicht ändern. Ein Ändern der IP-Adressen von Steuerungsebenen-VMs und Floating-IP-Adressen wird nicht unterstützt.

  Sie können einige der von DHCP übernommenen Einstellungen überschreiben, indem Sie Werte in die Textfelder für diese Einstellungen eingeben.

Option	Beschreibung
Netzwerk	Wählen Sie das Netzwerk aus, das den Verwaltungsdatenverkehr für Supervisor verarbeiten wird.
Floating IP-Adresse	Geben Sie eine IP-Adresse ein, die den Startpunkt für die Reservierung von fünf aufeinanderfolgenden IP-Adressen für die Kubernetes-Steuerungsebenen-VMs wie folgt festlegt: ■ Eine IP-Adresse für jede der Kubernetes-Steuerungsebenen-VMs. ■ Eine Floating-IP-Adresse für eine der Kubernetes-Steuerungsebenen-VMs als Schnittstelle zum Verwaltungsnetzwerk. Die Steuerungsebenen-VM mit der zugewiesenen Floating-IP-Adresse fungiert als führende VM für alle drei Kubernetes-Steuerungsebenen-VMs. Die Floating IP-Adresse wird zum Knoten der Steuerungsebene verschoben, der als etcd-Leader im Kubernetes-Cluster fungiert. Dadurch wird die Verfügbarkeit im Falle eines Netzwerkpartitionsereignisses verbessert. ■ Eine IP-Adresse, die als Puffer dienen soll, falls eine Kubernetes-Steuerungsebenen-VM ausfällt und eine neue Steuerungsebenen-VM als Ersatz bereitgestellt wird.

Option	Beschreibung
DNS-Server	Geben Sie die Adressen der DNS-Server ein, die Sie in Ihrer Umgebung verwenden. Wenn das vCenter Server-System mit einem FQDN registriert ist, müssen Sie die IP-Adressen der DNS-Server eingeben, die Sie mit der vSphere-Umgebung verwenden, damit der FQDN im Supervisor aufgelöst werden kann.
DNS-Suchdomänen	Geben Sie Domänennamen ein, die von DNS innerhalb der Kubernetes Control Plane-Knoten durchsucht werden, z. B. `corp.local`, damit der DNS-Server sie auflösen kann.
NTP-Server	Geben Sie die Adressen der NTP-Server ein, die Sie in Ihrer Umgebung verwenden (sofern vorhanden).

- **Statisch**. Geben Sie alle Netzwerkeinstellungen für das Verwaltungsnetzwerk manuell ein.

Option	Beschreibung
Netzwerk	Wählen Sie das Netzwerk aus, das den Verwaltungsdatenverkehr für Supervisor verarbeiten wird.
IP-Startadresse	Geben Sie eine IP-Adresse ein, die den Startpunkt für die Reservierung von fünf aufeinanderfolgenden IP-Adressen für die Kubernetes-Steuerungsebenen-VMs wie folgt festlegt: ■ Eine IP-Adresse für jede der Kubernetes-Steuerungsebenen-VMs. ■ Eine Floating-IP-Adresse für eine der Kubernetes-Steuerungsebenen-VMs als Schnittstelle zum Verwaltungsnetzwerk. Die Steuerungsebenen-VM mit der zugewiesenen Floating-IP-Adresse fungiert als führende VM für alle drei Kubernetes-Steuerungsebenen-VMs. Die Floating IP-Adresse wird zum Knoten der Steuerungsebene verschoben, der als etcd-Leader im Kubernetes-Cluster fungiert. Dadurch wird die Verfügbarkeit im Falle eines Netzwerkpartitionsereignisses verbessert. ■ Eine IP-Adresse, die als Puffer dienen soll, falls eine Kubernetes-Steuerungsebenen-VM ausfällt und eine neue Steuerungsebenen-VM als Ersatz bereitgestellt wird.
Subnetzmaske	Gilt nur für die Konfiguration statischer IP-Adressen. Geben Sie die Subnetzmaske für das Verwaltungsnetzwerk ein. Beispielsweise `255.255.255.0`

Option	Beschreibung
Gateway	Geben Sie ein Gateway für das Verwaltungsnetzwerk ein.
DNS-Server	Geben Sie die Adressen der DNS-Server ein, die Sie in Ihrer Umgebung verwenden. Wenn das vCenter Server-System mit einem FQDN registriert ist, müssen Sie die IP-Adressen der DNS-Server eingeben, die Sie mit der vSphere-Umgebung verwenden, damit der FQDN im Supervisor aufgelöst werden kann.
DNS-Suchdomänen	Geben Sie Domänennamen ein, die von DNS innerhalb der Kubernetes Control Plane-Knoten durchsucht werden, z. B. `corp.local`, damit der DNS-Server sie auflösen kann.
NTP-Server	Geben Sie die Adressen der NTP-Server ein, die Sie in Ihrer Umgebung verwenden (sofern vorhanden).

b Klicken Sie auf **Weiter**.

10 Konfigurieren Sie im Bereich **Arbeitslastennetzwerk** die Einstellungen für die Netzwerke für Namespaces.

Option	Bezeichnung
vSphere Distributed Switch	Wählen Sie den vSphere Distributed Switch aus, der das Overlay-Netzwerk für den Supervisor verarbeitet. Wählen Sie z. B. `DSwitch` aus.
DNS-Server	Geben Sie, sofern vorhanden, die IP-Adressen der DNS-Server ein, die Sie in Ihrer Umgebung verwenden. Beispiel: `10.142.7.1`.
NAT-Modus	Der NAT-Modus ist standardmäßig aktiviert. Wenn Sie die Option deaktivieren, sind alle Arbeitslasten wie die IP-Adressen der vSphere-Pods, VMs und Tanzu Kubernetes-Clusterknoten von außerhalb des Tier-0-Gateways direkt zugänglich, und Sie müssen die Egress-CIDRs nicht konfigurieren. **Hinweis** Wenn Sie den NAT-Modus deaktivieren, wird die Dateivolume-Speicherung nicht unterstützt.
Namespace-Netzwerk	Geben Sie einen oder mehrere IP-CIDRs ein, um Subnetze/Segmente zu erstellen und IP-Adressen Arbeitslasten zuzuweisen.
Ingress-CIDRs	Geben Sie eine CIDR-Anmerkung zur Ermittlung des Ingress-IP-Bereichs für die Kubernetes-Dienste ein. Dieser Bereich wird für Dienste vom Typ „Load Balancer“ und „Ingress“ verwendet.
Edge-Cluster	Wählen Sie den NSX Edge-Cluster mit dem Tier-0-Gateway aus, das Sie für das Namespace-Netzwerk verwenden möchten. Wählen Sie z. B. `EDGE-CLUSTER` aus.

Option	Bezeichnung
Tier-0-Gateway	Wählen Sie das Tier-0-Gateway aus, das mit dem Cluster-Tier-1-Gateway verknüpft werden soll.
Subnetz-Präfix	Geben Sie das Subnetzpräfix ein, das die Größe des für Namespace-Segmente reservierten Subnetzes angibt. Der Standardwert ist „28“.
Dienst-CIDRs	Geben Sie eine CIDR-Anmerkung ein, um den IP-Bereich für Kubernetes-Dienste zu ermitteln. Sie können den Standardwert verwenden.
Egress-CIDRs	Geben Sie eine CIDR-Anmerkung zur Ermittlung der Egress-IP für Kubernetes-Dienste ein. Für jeden Namespace im Supervisor wird nur eine Egress-IP-Adresse zugewiesen. Bei der Egress-IP handelt es sich um die IP-Adresse, die die Kubernetes-Arbeitslasten im jeweiligen Namespace verwenden, um außerhalb von NSX zu kommunizieren.

11 Klicken Sie auf **Weiter**.

12 Scrollen Sie auf der Seite **Überprüfen und bestätigen** nach oben und überprüfen Sie alle bisher konfigurierten Einstellungen und legen Sie erweiterte Einstellungen für die Supervisor-Bereitstellung fest.

Option	Beschreibung
Größe der Supervisor-Steuerungsebene	Wählen Sie die Dimensionierung für die Steuerungsebenen-VMs aus. Die Größe der Steuerungsebenen-VMs bestimmt die Menge der Arbeitslasten, die Sie auf dem Supervisor ausführen können. Sie können wählen zwischen: ■ Sehr klein – 2 CPUs, 8 GB Arbeitsspeicher, 32 GB Speicher ■ Klein – 4 CPUs, 16 GB Arbeitsspeicher, 32 GB Speicher ■ Mittel – 8 CPUs, 16 GB Arbeitsspeicher, 32 GB Speicher ■ Groß – 16 CPUs, 32 GB Arbeitsspeicher, 32 GB Speicher **Hinweis** Sobald Sie eine Größe der Steuerungsebene ausgewählt haben, können Sie nur noch vertikal hochskalieren. Sie können nicht auf eine kleinere Größe herunterskalieren.
DNS-Namen des API-Servers	Geben Sie optional die FQDNs ein, die für den Zugriff auf die Supervisor-Steuerungsebene verwendet werden sollen, anstatt die IP-Adresse der Supervisor-Steuerungsebene zu verwenden. Die von Ihnen eingegebenen FQDNs werden in ein automatisch generiertes Zertifikat eingebettet. Wenn Sie FQDNs für Supervisor verwenden, können Sie die Angabe eines IP-Sands im Zertifikat des Lastausgleichsdiensts auslassen.
Konfiguration exportieren	Exportieren Sie eine JSON-Datei, die die Werte der eingegebenen Supervisor-Konfiguration enthält. Sie können die Datei später ändern und importieren, wenn Sie die Supervisor erneut bereitstellen möchten oder wenn Sie eine neue Supervisor mit ähnlicher Konfiguration bereitstellen möchten. Wenn Sie die Supervisor Konfiguration exportieren, sparen Sie im Falle einer erneuten Bereitstellung von Supervisor zeitsparend alle Konfigurationswerte in diesen Assistenten.

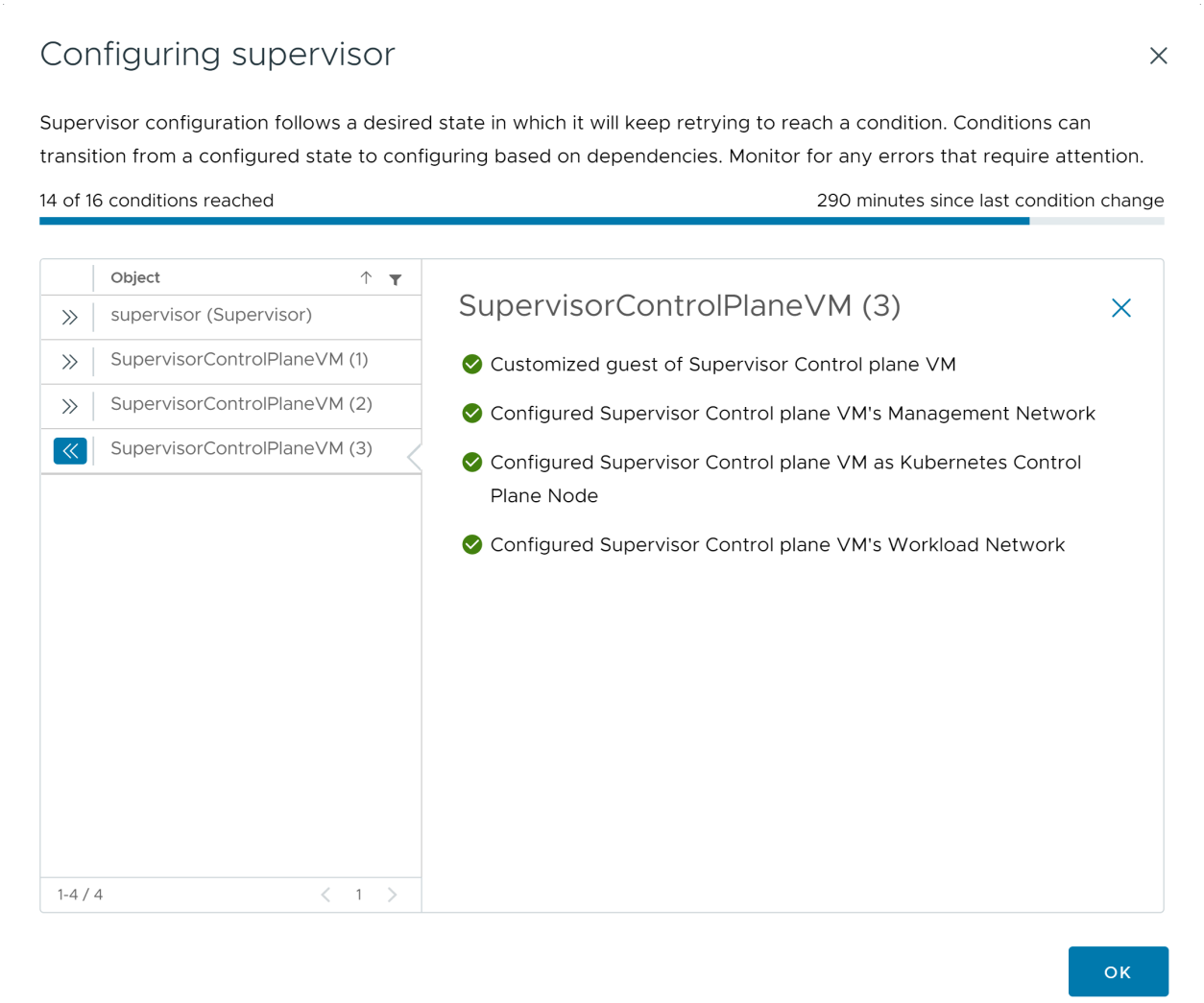
13 Klicken Sie auf **Beenden**, wenn Sie mit der Überprüfung der Einstellungen fertig sind.

Die Aktivierung von Supervisor initiiert die Erstellung und Konfiguration der Steuerungsebenen-VMs und anderer Komponenten.

Nächste Schritte

Sobald der Assistent zum Aktivieren eines Supervisors fertig ist, können Sie den Aktivierungsprozess verfolgen und nach potenzielle Problemen Ausschau halten, die eine Fehlerbehebung erfordern. Klicken Sie in der Spalte **Konfigurationsstatus** neben dem Status des Supervisors auf **Anzeigen**.

Abbildung 5-2. Supervisor-Aktivierungsansicht



Damit der Bereitstellungsvorgang abgeschlossen werden kann, muss der Supervisor den gewünschten Zustand erreichen. Demnach müssen alle 16 Bedingungen erfüllt sein. Wenn ein Supervisor erfolgreich aktiviert wurde, ändert sich sein Status von „Konfigurieren“ zu „Wird ausgeführt“. Während sich der Supervisor im Status „Konfigurieren“ befindet, wird kontinuierlich und wiederholt überprüft, ob die einzelnen Bedingungen erfüllt sind. Wenn eine Bedingung nicht

erfüllt wird, wird der Vorgang wiederholt, bis er erfolgreich ist. Aus diesem Grund kann sich die Anzahl der erreichten Bedingungen ändern. Beispiel: *10 von 16 Bedingungen wurden erfüllt*, dann *4 von 16 Bedingungen wurden erfüllt* usw. In sehr seltenen Fällen kann sich der Status in „Fehler“ ändern, wenn Fehler vorliegen, aufgrund derer der gewünschte Status nicht erreicht werden kann.

Weitere Informationen zu Bereitstellungsfehlern und zur Fehlerbehebung finden Sie unter Beheben von Fehlerzuständen auf den VMs einer Supervisor-Steuerungsebene während der Aktivierung oder Aktualisierung.

Falls Sie versuchen möchten, die Supervisor erneut bereitzustellen, indem Sie die Konfigurationswerte ändern, die Sie im Assistenten eingegeben haben, überprüfen Sie Kapitel 9 Bereitstellen eines Supervisor durch Importieren einer JSON-Konfigurationsdatei.

Bereitstellen einer Supervisor für eine Zone

6

Stellen Sie einen Supervisor auf einem vSphere Cluster bereit, der dann automatisch einer vSphere-Zone zugeordnet wird. Ein Supervisor für eine Zone verfügt über Hochverfügbarkeit auf Hostebene mit vSphere HA.

Lesen Sie als Nächstes die folgenden Themen:

- Bereitstellen eines Supervisor für eine Zone mit dem VDS-Netzwerk-Stack
- Bereitstellen einers Supervisors für eine Zone mit NSX-Netzwerk

Bereitstellen eines Supervisor für eine Zone mit dem VDS-Netzwerk-Stack

Erfahren Sie, wie Sie eine Supervisor für eine Zone mit dem VDS-Netzwerk-Stack und mit dem HAProxy-Lastausgleichsdienst oder NSX Advanced Load Balancer bereitstellen. Ein mit VDS-Netzwerk konfigurierter Supervisor für eine Zone unterstützt die Bereitstellung von Tanzu Kubernetes-Clustern, die unter Verwendung von Tanzu Kubernetes Grid erstellt wurden. Abgesehen von den von Supervisor-Dienste bereitgestellten wird die Ausführung von vSphere-Pods nicht unterstützt.

Hinweis Nachdem Sie einen Supervisor auf einem einzelnen vSphere Cluster bereitgestellt haben, was zum Erstellen einer vSphere-Zone führt, können Sie den Supervisor nicht auf eine Bereitstellung mit drei Zonen erweitern. Sie können einen Supervisor entweder in einer vSphere-Zone (Bereitstellung mit einem einzelnen Cluster) oder in drei vSphere-Zonen bereitstellen.

Voraussetzungen

- Erfüllen Sie die Voraussetzungen zum Konfigurieren von vSphere-Clustern als Supervisor. Weitere Informationen hierzu finden Sie unter Voraussetzungen für die Konfiguration von vSphere IaaS control plane in vSphere-Cluster.

Verfahren

1. Wählen Sie im Startmenü die Option **Arbeitslastverwaltung** aus.
2. Wählen Sie eine Lizenzierungsoption für den Supervisor aus.
   - Wenn Sie über eine gültige Tanzu Edition-Lizenz verfügen, klicken Sie auf **Lizenz hinzufügen**, um den Lizenzschlüssel der Lizenzbestandsliste von vSphere hinzuzufügen.

- Wenn Sie noch keine Tanzu Edition-Lizenz haben, geben Sie die Kontaktdetails ein, damit Sie Mitteilungen von VMware empfangen können, und klicken Sie auf **Erste Schritte**.

Der Testzeitraum eines Supervisors beträgt 60 Tage. Innerhalb dieses Zeitraums müssen Sie dem Cluster eine gültige Tanzu Edition-Lizenz zuweisen. Wenn Sie einen Tanzu Edition-Lizenzschlüssel hinzugefügt haben, können Sie diesen Schlüssel innerhalb des 60-Tage-Testzeitraums zuweisen, sobald Sie die Einrichtung des Supervisors abgeschlossen haben.

3 Klicken Sie auf dem Bildschirm **Arbeitslastverwaltung** erneut auf **Erste Schritte**.

4 Wählen Sie die Seite **vCenter Server und Netzwerk** aus, wählen Sie das vCenter Server-System aus, das für die Supervisor-Bereitstellung eingerichtet ist, wählen Sie **vSphere Distributed Switch (VDS)** als Netzwerk-Stack aus und klicken Sie auf **Weiter**.

5 Um eine Supervisor-Zone zu aktivieren, wählen Sie auf der Seite für den Supervisor-Speicherort die Option **CLUSTERBEREITSTELLUNG** aus.

Durch das Aktivieren der Arbeitslastverwaltung auf einem Supervisor-Cluster für eine Zone wird automatisch eine vSphere-Zone erstellt und der Cluster der Zone zugewiesen.

6 Wählen Sie einen Cluster aus der Liste der kompatiblen Cluster aus.

7 Geben Sie einen Namen für die Supervisor ein.

8 (Optional) Geben Sie einen Namen für die vSphere-Zone ein und klicken Sie auf **WEITER**.

Wenn Sie keinen Namen für die vSphere-Zone eingeben, wird automatisch ein Name zugewiesen und Sie können den Namen später nicht mehr ändern.

9 Konfigurieren Sie auf der Seite **Speicher** den Speicher für die Platzierung von Steuerungsebenen-VMs.

Option	Bezeichnung
Steuerungsebenenknoten	Wählen Sie die Speicherrichtlinie für die Platzierung der Control Plane-VMs aus.

10 Konfigurieren Sie auf dem Bildschirm **Lastausgleichsdienst** die Einstellungen eines Lastenausgleichs.

a Geben Sie einen Namen für den Lastausgleichsdienst ein.

b Wählen Sie den Typ des Lastausgleichsdiensts aus.

Sie können zwischen **NSX Advanced Load Balancer** und **HAProxy** auswählen.

c Konfigurieren Sie die Einstellungen für den Lastausgleichsdienst

- Geben Sie die folgenden Einstellungen für den NSX Advanced Load Balancer ein:

Option	Beschreibung
Name	Geben Sie einen Namen für die NSX Advanced Load Balancer-VM ein.
Controller-Endpoint von NSX Advanced Load Balancer	Die IP-Adresse des NSX Advanced Load Balancer-Controllers. Der Standardport ist `443`.
Benutzername	Der Benutzername, der für den NSX Advanced Load Balancer konfiguriert ist. Sie verwenden diesen Benutzernamen für den Zugriff auf den Controller.
Kennwort	Das Kennwort für den Benutzernamen.
Serverzertifikat	Das vom Controller verwendete Zertifikat. Sie können das Zertifikat bereitstellen, das Sie während der Konfiguration zugewiesen haben. Weitere Informationen finden Sie unter Zuweisen eines Zertifikats zum Controller.
Cloud-Name	Geben Sie den Namen der von Ihnen eingerichteten benutzerdefinierten Cloud ein. Beachten Sie, dass beim Cloud-Namen die Groß-/Kleinschreibung beachtet wird. Um **Standard-Cloud** zu verwenden, lassen Sie dieses Feld leer. Weitere Informationen finden Sie unter Konfigurieren des Controllers.

- Geben Sie die folgenden Einstellungen für HAProxy ein:

Option	Beschreibung
Controller-Endpoint des HAProxy-Lastausgleichsdiensts	Die IP-Adresse und der Port der HAProxy-Datenebenen-API, wobei es sich um die Verwaltungs-IP-Adresse der HAProxy-Appliance handelt. Diese Komponente steuert den HAProxy-Server und wird in der HAProxy-VM ausgeführt.
Benutzername	Der Benutzername, der in der HAProxy-OVA-Datei konfiguriert ist. Sie verwenden diesen Namen für die Authentifizierung bei der HAProxy-Datenebenen-API.
Kennwort	Das Kennwort für den Benutzernamen.

Option	Beschreibung
Bereiche für virtuelle IPs	Bereich von IP-Adressen, die im Arbeitslastnetzwerk von Tanzu Kubernetes-Clustern verwendet werden. Dieser IP-Bereich stammt aus der Liste der IPs, die in dem CIDR definiert wurden, den Sie während der Bereitstellung der HAProxy-Appliance konfiguriert haben. Sie können den gesamten in der HAProxy-Bereitstellung konfigurierten Bereich festlegen, Sie können aber auch einen Teilbereich dieses CIDR festlegen, wenn Sie mehrere Supervisoren erstellen und IPs aus diesem CIDR-Bereich verwenden möchten. Dieser Bereich darf sich nicht mit dem für das Arbeitslastnetzwerk in diesem Assistenten definierten IP-Bereich überschneiden. Der Bereich darf sich außerdem nicht mit DHCP-Bereichen in diesem Arbeitslastnetzwerk überschneiden.
TLS-Zertifikat der HAProxy-Verwaltung	Das Zertifikat im PEM-Format, das signiert ist oder das ein vertrauenswürdiger Root des Serverzertifikats ist, das von der Datenebenen-API präsentiert wird. ■ Option 1: Wenn der Root-Zugriff aktiviert ist, melden Sie sich über SSH bei der HAProxy-VM als Root an und kopieren Sie `/etc/haproxy/ca.crt` in die **Zertifizierungsstelle für den Server**. Verwenden Sie keine Escapezeilen im `\n`-Format. ■ Option 2: Klicken Sie mit der rechten Maustaste auf die HAProxy-VM und wählen Sie **Einstellungen bearbeiten** aus. Kopieren Sie das CA-Zertifikat aus dem entsprechenden Feld und konvertieren Sie es aus Base64 mithilfe eines Konvertierungstools, wie z. B. https://www.base64decode.org/. ■ Option 3: Führen Sie das folgende PowerCLI-Skript aus. Ersetzen Sie die Variablen `$vc`, `$vc_user` und `$vc_password` durch entsprechende Werte. `$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`

Option	Beschreibung
	`` 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 ```

11 Konfigurieren Sie auf dem Bildschirm **Verwaltungsnetzwerk** die Parameter für das Netzwerk, das für die VMs der Kubernetes-Steuerungsebene verwendet wird.

a Wählen Sie einen **Netzwerkmodus** aus.

- **DHCP-Netzwerk**. In diesem Modus werden alle IP-Adressen für das Verwaltungsnetzwerk, wie IP-Adressen von Steuerungsebenen-VMs, eine Floating-IP-Adresse, DNS-Server, DNS, Suchdomänen und NTP-Server, automatisch von einem DHCP-Server erfasst. Zum Abrufen von Floating-IP-Adressen muss der DHCP-Server so konfiguriert werden, dass Clientbezeichner unterstützt werden. Im DHCP-Modus verwenden alle Steuerungsebenen-VMs stabile DHCP-Clientbezeichner zum Erfassen von IP-Adressen. Diese Clientbezeichner können verwendet werden, um eine Zuweisung statischer IP-Adressen für die IPs der Steuerungsebenen-VMs auf dem DHCP-Server einzurichten und dadurch sicherzustellen, dass sich diese nicht ändern. Ein Ändern der IP-Adressen der Steuerungsebenen-VMs sowie von Floating-IP-Adressen wird nicht unterstützt.

  Sie können einige der von DHCP übernommenen Einstellungen überschreiben, indem Sie Werte in die Textfelder für diese Einstellungen eingeben.

Option	Beschreibung
Netzwerk	Wählen Sie das Netzwerk aus, das den Verwaltungsdatenverkehr für Supervisor verarbeiten wird.
Floating IP-Adresse	Geben Sie eine IP-Adresse ein, die den Startpunkt für die Reservierung von fünf aufeinanderfolgenden IP-Adressen für die Kubernetes-Steuerungsebenen-VMs wie folgt festlegt: ■ Eine IP-Adresse für jede der Kubernetes-Steuerungsebenen-VMs. ■ Eine Floating-IP-Adresse für eine der Kubernetes-Steuerungsebenen-VMs als Schnittstelle zum Verwaltungsnetzwerk. Die Steuerungsebenen-VM mit der zugewiesenen Floating-IP-Adresse fungiert als führende VM für alle drei Kubernetes-Steuerungsebenen-VMs. Die Floating IP-Adresse wird zum Knoten der Steuerungsebene verschoben, der als etcd-Leader im Kubernetes-Cluster fungiert. Dadurch wird die Verfügbarkeit im Falle eines Netzwerkpartitionsereignisses verbessert. ■ Eine IP-Adresse, die als Puffer dienen soll, falls eine Kubernetes-Steuerungsebenen-VM ausfällt und eine neue Steuerungsebenen-VM als Ersatz bereitgestellt wird.

Option	Beschreibung
DNS-Server	Geben Sie die Adressen der DNS-Server ein, die Sie in Ihrer Umgebung verwenden. Wenn das vCenter Server-System mit einem FQDN registriert ist, müssen Sie die IP-Adressen der DNS-Server eingeben, die Sie mit der vSphere-Umgebung verwenden, damit der FQDN im Supervisor aufgelöst werden kann.
DNS-Suchdomänen	Geben Sie Domänennamen ein, die von DNS innerhalb der Kubernetes Control Plane-Knoten durchsucht werden, z. B. `corp.local`, damit der DNS-Server sie auflösen kann.
NTP-Server	Geben Sie die Adressen der NTP-Server ein, die Sie in Ihrer Umgebung verwenden (sofern vorhanden).

- **Statisch**. Geben Sie alle Netzwerkeinstellungen für das Verwaltungsnetzwerk manuell ein.

Option	Beschreibung
Netzwerk	Wählen Sie das Netzwerk aus, das den Verwaltungsdatenverkehr für Supervisor verarbeiten wird.
IP-Startadresse	Geben Sie eine IP-Adresse ein, die den Startpunkt für die Reservierung von fünf aufeinanderfolgenden IP-Adressen für die Kubernetes-Steuerungsebenen-VMs wie folgt festlegt: ■ Eine IP-Adresse für jede der Kubernetes-Steuerungsebenen-VMs. ■ Eine Floating-IP-Adresse für eine der Kubernetes-Steuerungsebenen-VMs als Schnittstelle zum Verwaltungsnetzwerk. Die Steuerungsebenen-VM mit der zugewiesenen Floating-IP-Adresse fungiert als führende VM für alle drei Kubernetes-Steuerungsebenen-VMs. Die Floating IP-Adresse wird zum Knoten der Steuerungsebene verschoben, der als etcd-Leader im Kubernetes-Cluster fungiert. Dadurch wird die Verfügbarkeit im Falle eines Netzwerkpartitionsereignisses verbessert. ■ Eine IP-Adresse, die als Puffer dienen soll, falls eine Kubernetes-Steuerungsebenen-VM ausfällt und eine neue Steuerungsebenen-VM als Ersatz bereitgestellt wird.
Subnetzmaske	Gilt nur für die Konfiguration statischer IP-Adressen. Geben Sie die Subnetzmaske für das Verwaltungsnetzwerk ein. Beispielsweise `255.255.255.0`

Option	Beschreibung
Gateway	Geben Sie ein Gateway für das Verwaltungsnetzwerk ein.
DNS-Server	Geben Sie die Adressen der DNS-Server ein, die Sie in Ihrer Umgebung verwenden. Wenn das vCenter Server-System mit einem FQDN registriert ist, müssen Sie die IP-Adressen der DNS-Server eingeben, die Sie mit der vSphere-Umgebung verwenden, damit der FQDN im Supervisor aufgelöst werden kann.
DNS-Suchdomänen	Geben Sie Domänennamen ein, die von DNS innerhalb der Kubernetes Control Plane-Knoten durchsucht werden, z. B. `corp.local`, damit der DNS-Server sie auflösen kann.
NTP-Server	Geben Sie die Adressen der NTP-Server ein, die Sie in Ihrer Umgebung verwenden (sofern vorhanden).

b Klicken Sie auf **Weiter**.

12 Geben Sie auf der Seite **Arbeitslastnetzwerk** die Einstellungen für das Netzwerk ein, das den Netzwerkdatenverkehr für im Supervisor ausgeführte Kubernetes-Arbeitslasten verarbeitet.

Hinweis Wenn Sie die Verwendung eines DHCP-Servers zur Bereitstellung der Netzwerkeinstellungen für Arbeitslastnetzwerke aktivieren, können Sie keine neuen Arbeitslastnetzwerke erstellen, nachdem Sie die Supervisor-Konfiguration abgeschlossen haben.

a Wählen Sie einen Netzwerkmodus aus.

- **DHCP-Netzwerk**. In diesem Netzwerkmodus werden alle Netzwerkeinstellungen für Arbeitslastnetzwerke über DHCP abgerufen. Sie können auch einige der von DHCP übernommenen Einstellungen überschreiben, indem Sie Werte in die Textfelder für diese Einstellungen eingeben:

  Hinweis Die DHCP-Konfiguration für Arbeitslastnetzwerke wird mit Supervisor-Dienste auf einem mit dem VDS-Stack konfigurierten Supervisor nicht unterstützt. Um Supervisor-Dienste zu verwenden, konfigurieren Sie Arbeitslastnetzwerke mit statischen IP-Adressen. Sie können DHCP weiterhin für das Verwaltungsnetzwerk verwenden.

Option	Beschreibung
Internes Netzwerk für Kubernetes-Dienste	Geben Sie eine CIDR-Notation ein, welche den IP-Adressenbereich für Tanzu Kubernetes-Cluster und -Dienste festlegt, die innerhalb der Cluster ausgeführt werden.
Portgruppe	Wählen Sie die Portgruppe aus, die als primäres Arbeitslastnetzwerk für den Supervisor dienen soll. Das primäre Netzwerk verarbeitet den Datenverkehr für die Kubernetes-Steuerungsebenen-VMs und den Kubernetes-Arbeitslast-Datenverkehr. Je nach Ihrer Netzwerktopologie können Sie zu einem späteren Zeitpunkt eine andere Portgruppe als Netzwerk für jeden Namespace zuweisen. Auf diese Weise können Sie Schicht-2-Isolierung zwischen den Namespaces im Supervisor bereitstellen. Namespaces, denen keine andere Portgruppe als ihr Netzwerk zugewiesen ist, verwenden das primäre Netzwerk. Tanzu Kubernetes-Cluster verwenden nur das Netzwerk, das dem Namespace zugewiesen ist, in dem sie bereitgestellt werden, oder sie verwenden das primäre Netzwerk, wenn diesem Namespace kein explizites Netzwerk zugewiesen ist.
Netzwerkname	Geben Sie den Netzwerknamen ein.

Option	Beschreibung
DNS-Server	Geben Sie, sofern vorhanden, die IP-Adressen der DNS-Server ein, die Sie in Ihrer Umgebung verwenden. Beispiel: `10.142.7.1`. Wenn Sie die IP-Adresse des DNS-Servers eingeben, wird jeder Steuerungsebenen-VM eine statische Route hinzugefügt. Dadurch wird angegeben, dass der Datenverkehr zu den DNS-Servern über das Arbeitslastnetzwerk fließt. Wenn die von Ihnen angegebenen DNS-Server vom Verwaltungsnetzwerk und vom Arbeitslastnetzwerk gemeinsam genutzt werden, werden die DNS-Lookups auf den Steuerungsebenen-VMs nach der ersten Einrichtung über das Arbeitslastnetzwerk geleitet.
NTP-Server	Geben Sie, sofern vorhanden, die Adresse des NTP-Servers ein, den Sie in Ihrer Umgebung verwenden.

- **Statisch**. Konfigurieren Sie die Arbeitslastnetzwerkeinstellungen manuell

Option	Beschreibung
Internes Netzwerk für Kubernetes-Dienste	Geben Sie eine CIDR-Notation ein, welche den IP-Adressenbereich für Tanzu Kubernetes-Cluster und -Dienste festlegt, die innerhalb der Cluster ausgeführt werden.
Portgruppe	Wählen Sie die Portgruppe aus, die als primäres Arbeitslastnetzwerk für den Supervisor dienen soll. Das primäre Netzwerk verarbeitet den Datenverkehr für die Kubernetes-Steuerungsebenen-VMs und den Kubernetes-Arbeitslast-Datenverkehr. Je nach Ihrer Netzwerktopologie können Sie zu einem späteren Zeitpunkt eine andere Portgruppe als Netzwerk für jeden Namespace zuweisen. Auf diese Weise können Sie Schicht-2-Isolierung zwischen den Namespaces im Supervisor bereitstellen. Namespaces, denen keine andere Portgruppe als ihr Netzwerk zugewiesen ist, verwenden das primäre Netzwerk. Tanzu Kubernetes-Cluster verwenden nur das Netzwerk, das dem Namespace zugewiesen ist, in dem sie bereitgestellt werden, oder sie verwenden das primäre Netzwerk, wenn diesem Namespace kein explizites Netzwerk zugewiesen ist.
Netzwerkname	Geben Sie den Netzwerknamen ein.

Option	Beschreibung
IP-Adressbereiche	Geben Sie einen IP-Bereich für die Zuteilung der IP-Adresse von Kubernetes-Steuerungsebenen-VMs und -Arbeitslasten ein. Dieser Adressbereich verbindet die Supervisor-Knoten und verbindet im Falle eines einzelnen Arbeitslastnetzwerks auch die Clusterknoten von Tanzu Kubernetes. Dieser IP-Bereich darf sich nicht mit dem VIP-Bereich des Lastausgleichsdiensts überschneiden, wenn die Konfiguration **Standard** für HAProxy verwendet wird.
Subnetzmaske	Geben Sie die IP-Adresse der Subnetzmaske ein.
Gateway	Geben Sie das Gateway für das primäre Netzwerk ein.
NTP-Server	Geben Sie, sofern vorhanden, die Adresse des NTP-Servers ein, den Sie in Ihrer Umgebung verwenden.
DNS-Server	Geben Sie, sofern vorhanden, die IP-Adressen der DNS-Server ein, die Sie in Ihrer Umgebung verwenden. Beispiel: `10.142.7.1`.

b Klicken Sie auf **Weiter**.

13 Scrollen Sie auf der Seite **Überprüfen und bestätigen** nach oben und überprüfen Sie alle bisher konfigurierten Einstellungen und legen Sie erweiterte Einstellungen für die Supervisor-Bereitstellung fest.

Option	Beschreibung
Größe der Supervisor-Steuerungsebene	Wählen Sie die Dimensionierung für die Steuerungsebenen-VMs aus. Die Größe der Steuerungsebenen-VMs bestimmt die Menge der Arbeitslasten, die Sie auf dem Supervisor ausführen können. Sie können wählen zwischen: ■ Sehr klein – 2 CPUs, 8 GB Arbeitsspeicher, 32 GB Speicher ■ Klein – 4 CPUs, 16 GB Arbeitsspeicher, 32 GB Speicher ■ Mittel – 8 CPUs, 16 GB Arbeitsspeicher, 32 GB Speicher ■ Groß – 16 CPUs, 32 GB Arbeitsspeicher, 32 GB Speicher **Hinweis** Sobald Sie eine Größe der Steuerungsebene ausgewählt haben, können Sie nur noch vertikal hochskalieren. Sie können nicht auf eine kleinere Größe herunterskalieren.
DNS-Namen des API-Servers	Geben Sie optional die FQDNs ein, die für den Zugriff auf die Supervisor-Steuerungsebene verwendet werden sollen, anstatt die IP-Adresse der Supervisor-Steuerungsebene zu verwenden. Die von Ihnen eingegebenen FQDNs werden in ein automatisch generiertes Zertifikat eingebettet. Wenn Sie FQDNs für Supervisor verwenden, können Sie die Angabe eines IP-Sands im Zertifikat des Lastausgleichsdiensts auslassen.
Konfiguration exportieren	Exportieren Sie eine JSON-Datei, die die Werte der eingegebenen Supervisor-Konfiguration enthält. Sie können die Datei später ändern und importieren, wenn Sie die Supervisor erneut bereitstellen möchten oder wenn Sie eine neue Supervisor mit ähnlicher Konfiguration bereitstellen möchten. Wenn Sie die Supervisor Konfiguration exportieren, sparen Sie im Falle einer erneuten Bereitstellung von Supervisor zeitsparend alle Konfigurationswerte in diesen Assistenten.

