Dienste und Arbeitslasten 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

1 Informationen zu *Dienste und Arbeitslasten der vSphere IaaS-Steuerungsebene* 7

Aktualisierte Informationen 9

2 Workflows für vSphere IaaS control plane-Dienste und -Arbeitslasten 12

3 Konfigurieren und Verwalten von vSphere-Namespaces 18

Erstellen und Konfigurieren eines vSphere-Namespace im Supervisor. 19

Entfernen eines vSphere-Namespace vom Supervisor 26

Festlegen von Ressourcengrenzwerten in einem vSphere-Namespace 26

Konfigurieren von Objektbeschränkungen in einem vSphere-Namespace 27

Überwachen und Verwalten von Ressourcen in einem vSphere-Namespace 28

Bereitstellen einer Self-Service-Namespace-Vorlage in vSphere IaaS control plane 29

Erstellen und Konfigurieren einer Self-Service-Namespace-Vorlage 31

Deaktivieren eines Self-Service-Namespace 32

Erstellen eines Self-Service-Namespace 33

Erstellen eines Self-Service-Namespace mit Anmerkungen und Bezeichnungen 34

Aktualisieren eines Self-Service-Namespace mit kubectl annotate und kubectl label 35

Aktualisieren eines Self-Service-Namespace mit kubectl edit 37

Löschen eines Self-Service-Namespace 38

Ändern der Speichereinstellungen in einem vSphere Namespace 39

Hinzufügen von Sicherheitsrichtlinien zu einem NSX vSphere-Namespace 40

Erstellen einer Sicherheitsrichtlinie 40

Konfigurieren von Netzwerk- und Lastausgleichsdienstparametern für einen Namespacensraum 41

4 Verwalten von Supervisor-Dienste mit vSphere IaaS control plane 45

Hinzufügen eines Supervisor-Dienst zu vCenter Server 48

Installieren eines Supervisor-Diensts auf einem Supervisor 50

Aufrufen der Verwaltungsschnittstelle eines Supervisor-Dienst im Supervisor 52

Hinzufügen einer neuen Version zu einem Supervisor-Dienst 53

Upgrade eines Supervisor-Dienst auf eine neuere Version 53

Anzeigen der auf einem Supervisor installierten Supervisor-Dienste 56

Deaktivieren eines Supervisor-Dienst oder einer Version davon 57

Aktivieren einer Supervisor-Dienst-Version unter vCenter Server 58

Deinstallieren eines Supervisor-Dienst von einem Supervisor 59

Löschen einer Supervisor-Dienst-Version 59

Löschen eines Supervisor-Diensts 60

5 Verwenden der vSAN Data Persistence-Plattform mit modernen statusbehafteten Diensten 62

Aktivieren von statusbehafteten Diensten in vSphere IaaS control plane 67

Einrichten eines vSAN Direct-Datenspeichers für statusbehaftete Dienste 71

Markieren von Speichergeräten für vSAN Direct mit Tags 71

Verwenden eines Skripts, um Speichergeräte für vSAN Direct mit Tags zu versehen 71

Erstellen eines vSAN Direct-Datenspeichers 78

Überwachen von statusbehafteten Diensten in vSphere IaaS control plane 79

Überprüfen der für statusbehaftete Dienste verfügbaren Speicherrichtlinien 80

Erstellen von benutzerdefinierten Speicherrichtlinien für die vSAN Data Persistence-Plattform 81

Erstellen einer vSAN Direct-Speicherrichtlinie 82

vSAN SNA-Speicherrichtlinie erstellen 82

6 Bereitstellen und Verwalten von virtuellen Maschinen in vSphere IaaS control plane 84

Erstellen und Verwalten von Inhaltsbibliotheken für eigenständige VMs in vSphere IaaS control plane 89

Erstellen einer Inhaltsbibliothek für eigenständige VMs in vSphere IaaS control plane 89

Erstellen einer Inhaltsbibliothek für eigenständige VMs 90

Auffüllen einer Inhaltsbibliothek mit VM-Images für eigenständige VMs 92

Hinzufügen und Verwalten von VM-Inhaltsbibliotheken in vSphere IaaS control plane 94

Hinzufügen einer VM-Inhaltsbibliothek zu einem Namespace mit dem vSphere Client 94

Verwalten von VM-Inhaltsbibliotheken in einem Namespace mithilfe des vSphere Client 95

Hinzufügen einer VM-Inhaltsbibliothek zu einem Namespace mithilfe der Datencenter-CLI 96

Hinzufügen einer VM-Inhaltsbibliothek zu Supervisor mithilfe der Datencenter-CLI 97

Verwalten und Veröffentlichen von Inhaltsbibliotheks-Images in vSphere IaaS control plane 99

Arbeiten mit VM-Klassen in vSphere IaaS control plane 103

Erstellen einer benutzerdefinierten VM-Klasse mit dem vSphere Client 103

Bearbeiten einer VM-Klasse mithilfe des vSphere Client 104

Zuordnen einer VM-Klasse zu einem Namespace mit dem vSphere Client 109

Verwalten von VM-Klassen in einem Namespace mithilfe des vSphere Client 110

Erstellen und Verwalten von VM-Klassen mithilfe der Datencenter-CLI 110

Erstellen einer VM-Klasse mithilfe der Datencenter-CLI 111

Aktualisieren einer VM-Klasse mithilfe der Datencenter-CLI 113

Bereitstellen einer eigenständigen VM in vSphere IaaS control plane 116

Anzeigen der in einem Namespace verfügbaren VM-Ressourcen in vSphere IaaS control plane 117

Bereitstellen einer virtuellen Maschine in vSphere IaaS control plane 119
Bereitstellen einer VM mit vGPU und anderen PCI-Geräten in vSphere IaaS control plane 122
Bereitstellen einer VM mit vGPU in vSphere IaaS control plane 122
Hinzufügen eines vGPU-Geräts zu einer VM-Klasse mit vSphere Client 123
Hinzufügen eines vGPU-Geräts zu einer VM-Klasse mithilfe der Datencenter-CLI 126
Installieren des NVIDIA-Gasttreibers in einer VM in vSphere IaaS control plane 127
Bereitstellen einer VM mit PCI-Geräten in vSphere IaaS control plane 128
Bereitstellen einer VM mit Instanzspeicher in vSphere IaaS control plane 128
Erstellen eines vSAN Direct-Datenspeichers 129
Erstellen einer vSAN Direct-Speicherrichtlinie 131
Erstellen einer VM-Klasse mit Instanzspeicher 131
Bereitstellen einer VM mit Instanzspeicher 133
Bereitstellen von VMs mit konfigurierbaren OVF-Eigenschaften in vSphere IaaS control plane 134
Überwachen der in vSphere IaaS control plane verfügbaren virtuellen Maschinen 137
Fehlerbehebung bei VMs mithilfe der vSphere VM-Web-Konsole 139

7 Bereitstellen von Arbeitslasten in vSphere-Pods 140
Abrufen und Verwenden des Supervisor-Kontexts in vSphere IaaS control plane 143
Bereitstellen einer Anwendung auf einem vSphere Pod für einen vSphere-Namespace 145
Skalieren einer vSphere Pod-Anwendung 145
Bereitstellen eines vertraulichen vSphere Pods 146
vSphere Pod-Arbeitslastbereitstellung in vSphere IaaS control plane 149
WordPress bereitstellen 150
Teil 1. Zugreifen auf Ihren Namespace 150
Teil 2. WordPress-PVCs erstellen 151
Teil 3. Geheimnisse erstellen 151
Teil 4. Dienste erstellen 152
Teil 5. Pod-Bereitstellungen erstellen 152
Teil 6. WordPress testen 153
Beispiel-YAML-Dateien für die WordPress-Bereitstellung 153

8 Verwenden von persistentem Speicher mit Supervisor-Arbeitslasten in vSphere IaaS control plane 157
Anzeigen von Speicherklassen in einem vSphere-Namespace 160
Bereitstellen eines dynamischen dauerhaften Volumes in vSphere IaaS control plane 162
Bereitstellen eines statischen persistenten Volumes in vSphere IaaS control plane 164
Verwenden des vSAN-Dateidiensts zum Erstellen von ReadWriteMany-Volumes in vSphere IaaS control plane 166
Erweiterung von Volumes in vSphere IaaS control plane 169
Erweitern eines persistenten Volumes im Offline-Modus 170
Erweitern eines persistenten Volumes im Online-Modus 172

Überwachen von dauerhaften Volumes im vSphere Client 174

Überwachen der Volume-Integrität in einem vSphere-Namespace oder Tanzu Kubernetes Grid-Cluster 176

Best Practices für die Verwendung von persistentem Speicher auf einem Supervisor mit drei Zonen 178

Erstellen einer Speicherrichtlinie für einen Supervisor mit drei Zonen 180

Erstellen einer PVC auf einem Supervisor mit drei Zonen 181

9 Installieren und Konfigurieren von Harbor und Contour in vSphere IaaS control plane 183

Installieren von Contour als Supervisor-Dienst in vSphere IaaS control plane 184

Installieren und Konfigurieren von Harbor auf einem Supervisor in vSphere IaaS control plane 188

Installieren von Harbor als Supervisor-Dienst 188

Zuordnen des Harbor-FQDN zur IP-Adresse des Envoy-Ingress 192

Einrichten einer Vertrauensstellung mit dem Supervisor-Dienst von Harbor 193

Migrieren von Images aus der eingebetteten Registrierung zu Harbor in vSphere IaaS control plane 194

10 Bereitstellen von Supervisor-Dienste in einer Air-Gapped-Umgebung durch Abrufen von Images von einem Proxy 200

Verlagern der Supervisor-Dienste in eine private Registrierung 200

Installieren und Verwenden des Supervisor-Diensts 202

Informationen zu *Dienste und Arbeitslasten der vSphere IaaS-Steuerungsebene*

1

Dienste und Arbeitslasten der vSphere IaaS-Steuerungsebene, formell als *vSphere with Tanzu-Dienste und -Arbeitslasten* bezeichnet, beschreibt die Ausführung von Diensten und Arbeitslasten in einem vSphere-Namespace in einer vSphere IaaS control plane-Umgebung. Sie erfahren, wie Sie einen Namespace erstellen und Arbeitslasten wie Supervisor-Dienste, virtuelle Maschinen und vSphere-Pods bereitstellen.

Zielgruppe

Diese Informationen richten sich in erster Linie an vSphere-Administratoren, die vSphere IaaS control plane verwenden, um vSphere-Ressourcen zu konfigurieren und einem vSphere-Namespace auf einem Supervisor zuzuweisen. Diese Ressourcen können später von verschiedenen Diensten und Arbeitslasten verbraucht werden, die innerhalb des Namespace ausgeführt werden. vSphere-Administratoren, die vSphere IaaS control plane verwenden, verfügen in der Regel über Grundkenntnisse über Container und andere Kubernetes-Konzepte.

Das Handbuch kann auch von DevOps-Teams verwendet werden, die Arbeitslasten wie vSphere-Pods, VMs und Supervisor-Dienste auf dem Supervisor bereitstellen möchten.

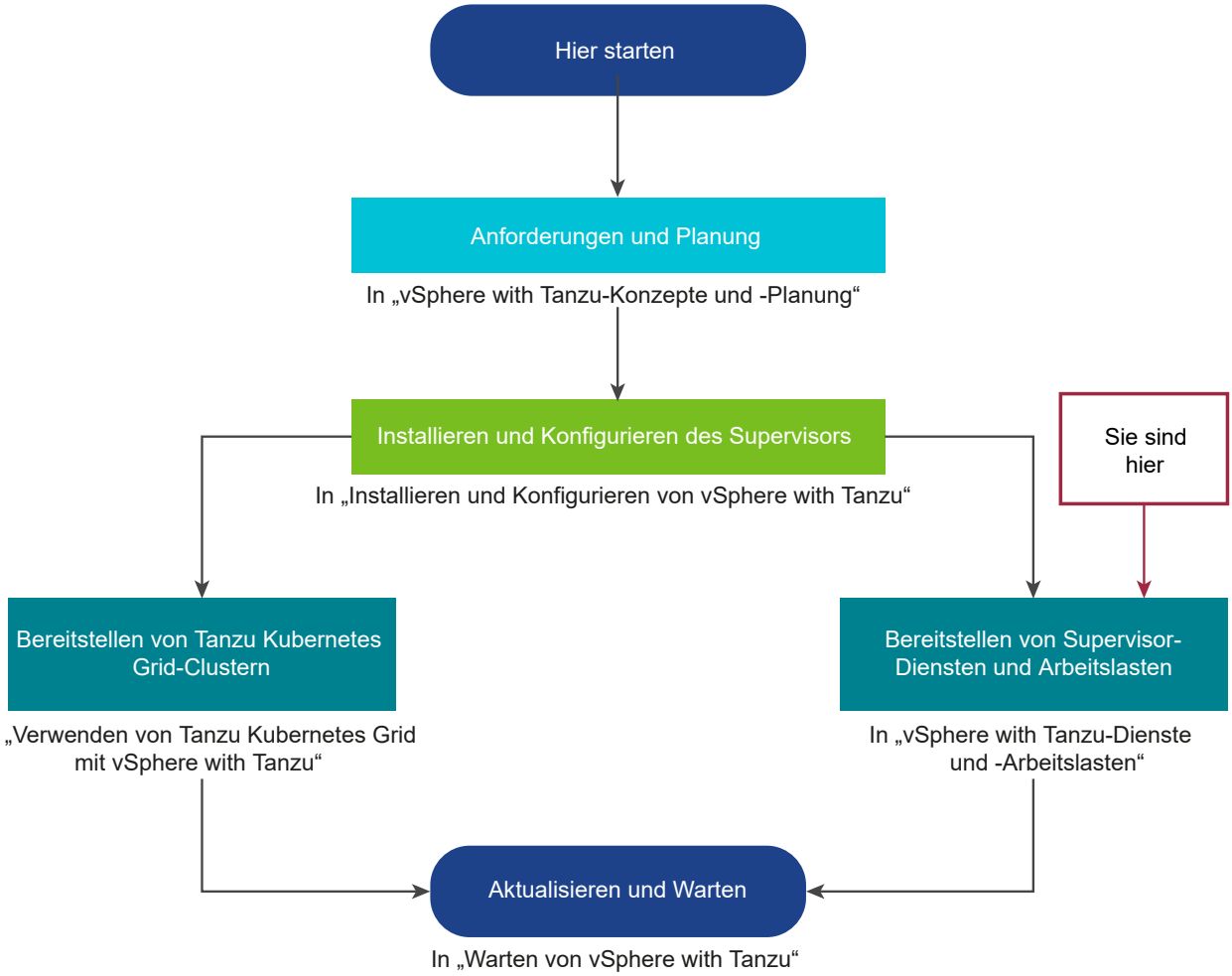
Hinweis *Dienste und Arbeitslasten der vSphere IaaS-Steuerungsebene* enthält keine Informationen zum Ausführen von Arbeitslasten auf einem Tanzu Kubernetes Grid-Cluster. Informationen zum Arbeiten mit Tanzu Kubernetes Grid-Clustern finden Sie unter Verwenden von Tanzu Kubernetes Grid auf dem Supervisor mit vSphere IaaS-Steuerungsebene.

Verwenden der *Dienste und Arbeitslasten der vSphere IaaS-Steuerungsebene*-Dokumentation

Zusätzlich zu diesem Handbuch, *Dienste und Arbeitslasten der vSphere IaaS-Steuerungsebene* enthält die vSphere IaaS control plane-Dokumentation mehrere weitere Handbücher. Machen Sie sich unbedingt mit der Hierarchie der vSphere IaaS control plane-Dokumentation vertraut, da einige der Handbücher als Voraussetzungen für dieses Handbuch, *Dienste und Arbeitslasten der vSphere IaaS-Steuerungsebene* dienen.

Diese Abbildung beschreibt, wie Sie den vSphere IaaS control plane-Dokumentationssatz verwenden können und welche Informationen Sie in den einzelnen Handbüchern finden können.

Abbildung 1-1. vSphere IaaS control plane-Dokumentationszuordnung



Aktualisierte Informationen

Dienste und Arbeitslasten der vSphere IaaS-Steuerungsebene wird mit jeder Produktversion oder bei Bedarf aktualisiert.

Diese Tabelle enthält den Updateverlauf für *Dienste und Arbeitslasten der vSphere IaaS-Steuerungsebene*.

Revision	Beschreibung
25. Juni 2024	Allgemeine Updates und Verbesserungen für vSphere 8.0 Update 3, einschließlich der folgenden Funktionen: ■ Bereitstellen von Supervisor-Dienste in einer Air-Gapped-Umgebung. Weitere Informationen hierzu finden Sie unter Kapitel 10 Bereitstellen von Supervisor-Dienste in einer Air-Gapped-Umgebung durch Abrufen von Images von einem Proxy. ■ Konfigurieren von Netzwerk- und Lastausgleichsdienstparametern für einen Namespace. Weitere Informationen hierzu finden Sie unter Konfigurieren von Netzwerk- und Lastausgleichsdienstparametern für einen Namespacensraum. ■ Unterstützung für den VM-Operator „v1alpha2“. Weitere Informationen hierzu finden Sie unter Kapitel 6 Bereitstellen und Verwalten von virtuellen Maschinen in vSphere IaaS control plane. ■ Möglichkeit, `kubectl get virtualmachineclass` zum Auflisten von VM-Klassen für einen bestimmten Supervisor-Namespace zu verwenden. Bisher handelte es sich bei VM-Klassen um eine clusterbezogene Ressource, weshalb nur schwer festgestellt werden konnte, welche VM-Klassen einem bestimmten Namespace zugewiesen waren. Weitere Informationen hierzu finden Sie unter Anzeigen der in einem Namespace verfügbaren VM-Ressourcen in vSphere IaaS control plane.
29. APR 2024	Es wurde ein Hinweis zu verfügbaren OVA-Images hinzugefügt, die über Recommended Images heruntergeladen werden können. Weitere Informationen hierzu finden Sie unter Erstellen einer Inhaltsbibliothek für eigenständige VMs in vSphere IaaS control plane.
1. April 2024	Bereitstellen einer VM mit vGPU und anderen PCI-Geräten in vSphere IaaS control plane wurde aktualisiert und enthält nun Informationen zu erweiterten Parametern, die mit NVIDIA GRID vGPU verwendet werden.
29. FEB 2024	Der Inhalt für die Bearbeitung einer VM-Klasse wurde aktualisiert, um die am Produkt vorgenommenen Änderungen zu berücksichtigen. Weitere Informationen hierzu finden Sie unter Bearbeiten einer VM-Klasse mithilfe des vSphere Client.
11. Dezember 2023	Es wurde eine Erklärung zu den Einschränkungen von RWX-Volumes hinzugefügt, die vom vSAN-Dateidienst gestützt werden. Weitere Informationen hierzu finden Sie unter Verwenden des vSAN-Dateidiensts zum Erstellen von ReadWriteMany-Volumes in vSphere IaaS control plane.
7. November 2023	Verwenden des vSAN-Dateidiensts zum Erstellen von ReadWriteMany-Volumes in vSphere IaaS control plane wurde aktualisiert, um klarzustellen, dass Datei-Volumes nur für Arbeitslasten in Tanzu Kubernetes Grid-Clustern unterstützt werden.
29. SEP 2023	■ Es wurden neue Informationen zur Plattformunterstützung über Supervisor-Dienste hinzugefügt. Weitere Informationen hierzu finden Sie unter Kapitel 4 Verwalten von Supervisor-Dienste mit vSphere IaaS control plane. ■ Kleinere Updates.

Revision	Beschreibung
21. SEP 2023	■ Es wurden neue Inhalte zur Verwendung der Data Center CLI-Befehle (DCLI-Befehle) hinzugefügt, um Inhaltsbibliotheken mit einem Namespace oder Supervisor zu verknüpfen. Weitere Informationen hierzu finden Sie unter Hinzufügen und Verwalten von VM-Inhaltsbibliotheken in vSphere IaaS control plane. ■ Es wurde ein Thema zum Veröffentlichen neuer VM-Images in einer mit einem Namespace verknüpften beschreibbaren Inhaltsbibliothek hinzugefügt. Weitere Informationen hierzu finden Sie unter Verwalten und Veröffentlichen von Inhaltsbibliotheks-Images in vSphere IaaS control plane. ■ Es wurden neue Inhalte zur Verwendung der DCLI-Befehle zum Erstellen und Verwalten der VM-Klassen hinzugefügt. Weitere Informationen hierzu finden Sie unter Erstellen und Verwalten von VM-Klassen mithilfe der Datencenter-CLI.
14. Juli 2023	■ Die Beschreibung, wie Supervisor-Dienste genutzt werden, wurde verbessert. Weitere Informationen hierzu finden Sie unter Kapitel 4 Verwalten von Supervisor-Dienste mit vSphere IaaS control plane. ■ Es wurde eine Anforderung zum Überschreiben von Einstellungen für das Tier-0-Arbeitslastnetzwerk in Erstellen und Konfigurieren eines vSphere-Namespace im Supervisor. hinzugefügt.
30. JUN 2023	Das Thema Entfernen eines vSphere-Namespace vom Supervisor wurde hinzugefügt.
21. JUN 2023	Die Aussage, dass Sie Volumes, die als Teil eines StatefulSet erstellt wurden, nicht erweitern können, wenn Sie die StatefulSet-Definition verwenden, wurde präzisiert. Weitere Informationen hierzu finden Sie unter Erweiterung von Volumes in vSphere IaaS control plane.
16. MAI 2023	Es wurde ein Hinweis hinzugefügt, dass ab der Version vSphere 8 Update 1 Supervisor-Dienste auf Supervisoren verfügbar sind, die mit beiden Typen von Netzwerken, NSX oder VDS, bereitgestellt werden. Weitere Informationen hierzu finden Sie unter Kapitel 4 Verwalten von Supervisor-Dienste mit vSphere IaaS control plane.
15. MAI 2023	Nebenversionen.
11. MAI 2023	■ Tabelle zur Unterstützung von Arbeitslasten wurde zu Kapitel 2 Workflows für vSphere IaaS control plane-Dienste und -Arbeitslasten hinzugefügt. ■ Es wurde ein Hinweis auf eine URL zur VM-Webkonsole hinzugefügt, die bei Nichtbenutzung innerhalb von zwei Minuten abläuft. Weitere Informationen hierzu finden Sie unter Fehlerbehebung bei VMs mithilfe der vSphere VM-Web-Konsole. ■ Es wurde eine Abbildung hinzugefügt, die die Hierarchie der vSphere IaaS control plane-Dokumentation zeigt. Weitere Informationen hierzu finden Sie unter Verwenden der Dienste und Arbeitslasten der vSphere IaaS-Steuerungsebene-Dokumentation.
9. MAI 2023	■ Es wurden Informationen hinzugefügt, dass ReadWriteMany-Volumes, die vom vSAN-Dateidienst gestützt werden, keine Erweiterung von Volumes unterstützen. Weitere Informationen hierzu finden Sie unter Erweiterung von Volumes in vSphere IaaS control plane. ■ Konzeptuelle Informationen zu vSphere-Pods zu Kapitel 7 Bereitstellen von Arbeitslasten in vSphere-Pods wurden hinzugefügt.
5. Mai 2023	■ Das Kapitel Kapitel 9 Installieren und Konfigurieren von Harbor und Contour in vSphere IaaS control plane wurde aktualisiert. ■ Es wurden Informationen darüber hinzugefügt, dass vSphere-Pods nur mit dem NSX-Netzwerk-Stack unterstützt werden. ■ Es wurde ein Beispiel für die vSphere Pod-Bereitstellung hinzugefügt. Siehe vSphere Pod-Arbeitslastbereitstellung in vSphere IaaS control plane.

Revision	Beschreibung
26. APR 2023	Kapitel Kapitel 3 Konfigurieren und Verwalten von vSphere-Namespaces wurde hinzugefügt.
18. APR 2023	■ Ein Thema zum Bereitstellen von VMs mit konfigurierbaren OVF-Eigenschaften wurde hinzugefügt. Weitere Informationen hierzu finden Sie unter Bereitstellen von VMs mit konfigurierbaren OVF-Eigenschaften in vSphere IaaS control plane. ■ Es wurden Informationen zur vSphere-VM-Webkonsole hinzugefügt, die DevOps-Ingenieure nutzen können, um zur Fehlerbehebung direkt auf eine VM und ihr Gastbetriebssystem zugreifen zu können. Weitere Informationen hierzu finden Sie unter Fehlerbehebung bei VMs mithilfe der vSphere VM-Web-Konsole.

Workflows für vSphere IaaS control plane-Dienste und -Arbeitslasten

2

Bei diesen Workflows wird davon ausgegangen, dass Sie vSphere IaaS control plane bereits aktiviert haben, einen Supervisor eingerichtet haben und jetzt bereit sind, vSphere-Namespaces zu erstellen und für Arbeitslasten zu verwenden.

Benutzerrollen

In der Regel umfasst die Interaktion mit dem Supervisor und die Ausführung von Arbeitslasten zwei Rollen, vSphere Administrator und DevOps-Ingenieur. Die Workflows für die Rollen „vSphere-Administrator“ und „DevOps-Ingenieur“ sind verschieden und werden durch den spezifischen Fachbereich bestimmt, die diese Rollen erfordern.

vSphere-Administrator

Als vSphere-Administrator verwenden Sie in der Regel den vSphere Client, um einen Supervisor und Namespaces zu konfigurieren, in denen DevOps-Ingenieure Kubernetes-Arbeitslasten bereitstellen können.

Wenn Sie Ihren Supervisor noch nicht erstellt haben und weitere Informationen zur Vorgehensweise benötigen, finden Sie weitere Informationen unter Installieren und Konfigurieren der vSphere IaaS-Steuerungsebene.

DevOps-Ingenieur

Auf einem Supervisor kann eine DevOps-Ingenieurrolle Aktivitäten kombinieren, die in der Regel von Kubernetes-Entwicklern, Anwendungsbesitzern und Kubernetes-Administratoren durchgeführt werden. Als DevOps-Ingenieur verwenden Sie kubectl-Befehle. Sie können vSphere-Pods, VMs und andere Arbeitslasten in Supervisor-Namespaces bereitstellen und ausführen, die der vSphere-Administrator für Sie erstellt. Sie können auch Self-Service-Namespaces erstellen.

In diesem Handbuch zu *Dienste und Arbeitslasten der vSphere IaaS-Steuerungsebene* werden keine Aufgaben behandelt, die der DevOps-Ingenieur auf einem Tanzu Kubernetes Grid-Cluster durchführt. Weitere Informationen zu diesen Aufgaben finden Sie im Thema über das Verwenden von Tanzu Kubernetes Grid auf dem Supervisor mit der vSphere IaaS-Steuerungsebene

Typen von Arbeitslasten, die ein Supervisor unterstützt

Die Unterstützung eines Supervisor für verschiedene Arten von Arbeitslasten hängt von der Konfiguration und dem Netzwerk ab, das der Supervisor verwendet.

Typen von Arbeitslasten	Supervisor für eine Zone mit VDS-Netzwerk	Supervisor für eine Zone mit NSX-Netzwerk	Supervisor für drei Zonen mit VDS-Netzwerk	Supervisor für drei Zonen mit NSX-Netzwerk
Kapitel 7 Bereitstellen von Arbeitslasten in vSphere-Pods	Nein	Ja	Nein	Nein
Kapitel 6 Bereitstellen und Verwalten von virtuellen Maschinen in vSphere IaaS control plane	Ja	Ja	Ja	Ja
Kapitel 4 Verwalten von Supervisor-Dienste mit vSphere IaaS control plane	Ja	Ja	Nein	Nein
Tanzu Kubernetes Grid-Cluster	Ja	Ja	Ja	Ja

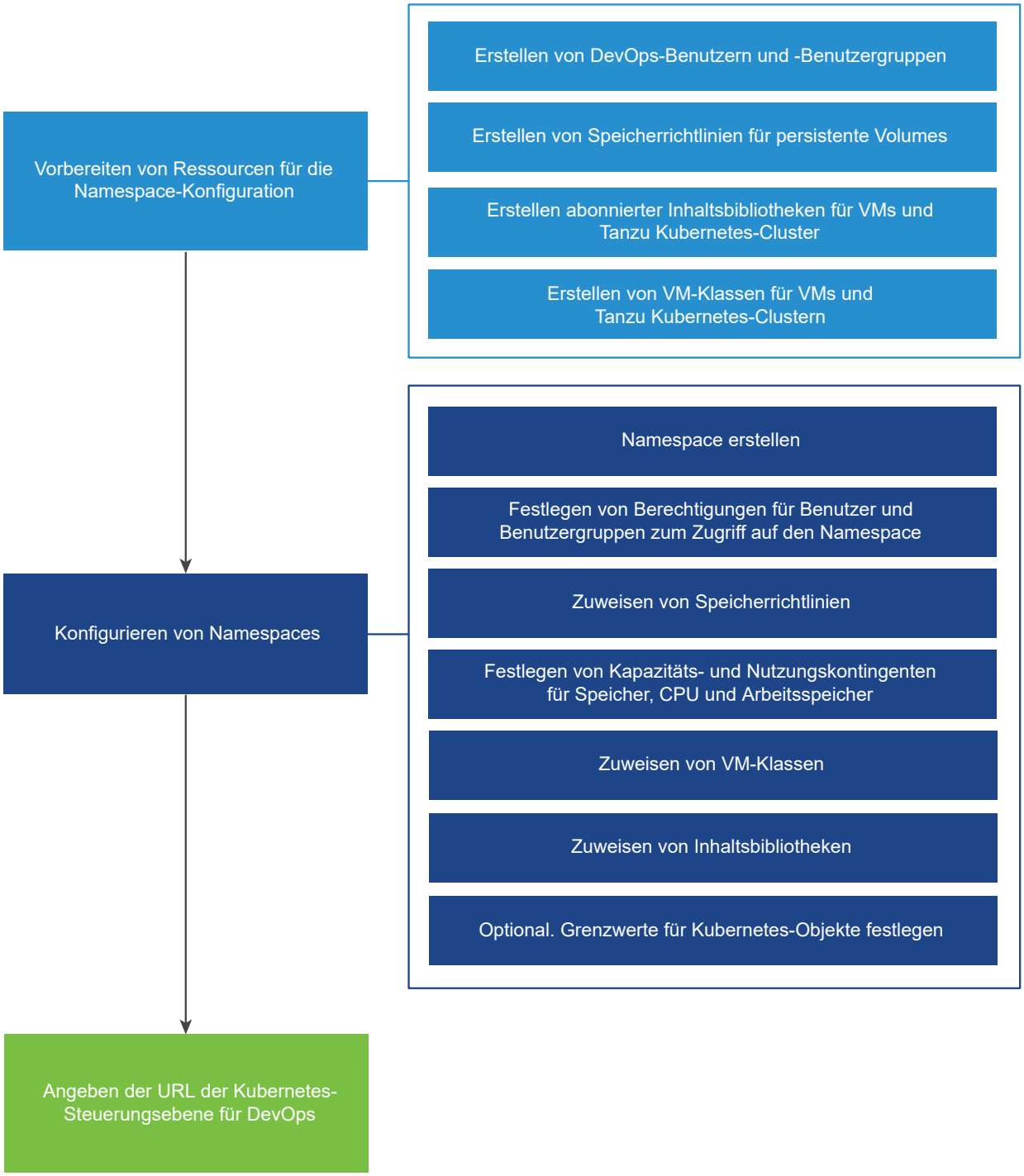
Workflow für die Konfiguration von Namespaces

Als vSphere-Administrator können Sie vSphere-Namespaces auf einem Supervisor erstellen und verwalten. Tanzu Kubernetes Grid Cluster

Bevor Sie einen Namespace erstellen, müssen Sie bestimmte Ressourcenanforderungen von DevOps-Ingenieuren zu den Anwendungen und Arbeitslasten erfassen, die sie ausführen möchten. Basierend auf diesen Spezifikationen können Sie dann die entsprechenden Ressourcen konfigurieren und sie dem Namespace zuweisen.

Weitere Informationen finden Sie unter Kapitel 3 Konfigurieren und Verwalten von vSphere-Namespaces.