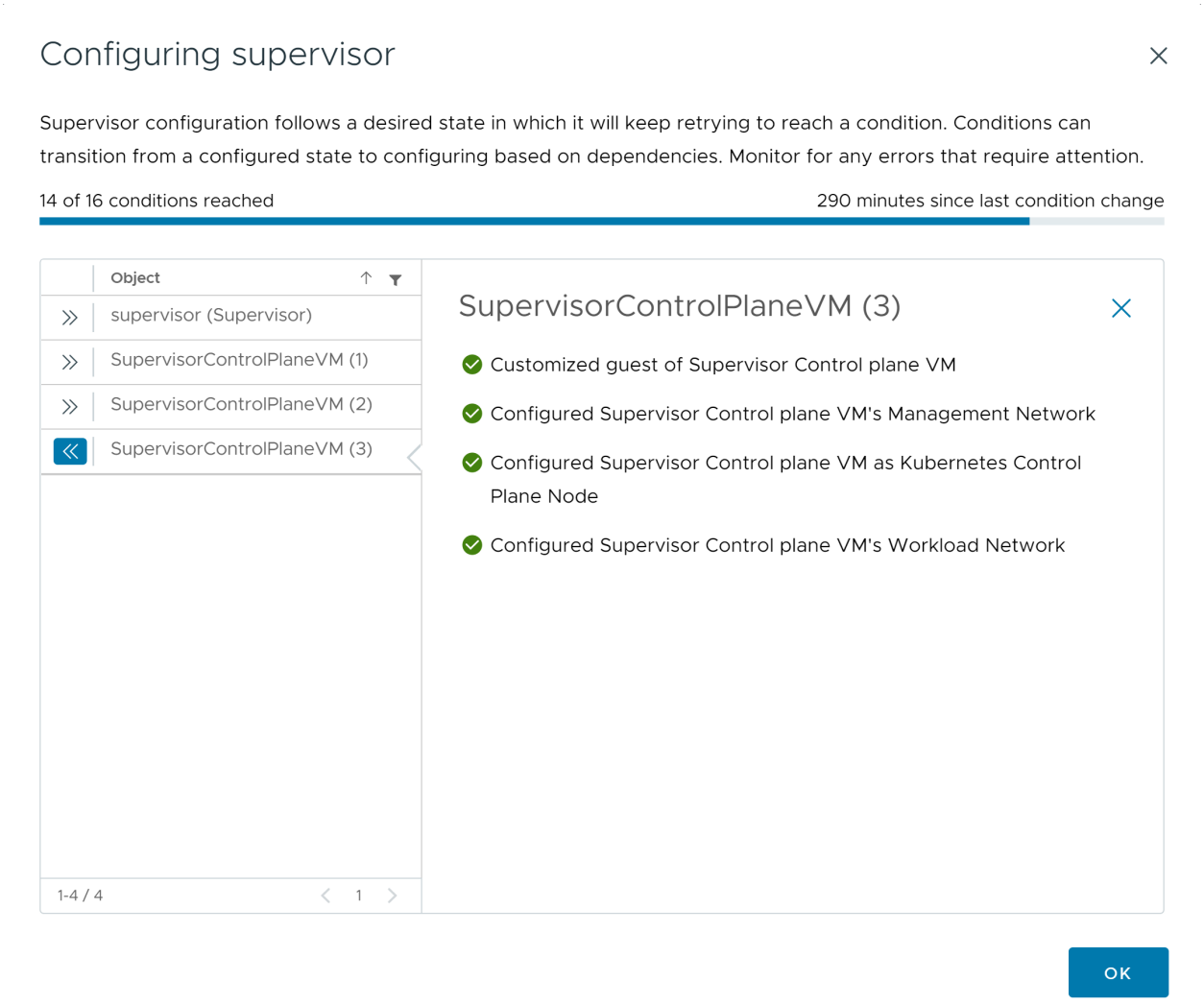
14 Klicken Sie auf **Beenden**, wenn Sie mit der Überprüfung der Einstellungen fertig sind.

Die Bereitstellung von Supervisor initiiert die Erstellung und Konfiguration der Steuerungsebenen-VMs und anderer Komponenten.

Nächste Schritte

Sobald der Assistent zum Aktivieren eines Supervisors fertig ist, können Sie den Aktivierungsprozess verfolgen und nach potenzielle Problemen Ausschau halten, die eine Fehlerbehebung erfordern. Klicken Sie in der Spalte **Konfigurationsstatus** neben dem Status des Supervisors auf **Anzeigen**.

Abbildung 6-1. Supervisor-Aktivierungsansicht



Damit der Bereitstellungsvorgang abgeschlossen werden kann, muss der Supervisor den gewünschten Zustand erreichen. Demnach müssen alle 16 Bedingungen erfüllt sein. Wenn ein Supervisor erfolgreich aktiviert wurde, ändert sich sein Status von „Konfigurieren“ zu „Wird ausgeführt“. Während sich der Supervisor im Status „Konfigurieren“ befindet, wird kontinuierlich und wiederholt überprüft, ob die einzelnen Bedingungen erfüllt sind. Wenn eine Bedingung nicht erfüllt wird, wird der Vorgang wiederholt, bis er erfolgreich ist. Aus diesem Grund kann sich die Anzahl der erreichten Bedingungen ändern. Beispiel: *10 von 16 Bedingungen wurden erfüllt*, dann *4 von 16 Bedingungen wurden erfüllt* usw. In sehr seltenen Fällen kann sich der Status in „Fehler“ ändern, wenn Fehler vorliegen, aufgrund derer der gewünschte Status nicht erreicht werden kann.

Weitere Informationen zu Bereitstellungsfehlern und zur Fehlerbehebung finden Sie unter Beheben von Fehlerzuständen auf den VMs einer Supervisor-Steuerungsebene während der Aktivierung oder Aktualisierung.

Falls Sie versuchen möchten, die Supervisor erneut bereitzustellen, indem Sie die Konfigurationswerte ändern, die Sie im Assistenten eingegeben haben, überprüfen Sie Kapitel 9 Bereitstellen eines Supervisor durch Importieren einer JSON-Konfigurationsdatei.

Bereitstellen einers Supervisors für eine Zone mit NSX-Netzwerk

Erfahren Sie, wie Sie einen Supervisor mit NSX-Netzwerk auf einem vSphere-Cluster bereitstellen, der einer vSphere-Zone zugeordnet ist. Der sich daraus ergebende Supervisor verfügt über eine Hochverfügbarkeit auf Hostebene, die von vSphere HA bereitgestellt wird. Ein Supervisor für eine Zone unterstützt alle Tanzu Kubernetes-Cluster, VMs und vSphere-Pods.

Wenn Sie NSX Version 4.1.1 oder höher konfiguriert haben und NSX Advanced Load Balancer Version 22.1.4 oder höher mit Enterprise-Lizenz für NSXinstalliert, konfiguriert und registriert haben, ist der Lastausgleichsdienst, der mit NSX verwendet wird, NSX Advanced Load Balancer. Wenn Sie Versionen von NSX vor 4.1.1 konfiguriert haben, wird der NSX-Lastausgleichsdienst verwendet. Weitere Informationen finden Sie unter Kapitel 7 Überprüfen des mit dem NSX-Netzwerk verwendeten Lastausgleichsdiensts.

Hinweis Nachdem Sie einen Supervisor auf einem einzelnen vSphere Cluster bereitgestellt haben, was zum Erstellen einer vSphere-Zone führt, können Sie den Supervisor nicht auf eine Bereitstellung mit drei Zonen erweitern. Sie können einen Supervisor entweder in einer vSphere-Zone (Bereitstellung mit einem einzelnen Cluster) oder in drei vSphere-Zonen bereitstellen.

Voraussetzungen

Überprüfen Sie, ob Ihre Umgebung die Systemanforderungen für die Konfiguration eines vSphere-Clusters als Supervisor erfüllt. Informationen zu den Anforderungen finden Sie unter Voraussetzungen für die Konfiguration von vSphere IaaS control plane in vSphere-Cluster.

Verfahren

1. Wählen Sie im Startmenü die Option **Arbeitslastverwaltung** aus.
2. Wählen Sie eine Lizenzierungsoption für den Supervisor aus.
   - Wenn Sie über eine gültige Tanzu Edition-Lizenz verfügen, klicken Sie auf **Lizenz hinzufügen**, um den Lizenzschlüssel der Lizenzbestandsliste von vSphere hinzuzufügen.
   - Wenn Sie noch keine Tanzu Edition-Lizenz haben, geben Sie die Kontaktdetails ein, damit Sie Mitteilungen von VMware empfangen können, und klicken Sie auf **Erste Schritte**.

   Der Testzeitraum eines Supervisors beträgt 60 Tage. Innerhalb dieses Zeitraums müssen Sie dem Cluster eine gültige Tanzu Edition-Lizenz zuweisen. Wenn Sie einen Tanzu Edition-Lizenzschlüssel hinzugefügt haben, können Sie diesen Schlüssel innerhalb des 60-Tage-Testzeitraums zuweisen, sobald Sie die Einrichtung des Supervisors abgeschlossen haben.
3. Klicken Sie auf dem Bildschirm **Arbeitslastverwaltung** erneut auf **Erste Schritte**.

4 Wählen Sie auf der Seite **vCenter-Server und -Netzwerk** das vCenter Server-System aus, das für die Supervisor-Bereitstellung eingerichtet ist, und wählen Sie **NSX** als Netzwerk-Stack aus.

5 Wählen Sie auf der Seite **Supervisor-Speicherort** die Option **Cluster-Bereitstellung** aus.

   a Geben Sie einen Namen für den neuen Supervisor ein.

   b Wählen Sie einen kompatiblen vSphere-Cluster aus.

   c Geben Sie einen Namen für die vSphere-Zone ein, der automatisch für den ausgewählten Cluster erstellt wird.

   Wenn Sie keinen Namen für die Zone angeben, wird automatisch ein Name für die Zone generiert.

   d Klicken Sie auf **Weiter**.

6 Wählen Sie Speicherrichtlinien für den Supervisor aus.

Mit der Speicherrichtlinie, die Sie für jedes der folgenden Objekte auswählen, wird sichergestellt, dass das Objekt in dem Datenspeicher platziert wird, auf den in der Speicherrichtlinie verwiesen wird. Sie können dieselben oder unterschiedliche Speicherrichtlinien für die Objekte verwenden.

Option	Bezeichnung
Speicherrichtlinie für Steuerungsebene	Wählen Sie die Speicherrichtlinie für die Platzierung der Control Plane-VMs aus.
Speicherrichtlinie für flüchtige Festplatten	Wählen Sie die Speicherrichtlinie für die Platzierung der vSphere-Pods aus.
Speicherrichtlinie für Image-Cache	Wählen Sie die Speicherrichtlinie für die Platzierung des Caches von Container-Images aus.

7 Konfigurieren Sie auf dem Bildschirm **Verwaltungsnetzwerk** die Parameter für das Netzwerk, das für die VMs der Kubernetes-Steuerungsebene verwendet wird.

a Wählen Sie einen **Netzwerkmodus** aus.

- **DHCP-Netzwerk**. In diesem Modus werden alle IP-Adressen für das Verwaltungsnetzwerk, wie IP-Adressen von Steuerungsebenen-VMs, DNS-Server, DNS, Suchdomänen und NTP-Server, automatisch von einem DHCP erfasst.
- **Statisch**. Geben Sie alle Netzwerkeinstellungen für das Verwaltungsnetzwerk manuell ein.

b Konfigurieren Sie die Einstellungen für das Verwaltungsnetzwerk.

Wenn Sie den DHCP-Netzwerkmodus ausgewählt haben, aber die von DHCP erfassten Einstellungen überschreiben möchten, klicken Sie auf **Zusätzliche Einstellungen** und geben Sie neue Werte ein. Wenn Sie den statischen Netzwerkmodus ausgewählt haben, geben Sie die Werte für die Verwaltungsnetzwerkeinstellungen manuell ein.

Option	Bezeichnung
Netzwerk	Wählen Sie ein Netzwerk aus, für das ein VMkernel-Adapter für den Verwaltungsdatenverkehr konfiguriert ist.
Steuerungs-IP-Startadresse	Geben Sie eine IP-Adresse ein, die den Startpunkt für die Reservierung von fünf aufeinanderfolgenden IP-Adressen für die Kubernetes-Steuerungsebenen-VMs wie folgt festlegt: ■ Eine IP-Adresse für jede der Kubernetes-Steuerungsebenen-VMs. ■ Eine Floating-IP-Adresse für eine der Kubernetes-Steuerungsebenen-VMs als Schnittstelle zum Verwaltungsnetzwerk. Die Steuerungsebenen-VM mit der zugewiesenen Floating-IP-Adresse fungiert als führende VM für alle drei Kubernetes-Steuerungsebenen-VMs. Die Floating IP-Adresse wird zum Knoten der Steuerungsebene verschoben, der als etcd-Leader im Kubernetes-Cluster fungiert. Bei diesem handelt es sich um den Supervisor. Dadurch wird die Verfügbarkeit im Falle eines Netzwerkpartitionsereignisses verbessert. ■ Eine IP-Adresse, die als Puffer dienen soll, falls eine Kubernetes-Steuerungsebenen-VM ausfällt und eine neue Steuerungsebenen-VM als Ersatz bereitgestellt wird.
Subnetzmaske	Gilt nur für die Konfiguration statischer IP-Adressen. Geben Sie die Subnetzmaske für das Verwaltungsnetzwerk ein. Beispielsweise `255.255.255.0`
DNS-Server	Geben Sie die Adressen der DNS-Server ein, die Sie in Ihrer Umgebung verwenden. Wenn das vCenter Server-System mit einem FQDN registriert ist, müssen Sie die IP-Adressen der DNS-Server eingeben, die Sie mit der vSphere-Umgebung verwenden, damit der FQDN im Supervisor aufgelöst werden kann.

Option	Bezeichnung
DNS-Suchdomänen	Geben Sie Domänennamen ein, die von DNS innerhalb der Kubernetes Control Plane-Knoten durchsucht werden, z. B. `corp.local`, damit der DNS-Server sie auflösen kann.
NTP	Geben Sie die Adressen der NTP-Server ein, die Sie in Ihrer Umgebung verwenden (sofern vorhanden).

8 Konfigurieren Sie im Bereich **Arbeitslastennetzwerk** die Einstellungen für die Netzwerke für Namespaces.

Option	Bezeichnung
vSphere Distributed Switch	Wählen Sie den vSphere Distributed Switch aus, der das Overlay-Netzwerk für den Supervisor verarbeitet. Wählen Sie z. B. `DSwitch` aus.
DNS-Server	Geben Sie, sofern vorhanden, die IP-Adressen der DNS-Server ein, die Sie in Ihrer Umgebung verwenden. Beispiel: `10.142.7.1`.
NAT-Modus	Der NAT-Modus ist standardmäßig aktiviert. Wenn Sie die Option deaktivieren, sind alle Arbeitslasten wie die IP-Adressen der vSphere-Pods, VMs und Tanzu Kubernetes-Clusterknoten von außerhalb des Tier-0-Gateways direkt zugänglich, und Sie müssen die Egress-CIDRs nicht konfigurieren. **Hinweis** Wenn Sie den NAT-Modus deaktivieren, wird die Dateivolume-Speicherung nicht unterstützt.
Namespace-Netzwerk	Geben Sie einen oder mehrere IP-CIDRs ein, um Subnetze/Segmente zu erstellen und IP-Adressen Arbeitslasten zuzuweisen.
Ingress-CIDRs	Geben Sie eine CIDR-Anmerkung zur Ermittlung des Ingress-IP-Bereichs für die Kubernetes-Dienste ein. Dieser Bereich wird für Dienste vom Typ „Load Balancer“ und „Ingress“ verwendet.
Edge-Cluster	Wählen Sie den NSX Edge-Cluster mit dem Tier-0-Gateway aus, das Sie für das Namespace-Netzwerk verwenden möchten. Wählen Sie z. B. `EDGE-CLUSTER` aus.
Tier-0-Gateway	Wählen Sie das Tier-0-Gateway aus, das mit dem Cluster-Tier-1-Gateway verknüpft werden soll.
Subnetz-Präfix	Geben Sie das Subnetzpräfix ein, das die Größe des für Namespace-Segmente reservierten Subnetzes angibt. Der Standardwert ist „28“.
Dienst-CIDRs	Geben Sie eine CIDR-Anmerkung ein, um den IP-Bereich für Kubernetes-Dienste zu ermitteln. Sie können den Standardwert verwenden.
Egress-CIDRs	Geben Sie eine CIDR-Anmerkung zur Ermittlung der Egress-IP für Kubernetes-Dienste ein. Für jeden Namespace im Supervisor wird nur eine Egress-IP-Adresse zugewiesen. Bei der Egress-IP handelt es sich um die IP-Adresse, die die Kubernetes-Arbeitslasten im jeweiligen Namespace verwenden, um außerhalb von NSX zu kommunizieren.

9 Scrollen Sie auf der Seite **Überprüfen und bestätigen** nach oben und überprüfen Sie alle bisher konfigurierten Einstellungen und legen Sie erweiterte Einstellungen für die Supervisor-Bereitstellung fest.

Option	Beschreibung
Größe der Supervisor-Steuerungsebene	Wählen Sie die Dimensionierung für die Steuerungsebenen-VMs aus. Die Größe der Steuerungsebenen-VMs bestimmt die Menge der Arbeitslasten, die Sie auf dem Supervisor ausführen können. Sie können wählen zwischen: ■ Sehr klein – 2 CPUs, 8 GB Arbeitsspeicher, 32 GB Speicher ■ Klein – 4 CPUs, 16 GB Arbeitsspeicher, 32 GB Speicher ■ Mittel – 8 CPUs, 16 GB Arbeitsspeicher, 32 GB Speicher ■ Groß – 16 CPUs, 32 GB Arbeitsspeicher, 32 GB Speicher **Hinweis** Sobald Sie eine Größe der Steuerungsebene ausgewählt haben, können Sie nur noch vertikal hochskalieren. Sie können nicht auf eine kleinere Größe herunterskalieren.
DNS-Namen des API-Servers	Geben Sie optional die FQDNs ein, die für den Zugriff auf die Supervisor-Steuerungsebene verwendet werden sollen, anstatt die IP-Adresse der Supervisor-Steuerungsebene zu verwenden. Die von Ihnen eingegebenen FQDNs werden in ein automatisch generiertes Zertifikat eingebettet. Wenn Sie FQDNs für Supervisor verwenden, können Sie die Angabe eines IP-Sands im Zertifikat des Lastausgleichsdiensts auslassen.
Konfiguration exportieren	Exportieren Sie eine JSON-Datei, die die Werte der eingegebenen Supervisor-Konfiguration enthält. Sie können die Datei später ändern und importieren, wenn Sie die Supervisor erneut bereitstellen möchten oder wenn Sie eine neue Supervisor mit ähnlicher Konfiguration bereitstellen möchten. Wenn Sie die Supervisor Konfiguration exportieren, sparen Sie im Falle einer erneuten Bereitstellung von Supervisor zeitsparend alle Konfigurationswerte in diesen Assistenten.

10 Klicken Sie auf **Beenden**, wenn Sie mit der Überprüfung der Einstellungen fertig sind.

Die Bereitstellung von Supervisor initiiert die Erstellung und Konfiguration der Steuerungsebenen-VMs und anderer Komponenten.

11 Verfolgen Sie auf der Registerkarte **Supervisoren** den Bereitstellungsvorgang des Supervisors.

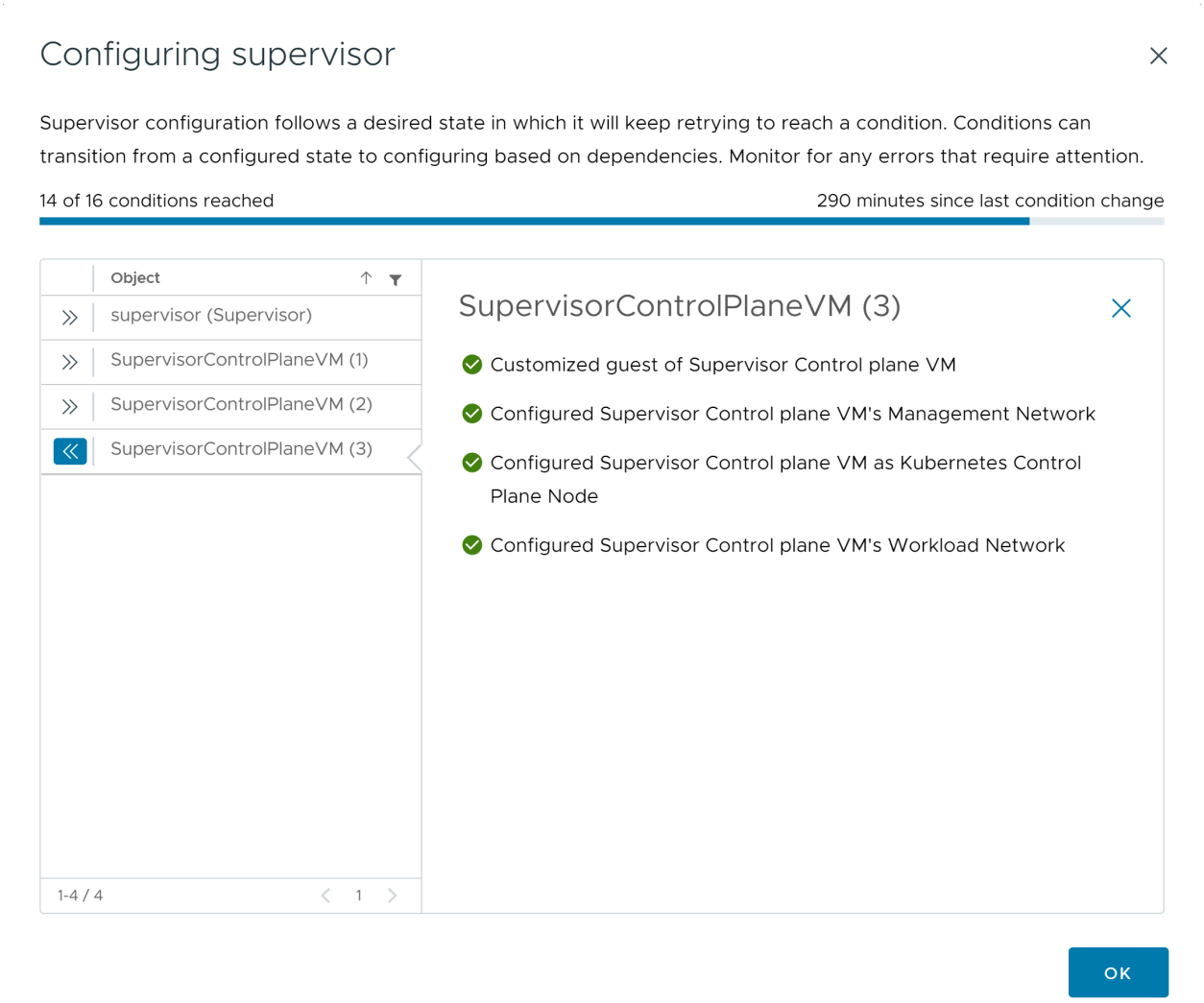
a Klicken Sie in der Spalte **Konfigurationsstatus** neben dem Status des Supervisors auf **Anzeigen**.

b Zeigen Sie den Konfigurationsstatus für jedes Objekt an und halten Sie nach möglichen zu behebenden Problemen Ausschau.

Nächste Schritte

Sobald der Assistent zum Aktivieren eines Supervisors fertig ist, können Sie den Aktivierungsprozess verfolgen und nach potenzielle Problemen Ausschau halten, die eine Fehlerbehebung erfordern. Klicken Sie in der Spalte **Konfigurationsstatus** neben dem Status des Supervisors auf **Anzeigen**.

Abbildung 6-2. Supervisor-Aktivierungsansicht



Damit der Bereitstellungsvorgang abgeschlossen werden kann, muss der Supervisor den gewünschten Zustand erreichen. Demnach müssen alle 16 Bedingungen erfüllt sein. Wenn ein Supervisor erfolgreich aktiviert wurde, ändert sich sein Status von „Konfigurieren“ zu „Wird ausgeführt“. Während sich der Supervisor im Status „Konfigurieren“ befindet, wird kontinuierlich und wiederholt überprüft, ob die einzelnen Bedingungen erfüllt sind. Wenn eine Bedingung nicht erfüllt wird, wird der Vorgang wiederholt, bis er erfolgreich ist. Aus diesem Grund kann sich die Anzahl der erreichten Bedingungen ändern. Beispiel: *10 von 16 Bedingungen wurden erfüllt*, dann *4 von 16 Bedingungen wurden erfüllt* usw. In sehr seltenen Fällen kann sich der Status in „Fehler“ ändern, wenn Fehler vorliegen, aufgrund derer der gewünschte Status nicht erreicht werden kann.

Weitere Informationen zu Bereitstellungsfehlern und zur Fehlerbehebung finden Sie unter Beheben von Fehlerzuständen auf den VMs einer Supervisor-Steuerungsebene während der Aktivierung oder Aktualisierung.

Falls Sie versuchen möchten, die Supervisor erneut bereitzustellen, indem Sie die Konfigurationswerte ändern, die Sie im Assistenten eingegeben haben, überprüfen Sie Kapitel 9 Bereitstellen eines Supervisor durch Importieren einer JSON-Konfigurationsdatei.

Überprüfen des mit dem NSX-Netzwerk verwendeten Lastausgleichsdiensts

7

Ein Supervisor, der mit NSX-Netzwerk konfiguriert ist, kann den NSX-Lastausgleichsdienst oder den NSX Advanced Load Balancer verwenden.

Wenn Sie NSX Version 4.1.1 oder höher konfiguriert haben und NSX Advanced Load Balancer Version 22.1.4 oder höher mit einer Enterprise-Lizenz im NSX installiert, konfiguriert und registriert haben, handelt es sich bei dem Lastausgleichsdienst, der mit NSX verwendet wird, um NSX Advanced Load Balancer. Wenn Sie Versionen von NSX vor 4.1.1 konfiguriert haben, wird der NSX-Lastausgleichsdienst verwendet.

Führen Sie den folgenden Befehl aus, um zu überprüfen, welcher Lastausgleichsdienst mit NSX konfiguriert ist:

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

Wenn sich ein Gateway-Finalizer `gateway.ako.vmware.com` oder Ingress-Finalizer-`ingress.ako.vmware.com/finalizer` in der Spezifikation befindet, zeigt dies an, dass der NSX Advanced Load Balancer konfiguriert ist.

Exportieren einer Supervisor-Konfiguration

8

Erfahren Sie, wie Sie die Konfiguration eines vorhandenen Supervisor exportieren, den Sie später in den Supervisor-Aktivierungsassistenten importieren können, um eine neue Supervisor-Instanz mit einer ähnlichen Konfiguration bereitzustellen. Der Supervisor exportiert in eine JSON-Konfigurationsdatei, die Sie nach Bedarf ändern und zum Bereitstellen einer neuen Supervisor-Instanz verwenden können.

Das Exportieren einer Supervisor-Konfiguration ermöglicht Ihnen Folgendes:

- Supervisor-Konfigurationen beibehalten. Sie können alle vorherigen Supervisor-Konfigurationen exportieren und bei Bedarf wiederverwenden.
- Effizientere Fehlerbehebung. Wenn eine Supervisor-Aktivierung fehlschlägt, können Sie die Supervisor-Konfiguration direkt in der JSON-Datei anpassen und den Prozess neu starten. Das ermöglicht eine schnelle Fehlerbehebung, da Sie die Einstellungen direkt in der JSON-Datei ändern können, bevor Sie sie importieren.
- Optimierte Verwaltung. Sie können die exportierte Supervisor-Konfiguration für andere Administratoren freigeben, um neue Supervisoren mit ähnlichen Einstellungen einzurichten.
- Einheitliches Format. Die exportierten Supervisor-Konfigurationen folgen einem standardisierten Format, das für die unterstützten Bereitstellungstypen gilt.

Sie können die Supervisor-Konfiguration auch während des Supervisor-Aktivierungsworkflows exportieren. Weitere Informationen hierzu finden Sie unter Kapitel 5 Bereitstellen eines Supervisor für drei Zonen und Kapitel 6 Bereitstellen einer Supervisor für eine Zone .

Voraussetzungen

Stellen Sie einen Supervisor bereit.

Verfahren

1. Navigieren Sie zu **Arbeitslastmanagement > Supervisor > Supervisoren**.
2. Wählen Sie einen Supervisor aus und wählen Sie **Konfiguration exportieren** aus.

Ergebnisse

Die Konfiguration wird exportiert und in einer ZIP-Datei mit dem Namen `wcp-config.zip` gespeichert, die lokal im standardmäßigen Download-Ordner des Browsers gespeichert ist. In der `wcp-config.zip`-Datei finden Sie Folgendes:

- Eine JSON-Datei, die die Supervisor-Konfiguration mit dem Namen `wcp-config.jso` enthält. Jede Konfigurationseinstellung hat einen entsprechenden Namen und Speicherort in der JSON-Datei. Diese JSON-Datei ist Teil einer hierarchischen Datenstruktur.
- Eine gültige JSON-Schemadatei mit dem Namen `wcp-config-schema.json`. Diese Datei beschreibt alle exportierbaren Einstellungen für den Supervisor. Dazu gehören der Typ, der Speicherort in der JSON-Datei und ob sie erforderlich sind. Sie können die Schemadatei verwenden, um eine JSON-Beispielkonfigurationsdatei zu generieren, die Sie manuell beauffüllen und in einen neuen Aktivierungsworkflow importieren können.

Nächste Schritte

'

Bearbeiten Sie die JSON-Konfiguration nach Bedarf und verwenden Sie sie, um neue Supervisoren bereitzustellen. Weitere Informationen hierzu finden Sie unter Kapitel 9 Bereitstellen eines Supervisor durch Importieren einer JSON-Konfigurationsdatei.

Bereitstellen eines Supervisor durch Importieren einer JSON-Konfigurationsdatei

9

Erfahren Sie, wie Sie alle Konfigurationswerte im Supervisor-Aktivierungsassistenten automatisch auffüllen, indem Sie eine JSON-Konfigurationsdatei importieren, die Sie aus vorherigen Supervisor-Bereitstellungen exportiert haben. Bei der Fehlerbehebung bei einer nicht erfolgreichen Supervisor-Bereitstellung oder bei der Bereitstellung eines neuen Supervisor mit einer ähnlichen Konfiguration können Sie die Konfigurationswerte direkt in der JSON-Datei ändern, bevor Sie sie in den Assistenten importieren. Auf diese Weise sparen Sie Zeit beim manuellen Ausfüllen aller Werte im Aktivierungsassistenten und können sich einfach auf die Bereiche konzentrieren, für die eine Änderung erforderlich ist.

Sie können die Konfiguration eines Supervisor auf zwei Arten exportieren:

- Während der Supervisor-Bereitstellung auf der Seite **Bereit zum Abschließen** des Assistenten. Weitere Informationen hierzu finden Sie unter Kapitel 5 Bereitstellen eines Supervisor für drei Zonen und Kapitel 6 Bereitstellen einer Supervisor für eine Zone .
- Exportieren Sie die Konfiguration eines bereits bereitgestellten Supervisor. Weitere Informationen hierzu finden Sie unter Kapitel 8 Exportieren einer Supervisor-Konfiguration.

Voraussetzungen

- Erfüllen Sie die Voraussetzungen zum Konfigurieren von vSphere-Clustern als Supervisor. Weitere Informationen hierzu finden Sie unter Voraussetzungen für die Konfiguration von vSphere IaaS control plane in vSphere-Cluster.
- Stellen Sie sicher, dass Sie über eine JSON-Konfigurationsdatei verfügen, die Sie aus einer vorherigen Supervisor-Bereitstellung exportiert haben. Der Standardname der Datei ist `wcp-config.json`.

Verfahren

1 Initiieren Sie eine SupervisorBereitstellung auf eine der folgenden Arten:

   - Wenn Sie Supervisor noch nicht erfolgreich bereitgestellt haben, klicken Sie auf der Seite **Arbeitslastverwaltung** auf **Gestartet**.
   - Wenn Sie eine zusätzliche Supervisor in Ihrer Umgebung bereitstellen möchten, wählen Sie **Arbeitslastverwaltung > Supervisor > Supervisoren > Supervisor hinzufügen** aus.

2 Wählen Sie in der oberen rechten Ecke **Konfiguration importieren** aus.

   Der vSphere Client überprüft die Werte in der JSON-Datei. Wenn die hochgeladene JSON-Datei ungültig oder beschädigt ist, werden möglicherweise Fehler angezeigt. Ebenso werden Fehler angezeigt, wenn in der JSON-Datei die Spezifikationsversion fehlt oder wenn die Spezifikationsversion höher ist als die aktuell vom Client unterstützte Version. Aus diesem Grund sollten Sie nur die Einstellungen bearbeiten, die Sie vor dem Importieren der Konfigurationsdatei benötigt haben. Wenn die Datei beschädigt ist, können Sie das JSON-Schema verwenden, um eine leere Supervisor-Konfiguration zu generieren, die Sie mit den benötigten Werten ausfüllen können.

3 Klicken Sie im Dialogfeld **Supervisor-Konfiguration** auf **Hochladen** und wählen Sie eine JSON-Konfigurationsdatei aus, die Sie zuvor exportiert haben.

4 Klicken Sie auf **Import**.

   Die in der JSON-Konfigurationsdatei aufgezeichneten Werte werden im Supervisor-Aktivierungsassistenten aufgefüllt. Möglicherweise müssen Sie bestimmte Einstellungen manuell eingeben, z. B. das Kennwort des Lastausgleichsdiensts.

5 Klicken Sie im Assistenten auf **Weiter** und geben Sie ggf. Werte ein.

6 Scrollen Sie auf der Seite **Überprüfen und bestätigen** nach oben und überprüfen Sie alle bisher konfigurierten Einstellungen. Führen Sie dann gegebenenfalls letzte Änderungen durch.

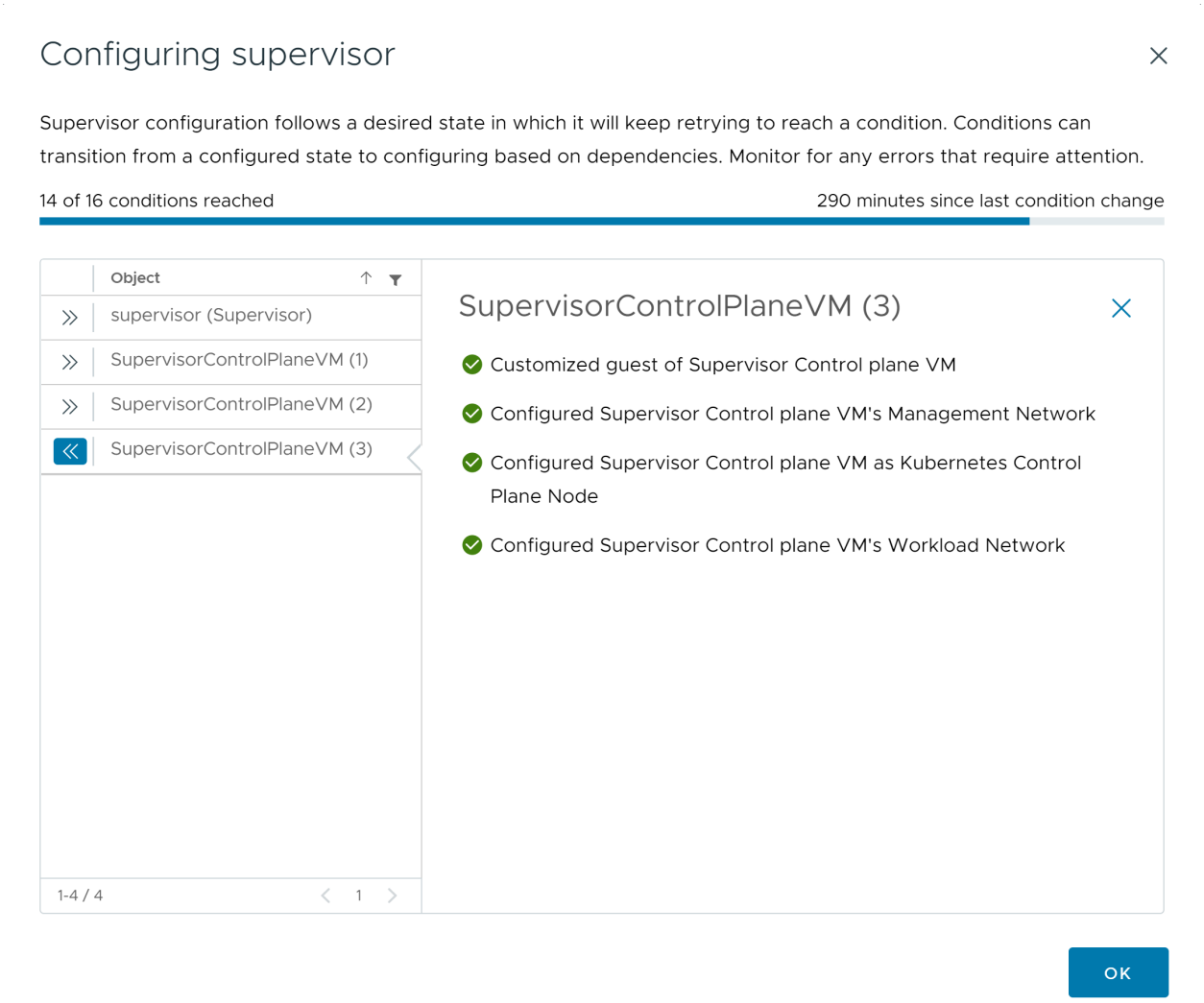
7 Klicken Sie auf **Beenden**, wenn Sie mit der Überprüfung der Einstellungen fertig sind.

   Die Aktivierung von Supervisor initiiert die Erstellung und Konfiguration der Steuerungsebenen-VMs und anderer Komponenten.

Nächste Schritte

Sobald der Assistent zum Aktivieren eines Supervisors fertig ist, können Sie den Aktivierungsprozess verfolgen und nach potenzielle Problemen Ausschau halten, die eine Fehlerbehebung erfordern. Klicken Sie in der Spalte **Konfigurationsstatus** neben dem Status des Supervisors auf **Anzeigen**.

Abbildung 9-1. Supervisor-Aktivierungsansicht



Damit der Bereitstellungsvorgang abgeschlossen werden kann, muss der Supervisor den gewünschten Zustand erreichen. Demnach müssen alle 16 Bedingungen erfüllt sein. Wenn ein Supervisor erfolgreich aktiviert wurde, ändert sich sein Status von „Konfigurieren“ zu „Wird ausgeführt“. Während sich der Supervisor im Status „Konfigurieren“ befindet, wird kontinuierlich und wiederholt überprüft, ob die einzelnen Bedingungen erfüllt sind. Wenn eine Bedingung nicht erfüllt wird, wird der Vorgang wiederholt, bis er erfolgreich ist. Aus diesem Grund kann sich die Anzahl der erreichten Bedingungen ändern. Beispiel: *10 von 16 Bedingungen wurden erfüllt*, dann *4 von 16 Bedingungen wurden erfüllt* usw. In sehr seltenen Fällen kann sich der Status in „Fehler“ ändern, wenn Fehler vorliegen, aufgrund derer der gewünschte Status nicht erreicht werden kann.

Weitere Informationen zu Bereitstellungsfehlern und zur Fehlerbehebung finden Sie unter Beheben von Fehlerzuständen auf den VMs einer Supervisor-Steuerungsebene während der Aktivierung oder Aktualisierung.

Zuweisen einer Lizenz zum Supervisor

10

Wenn Sie einen Supervisor im Testmodus verwenden, müssen Sie dem Cluster vor Ablauf der 60-Tage-Testphase eine Lösungslizenz (VVF oder VCF) oder eine Tanzu Edition-Lizenz zuweisen.

Unter Lizenzierung für vSphere IaaS control plane finden Sie Informationen zur Funktionsweise der Tanzu-Lizenz.