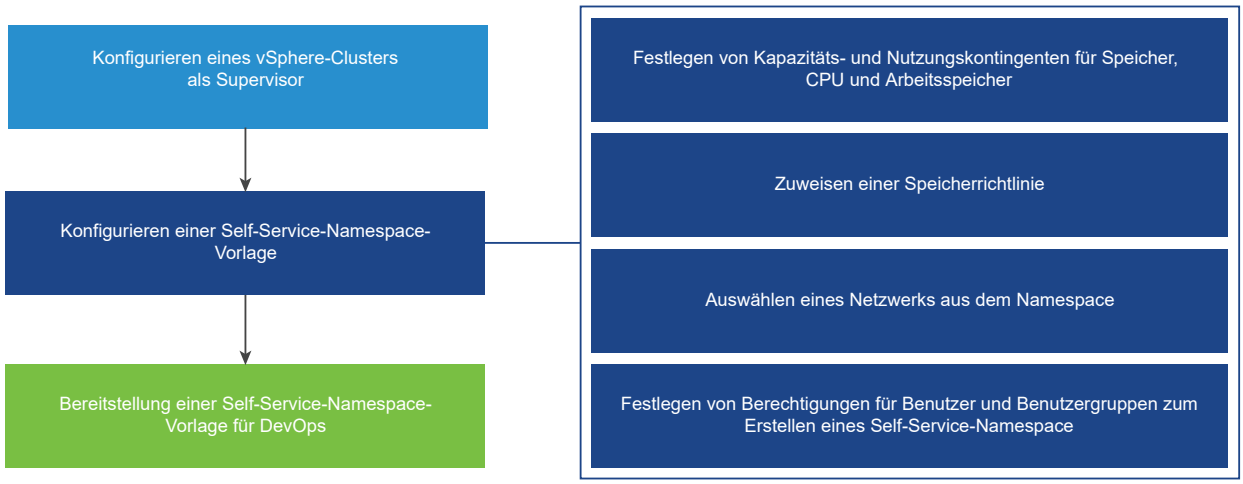
Abbildung 2-1. Workflow für die Konfiguration von Namespaces



Workflow für die Konfiguration von Self-Service-Namespaces

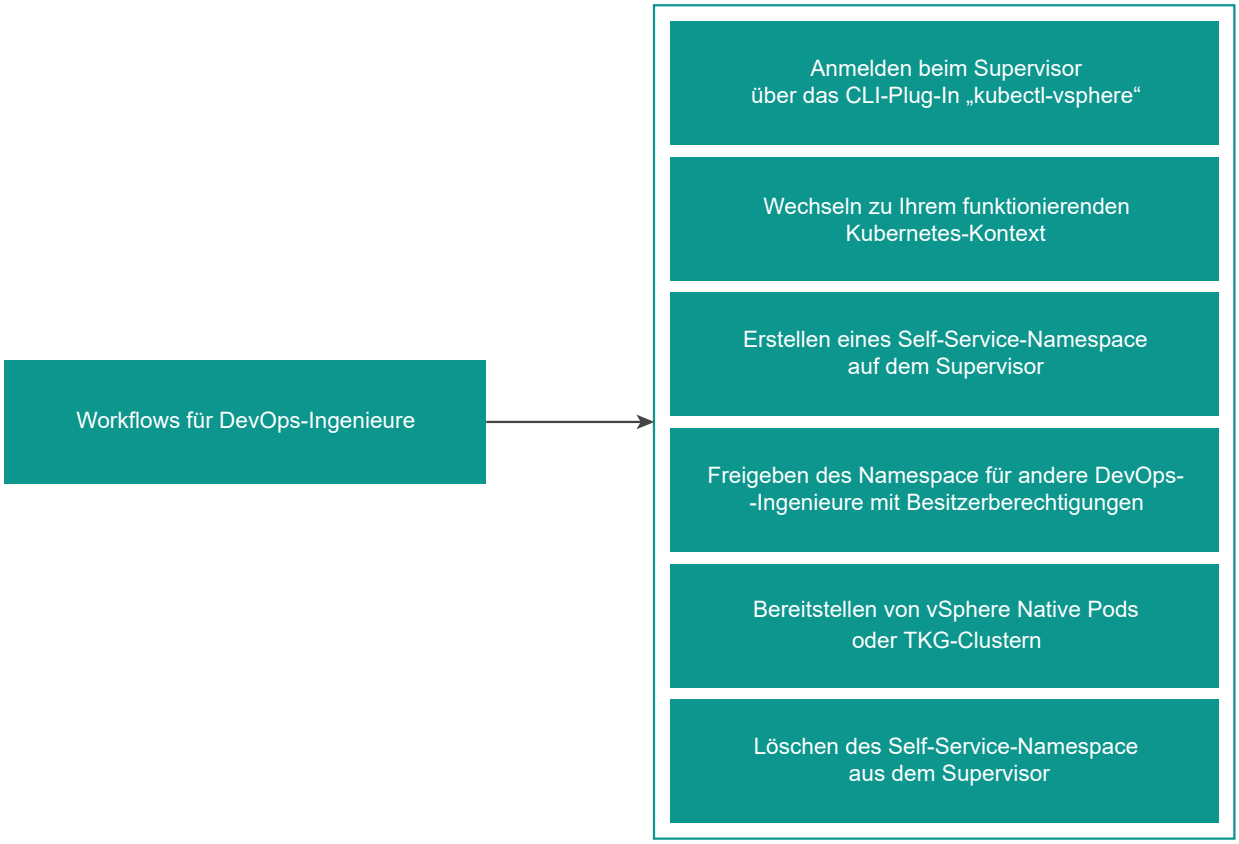
Als vSphere-Administrator können Sie einen vSphere-Namespace erstellen, CPU-, Arbeitsspeicher- und Speichergrenzwerte für den Namespace festlegen, Berechtigungen zuweisen und den Namespace-Dienst auf einem Cluster als Vorlage bereitstellen oder aktivieren. Weitere Informationen finden Sie unter Bereitstellen einer Self-Service-Namespace-Vorlage in vSphere IaaS control plane.

Abbildung 2-2. vSphere Administrator-Workflow für Self-Service-Namespace



Als DevOps-Ingenieur können Sie einen vSphere-Namespace in einer Self-Service-Form erstellen und Arbeitslasten darin bereitstellen. Sie können ihn für andere DevOps-Ingenieure freigeben oder löschen, wenn sie nicht mehr benötigt wird.

Abbildung 2-3. DevOps-Workflow für Self-Service-Namespace

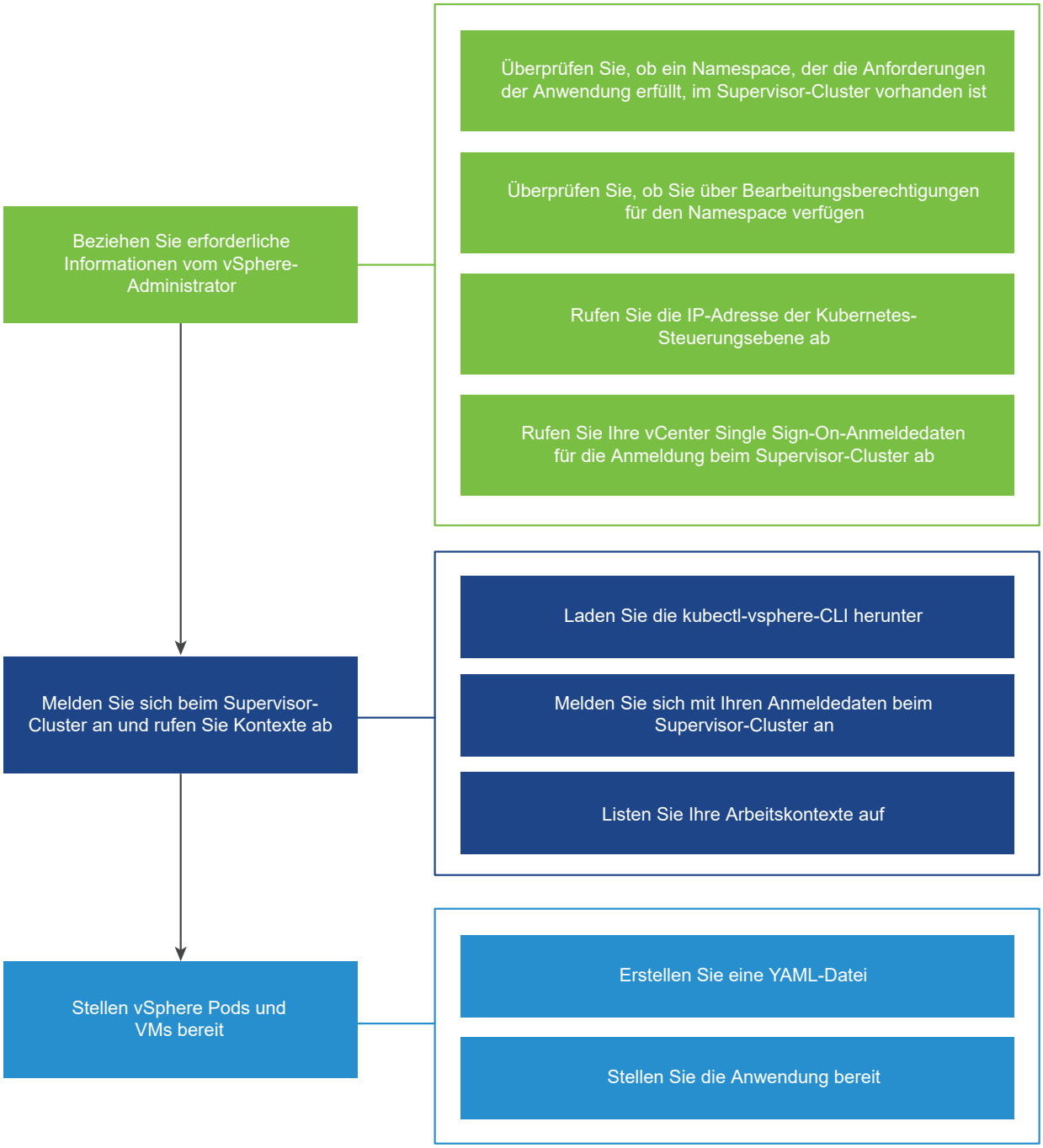


Workflow für die Bereitstellung von vSphere-Pods und VMs

Als DevOps-Ingenieur können Sie vSphere-Pods und VMs innerhalb der Ressourcengrenzen eines auf einem Supervisor ausgeführten Namespace bereitstellen.

Weitere Informationen finden Sie unter Kapitel 7 Bereitstellen von Arbeitslasten in vSphere-Pods und Kapitel 6 Bereitstellen und Verwalten von virtuellen Maschinen in vSphere IaaS control plane.

Abbildung 2-4. Workflow für vSphere-Pods und VM-Bereitstellung



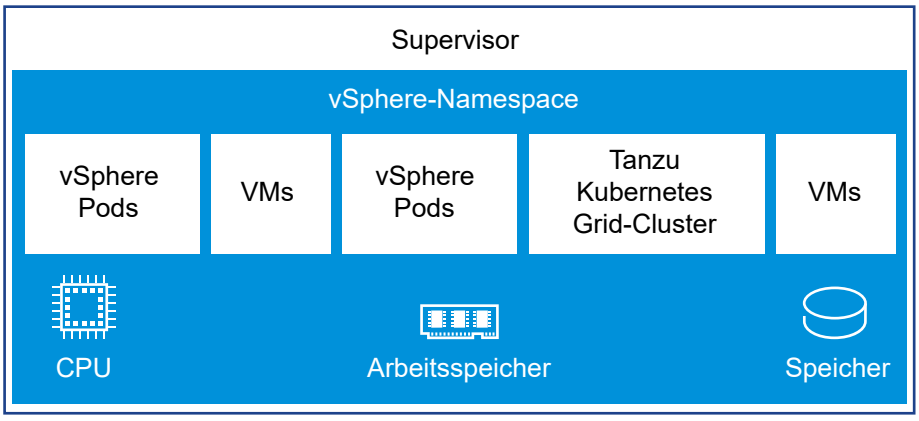
Konfigurieren und Verwalten von vSphere-Namespaces

3

vSphere IaaS control plane-Arbeitslasten, einschließlich vSphere-Pods, VMs und Tanzu Kubernetes-Cluster, werden in einem vSphere-Namespace bereitgestellt. Ein vSphere-Administrator definiert den Namespace auf einem Supervisor und konfiguriert ihn mit Ressourcenkontingent und Benutzerberechtigungen. Je nach den Anforderungen der DevOps und den Arbeitslasten, die er ausführen möchte, weist der vSphere-Administrator möglicherweise auch Speicherrichtlinien, VM-Klassen und Inhaltsbibliotheken zum Abrufen von VM-Images zu.

Bei der anfänglichen Erstellung verfügt der Namespace über unbegrenzte Ressourcen innerhalb des Supervisor. Als vSphere-Administrator können Sie Grenzwerte für CPU, RAM und Speicher sowie die Anzahl der Kubernetes-Objekte festlegen, die innerhalb des Namespace ausgeführt werden können. Speichereinschränkungen werden in Kubernetes als Speicherkontingente dargestellt. In vSphere wird für jeden Namespace auf dem Supervisor ein Ressourcenpool erstellt.

In einem auf vSphere-Zonen aktivierten Supervisor wird ein Namespace-Ressourcenpool auf jedem vSphere-Cluster erstellt, der einer Zone zugeordnet ist. Die für einen Namespace auf einem Supervisor mit drei Zonen verwendeten Ressourcen werden zu gleichen Teilen aus allen drei zugrunde liegenden vSphere-Clustern bezogen. Wenn Sie beispielsweise 300 MHz an CPU zuweisen, kommen von jedem vSphere-Cluster 100 MHz.



Um dem DevOps-Ingenieur Zugriff auf Namespaces zu gewähren, weist ein vSphere-Administrator den verfügbaren Benutzern oder Benutzergruppen Berechtigungen innerhalb einer Identitätsquelle zu, die mit vCenter Single Sign-On verknüpft ist. Alternativ kann er Anmeldedaten von einem ODIC-Anbieter verwenden, der beim Supervisor registriert ist. Weitere Informationen finden Sie unter Identitäts- und Zugriffsverwaltung der vSphere IaaS-Steuerungsebene.

Nachdem ein Namespace mit Ressourcen- und Objektgrenzwerten sowie mit Berechtigungen und Speicherrichtlinien erstellt und konfiguriert wurde, können Sie als DevOps-Ingenieur auf den Namespace zugreifen, um die folgenden Arbeitslasten auszuführen:

- Informationen zum Ausführen von Supervisor-Dienste finden Sie unter Kapitel 4 Verwalten von Supervisor-Dienste mit vSphere IaaS control plane.
- Informationen zum Ausführen von vSphere-Pods finden Sie unter Kapitel 7 Bereitstellen von Arbeitslasten in vSphere-Pods.
- Informationen zum Bereitstellen von VMs finden Sie unter Kapitel 6 Bereitstellen und Verwalten von virtuellen Maschinen in vSphere IaaS control plane.

Hinweis Dieses *Dienste und Arbeitslasten der vSphere IaaS-Steuerungsebene*-Handbuch enthält keine Informationen zum Ausführen von Arbeitslasten auf einem Tanzu Kubernetes Grid-Cluster. Informationen zum Arbeiten mit Tanzu Kubernetes Grid-Clustern finden Sie unter Verwenden von Tanzu Kubernetes Grid auf dem Supervisor mit vSphere IaaS-Steuerungsebene.

Lesen Sie als Nächstes die folgenden Themen:

- Erstellen und Konfigurieren eines vSphere-Namespace im Supervisor.
- Entfernen eines vSphere-Namespace vom Supervisor
- Festlegen von Ressourcengrenzwerten in einem vSphere-Namespace
- Konfigurieren von Objektbeschränkungen in einem vSphere-Namespace
- Überwachen und Verwalten von Ressourcen in einem vSphere-Namespace
- Bereitstellen einer Self-Service-Namespace-Vorlage in vSphere IaaS control plane
- Ändern der Speichereinstellungen in einem vSphere Namespace
- Hinzufügen von Sicherheitsrichtlinien zu einem NSX vSphere-Namespace
- Konfigurieren von Netzwerk- und Lastausgleichsdienstparametern für einen Namespacensraum

Erstellen und Konfigurieren eines vSphere-Namespace im Supervisor.

Erfahren Sie, wie Sie einen vSphere-Namespace auf dem Supervisor erstellen und konfigurieren. Als vSphere-Administrator legen Sie nach dem Erstellen eines vSphere-Namespace Ressourcengrenzwerte für den Namespace und Berechtigungen fest, damit DevOps-Ingenieure darauf zugreifen können. Sie stellen DevOps-Ingenieuren die URL der Kubernetes-Steuerungsebene bereit, auf der Arbeitslasten in den Namespaces ausgeführt werden können, für die die Ingenieure Berechtigungen haben.

Namespaces in Supervisoren, die mit dem VDS-Netzwerk-Stack konfiguriert sind, und Namespaces in Clustern, die mit NSX konfiguriert sind, weisen verschiedene Netzwerkkonfigurationen und -funktionen auf. Namespaces, die auf Supervisoren mit Bereitstellung in drei vSphere-Zonen konfiguriert sind, unterstützen auch andere Funktionen als Namespaces in Supervisoren mit einer Zone.

- Supervisor mit einer Zone und NSX-Konfiguration. vSphere-Namespaces auf diesen Supervisoren unterstützen vSphere-Pods, VMs, Tanzu Kubernetes Grid-Cluster und Supervisor-Dienste. Die Unterstützung des Arbeitslastnetzwerks für diese vSphere-Namespaces wird von NSX bereitgestellt.
- Supervisor mit drei Zonen und NSX-Konfiguration. vSphere-Namespaces auf einem Supervisor mit drei Zonen und NSX-Konfiguration unterstützen nur Tanzu Kubernetes Grid-Cluster und VMs. Sie unterstützen keine vSphere-Pods und Supervisor-Dienste.
- Supervisor mit einer Zone und VDS-Konfiguration. vSphere-Namespaces auf Supervisoren mit einer Zone und VDS unterstützen Tanzu Kubernetes Grid, VMs und Supervisor-Dienste. Sie unterstützen keine vSphere-Pods – abgesehen von denen, die Supervisor-Dienste für die eigene Verwendung bereitstellen.
- Supervisor mit drei Zonen und VDS-Konfiguration. vSphere-Namespaces, die auf einem Supervisor mit drei Zonen mit VDS ausgeführt werden, unterstützen nur Tanzu Kubernetes Grid-Cluster und VMs. Sie unterstützen keine vSphere-Pods und Supervisor-Dienste.

Weitere Informationen finden Sie unter Anforderungen zum Aktivieren eines Drei-Zonen-Supervisors mit HA-Proxy-Lastausgleichsdienst und Anforderungen zum Aktivieren eines einzelnen Cluster-Supervisors mit VDS-Netzwerk und HA-Proxy-Lastausgleichsdienst in *Konzepte und Planung der vSphere IaaS-Steuerungsebene*.

Sie können auch Ressourcengrenzwerte für den Namespace festlegen, Berechtigungen zuweisen und den Namespace-Dienst auf einem Cluster als Vorlage bereitstellen oder aktivieren. Daher können DevOps-Ingenieure einen Supervisor-Namespace im Self-Service-Modus erstellen und Arbeitslasten innerhalb des Namespace bereitstellen. Weitere Informationen finden Sie unter Bereitstellen einer Self-Service-Namespace-Vorlage in vSphere IaaS control plane.

Wenn Sie NSX für Ihre Supervisoren verwenden, haben Sie die Möglichkeit, die Netzwerkeinstellungen auf vSphere-Namespace-Ebene zu überschreiben. Stellen Sie die folgenden Überlegungen an, wenn Sie diese Option auswählen:

Tabelle 3-1. Überlegungen zur vSphere-Namespace-Netzwerkplanung

Überlegungen	Beschreibung
NSX-Installation	Um Supervisor-Netzwerkeinstellungen für einen bestimmten vSphere-Namespace zu überschreiben, muss NSX einen für Tier-0-Gateways (Router) dedizierten Edge-Cluster und einen anderen für Tier-1-Gateways dedizierten Edge-Cluster enthalten. Weitere Informationen finden Sie in den NSX-Installationsanweisungen im Handbuch *Installieren und Konfigurieren der vSphere IaaS-Steuerungsebene*.
IPAM erforderlich	Wenn Sie Supervisor-Netzwerkeinstellungen für einen bestimmten vSphere-Namespace überschreiben, muss das neue vSphere-Namespace-Netzwerk Subnetze für Ingress, Egress und Namespace-Netzwerk angeben, die auf dem Supervisor und im Vergleich zu anderen vSphere-Namespace-Netzwerken eindeutig sind. Sie müssen die Zuteilung von IP-Adressen entsprechend verwalten.
Supervisor-Routing	Der Supervisor muss direkt zu den TKG-Clusterknoten und Ingress-Subnetzen weitergeleitet werden können. Bei Auswahl eines Tier-0-Gateways für den vSphere-Namespace haben Sie zwei Optionen zum Konfigurieren des erforderlichen Routings: ■ Verwenden Sie ein VRF-Gateway (Virtual Routing and Forwarding), um die Konfiguration vom Tier-0-Gateway vom Supervisor zu übernehmen ■ Verwenden Sie das Border Gateway Protocol (BGP) zum Konfigurieren von Routen zwischen dem Tier-0-Gateway vom Supervisor und dem dedizierten Tier-0-Gateway Weitere Informationen zu diesen Optionen finden Sie in der Dokumentation zu NSX Tier-0-Gateways.

Voraussetzungen

- Stellen Sie einen Supervisor bereit.
- Erstellen Sie Benutzer und Gruppen für DevOps-Ingenieure und Entwickler, die Zugriff auf den vSphere-Namespace benötigen. Erstellen Sie die Benutzer oder Gruppen in Identitätsquellen, die mit vCenter Single Sign-On verbunden sind, oder in einem OIDC-Anbieter, der mit dem Supervisor konfiguriert ist.
- Erstellen von Speicherrichtlinien für persistenten Speicher. Wenn sich der Namespace in einem Supervisor mit drei Zonen befindet, verwenden Sie topologiefähige Richtlinien. Sie können dem Namespace mit drei Zonen keine Speicherrichtlinien zuweisen, die nicht topologiefähig sind.
- Erstellen Sie VM-Klassen und Inhaltsbibliotheken für eigenständige VMs.
- Erforderliche Rechte:
  - **Namespaces.Clusterweite Konfiguration ändern**
  - **Namespaces.Namespace-Konfiguration ändern**

Verfahren

1 Wählen Sie im vSphere Client-Startmenü die Option **Arbeitslastverwaltung** aus.

2 Wählen Sie die Registerkarte **Namespaces** aus.

3 Klicken Sie auf **Namespace erstellen**.

4 Wählen Sie den Supervisor aus, in dem Sie den vSphere-Namespace platzieren möchten.

5 Geben Sie einen Namen für den Namespace ein.

Der Name muss in einem DNS-konformen Format vorliegen.

6 Wählen Sie im Dropdown-Menü **Netzwerk** ein Arbeitslastnetzwerk für den vSphere-Namespace aus.

Hinweis Dieser Schritt ist nur dann verfügbar, wenn Sie den Namespace auf einem Cluster erstellen, der mit dem vSphere-Netzwerk-Stack konfiguriert ist.

7 Wenn Sie den NSX-Netzwerk-Stack für Ihren Supervisor konfiguriert haben, können Sie **Cluster-Netzwerkeinstellungen überschreiben** auswählen, um die Supervisor-Netzwerkeinstellungen zu überschreiben und Netzwerkeinstellungen für den Namespace zu konfigurieren.

Konfigurieren Sie die folgenden Netzwerkeinstellungen für den Namespace:

Option	Beschreibung
Tier-0-Gateway	Wählen Sie das Tier-0-Gateway aus, das mit dem Namespace-Tier-1-Gateway verknüpft werden soll. Wenn Sie ein Tier-0-Gateway auswählen, wird das Tier-0-Gateway, das Sie beim Aktivieren des Clusters konfiguriert haben, überschrieben. Daher müssen Sie die CIDR-Bereiche erneut konfigurieren. **Hinweis** Der Supervisor muss direkt zu den TKG-Clusterknoten und Ingress-Subnetzen weitergeleitet werden können. ■ Wenn Sie ein VRF-Gateway auswählen, das mit dem Tier-0-Gateway verknüpft ist, werden das Netzwerk und die Subnetze automatisch konfiguriert. ■ Wenn Sie den NAT-Modus ausgewählt haben, müssen Sie die Subnetz-, Ingress- und Egress-CIDRs konfigurieren. ■ Wenn Sie den NAT-Modus deaktivieren, müssen Sie nur das Subnetz und die Ingress-CIDRs konfigurieren. **Hinweis** Nachdem Sie ein Tier-0-Gateway ausgewählt haben, können Sie es nicht mehr ändern.
NAT-Modus	Der NAT-Modus ist standardmäßig aktiviert. Wenn Sie diese Option deaktivieren, sind alle Arbeitslasten wie die IP-Adressen der vSphere-Pods, VMs und Tanzu Kubernetes Grid-Clusterknoten von außerhalb des Tier-0-Gateways direkt zugänglich, und Sie müssen die Egress-CIDRs nicht konfigurieren. **Hinweis** Nachdem Sie einen Namespace-Modus aktiviert haben, können Sie ihn nicht mehr ändern.
Größe des Lastausgleichsdiensts	Wählen Sie die Größe der Lastausgleichsdienstinstanz auf dem Tier-1-Gateway für den Namespace aus.

Option	Beschreibung
Namespace-Netzwerk	Geben Sie einen oder mehrere IP-CIDRs ein, um Subnetze / Segmente zu erstellen und IP-Adressen für Arbeitslasten zuzuweisen, die mit Namespaces verbunden sind. **Hinweis** Geben Sie den CIDR-Bereich ein, wenn Sie ihn nicht für den Cluster konfiguriert haben. Sie können zusätzliche CIDRs konfigurieren, nachdem Sie den Namespace erstellt haben, indem Sie die Namespace-Netzwerkeinstellungen bearbeiten.
Namespace-Subnetzpräfix	Geben Sie das Subnetzpräfix ein, das die Größe des für Namespace-Segmente reservierten Subnetzes angibt. Der Standardwert ist „28“. **Hinweis** Nachdem Sie das Subnetzpräfix angegeben haben, können Sie es nicht mehr ändern.
Ingress	Geben Sie eine CIDR-Anmerkung ein, die den Ingress-IP-Bereich für die virtuellen IP-Adressen festlegt, die vom Lastausgleichsdienst für vSphere-Pods oder Tanzu Kubernetes Grid-Cluster veröffentlicht werden. Sie können zusätzliche CIDRs konfigurieren, nachdem Sie den Namespace erstellt haben, indem Sie die Namespace-Netzwerkeinstellungen bearbeiten.
Egress	Geben Sie eine CIDR-Anmerkung ein, die den Egress-IP-Bereich für die SNAT-IP-Adressen bestimmt. Sie können zusätzliche CIDRs konfigurieren, nachdem Sie den Namespace erstellt haben, indem Sie die Namespace-Netzwerkeinstellungen bearbeiten.

8 Geben Sie eine Beschreibung ein und klicken Sie auf **Erstellen**.

Der Namespace wird im Supervisor erstellt.

9 Legen Sie Berechtigungen für Benutzer fest, die auf den Namespace zugreifen können.

Als vSphere-Administrator legen Sie Berechtigungen für einen vSphere-Namespace für Entwickler und DevOps-Ingenieure fest, die auf den Namespace zugreifen müssen. Ein Benutzerkonto kann auf mehrere Namespaces zugreifen. Benutzer, die Mitglieder der Administratorengruppen sind, haben Zugriff auf alle Namespaces auf dem Supervisor.

a Wählen Sie im Bereich **Berechtigungen** die Option **Berechtigungen hinzufügen**.

b Wählen Sie eine Identitätsquelle, einen Benutzer oder eine Gruppe und eine Rolle aus und klicken Sie auf **OK**.

Rolle	Beschreibung
Kann ansehen	Schreibgeschützter Zugriff für den Benutzer oder die Gruppe. Der Benutzer oder die Gruppe kann sich bei der Supervisor-Steuerungsebene anmelden und die Arbeitslasten, die in der vSphere-Namespace ausgeführt werden, wie z. B. vSphere-Pods- und Tanzu Kubernetes Grid-Cluster und VMs, auflisten.
Kann bearbeiten	Der Benutzer oder die Gruppe kann vSphere-Pods, Tanzu Kubernetes Grid Cluster und VMs erstellen, lesen, aktualisieren und löschen. Benutzer, die Teil der Administratorengruppe sind, verfügen über Bearbeitungsberechtigungen für alle Namespaces im Supervisor.
Besitzer	Benutzerkonten mit Besitzerberechtigungen können die folgenden Aktionen durchführen: ■ Bereitstellen und Verwalten von Arbeitslasten im Namespace. ■ Freigeben des Namespace für andere Benutzer oder Gruppen. ■ Erstellen und löschen Sie mithilfe von kubectl zusätzliche vSphere-Namespaces. Wenn Benutzer mit Besitzerberechtigungen den Namensraum freigeben, können sie anderen Benutzern oder Gruppen Ansichts-, Bearbeitungs- oder Besitzerberechtigungen zuweisen. **Hinweis** Die Besitzerrolle wird für Benutzer unterstützt, die in der vCenter Single Sign-On-Identitätsquelle verfügbar sind. Sie können die Rolle „Besitzer“ nicht mit einem Benutzer / einer Gruppe eines externen Identitätsanbieters verwenden.

Wenn Sie der Rolle **`Kann ansehen`** oder **`Kann bearbeiten`** einen Benutzer oder eine Gruppe zuweisen, erstellt das System ein RoleBinding-Objekt und ordnet es einem ClusterRole-Objekt zu. Beispielsweise wird ein Benutzer oder eine Gruppe, der/die der **`Kann bearbeiten`**-Rolle zugewiesen ist, über ein RoleBinding-Objekt dem Kubernetes-`edit`-ClusterRole-Objekt zugewiesen. Benutzer mit der Rolle `edit` können Cluster bereitstellen und betreiben. Sie können diese Zuordnung mithilfe des Befehls `kubectl get rolebinding` im Ziel-vSphere-Namespace anzeigen.

```
kubectl get rolebinding -n tkg2-cluster-namespace
NAME
ROLE                          AGE
```

```
wcp:tkg-cluster-namespace:group:vsphere.local:administrators   ClusterRole/
edit             33d
wcp:tkg-cluster-namespace:user:vsphere.local:administrator     ClusterRole/
edit             33d
```

Wenn Sie der Besitzerrolle einen Benutzer oder eine Gruppe zuweisen, erstellt das System ein ClusterRoleBinding-Objekt und ordnet es einem ClusterRole-Objekt zu, mit dessen Hilfe der Benutzer oder die Gruppe vSphere-Namespaces mithilfe von kubectl erstellen und löschen kann. Um diese Zuordnung anzuzeigen, können Sie eine SSH-Verbindung zu einem Supervisor-Steuerungsebenenknoten herstellen.

10 Weisen Sie dem Namespace Speicherplatz zu.

Speicherrichtlinien, die Sie dem Namespace zuweisen, stellen dem DevOps-Team dauerhaften Speicher zur Verfügung.

a Wählen Sie im Bereich **Speicher** die Option **Speicher hinzufügen** aus.

b Wählen Sie eine Speicherrichtlinie aus, um die Datenspeicherplatzierung dauerhafter Volumes zu steuern, und klicken Sie auf **OK**.

Nach der Zuweisung der Speicherrichtlinie erstellt vSphere IaaS control plane im vSphere-Namespace eine übereinstimmende Kubernetes-Speicherklasse. Bei Verwendung von Tanzu Kubernetes Grid wird die Speicherklasse automatisch aus dem Namespace in den Tanzu Kubernetes Grid-Cluster repliziert. Wenn Sie dem Namespace mehrere Speicherrichtlinien zuweisen, wird für jede Speicherrichtlinie eine separate Speicherklasse erstellt.

11 Wählen Sie im Bereich „Kapazität und Nutzung“ **Grenzwerte bearbeiten** aus und konfigurieren Sie Ressourceneinschränkungen für den Namespace.

Option	Bezeichnung
CPU	Die Menge der CPU-Ressourcen, die für den Namespace reserviert werden soll.
Arbeitsspeicher	Die Menge an Arbeitsspeicher, die für den Namespace reserviert werden soll.
Speicher	Die Gesamtmenge an Speicherplatz, die für den Namespace reserviert werden soll.
Grenzwerte für Speicherrichtlinien	Legen Sie die Speichermenge fest, die für jede mit dem Namespace verknüpfte Speicherrichtlinie einzeln reserviert ist.

Ein Ressourcenpool für den Namespace wird in vCenter Server erstellt. Die Speicherbeschränkung bestimmt die Gesamtmenge des Speichers, die dem Namespace zur Verfügung steht, während Speicherrichtlinien die Platzierung dauerhafter Volumes für vSphere-Pods in den zugeordneten Speicherklassen bestimmen.

12 Richten Sie den VM-Dienst für eigenständige VMs ein.

Weitere Informationen finden Sie unter Kapitel 6 Bereitstellen und Verwalten von virtuellen Maschinen in vSphere IaaS control plane.

Nächste Schritte

Teilen Sie die Kubernetes-Steuerungsebenen-URL mit DevOps-Ingenieuren und geben Sie den Benutzernamen an, den sie für die Anmeldung beim Supervisor über die Kubernetes-CLI-Tools für vSphere verwenden können. Sie können einem DevOps-Ingenieur Zugriff auf mehr als einen Namespace gewähren. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit vSphere IaaS-Steuerungsebenen-Clustern.

Hinweis Dieses *Dienste und Arbeitslasten der vSphere IaaS-Steuerungsebene*-Handbuch enthält keine Informationen zum Ausführen von Arbeitslasten auf einem Tanzu Kubernetes Grid-Cluster. Informationen zum Arbeiten mit Tanzu Kubernetes Grid-Clustern finden Sie unter Verwenden von Tanzu Kubernetes Grid auf dem Supervisor mit vSphere IaaS-Steuerungsebene.

Entfernen eines vSphere-Namespace vom Supervisor

Sie können einen vSphere-Namespace vom Supervisor entfernen.

Voraussetzungen

- Entfernen Sie alle bereitgestellten Arbeitslasten, einschließlich VMs, vSphere-Pods und TKG-Cluster. Informationen zum Entfernen eines TKG-Clusters finden Sie unter Löschen eines TKG 2.0-Clusters mithilfe von Kubectl oder der Tanzu-CLI.
- Erforderliche Rechte:
  - **Namespaces.Clusterweite Konfiguration ändern**
  - **Namespaces.Namespace-Konfiguration ändern**

Verfahren

1. Wählen Sie im vSphere Client-Startmenü die Option **Arbeitslastverwaltung** aus.
2. Klicken Sie auf die Registerkarte **Namespaces**.
3. Wählen Sie in der Liste der auf dem Supervisor verfügbaren Namespaces den vSphere-Namespace aus, den Sie entfernen möchten.
4. Klicken Sie auf **Entfernen**.

   Das System entfernt den vSphere-Namespace. Es kann einige Zeit dauern, bis der Vorgang abgeschlossen ist.

Festlegen von Ressourcengrenzwerten in einem vSphere-Namespace

Als vSphere-Administrator können Sie Ressourcengrenzwerte und Standardeinstellungen für Container in einem vSphere-Namespace festlegen. DevOps-Techniker können die Container-Standardeinstellungen in Pod-Spezifikationen später überschreiben, ohne jedoch die vom

vSphere Administrator für den Namespace festgelegten Ressourcengrenzwerte insgesamt zu überschreiten. Container-Anforderungen werden in Ressourcenreservierungen in Pods übersetzt.

Voraussetzungen

- Stellen Sie sicher, dass Sie über das Recht **Namespace-Konfiguration ändern** für den Supervisor verfügen.

Verfahren

1. Wählen Sie im vSphere Client-Startmenü die Option **Arbeitslastverwaltung** aus.
2. Wählen Sie einen vSphere-Namespace und anschließend **Konfigurieren** aus und klicken Sie auf **Ressourcengrenzwerte**.
3. Klicken Sie auf **Bearbeiten**.

   Die Auswirkungen der Einrichtung von Ressourcengrenzwerten für einen vSphere-Namespace, in dem Tanzu Kubernetes Grid-Cluster bereitgestellt werden, unterscheiden sich je nach dem Typ der für Clusterknoten verwendeten VM-Klasse. Machen Sie sich mit den Unterschieden zwischen bestmöglicher und garantierter Leistung vertraut, bevor Sie Ressourcengrenzwerte festlegen. Weitere Informationen finden Sie unter VM-Klassen für Tanzu Kubernetes-Cluster in *Verwenden des TKG-Dienstes mit der vSphere IaaS-Steuerungsebene*.