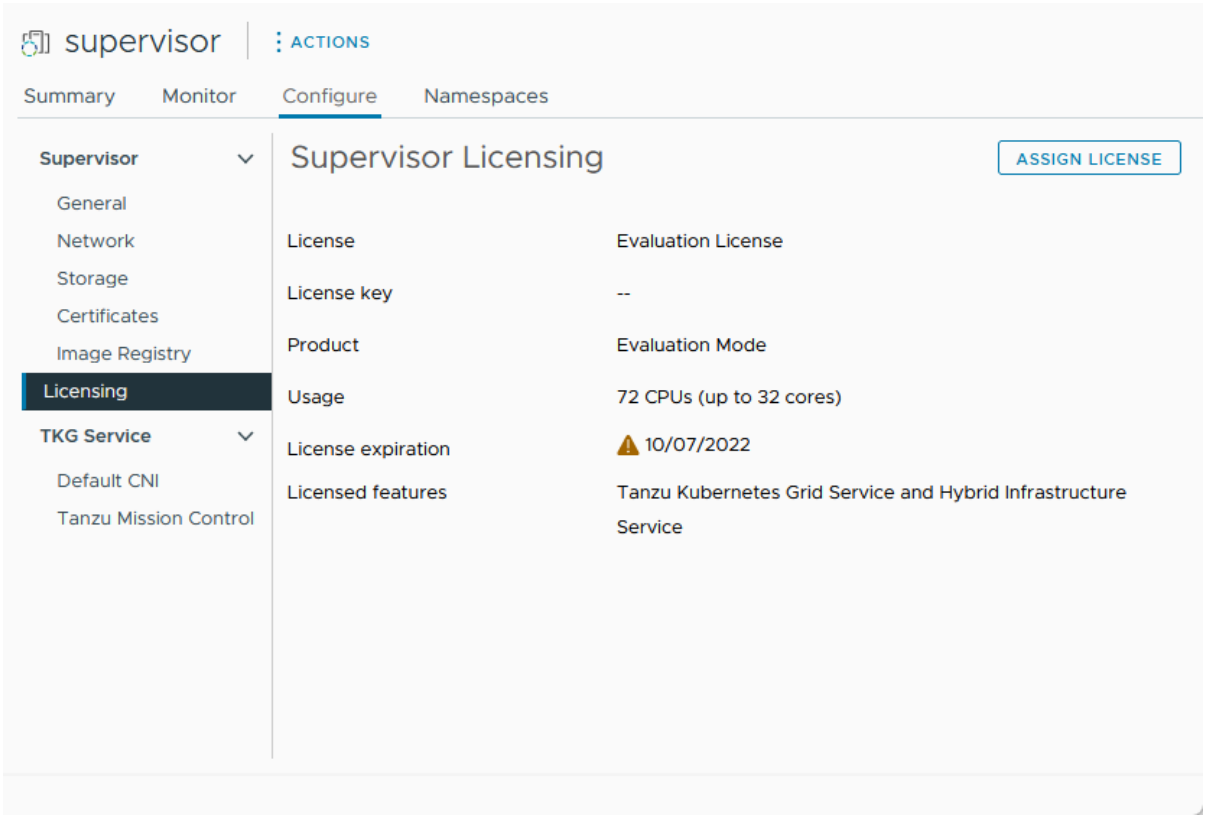
Verfahren

1 Navigieren Sie im vSphere Client zu **Arbeitslastverwaltung**.

2 Wählen Sie **Supervisoren** und dann den Supervisor aus der Liste aus.

3 Wählen Sie **Konfigurieren > Lizenzierung** aus.

Abbildung 10-1. Weisen Sie der Supervisor-Benutzeroberfläche eine Lizenz zu.



4 Klicken Sie auf **Lizenz zuweisen**.

5 Klicken Sie im **Lizenz zuweisen** auf **Neue Lizenz**.

6 Geben Sie einen gültigen Lizenzschlüssel ein und klicken Sie auf **OK**.

Herstellen einer Verbindung mit vSphere IaaS control plane-Clustern

11

Sie stellen eine Verbindung mit dem Supervisor her, um Tanzu Kubernetes-Cluster, vSphere-Pods und VMs bereitzustellen. Sobald die Bereitstellung abgeschlossen ist, können Sie mit verschiedenen Methoden eine Verbindung mit Tanzu Kubernetes Grid-Clustern herstellen und sich basierend auf Ihrer Rolle und dem von Ihnen verfolgten Ziel authentifizieren.

Lesen Sie als Nächstes die folgenden Themen:

- Herunterladen und Installieren von Kubernetes-CLI-Tools für vSphere
- Konfigurieren der sicheren Anmeldung für vSphere IaaS control plane-Cluster
- Herstellen einer Verbindung mit dem Supervisor als vCenter Single Sign-On-Benutzer
- Gewähren des Entwicklerzugriffs auf Tanzu Kubernetes-Cluster

Herunterladen und Installieren von Kubernetes-CLI-Tools für vSphere

Sie können Kubernetes-CLI-Tools für vSphere verwenden, um sich bei der Supervisor-Steuerungsebene anzumelden, auf die vSphere-Namespaces zuzugreifen, für die Sie über Berechtigungen verfügen, sowie vSphere-Pods, Tanzu Kubernetes Grid-Cluster und VMs bereitzustellen und zu verwalten.

Das Downloadpaket der Kubernetes CLI-Tools enthält zwei ausführbare Dateien: die standardmäßige kubectl-Open Source-Datei und das vSphere-Plug-In für kubectl. Die kubectl-CLI weist eine austauschbare Architektur (Pluggable Storage Architecture, PSA) auf. Durch das vSphere-Plug-In für kubectl werden die für kubectl verfügbaren Befehle erweitert, sodass Sie mithilfe der vCenter Single Sign-On-Anmeldedaten eine Verbindung mit dem Supervisor und den Tanzu Kubernetes Grid-Clustern herstellen können.

Hinweis Es hat sich als Best Practice bewährt, nach dem Durchführen eines vSphere-Namespace-Updates und dem Upgrade von Supervisor das vSphere-Plug-In für kubectl zu aktualisieren. Weitere Informationen finden Sie unter Aktualisieren des vSphere-Plug-Ins für kubectl in *Wartung der vSphere IaaS-Steuerungsebene*.

Verfahren

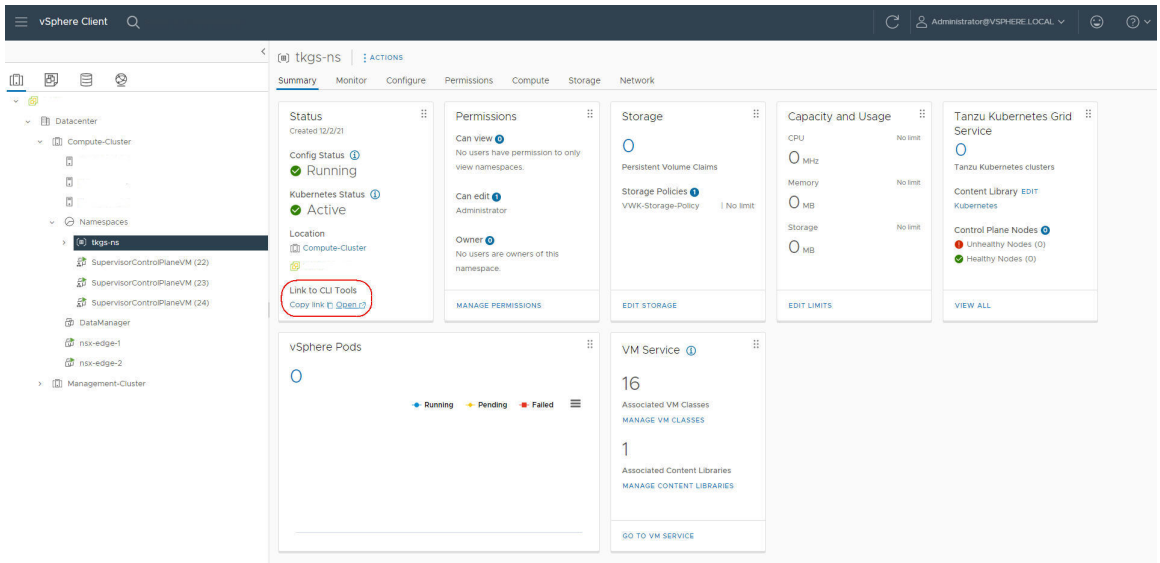
1 Rufen Sie die IP-Adresse oder den FQDN der Supervisor-Steuerungsebene ab, die auch die Download-URL für Kubernetes-CLI-Tools für vSphere ist.

Falls Sie ein DevOps-Techniker sind, der keinen Zugriff auf die vSphere-Umgebung hat, können Sie Ihren vSphere-Administrator bitten, die folgenden Schritte auszuführen.

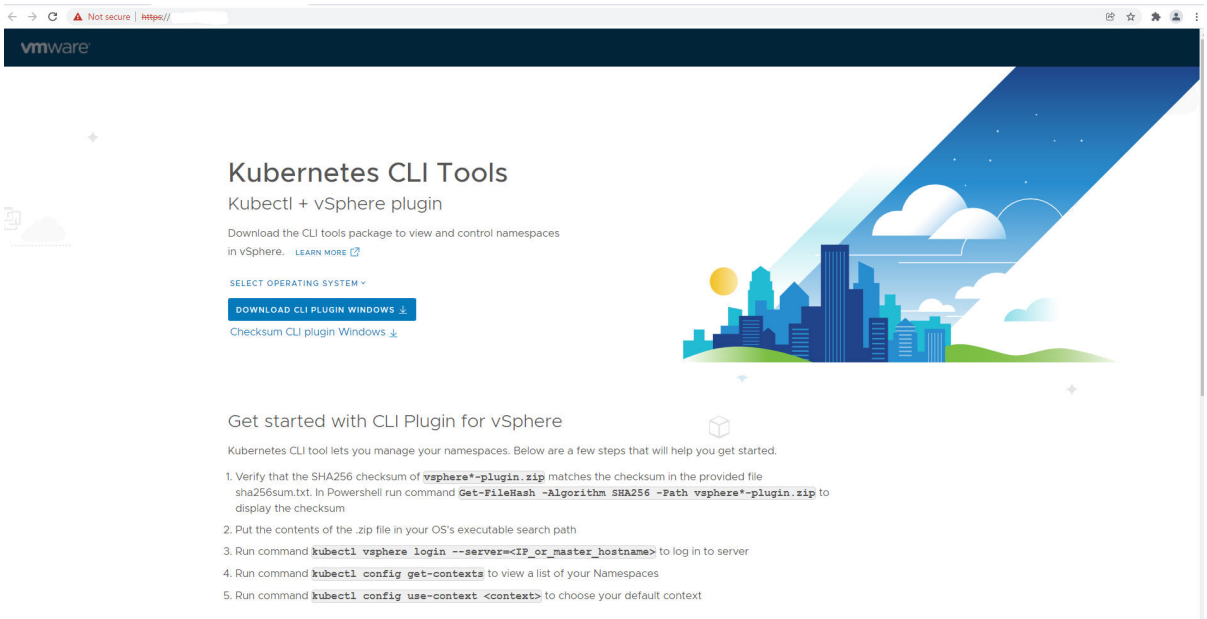
a Navigieren Sie in vSphere Client zu **Arbeitslastmanagement > Namespaces** und wählen Sie einen vSphere-Namespace aus.

b Wählen Sie die Registerkarte **Übersicht** aus und suchen Sie nach dem Bereich **Status**.

c Klicken Sie unter **Link zu CLI-Tools** auf **Öffnen** oder auf **Link kopieren**.



2 Öffnen Sie in einem Browser die Download-URL der **Kubernetes CLI-Tools**.



3 Wählen Sie das Betriebssystem aus.

4 Laden Sie die Datei `vsphere-plugin.zip` herunter.

5 Extrahieren Sie den Inhalt der ZIP-Datei in ein Arbeitsverzeichnis.

   Das Paket `vsphere-plugin.zip` enthält zwei ausführbare Dateien: kubectl und vSphere-Plug-In für kubectl. `kubectl` ist die standardmäßige Kubernetes-CLI. `kubectl-vsphere` ist das vSphere-Plug-In für kubectl, mit dem Sie sich mithilfe Ihrer vCenter Single Sign-On Anmeldedaten beim Supervisor und bei den Tanzu Kubernetes-Clustern authentifizieren können.

6 Fügen Sie den Speicherort der beiden ausführbaren Dateien der Variable PATH Ihres Systempfads hinzu.

7 Um die Installation der kubectl-CLI zu überprüfen, starten Sie eine Sitzung über eine Shell, ein Terminal oder eine Eingabeaufforderung und führen Sie den `kubectl`-Befehl aus.

   Die kubectl-Banner-Meldung und die Liste der Befehlszeilenoptionen werden für die CLI angezeigt.

8 Führen Sie zum Überprüfen der Installation des vSphere-Plug-In für kubectl den Befehl `kubectl vsphere` aus.

   Die vSphere-Plug-In für kubectl-Banner-Meldung und die Liste der Befehlszeilenoptionen für das Plug-In werden angezeigt.

Nächste Schritte

Konfigurieren der sicheren Anmeldung für vSphere IaaS control plane-Cluster.

Konfigurieren der sicheren Anmeldung für vSphere IaaS control plane-Cluster

Damit Sie sich sicher bei Supervisor- und Tanzu Kubernetes Grid-Clustern anmelden können, konfigurieren Sie das vSphere-Plug-In für kubectl mit dem entsprechenden TLS-Zertifikat und achten Sie darauf, dass Sie die neueste Version des Plug-In ausführen.

Supervisor-CA-Zertifikat

vSphere IaaS control plane unterstützt vCenter Single Sign-On für den Clusterzugriff mithilfe des vSphere-Plug-In für kubectl-Befehls `kubectl vsphere login ...`. Informationen zum Installieren und Verwenden dieses Dienstprogramms finden Sie unter Herunterladen und Installieren von Kubernetes-CLI-Tools für vSphere.

Das vSphere-Plug-In für kubectl verwendet standardmäßig eine sichere Anmeldung und erfordert ein vertrauenswürdiges Zertifikat, wobei standardmäßig das von der vCenter Server-Stammzertifizierungsstelle signierte Zertifikat verwendet wird. Das Plug-In unterstützt zwar das `--insecure-skip-tls-verify`-Flag, aber dies wird aus Sicherheitsgründen nicht empfohlen.

Um sich mit dem vSphere-Plug-In für kubectl sicher bei den Supervisor- und Tanzu Kubernetes Grid-Clustern anzumelden, haben Sie zwei Möglichkeiten:

Option	Anleitung
Laden Sie das Zertifikat der vCenter Server-Stammzertifizierungsstelle herunter und installieren Sie es auf jedem Clientcomputer.	Weitere Informationen finden Sie im VMware-Knowledgebase-Artikel Vorgehensweise zum Herunterladen und Installieren von vCenter Server-Stammzertifikaten.
Ersetzen Sie das für Supervisor verwendete VIP-Zertifikat durch ein Zertifikat, das von einer Zertifizierungsstelle signiert wurde, der jede Clientmaschine vertraut.	Siehe Ersetzen des VIP-Zertifikats zur sicheren Verbindung mit dem Supervisor-API-Endpoint.

Hinweis Weitere Informationen zur vSphere-Authentifizierung, einschließlich vCenter Single Sign-On, Verwaltung und Rotation von vCenter Server-Zertifikaten und Fehlerbehebung bei der Authentifizierung, finden Sie in der Dokumentation zu vSphere Authentication. Weitere Informationen zu Zertifikaten für vSphere IaaS control plane finden Sie im VMware Knowledgebase-Artikel 89324.

CA-Zertifikat für Tanzu Kubernetes Grid-Cluster

Um mithilfe der `kubectl`-CLI eine sichere Verbindung mit dem API-Server des Tanzu Kubernetes-Clusters herzustellen, müssen Sie das CA-Zertifikat für den Tanzu Kubernetes-Cluster herunterladen.

Wenn Sie die neueste Ausgabe des vSphere-Plug-In für kubectl verwenden, registriert das Plug-In bei Ihrer ersten Anmeldung beim Tanzu Kubernetes Grid-Cluster das CA-Zertifikat für den Tanzu Kubernetes-Cluster in Ihrer `kubeconfig`-Datei. Dieses Zertifikat wird im geheimen Kubernetes-Schlüssel mit dem Namen *`TANZU-KUBERNETES-CLUSTER-NAME`*`-ca` gespeichert. Das Plug-In verwendet dieses Zertifikat, um die CA-Informationen im Datenspeicher der Zertifizierungsstelle des entsprechenden Clusters aufzufüllen.

Wenn Sie vSphere IaaS control plane aktualisieren, stellen Sie sicher, dass das Update auf die neueste Version des Plug-Ins erfolgt. Weitere Informationen finden Sie unter Aktualisieren des vSphere-Plug-Ins für kubectl in *Wartung der vSphere IaaS-Steuerungsebene*.

Herstellen einer Verbindung mit dem Supervisor als vCenter Single Sign-On-Benutzer

Zur Bereitstellung von vSphere-Pods, Tanzu Kubernetes Grid-Clustern oder VMs verbinden Sie sich mit dem Supervisor mittels vSphere-Plug-In für kubectl und authentifizieren Sie sich mit Ihren vCenter Single Sign-On-Anmeldedaten.

Nach der Anmeldung beim Supervisor generiert das vSphere-Plug-In für kubectl den Kontext für den Supervisor. In Kubernetes enthält ein Konfigurationskontext einen Supervisor, einen vSphere-Namespace und einen Benutzer. Sie können sich den Clusterkontext in der Datei `.kube/config` ansehen. Diese Datei wird gemeinhin als `kubeconfig`-Datei bezeichnet.

Hinweis Wenn Sie über eine bestehende `kubeconfig`-Datei verfügen, wird diese an jeden Supervisor-Kontext angehängt. Das vSphere-Plug-In für kubectl berücksichtigt die KUBECONFIG-Umgebungsvariable, die kubectl selbst verwendet. Auch wenn dies nicht erforderlich ist, kann es hilfreich sein, diese Variable vor der Ausführung von `kubectl vsphere login ...` festzulegen, damit die Informationen in eine neue Datei geschrieben werden (und nicht Ihrer aktuellen `kubeconfig`-Datei hinzugefügt werden).

Voraussetzungen

- Erfragen Sie Ihre vCenter Single Sign-On-Anmeldedaten beim vSphere-Administrator.
- Fragen Sie den vSphere-Administrator nach der IP-Adresse für die Supervisor-Steuerungsebene. Die IP-Adresse der Supervisor-Steuerungsebene ist auf der Benutzeroberfläche jedes vSphere-Namespace unter **Arbeitslastmanagement** im vSphere Client verknüpft.
- Um sich mithilfe eines FQDN anstelle der IP-Adresse der Steuerungsebene anzumelden, rufen Sie während der Aktivierung einen FQDN ab, der für den Supervisor konfiguriert wurde.
- Rufen Sie den Namen des vSphere-Namespace ab, für den Sie Berechtigungen haben.
- Lassen Sie sich bestätigen, dass Sie Berechtigungen des Typs **Bearbeiten** für den vSphere-Namespace haben.
- Herunterladen und Installieren von Kubernetes-CLI-Tools für vSphere.
- Stellen Sie sicher, dass das Zertifikat, das von der Kubernetes-Steuerungsebene bereitgestellt wird, auf Ihrem System als vertrauenswürdig eingestuft wird, indem Sie entweder die signierende Zertifizierungsstelle als vertrauenswürdigen Root installieren oder das Zertifikat direkt als vertrauenswürdigen Root hinzufügen. Weitere Informationen hierzu finden Sie unter Konfigurieren der sicheren Anmeldung für vSphere IaaS control plane-Cluster.

Verfahren

1. Um die Befehlssyntax und die Optionen für die Anmeldung anzuzeigen, führen Sie folgenden Befehl aus:

   ```
   kubectl vsphere login --help
   ```

2. Um eine Verbindung mit dem Supervisor herzustellen, führen Sie den folgenden Befehl aus.

   ```
   kubectl vsphere login --server=<KUBERNETES-CONTROL-PLANE-IP-ADDRESS> --vsphere-username
   <VCENTER-SSO-USER>
   ```

Sie können sich auch mithilfe eines FQDN anmelden:

```
kubectl vsphere login --server <KUBERNETES-CONTROL-PLANE-FQDN --vsphere-username <VCENTER-SSO-USER>
```

Beispiel:

```
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
```

Bei dieser Aktion wird eine Konfigurationsdatei mit dem JSON-Web-Token (JWT) für die Authentifizierung bei der Kubernetes-API erstellt.

3 Geben Sie zur Authentifizierung das Kennwort für den Benutzer ein.

Nachdem Sie eine Verbindung mit dem Supervisor hergestellt haben, werden Ihnen die Konfigurationskontexte angezeigt, auf die zugegriffen werden kann. Beispiel:

```
You have access to the following contexts:
tanzu-ns-1
tkg-cluster-1
tkg-cluster-2
```

4 Führen Sie folgenden `kubectl`-Befehl aus, um Details zu den Konfigurationskontexten anzuzeigen, auf die Sie zugreifen können:

```
kubectl config get-contexts
```

Die CLI zeigt die Details für jeden verfügbaren Kontext an.

5 Verwenden Sie den folgenden Befehl, um zwischen den Kontexten zu wechseln:

```
kubectl config use-context <example-context-name>
```

Nächste Schritte

Herstellen einer Verbindung mit einem Tanzu Kubernetes Grid-Cluster als vCenter Single Sign-On. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit einem TKG-Cluster als vCenter Single Sign-On-Benutzer in *Verwenden des TKG-Dienstes mit der vSphere IaaS-Steuerungsebene*.

Gewähren des Entwicklerzugriffs auf Tanzu Kubernetes-Cluster

Entwickler sind die Zielbenutzer von Kubernetes. Sobald ein Tanzu Kubernetes-Cluster bereitgestellt wurde, können Sie mittels vCenter Single Sign-On-Authentifizierung Entwicklerzugriff darauf gewähren.

Authentifizierung für Entwickler

Ein Clusteradministrator kann anderen Benutzern, z. B. Entwicklern, Clusterzugriff gewähren. Entwickler können Pods für Cluster direkt über ihre Benutzerkonten oder indirekt über Dienstkonten bereitstellen. Weitere Informationen finden Sie unter Gewähren von SSO-Zugriff für Entwickler auf Arbeitslastclustern in *Verwenden des TKG-Dienstes mit der vSphere IaaS-Steuerungsebene*.

- Für die Authentifizierung über Benutzerkonten bieten Tanzu Kubernetes-Cluster Unterstützung für vCenter Single Sign-On-Benutzer und -Gruppen. Der Benutzer oder die Gruppe kann sich lokal in vCenter Server befinden oder von einem unterstützten Verzeichnisserver aus synchronisiert werden.
- Für die Authentifizierung über Dienstkonten können Sie Diensttoken verwenden. Weitere Informationen dazu finden Sie in der Kubernetes-Dokumentation.

Hinzufügen von Entwicklern zu einem Cluster

So gewähren Sie Entwicklern Clusterzugriff:

1 Definieren Sie ein Role- oder ClusterRole-Objekt für den Benutzer bzw. die Gruppe und wenden Sie es auf den Cluster an. Weitere Informationen dazu finden Sie in der Kubernetes-Dokumentation.

2 Erstellen Sie ein RoleBinding- oder ClusterRoleBinding-Objekt für den Benutzer bzw. die Gruppe und wenden Sie es auf den Cluster an. Betrachten Sie das folgende Beispiel.

RoleBinding – Beispiel

Um einem vCenter Single Sign-On-Benutzer oder einer vCenter Single Sign-On-Gruppe Zugriff zu gewähren, muss im RoleBinding-Objekt unter „subjects“ einer der folgenden Werte für den Parameter `name` angegeben sein.

Tabelle 11-1. Unterstützte Felder für Benutzer und Gruppen

Feld	Beschreibung
`sso:`*`USER-NAME@DOMAIN`*	Beispielsweise ein lokaler Benutzername wie `sso:joe@vsphere.local`.
`sso:`*`GROUP-NAME@DOMAIN`*	Beispielsweise ein von einem in vCenter Server integrierten Verzeichnisserver stammender Gruppenname wie `sso:devs@ldap.example.com`.

Im folgenden Beispiel für ein RoleBinding-Objekt wird der lokale vCenter Single Sign-On-Benutzer mit dem Namen „Joe“ an das standardmäßige ClusterRole-Objekt mit dem Namen `edit` gebunden. Diese Rolle ermöglicht Lese-/Schreibzugriff auf die meisten Objekte in einem Namespace. In diesem Fall ist dies der Namespace `default`.

```
kind: RoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: rolebinding-cluster-user-joe
  namespace: default
roleRef:
  kind: ClusterRole
  name: edit                              #Default ClusterRole
  apiGroup: rbac.authorization.k8s.io
subjects:
- kind: User
  name: sso:joe@vsphere.local             #sso:<username>@<domain>
  apiGroup: rbac.authorization.k8s.io
```

Konfigurieren und Verwalten eines Supervisors

12

Als vSphere-Administrator aktivieren Sie einen vSphere-Cluster als Supervisor. Sie haben die Wahl zwischen der Erstellung des Supervisors mit dem vSphere-Netzwerk-Stack oder mit VMware NSX® (NSX) als Netzwerklösung. Ein mit NSX konfigurierter Cluster unterstützt die Ausführung eines vSphere Pods und einesTanzu Kubernetes-Clusters, der über den VMware Tanzu™ Kubernetes Grid™ erstellt wurde. Ein mit dem vSphere-Netzwerk-Stack konfigurierter Supervisor unterstützt ausschließlich Tanzu Kubernetes-Cluster.

Nachdem Sie den Supervisor aktiviert haben, können Sie den vSphere Client zum Verwalten und Überwachen des Clusters verwenden.

Lesen Sie als Nächstes die folgenden Themen:

- Ersetzen des VIP-Zertifikats zur sicheren Verbindung mit dem Supervisor-API-Endpoint
- Integrieren des Tanzu Kubernetes Grid auf dem Supervisor in Tanzu Mission Control
- Festlegen der Standard-CNI für Tanzu Kubernetes Grid-Cluster
- Ändern der Größe der Steuerungsebene eines Supervisors
- Ändern der Einstellungen für den Lastausgleichsdienst auf einem Supervisor, der mit VDS-Netzwerk konfiguriert ist
- Hinzufügen von Arbeitslastnetzwerken zu einem mit vDS-Netzwerk konfigurierten Supervisor
- Ändern der Verwaltungsnetzwerkeinstellungen auf einem Supervisor
- Ändern der Einstellungen für das Arbeitslastnetzwerk auf einem Supervisor, der mit vDS-Netzwerk konfiguriert ist
- Ändern von Einstellungen für das Arbeitslastnetzwerk auf einem Supervisor, der mit NSX konfiguriert ist
- Konfigurieren von HTTP-Proxy-Einstellungen in vSphere IaaS control plane
- Konfigurieren eines externen IDP für die Verwendung mit TKG-Dienstclustern
- Registrieren eines externen IDP bei Supervisor
- Ändern der Speichereinstellungen im Supervisor
- Streamen von Supervisor-Metriken auf einer benutzerdefinierten Beobachtbarkeitsplattform
- Ändern der Liste der DNS-Namen der Supervisor Control Plane

- Weiterleiten von Supervisor-Protokollen an externe Überwachungssysteme

Ersetzen des VIP-Zertifikats zur sicheren Verbindung mit dem Supervisor-API-Endpoint

Als vSphere-Administrator können Sie das Zertifikat für die virtuelle IP-Adresse (VIP) zur sicheren Verbindung mit dem Supervisor-API-Endpoint durch ein Zertifikat ersetzen, das von einer Zertifizierungsstelle signiert wurde, der Ihre Hosts bereits vertrauen. Das Zertifikat authentifiziert die Kubernetes-Steuerungsebene für DevOps-Techniker, sowohl während der Anmeldung als auch bei nachfolgenden Interaktionen mit dem Supervisor.

Voraussetzungen

Überprüfen Sie, ob Sie Zugriff auf eine Zertifizierungsstelle haben, die CSRs signieren kann. Für DevOps-Techniker muss die Zertifizierungsstelle auf ihrem System als vertrauenswürdiger Root installiert sein.

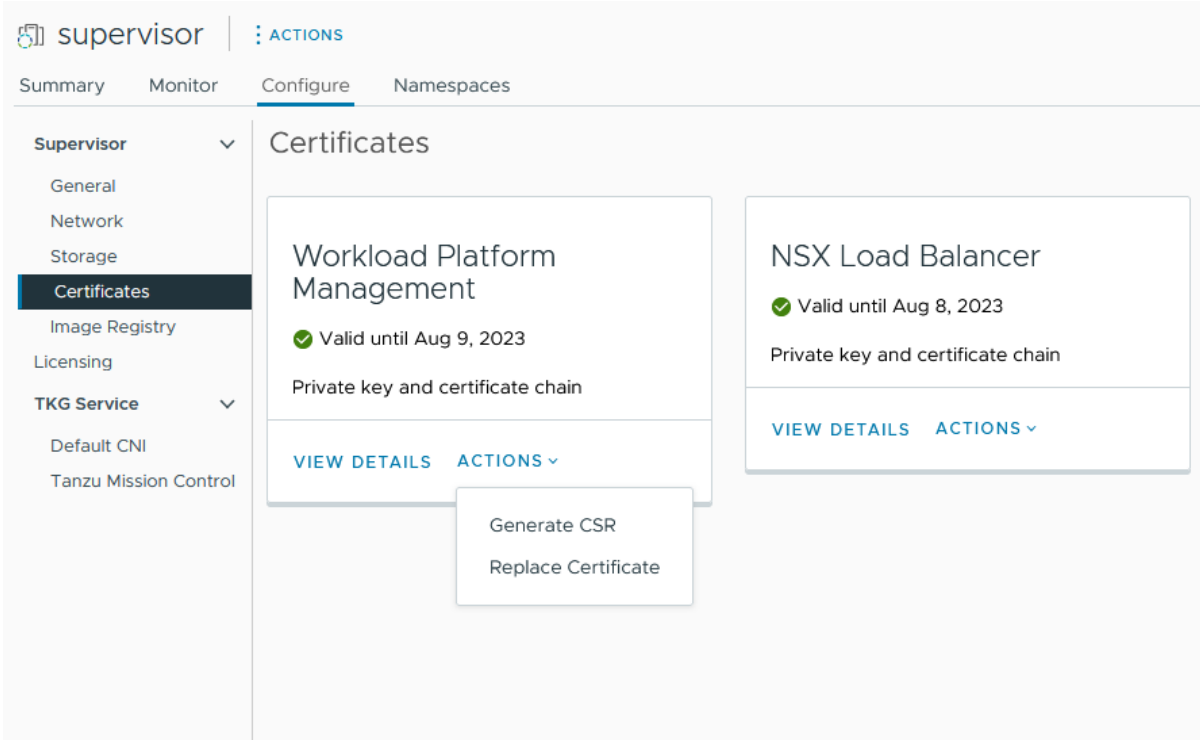
Weitere Informationen zum Supervisor-Zertifikat finden Sie unter Supervisor-CA-Zertifikat.

Verfahren

1. Navigieren Sie im vSphere Client zu **Arbeitslastverwaltung**.
2. Wählen Sie **Supervisoren** und dann den Supervisor aus der Liste aus.
3. Klicken Sie auf **Konfigurieren** und wählen Sie **Zertifikate** aus.

4 Wählen Sie im Bereich **Arbeitslastverwaltungs-Plattform** die Option **Aktionen > CSR generieren** aus.

Abbildung 12-1. Ersetzen des Supervisor-Standardzertifikats



5 Geben Sie die Details für das Zertifikat an.

Hinweis Wenn Sie einen Identitätsanbieterdienst verwenden, müssen Sie auch die gesamte Zertifikatskette einschließen. Die Kette ist jedoch für den standardmäßigen HTTPS-Datenverkehr nicht erforderlich.

6 Nachdem das CSR generiert wurde, klicken Sie auf **Kopieren**.

7 Signieren Sie das Zertifikat mit einer Zertifizierungsstelle.

8 Wählen Sie im Bereich **Arbeitslastverwaltungs-Plattform** die Option **Aktionen > Zertifikat ersetzen** aus.

9 Laden Sie die signierte Zertifikatsdatei hoch und klicken Sie auf **Zertifikat ersetzen**.

10 Validieren Sie das Zertifikat hinsichtlich der IP-Adresse der Kubernetes-Steuerungsebene.

Sie können beispielsweise die Downloadseite Kubernetes-CLI-Tools für vSphere öffnen und durch Nutzung des Browsers bestätigen, dass das Zertifikat erfolgreich ersetzt wurde. Auf einem Linux- oder UNIX-System können Sie auch `echo | openssl s_client -connect https://ip:6443` verwenden.

Integrieren des Tanzu Kubernetes Grid auf dem Supervisor in Tanzu Mission Control

Sie können Tanzu Kubernetes Grid, der auf dem Supervisor ausgeführt wird, in Tanzu Mission Control integrieren. Dadurch können Sie Tanzu Kubernetes-Cluster mithilfe von Tanzu Mission Control bereitstellen und verwalten.

Weitere Informationen zu Tanzu Mission Control finden Sie unter Verwalten des Lebenszyklus von Tanzu Kubernetes-Clustern. Eine Vorführung der Integration sehen Sie im Video Tanzu Mission Control mit Integration in den Tanzu Kubernetes Grid Service.

Anzeigen des Tanzu Mission Control-Namespace im Supervisor

vSphere IaaS control plane v7.0.1 U1 und höher wird mit einem vSphere-Namespace für Tanzu Mission Control geliefert. Dieser Namespace existiert auf dem Supervisor, in dem Sie den Tanzu Mission Control-Agent installieren. Sobald der Agent installiert ist, können Sie Tanzu Kubernetes Grid-Cluster mithilfe der Tanzu Mission Control-Webschnittstelle bereitstellen und verwalten.

1. Authentifizieren Sie sich mithilfe des vSphere-Plug-In für kubectl beim Supervisor. Weitere Informationen hierzu finden Sie unter Herstellen einer Verbindung mit dem Supervisor als vCenter Single Sign-On-Benutzer.
2. Wechseln Sie in den Supervisor-Kontext, z. B.:

   ```
   kubectl config use-context 10.199.95.59
   ```

3. Führen Sie den folgenden Befehl aus, um die Namespaces aufzulisten.

   ```
   kubectl get ns
   ```

4. Der für Tanzu Mission Control bereitgestellte vSphere-Namespace wird als `svc-tmc-cXX` identifiziert (wobei xx eine Ziffer ist).
5. Installieren Sie den Tanzu Mission Control-Agenten in diesem Namespace. Weitere Informationen hierzu finden Sie unter Installieren des Tanzu Mission Control-Agenten im Supervisor.

Installieren des Tanzu Mission Control-Agenten im Supervisor

Um den Tanzu Kubernetes Grid in Tanzu Mission Control zu integrieren, installieren Sie den Agenten im Supervisor.

Hinweis Für das folgende Verfahren benötigen Sie mindestens vSphere 7.0 U3 mit der Supervisor-Version 1.21.0 oder höher.

1. Registrieren Sie mithilfe der Tanzu Mission Control-Webschnittstelle den Supervisor bei Tanzu Mission Control. Siehe Registrieren eines Verwaltungsclusters bei Tanzu Mission Control.
2. Rufen Sie über die Tanzu Mission Control-Webschnittstelle die Registrierungs-URL ab, indem Sie zu **Verwaltung > Verwaltungscluster** navigieren.

3 Öffnen Sie einen Firewall-Port in Ihrer vSphere IaaS control plane-Umgebung für den Port, der für Tanzu Mission Control erforderlich ist (normalerweise `443`). Weitere Informationen hierzu finden Sie unter Von den Cluster-Agent-Erweiterungen hergestellte ausgehende Verbindungen.

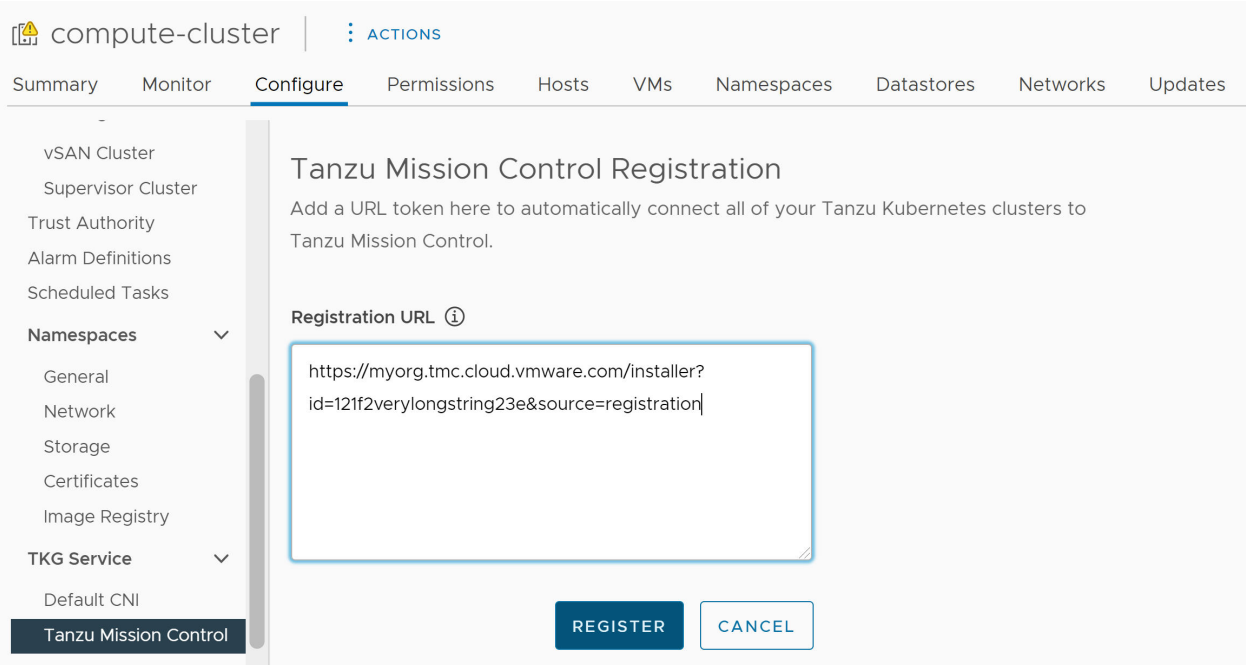
4 Melden Sie sich mit dem vSphere Client bei Ihrer vSphere IaaS control plane-Umgebung an.

5 Wählen Sie **Arbeitslastverwaltung** und dann den Supervisor aus.

6 Wählen Sie **Konfigurieren** und dann **TKG-Dienst > Tanzu Mission Control** aus.

7 Geben Sie die Registrierungs-URL in das Feld **Registrierungs-URL** ein.

8 Klicken Sie auf **Registrieren**.



Deinstallieren des Tanzu Mission Control-Agenten

Informationen zum Deinstallieren des Tanzu Mission Control-Agents über den Supervisor finden Sie unter Manuelles Entfernen des Cluster-Agents aus einem Supervisor-Cluster in vSphere IaaS control plane.

Festlegen der Standard-CNI für Tanzu Kubernetes Grid-Cluster

Als vSphere-Administrator können Sie die standardmäßige Container-Netzwerkschnittstelle (Container Network Interface, CNI) für Tanzu Kubernetes-Cluster festlegen.

Standard-CNI

Tanzu Kubernetes Grid unterstützt zwei CNI-Optionen für Tanzu Kubernetes Grid-Cluster: Antrea und Calico.

Die vom System festgelegte Standard-CNI ist Antrea. Weitere Informationen zur CNI-Standardeinstellung finden Sie unter *Verwenden des TKG-Dienstes mit der vSphere IaaS-Steuerungsebene*.

Sie können die Standard-CNI mit dem vSphere Client ändern. Gehen Sie wie folgt vor, um die Standard-CNI festzulegen.

Vorsicht Das Ändern der Standard-CNI ist ein globaler Vorgang. Der neu festgelegte Standard gilt für alle neuen Cluster, die vom Dienst erstellt wurden. Vorhandene Cluster bleiben unverändert.