Option	Bezeichnung
CPU	Legen Sie einen Grenzwert für den CPU-Verbrauch im vSphere-Namespace fest.
Arbeitsspeicher	Legen Sie einen Grenzwert für den Arbeitsspeicherverbrauch im vSphere-Namespace fest.
Speicher	Legen Sie pro verwendeter Speicherrichtlinie einen Grenzwert für die Speicherbelegung im vSphere-Namespace fest.
Standardeinstellungen für Container	Legen Sie die Standardwerte für CPU-Grenzwerte, CPU-Anforderungen, Arbeitsspeicheranforderungen und Arbeitsspeichergrenzwerte für Container im vSphere-Namespace fest.

Konfigurieren von Objektbeschränkungen in einem vSphere-Namespace

Sie können Beschränkungen für Objekte konfigurieren, die im vSphere-Namespace ausgeführt werden, wie z. B. die Anzahl der Bereitstellungen, Aufträge, Daemon-Sätze, zustandsorientierten Sätze usw. Die für ein Objekt konfigurierten Beschränkungen richten sich nach den Besonderheiten Ihrer Anwendungen und der Art und Weise, wie diese Anwendungen Ressourcen innerhalb eines vSphere-Namespace verbrauchen sollen.

Voraussetzungen

- Stellen Sie sicher, dass Sie über das Recht **Namespace-Konfiguration ändern** für den Supervisor verfügen.

Verfahren

1. Wählen Sie im vSphere Client-Startmenü die Option **Arbeitslastverwaltung** aus.
2. Wählen Sie den vSphere-Namespace aus, auf den Sie Objekt- oder Containereinschränkungen anwenden möchten.
3. Wählen Sie **Konfigurieren** und anschließend **Objektgrenzwerte** aus.
4. Klicken Sie auf **Bearbeiten**.

Option	Bezeichnung
vSphere-Pods	Die Anzahl der vSphere-Pods, die im vSphere-Namespace ausgeführt werden können.
Bereitstellungen	Die Anzahl der Bereitstellungen, die im vSphere-Namespace ausgeführt werden können.
Aufträge	Die Anzahl der Aufträge, die im vSphere-Namespace ausgeführt werden können.
Daemon-Sets	Die Anzahl der Daemon-Sätze, die im vSphere-Namespace ausgeführt werden können.
Replikat-Sets	Die Anzahl der Replikat-Sets im vSphere-Namespace.
Replizierungssteuerungen	Die Anzahl der Replizierungssteuerungen, die im vSphere-Namespace ausgeführt werden können.
Zustandsorientierte Sätze	Die Anzahl der zustandsorientierten Sätze, die im vSphere-Namespace ausgeführt werden können.
Konfigurationszuordnungen	Die Anzahl der Konfigurationszuordnungen, die im vSphere-Namespace ausgeführt werden können.
Geheimnisse	Die Anzahl der Geheimnisse, die im vSphere-Namespace ausgeführt werden können.
Anforderungen von persistenten Datenträgern	Die Anforderungen von persistenten Datenträgern, die im vSphere-Namespace vorhanden sein können.
Dienste	Die Dienste, die im vSphere-Namespace vorhanden sein können.

Überwachen und Verwalten von Ressourcen in einem vSphere-Namespace

Sie können verschiedene Aspekte eines vSphere-Namespace überwachen und verwalten, wie z. B. den Ressourcenverbrauch für den Namespace sowie die Anzahl der verschiedenen Kubernetes-Elemente, die in einem Namespace vorhanden sind, und deren Zustände.

Voraussetzungen

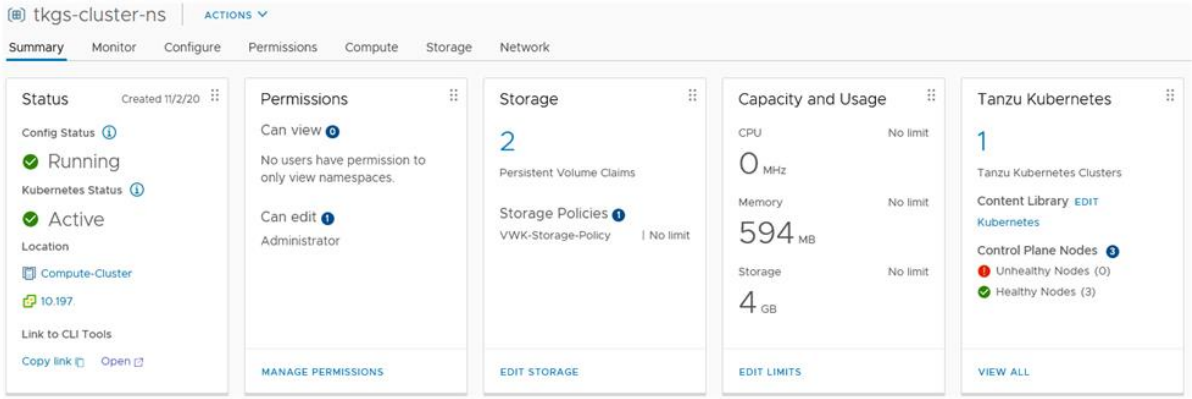
Erstellen und Konfigurieren eines vSphere-Namespace.

Verfahren

1. Melden Sie sich über vSphere Client bei vCenter Server an.
2. Navigieren Sie zur Ansicht **Menü > Hosts und Cluster**.
3. Wählen Sie den vCenter-Cluster aus, in dem Sie **Arbeitslastverwaltung** aktiviert haben.
4. Wählen Sie den Ressourcenpool **Namespaces** aus und erweitern Sie dessen Inhalte.

   Die Knoten der Steuerungsebene von Supervisor befinden sich im Ressourcenpool der Namespaces. Darüber hinaus befindet sich jeder vSphere-Namespace, der für diesen Supervisor erstellt wird, im Ressourcenpool **Namespaces**.
5. Wählen Sie das vSphere-Namespace-Objekt aus, das als Fenstersymbol dargestellt wird.

   Auf der Registerkarte **Übersicht** sehen Sie die verschiedenen Konfigurationsabschnitte für den vSphere-Namespace, einschließlich **Status**, **Berechtigungen**, **Speicher**, **Kapazität und Nutzung** sowie **Tanzu Kubernetes**. Von diesem Bildschirm aus können Sie diese Einstellungen verwalten.



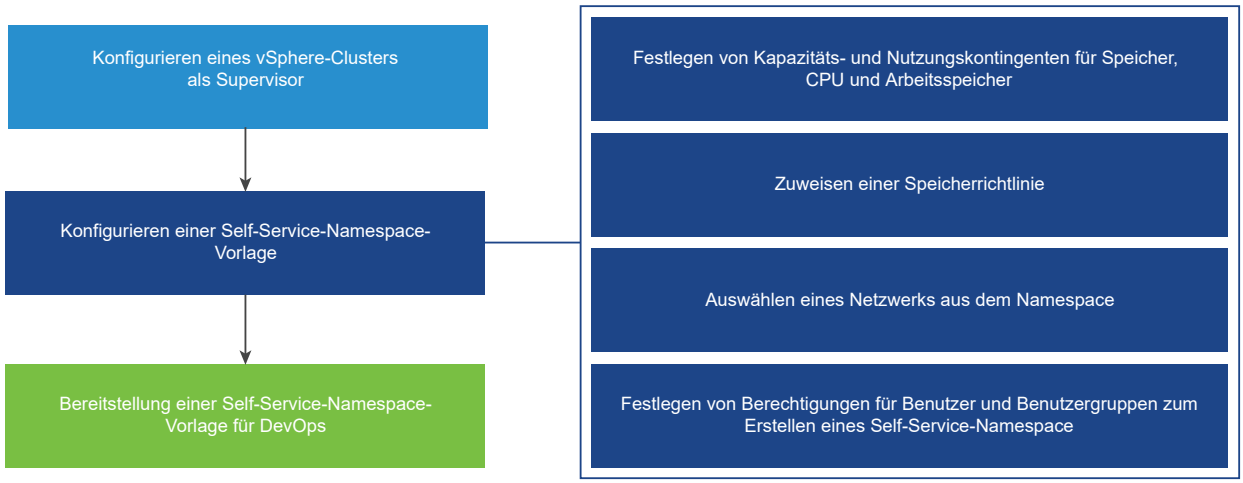
Bereitstellen einer Self-Service-Namespace-Vorlage in vSphere IaaS control plane

Als vSphere-Administrator können Sie einen Supervisor-Namespace erstellen, CPU-, Arbeitsspeicher- und Speichergrenzwerte für den Namespace festlegen, Berechtigungen zuweisen und den Namespace-Dienst auf einem Cluster als Vorlage aktivieren. Daher können DevOps-Ingenieure einen Supervisor-Namespace im Self-Service-Modus erstellen und Arbeitslasten innerhalb des Namespace bereitstellen.

Workflow zum Erstellen und Konfigurieren eines Self-Service-Namespace

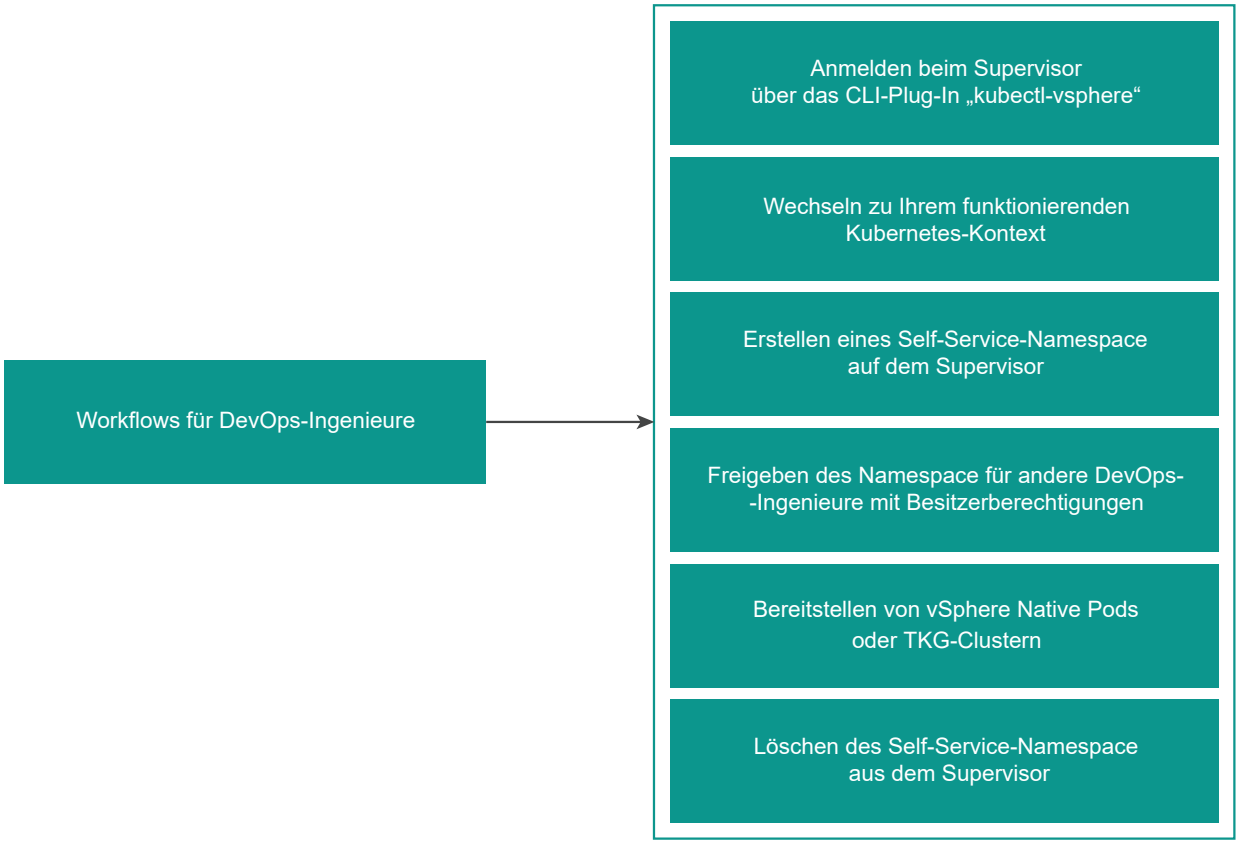
Als vSphere-Administrator können Sie einen Supervisor-Namespace erstellen, CPU-, Arbeitsspeicher- und Speichergrenzwerte für den Namespace festlegen, Berechtigungen zuweisen und den Namespace-Dienst auf einem Cluster als Vorlage bereitstellen oder aktivieren.

Abbildung 3-1. Workflow zur Bereitstellung einer Self-Service-Namespace-Vorlage



Als DevOps-Ingenieur können Sie einen Supervisor-Namespace in einer Self-Service-Form erstellen und Arbeitslasten darin bereitstellen. Sie können ihn für andere DevOps-Ingenieure freigeben oder löschen, wenn sie nicht mehr benötigt wird. Um den Namespace für andere DevOps-Ingenieure freizugeben, wenden Sie sich an den vSphere-Administrator.

Abbildung 3-2. Workflow zur Erstellung von Self-Service-Namespaces



Erstellen und Konfigurieren einer Self-Service-Namespace-Vorlage

Als vSphere-Administrator können Sie einen Supervisor-Namespace als Self-Service-Namespace-Vorlage erstellen und konfigurieren. DevOps-Ingenieure können dann Supervisor-Namespaces mithilfe des `kubectl`-Befehls erstellen und löschen.

Voraussetzungen

Konfigurieren Sie einen Cluster mit vSphere IaaS control plane.

Verfahren

1. Navigieren Sie in vSphere Client zum Supervisor.
2. Klicken Sie auf die Registerkarte **Konfigurieren** und wählen Sie **Allgemein** unter **Supervisor**.
3. Wählen Sie **Namespace-Dienst** aus.
4. Klicken Sie auf den Schalter **Status**, um die Funktion zu aktivieren.

   Die Seite **Namespace-Vorlage erstellen** wird angezeigt.

5 Konfigurieren Sie im Bereich **Konfiguration** die Ressourcen für den Namespace.

Option	Beschreibung
CPU	Die Menge der CPU-Ressourcen, die für den Namespace reserviert werden soll.
Arbeitsspeicher	Die Menge an Arbeitsspeicher, die für den Namespace reserviert werden soll.
Speicher	Die Gesamtmenge an Speicherplatz, die für den Namespace reserviert werden soll.
Speicherrichtlinie	Speicherrichtlinien für Arbeitslasten, die dauerhaften Speicher erfordern.
Netzwerk	Wählen Sie im Dropdown-Menü **Netzwerk** ein Netzwerk für den Namespace aus.
VM-Klassen	VM-Klassen zur Bereitstellung eigenständiger VMs.
Inhaltsbibliotheken	Inhaltsbibliotheken mit VM-Images zur Verwendung für VM-Bereitstellungen.

6 Klicken Sie auf **Weiter**.

7 Fügen Sie im Bereich **Berechtigungen** DevOps-Ingenieure und -Gruppen hinzu, damit sie die Vorlage zum Erstellen von Namespaces verwenden können.

Wählen Sie eine Identitätsquelle und einen Benutzer oder eine Gruppe aus und klicken Sie auf **Weiter**.

8 Im Bereich **Überprüfen und bestätigen** werden die von Ihnen konfigurierten Eigenschaften angezeigt.

Überprüfen Sie die Eigenschaften und klicken Sie auf **Fertig**.

Ergebnisse

Eine Namespace-Vorlage ist konfiguriert und befindet sich im Zustand „Aktiven“. Als vSphere-Administrator können Sie die Vorlage bearbeiten. DevOps-Ingenieure können die Vorlage zum Erstellen von Namespaces verwenden.

Deaktivieren eines Self-Service-Namespace

Als vSphere-Administrator können Sie einen Self-Service-Namespace auf dem Cluster deaktivieren.

Wenn Sie eine Self-Service-Namespace-Vorlage deaktivieren, können DevOps-Ingenieure die Vorlage nicht zum Erstellen neuer Namespaces im Cluster verwenden. Sie können die Namespaces löschen, die sie bereits erstellt haben.

Verfahren

1 Navigieren Sie in vSphere Client zum Supervisor.

2 Klicken Sie auf die Registerkarte **Konfigurieren** und wählen Sie **Allgemein** unter **Supervisor**.

3 Schalten Sie im Bereich **Namespace-Dienst** den Schalter **Status** um, um die Vorlage zu deaktivieren.

4 Um die Vorlage erneut zu aktivieren, schalten Sie den **Status** um.

Sie können entweder einen anderen Self-Service-Namespace erstellen oder den vorhandenen verwenden.

Erstellen eines Self-Service-Namespace

Als DevOps-Ingenieur können Sie einen Self-Service-Namespace erstellen und darin Arbeitslasten ausführen. Nachdem Sie den Namespace erstellt haben, können Sie ihn für andere DevOps-Ingenieure freigeben oder löschen, wenn er nicht mehr benötigt wird.

Voraussetzungen

- Stellen Sie sicher, dass ein vSphere-Administrator eine Self-Service-Namespace-Vorlage im Cluster erstellt und aktiviert hat. Weitere Informationen finden Sie unter Erstellen und Konfigurieren einer Self-Service-Namespace-Vorlage .
- Überprüfen Sie, ob Sie der Berechtigungsliste in der Self-Service-Namespace-Vorlage entweder einzeln oder als Mitglied einer Gruppe hinzugefügt wurden.
- Rufen Sie die IP-Adresse der Supervisor-Steuerungsebene ab.

Verfahren

1 Authentifizieren Sie sich mithilfe des vSphere-Plug-In für kubectl beim Supervisor. Weitere Informationen finden Sie unter Verbindung zum Supervisor als vCenter Single Sign-On Benutzer herstellen.

```
kubectl vsphere login --server=IP-ADDRESS --vsphere-username USERNAME
```

2 Führen Sie einen Kontextwechsel zum Supervisor durch.

```
kubectl config use-context SUPERVISOR-CLUSTER-IP
```

3 Erstellen Sie einen Self-Service-Namespace auf dem Cluster.

```
kubectl create namespace NAMESPACE NAME
```

Beispiel:

```
kubectl create namespace test-ns
```

Hinweis Besitzerberechtigungen stehen DevOps-Ingenieuren zur Verfügung, nachdem Sie vSphere IaaS control plane aktiviert und den Cluster aktualisiert haben. Wenn Sie nur vCenter Server und nicht den Cluster aktualisiert haben, verfügen die DevOps-Ingenieure nur über Bearbeitungsberechtigungen für die Namespaces.

Der von Ihnen erstellte Namespace wird im Cluster angezeigt. Um den Namespace für andere DevOps-Ingenieure freizugeben, wenden Sie sich an den vSphere-Administrator.

Erstellen eines Self-Service-Namespace mit Anmerkungen und Bezeichnungen

DevOps-Ingenieure können über die kubectl-Befehlszeile Self-Service-Namespaces mit Anmerkungen und Bezeichnungen erstellen.

DevOps-Ingenieure können ein YAML-Manifest mit benutzerdefinierten Anmerkungen und Bezeichnungen verwenden.

Verfahren

1 Melden Sie sich beim Supervisor an.

```
kubectl vsphere login --server IP-ADDRESS-SUPERVISOR-CLUSTER --vsphere-username VCENTER-SSO-USERNAME
```

2 Erstellen Sie eine Namespace-YAML-Manifestdatei mit Anmerkungen und Bezeichnungen.

```
kubectl create -f ns-create.yaml
```

Erstellen Sie z. B. die folgende `ns-create.yaml`-Datei:

```
apiVersion: v1
kind: Namespace
metadata:
  name: test-ns-yaml
  labels:
    my-label: "my-label-val-yaml"
  annotations:
    my-ann-yaml: "my-ann-val-yaml"
```

3 Wenden Sie das YAML-Manifest an.

```
kubectl create -f ns-create.yaml
```

oder

```
kubectl apply -f ns-create.yaml
```

4 Beschreiben Sie den Namespace, den Sie erstellt haben, um die Änderungen anzuzeigen.

```
root@localhost [ /tmp ]# kubectl describe ns test-ns-yaml
Name:         test-ns-yaml
Labels:       my-label=my-label-val-yaml
              vSphereClusterID=domain-c50
Annotations:  my-ann-yaml: my-ann-val-yaml
              vmware-system-namespace-owner-count: 1
              vmware-system-resource-pool: resgroup-171
              vmware-system-resource-pool-cpu-limit: 0.4770
              vmware-system-resource-pool-memory-limit: 2000Mi
              vmware-system-self-service-namespace: true
              vmware-system-vm-folder: group-v172
Status:       Active
```

```
Resource Quotas
 Name:             test-ns-yaml
 Resource          Used  Hard
 --------          ---   ---
 requests.storage  0     5000Mi

 Name:                                                                                test-ns-
yaml-storagequota
 Resource                                                                             Used  Hard
 --------                                                                             ---   ---
 namespace-service-storage-profile.storageclass.storage.k8s.io/requests.storage  0
9223372036854775807

No LimitRange resource.
```

Aktualisieren eines Self-Service-Namespace mit kubectl annotate und kubectl label

Als DevOps-Ingenieur können Sie Anmerkungen und Beschriftungen von Self-Service-Namespaces mit den Befehlen `kubectl annotate` und `kubectl label` aktualisieren oder löschen.

Voraussetzungen

Vergewissern Sie sich, dass Sie über Eigentümerberechtigungen für den Namespace verfügen, den Sie aktualisieren möchten.

Verfahren

1 Melden Sie sich beim Supervisor an.

```
kubectl vsphere login --server IP-ADDRESS-SUPERVISOR-CLUSTER --vsphere-
username VCENTER-SSO-USERNAME
```

2 Beschreiben Sie den Namespace, den Sie aktualisieren möchten.

```
root@localhost [ /tmp ]# kubectl describe ns testns
Name:         testns
Labels:       my-label=test-label-2
              vSphereClusterID=domain-c50
Annotations:  my-ann: test-ann-2
              vmware-system-namespace-owner-count: 2
              vmware-system-resource-pool: resgroup-153
              vmware-system-resource-pool-cpu-limit: 0.4770
              vmware-system-resource-pool-memory-limit: 2000Mi
              vmware-system-self-service-namespace: true
              vmware-system-vm-folder: group-v154
Status:       Active


Resource Quotas
 Name:             testns
 Resource          Used  Hard
 --------          ---   ---
```

```
 requests.storage  0     5000Mi


 Name:                                                                                testns-
storagequota
 Resource                                                                             Used  Hard
 --------                                                                             ---   ---
 namespace-service-storage-profile.storageclass.storage.k8s.io/requests.storage  0
9223372036854775807
```

3 Aktualisieren Sie Anmerkungen mit dem Befehl `kubectl annotate`.

Beispielsweise `kubectl annotate --overwrite ns testns my-ann="test-ann-3"`

Um eine Anmerkung zu löschen, führen Sie den Befehl `kubectl annotate --overwrite ns testns my-ann-` aus.

4 Aktualisieren Sie Beschriftungen mit dem Befehl `kubectl label`.

Beispielsweise `kubectl label --overwrite ns testns my-label="test-label-3"`

Um eine Beschriftung zu löschen, führen Sie den Befehl `kubectl label --overwrite ns testns my-label-` aus.

5 Beschreiben Sie den Namespace, um die Updates anzuzeigen.

```
root@localhost [ /tmp ]# kubectl describe ns testns
Name:         testns
Labels:       my-label=test-label-3
              vSphereClusterID=domain-c50
Annotations:  my-ann: test-ann-3
              vmware-system-namespace-owner-count: 2
              vmware-system-resource-pool: resgroup-153
              vmware-system-resource-pool-cpu-limit: 0.4770
              vmware-system-resource-pool-memory-limit: 2000Mi
              vmware-system-self-service-namespace: true
              vmware-system-vm-folder: group-v154
Status:       Active


Resource Quotas
 Name:             testns
 Resource          Used  Hard
 --------          ---   ---
 requests.storage  0     5000Mi


 Name:                                                                                testns-
storagequota
 Resource                                                                             Used  Hard
 --------                                                                             ---   ---
 namespace-service-storage-profile.storageclass.storage.k8s.io/requests.storage  0
```

```
9223372036854775807


No LimitRange resource.
```

Aktualisieren eines Self-Service-Namespace mit kubectl edit

Als DevOps-Ingenieur können Sie Self-Service-Namespaces mit dem Befehl `kubectl edit` aktualisieren.

Voraussetzungen

Vergewissern Sie sich, dass Sie über Eigentümerberechtigungen für den Namespace verfügen, den Sie aktualisieren möchten.

Verfahren

1 Melden Sie sich beim Supervisor an.

```
kubectl vsphere login --server IP-ADDRESS-SUPERVISOR-CLUSTER --vsphere-username VCENTER-SSO-USERNAME
```

2 Beschreiben Sie den Namespace, den Sie aktualisieren möchten.

```
kubectl describe ns testns-1
Name:         testns
Labels:       vSphereClusterID=domain-c50
Annotations:  my-ann: test-ann-2
              vmware-system-namespace-owner-count: 2
              vmware-system-resource-pool: resgroup-153
              vmware-system-resource-pool-cpu-limit: 0.4770
              vmware-system-resource-pool-memory-limit: 2000Mi
              vmware-system-self-service-namespace: true
              vmware-system-vm-folder: group-v154
Status:       Active


Resource Quotas
 Name:             testns-1
 Resource          Used  Hard
 --------          ---   ---
 requests.storage  0     5000Mi


 Name:                                                                                 testns-1-
storagequota
 Resource                                                                              Used  Hard
 --------                                                                              ---   ---
 namespace-service-storage-profile.storageclass.storage.k8s.io/requests.storage  0
9223372036854775807
```

3 Bearbeiten Sie den Namespace mit dem Befehl `kubectl edit`.

Beispielsweise `kubectl edit ns testns-1`

Der Befehl `kubectl edit` öffnet das Namespace-Manifest in dem durch Ihre KUBE_EDITOR- oder EDITOR-Umgebungsvariable definierten Texteditor geöffnet.

4 Aktualisieren Sie die Beschriftungen.

Beispielsweise `my-label=test-label`

5 Aktualisieren Sie die Anmerkungen.

Beispielsweise `my-ann: test-ann`

6 Beschreiben Sie den Namespace, um die Updates anzuzeigen.

```
root@localhost [ /tmp ]# kubectl describe ns testns-1
Name:         testns-1
Labels:       my-label=test-label
              vSphereClusterID=domain-c50
Annotations:  my-ann: test-ann
              vmware-system-namespace-owner-count: 1
              vmware-system-resource-pool: resgroup-173
              vmware-system-resource-pool-cpu-limit: 0.4770
              vmware-system-resource-pool-memory-limit: 2000Mi
              vmware-system-self-service-namespace: true
              vmware-system-vm-folder: group-v174
Status:       Active


Resource Quotas
 Name:             testns-1
 Resource          Used  Hard
 --------          ---   ---
 requests.storage  0     5000Mi


 Name:                                                                          testns-1-
storagequota
 Resource                                                                       Used  Hard
 --------                                                                       ---   ---
 namespace-service-storage-profile.storageclass.storage.k8s.io/requests.storage  0
9223372036854775807


No LimitRange resource.
```

Löschen eines Self-Service-Namespace

Als DevOps-Ingenieur können Sie einen von Ihnen erstellten Self-Service-Namespace löschen.

Voraussetzungen

Stellen Sie sicher, dass Sie einen Self-Service-Namespace mithilfe des vSphere-Plug-In für kubectl erstellt haben.

Verfahren

1 Authentifizieren Sie sich mithilfe des vSphere-Plug-In für kubectl beim Supervisor. Weitere Informationen finden Sie unter Verbindung zum Supervisor als vCenter Single Sign-On Benutzer herstellen.

2 Löschen Sie den Self-Service-Namespace aus dem Cluster.

```
kubectl delete namespace NAMESPACE NAME
```

Beispiel:

```
kubectl delete namespace test-ns
```

Ändern der Speichereinstellungen in einem vSphere Namespace

Speicherrichtlinien, die einem Namespace in einem Supervisor zugewiesen sind, stellen dem DevOps-Team persistenten Speicher zur Verfügung. Diese Speicherrichtlinien steuern, wie persistente Volumes und Tanzu Kubernetes-Clusterknoten in vSphere-Datenspeichern platziert werden. Als vSphere-Administrator weisen Sie die Speicherrichtlinien in der Regel zu, wenn Sie den Namespace konfigurieren. Wenn Sie Änderungen an den ursprünglichen Zuweisungen der Speicherrichtlinien vornehmen müssen, führen Sie diese Aufgabe aus.

Voraussetzungen

- Bevor Sie eine Speicherrichtlinie aus VMware vCenter oder einem vSphere-Namespace löschen oder die Zuweisung der Speicherrichtlinie ändern, stellen Sie sicher, dass keine Beanspruchung eines dauerhaften Volumes mit der entsprechenden Speicherklasse im Namespace ausgeführt wird. Stellen Sie außerdem sicher, dass kein Tanzu Kubernetes-Cluster die Speicherklasse verwendet.
- Wenn sich der Namespace in einem Supervisor mit drei Zonen befindet, verwenden Sie topologiefähige Richtlinien. Sie können dem Namespace mit drei Zonen keine Speicherrichtlinien zuweisen, die nicht topologiefähig sind.

Verfahren

1 Navigieren Sie in vSphere Client zum Namespace.

   a Wählen Sie im vSphere Client-Startmenü die Option **Arbeitslastverwaltung** aus.

   b Klicken Sie auf die Registerkarte **Namespaces** und klicken Sie dann auf den Namespace.

2 Klicken Sie auf die Registerkarte **Speicher** und anschließend auf **Speicherrichtlinien**.

3 Klicken Sie auf das Symbol **Bearbeiten**, um die Zuweisungen der Speicherrichtlinien zu ändern.

Hinzufügen von Sicherheitsrichtlinien zu einem NSX vSphere-Namespace

Ein Supervisor, der ein NSX-Netzwerk nutzt, unterstützt Netzwerksicherheitsrichtlinien, die über eine Sicherheitsrichtlinien-CRD konfiguriert sind.

Erstellen einer Sicherheitsrichtlinie

Als DevOps können Sie die Sicherheitsrichtlinien-CRD so konfigurieren, dass eine NSX-basierte Sicherheitsrichtlinie auf einen Supervisor-Namespace angewendet wird. Die Sicherheitsrichtlinie schützt den Datenverkehr für vSphere-Pods und VMs. VMs enthalten TKG-Clusterknoten und andere VMs, die im Supervisor bereitgestellt werden.

Voraussetzungen

Verwenden Sie NSX, Version 3.2 oder höher.

Verfahren

1. Erstellen Sie eine Sicherheitsrichtlinien-CRD.

   Die zu verwendenden Felder und CRD-Beispiele finden Sie in der Dokumentation zur NSX-Operator-Sicherheitsrichtlinien-CRD auf GitHub.

2. Greifen Sie in der Kubernetes-Umgebung auf Ihren Namespace zu.

   Weitere Informationen finden Sie unter Festlegen und Verwenden des Supervisor-Kontexts.

3. Wenden Sie die Sicherheitsrichtlinie auf den Namespace an.

   ```
   kubectl apply -f policy-name.yaml
   ```

4. Zeigen Sie Ihre Sicherheitsrichtlinie an.

   a. Zeigen Sie Details für die Sicherheitsrichtlinie an.

   ```
   kubectl get securitypolicy policy-name
   ```

   b. Zeigen Sie eine Beschreibung Ihrer Sicherheitsrichtlinie an.

   ```
   kubectl describe securitypolicy policy-name
   ```

Ergebnisse

Sie können auch die NSX-Benutzeroberfläche verwenden, um Details Ihrer Richtlinie anzuzeigen. Weitere Informationen finden Sie auf der Seite mit der *VMware NSX-Dokumentation*.

Konfigurieren von Netzwerk- und Lastausgleichsdienstparametern für einen Namespacensraum

vSphere IaaS control plane unterstützt nicht die Bearbeitung der NCP-Konfigurationsdatei `ncp.ini`. Sie können CustomResourceDefinitions (CRDs) in NCP erstellen, um Netzwerk- und Lastausgleichsdienstparameter zu konfigurieren.

NCPSetting-CRD

Erstellen Sie eine **NCPSetting**-CRD und legen Sie Werte für die NCP-Konfiguration fest.

In der folgenden Tabelle werden die Netzwerk- und Lastausgleichsdienstparameter beschrieben, die Sie konfigurieren können:

Parameter	Beschreibung
`log_dropped_traffic`	Gibt an, ob DENY-Regeln für verteilte Firewalls protokolliert werden. Werte: `True`, `False` Der Standardwert lautet `false`.
`log_firewall_traffic`	Gibt an, ob DFW-Regeln protokolliert werden. Werte sind: ■ `ALL`. Aktiviert die Protokollierung für alle DFW-Regeln. ■ `DENY`. Aktiviert die Protokollierung nur für DENY-Regeln.
`pool_algorithm`	Option zum Festlegen des Lastausgleichsalgorithmus im Poolobjekt des Lastausgleichsdiensts. Werte sind: ■ Round_Robin ■ Weighted_Round_Robin ■ Least_Connection ■ Weighted_Least_Connection ■ IP-Hash Der Standardwert ist Round-Robin.
`service_size`	Option zum Festlegen der Größe des Lastausgleichsdiensts. Werte sind `Small`, `Medium` und `Large`. Der Standardwert lautet `Small`.
`l7_persistence`	Option zum Festlegen der Persistenzoption des Lastausgleichsdiensts. Werte sind: ■ `cookie`. ■ `source_ip`
`l7_persistence_timeout`	Persistenz-Zeitüberschreitungswert in Sekunden für das L7-Persistenzprofil.

Parameter	Beschreibung
`cookie_name`	Geben Sie einen Cookie-Namen an, wenn `l7_persistence type` auf `cookie` festgelegt ist.
`x_forward_for`	Aktivieren Sie X_forward_for für Kopfzeilen im Ingress. Werte sind: ■ `Insert` ■ `Replace`
`snat_rule_logging`	Option zur Auswahl der Protokollierung für SNAT-Regeln. Werte sind: ■ `None` ■ `Basic`. Protokollierung für alle NamespacesNamensräume. ■ `Extended`. Protokollierung für alle Namespaces Namensräume und Dienste.
`vs_access_log`	Protokolleigenschaften des virtuellen Servers für Ingress und Route. Werte sind: ■ `VS_access_log_none` ■ `access_log_enabled`. Aktiviert die Protokollierung für den virtuellen Layer 7-Server. ■ `log_significant_event_only`. Anforderungen mit einem HTTP-Antwortstatus >=400 werden als wichtiges Ereignis behandelt. Der Standardwert lautet `VS_access_log_none`.
`ip_reallocation_time`	Zeit in Sekunden, bevor eine freigegebene IP-Adresse neu zugewiesen werden kann.