1 Melden Sie sich mit dem vSphere Client bei Ihrer vSphere IaaS control plane-Umgebung an.

2 Wählen Sie **Arbeitslastverwaltung** und anschließend **Supervisoren** aus.

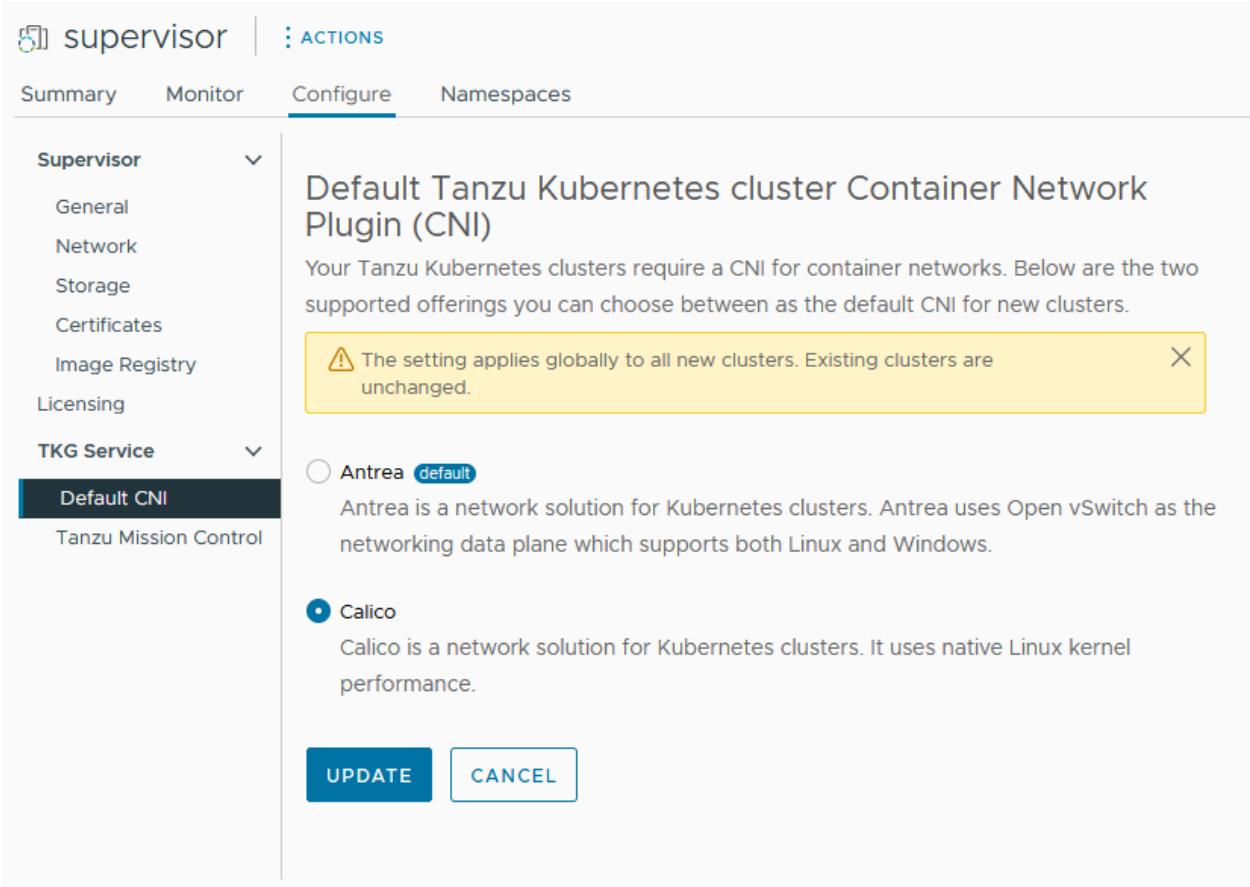
3 Wählen Sie die Supervisor-Instanz aus der Liste aus.

4 Wählen Sie **Konfigurieren** und anschließend **TKG-Dienst > Standard-CNI** aus.

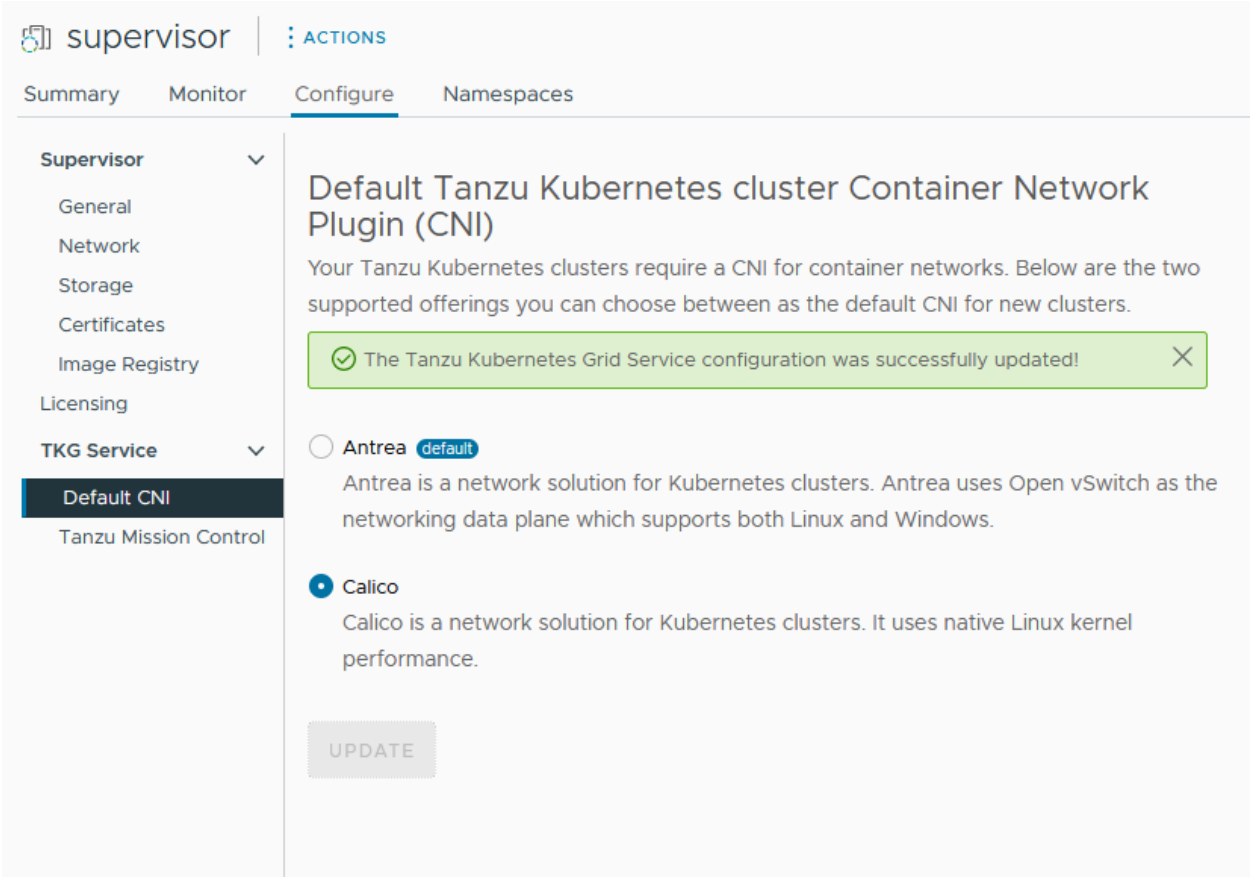
5 Wählen Sie die Standard-CNI für neue Cluster aus.

6 Klicken Sie auf **Aktualisieren**.

Die folgende Abbildung zeigt die Auswahl der Standard-CNI.



Die folgende Abbildung zeigt die Änderung der CNI-Auswahl von Antrea zu Calico.



Ändern der Größe der Steuerungsebene eines Supervisors

Unter diesem Thema wird erläutert, wie Sie die Größe der Kubernetes-Steuerungsebenen-VMs in einem Supervisor in Ihrer vSphere IaaS control plane-Umgebung ändern.

Voraussetzungen

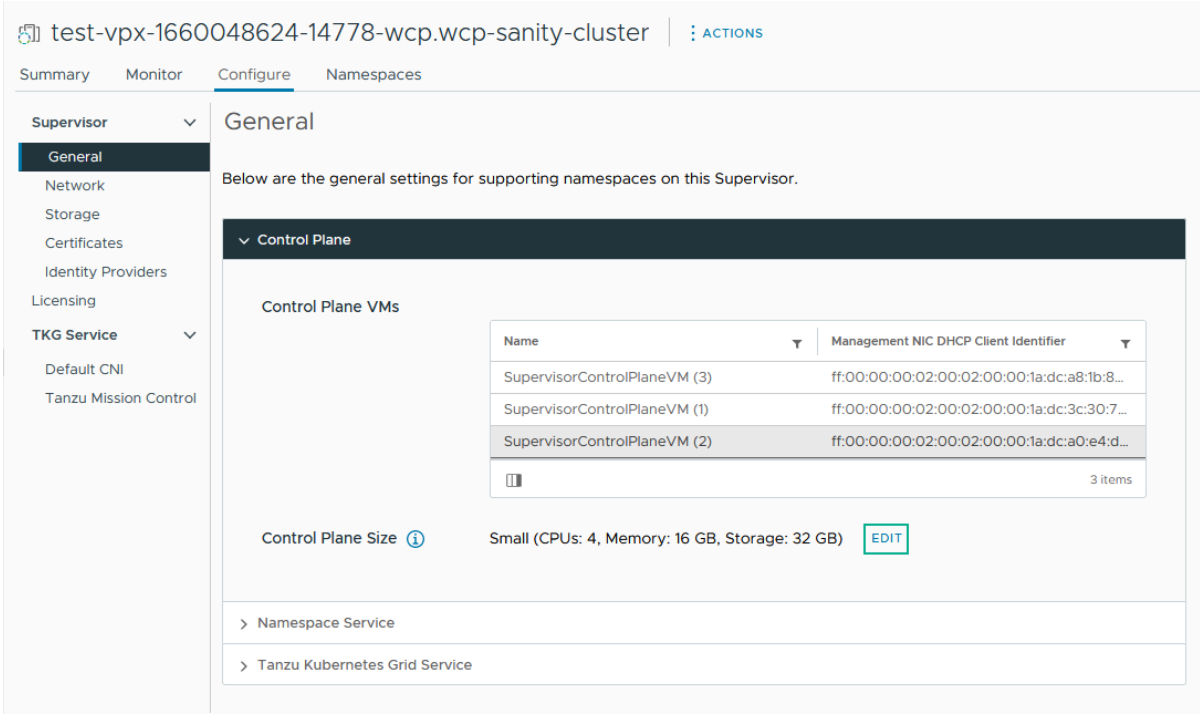
- Stellen Sie sicher, dass Sie über das Recht **Clusterweite Konfiguration ändern** auf dem Cluster verfügen.

Verfahren

1. Wechseln Sie im vSphere Client zur **Arbeitslastverwaltung**.
2. Wählen Sie unter **Supervisoren** die Option Supervisor aus.
3. Wählen Sie **Konfigurieren** und dann **Allgemein** aus.

4 **Größe der Steuerungsebene** erweitern.

Abbildung 12-2. Einstellungen der Supervisor-Steuerungsebene



5 Klicken Sie auf **Bearbeiten** und wählen Sie im Dropdown-Menü die neue Größe der Steuerungsebene aus.

Option	Bezeichnung
Sehr klein	2 CPUs, 8 GB Arbeitsspeicher, 32 GB Speicher
Klein	4 CPUs, 16 GB Arbeitsspeicher, 32 GB Speicher
Mittel	8 CPUs, 16 GB Arbeitsspeicher, 32 GB Speicher
Groß	16 CPUs, 32 GB Arbeitsspeicher, 32 GB Speicher

Hinweis Sobald Sie eine Größe der Steuerungsebene ausgewählt haben, können Sie nicht mehr herunterskalieren. Wenn Sie beispielsweise die Option Sehr klein während der Aktivierung von Supervisor bereits festgelegt haben, können Sie sie nur vertikal hochskalieren.

6 Klicken Sie auf **Speichern**.

Sie können nur die Größe der Steuerungsebene vertikal hochskalieren.

Ändern der Einstellungen für den Lastausgleichsdienst auf einem Supervisor, der mit VDS-Netzwerk konfiguriert ist

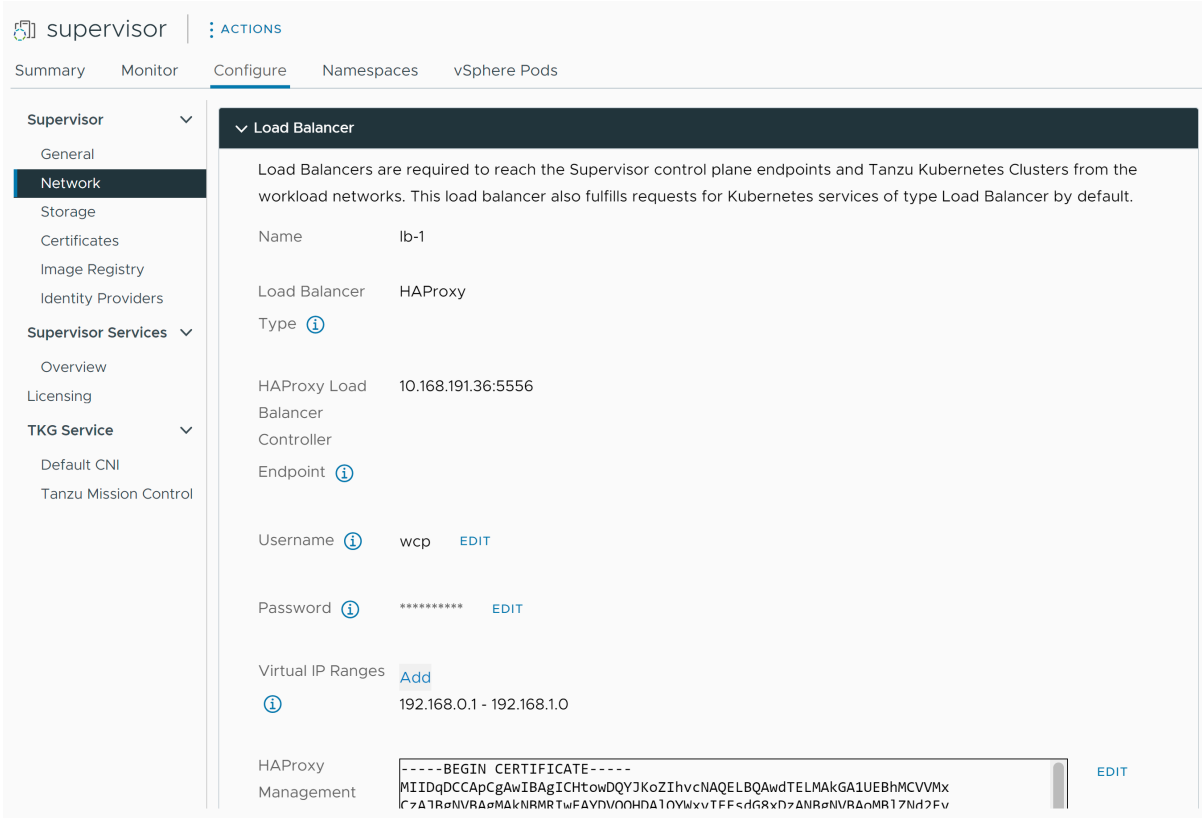
Erfahren Sie, wie Sie die Einstellungen des Lastausgleichsdiensts ändern können, der mit dem VDS-Netzwerk-Stack auf Ihrem Supervisor konfiguriert ist. Sie können Einstellungen wie Benutzername und Kennwort ändern, neue IP-Bereiche hinzufügen und das mit dem Lastausgleichsdienst verwendete Zertifikat aktualisieren.

Voraussetzungen

- Stellen Sie sicher, dass Sie über das Recht **Clusterweite Konfiguration ändern** auf dem Cluster verfügen.

Verfahren

1. Wechseln Sie im vSphere Client zur **Arbeitslastverwaltung**.
2. Wählen Sie unter **Supervisoren** den Supervisor aus und wählen Sie **Konfigurieren**.
3. Wählen Sie **Netzwerk** aus und erweitern Sie **Arbeitslastennetzwerk**.



Option	Bezeichnung
Einstellung	Beschreibung
Benutzername	Bearbeiten Sie den Benutzernamen, den der Supervisor zur Authentifizierung am Endpunkt des Lastausgleichsdiensts verwendet.

Option	Bezeichnung
Kennwort	Ändern Sie das Kennwort, das der Supervisor zur Authentifizierung am Endpunkt des Lastausgleichsdiensts verwendet.
Bereiche für virtuelle IPs	Fügen Sie IP-Bereiche hinzu, die eine Teilmenge des virtuellen IP-CIDR-Bereichs sind, den Sie ursprünglich mit dem Lastausgleichsdienst konfiguriert haben. **Hinweis** Sie können nur neue IP-Bereiche hinzufügen. Sie können vorhandene IP-Bereiche nicht entfernen oder ändern.
TLS-Zertifikat	Ändern Sie das TLS-Zertifikat, das verwendet wird, um eine sichere Verbindung zwischen dem Supervisor und dem Lastausgleichsdienst sicherzustellen.

Hinzufügen von Arbeitslastnetzwerken zu einem mit vDS-Netzwerk konfigurierten Supervisor

Für einen mit dem vSphere-Netzwerkstack konfigurierten Supervisor können Sie Ebene-2-Isolierung für Ihre Kubernetes-Arbeitslasten bereitstellen, indem Sie Arbeitslastnetzwerke erstellen und sie Namespaces zuweisen. Arbeitslastnetzwerke ermöglichen die Konnektivität mit Tanzu Kubernetes Grid-Clustern im Namespace und werden von verteilten Portgruppen auf dem Switch gestützt, der mit den Hosts im Supervisor verbunden ist.

Weitere Informationen zu den Topologien, die Sie für die Supervisor implementieren können, finden Sie unter Topologie für Supervisor mit vSphere-Netzwerk und NSX Advanced Load Balancer oder Topologien für die Bereitstellung des HAProxy-Lastausgleichsdiensts in *Konzepte und Planung der vSphere IaaS-Steuerungsebene*.

Hinweis Wenn Sie den Supervisor mit einem DHCP-Server konfiguriert haben, der Netzwerkeinstellungen für Arbeitslastnetzwerke bereitstellt, können Sie nach der Konfiguration des Supervisors keine neuen Arbeitslastnetzwerke erstellen.

Voraussetzungen

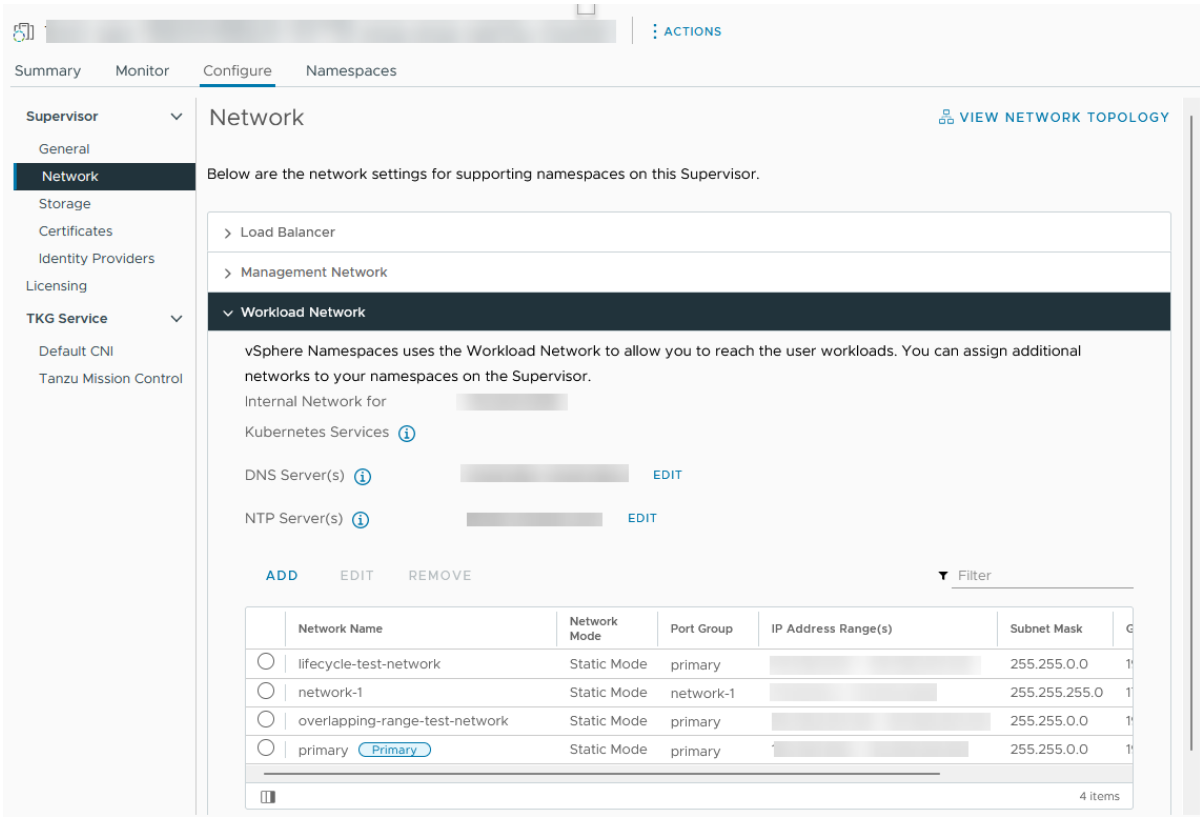
- Erstellen Sie eine verteilte Portgruppe, die das Arbeitslastnetzwerk unterstützt.
- Überprüfen Sie, ob der IP-Bereich, den Sie dem Arbeitslastnetzwerk zuweisen, innerhalb aller in Ihrer Umgebung verfügbaren Supervisor eindeutig ist.

Verfahren

1. Wechseln Sie im vSphere Client zur **Arbeitslastverwaltung**.
2. Wählen Sie unter **Supervisoren** die Option Supervisor aus.

3 Wählen Sie **Konfigurieren** und dann **Netzwerk** aus.

Abbildung 12-3. Hinzufügen eines Supervisor-Arbeitslastnetzwerks



4 Wählen Sie **Arbeitslastnetzwerk** aus und klicken Sie auf **Hinzufügen**.

Option	Bezeichnung
Portgruppe	Wählen Sie die verteilte Portgruppe aus, die diesem Arbeitslastnetzwerk zugeordnet werden soll. Der für das Supervisor-Netzwerk konfigurierte vSphere Distributed Switch (vDS) enthält die Portgruppen, aus denen Sie auswählen können.
Netzwerkname	Der Netzwerkname, der das Arbeitslastnetzwerk bezeichnet, wenn es Namespaces zugewiesen wird. Dieser Wert wird automatisch mit dem Namen der ausgewählten Portgruppe aufgefüllt. Sie können ihn jedoch nach Bedarf ändern.
IP-Adressbereiche	Geben Sie einen IP-Bereich für die Zuteilung von Tanzu Kubernetes Grid-Clusterknoten ein. Der IP-Bereich muss sich in dem von der Subnetzmaske angegebenen Subnetz befinden. **Hinweis** Sie müssen für jedes Arbeitslastnetzwerk eindeutige IP-Adressbereiche verwenden. Konfigurieren Sie nicht denselben IP-Adressbereich für mehrere Netzwerke.

Option	Bezeichnung
Subnetzmaske	Geben Sie die IP-Adresse der Subnetzmaske für das Netzwerk in der Portgruppe ein.
Gateway	Geben Sie das Standard-Gateway für das Netzwerk in der Portgruppe ein. Das Gateway muss sich in dem von der Subnetzmaske angegebenen Subnetz befinden. **Hinweis** Verwenden Sie nicht das Gateway, das dem HAProxy-Lastausgleichsdienst zugewiesen ist.

5 Klicken Sie auf **Hinzufügen**.

Nächste Schritte

Weisen Sie das neu erstellte Arbeitslastnetzwerk vSphere-Namespaces zu.

Ändern der Verwaltungsnetzwerkeinstellungen auf einem Supervisor

Unter diesem Thema wird erläutert, wie Sie die DNS- und NTP-Einstellungen im Supervisor-Verwaltungsnetzwerk in Ihrer vSphere IaaS control plane-Umgebung aktualisieren.

Voraussetzungen

- Stellen Sie sicher, dass Sie über das Recht **Clusterweite Konfiguration ändern** auf dem Cluster verfügen.

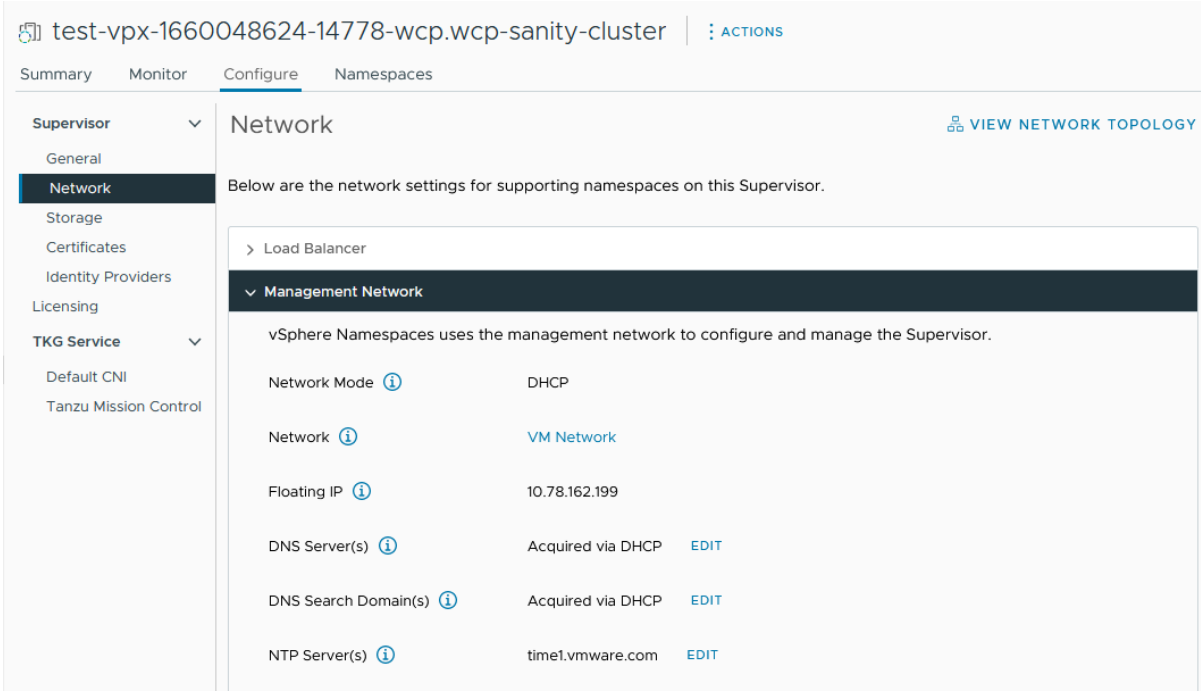
Verfahren

1 Wählen Sie im vSphere Client **Arbeitslastverwaltung** aus.

2 Wählen Sie unter **Supervisoren** den Supervisor aus und wählen Sie **Konfigurieren**.

3 Wählen Sie **Netzwerk** aus und erweitern Sie **Verwaltungsnetzwerk**.

Abbildung 12-4. Aktualisieren der Supervisor-Verwaltungsnetzwerkeinstellungen



4 Bearbeiten Sie die DNS- und NTP-Einstellungen.

Option	Bezeichnung
DNS-Server	Geben Sie die Adressen der DNS-Server ein, die Sie in Ihrer Umgebung verwenden. Wenn das vCenter Server-System mit einem FQDN registriert ist, müssen Sie die IP-Adressen der DNS-Server eingeben, die Sie mit der vSphere-Umgebung verwenden, damit der FQDN im Supervisor aufgelöst werden kann.
DNS-Suchdomäne(n)	Geben Sie Domänennamen ein, die von DNS innerhalb der Kubernetes Control Plane-Knoten durchsucht werden, z. B. `corp.local`, damit der DNS-Server sie auflösen kann.
NTP-Server	Geben Sie die Adressen der NTP-Server ein, die Sie in Ihrer Umgebung verwenden (sofern vorhanden).

Ändern der Einstellungen für das Arbeitslastnetzwerk auf einem Supervisor, der mit vDS-Netzwerk konfiguriert ist

Unter diesem Thema wird erläutert, wie Sie die NTP- und DNS-Servereinstellungen für die Arbeitslastnetzwerke eines Supervisors, der mit dem vDS-Netzwerk-Stack konfiguriert ist, ändern. Bei den DNS-Servern, die Sie für Arbeitslastnetzwerke konfigurieren, handelt es sich um externe DNS-Server, die für Kubernetes-Arbeitslasten verfügbar gemacht werden, und sie lösen Standarddomänennamen auf, die außerhalb des Supervisors gehostet werden.

Voraussetzungen

- Stellen Sie sicher, dass Sie über das Recht **Clusterweite Konfiguration ändern** auf dem Cluster verfügen.

Verfahren

1 Wählen Sie im vSphere Client **Arbeitslastverwaltung** aus.

2 Wählen Sie unter **Supervisoren** den Supervisor aus und wählen Sie **Konfigurieren**.

3 Wählen Sie **Netzwerk** aus und erweitern Sie **Arbeitslastennetzwerk**.

Hinweis Sie können kein Arbeitslastnetzwerk entfernen, das bereits einem vSphere-Namespace zugewiesen ist. Wenn Sie ein Arbeitslastnetzwerk entfernen müssen, müssen Sie alle an dieses Netzwerk angehängten vSphere-Namespaces löschen. Außerdem können Sie das primäre Arbeitslastnetzwerk nicht bearbeiten oder entfernen.

4 Bearbeiten Sie die DNS-Servereinstellungen.

Geben Sie die Adressen der DNS-Server ein, die die Domänennamen der vSphere-Verwaltungskomponenten auflösen können, z. B. vCenter Server.

Beispiel: `10.142.7.1`.

Wenn Sie die IP-Adresse des DNS-Servers eingeben, wird jeder Steuerungsebenen-VM eine statische Route hinzugefügt. Dadurch wird angegeben, dass der Datenverkehr zu den DNS-Servern über das Arbeitslastnetzwerk fließt.

Wenn die von Ihnen angegebenen DNS-Server vom Verwaltungsnetzwerk und vom Arbeitslastnetzwerk gemeinsam genutzt werden, werden die DNS-Lookups auf den Steuerungsebenen-VMs nach der ersten Einrichtung über das Arbeitslastnetzwerk geleitet.

5 Bearbeiten Sie bei Bedarf die NTP-Einstellungen.

6 Bearbeiten Sie die Arbeitslastnetzwerk-Einstellungen.

a Wählen Sie ein Arbeitslastnetzwerk aus und klicken Sie auf **Bearbeiten**.

b Klicken Sie auf **Hinzufügen** neben **IP-Adressbereich(e)**, um neue IP-Bereiche hinzuzufügen, die mit Arbeitslasten in diesem Netzwerk verwendet werden sollen.

Die IP-Bereiche müssen sich in dem von der Subnetzmaske angegebenen Subnetz befinden.

Hinweis Die IP-Bereiche, die Sie hinzufügen, dürfen sich nicht mit den virtuellen IPs der Frontend-Netzwerkkonfiguration des Lastausgleichsdiensts überschneiden.

Ändern von Einstellungen für das Arbeitslastnetzwerk auf einem Supervisor, der mit NSX konfiguriert ist

In diesem Thema wird erläutert, wie Sie die Netzwerkeinstellungen für DNS-Server, Namespace-Netzwerke, Ingress und Egress eines Supervisors, der für NSX als Netzwerk-Stack konfiguriert ist, ändern.

Voraussetzungen

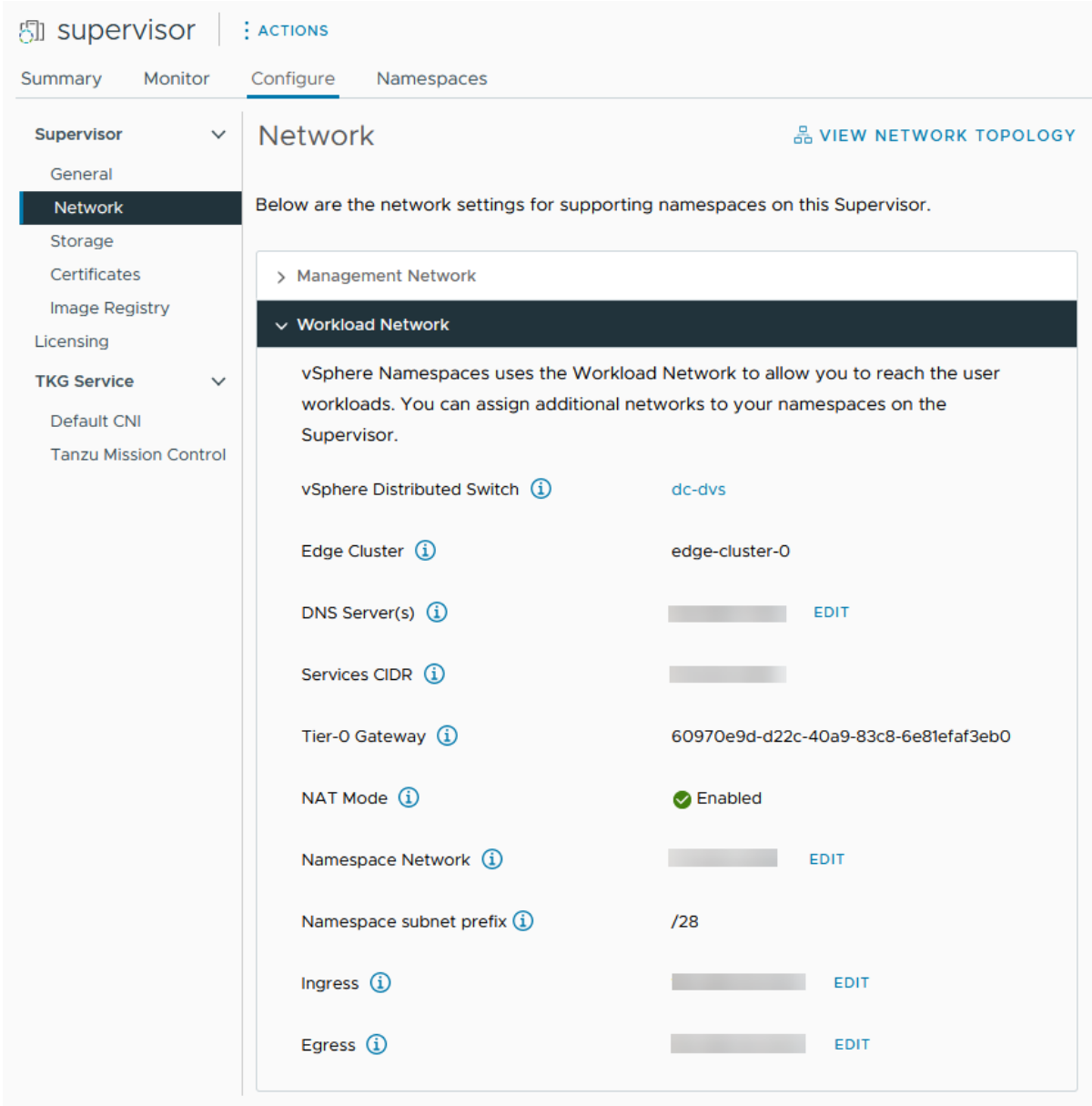
- Stellen Sie sicher, dass Sie über das Recht **Clusterweite Konfiguration ändern** auf dem Cluster verfügen.

Verfahren

1. Navigieren Sie im vSphere Client zu **Arbeitslastverwaltung**.
2. Wählen Sie unter **Supervisoren** den Supervisor aus und wählen Sie **Konfigurieren**.

3 Wählen Sie **Netzwerk** aus und erweitern Sie **Arbeitslastennetzwerk**.

Abbildung 12-5. Aktualisieren von Supervisor-Arbeitslastnetzwerkeinstellungen



4 Ändern Sie bei Bedarf die Netzwerkeinstellungen.

Option	Bezeichnung
DNS-Server	Geben Sie die Adressen der DNS-Server ein, die die Domänennamen der vSphere-Verwaltungskomponenten auflösen können, z. B. vCenter Server. Beispiel: `10.142.7.1`. Wenn Sie die IP-Adresse des DNS-Servers eingeben, wird jeder Steuerungsebenen-VM eine statische Route hinzugefügt. Dadurch wird angegeben, dass der Datenverkehr zu den DNS-Servern über das Arbeitslastnetzwerk fließt. Wenn die von Ihnen angegebenen DNS-Server vom Verwaltungsnetzwerk und vom Arbeitslastnetzwerk gemeinsam genutzt werden, werden die DNS-Lookups auf den Steuerungsebenen-VMs nach der ersten Einrichtung über das Arbeitslastnetzwerk geleitet.
Namespace-Netzwerk	Geben Sie eine CIDR-Anmerkung ein, um den IP-Bereich für Kubernetes-Arbeitslasten zu ändern, die an die Namespace-Segmente von Supervisor angehängt sind. Wenn der NAT-Modus nicht konfiguriert ist, muss dieser IP-CIDR-Bereich eine routingfähige IP-Adresse sein.
Ingress	Geben Sie eine CIDR-Anmerkung zum Ändern des Ingress-IP-Bereichs für die Kubernetes-Dienste ein. Dieser Bereich wird für Dienste vom Typ „Load Balancer“ und „Ingress“ verwendet. Für Tanzu Kubernetes Grid-Cluster ruft die Veröffentlichung von Diensten über den ServiceType-Lastausgleichsdienst auch die IP-Adressen aus diesem IP-CIDR-Block ab. **Hinweis** Sie können CIDRs ausschließlich zu Ingress- und Arbeitslastnetzwerkfeldern hinzufügen. Es ist nicht möglich, vorhandene CIDRs zu bearbeiten oder zu entfernen.
Egress	Geben Sie eine CIDR-Anmerkung für die Zuteilung von IP-Adressen für SNAT (Source Network Address Translation) für den Datenverkehr ein, der den Supervisor verlässt, um auf externe Dienste zuzugreifen. Für jeden Namespace im Supervisor wird nur eine Egress-IP-Adresse zugewiesen. Bei der Egress-IP handelt es sich um die IP-Adresse, die die vSphere-Pods im jeweiligen Namespace verwenden, um außerhalb von NSX zu kommunizieren.

Konfigurieren von HTTP-Proxy-Einstellungen in vSphere IaaS control plane

Informieren Sie sich über die Konfiguration der HTTP-Proxy-Einstellungen für Supervisor- und TKG-Cluster und den Workflow zum Konfigurieren eines Proxys, wenn Sie Supervisor- und TKG-Cluster bei Tanzu Mission Control registrieren.

Sie können einen Proxy für den Supervisor über vSphere Client, die Cluster-Verwaltungs-API oder DCLI-Befehle konfigurieren. Sie können einen Proxy verwenden, wenn Sie Container-Datenverkehr oder Image-Abrufe von externen Netzwerken zu Supervisor ausführen müssen. Für lokale Supervisoren, die Sie als Verwaltungscluster in Tanzu Mission Control registrieren, nutzen Sie einen HTTP-Proxy für das Abrufen von Images und den Container-Datenverkehr.

Konfigurieren der Proxy-Einstellungen in neu erstellten vSphere 7.0 Update 3 und höher Supervisoren

Für neu erstellte Supervisoren in einer vSphere 7.0 Update 3 und höheren Umgebung werden die HTTP-Proxy-Einstellungen von vCenter Server übernommen. Unabhängig davon, ob Sie Supervisoren vor oder nach der Konfiguration der HTTP-Proxy-Einstellungen auf vCenter Server erstellen, werden die Einstellungen von den Clustern übernommen.

Unter Konfigurieren der DNS-, IP-Adress- und Proxy-Einstellungen finden Sie Informationen zum Konfigurieren der HTTP-Proxy-Einstellungen auf vCenter Server.

Sie können die übernommene HTTP-Proxy-Konfiguration auch auf einzelnen Supervisoren über vSphere Client, die Clusterverwaltungs-API oder DCLI überschreiben.

Da die Übernahme der vCenter Server-Proxy-Einstellungen als Standardkonfiguration für neu erstellte vSphere 7.0.3-Supervisoren dient, können Sie auch die Clusterverwaltungs-API oder DCLI verwenden, um keine HTTP-Proxy-Einstellungen für den Fall zu übernehmen, dass die Supervisoren keinen Proxy benötigen, während dies bei vCenter Server jedoch weiterhin erforderlich ist.

Konfigurieren der Proxy-Einstellungen auf Supervisoren, die auf vSphere 7.0 Update 3 und höher aktualisiert wurden

Nach der Aktualisierung der Supervisoren auf vSphere 7.0 Update 3 und höher werden die HTTP-Proxy-Einstellungen von vCenter Server nicht automatisch übernommen. In diesem Fall konfigurieren Sie die Proxy-Einstellungen für Supervisoren mithilfe von vSphere Client, der `vcenter/namespace-management/clusters`-API oder der DCLI-Befehlszeile.