Weitere Informationen zu NCP- und NSX-Objekten finden Sie in der *NSX*-Dokumentation.

Führen Sie die folgenden Schritte aus, um diese Funktion zu aktivieren:

1 Legen Sie **enable_ncp_setting_crd** auf **True** fest.

2 Erstellen einer YAML-Datei mit der folgenden Vorlage:

```
apiVersion: apiextensions.k8s.io/v1
kind: CustomResourceDefinition
metadata:
  name: ncpsettings.vmware.com
spec:
  group: vmware.com
  versions:
    - name: v1
      served: true
      storage: true
      schema:
        openAPIV3Schema:
          type: object
            properties:
              spec:
```

```
                type: object
                properties:
                  nsx_v3:
                    type: object
                    properties:
                      log_dropped_traffic:
                        description: 'Indicates whether distributed firewall DENY rules
are logged.'
                        type: boolean
                      log_firewall_traffic:
                        description: 'Indicate whether DFW rules are logged.'
........ All configs that are allow to be configured via CRD........

  scope: Cluster
  names:
    plural: ncpsettings
    singular: ncpsetting
    kind: NCPSetting
    shortNames:
    - ncpstg
```

Beispiel:

```
apiVersion: vmware.com/v1alpha2
kind: NCPSetting
metadata:
    name: ncp-setting-crd
spec:
    nsx_v3:
        log_dropped_traffic: True
        log_firewall_traffic: ALL
        pool_algorithm: Round_Robin
        l7_persistence: cookie
        x_forwarded_for: Insert
```

3 Wenden Sie die YAML-Datei mit dem folgenden Befehl an:

```
kubectl apply -f ncp-setting-crd.yaml.j2
```

Um zu verhindern, dass mehrere CRDs denselben Konfigurationswert überschreiben, verarbeitet NCP nur das CRD-Objekt mit dem Namen **ncp-setting-crd**. Andere CRDs mit unterschiedlichen Namen werden mit Fehlern vermerkt, und NCP verarbeitet diese CRDs nicht.

NCP-Konfiguration wird überschrieben

Die Konfigurationsparameter in der CRD haben möglicherweise entsprechende NSX-Objekte. Wenn Sie eine CRD erstellen, um die Parameter zu überschreiben, ändert die CRD die Parameter in den Objekten nicht, außer in folgenden Fällen:

- `l7_persistence`, `l7_persistence_timeout` und `cookie_name`. Wenn `l7_persistence` von der CRD geändert wird, erstellt NCP ein neues Persistenzprofil mit den Werten von `l7_persistence`, `l7_persistence_timeout` und `cookie_name`.

Wenn `l7_persistence_timeout` und `cookie_name` über die CRD geändert werden, wird das vorhandene Profil basierend auf den neuen Werten aktualisiert.

- `x_forwarded_for`. Wenn `x_forwarded_for` von der CRD geändert wird, erstellt NCP ein neues Anwendungsprofil basierend auf seinem Wert.
- `vs_access_log`. Wenn `vs_access_log` durch die CRD geändert wird, aktualisiert NCP die Protokollierungsoption der virtuellen Server entsprechend.

Verwalten von Supervisor-Dienste mit vSphere IaaS control plane 4

Supervisor-Dienste sind vSphere-zertifizierte Kubernetes-Operatoren, die Infrastructure-as-a-Service-Komponenten und eng integrierte Dienste von unabhängigen Softwareanbietern für Entwickler bereitstellen. Sie können Supervisor-Dienste in der vSphere IaaS control plane-Umgebung installieren und verwalten, um sie für die Verwendung mit Arbeitslasten verfügbar zu machen.

Wenn Supervisor-Dienste auf Supervisoren installiert sind, können DevOps-Ingenieure diese auf verschiedene Arten nutzen:

- Gemeinsam genutzte Supervisor-Dienste wie Harbor stellen Funktionen direkt für Arbeitslasten bereit, die in TKG-Clustern, vSphere-Pods oder VMs ausgeführt werden.
- Supervisor-Dienste, die einen Operator wie MinIO enthalten, stellen in der Regel API- oder grafische Oberflächen bereit, mit denen DevOps-Ingenieure Instanzen des Diensts in einem vSphere-Namespace über CRDs erstellen und verwalten können. Um beispielsweise einen MinIO-Bucket zu erstellen, verwenden Sie eine CRD, um den Bucket in einem vSphere-Namespace zu erstellen.

Weitere Informationen zu den unterstützten Supervisor-Dienste und zur Vorgehensweise beim Herunterladen ihrer YAML-Dienstdateien finden Sie unter http://vmware.com/go/supervisor-service.

Unterstützte Supervisor-Bereitstellungen mit Supervisor-Dienste

Supervisor-Dienste-Dienste werden als vSphere-Pods bereitgestellt. In vSphere 8.0 unterstützen nur Supervisoren, die mit dem NSX-Netzwerk-Stack konfiguriert sind, vSphere-Pods bzw. Supervisor-Dienste. Ab vSphere 8 Update 1 werden vSphere-Pods, die von Supervisor-Dienste bereitgestellt werden, auf Supervisoren unterstützt, die mit den beiden Netzwerktypen NSX oder VDS bereitgestellt werden.

Hinweis Wenn der Supervisor mit dem VDS-Netzwerk-Stack konfiguriert ist, können Sie Supervisor-Dienste nicht auf NSX-gestützten Netzwerken (von NSX erstellte verteilte Portgruppen) ausführen.

In der folgenden Tabelle wird die Unterstützung für vSphere-Pods aufgelistet, die von Supervisor-Dienste in den vorhandenen Supervisor-Bereitstellungen für vSphere 8 und höher zur Verfügung gestellt werden:

vSphere-Version	NSX-Netzwerk	VDS-Netzwerk	Supervisor-Version	Supervisor mit einer Zone	Supervisor mit drei Zonen
vSphere 8	Ja	Nein	1.23 und höher	Ja	Nein
vSphere 8.0.1 und höher	Ja	Ja	1.24 und höher	Ja	Nein
vSphere 8.0.3 und höher	Ja	Ja	1.28 und höher	Ja	Ja

Supervisor-Dienste-Lebenszyklusverwaltung

Sie verwalten Supervisor-Diensteüber den vSphere Client. Sie können Supervisor-Dienste auf Supervisoren installieren, die zugehörigen Versionen aktualisieren oder Supervisor-Dienste aus Supervisoren deinstallieren. Ein Supervisor-Dienst kann über mehrere Versionen verfügen, die bei vCenter Server registriert sind. Sie können jedoch nur jeweils eine Version auf einem Supervisor installieren.

Tabelle 4-1. Status von Supervisor-Dienst

Zustand	Dienstversion	Gesamter Dienst
Aktiv	Die Dienstversion kann jetzt auf Supervisoren installiert werden.	Mindestens eine Dienstversion befindet sich im aktiven Zustand.
Deaktiviert	Die Dienstversion kann nicht in Supervisoren installiert werden. Sie kann weiterhin in beliebigen Supervisoren ausgeführt werden, in denen sie installiert ist, aber Sie können eine deaktivierte Dienstversion nicht in neuen Supervisoren installieren.	Wenn ein gesamter Supervisor-Dienst deaktiviert wird, werden alle seine Versionen ebenfalls deaktiviert, und solange Sie den Dienst nicht erneut aktivieren, können Sie weder Versionen in Supervisoren installieren noch neue Dienstversionen hinzufügen.

Die Verwaltung des Lebenszyklus eines Supervisor-Dienst umfasst die folgenden Vorgänge:

Vorgang	Beschreibung
Hinzufügen eines neuen Supervisor-Dienstzu vCenter Server	Wenn Sie einen neuen Dienst zu vCenter Server hinzufügen, werden der Dienst und alle Informationen darüber bei vCenter Server registriert. Der Dienst ist noch nicht in einem Supervisor installiert. Nachdem der Dienst bei vCenter Server registriert wurde, lautet sein Status „Aktiv“. Dies bedeutet, dass Sie diesen Dienst in Supervisoren installieren können.
Hinzufügen einer neuen Supervisor-Dienst-Version zu vCenter Server	Nachdem Sie einen Supervisor-Dienst zu vCenter Server hinzugefügt haben, können Sie neue Versionen dieses Diensts hinzufügen. Nachdem die neue Dienstversion bei vCenter Server registriert wurde, wird sie in den aktiven Zustand versetzt und Sie können die Version in Supervisoren installieren.
Installieren eines Supervisor-Dienst in Supervisoren	Wenn Sie einen Supervisor-Dienst auf einem Supervisor installieren, wird die YAML-Datei des Diensts auf den Supervisor angewendet, und alle vSphere-Pods und erforderlichen Ressourcen werden erstellt, damit der Dienst ausgeführt werden kann. Ein vSphere-Namespace wird automatisch für jeden Supervisor-Dienst erstellt, den Sie auf einem Supervisor installieren. Sie können die Dienstressourcen über diesen vSphere-Namespace verwalten. Supervisor-Dienste verfügen möglicherweise auch über ein Benutzeroberflächen-Plug-In für vCenter Server, mit dem Sie die Dienstkonfiguration verwalten können.
Upgrade eines Supervisor-Diensts	Sie können einen Dienst aktualisieren, der in einem Supervisor installiert ist, indem Sie zuerst eine neue Dienstversion zu vCenter Server hinzufügen und dann die neue Version im Supervisor installieren. Während des Dienst-Upgrades wird die YAML-Datei der neuen Version auf den Supervisor angewendet. Alle Ressourcen, die in der vorherigen Dienstversion angegeben sind und von der neuen Version nicht benötigt werden, werden gelöscht. Wenn beispielsweise in Version 1 Pod A und in Version 2 Pod B angegeben ist, wird nach dem Upgrade auf Version 2 ein neuer Pod B erstellt und Pod A gelöscht. Während des Vorgangs sind keine aktuell ausgeführten Arbeitslasten betroffen.
Deinstallieren einer Supervisor-Dienst-Version	Wenn Sie eine Dienstversion aus einem Supervisor deinstallieren, führt dies dazu, dass alle Dienstressourcen aus dem Cluster entfernt werden, einschließlich des Dienst-Namespace. Anwendungsinstanzen des Diensts in Kubernetes-Arbeitslasten werden weiterhin ausgeführt.

Vorgang	Beschreibung
Löschen einer Supervisor-Dienst-Version	Um eine Dienstversion zu löschen, müssen Sie diese Version zunächst deaktivieren und aus den Supervisoren deinstallieren, in denen sie ausgeführt wird. Dann können Sie die Dienstversion aus vCenter Server löschen.
Löschen eines ganzen Supervisor-Diensts	Um einen ganzen Dienst zu löschen, müssen Sie alle seine Versionen deaktivieren, diese Versionen dann aus Supervisoren deinstallieren und schließlich alle Dienstversionen löschen.

Kern-Supervisor-Dienste

Bei Kern-Supervisor-Dienste handelt es sich um Dienste, deren Operatoren auf der vSphere IaaS control plane während der Aktivierung des Supervisor vorinstalliert werden. Sie können Kern-Supervisor-Dienste auf Supervisoren installieren und deren Versionen aktualisieren, ohne zuerst den Supervisor aktualisieren zu müssen. Sie können die Operatoren von Kern-Supervisor-Dienste jedoch nicht aus der vSphere IaaS control plane entfernen.

Beispiele für Kern-Supervisor-Dienste sind der TKG- und der Velero-vSphere-Operator-Dienst.

Lesen Sie als Nächstes die folgenden Themen:

- Hinzufügen eines Supervisor-Dienst zu vCenter Server
- Installieren eines Supervisor-Diensts auf einem Supervisor
- Aufrufen der Verwaltungsschnittstelle eines Supervisor-Dienst im Supervisor
- Hinzufügen einer neuen Version zu einem Supervisor-Dienst
- Upgrade eines Supervisor-Dienst auf eine neuere Version
- Anzeigen der auf einem Supervisor installierten Supervisor-Dienste
- Deaktivieren eines Supervisor-Dienst oder einer Version davon
- Aktivieren einer Supervisor-Dienst-Version unter vCenter Server
- Deinstallieren eines Supervisor-Dienst von einem Supervisor
- Löschen einer Supervisor-Dienst-Version
- Löschen eines Supervisor-Diensts

Hinzufügen eines Supervisor-Dienst zu vCenter Server

Schauen Sie sich an, wie Sie Supervisor-Dienste zum vCenter Server-System hinzufügen können, auf dem Ihre vSphere IaaS control plane-Umgebung ausgeführt wird. Nachdem Sie Dienste zu

vCenter Server hinzugefügt haben, installieren Sie Supervisor-Dienste auf Supervisoren, damit Ihre DevOps-Ingenieure die Dienste in Kubernetes-Arbeitslasten verwenden können.

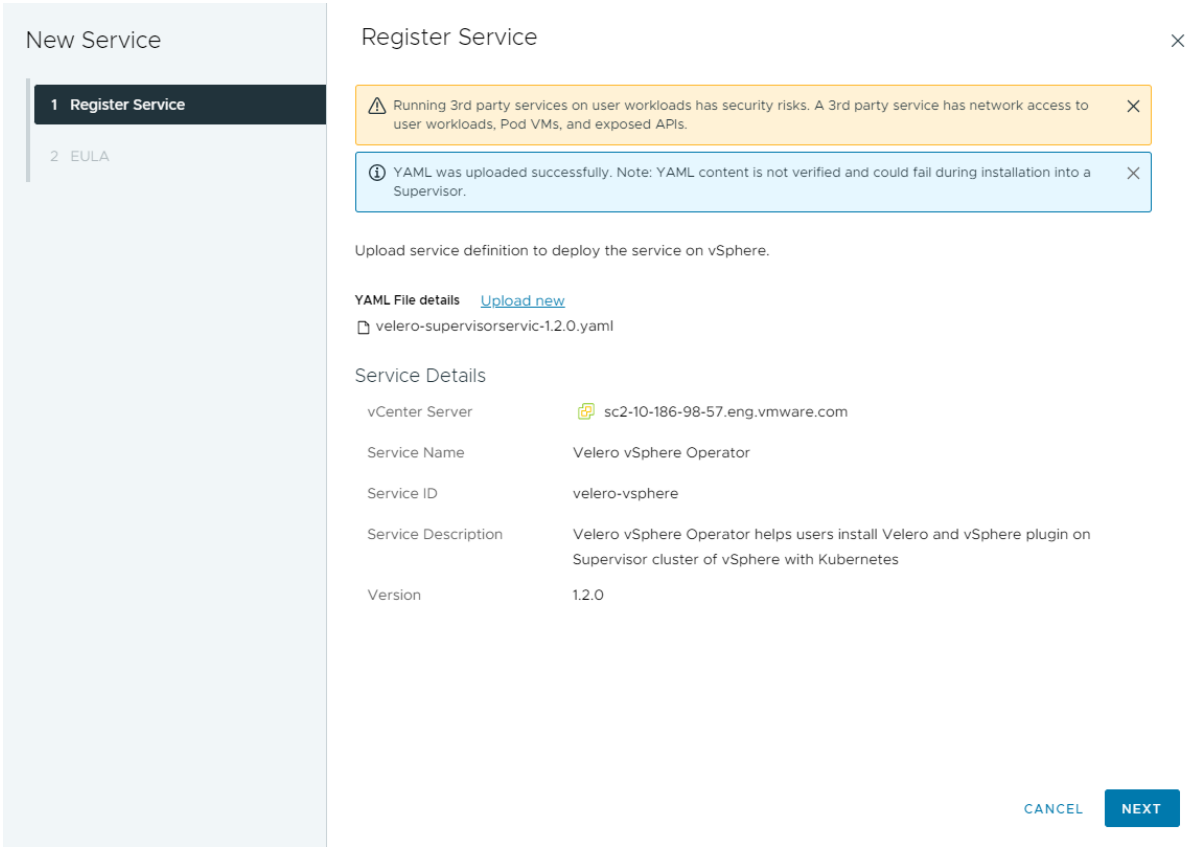
- Weitere Informationen zu den unterstützten Supervisor-Dienste und zur Vorgehensweise beim herunterladen ihrer YAML-Dienstdateien finden Sie unter http://vmware.com/go/supervisor-service.

Voraussetzungen

- Überprüfen Sie, ob Sie auf dem vCenter Server-System, dem Sie den Dienst hinzufügen, über das Recht **Supervisor-Dienste verwalten** verfügen.