Konfigurieren des HTTP-Proxys für TKG-Cluster in vSphere IaaS control plane

Verwenden Sie eine der folgenden Methoden, um einen Proxy für Ihre Tanzu Kubernetes-Cluster in vSphere IaaS control plane zu konfigurieren:

- Konfigurieren von Proxy-Einstellungen für einzelne TKG-Cluster. Weitere Informationen finden Sie unter Konfigurationsparameter für die Bereitstellung von Tanzu Kubernetes-Clustern mit der Tanzu Kubernetes Grid-Dienst-v1alpha2-API. Ein Beispiel für die Konfiguration mit YAML finden Sie unter Beispiel-YAML für die Bereitstellung eines benutzerdefinierten Tanzu Kubernetes-Clusters mit der Tanzu Kubernetes Grid-Dienst-v1alpha2-API.
- Erstellen Sie eine globale Proxy-Konfiguration, die auf alle TKG-Cluster angewendet wird. Weitere Informationen finden Sie unter Konfigurationsparameter für die Tanzu Kubernetes Grid-Dienst-v1alpha2-API.

Hinweis Wenn Sie Tanzu Mission Control zum Verwalten Ihrer TKG-Cluster verwenden, brauchen Sie die Proxy-Einstellungen nicht über die YAML-Clusterdatei in vSphere IaaS control plane zu konfigurieren. Sie können Proxy-Einstellungen konfigurieren, wenn Sie die TKG-Cluster als Arbeitslast-Cluster zu Tanzu Mission Control hinzufügen.

Konfigurieren der HTTP-Proxy-Einstellung auf dem Supervisor mithilfe von vSphere Client

Erfahren Sie, wie Sie HTTP-Proxy-Einstellungen für den Supervisor mit vSphere Client konfigurieren können. Sie können die von vCenter Server übernommenen Proxy-Einstellungen auf einzelnen Supervisoren überschreiben oder keine Proxy-Einstellungen verwenden.

Voraussetzungen

- Stellen Sie sicher, dass Sie über das Recht **Clusterweite Konfiguration ändern** auf dem Cluster verfügen.

Verfahren

1. Navigieren Sie im vSphere Client zu **Arbeitslastverwaltung**.
2. Wählen Sie unter **Supervisoren** den Supervisor aus und wählen Sie **Konfigurieren**.
3. Wählen Sie **Netzwerk** aus, erweitern Sie **Proxy-Konfiguration** und klicken Sie auf **Bearbeiten**.
4. Wählen Sie „Proxy-Einstellungen auf Supervisor konfigurieren“ aus und geben Sie die Proxy-Einstellungen ein.

Option	Beschreibung
TLS-Zertifikat	Das TLS-Root-CA-Paket des Proxys, das zur Verifizierung der Proxy-Zertifikate verwendet wird. Geben Sie das Paket als Klartext ein.
Vom Proxy ausgeschlossene Hosts und IP-Adressen	Eine kommagetrennte Liste mit IPv4-Adressen, FQDNs oder Domänennamen, die den Proxyserver nicht benötigen und auf die direkt zugegriffen werden kann.
HTTPS-Konfiguration	HTTPS-Einstellungen wie URL, Port, Benutzername und Kennwort.
HTTP-Konfiguration	HTTP-Einstellungen wie URL, Port, Benutzername und Kennwort.

5. Klicken Sie auf **OK**.

Ergebnisse

Die Proxy-Einstellungen, die Sie auf diesem Supervisor konfiguriert haben, überschreiben die von vCenter Server übernommenen Einstellungen.

Verwenden der Clusterverwaltungs-API und DCLI zum Konfigurieren eines HTTP-Proxy auf Supervisoren

Sie können die Supervisor-Proxy-Einstellungen über die `vcenter/namespace-management/clusters`-API oder DCLI konfigurieren.

Die API stellt drei Optionen für die Proxy-Konfiguration auf dem Supervisor bereit:

API-Einstellung	Neu erstellte vSphere 7.0.3 und höher Supervisoren	Supervisoren wurde auf vSphere 7.0.3 und höher aktualisiert
VC_INHERITED	Hierbei handelt es sich um die Standardeinstellung für die neuen Supervisoren. Sie brauchen die API nicht zum Konfigurieren der Proxy-Einstellungen für Supervisoren zu verwenden. Sie können Proxy-Einstellungen auf vCenter Server einfach über die Verwaltungsschnittstelle konfigurieren.	Verwenden Sie diese Einstellung zur Übertragung der HTTP-Proxy-Konfiguration auf Supervisoren, die auf vSphere 7.0.3 und höher aktualisiert wurden.
CLUSTER_CONFIGURED	Verwenden Sie diese Einstellung, um die aus vCenter Server übernommene HTTP-Proxy-Konfiguration in einem der folgenden Fälle außer Kraft zu setzen: ■ Ein Supervisor befindet sich in einem anderen Subnetz als vCenter Server, und ein anderer Proxy-Server ist erforderlich. ■ Der Proxy-Server verwendet benutzerdefinierte CA-Pakete.	Verwenden Sie diese Einstellung, um den HTTP-Proxy für einzelne Supervisoren zu konfigurieren, die in einem der folgenden Fälle auf vSphere 7.0.3 und höher aktualisiert wurden: ■ Sie können den vCenter Server-Proxy nicht verwenden, da sich der Supervisor in einem anderen Subnetz als vCenter Server befindet und ein anderer Proxy-Server erforderlich ist. ■ Der Proxy-Server verwendet benutzerdefinierte CA-Pakete.
NONE	Verwenden Sie diese Einstellung, wenn der Supervisor über eine direkte Verbindung zum Internet verfügt und vCenter Server einen Proxy benötigt. Mit der Einstellung KEINE wird verhindert, dass die Proxy-Einstellungen von vCenter Server von Supervisoren übernommen werden.	

Um einen HTTP-Proxy auf einen Supervisor festzulegen oder die vorhandenen Einstellungen zu ändern, verwenden Sie die folgenden Befehle in einer SSH-Sitzung mit vCenter Server:

```
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
```

Sie müssen lediglich `domain_c<number>` aus der vollständigen Cluster-ID übergeben. Verwenden Sie beispielsweise `domain-c50` aus der folgenden Cluster-ID: `ClusterComputeResource:domain-c50:5bbb510f-759f-4e43-96bd-97fd703b4edb`.

Wenn Sie die Einstellung `VC_INHERITED` oder `NONE` verwenden, lassen Sie `"http_proxy_config:<proxy_url>"` im Befehl aus.

Zur Verwendung eines benutzerdefinierten CA-Pakets fügen Sie `"tlsRootCaBundle": "<TLS_certificate>` zum Befehl hinzu, indem Sie das TSL-CA-Zertifikat im Klartext angeben.

Für HTTPS-Proxy-Einstellungen verwenden Sie den folgenden Befehl:

```
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
```

Verwenden der DCLI zum Konfigurieren von HTTP-Proxy-Einstellungen auf Supervisoren

Sie können den folgenden DCLI-Befehl verwenden, um die HTTP-Proxy-Einstellungen für Supervisoren mithilfe der Einstellung `CLUSTER_CONFIGURED` zu konfigurieren.

```
<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
```

Konfigurieren der HTTP-Proxy-Einstellungen auf den Supervisor- und TKG-Clustern für Tanzu Mission Control

Führen Sie zum Konfigurieren eines HTTP-Proxys auf Supervisoren, die Sie als Verwaltungscluster bei Tanzu Mission Control registrieren möchten, die folgenden Schritte aus:

1. Konfigurieren Sie in vSphere den HTTP-Proxy auf Supervisoren, indem Sie entweder die HTTP-Proxy-Einstellungen aus vCenter Server übernehmen oder Proxy-Einstellungen auf einzelnen Supervisoren über vSphere Client, APIs der Namespace-Verwaltungscluster oder die DCLI-Befehlszeile konfigurieren.
2. Erstellen Sie in Tanzu Mission Control ein Proxy-Konfigurationsobjekt, indem Sie die Proxy-Einstellungen verwenden, die Sie für die Supervisoren in vSphere IaaS control plane konfiguriert haben. Weitere Informationen finden Sie unter Erstellen eines Proxy-Konfigurationsobjekts für einen Tanzu Kubernetes Grid Service-Cluster.
3. Verwenden Sie dieses Proxy-Konfigurationsobjekt in Tanzu Mission Control, wenn Sie die Supervisoren als Verwaltungscluster registrieren. Weitere Informationen finden Sie unter Registrieren eines Verwaltungsclusters bei Tanzu Mission Control und Abschließen der Registrierung eines Supervisor-Clusters.

So konfigurieren Sie einen HTTP-Proxy für TKG-Cluster, die Sie als Arbeitslast-Cluster in Tanzu Mission Control bereitstellen oder hinzufügen:

1. Erstellen Sie ein Proxy-Konfigurationsobjekt mit den Proxy-Einstellungen, die Sie mit Tanzu Kubernetes-Clustern verwenden möchten. Weitere Informationen finden Sie unter Erstellen eines Proxy-Konfigurationsobjekts für einen Tanzu Kubernetes Grid Service-Cluster.

2 Verwenden Sie dieses Proxy-Konfigurationsobjekt, wenn Sie Tanzu Kubernetes-Cluster als Arbeitslastcluster bereitstellen oder hinzufügen. Weitere Informationen finden Sie unter Bereitstellen eines Clusters und Hinzufügen eines Arbeitslastclusters zur Tanzu Mission Control-Verwaltung

Konfigurieren eines externen IDP für die Verwendung mit TKG-Dienstclustern

Sie können Supervisor mit jedem OIDC-konformen Identitätsanbieter (IDP), z. B. Okta, konfigurieren. Um die Integration abzuschließen, konfigurieren Sie den IDP mit der Callback-URL für Supervisor.

Unterstützte externe OIDC-Anbieter

Sie können Supervisor mit jedem OIDC-konformen Identitätsanbieter konfigurieren. Die Tabelle enthält gängige Beispiele und Links zu Konfigurationsanweisungen.

Externer IDP	Konfiguration
Okta	Beispiel für eine OIDC-Konfiguration mit Okta Weitere Informationen finden Sie unter Konfigurieren von Okta als OIDC-Anbieter für Pinniped
Workspace ONE	Konfigurieren von Workspace ONE Access als OIDC-Anbieter für Pinniped
Dex	Konfigurieren von Dex als OIDC-Anbieter für Pinniped
GitLab	Konfigurieren von GitLab als OIDC-Anbieter für Pinniped
Google OAuth	Verwenden von Google OAuth 2

Konfigurieren des IDP mit der Callback-URL für Supervisor

Supervisor fungiert als OAuth 2.0-Client für den externen Identitätsanbieter. Die Supervisor-Callback-URL ist die Umleitungs-URL, die zum Konfigurieren des externen Identitätsanbieters verwendet wird. Die Callback-URL hat das Format *https://SUPERVISOR-VIP/wcp/pinniped/callback*.

Hinweis Bei der IDP-Registrierung wird die Callback-URL in dem OIDC-Anbieter, den Sie konfigurieren, möglicherweise als „Weiterleitungs-URL“ bezeichnet.

Wenn Sie den externen Identitätsanbieter für die Verwendung mit TKG auf Supervisor konfigurieren, übermitteln Sie dem externen Identitätsanbieter die **Callback-URL**, die in vCenter Server im Bildschirm **Arbeitslastverwaltung > Supervisoren > Konfigurieren > Identitätsanbieter** verfügbar ist.

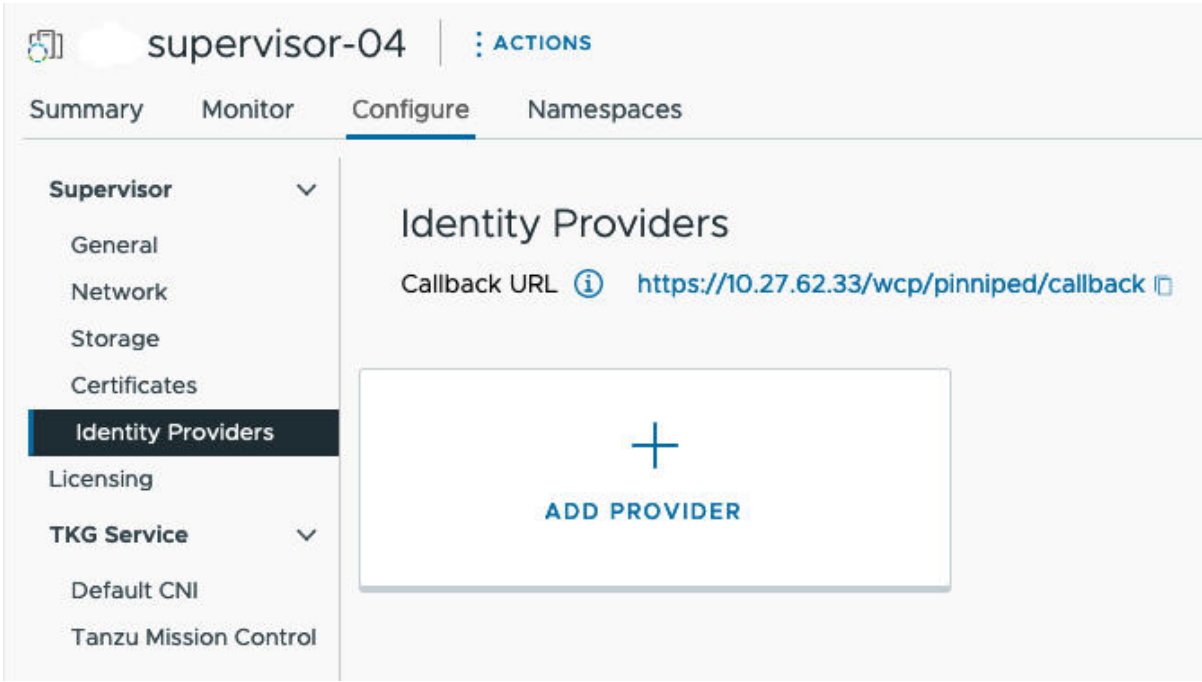
Beispiel für eine OIDC-Konfiguration mit Okta

Mit Okta können sich Benutzer mit dem OpenID Connect-Protokoll bei Anwendungen anmelden. Wenn Sie Okta als externen Identitätsanbieter für Tanzu Kubernetes Grid auf Supervisor konfigurieren, steuern die Pinniped-Pods auf Supervisor und auf Tanzu Kubernetes Grid-Clustern den Benutzerzugriff für vSphere-Namespaces und für Arbeitslastcluster.

1 Kopieren Sie die Callback-URL des Identitätsanbieters, die Sie zum Erstellen einer OIDC-Verbindung zwischen Okta und vCenter Server benötigen.

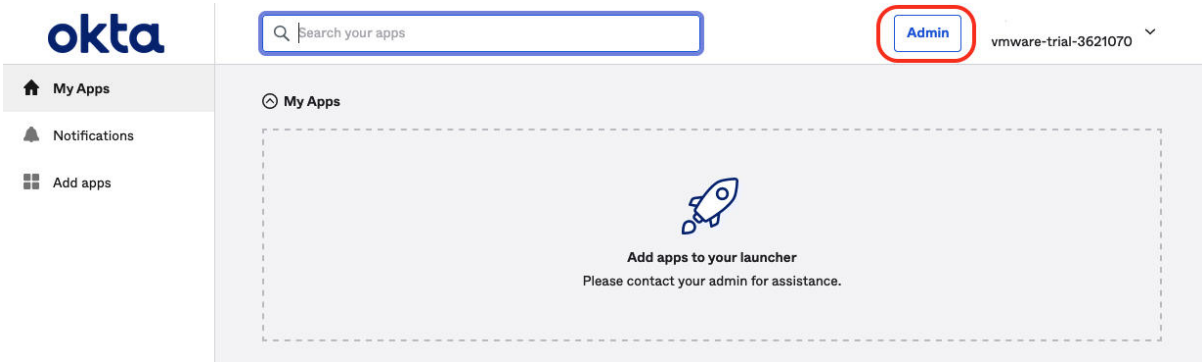
Rufen Sie die Callback-URL des Identitätsanbieters im vSphere Client unter **Arbeitslastverwaltung > Supervisoren > Konfigurieren > Identitätsanbieter** ab. Kopieren Sie diese URL an einen temporären Speicherort.

Abbildung 12-6. IDP-Callback-URL



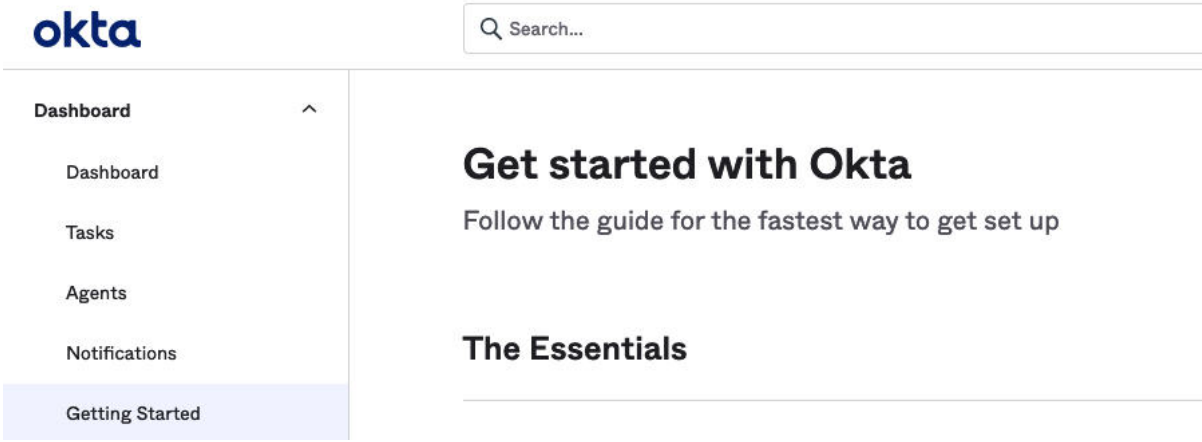
2 Melden Sie sich beim Okta-Konto für Ihre Organisation an oder erstellen Sie ein Testkonto unter https://www.okta.com/. Klicken Sie auf die Schaltfläche **Admin**, um die Okta-Verwaltungskonsole zu öffnen.

Abbildung 12-7. Okta-Verwaltungskonsole



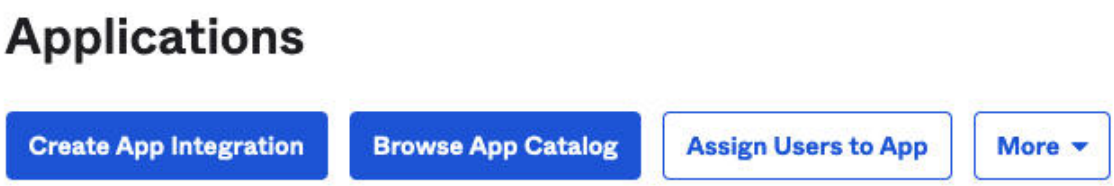
3 Navigieren Sie in der Verwaltungskonsole auf der Seite „Erste Schritte“ zu **Anwendungen > Anwendungen**.

Abbildung 12-8. Okta – Erste Schritte



4 Wählen Sie die Option **App-Integration erstellen** aus.

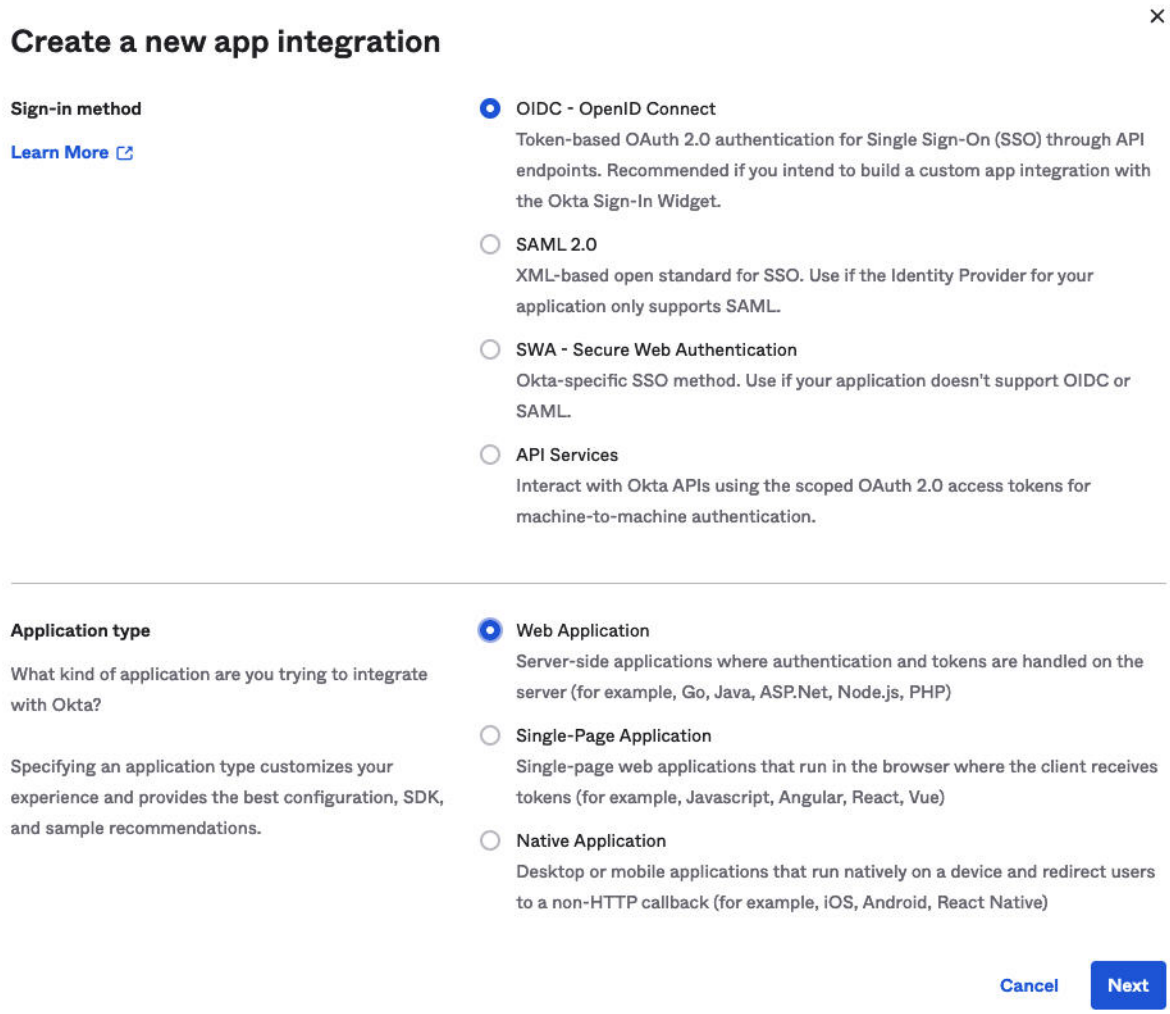
Abbildung 12-9. Okta – App-Integration erstellen



5 Erstellen Sie die neue App-Integration.

- Legen Sie die Anmeldemethode auf **OIDC - OpenID Connect** fest.
- Legen Sie den Anwendungstyp auf **Webanwendung** fest.

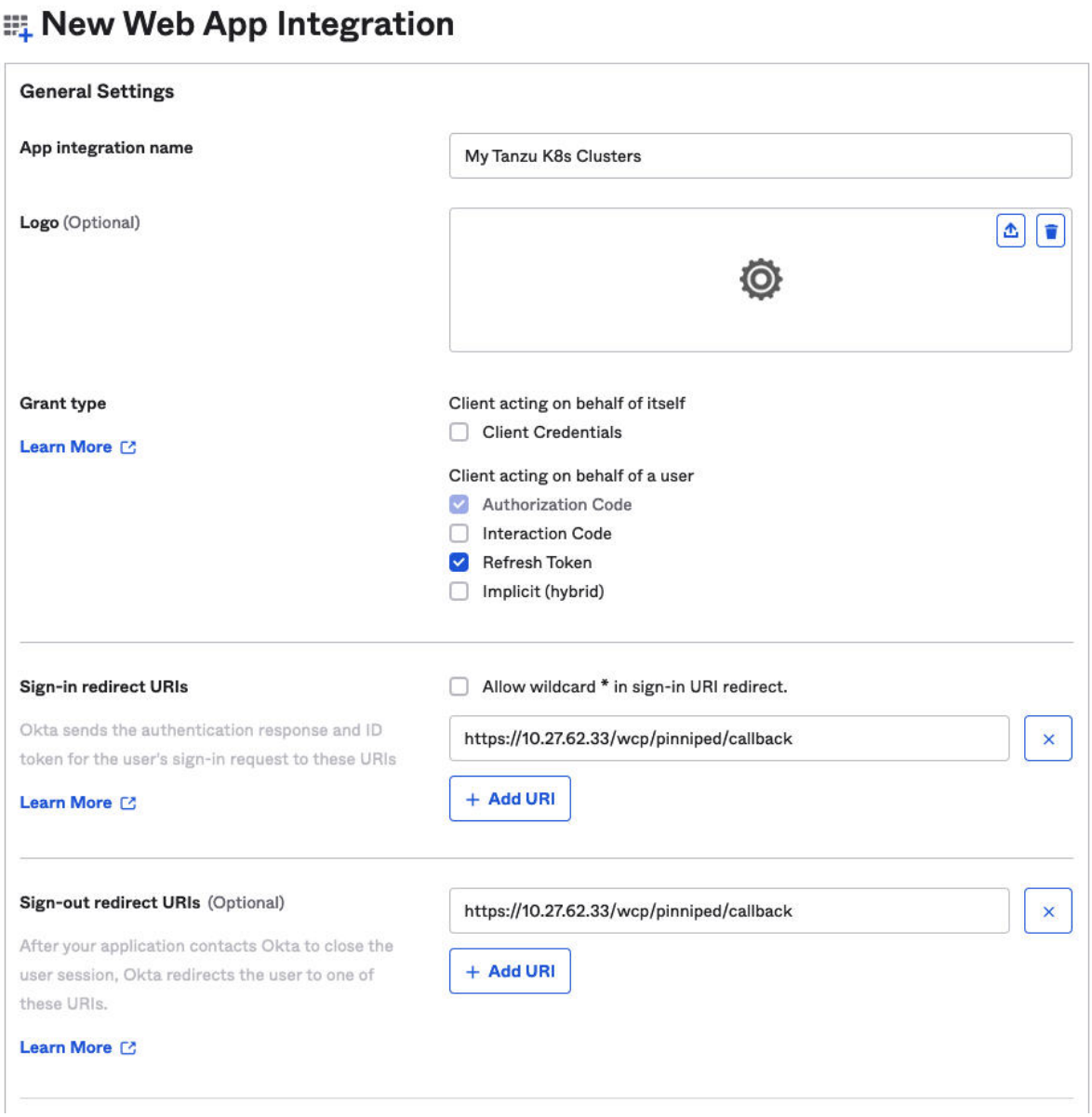
Abbildung 12-10. Okta-Anmeldemethode und Anwendungstyp



6 Konfigurieren Sie die Details der Okta-Webanwendungsintegration.

- Geben Sie einen **Namen für die App-Integration** an, der eine benutzerdefinierte Zeichenfolge ist.
- Geben Sie den **Gewährungstyp** an: Wählen Sie **Autorisierungscode** und außerdem **Token aktualisieren** aus.
- Weiterleitungs-URIs für die Anmeldung: Geben Sie die Callback-URL des Identitätsanbieters ein, die Sie von Supervisor kopiert haben (siehe Schritt 1), z. B. https://10.27.62.33/wcp/pinnipend/callback.
- Weiterleitungs-URIs für die Abmeldung: Geben Sie die Callback-URL des Identitätsanbieters ein, die Sie von Supervisor kopiert haben (siehe Schritt 1), z. B. https://10.27.62.33/wcp/pinnipend/callback.

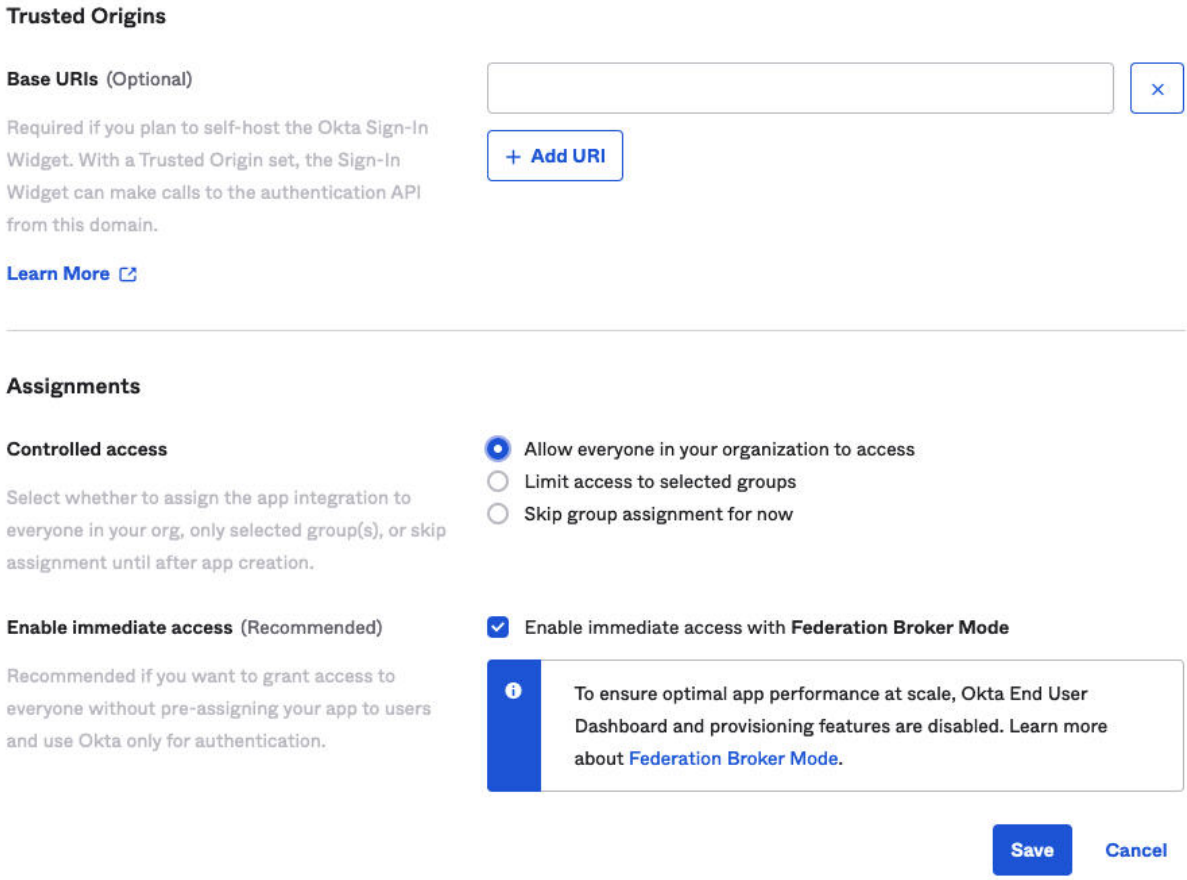
Abbildung 12-11. Details der Okta-Webanwendungsintegration



7 Konfigurieren Sie die Benutzerzugriffssteuerung.

Im Abschnitt **Zuweisungen > Kontrollierter Zugriff** können Sie optional steuern, welche der in Ihrer Organisation vorhandenen Okta-Benutzer auf Tanzu Kubernetes Grid-Cluster zugreifen können. Im Beispiel gewähren Sie allen in der Organisation definierten Benutzern Zugriff.

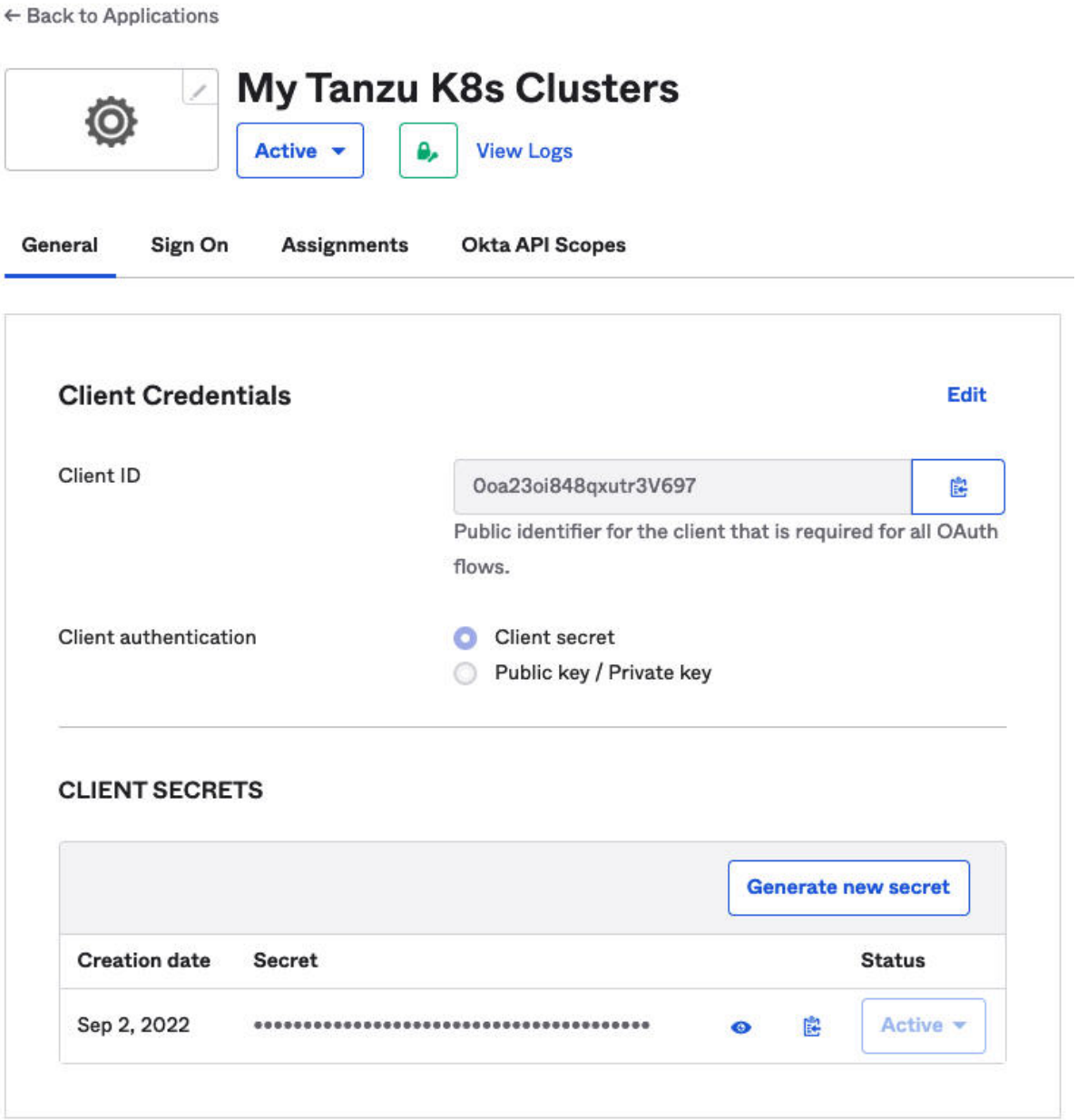
Abbildung 12-12. Okta-Zugriffssteuerung



8 Klicken Sie auf **Speichern** und kopieren Sie die **Client-ID** und den **geheimen Clientschlüssel**, die zurückgegeben werden.

Wenn Sie die OKTA-Konfiguration speichern, stellt Ihnen die Verwaltungskonsole eine **Client-ID** und einen **geheimen Clientschlüssel** zur Verfügung. Kopieren Sie beide Elemente, da Sie diese benötigen, um Supervisor mit einem externen Identitätsanbieter zu konfigurieren.

Abbildung 12-13. OIDC-Client-ID und geheimer Schlüssel

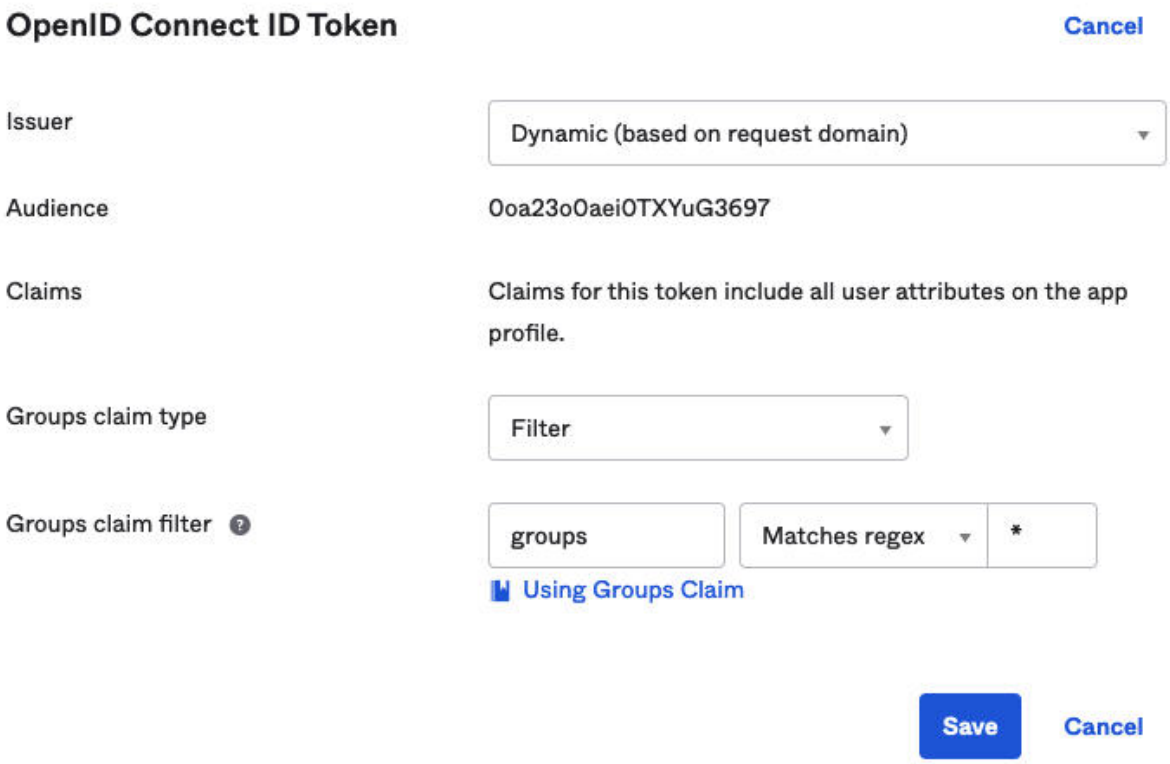


9 Konfigurieren Sie das OpenID Connect-ID-Token.

Klicken Sie auf die Registerkarte **Anmelden**. Klicken Sie im Abschnitt **OpenID Connect ID-Token** auf den Bearbeitungslink, geben Sie als **Gruppenanspruchstyp** „Filter“ ein und **speichern** Sie die Einstellungen.

Wenn der Anspruchname „Gruppen“ allen Gruppen entsprechen soll, wählen Sie **Gruppen > Entspricht regex >** * aus.

Abbildung 12-14. OpenID Connect-ID-Token

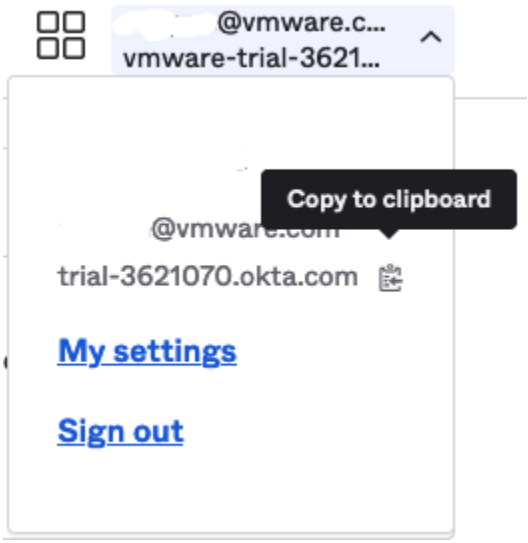


10 Kopieren Sie die **Aussteller-URL**.

Um Supervisor zu konfigurieren, benötigen Sie die **Aussteller-URL** sowie die **Client-ID** und den **geheimen Clientschlüssel**.

Kopieren Sie die **Aussteller-URL** aus der Okta-Verwaltungskonsole.

Abbildung 12-15. Okta-Aussteller-URL



Registrieren eines externen IDP bei Supervisor

Um mithilfe der Tanzu-CLI eine Verbindung zu Tanzu Kubernetes Grid 2.0-Clustern auf Supervisor herzustellen, registrieren Sie Ihren OIDC-Anbieter bei Supervisor.

Voraussetzungen

Bevor Sie einen externen ODIC-Anbieter bei Supervisor registrieren, müssen Sie die folgenden Voraussetzungen erfüllen:

- Aktivieren Sie die Arbeitslastverwaltung und stellen Sie eine Supervisor-Instanz bereit. Weitere Informationen finden Sie unter Ausführen von TKG 2.0-Clustern auf Supervisor.
- Konfigurieren Sie einen externen OpenID Connect-Identitätsanbieter mit der Supervisor-Callback-URL. Weitere Informationen finden Sie unter Konfigurieren eines externen IDP für die Verwendung mit TKG-Dienstclustern.
- Rufen Sie die Client-ID, den geheimen Clientschlüssel und die Aussteller-URL des externen IDP ab. Weitere Informationen finden Sie unter Konfigurieren eines externen IDP für die Verwendung mit TKG-Dienstclustern.

Registrieren eines externen IDP bei Supervisor

Supervisor führt die Pinniped-Supervisor- und Pinniped-Concierge-Komponenten als Pods aus. Tanzu Kubernetes Grid-Cluster führen nur die Pinniped-Concierge-Komponente als Pods aus. Weitere Informationen zu diesen Komponenten und deren Interaktion finden Sie in der Dokumentation zum Pinniped-Authentifizierungsdienst.

Sobald Sie einen externen Identitätsanbieter bei Supervisor registriert haben, aktualisiert das System die Pinniped-Supervisor- und Pinniped-Concierge-Pods auf Supervisor und die Pinniped-Concierge-Pods in Tanzu Kubernetes Grid-Clustern. Alle in dieser Supervisor-Instanz ausgeführten Tanzu Kubernetes Grid-Cluster werden automatisch mit demselben externen Identitätsanbieter konfiguriert.

Führen Sie das folgende Verfahren aus, um einen externen ODIC-Anbieter bei Supervisor zu registrieren:

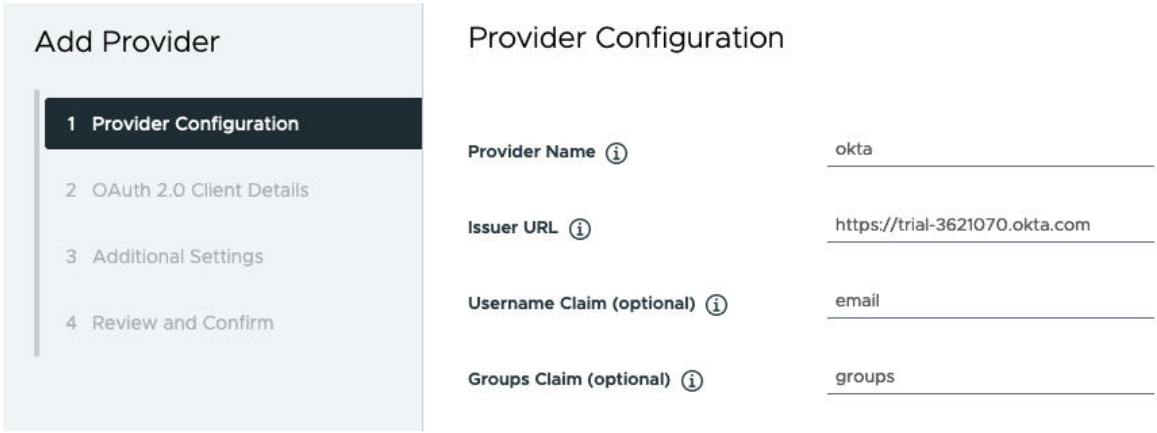
1 Melden Sie sich über vSphere Client bei vCenter Server an.

2 Wählen Sie **Arbeitslastverwaltung > Supervisoren > Konfigurieren > Identitätsanbieter** aus.

3 Klicken Sie auf das Pluszeichen, um den Registrierungsvorgang zu starten.

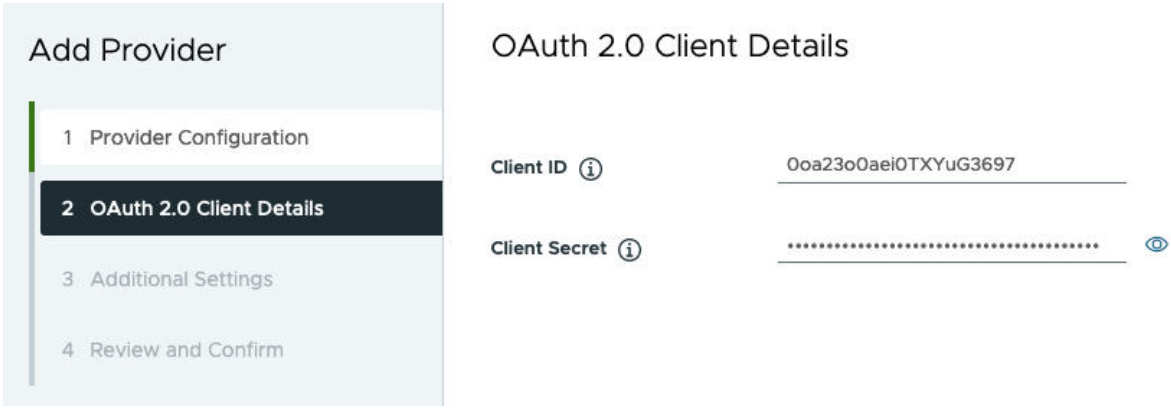
4 Konfigurieren Sie den Identitätsanbieter. Weitere Informationen finden Sie unter Konfiguration des OIDC-Anbieters.

Abbildung 12-16. Konfiguration des OIDC-Anbieters



5 Konfigurieren Sie OAuth 2.0-Client-Details. Weitere Informationen finden Sie unter OAuth 2.0-Client-Details.

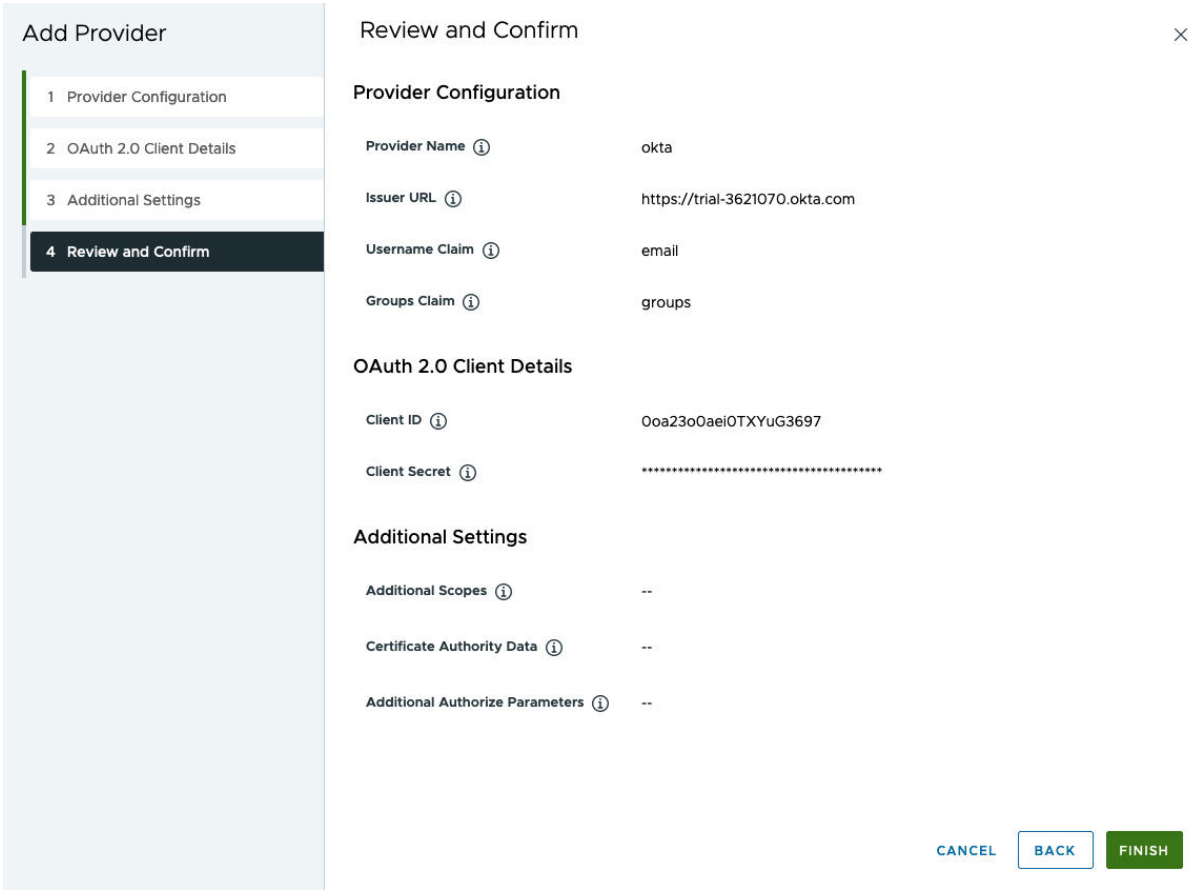
Abbildung 12-17. OAuth 2.0-Client-Details



6 Konfigurieren Sie zusätzliche Einstellungen. Weitere Informationen finden Sie unter Weitere Einstellungen.

7 Bestätigen Sie die Anbietereinstellungen.

Abbildung 12-18. Anbietereinstellungen bestätigen



8 Klicken Sie auf **Beenden**, um die OIDC-Anbieterregistrierung abzuschließen.

Konfiguration des OIDC-Anbieters

Beachten Sie die folgenden Konfigurationsdetails des Anbieters beim Registrieren eines externen OIDC-Anbieters bei Supervisor.

Tabelle 12-1. Konfiguration des OIDC-Anbieters

Bereich	Gewichtung	Beschreibung
Anbietername	Erforderlich	Benutzerdefinierter Name für den externen Identitätsanbieter.
Aussteller-URL	Erforderlich	Die URL zum Identitätsanbieter, der Token ausstellt. Die OIDC-Erkennungs-URL wird von der Aussteller-URL abgeleitet. Für Okta sieht die Aussteller-URL beispielsweise wie folgt aus und kann über die Admin-Konsole abgerufen werden: *https://trial-4359939-admin.okta.com*.

Tabelle 12-1. Konfiguration des OIDC-Anbieters (Fortsetzung)

Bereich	Gewichtung	Beschreibung
Benutzernamensanspruch	Optional	Der Anspruch vom ID-Token des Upstream-Identitätsanbieters oder vom Benutzerinformations-Endpoint, der überprüft werden soll, um den Benutzernamen für den angegebenen Benutzer abzurufen. Wenn Sie dieses Feld leer lassen, wird die Upstream-Aussteller-URL mit dem Anspruch „sub“ verkettet, um den Benutzernamen zu generieren, der mit Kubernetes verwendet werden soll. Dieses Feld gibt an, was Pinniped vom Upstream-ID-Token aus suchen soll, um die Authentifizierung zu ermitteln. Wenn keine Angaben gemacht werden, wird die Benutzeridentität als *https://IDP-ISSUER?sub=UUID* formatiert.
Gruppenanspruch	Optional	Der Anspruch vom ID-Token des Upstream-Identitätsanbieters oder vom Benutzerinformations-Endpoint, der überprüft werden soll, um die Gruppen für den angegebenen Benutzer abzurufen. Wenn Sie dieses Feld leer lassen, werden keine Gruppen des Upstream-Identitätsanbieters verwendet. Das Feld „Gruppenanspruch“ teilt Pinniped mit, was aus dem Upstream-ID-Token zur Authentifizierung der Benutzeridentität zu entnehmen ist.

OAuth 2.0-Client-Details

Beachten Sie die folgenden OAuth 2.0-Client-Details des Anbieters, wenn Sie einen externen OIDC-Anbieter bei Supervisor registrieren.

Tabelle 12-2. OAuth 2.0-Client-Details

OAuth 2.0-Client-Details	Gewichtung	Beschreibung
Client-ID	Erforderlich	Client-ID des externen IDP
Geheimer Clientschlüssel	Erforderlich	Geheimer Clientschlüssel vom externen IDP

Weitere Einstellungen

Beachten Sie die folgenden zusätzlichen Einstellungen, wenn Sie einen externen OIDC-Anbieter bei Supervisor registrieren.

Tabelle 12-3. Weitere Einstellungen

Einstellung	Gewichtung	Beschreibung
Zusätzliche Geltungsbereiche	Optional	Zusätzliche Geltungsbereiche, die in Token angefordert werden müssen
Daten zur Zertifizierungsstelle	Optional	Daten der TLS-Zertifizierungsstelle für eine sichere externe IDP-Verbindung
Zusätzliche Autorisierungsparameter	Optional	Zusätzliche Parameter während der OAuth2-Autorisierungsanforderung

Ändern der Speichereinstellungen im Supervisor

Durch Speicherrichtlinien, die dem Supervisor zugewiesen sind, wird verwaltet, wie Objekte wie eine Steuerungsebenen-VM, flüchtige vSphere Pod-Festplatten und der Cache des Container-Image in Datenspeichern in der vSphere-Speicherumgebung platziert werden. Als vSphere-Administrator konfigurieren Sie die Speicherrichtlinien in der Regel, wenn Sie den Supervisor aktivieren. Falls Sie nach der Erstkonfiguration des Supervisors Änderungen an den Zuweisungen der Speicherrichtlinien vornehmen müssen, führen Sie diese Aufgabe aus. Sie können diese Aufgabe auch verwenden, um die Unterstützung von Datei-Volumes für persistente ReadWriteMany-Volumes in TKG-Clustern zu aktivieren oder zu deaktivieren.

Die Änderungen, die Sie an den Speichereinstellungen vornehmen, gelten generell nur für neue Objekte in Supervisor. Wenn Sie dieses Verfahren verwenden, um die Unterstützung von Datei-Volumes in TKG-Clustern zu aktivieren, können Sie dies für die vorhandenen Cluster tun.

Voraussetzungen

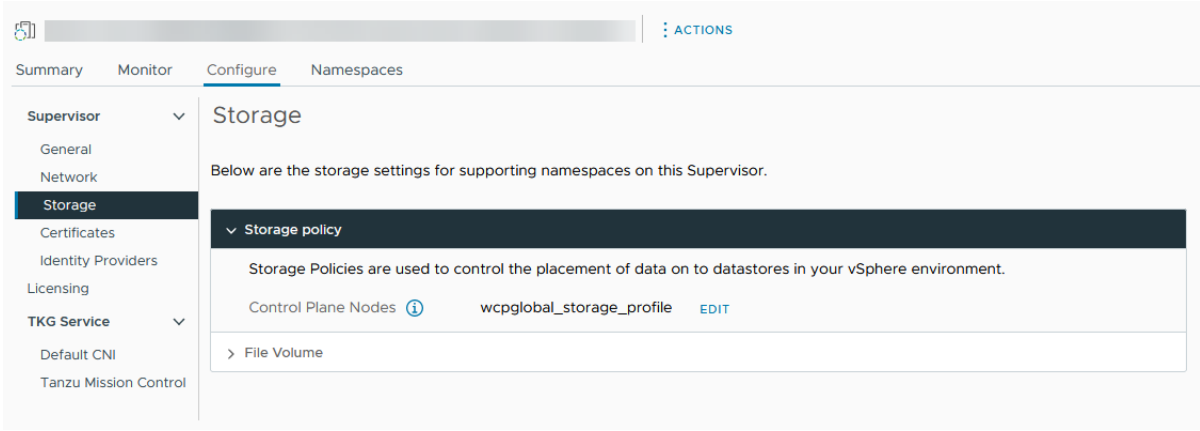
Wenn Sie die Unterstützung von Datei-Volumes auf TKG-Clustern für dauerhafte Volumes im ReadWriteMany-Modus aktivieren möchten, befolgen Sie die Voraussetzungen unter Erstellen von dauerhaften ReadWriteMany-Volumes in vSphere IaaS control plane in der *Dienste und Arbeitslasten der vSphere IaaS-Steuerungsebene*-Dokumentation.

Verfahren

1. Navigieren Sie im vSphere Client zu **Arbeitslastverwaltung**.
2. Klicken Sie auf die Registerkarte **Supervisoren** und wählen Sie den zu bearbeitenden Supervisor aus der Hardwareliste aus.

3 Klicken Sie auf die Registerkarte **Konfigurieren** und anschließend auf **Speicher**.

Abbildung 12-19. Aktualisieren von Supervisor-Speichereinstellungen



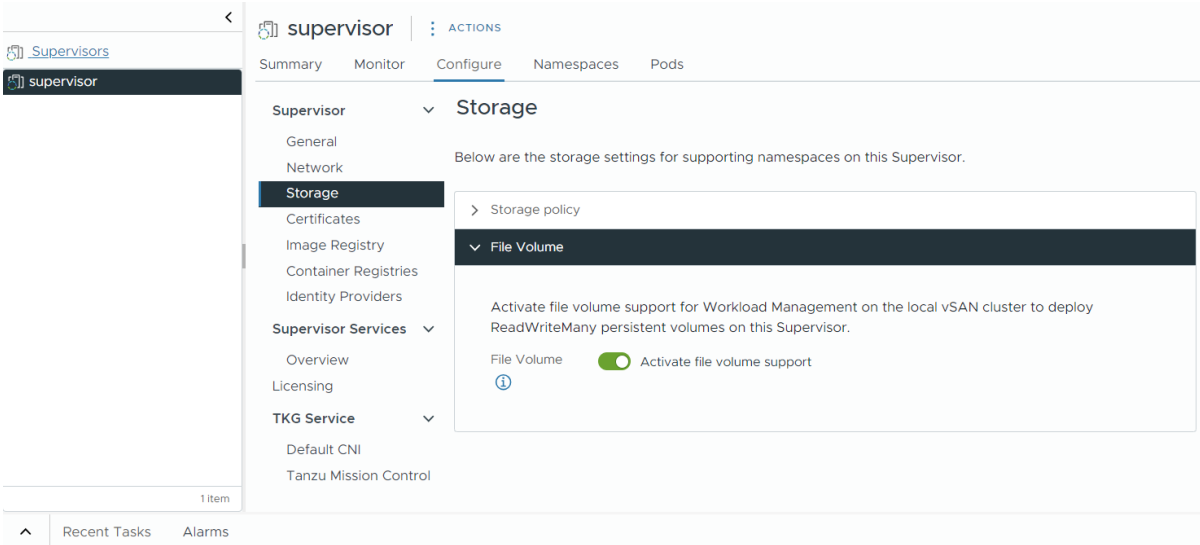
4 Ändern Sie die Speicherrichtlinienzuweisungen für die Steuerungsebenen-VMs.

Wenn Ihre Umgebung einen vSphere Pod unterstützt, können Sie auch Speicherrichtlinien für eine flüchtige virtuelle Festplatte und den Container-Image-Cache ändern.

Option	Bezeichnung
Steuerungsebenenknoten	Wählen Sie die Speicherrichtlinie für die Platzierung der Control Plane-VMs aus.
Flüchtige Pod-Festplatten	Wählen Sie die Speicherrichtlinie für die Platzierung der vSphere-Pods aus.
Container-Image-Cache	Wählen Sie die Speicherrichtlinie für die Platzierung des Caches von Container-Images aus.

5 Aktivieren Sie die Unterstützung für Datei-Volumes, um persistente ReadWriteMany-Volumes bereitzustellen.

Diese Option ist nur verfügbar, wenn Ihre Umgebung mit dem vSAN-Dateidienst konfiguriert wurde. Weitere Informationen finden Sie unter vSAN-Dateidienst aktivieren.



Streamen von Supervisor-Metriken auf einer benutzerdefinierten Beobachtbarkeitsplattform

Erfahren Sie, wie Sie von Telegraf erfasste Supervisor-Metriken auf einer benutzerdefinierten Beobachtbarkeitsplattform streamen. Telegraf ist standardmäßig auf dem Supervisor aktiviert und erfasst Metriken im Prometheus-Format aus Supervisor-Komponenten, z. B. vom Kubernetes-API-Server, VM-Dienst, Tanzu Kubernetes Grid usw. Als vSphere-Administrator können Sie eine Beobachtbarkeitsplattform wie VMware Aria Operations for Applications, Grafana und andere konfigurieren, um die erfassten Supervisor-Metriken anzuzeigen und zu analysieren.

Telegraf ist ein serverbasierter Agent zum Erfassen und Senden von Metriken aus verschiedenen Systemen, Datenbanken und Internet der Dinge. Jede Supervisor-Komponente stellt einen Endpoint zur Verfügung, auf dem Telegraf eine Verbindung herstellt. Telegraf sendet dann die erfassten Metriken an eine Beobachtbarkeitsplattform Ihrer Wahl. Sie können ein beliebiges der von Telegraf unterstützten Ausgabe-Plug-Ins als Beobachtbarkeitsplattform für die Aggregierung und Analyse der Supervisor-Metriken konfigurieren. Informationen zu den unterstützten Ausgabe-Plug-Ins finden Sie in der Telegraf-Dokumentation.

Die folgenden Komponenten stellen Endpunkte zur Verfügung, auf denen Telegraf eine Verbindung herstellt und Metriken erfasst: Kubernetes-API-Server, etcd, kubelet, Kubernetes-Controller-Manager, Kubernetes-Scheduler, Tanzu Kubernetes Grid, VM-Dienst, VM-Imageservice, NSX Container Plug-in (NCP), Container Storage Interface (CSI), Zertifikatsmanager, NSX und verschiedene Hostmetriken wie CPU, Arbeitsspeicher und Speicher.

Anzeigen der Telegraf-Pods und -Konfiguration

Telegraf wird unter dem `vmware-system-monitoring`-System-Namespace auf dem Supervisor ausgeführt. So zeigen Sie die Telegraf-Pods und ConfigMaps an:

1 Melden Sie sich bei der Supervisor-Steuerungsebene mit einem vCenter Single Sign-On-Administratorkonto an.

```
kubectl vsphere login --server <control plane IP> --vsphere-username
administrator@vsphere.local
```

2 Verwenden Sie den folgenden Befehl, um die Telegraf-Pods anzuzeigen:

```
kubectl -n vmware-system-monitoring get pods
```

Die resultierenden Pods lauten wie folgt:

```
telegraf-csqsl
telegraf-dkwtk
telegraf-l4nxk
```

3 Verwenden Sie den folgenden Befehl, um die Telegraf-ConfigMaps anzuzeigen:

```
kubectl -n vmware-system-monitoring get cm
```

Die resultierenden ConfigMaps lauten wie folgt:

```
default-telegraf-config
kube-rbac-proxy-config
kube-root-ca.crt
telegraf-config
```

Die `default-telegraf-config`-ConfigMap enthält die Telegraf-Standardkonfiguration und ist schreibgeschützt. Sie können sie als Fallback-Option verwenden, um die Konfiguration in `telegraf-config` wiederherzustellen für den Fall, dass die Datei beschädigt ist oder Sie einfach die Standardwerte wiederherstellen möchten. Die einzige bearbeitbare ConfigMap ist `telegraf-config`. Sie definiert, welche Komponenten Metriken an die Telegraf-Agenten senden und an welche Plattformen sie senden.

4 Anzeigen der `telegraf-config`-ConfigMap:

```
kubectl -n vmware-system-monitoring get cm telegraf-config -o yaml
```

Im Abschnitt `inputs` der ConfigMap `telegraf-config` werden alle Endpunkte der Supervisor-Komponenten definiert, von denen Telegraf Metriken sowie die Metriktypen selbst erfasst. Beispielsweise definiert die folgende Eingabe den Kubernetes-API-Server als Endpunkt:

```
  [[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"
```

Die `alias`-Eigenschaft gibt die Komponente an, aus der Metriken erfasst werden. Die `namepass`-Eigenschaft gibt an, welche Komponentenmetriken von den Telegraf-Agenten offengelegt bzw. erfasst werden.

Obwohl die ConfigMap `telegraf-config` bereits eine breite Palette von Metriken enthält, können Sie dennoch zusätzliche Metriken definieren. Weitere Informationen finden Sie unter Metriken für Kubernetes-Systemkomponenten und Kubernetes-Metrikreferenz.

Konfigurieren der Beobachtbarkeitsplattform für Telegraf

Im Abschnitt `outps` von `telegraf-config` können Sie konfigurieren, wo Telegraf die erfassten Metriken streamt. Es gibt mehrere Optionen wie `outputs.file`, `outputs.wavefront`, `outputs.prometheus_client` und `outps-https`. Im Abschnitt `outps-https` können Sie die Beobachtungsplattformen konfigurieren, die Sie für die Zusammenfassung und Überwachung der Supervisor-Metriken verwenden möchten. Sie können Telegraf so konfigurieren, dass Metriken an mehr als eine Plattform gesendet werden. Um die ConfigMap `telegraf-config` zu bearbeiten und eine Beobachtbarkeitsplattform zum Anzeigen von Supervisor-Metriken zu konfigurieren, führen Sie die folgenden Schritte aus:

1 Melden Sie sich bei der Supervisor-Steuerungsebene mit einem vCenter Single Sign-On-Administratorkonto an.

```
kubectl vsphere login --server <control plane IP> --vsphere-username
administrator@vsphere.local
```

2 Speichern Sie die ConfigMap `telegraf-config` im lokalen kubectl-Ordner:

```
kubectl get cm telegraf-config -n vmware-system-monitoring -o
jsonpath="{.data['telegraf\.conf']}">telegraf.conf
```

Speichern Sie die `telegraf-config`-ConfigMap in einem Versionskontrollsystem, bevor Sie Änderungen daran vornehmen, falls Sie eine vorherige Version der Datei wiederherstellen möchten. Wenn Sie die Standardkonfiguration wiederherstellen möchten, können Sie die Werte aus der `default-telegraf-config`-ConfigMap verwenden.

3 Fügen Sie `outputs.http`-Abschnitte mit den Verbindungseinstellungen der Beobachtbarkeitsplattformen Ihrer Wahl hinzu, indem Sie einen Texteditor verwenden, z. B. VIM:

```
vim telegraf.config
```

Sie können die Auskommentierung des folgenden Abschnitts direkt aufheben und die Werte entsprechend bearbeiten oder nach Bedarf neue `outputs.http`-Abschnitte hinzufügen.

```
    #[[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>
```

So sieht beispielsweise eine `outputs.http`-Konfiguration für Grafana aus:

```
    [[outputs.http]]
url = "http://<grafana-host>:<grafana-metrics-port>/<prom-metrics-push-path>"
data_format = "influx"
[outputs.http.headers]
  Authorization = "Bearer <grafana-bearer-token>"
```

Weitere Informationen zum Konfigurieren von Dashboards und zur Nutzung von Metriken von Telegraf finden Sie unter Streamen von Metriken von Telegraf zu Grafana.

Im Folgenden finden Sie nun ein Beispiel mit VMware Aria Operations for Applications (ehemals Wavefront):

```
    [[outputs.wavefront]]
      url = "http://<wavefront-proxy-host>:<wavefront-proxy-port>"
```

Die empfohlene Methode zur Erfassung von Metriken für Aria Operations for Applications ist Proxy-basiert. Weitere Informationen dazu finden Sie unter Wavefront-Proxies .

4 Ersetzen Sie die vorhandene `telegraf-config`-Datei auf dem Supervisor durch die Datei, die Sie in Ihrem lokalen Ordner bearbeitet haben:

```
kubectl create cm --from-file telegraf.conf -n vmware-system-monitoring telegraf-config
--dry-run=client -o yaml | kubectl replace -f -
```

5 Überprüfen Sie, ob die neue Konfiguration erfolgreich gespeichert wurde:

- Zeigen Sie die neue `telegraf-config`-ConfigMap an:

  ```
  kubectl -n vmware-system-monitoring get cm telegraf-config -o yaml
  ```

- Überprüfen Sie, ob alle Telegraf-Pods ausgeführt werden:

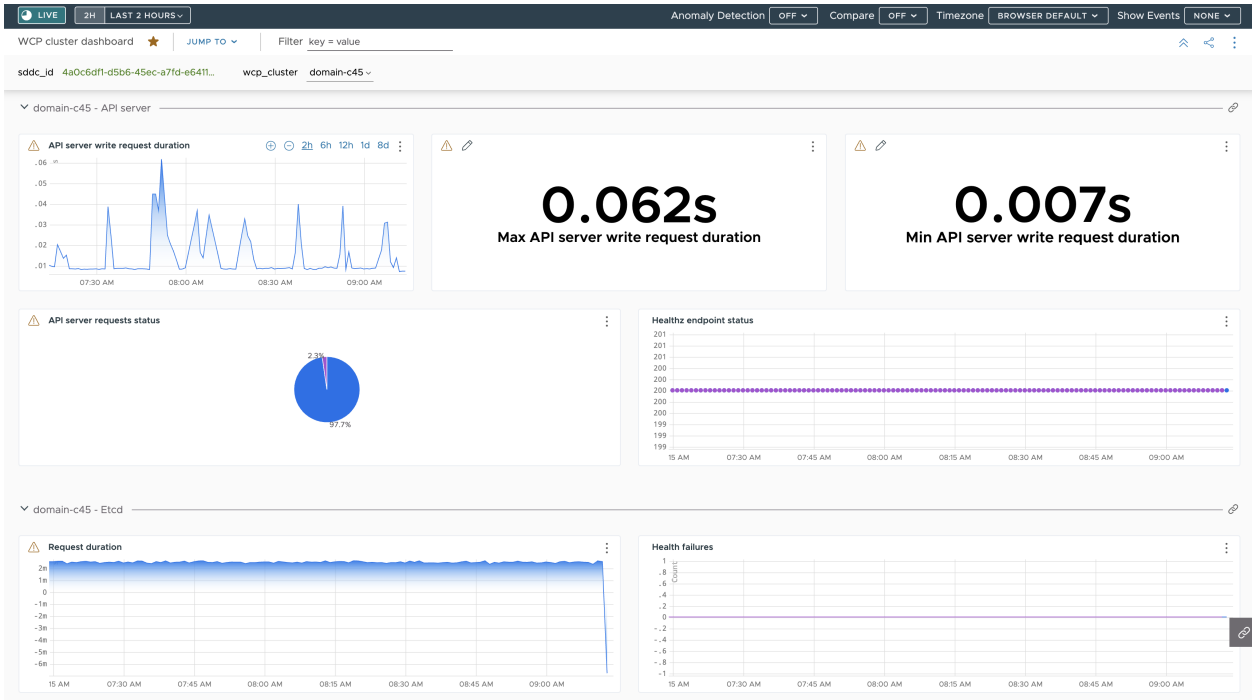
  ```
  kubectl -n vmware-system-monitoring get pods
  ```

- Wenn einige der Telegraf-Pods nicht ausgeführt werden, überprüfen Sie die Telegraf-Protokolle für diesen Pod, um eine Fehlerbehebung durchzuführen:

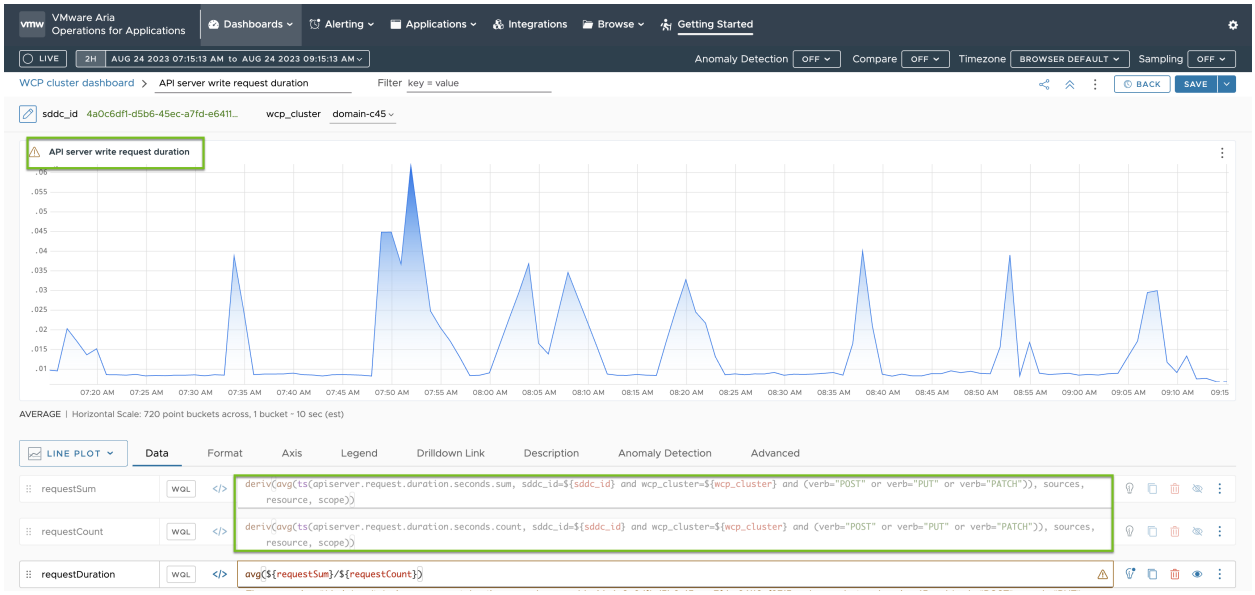
  ```
  kubectl -n vmware-system-monitoring logs <telegraf-pod>
  ```

Beispiel-Dashboards für Operations for Applications

Im Folgenden wird ein Dashboard mit einer Übersicht für die Metriken gezeigt, die vom API-Server und von etcd auf einem Supervisor über Telegraf empfangen wurden:



Die Metriken für die Dauer der API-Server-Schreibanforderung basieren auf den Metriken, die in der ConfigMap `telegraf-config` angegeben sind. Sie sind grün hervorgehoben:



Ändern der Liste der DNS-Namen der Supervisor Control Plane

Erfahren Sie, wie Sie die Liste der FQDNs für den Zugriff auf die Supervisor Control Plane ändern. Sie können während der Aktivierung des Supervisors eine Liste der Supervisor-FQDNs angeben und diese Liste später aktualisieren. Sie können auch eine Liste von Supervisor-FQDNs festlegen, wenn Sie während der Aktivierung des Supervisors keine FQDNs bereitgestellt haben.

Verfahren

- Verwenden Sie den folgenden DCLI-Befehl, um die Liste der FQDNs für die Supervisor Control Plane zu aktualisieren:

  ```
  dcli com vmware vcenter namespacemanagement clusters update --cluster <cluster_ID> --
  master-dns-name <FQDN 1> --master-dns-name <FQDN_2>
  ```

  - Um der Liste einen neuen FQDN hinzuzufügen, übergeben Sie die bereits vorhandenen Namen als Argumente und fügen den neuen FQDN hinzu.
  - Um einen FQDN aus der Liste zu entfernen, rufen Sie den `update`-Befehl auf. Lassen Sie den zu entfernenden FQDN aus und übergeben Sie die restlichen FQDNs, die Sie beibehalten möchten.

  Bei einem Supervisor mit drei Zonen können Sie die ID eines beliebigen Clusters übergeben, der Teil des Supervisors ist.

  Im folgenden Beispiel ist der auf Cluster `domain-c50` ausgeführte Supervisor bereits mit einem FQDN `supervisor.acme.com` konfiguriert. Sie fügen der Liste der DNS-Namen für den Supervisor einen neuen FQDN `supervisor.vmware.com` hinzu:

  ```
  dcli com vmware vcenter namespacemanagement clusters update --cluster domain-c50 --master-
  dns-name supervisor.acme.com --master-dns-name supervisor.vmware.com
  ```

Nächste Schritte

- Das VIP-Zertifikat für die sichere Verbindung mit dem Supervisor wird nicht automatisch mit den neuen FQDNs aktualisiert. Daher müssen Sie dies manuell tun. Weitere Informationen finden Sie unter Ersetzen des VIP-Zertifikats zur sicheren Verbindung mit dem Supervisor-API-Endpoint.
- Nachdem Sie das VIP-Zertifikat aktualisiert haben, um eine Verbindung mit dem Supervisor herzustellen, melden Sie sich mithilfe der neu hinzugefügten FQDNs bei der Supervisor Control Plane an. Siehe Herstellen einer Verbindung mit dem Supervisor als vCenter Single Sign-On-Benutzer.

Weiterleiten von Supervisor-Protokollen an externe Überwachungssysteme

Erfahren Sie, wie Sie mit Fluent Bit die Weiterleitung der Protokolle der Supervisor-Control Plane an externe Überwachungssysteme wie Grafana Loki oder Elastic Search konfigurieren.

Protokolle der Supervisor-Control Plane werden mit Fluent Bit automatisch an den für die vCenter Server-Appliance konfigurierten Syslog-Server weitergeleitet. Fluent Bit ist ein leichtgewichtiger Open Source-Prozessor und -Forwarder für Protokolle und Metriken, der Konfigurationen zur Unterstützung verschiedener Protokolldatentypen, Filterung und Protokoll-Tag-Erweiterungen bereitstellt.

Während der Supervisor-Aktivierung oder einem -Upgrade werden Bootstrap-Protokolle weiterhin von rsyslog an die für die vCenter Server-Appliance konfigurierten Syslog-Server weitergeleitet. Sobald die VMs der Supervisor-Control Plane ausgeführt werden, wird Fluent Bit zur Standardprotokollweiterleitung für die Protokolle der Supervisor-Control Plane.

Als vSphere-Administrator können Sie Fluent Bit für Folgendes nutzen:

- Weiterleiten der Protokolle und Systemjournalprotokolle der Supervisor-Control Plane an wichtige externe Protokollüberwachungsplattformen wie Loki, Elastic Search, Grafana und andere Plattformen, die von Fluent Bit unterstützt werden.
- Aktualisieren oder Zurücksetzen der Konfiguration für die Protokollweiterleitung für die Supervisor-Control Plane über die k8s-API.

Fluent Bit wird als DeamonSet auf Knoten der Supervisor-Control Plane ausgeführt. Es stellt die ConfigMap `fluentbit-config-custom` unter dem Namespace `vmware-system-logging` bereit. Diese können vSphere-Administratoren bearbeiten, um die Protokollweiterleitung an externe Plattformen zu konfigurieren, indem sie Protokollserver definieren.

```
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
```

Anpassen der Fluent Bit-Protokollweiterleitung

Führen Sie folgende Schritte aus, um die Konfiguration der Fluent Bit-Protokollweiterleitung anzupassen:

1 Melden Sie sich bei der Supervisor-Control Plane als vCenter Single Sign-On-Administrator an.

```
> kubectl vsphere login --server=<supervisor-cluster-vip> -u administrator@vsphere.local
> kubectl config use-context <supervisor-cluster-vip>
```

2 Aktualisieren oder fügen Sie im Abschnitt `outputs-custom.conf` in der ConfigMap `fluentbit-config-custom` eine Syslog-Ausgabe hinzu, die alle Systemprotokolle der Control Plane-VM an einen externen Server weiterleitet.

```
[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 Wenden Sie die Änderungen der ConfigMap `fluentbit-config-custom` an.

```
> 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 Überwachen Sie den Fluent Bit-Pod, um die Konfigurationsänderungen automatisch anzuwenden. Fragen Sie Supervisor-Protokolle auf dem Syslog-Server ab. Falls das Fluentbit-DaemonSet nach dem erneuten Laden der aktualisierten Konfiguration fehlerhaft ausgeführt wird, reparieren Sie die Konfiguration oder setzen Sie sie in der ConfigMap `fluentbit-config-custom` zurück, um sicherzustellen, dass das Fluentbit-DaemonSet fehlerfrei ist.

```
> kubectl -n vmware-system-logging get pod
> kubectl -n vmware-system-logging logs <fluentbit-pod-name>
```

Weiterleiten von Überwachungsprotokollen des Kubernetes-API-Servers an einen Grafana Loki-Server

Führen Sie folgende Schritte aus, um die Protokollweiterleitung an einen externen Grafana Loki-Server zu konfigurieren:

1 Melden Sie sich bei der Supervisor-Control Plane als vCenter Single Sign-On-Administrator an.

```
> kubectl vsphere login --server=<supervisor-cluster-vip> -u administrator@vsphere.local
> kubectl config use-context <supervisor-cluster-vip>
```

2 Aktualisieren Sie eine Loki-Ausgabe im Abschnitt `outputs-custom.conf` in der ConfigMap `fluentbit-config-custom` bzw. fügen Sie eine Loki-Ausgabe hinzu. Dadurch werden alle Systemprotokolle der Control Plane-VM an den Loki-Protokollserver weitergeleitet.

```
[OUTPUT]
        Name loki
        Alias system_output_loki
        Match system*
        Host <loki-server-host>
        Port <loki-server-port>
        Labels $hostname,$appname,$filename,$procid,$labels
```

3 Wenden Sie die Änderungen der ConfigMap `fluentbit-config-custom` an.

```
> 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 Überwachen Sie den Fluent Bit-Pod, um die Konfigurationsänderungen automatisch anzuwenden. Fragen Sie Supervisor-Protokolle auf dem Syslog-Server ab. Falls das Fluentbit-DaemonSet nach dem erneuten Laden der aktualisierten Konfiguration fehlerhaft ausgeführt wird, reparieren Sie die Konfiguration oder setzen Sie sie in der ConfigMap `fluentbit-config-custom` zurück, um sicherzustellen, dass das Fluentbit-DaemonSet fehlerfrei ist.

```
> kubectl -n vmware-system-logging get pod
> kubectl -n vmware-system-logging logs <fluentbit-pod-name>
```

Weiterleiten von Protokollen an Elastic Search

Führen Sie folgende Schritte aus, um die Protokollweiterleitung an einen externen Elastic Search-Server zu konfigurieren:

1 Melden Sie sich bei der Supervisor-Control Plane als vCenter Single Sign-On-Administrator an.

```
> kubectl vsphere login --server=<supervisor-cluster-vip> -u administrator@vsphere.local
> kubectl config use-context <supervisor-cluster-vip>
```

2 Aktualisieren Sie eine Elastic Search-Ausgabe im Abschnitt `outputs-custom.conf` in der ConfigMap `fluentbit-config-custom` bzw. fügen Sie eine Elastic Search-Ausgabe hinzu. Dadurch werden alle Systemprotokolle der Control Plane-VM an den Elastic Search-Protokollserver weitergeleitet.

```
[OUTPUT]
       Name es
       Alias system_output_es
       Match system*
       Host <es-server-host>
       Port <es-server-port>
       Index supervisor
       Type controlplanevm
```

3 Wenden Sie die Änderungen der ConfigMap `fluentbit-config-custom` an.

```
> 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 Überwachen Sie den Fluent Bit-Pod, um die Konfigurationsänderungen automatisch anzuwenden. Fragen Sie Supervisor-Protokolle auf dem Syslog-Server ab.

```
> kubectl -n vmware-system-logging get pod
> kubectl -n vmware-system-logging logs <fluentbit-pod-name>
```

Weiterleiten von API-Überwachungsprotokollen an einen Syslog-Server

Führen Sie folgende Schritte aus, um die Weiterleitung von Überwachungsprotokollen der Kubernetes-API an einen externen Syslog-Server zu konfigurieren:

1 Fügen Sie die Eingaben `kubectl-plugin-vsphere` und `authproxy` zur ConfigMap `fluentbit-config` hinzu:

```
[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 Fügen Sie die Filter `kubectl-plugin-vsphere` und `authproxy` zur ConfigMap `fluentbit-config` hinzu:

```
[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 Fügen Sie die `kubectl-plugin-vsphere` für die Ausgabe an den Syslog-Server zur ConfigMap `fluentbit-config` hinzu:

```
[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 Fügen Sie die oben genannten Dateien in der ConfigMap `fluentbit-config` unter dem Namespace `vmware-system-logging` ein.

```
> 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
```

Bereitstellen eines Supervisor durch Klonen einer vorhandenen Konfiguration

13

Erfahren Sie, wie Sie einen Supervisor durch Klonen der Konfiguration einer vorhandenen Supervisor-Instanz bereitstellen. Klonen Sie einen Supervisor für den Fall, dass Sie eine neue Supervisor-Instanz mit ähnlichen Einstellungen wie einen bereits bereitgestellten Supervisor bereitstellen möchten.

Voraussetzungen

- Erfüllen Sie die Voraussetzungen zum Konfigurieren von vSphere-Clustern als Supervisor. Weitere Informationen finden Sie unter Voraussetzungen für die Konfiguration von vSphere IaaS control plane in vSphere-Cluster.
- Stellen Sie einen Supervisor bereit.

Verfahren

1. Navigieren Sie zu **Arbeitslastmanagement > Supervisor > Supervisoren**.
2. Wählen Sie den Supervisor aus, den Sie klonen möchten, und wählen Sie **Klonkonfiguration** aus.

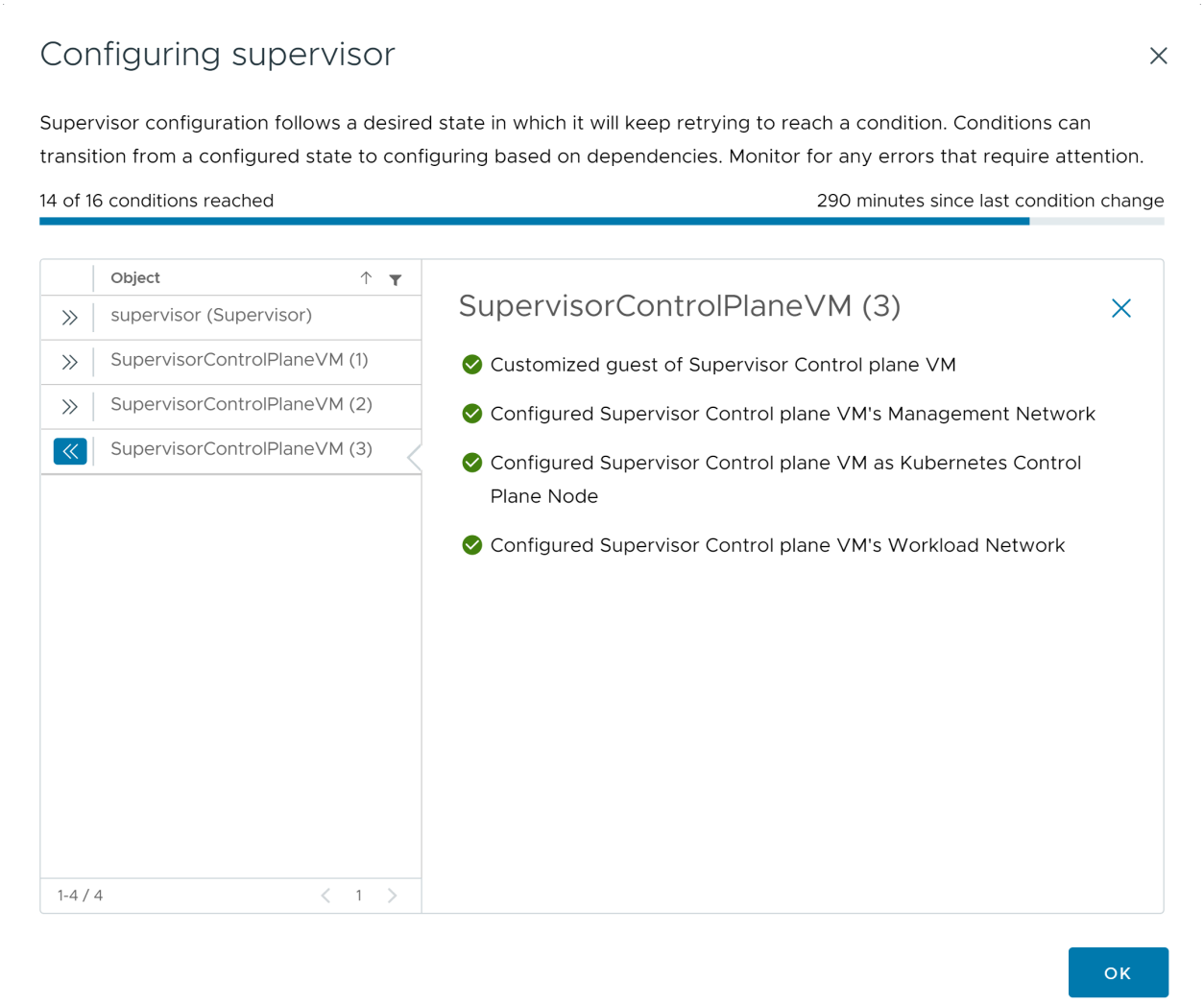
   Der Supervisor-Aktivierungsassistent wird geöffnet, wobei die Werte der ausgewählten Supervisor bereits ausgefüllt sind.
3. Gehen Sie durch den Assistenten, indem Sie die Werte nach Bedarf ändern.

   Weitere Informationen zu den Werten des Assistenten finden Sie unter Kapitel 5 Bereitstellen eines Supervisor für drei Zonen und Kapitel 6 Bereitstellen einer Supervisor für eine Zone .

Nächste Schritte

Sobald der Assistent zum Aktivieren eines Supervisors fertig ist, können Sie den Aktivierungsprozess verfolgen und nach potenzielle Problemen Ausschau halten, die eine Fehlerbehebung erfordern. Klicken Sie in der Spalte **Konfigurationsstatus** neben dem Status des Supervisors auf **Anzeigen**.

Abbildung 13-1. Supervisor-Aktivierungsansicht



Damit der Bereitstellungsvorgang abgeschlossen werden kann, muss der Supervisor den gewünschten Zustand erreichen, es müssen also alle 16 Bedingungen erfüllt sein. Wenn ein Supervisor erfolgreich aktiviert wurde, ändert sich sein Status von „Konfigurieren“ zu „Wird ausgeführt“. Während sich der Supervisor im Status „Konfigurieren“ befindet, wird kontinuierlich und wiederholt überprüft, ob alle 16 Bedingungen erfüllt sind. Wenn eine Bedingung nicht erfüllt wird, wird der Vorgang wiederholt, bis er erfolgreich ist. Aus diesem Grund kann sich die Anzahl der erreichten Bedingungen ändern. Beispiel: *10 von 16 Bedingungen wurden erfüllt*, dann *4 von 16 Bedingungen wurden erfüllt* usw. In sehr seltenen Fällen kann sich der Status in „Fehler“ ändern, wenn Fehler vorliegen, aufgrund derer der gewünschte Status nicht erreicht werden kann.

Weitere Informationen zu Bereitstellungsfehlern und zur Fehlerbehebung finden Sie unter Beheben von Fehlerzuständen auf den VMs einer Supervisor-Steuerungsebene während der Aktivierung oder Aktualisierung.

Fehlerbehebung bei der Supervisor-Aktivierung

14

Erfahren Sie, wie Sie Fehler bei der Aktivierung des Supervisors beheben, sodass der gewünschte Zustand erreicht wird und alle 16 Aktivierungsbedingungen erfüllt sind.

Lesen Sie als Nächstes die folgenden Themen:

- Beheben von Fehlerzuständen auf den VMs einer Supervisor-Steuerungsebene während der Aktivierung oder Aktualisierung
- Streamen von Protokollen der Supervisor-Steuerungsebene an ein Remote-rsyslog
- Beheben von Cluster-Kompatibilitätsfehlern bei der Aktivierung der Arbeitslastverwaltung
- Tailing der Protokolldatei der Arbeitslastverwaltung

Beheben von Fehlerzuständen auf den VMs einer Supervisor-Steuerungsebene während der Aktivierung oder Aktualisierung

Nachdem Sie einen Supervisor aktiviert haben, aktualisieren Sie die Supervisor-Kubernetes-Version, oder bearbeiten Sie die Einstellungen eines vorhandenen Supervisors. Alle von Ihnen angegebene Einstellungen werden validiert und auf den Supervisor angewendet, bis die Konfiguration abgeschlossen ist. Bei den eingegebenen Parametern werden Statusprüfungen durchgeführt, um etwaige Fehler in der Konfiguration aufzudecken, die zu einem Fehlerzustand des Supervisors führen könnten. Sie müssen diese Fehlerzustände beheben, damit der Supervisor konfiguriert oder aktualisiert werden kann.

Tabelle 14-1. vCenter Server-Verbindungsfehler

Fehlermeldung	Ursache	Lösung
Der Bezeichner des primären vCenter-Netzwerks <*FQDN*> kann mit dem bzw. den konfigurierten Verwaltungs-DNS-Server(n) in der Steuerungsebenen-VM <*VM-Name*> nicht aufgelöst werden. Überprüfen Sie, ob die Verwaltungs-DNS-Server <Servername> <*Netzwerkname*> auflösen können.	■ Mindestens ein Verwaltungs-DNS-Server ist erreichbar. ■ Mindestens ein Verwaltungs-DNS wird statisch bereitgestellt. ■ Die Verwaltungs-DNS-Server verfügen über keine Hostnamen-Lookups für die vCenter Server-PNID. ■ Die vCenter Server-PNID ist ein Domänenname, keine statische IP-Adresse.	■ Fügen Sie den Management-DNS-Servern einen Host-Eintrag für die vCenter Server-PNID hinzu. ■ Vergewissern Sie sich, dass die konfigurierten DNS-Server korrekt sind.
Der Bezeichner des primären vCenter-Netzwerks <*Netzwerkname*> mit dem bzw. den über DHCP im Verwaltungsnetzwerk der Steuerungsebenen-VM <*VM-Name*> erfassten DNS-Server(n) kann nicht aufgelöst werden. Überprüfen Sie, ob die Verwaltungs-DNS-Server <*Netzwerkname*> auflösen können.	■ Die vom DHCP-Server (mindestens einem) bereitgestellten Verwaltungs-DNS-Server sind erreichbar. ■ Die Verwaltungs-DNS-Server werden statisch bereitgestellt. ■ Die Verwaltungs-DNS-Server verfügen über keine Hostnamen-Lookups für die vCenter Server-PNID. ■ Die Verwaltungs-DNS-Server verfügen über keine Hostnamen-Lookups für die vCenter Server-PNID. ■ Die vCenter Server-PNID ist ein Domänenname, keine statische IP-Adresse.	■ Fügen Sie einen Host-Eintrag für die vCenter Server-PNID zu den Verwaltungs-DNS-Servern hinzu, die vom konfigurierten DHCP-Server bereitgestellt werden. ■ Überprüfen Sie, ob die vom DHCP-Server bereitgestellten DNS-Server korrekt sind.
Der Host <*Hostname*> in der Steuerungsebenen-VM <*VM-Name*> kann nicht aufgelöst werden, da keine konfigurierten Verwaltungs-DNS-Server vorhanden sind.	■ Die vCenter Server-PNID ist ein Domänenname, keine statische IP-Adresse. ■ Es sind keine DNS-Server konfiguriert.	Konfigurieren Sie einen Verwaltungs-DNS-Server.
Der Host <*Hostname*> in der Steuerungsebenen-VM <*VM-Name*>. Der Hostname endet mit der Top-Level-Domain „.local“. Hierzu ist es erforderlich, dass „local“ in die Suchdomänen des Verwaltungs-DNS aufgenommen wird.	Die vCenter Server-PNID enthält **`.local`** als Top-Level-Domäne (TLD), aber die konfigurierten Suchdomänen enthalten **`local`** nicht.	Fügen Sie **`local`** zu den Suchdomänen des Verwaltungs-DNS hinzu.

Tabelle 14-1. vCenter Server-Verbindungsfehler (Fortsetzung)

Fehlermeldung	Ursache	Lösung
Es kann keine Verbindung zu den Verwaltungs-DNS-Servern <*Servername*> von der Steuerungsebenen-VM <*VM-Name*> hergestellt werden. Der Verbindungsversuch erfolgte über das Arbeitslastnetzwerk.	■ Die Verwaltungs-DNS-Server können nicht mit vCenter Server verbunden werden. ■ Die angegebenen `worker_dns`-Werte enthalten vollständig die angegebenen Verwaltungs-DNS-Werte. Dies bedeutet, dass der Datenverkehr über das Arbeitslastnetzwerk geleitet wird, da der Supervisor eine Netzwerkschnittstelle auswählen muss, um statischen Datenverkehr zu diesen IPs zu leiten.	■ Überprüfen Sie im Arbeitslastnetzwerk, ob die Weiterleitung zu den konfigurierten Verwaltungs-DNS-Servern möglich ist. ■ Überprüfen Sie, ob keine konkurrierenden IP-Adressen vorhanden sind, die ein alternatives Routing zwischen den DNS-Servern und einigen anderen Servern im Arbeitslastnetzwerk auslösen könnten. ■ Überprüfen Sie, ob es sich bei dem konfigurierten DNS-Server tatsächlich um einen DNS-Server handelt und ob er seinen DNS-Port auf Port 53 hostet. ■ Überprüfen Sie, ob die Arbeitslast-DNS-Server so konfiguriert sind, dass Verbindungen von den IPs der Steuerungsebenen-VMs (den vom Arbeitslastnetzwerk bereitgestellten IPs) zugelassen werden. ■ Überprüfen Sie die Adressen der Verwaltungs-DNS-Server auf Schreibfehler. ■ Überprüfen Sie, ob die Suchdomänen kein unnötiges „~“ enthalten, das den Hostnamen falsch auflösen könnte.

Tabelle 14-1. vCenter Server-Verbindungsfehler (Fortsetzung)

Fehlermeldung	Ursache	Lösung
Es kann keine Verbindung zu den Verwaltungs-DNS-Servern <*Servername*> von der Steuerungsebenen-VM <*VM-Name*> hergestellt werden.	Es konnte keine Verbindung zu den DNS-Servern hergestellt werden.	■ Überprüfen Sie das Verwaltungsnetzwerk, um sicherzustellen, dass Routen zu den Verwaltungs-DNS-Servern vorhanden sind. ■ Überprüfen Sie, ob keine konkurrierenden IP-Adressen vorhanden sind, die ein alternatives Routing zwischen den DNS-Servern und anderen Servern auslösen könnten. ■ Überprüfen Sie, ob es sich bei dem konfigurierten DNS-Server tatsächlich um einen DNS-Server handelt und ob er seinen DNS-Port auf Port 53 hostet. ■ Überprüfen Sie, ob die Verwaltungs-DNS-Server so konfiguriert sind, dass Verbindungen von den IPs der Steuerungsebenen-VMs zugelassen werden. ■ Überprüfen Sie die Adressen der Verwaltungs-DNS-Server auf Schreibfehler. ■ Überprüfen Sie, ob die Suchdomänen kein unnötiges „~“ enthalten, das den Hostnamen falsch auflösen könnte.
Es kann keine Verbindung mit <*Komponentenname*> <*Komponentenadresse*> aus der Steuerungsebenen-VM <VM-Name> hergestellt werden. Fehler: *Text der Fehlermeldung*	■ Ein allgemeiner Netzwerkfehler ist aufgetreten. ■ Beim Herstellen der Verbindung mit vCenter Server ist ein Fehler aufgetreten.	■ Überprüfen Sie, ob der Hostname oder die IP-Adresse der konfigurierten Komponenten wie vCenter Server, HAProxy, NSX Manager oder NSX Advanced Load Balancer korrekt sind. ■ Überprüfen Sie alle externen Netzwerkeinstellungen, wie unter anderem konkurrierende IP-Adressen und Firewall-Regeln, im Verwaltungsnetzwerk.

Tabelle 14-1. vCenter Server-Verbindungsfehler (Fortsetzung)

Fehlermeldung	Ursache	Lösung
Die Steuerungsebenen-VM <*VM-Name*> konnte das vCenter <*vCenter Server-Name*>-Zertifikat nicht validieren. Das vCenter Server-Zertifikat ist ungültig.	Das von vCenter Server bereitgestellte Zertifikat hat ein ungültiges Format und ist daher nicht vertrauenswürdig.	■ Starten Sie `wcpsvc` erneut, um zu überprüfen, ob das Paket Trusted Roots in den Steuerungsebenen-VMs mit den neuesten vCenter Server-Stammzertifikaten auf dem neuesten Stand ist. ■ Überprüfen Sie, ob es sich bei dem vCenter Server-Zertifikat tatsächlich um ein gültiges Zertifikat handelt.
Die Steuerungsebenen-VM <*VM-Name*> vertraut dem vCenter <*vCenter Server-Name*>-Zertifikat nicht.	■ Das von vCenter Server präsentierte `vmca.pem`-Zertifikat entspricht nicht der Konfiguration für die Steuerungsebenen-VMs. ■ Die vertrauenswürdigen Stammzertifikate wurden in der vCenter Server Appliance ersetzt, aber `wcpsvc` wurde nicht neu gestartet.	■ Starten Sie `wcpsvc` erneut, um zu überprüfen, ob das Paket Zertifikat in den Steuerungsebenen-VMs mit den neuesten vCenter Server-Stammzertifikaten auf dem neuesten Stand ist.

Tabelle 14-2. NSX Manager-Verbindungsfehler

Die Steuerungsebenen-VM <*VM-Name*> konnte das NSX Server <*NSX Server-Name*>-Zertifikat nicht validieren. Der vom Server zurückgegebene Fingerabdruck <*NSX-T-Adresse*> stimmt nicht mit dem erwarteten Client-Zertifikatfingerabdruck in vCenter <*vCenter Server-Name*> überein.	Die beim Supervisor registrierten SSL-Fingerabdrücke stimmen nicht mit dem SHA-1-Hash des vom NSX Manager präsentierten Zertifikats überein.	■ Aktivieren Sie das Vertrauen in den NSX Manager zwischen NSX und der vCenter Server-Instanz erneut. ■ Starten Sie `wcpsvc` unter vCenter Server erneut.
Es kann keine Verbindung mit <*Komponentenname*> <*Komponentenadresse*> aus der Steuerungsebenen-VM <*VM-Name*> hergestellt werden. Fehler: *Text der Fehlermeldung*	Ein allgemeiner Netzwerkfehler ist aufgetreten.	■ Überprüfen Sie alle externen Netzwerkeinstellungen, konkurrierenden IP-Adressen, Firewall-Regeln usw. im Verwaltungsnetzwerk für den NSX Manager. ■ Überprüfen Sie, ob die IP des NSX Managers in der NSX-Erweiterung korrekt ist. ■ Stellen Sie sicher, dass der NSX Manager ausgeführt wird.

Tabelle 14-3. Fehler des Lastausgleichsdiensts

Die Steuerungsebenen-VM <*VM-Name*> vertraut nicht dem Zertifikat des Lastausgleichsdiensts (<*Lastausgleichsdienst*> – <*Lastausgleichsdienst-Endpoint*>).	Das vom Lastausgleichsdienst präsentierte Zertifikat unterscheidet sich von dem für die Steuerungsebenen-VMs konfigurierten Zertifikat.	Überprüfen Sie, ob Sie das richtige Verwaltungs-TLS-Zertifikat für den Lastausgleichsdienst konfiguriert haben.
Die Steuerungsebenen-VM <*VM-Name*> war nicht in der Lage, das Zertifikat des Lastausgleichsdiensts (<*Lastausgleichsdienst*> – <*Lastausgleichsdienst-Endpoint*> zu validieren. Das Zertifikat ist ungültig.	Das vom Lastausgleichsdienst präsentierte Zertifikat befindet sich in einem ungültigen Format oder ist abgelaufen.	Korrigieren Sie das Serverzertifikat des konfigurierten Lastausgleichsdiensts.
Die Steuerungsebenen-VM <*VM-Name*> konnte die Authentifizierung beim Lastausgleichsdienst (<*Lastausgleichsdienst*> – <*Lastausgleichsdienst-Endpoint*> mit dem Benutzernamen <*Benutzername*> und dem angegebenen Kennwort nicht durchführen.	Der Benutzername oder das Kennwort des Lastausgleichsdiensts ist falsch.	Überprüfen Sie die Anmeldedaten für den Lastausgleichsdienst (Benutzername und Kennwort) auf ihre Richtigkeit.
Bei dem Verbindungsversuch mit dem Lastausgleichsdienst (<*Lastausgleichsdienst*> – <*Lastausgleichsdienst-Endpoint*> aus der Steuerungsebenen-VM <*vm name*> ist ein HTTP-Fehler aufgetreten.	Die Steuerungsebenen-VMs können eine Verbindung zum Lastausgleichsdienst-Endpoint herstellen, aber der Endpoint gibt keine erfolgreiche (200) HTTP-Antwort zurück.	Überprüfen Sie den Zustand des Lastausgleichsdiensts und ob dieser Anforderungen annimmt.
Es kann keine Verbindung mit dem <*Lastausgleichsdienst*> (<*Lastausgleichsdienst-Endpoint*>) aus der Steuerungsebenen-VM <*VM-Name*> hergestellt werden. Fehler: <*Fehlertext*>	■ Ein allgemeiner Netzwerkfehler ist aufgetreten. ■ Typischerweise bedeutet dies, dass der Lastausgleichsdienst nicht funktioniert oder dass eine Firewall die Verbindung blockiert.	■ Überprüfen Sie, ob auf den Lastausgleichsdienst-Endpoint zugegriffen werden kann. ■ Prüfen Sie nach, ob keine Firewalls die Verbindung mit dem Lastausgleichsdienst blockieren.

Streamen von Protokollen der Supervisor-Steuerungsebene an ein Remote-rsyslog

Machen Sie sich mit der Konfiguration zum Streamen von Protokollen von den Supervisor-Steuerungsebenen-VMs zu einem Remote-rsyslog-Empfänger vertraut, um den Verlust wichtiger Protokollierungsdaten zu vermeiden.

Von den Komponenten in den Supervisor-Steuerungsebenen-VMs erzeugte Protokolle werden lokal in den Dateisystemen der VMs gespeichert. Wenn sich eine große Anzahl an Protokollen angesammelt hat, werden die Protokolle in hohem Tempo rotiert. Dies kann dazu führen, dass wichtige Nachrichten verloren gehen, die bei der Ermittlung der Hauptursache verschiedener

Probleme hilfreich sein könnten. vCenter Server und die Supervisor-Steuerungsebenen-VMs bieten Unterstützung für das Streamen ihrer lokalen Protokolle an einen Remote-rsyslog-Empfänger. Diese Funktion hilft bei der Erfassung von Protokollen für die folgenden Dienste und Komponenten:

- Auf vCenter Server: Dienst für die Arbeitslast-Steuerungsebene, ESX Agent Manager-Dienst, Zertifizierungsstellendienst und alle anderen Dienste unter vCenter Server.
- Komponenten der Supervisor-Steuerungsebene und eingebettete Supervisor-Dienste, wie z. B. der VM-Dienst und Tanzu Kubernetes Grid.

Sie können die vCenter Server Appliance so konfigurieren, dass lokale Protokolldaten erfasst und an einen Remote-rsyslog-Empfänger gestreamt werden. Nach Anwendung dieser Konfiguration auf vCenter Server beginnt der in vCenter Server ausgeführte rsyslog-Absender mit dem Senden von Protokollen, die von Diensten innerhalb dieses vCenter Server-Systems erzeugt wurden.

Supervisor verwendet denselben Mechanismus wie vCenter Server, um lokale Protokolle auszulagern und den Aufwand für die Konfigurationsverwaltung zu reduzieren. Der Dienst für die Arbeitslast-Steuerungsebene überwacht die Konfiguration des vCenter Server-rsyslog durch regelmäßiges Abrufen der Protokolle. Wenn der Dienst für die Arbeitslast-Steuerungsebene feststellt, dass die Konfiguration des vCenter Server-rsyslog nicht leer ist, gibt der Dienst diese Konfiguration an alle Steuerungsebenen-VMs in sämtlichen Supervisoren weiter. Hierdurch kann sehr hoher rsyslog-Meldungsverkehr entstehen, der zu einer Überlastung des Remote-rsyslog-Empfängers führen kann. Daher muss die Empfängermaschine über ausreichend Speicherkapazität verfügen, um große Mengen an rsyslog-Meldungen zu verarbeiten.

Durch Entfernen der rsyslog-Konfiguration aus vCenter Server werden rsyslog-Meldungen von vCenter Server angehalten. Der Dienst für die Arbeitslast-Steuerungsebene erkennt die Änderung und gibt sie an alle Steuerungsebenen-VMs in sämtlichen Supervisor weiter, wodurch letztlich auch die Streams der Steuerungsebenen-VMs angehalten werden.

Konfigurationsschritte

Führen Sie die folgenden Schritte aus, um rsyslog-Streaming für Supervisor-Steuerungsebenen-VMs zu konfigurieren:

1 Konfigurieren Sie einen rsyslog-Empfänger, indem Sie eine Maschine bereitstellen, die:
   - den rsyslog-Dienst im Empfängermodus ausführt. Weitere Informationen finden Sie im Beispiel Empfangen einer sehr hohen Anzahl an Meldungen mit hoher Leistung in der rsyslog-Dokumentation.
   - Über ausreichend Speicherplatz für große Mengen an Protokolldaten verfügt.
   - Über Netzwerkkonnektivität zum Empfangen von Daten aus vCenter Server und den Supervisor-Steuerungsebenen-VMs verfügt.
2 Melden Sie sich bei der Verwaltungsschnittstelle der vCenter Server Appliance unter *https://<vcenter Server address>:5480* als Root-Benutzer an.

3 Konfigurieren Sie vCenter Server für Streaming an den rsyslog-Empfänger über die Verwaltungsschnittstelle der vCenter Server Appliance. Weitere Informationen finden Sie unter Weiterleiten von vCenter Server-Protokolldateien an Remote-Syslog-Server.

Es kann einige Minuten dauern, bis die rsyslog-Konfiguration von vCenter Server auf die Supervisor-Steuerungsebenen-VMs angewendet wird. Der Dienst für die Arbeitslast-Steuerungsebene auf der vCenter Server Appliance fragt die Appliance-Konfiguration alle 5 Minuten ab und gibt sie an alle verfügbaren Supervisoren weiter. Die Zeit bis zum Abschließen der Weitergabe richtet sich nach der Anzahl der Supervisoren in Ihrer Umgebung. Wenn einige der Steuerungsebenen-VMs auf den Supervisoren fehlerhaft sind oder einen anderen Vorgang ausführen, wendet der Dienst für die Arbeitslast-Steuerungsebene die rsyslog-Konfiguration solange an, bis sie erfolgreich ausgeführt wird.

Überprüfen der Protokolle der Komponenten von Steuerungsebenen-VMs

Das rsyslog der Supervisor-Steuerungsebenen-VMs bettet Tags in die Protokollmeldungen ein, die die Quellkomponente dieser Protokollmeldungen angeben.

Protokoll-Tags	Beschreibung
`vns-control-plane-pods <pod_name>/ <instance_number>.log`	Protokolle, die aus Kubernetes-Pods in Steuerungsebenen-VMs stammen. Beispiel: `vns-control-plane-pods etcd/0.log` oder `vns-control-plane-pods nsx-ncp/573.log`
`vns-control-plane-imc`	Protokolle der Erstkonfiguration aus Steuerungsebenen-VMs.
`vns-control-plane-boostrap`	Bootstrap-Protokolle aus der Steuerungsebenenbereitstellung von Kubernetes-Knoten.
`vns-control-plane-upgrade-logs`	Protokolle aus Patches der Steuerungsebenenknoten und Upgrades von Nebenversionen.
`vns-control-plane-svchost-logs`	Host- oder Agent-Protokolle der Steuerungsebenen-VM auf Systemebene.
`vns-control-plane-update-controller`	Synchronisierungs- und Realisierungsprotokoll für den gewünschten Zustand der Steuerungsebene.
`vns-control-plane-compact-etcd-logs`	Protokolle zur Beibehaltung der Speicherkomprimierung für den etcd-Dienst der Steuerungsebene.

Beheben von Cluster-Kompatibilitätsfehlern bei der Aktivierung der Arbeitslastverwaltung

Befolgen Sie diese Tipps zur Fehlerbehebung, wenn das System angibt, dass Ihr vSphere-Cluster nicht für die Aktivierung der Arbeitslastverwaltung kompatibel ist.

Problem

Auf der Seite **Arbeitslastverwaltung** wird angegeben, dass Ihr vCenter Cluster nicht kompatibel ist, wenn Sie versuchen, die Arbeitslastverwaltung zu aktivieren.

Ursache

Dieser Fehler kann mehrere Gründe haben. Stellen Sie zunächst sicher, dass Ihre Umgebung die Mindestanforderungen für die Aktivierung der Arbeitslastverwaltung erfüllt:

- Gültige Lizenz: VMware vSphere 7 Enterprise Plus mit Add-On für Kubernetes
- Mindestens zwei ESXi-Hosts
- Vollautomatisiertes DRS
- vSphere HA
- vSphere Distributed Switch 7.0
- Ausreichende Speicherkapazität

Wenn Ihre Umgebung diese Voraussetzungen erfüllt, der vCenter-Zielcluster jedoch nicht kompatibel ist, verwenden Sie VMware Datacenter CLI (DCLI), um die Probleme zu identifizieren.

Lösung

1. SSH für vCenter Server.
2. Melden Sie sich als Root-Benutzer an.
3. Führen Sie den Befehl `dcli` aus, um die Hilfe von VMware Datacenter CLI anzuzeigen.
4. Listen Sie die verfügbaren vCenter-Cluster auf, indem Sie den folgenden DCLI-Befehl ausführen.

   ```
   dcli com vmware vcenter cluster list
   ```

   Beispiel:

   ```
   dcli +username VI-ADMIN-USER-NAME +password VI-ADMIN-PASSWORD com vmware vcenter cluster
   list
   ```

   Beispielergebnis:

   ```
   |-----------|---------|------------|----------|
   |drs_enabled|cluster  |name        |ha_enabled|
   |-----------|---------|------------|----------|
   |True       |domain-d7|vSAN Cluster|True      |
   |-----------|---------|------------|----------|
   ```

5 Überprüfen Sie die Kompatibilität der vCenter-Cluster, indem Sie den folgenden DCLI-Befehl ausführen.

```
dcli com vmware vcenter namespacemanagement clustercompatibility list
```

Beispiel:

```
dcli +username VI-ADMIN-USER-NAME +password VI-ADMIN-PASSWORD com vmware vcenter
namespacemanagement clustercompatibility list
```

Das folgende Beispielergebnis weist darauf hin, dass in der Umgebung ein kompatibler NSX-VDS-Switch fehlt.

```
|---------|----------|-----------------------------------------------------------------------
------------------|
|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 Führen Sie je nach Bedarf weitere DCLI-Befehle aus, um weitere Kompatibilitätsprobleme zu ermitteln. Zusätzlich zu den NSX-Fehlern sind DNS- und NTP-Konnektivitätsprobleme häufige Gründe für die Inkompatibilität.

7 Führen Sie zur weiteren Fehlerbehebung die folgenden Schritte aus.

a Führen Sie ein Tailing der Datei `wcpsvc.log` durch. Weitere Informationen hierzu finden Sie unter Tailing der Protokolldatei der Arbeitslastverwaltung.

b Navigieren Sie zur Seite **Arbeitslastverwaltung** und klicken Sie auf **Aktivieren**.

Tailing der Protokolldatei der Arbeitslastverwaltung

Das Tailing der Protokolldatei der Arbeitslastverwaltung kann bei der Behebung von Aktivierungsproblemen und Problemen bei der Supervisor-Bereitstellung nützlich sein.

Lösung

1 Stellen Sie eine SSH-Verbindung mit der vCenter Server Appliance her.

2 Melden Sie sich als `root`-Benutzer an.

3 Führen Sie den Befehl `shell` aus.

Es wird Folgendes angezeigt:

```
Shell access is granted to root
root@localhost [ ~ ]#
```

4 Führen Sie den folgenden Befehl aus, um das Tailing des Protokolls durchzuführen.

```
tail -f /var/log/vmware/wcp/wcpsvc.log
```

Fehlerbehebung beim Netzwerk 15

Sie können Probleme bei Netzwerken und Lastausgleichsdiensten beheben, die bei der Aktivierung von Supervisor auftreten können.

Lesen Sie als Nächstes die folgenden Themen:

- vCenter Server bei NSX Manager erneut registrieren
- Erfassen von Support-Paketen für die NSX Advanced Load Balancer-Fehlerbehebung
- Für den Datenverkehr des Hosttransportknotens erforderlicher VDS

vCenter Server bei NSX Manager erneut registrieren

Möglicherweise müssen Sie vCenter Server OIDC mit NSX Manager in bestimmten Situationen erneut registrieren, z. B. wenn sich der FQDN/die PNID von vCenter Server ändert.

Verfahren

1. Stellen Sie über SSH eine Verbindung mit der vCenter Server Appliance her.
2. Führen Sie den Befehl `shell` aus.
3. Um den vCenter Server-Fingerabdruck zu aktualisieren, führen Sie den folgenden Befehl aus:

   ```
   - openssl s_client -connect vcenterserver-FQDN:443 </dev/null 2>/dev/null | openssl x509
   -fingerprint -sha256 -noout -in /dev/stdin
   ```

   Der Fingerabdruck wird angezeigt. Beispielsweise `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. Kopieren Sie den SHA256-Fingerabdruck und entfernen Sie die Kommas.

   `08774329E4D16F2996785FBFD64521F40E3B2A680599C3A4898FF20BEA3ABE9D`
5. Führen Sie zum Aktualisieren des OIDC von vCenter Server folgenden Befehl aus:

   ```
   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>"
    }'
```

Das Kennwort der NSX-Appliance kann nicht geändert werden

Möglicherweise können Sie das NSX-Appliance-Kennwort für `root`-, `admin`- oder `audit`-Benutzer nicht ändern.

Problem

Versuche, das Kennwort der NSX-Appliance für `root`-, `admin`- oder `audit`-Benutzer über den vSphere Client zu ändern, schlagen möglicherweise fehl.

Ursache

Während der Installation von NSX Manager akzeptiert der Vorgang nur ein Kennwort für alle drei Rollen. Versuche, dieses Kennwort später zu ändern, schlagen möglicherweise fehl.

Lösung

- Verwenden Sie die NSX-APIs, um die Kennwörter zu ändern.

  Weitere Informationen finden Sie unter https://kb.vmware.com/s/article/70691 und im *Administratorhandbuch für NSX*.

Fehlerbehebung bei fehlgeschlagenen Workflows und instabilen NSX Edges

Wenn Ihre Workflows fehlschlagen oder die NSX Edges instabil sind, können Sie Fehlerbehebungsschritte durchführen

Problem

Wenn Sie die Konfiguration für verteilte Portgruppen im vSphere Client ändern, können Workflows fehlschlagen und der NSX Edge instabil werden.

Ursache

Das Entfernen oder Ändern der verteilten Portgruppen für Overlay und Uplink, die während der Konfiguration des NSX Edge-Clusters für die Clusterkonfiguration erstellt wurden, ist aufbaubedingt nicht zulässig.

Lösung

Wenn Sie die VLAN- oder IP-Pool-Konfiguration von NSX Edges ändern möchten, müssen Sie zuerst Elemente von NSX und die vSphere IaaS control plane-Konfiguration aus dem Cluster entfernen.

Informationen zum Entfernen von NSX-Elementen finden Sie im *Installationshandbuch für NSX*.

Erfassen von Support-Paketen für die NSX-Fehlerbehebung

Sie können Support-Pakete in registrierten Cluster- und Fabric-Knoten für die Fehlerbehebung erfassen und die Pakete auf Ihren Computer herunterladen oder auf einen Dateiserver hochladen.

Wenn Sie die Pakete auf Ihren Computer herunterladen möchten, erhalten Sie eine einzelne Archivdatei, die aus einer Manifestdatei und Support-Paketen für jeden Knoten besteht. Wenn Sie die Pakete auf einen Dateiserver hochladen, werden die Manifestdatei und die einzelnen Pakete separat auf den Dateiserver hochgeladen.

Verfahren

1. Melden Sie sich über Ihren Browser mit Administratorrechten bei NSX Manager an.
2. Wählen Sie **System > Support-Paket** aus.
3. Wählen Sie die Zielknoten aus.

   Die verfügbaren Knotentypen sind **Verwaltungsknoten**, **Edges**, **Hosts** und **Public Cloud-Gateways**.
4. (Optional) Geben Sie das Protokollalter in Tagen an, um Protokolle auszuschließen, die älter als die angegebene Anzahl an Tagen sind.
5. (Optional) Schalten Sie den Switch um, der angibt, ob Core-Dateien und Überwachungsprotokolle einbezogen oder ausgeschlossen werden sollen.

   Hinweis Core-Dateien und Überwachungsprotokolle enthalten möglicherweise vertrauliche Informationen, wie z. B. Kennwörter oder Verschlüsselungsschlüssel.
6. (Optional) Aktivieren Sie das Kontrollkästchen, um die Pakete auf einen Dateiserver hochzuladen
7. Klicken Sie auf **Paketerfassung starten**, um Support-Pakete zu erfassen.

   Die Anzahl der Protokolldateien für jeden Knoten bestimmt die Zeit, die die Erfassung von Support-Paketen in Anspruch nimmt.
8. Überwachen Sie den Status des Erfassungsvorgangs.

   Die Registerkarte **Status** zeigt den Fortschritt der Erfassung von Support-Paketen an.
9. Klicken Sie auf **Herunterladen**, um das Paket herunterzuladen, wenn die Option zum Senden des Pakets an einen Dateiserver nicht festgelegt wurde.

Erfassen von Protokolldateien für NSX

Sie können Protokolle erfassen, die sich in den vSphere IaaS control plane- und NSX-Komponenten befinden, um Fehler zu erkennen und zu beheben. Die Protokolldateien werden möglicherweise vom VMware Support angefordert.

Verfahren

1. Melden Sie sich über vSphere Client bei vCenter Server an.

2 Erfassen Sie die folgenden Protokolldateien.

Protokolldatei	Beschreibung
/var/log/vmware/wcp/wcpsvc.log	Enthält Informationen im Zusammenhang mit der vSphere IaaS control plane-Aktivierung.
/var/log/vmware/wcp/nsxd.log	Enthält Informationen im Zusammenhang mit der Konfiguration der NSX-Komponenten.

3 Melden Sie sich bei NSX Manager an.

4 Erfassen Sie die Daten in der Datei `/var/log/proton/nsxapi.log`, um Informationen zu dem Fehler zu erhalten, der von NSX Manager zurückgegeben wird, wenn ein bestimmter vSphere IaaS control plane-Vorgang fehlgeschlagen ist.

Neustarten des WCP-Diensts bei Änderung des NSX-Verwaltungszertifikats, Fingerabdrucks oder der IP-Adresse

Wenn sich das NSX-Verwaltungszertifikat, der Fingerabdruck oder die IP-Adresse ändert, nachdem Sie vSphere IaaS control plane installiert haben, müssen Sie den `WCP`-Dienst neu starten.

Neustarten des vSphere IaaS control plane-Diensts bei Änderung des NSX-Zertifikats

Derzeit erfordert vSphere IaaS control plane, dass bei Änderung des NSX-Zertifikats, -Fingerabdrucks oder der NSX-IP-Adresse der `WCP`-Dienst neu gestartet wird, damit die Änderungen wirksam werden. Wenn eine der beiden Änderungen ohne einen Neustart des Diensts stattfindet, schlägt die Kommunikation zwischen vSphere IaaS control plane und NSX fehl, und es können bestimmte Symptome auftreten, z. B., dass NCP in die CrashLoopBackoff-Phase eintritt oder dass die Bereitstellung von Supervisor-Ressourcen aufgehoben wird.

Verwenden Sie zum Neustarten des `WCP`-Diensts `vmon-cli`.

1 Greifen Sie per SSH auf den vCenter Server zu und melden Sie sich als „root“-Benutzer an.

2 Führen Sie den Befehl `shell` aus.

3 Führen Sie den Befehl `vmon-cli -h` aus, um die Syntax für die Verwendung und die Optionen anzuzeigen.

4 Führen Sie den Befehl `vmon-cli -l` aus, um den `wcp`-Prozess anzuzeigen.

   Der `wcp`-Dienst wird am Ende der Liste angezeigt.

5 Führen Sie den Befehl `vmon-cli --restart wcp` aus, um den `wcp`-Dienst neu zu starten.

   Folgende Meldung wird angezeigt: `Completed Restart service request`.

6 Führen Sie den Befehl `vmon-cli -s wcp` aus und überprüfen Sie, ob der `wcp`-Dienst gestartet wurde.

Beispiel:

```
root@localhost [ ~ ]# vmon-cli -s wcp
Name: wcp
Starttype: AUTOMATIC
RunState: STARTED
RunAsUser: root
CurrentRunStateDuration(ms): 22158
HealthState: HEALTHY
FailStop: N/A
MainProcessId: 34372
```

Erfassen von Support-Paketen für die NSX Advanced Load Balancer-Fehlerbehebung

Für die Fehlerbehebung von NSX Advanced Load Balancer-Problemen können Sie Support-Pakete erfassen. Die Support-Pakete werden möglicherweise vom VMware Support angefordert.

Wenn Sie das Support-Paket generieren, erhalten Sie eine einzelne Datei für die Debug-Protokolle, die Sie herunterladen können.

Verfahren

1. Klicken Sie im NSX Advanced Load Balancer Controller-Dashboard auf das Menü in der oberen linken Ecke und wählen Sie **Verwaltung** aus.
2. Wählen Sie im Abschnitt **Verwaltung** die Option **System** aus.
3. Wählen Sie auf dem Bildschirm **System** die Option **Tech Support** aus.
4. Um ein Diagnosepaket zu generieren, klicken Sie auf **Tech Support erstellen**.
5. Wählen Sie im Fenster **Tech-Support erstellen** den Typ **Debug-Protokolle** aus und klicken Sie auf **Erstellen**.
6. Sobald das Paket erstellt wurde, klicken Sie auf das Downloadsymbol, um es auf Ihren Computer herunterzuladen.

   Weitere Informationen zur Erfassung von Protokollen finden Sie unter https://avinetworks.com/docs/21.1/collecting-tech-support-logs/.

NSX Advanced Load Balancer Konfiguration wird nicht angewendet

Wenn Sie den Supervisor bereitstellen, wird die Bereitstellung nicht abgeschlossen und die NSX Advanced Load Balancer-Konfiguration nicht angewendet.

Problem

Die Konfiguration von NSX Advanced Load Balancer wird nicht angewendet, wenn Sie ein von einer privaten Zertifizierungsstelle signiertes Zertifikat bereitstellen.

Möglicherweise wird eine Fehlermeldung mit `Unable to find certificate chain` in den Protokolldateien eines der NCP-Pods angezeigt, die auf dem Supervisor ausgeführt werden.

1 Melden Sie sich bei der Supervisor-VM an.

2 Anzeigen aller Pods mit dem Befehl `kubectl get pods -A`

3 Rufen Sie die Protokolle von allen NCP-Pods auf dem Supervisor ab.

```
kubectl -n vmware-system-nsx logs nsx-ncp-<id> | grep -i alb
```

Ursache

Das Java SDK wird verwendet, um die Kommunikation zwischen NCP und dem NSX Advanced Load Balancer Controller herzustellen. Dieser Fehler tritt auf, wenn der NSX Trust Store nicht mit dem Trust Store des Java-Zertifikats synchronisiert ist.

Lösung

1 Exportieren Sie das Stamm-CA-Zertifikat aus dem NSX Advanced Load Balancer und speichern Sie es im NSX Manager.

2 Melden Sie sich als Root-Benutzer an NSX Manager an.

3 Führen Sie auf allen NSX Manager-Knoten nacheinander die folgenden Befehle aus.

```
keytool -importcert -alias startssl -keystore /usr/lib/jvm/jre/lib/security/cacerts
-storepass changeit -file <ca-file-path>
```

Wenn der Pfad nicht gefunden wird, führen Sie `keytool -importcert -alias startssl -keystore /usr/java/jre/lib/security/cacerts -storepass changeit -file <ca-file-path>` aus.

```
sudo cp <ca-file-path> /usr/local/share/ca-certificates/
sudo update-ca-certificates
service proton restart
```

Hinweis Sie können die gleichen Schritte ausführen, um ein CA-Zwischenzertifikat zuzuweisen.

4 Warten Sie, bis die Supervisor-Bereitstellung abgeschlossen ist. Wenn die Bereitstellung nicht erfolgt, stellen Sie ihn erneut bereit.

ESXi Host kann nicht in den Wartungsmodus wechseln

Sie versetzten einen ESXi-Host in den Wartungsmodus, wenn Sie ein Upgrade durchführen möchten.

Problem

Der ESXi-Host kann nicht in den Wartungsmodus wechseln, und dies kann sich auf das ESXi- und das NSX-Upgrade auswirken.

Ursache

Dieser Fall kann auftreten, wenn auf dem ESXi-Host eine Dienst-Engine vorhanden ist, die sich in einem eingeschalteten Zustand befindet.

Lösung

- Schalten Sie die Dienst-Engine aus, damit der ESXi-Host in den Wartungsmodus wechseln kann.

Fehlerbehebung bei Problemen mit IP-Adressen

Befolgen Sie diese Tipps zur Fehlerbehebung, wenn Probleme bei der Zuweisung externer IP-Adressen auftreten.

Probleme mit der IP-Adresse können aus den folgenden Gründen auftreten:

- Kubernetes-Ressourcen, wie z. B. die Gateways und der Ingress, erhalten keine externe IP-Adresse vom AKO.
- Externe IPs, die Kubernetes-Ressourcen zugewiesen sind, sind nicht erreichbar.
- Externe IPs, die falsch zugewiesen sind.

Kubernetes-Ressourcen erhalten keine externe IP vom AKO

Dieser Fehler tritt auf, wenn AKO den entsprechenden virtuellen Dienst im NSX Advanced Load Balancer Controller nicht erstellen kann.

Überprüfen Sie, ob der AKO-Pod ausgeführt wird. Wenn der Pod ausgeführt wird, überprüfen Sie die AKO-Containerprotokolle auf den Fehler.

Externe IPs, die Kubernetes-Ressourcen zugewiesen sind, sind nicht erreichbar

Dieser Zustand kann aus folgenden Gründen auftreten:

- Die externe IP-Adresse ist nicht sofort verfügbar, beginnt jedoch innerhalb weniger Minuten nach der Erstellung mit der Annahme des Datenverkehrs. Dies tritt auf, wenn die Erstellung einer neuen Dienst-Engine für die Platzierung des virtuellen Diensts ausgelöst wird.
- Die externe IP ist nicht verfügbar, da der entsprechende virtuelle Dienst einen Fehler anzeigt.

Ein virtueller Dienst kann auf einen Fehler hinweisen oder rot angezeigt werden, wenn sich keine Server im Pool befinden. Dies kann auftreten, wenn das Kubernetes-Gateway oder die Ingress-Ressource nicht auf ein Endpoint-Objekt verweist.

Um die Endpoints anzuzeigen, führen Sie den Befehl `kubectl get endpoints -n <servce_namespace>` aus und beheben Sie alle Probleme bei der Auswahlbezeichnung.

Der Pool kann mit einem Fehlerzustand angezeigt werden, wenn die Integritätsüberwachung die Integrität der Poolserver als rot anzeigt.

Führen Sie zum Beheben des Problems einen der folgenden Schritte durch.

- Überprüfen Sie, ob die Poolserver oder Kubernetes-Pods den konfigurierten Port überwachen.
- Stellen Sie sicher, dass in der NSX DFW-Firewall keine Drop-Regeln vorhanden sind, die eingehenden oder ausgehenden Datenverkehr auf die Dienst-Engine blockieren.
- Stellen Sie sicher, dass in der Kubernetes-Umgebung keine Netzwerkrichtlinien vorhanden sind, die eingehenden oder ausgehenden Datenverkehr auf den Dienst-Engines blockieren.

Zu den Problemen des Dienstmoduls gehören die folgenden:

1 Die Erstellung von Dienstmodulen schlägt fehl.

   Die Erstellung von Dienst-Engines kann aus den folgenden Gründen fehlschlagen:

   - Eine Lizenz mit unzureichenden Ressourcen wird im NSX Advanced Load Balancer Controller verwendet.
   - Die Anzahl der in einer Dienst-Engine-Gruppe erstellten Dienst-Engines hat den maximalen Grenzwert erreicht.
   - Die Daten-Netzwerkkarte der Dienst-Engine konnte die IP nicht abrufen.

2 Die Erstellung der Dienst-Engine schlägt mit einer `Insufficient licensable resources available`-Fehlermeldung fehl.

   Dieser Fehler tritt auf, wenn eine Lizenz mit unzureichenden Ressourcen zum Erstellen der Dienst-Engine verwendet wurde.

   Rufen Sie eine -Lizenz mit einem größeren Ressourcenkontingent ab und weisen Sie sie dem NSX Advanced Load Balancer Controller zu.

3 Die Erstellung der Dienst-Engine schlägt mit einer `Reached configuration maximum limit`-Fehlermeldung fehl.

   Dieser Fehler tritt auf, wenn die Anzahl der in einer Dienst-Engine-Gruppe erstellten Dienst-Engines den maximalen Grenzwert erreicht hat.

   Um dieses Problem zu beheben, führen Sie die folgenden Schritte aus:

   a Wählen Sie im NSX Advanced Load Balancer Controller-Dashboard **Infrastruktur > Cloud-Ressourcen > Dienst-Engine-Gruppe** aus.

   b Suchen Sie die Dienst-Engine-Gruppe mit demselben Namen wie der Supervisor, in dem der IP-Datenverkehrsfehler auftritt, und klicken Sie auf das Symbol **Bearbeiten**.

   c Konfigurieren Sie einen höheren Wert für **Anzahl der Dienst-Engines**.

4 Die Daten-Netzwerkkarte der Dienst-Engine kann keine IP abrufen.

   Dieser Fehler kann auftreten, wenn der DHCP-IP-Pool aus einem der folgenden Gründe ausgeschöpft ist:

   - Für eine umfangreiche Bereitstellung wurden zu viele Dienst-Engines erstellt.

- Wenn eine Dienst-Engine direkt über die NSX Advanced Load Balancer-Benutzeroberfläche oder die vSphere Client gelöscht wird. Ein solcher Löschvorgang gibt die DHCP-Adresse nicht aus dem DHCP-Pool frei und führt zu einem Fehler bei der LEASE-Zuteilung.

Externe IPs sind falsch zugewiesen

Dieser Fehler tritt auf, wenn zwei Ingresses in unterschiedlichen Namespaces denselben Hostnamen verwenden. Überprüfen Sie Ihre Konfiguration und stellen Sie sicher, dass nicht zwei Ingresses in unterschiedlichen Namespaces derselbe Name zugewiesen wird.

Beheben von Problemen mit Datenverkehrsfehlern

Nachdem Sie den NSX Advanced Load Balancer konfiguriert haben, treten Datenverkehrsfehler auf.

Problem

Datenverkehrsfehler können auftreten, wenn sich der Endpoint für den Dienst vom Typ LB in einem anderen Namespace befindet.

Ursache

In vSphere IaaS control plane-Umgebungen, die mit NSX Advanced Load Balancer konfiguriert sind, verfügen Namespaces über ein dediziertes Tier-1-Gateway und jedes Tier-1-Gateway verfügt über ein Dienst-Engine-Segment mit demselben CIDR. Datenverkehrsfehler können auftreten, wenn sich der NSX Advanced Load Balancer-Dienst in einem Namespace befindet und die Endpoints sich in einem anderen Namespace befinden. Der Fehler tritt auf, weil der NSX Advanced Load Balancer dem Dienst eine externe IP-Adresse zuordnet und der Datenverkehr zu dieser externen IP fehlschlägt.

Lösung

- Um Nord-Süd-Datenverkehr zuzulassen, erstellen Sie eine Regel für die verteilte Firewall, die den Ingress von der SNAT-IP des Dienst-Namespaces von NSX Advanced Load Balancer zulässt.

Fehlerbehebung bei Problemen, die durch Sicherung und Wiederherstellung von NSX verursacht werden

NSX Sicherung und Wiederherstellung kann zu einem Ausfall des Datenverkehrs für alle externen IPs führen, die vom NSX Advanced Load Balancer bereitgestellt werden.

Problem

Wenn Sie eine Sicherung und Wiederherstellung von NSX durchführen, kann dies zu einem Ausfall des Datenverkehrs führen.

Ursache

Dieser Fehler tritt auf, da die Dienst-Engine-Netzwerkkarten nach einer Wiederherstellung nicht wieder verfügbar sind und der IP-Pool daher als ausgefallen angezeigt wird.

Lösung

1. Wählen Sie im NSX Advanced Load Balancer Controller-Dashboard **Infrastruktur > Clouds** aus.
2. Wählen Sie die Cloud aus und speichern Sie sie, ohne Änderungen vorzunehmen, und warten Sie, bis der Status grün wird.
3. Deaktivieren Sie alle virtuellen Dienste.

   Warten Sie, bis der NSX Advanced Load Balancer Controller die veralteten Netzwerkkarten aus allen Dienst-Engines entfernt hat.
4. Aktivieren Sie alle virtuellen Dienste.

   Die Status der virtuellen Dienste werden grün angezeigt.

   Wenn der Datenverkehr weiterhin fehlschlägt, konfigurieren Sie die statischen Routen im NSX Manager neu.

Veraltete Tier-1-Segmente nach NSX-Sicherung und -Wiederherstellung

Bei der NSX-Sicherung und -Wiederherstellung kann es zur Wiederherstellung veralteter Tier-1-Segmente kommen.

Problem

Nach einem NSX-Sicherungs- und -Wiederherstellungsvorgangs werden veraltete Tier-1-Segmente, die Dienst-Engine-Netzwerkkarten aufweisen, nicht bereinigt.

Ursache

Wenn ein Namespace nach einer NSX-Sicherung gelöscht wird, stellt der Wiederherstellungsvorgang veraltete Tier-1-Segmente wieder her, die den Dienst-Engine-Netzwerkkarten des NSX Advanced Load Balancer Controllers zugeordnet sind.

Lösung

1. Melden Sie sich beim NSX Manager an.
2. Wählen Sie **Netzwerk > Segmente** aus.
3. Suchen Sie die veralteten Segmente, die mit dem gelöschten Namespace verknüpft sind.
4. Löschen Sie die veralteten Dienst-Engine-Netzwerkkarten aus dem Abschnitt **Ports/ Schnittstellen**.

Für den Datenverkehr des Hosttransportknotens erforderlicher VDS

vSphere IaaS control plane erfordert die Verwendung eines vSphere 8,0 Virtual Distributed Switch (VDS) für den Datenverkehr des Hosttransportknotens. Für den Datenverkehr des Hosttransportknotens mit vSphere IaaS control plane können Sie nicht den NSX-VDS (N-VDS) verwenden.

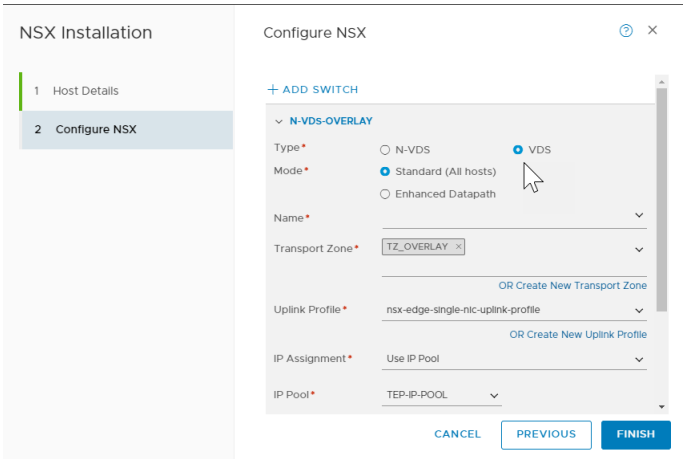
VDS ist erforderlich

vSphere IaaS control plane erfordert eine Converged VDS-Instanz, die sowohl vSphere-Datenverkehr als auch NSX-Datenverkehr in derselben VDS-Instanz unterstützt. In früheren Versionen von vSphere und NSX gibt es eine VDS (oder VSS)-Instanz für vSphere-Datenverkehr und eine N-VDS-Instanz für NSX-Datenverkehr. Diese Konfiguration wird von vSphere IaaS control plane nicht unterstützt. Wenn Sie versuchen, die Arbeitslastverwaltung unter Verwendung einer N-VDS-Instanz zu aktivieren, meldet das System, dass der vCenter-Cluster nicht kompatibel ist. Weitere Informationen finden Sie unter Beheben von Cluster-Kompatibilitätsfehlern bei der Aktivierung der Arbeitslastverwaltung.

Um eine Converged VDS-Instanz zu verwenden, erstellen Sie mithilfe von vCenter einen vSphere 8.0 vDS. Geben Sie dann diesen VDS in NSX an, wenn Sie die ESXi-Hosts als Transportknoten vorbereiten. VDS-DSwitch allein reicht für vCenter nicht aus. VDS-DSwitch 8.0 muss, wie im Thema Erstellen eines Transportknotenprofils dokumentiert und nachstehend dargestellt, mit NSX-Transportknotenprofil konfiguriert werden.

Weitere Informationen zum Vorbereiten von ESXiHosts als Transportknoten finden Sie unter https://kb.vmware.com/s/article/95820 und Vorbereiten von ESXi-Hosts als Transportknoten in der NSX-Dokumentation.

Abbildung 15-1. VDS-Konfiguration in NSX



Wenn Sie ein Upgrade von früheren Versionen auf vSphere 8.0 und NSX 4.x ausgeführt haben, müssen Sie N-VDS von allen ESXi-Transportknoten deinstallieren und die einzelnen Hosts mit einem VDS neu konfigurieren. Weitere Informationen erhalten Sie bei VMware Global Support Services.

Fehlerbehebung für vSphere IaaS control plane

16

Wenden Sie die folgenden Best Practices und Fehlerbehebungsverfahren für Ihre Infrastruktur in vSphere IaaS control plane an.

Lesen Sie als Nächstes die folgenden Themen:

- Best Practices für Speicher und Fehlerbehebung
- Fehlerbehebung beim Upgrade der Netzwerktopologie
- Herunterfahren und Starten der vSphere IaaS control plane-Arbeitslastdomäne
- Erfassen des Support-Pakets für einen Supervisor

Best Practices für Speicher und Fehlerbehebung

In vSphere IaaS control plane können Sie die Best Practices und Fehlerbehebungstechniken für Ihre Speicherumgebung anwenden.

Verwenden von Anti-Affinitätsregeln für VMs der Steuerungsebene in Nicht-vSAN-Datenspeichern

Wenn Sie andere Datenspeicher als vSAN in Ihrem Cluster mit vSphere IaaS control plane verwenden, platzieren Sie die drei VMs der Steuerungsebene aus Verfügbarkeitsgründen in unterschiedlichen Datenspeichern.

Da die VMs der Steuerungsebene vom System verwaltet werden, können Sie sie nicht manuell migrieren. Verwenden Sie eine Kombination aus einem Datenspeichercluster und Storage DRS, um die VMs der Steuerungsebene neu zu verteilen und sie in verschiedenen Datenspeichern zu platzieren.

Verfahren

1 Erstellen Sie im vSphere Client einen Datenspeichercluster.

   a Navigieren Sie zu den Datencentern.

   b Klicken Sie mit der rechten Maustaste auf das Datencenterobjekt und wählen Sie **Neuer Datenspeicher-Cluster**.

   c Benennen Sie Ihren Datenspeichercluster und stellen Sie sicher, dass **Storage DRS einschalten** aktiviert ist.

d Legen Sie die Automatisierungsebene für den Cluster auf **Keine Automatisierung (Manueller Modus)** fest.

e Behalten Sie die Storage DRS-Laufzeiteinstellungen standardmäßig bei.

f Wählen Sie den ESXi-Cluster aus, der mit vSphere IaaS control plane aktiviert ist.

g Wählen Sie alle gemeinsam genutzten Datenspeicher aus, die dem Datenspeichercluster hinzugefügt werden sollen.

h Klicken Sie auf **Beenden**.

2 Definieren Sie Storage DRS-Regeln für VMs der Steuerungsebene.

a Navigieren Sie zum Datenspeichercluster.

b Klicken Sie auf die Registerkarte **Konfigurieren** und dann unter **Konfiguration** auf **Regeln**.

c Klicken Sie auf das Symbol **Hinzufügen** und geben Sie einen Namen für die Regel ein.

d Stellen Sie sicher, dass **Regel aktivieren** aktiviert ist.

e Legen Sie den **Regeltyp** auf **VM-Anti-Affinität** fest.

f Klicken Sie auf das Symbol **Hinzufügen** und wählen Sie die drei Supervisor-VMs der Steuerungsebene aus.

g Klicken Sie auf **OK**, um Ihre Konfiguration abzuschließen.

3 Erstellen Sie VM-Außerkraftsetzungen.

a Navigieren Sie zum Datenspeichercluster.

b Klicken Sie auf die Registerkarte **Konfigurieren** und klicken Sie unter **Konfiguration** auf **VM-Außerkraftsetzungen**.

c Klicken Sie auf das Symbol **Hinzufügen** und wählen Sie die drei VMs der Steuerungsebene aus.

d Zum Aktivieren der Storage DRS-Automatisierungsebene aktivieren Sie das Kontrollkästchen **Überschreiben** und legen Sie den Wert auf **Vollautomatisiert** fest.

e Klicken Sie auf **Beenden**.

Ergebnisse

Diese Aufgabe aktiviert Storage DRS nur für die VMs der Steuerungsebene und gleicht die VMs neu auf unterschiedlichen Datenspeichern aus.

Sobald Storage vMotion ausgeführt wird, können Sie die SDRS-Regeln und die Außerkraftsetzungen entfernen, Storage DRS deaktivieren und den Datenspeichercluster entfernen.

Die aus vSphere entfernte Speicherrichtlinie wird weiterhin als Kubernetes-Speicherklasse angezeigt

Wenn Sie die Speicherrichtlinie mithilfe von vSphere Client aus VMware vCenter oder einem Namespace im Supervisor entfernen, bleibt ihre übereinstimmende Speicherklasse zwar in der Kubernetes-Umgebung erhalten, sie kann aber nicht verwendet werden.

Problem

Bei der Ausführung des Befehls **`kubectl get sc`** wird die Speicherklasse in der Ausgabe weiterhin als im Namespace verfügbar angezeigt. Sie kann jedoch nicht verwendet werden. Wenn Sie beispielsweise versuchen, die Speicherklasse für eine neue Beanspruchung eines dauerhaften Volumes zu verwenden, schlägt dies fehl.

Falls die Speicherklasse bereits von einer Kubernetes-Bereitstellung verwendet wird, verhält sich die Bereitstellung möglicherweise unvorhersehbar.

Lösung

1. Zur Überprüfung, welche Speicherklassen im Namespace vorhanden sind, führen Sie den Befehl **`kubectl describe namespace`** ***`namespace_name`*** aus.

   Die Speicherklasse wird in der Ausgabe für diesen Befehl nicht aufgeführt, wenn die übereinstimmende Speicherrichtlinie entfernt wurde.

2. Falls die Speicherklasse bereits von einer Bereitstellung verwendet wird, stellen Sie die Speicherklasse wieder her.

   a. Erstellen Sie mithilfe von vSphere Client eine neue Speicherrichtlinie und geben Sie ihr den Namen der von Ihnen entfernten Richtlinie.

      Wenn Sie beispielsweise die Richtlinie *Gold* gelöscht haben, geben Sie der neuen Richtlinie den Namen *Gold*. Weitere Informationen finden Sie unter Erstellen von Speicherrichtlinien für vSphere with Tanzu in *Installieren und Konfigurieren der vSphere IaaS-Steuerungsebene*.

   b. Weisen Sie die Richtlinie dem Namespace zu.

      Weitere Informationen finden Sie unter Ändern der Speichereinstellungen in einem Namespace in *Dienste und Arbeitslasten der vSphere IaaS-Steuerungsebene*.

      Nachdem Sie die Richtlinie dem Namespace zugewiesen haben, löscht vSphere IaaS control plane die alte Speicherklasse und erstellt eine übereinstimmende Speicherklasse mit demselben Namen.

Externen Speicher mit vSAN Direct

Wenn Sie -vSAN Direct in der vSphere IaaS control plane-Umgebung verwenden, können Sie externen gemeinsam genutzten Speicher verwenden, um interne VMs und andere Metadaten für die Verwaltung zu speichern.

Problem

Wenn Sie einen homogenen vSAN Direct-Cluster bereitstellen, müssen Sie einen replizierten vSAN-Datenspeicher auf jedem ESXi-Host im Cluster erstellen, um Supervisor-Steuerungsebenen-VMs und andere Metadaten zu speichern. Der vSAN verbraucht Speicherplatz, benötigt einen zusätzlichen E/A-Controller auf jedem Host und schränkt die Hardwarekonfiguration ein, auf der vSAN Direct unterstützt werden können.

Anstelle einer vSAN-Datenspeicherkonfiguration können Sie externen gemeinsam genutzten Speicher zum Speichern interner Verwaltungs-VMs und anderer Metadaten verwenden.

Lösung

1 Wenn vSAN oder vSAN Direct auf den ESXi-Hosts im Cluster bereitgestellt wurde, löschen Sie die Hosts aus allen Konfigurationen.

   a Entfernen Sie alle Festplatten, die dem vSAN oder vSAN Direct zugewiesen sind. Siehe Entfernen von Festplattengruppen oder Geräten aus vSAN in *Verwalten von VMware vSAN*.

   b (Optional) Verwenden Sie das Skript zum Kennzeichnen von Festplatten auf den Hosts für vSAN Direct. Weitere Informationen finden Sie unter Verwenden von Skripts zum Kennzeichnen von Speichergeräten für vSAN Direct.

2 Verwenden Sie VMware Cloud Foundation zum Erstellen einer Arbeitslastdomäne mit externem Speicher.

   Stellen Sie sicher, dass Sie eine der Speicheroptionen auswählen, z. B. NFS, vVols oder Fibre Channel. Es kann nur eine dieser Optionen ausgewählt werden.

   Weitere Informationen finden Sie unter *Arbeiten mit Arbeitslastdomänen* in der VMware Cloud Foundation-Dokumentation.

   In diesem Schritt wird eine Arbeitslastdomäne mit vCenter Server und festgelegten ESXi bereitgestellt. Der externe Speicher wird auf allen Hosts gemountet und zum Standardcluster hinzugefügt.

3 Aktivieren Sie vSAN.

   Stellen Sie sicher, dass keine Festplatten für vSAN beansprucht sind.

   Weitere Informationen finden Sie unter Aktivieren von vSAN auf einem vorhandenen Cluster in *Verwalten von VMware vSAN*.

   In diesem Schritt wird ein Null-Byte-vSAN-Datenspeicher mit vSAN-Netzwerk erstellt. Es werden keine lokalen Festplatten für vSAN verwendet.

4 Beanspruchen Sie lokale Festplatten auf den Hosts für vSAN Direct.

   Weitere Informationen finden Sie unter Erstellen eines vSAN Direct-Datenspeichers in *Dienste und Arbeitslasten der vSphere IaaS-Steuerungsebene*.

   Für jedes von Ihnen beanspruchte Gerät erstellt vSAN Direct einen separaten Datenspeicher.

5 Erstellen Sie Speicherrichtlinien für vSAN Direct.

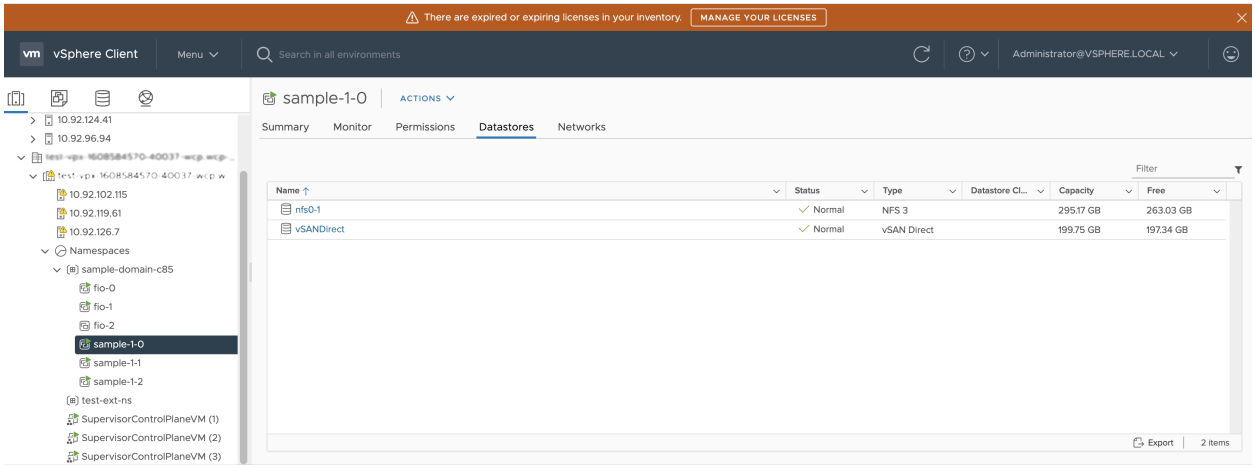
Weitere Informationen finden Sie unter Create vSAN Direct Storage Policy in *Dienste und Arbeitslasten der vSphere IaaS-Steuerungsebene*.

6 Aktivieren Sie die Supervisor.

Weitere Informationen finden Sie in der Dokumentation zu *Installieren und Konfigurieren der vSphere IaaS-Steuerungsebene*.

Beispiel

In diesem Beispiel enthält eine Konfiguration externen NFS-Speicher und einen vSAN Direct-Datenspeicher. Control Plane VMs und vSphere-Pods werden in externem NFS-Speicher ausgeführt. Persistente Volumes werden auf vSAN Direct ausgeführt.



Fehlerbehebung beim Upgrade der Netzwerktopologie

Wenn Sie vSphere IaaS control plane, Version 7.0 Update 1c installieren oder ein Upgrade des Supervisors von Version 7.0 Update 1 auf Version 7.0 Update 1c durchführen, wird ein Upgrade der Netzwerktopologie von einer einzelnen Tier-1-Gateway-Topologie auf eine Topologie durchgeführt, die ein Tier-1-Gateway für jeden Namespace im Supervisor aufweist.

Sie können Probleme beheben, die während des Upgrades auftreten können.

Vorabprüfung des Upgrades schlägt aufgrund unzureichender Kapazität des Edge-Lastausgleichsdiensts fehl

Die Vorabprüfung für das Upgrade schlägt fehl, und die Fehlermeldung weist auf unzureichende Kapazität des Lastausgleichsdiensts hin.

Problem

Der Vorgang zur Vorabprüfung des Upgrades schlägt mit einer Fehlermeldung fehl, die angibt, dass die Kapazität des Lastausgleichsdiensts kleiner als die vom Supervisor benötigte Kapazität ist.

Lösung

Führen Sie zum Beheben des Problems einen der folgenden Schritte durch.

- Erzwingen Sie das Upgrade, indem Sie in der Fehlermeldung auf die Schaltfläche **Upgrade erzwingen** klicken oder die vCenter Server-Befehlszeile mit dem Flag `--ingnore-precheck-warnings true` verwenden.

  Hinweis Diese Lösung wird nur empfohlen, wenn der Edge-Cluster die vorhandenen Arbeitslasten des Namespace unterstützt. Andernfalls können diese Arbeitslasten während des Upgrades übersprungen werden.

- Löschen Sie nicht verwendete Arbeitslasten.
- Fügen Sie dem Cluster zusätzliche Edge-Knoten hinzu.

Namespaces für Supervisor-Arbeitslast wurden während des Upgrades übersprungen

Während des Supervisor-Upgrades werden einige Namespace-Arbeitslasten nicht aktualisiert.

Problem

Das Supervisor-Upgrade ist erfolgreich, aber einige Namespace-Arbeitslasten werden beim Upgrade übersprungen. Die Kubernetes-Ressourcen geben unzureichende Ressourcen an, und das neu erstellte Tier-1-Gateway befindet sich im Zustand `ERROR`.

Ursache

Die Kapazität des Lastausgleichsdiensts reicht nicht aus, um die Arbeitslasten zu stützen.

Lösung

Führen Sie zum Beheben des Problems einen der folgenden Schritte durch.

- Löschen Sie nicht verwendete Arbeitslasten, starten Sie NCP neu und führen Sie das Upgrade erneut aus.
- Fügen Sie dem Cluster zusätzliche Edge-Knoten hinzu und lösen Sie eine erneute Zuteilung für das Tier-1-Gateway aus. Starten Sie NCP neu und führen Sie das Upgrade erneut aus.

Lastausgleichsdienst während Upgrade übersprungen

Während des Supervisor-Upgrades werden einige Lastausgleichsdienste nicht aktualisiert.

Problem

Das Supervisor-Upgrade verläuft erfolgreich, aber einige Kubernetes-Lastausgleichsdienste werden während des Upgrades übersprungen.

Ursache

Die Anzahl der Kubernetes-Lastausgleichsdienste in den Supervisor-Arbeitslasten und dem zugehörigen Tanzu Kubernetes-Cluster überschreitet den Grenzwert für die virtuellen NSX Edge-Server.

Lösung

Löschen Sie nicht verwendete Arbeitslasten, starten Sie NCP neu und führen Sie das Upgrade erneut aus.

Herunterfahren und Starten der vSphere IaaS control plane-Arbeitslastdomäne

Um Datenverlust zu vermeiden und die Komponenten und Arbeitslasten Ihrer vSphere IaaS control plane-Umgebung betriebsbereit zu halten, müssen Sie beim Herunterfahren oder Starten der Komponenten die angegebene Reihenfolge einhalten.

Normalerweise führen Sie die Herunterfahr- und Startvorgänge aus, nachdem Sie ein Patch, ein Upgrade oder eine Wiederherstellung Ihrer vSphere IaaS control plane-Umgebung angewendet haben.

Die vSphere IaaS control plane-Lösung, einschließlich der Tanzu Kubernetes-Cluster, die vom Tanzu Kubernetes Grid bereitgestellt werden, ist Teil des vSphere-SDDC (Software Defined Data Center). Daher müssen Sie beim Herunterfahren und Starten Ihrer vSphere IaaS control plane-Umgebung den gesamten vSphere-Infrastrukturstapel berücksichtigen. Weitere Informationen finden Sie in den folgenden validierten Verfahren zum Herunterfahren und Starten des vSphere-SDDC, einschließlich vSphere IaaS control plane:

- vSphere SDDC, einschließlich des vSphere IaaS control plane Vorgangs zum Herunterfahren
- vSphere SDDC, einschließlich des vSphere IaaS control plane Vorgangs zum Starten

Erfassen des Support-Pakets für einen Supervisor

Erfahren Sie, wie Sie ein Support-Paket für einen Supervisor erfassen. Sie können ein Support-Paket auch dann erfassen, wenn sich der Supervisor in einem Fehler- oder Konfigurationszustand befindet.

Voraussetzungen

- Ihr Benutzerkonto muss über das Recht **Global.Diagnose** verfügen.

Verfahren

1. Melden Sie sich mit dem vSphere Client bei Ihrer vSphere IaaS control plane-Umgebung an.
2. Wählen Sie **Menü > Arbeitslastverwaltung** aus.
3. Wählen Sie die Registerkarte **Supervisoren** aus.

4 Wählen Sie den Ziel-Supervisor aus.

5 Klicken Sie auf **Protokolle exportieren**.

Ergebnisse

Lesen Sie nach der Erfassung des Support-Pakets folgenden KB-Artikel: Hochladen von Diagnoseinformationen für VMware über das Secure FTP-Portal: http://kb.vmware.com/kb/2069559.