Verfahren

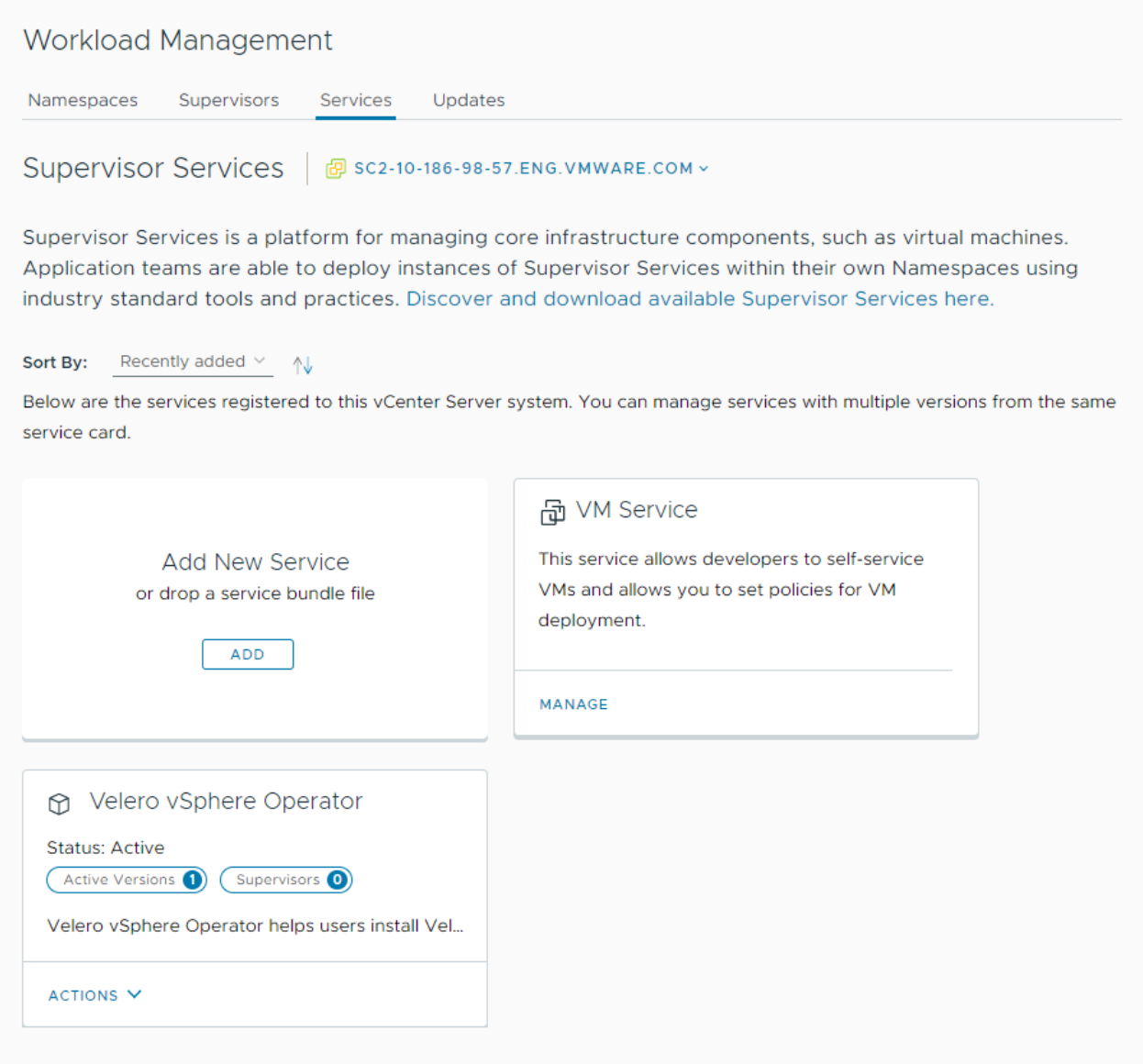
1. Wählen Sie im vSphere Client-Startmenü die Option **Arbeitslastverwaltung** aus.
2. Wählen Sie **Dienste** aus.
3. Wählen Sie oben im Dropdown-Menü ein vCenter Server-System aus.
4. Ziehen Sie die YAML-Datei des Diensts auf die Karte **Neuen Dienst hinzufügen** und legen Sie sie dort ab.



5. Klicken Sie auf **Weiter** und akzeptieren Sie gegebenenfalls die Endbenutzer-Lizenzvereinbarung.
6. Klicken Sie auf **Beenden**.

Ergebnisse

Der Supervisor-Dienst und alle zugehörigen Informationen werden beim vCenter Server-System registriert. Der Dienst befindet sich im Zustand „Aktiv“.



Nächste Schritte

Installieren Sie den Supervisor-Dienst auf Supervisoren, damit Ihre DevOps-Ingenieure ihn in Kubernetes-Arbeitslasten verwenden können. Weitere Informationen hierzu finden Sie unter Installieren eines Supervisor-Diensts auf einem Supervisor.

Installieren eines Supervisor-Diensts auf einem Supervisor

Nachdem Sie einen Supervisor-Dienst zu vCenter Server hinzugefügt haben, können Sie ihn in einem Supervisor in Ihrer vSphere IaaS control plane-Umgebung installieren. Wenn

Sie eine neuere Version eines Supervisor-Dienst installieren, überschreibt diese alle älteren Dienstversionen in dem betreffenden Supervisor. Auf einem Supervisor kann nur jeweils eine Supervisor-Dienst-Version gleichzeitig ausgeführt werden.

- Weitere Informationen zu den unterstützten Supervisor-Dienste und zur Vorgehensweise beim herunterladen ihrer YAML-Dienstdateien finden Sie unter http://vmware.com/go/supervisor-service.

Voraussetzungen

- Fügen Sie einen neuen Supervisor-Dienst oder eine neuere Version davon und einen bestehenden Dienst zu vCenter Server hinzu. Weitere Informationen finden Sie unter Hinzufügen eines Supervisor-Dienst zu vCenter Server oder Hinzufügen einer neuen Version zu einem Supervisor-Dienst.
- Stellen Sie sicher, dass Sie über die Berechtigung **Supervisor-Dienste auf Supervisoren verwalten** auf dem Supervisor verfügen, auf dem der Dienst installiert werden soll.
- Wenn der Supervisor-Dienst persistenten Speicher erfordert, konfigurieren Sie die vSAN Data Persistence-Plattform. Weitere Informationen hierzu finden Sie unter Kapitel 5 Verwenden der vSAN Data Persistence-Plattform mit modernen statusbehafteten Diensten.

Verfahren

1. Wählen Sie im vSphere Client-Startmenü die Option **Arbeitslastverwaltung** aus.
2. Wählen Sie **Dienste** aus.
3. Wählen Sie auf der Karte des Supervisor-Diensts, der installiert werden soll, **Aktionen > Dienst verwalten** aus.
4. Wählen Sie im Dropdown-Menü **Version installieren** die Supervisor-Dienst-Version aus.

   Hinweis Sie können keine Supervisor-Dienst-Versionen installieren, die deaktiviert sind.

5. Wählen Sie den Supervisor aus, in dem Sie den Dienst installieren möchten.
6. Klicken Sie auf **Weiter**.

   Kompatibilitätsvorabprüfungen werden durchgeführt, um festzustellen, ob die Supervisor-Dienstversion, die Sie installieren möchten, mit dem Supervisor kompatibel ist. Wenn die Dienstversion mit dem Supervisor kompatibel ist, können Sie mit der Installation fortfahren. Falls die ausgewählte Dienstversion nicht mit dem Supervisor kompatibel ist, werden zwei Arten von Meldungen angezeigt, die die genaue Inkompatibilität beschreiben:

   - Warnmeldungen: Sie können die Warnmeldungen überspringen, müssen sie jedoch bestätigen, um mit der Installation fortfahren zu können.
   - Fehlermeldungen. Fehlermeldung gibt an, dass die Supervisor-Dienstversion mit dem Supervisor nicht kompatibel ist und nicht installiert werden kann. Im Falle von Fehlermeldungen müssen Sie zuerst die erkannte Inkompatibilität beheben, bevor Sie den Dienst auf dem jeweiligen Supervisor installieren können.

7 Geben Sie im Feld **YAML-Dienstkonfiguration** Konfigurationseigenschaften ein, wenn der Dienst diese erfordert.

8 Zeigen Sie den Installationsfortschritt für den Dienst auf Supervisoren an.

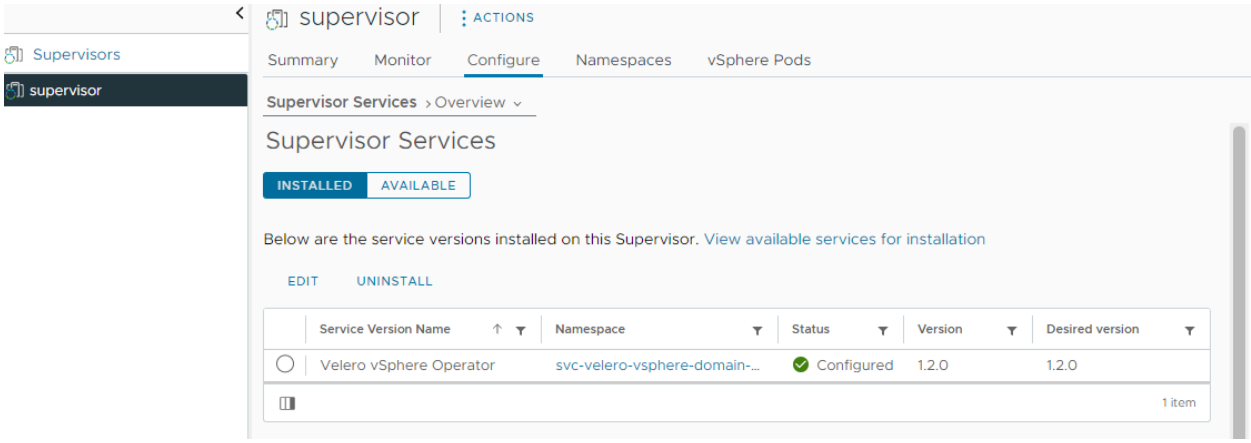
   a Wählen Sie die Registerkarte **Supervisoren** und einen Supervisor aus, auf dem Sie den Dienst installieren.

   b Klicken Sie auf **Konfigurieren** und dann auf **Supervisor Services > Überblick**.

   c Wählen Sie die Registerkarte **Installiert**.

Ergebnisse

Der Supervisor-Dienst befindet sich im Status „Wird konfiguriert“, was bedeutet, dass alle erforderlichen Ressourcen im Supervisor erstellt werden und die Dienst-YAML auf den Cluster angewendet wird. Nachdem die YAML erfolgreich auf den Supervisor mit allen seinen erstellten oder aktualisierten Ressourcen und Namespaces angewendet wurde, wechselt der Dienststatus zu „Konfiguriert“. Der Dienst ist für alle Namespaces in diesem Cluster verfügbar und DevOps-Ingenieure können ihn mit ihren Arbeitslasten verwenden.



Nächste Schritte

Konfigurieren Sie den Supervisor-Dienst über die Schnittstelle. Informationen dazu, wie Sie diese finden, erhalten Sie unter Aufrufen der Verwaltungsschnittstelle eines Supervisor-Dienst im Supervisor.

Aufrufen der Verwaltungsschnittstelle eines Supervisor-Dienst im Supervisor

Erfahren Sie, wo Sie die Verwaltungsbenutzerschnittstelle von Supervisor-Dienste finden, nachdem Sie diese in einem Supervisor installiert haben. Supervisor-Dienste können ihr eigenes Benutzeroberflächen-Plug-In für vCenter Server bereitstellen, das die Dienstschnittstelle zu der Supervisor-Ansicht im vSphere Client hinzufügt. Je nach den Besonderheiten des Supervisor-Dienst können Sie über seine Benutzeroberfläche den Dienst konfigurieren und verwalten und auch Dienstinstanzen dieses Diensts bereitstellen.

Verfahren

1 Navigieren Sie in der vSphere Client-Bestandsliste zu dem Hostcluster, den Sie in einen Supervisor konvertiert haben.

2 Klicken Sie auf die Registerkarte **Konfigurieren** und scrollen Sie nach unten zur Dienstschnittstelle. Diese ist in der Regel nach dem Dienst benannt, z. B. **MinIO**.

Hinzufügen einer neuen Version zu einem Supervisor-Dienst

Sobald Sie einen Supervisor-Dienst zu dem vCenter Server hinzugefügt haben, in dem sich Ihre vSphere IaaS control plane-Umgebung befindet, können Sie diesem Dienst eine neue Version hinzufügen. Sie können verschiedene Dienstversionen auf Supervisoren installieren.

- Weitere Informationen zu den unterstützten Supervisor-Dienste und zur Vorgehensweise beim herunterladen ihrer YAML-Dienstdateien finden Sie unter http://vmware.com/go/supervisor-service.

Voraussetzungen

- Fügen Sie den Dienst zum vCenter Server hinzu. Weitere Informationen finden Sie unter Hinzufügen eines Supervisor-Dienst zu vCenter Server.
- Überprüfen Sie, ob Sie auf dem vCenter Server-System, dem Sie die neue Dienstversion hinzufügen, über das Recht **Supervisor-Dienste verwalten** verfügen.

Verfahren

1 Wählen Sie im vSphere Client-Startmenü die Option **Arbeitslastverwaltung** aus.

2 Wählen Sie **Dienste** aus.

3 Wählen Sie auf der Karte des Diensts, dem Sie eine neue Version hinzufügen möchten, **Aktionen > Neue Version hinzufügen** aus.

4 Laden Sie die YAML-Datei der neuen Dienstversion hoch und klicken Sie auf **Weiter**.

5 Akzeptieren Sie ggf. die Endbenutzer-Lizenzvereinbarung und klicken Sie auf **Fertigstellen**.

Ergebnisse

Die neue Dienstversion wird hinzugefügt und befindet sich im Zustand „Aktiv“.

Nächste Schritte

Installieren Sie die neue Dienstversion auf Supervisoren. Weitere Informationen finden Sie unter Installieren eines Supervisor-Diensts auf einem Supervisor.

Upgrade eines Supervisor-Dienst auf eine neuere Version

Nach dem Hinzufügen einer neuen Supervisor-Dienst-Version zu vCenter Server können Sie diese Version auf Supervisoren installieren. Sie können nur Supervisor-Dienst-Versionen installieren,

die aktiv und mit den Supervisoren kompatibel sind, auf denen sie installiert werden sollen. Vorabprüfungen der Kompatibilität werden durchgeführt, um sicherzustellen, dass die neue Supervisor-Dienst-Version mit den Ziel-Supervisoren kompatibel ist.

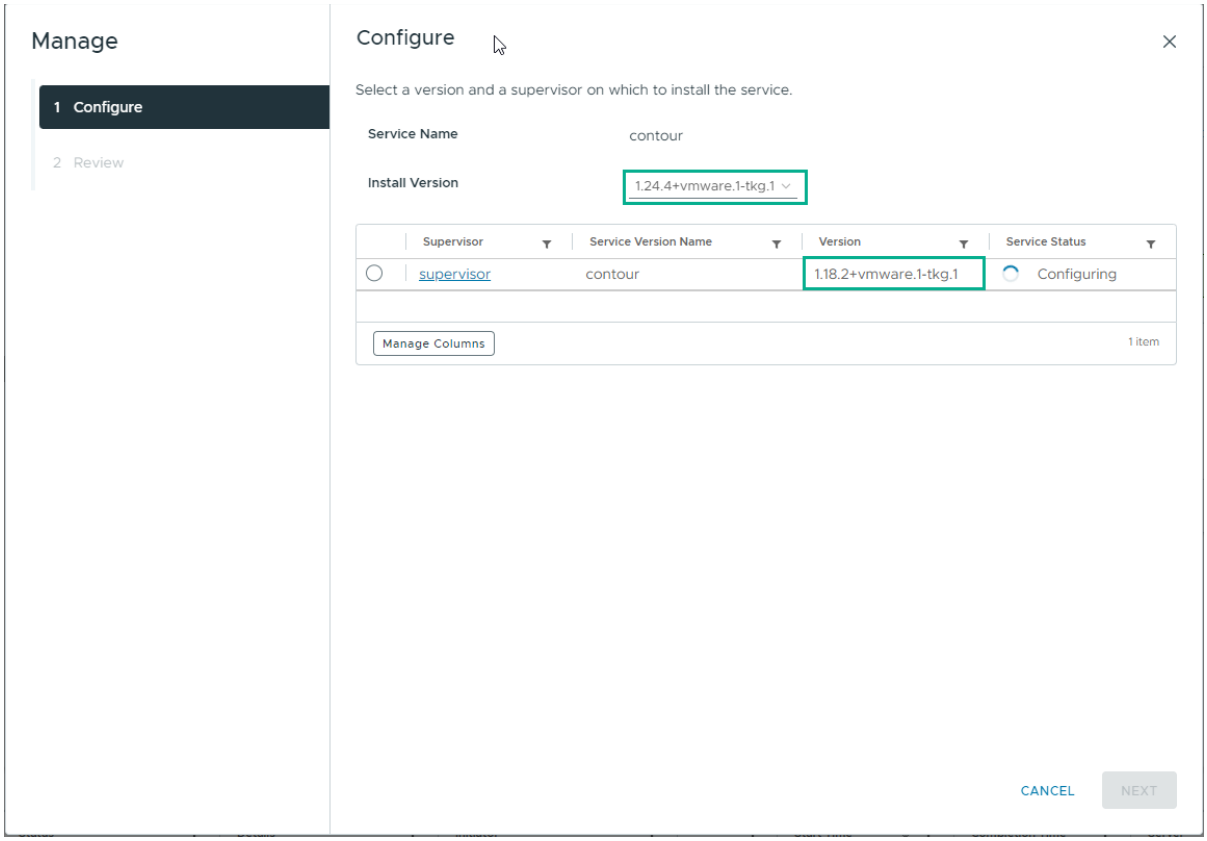
Voraussetzungen

- Fügen Sie die neue Supervisor-Dienst-Version zu vCenter Server hinzu. Weitere Informationen hierzu finden Sie unter Hinzufügen einer neuen Version zu einem Supervisor-Dienst.
- Stellen Sie sicher, dass Sie über die Berechtigung **Supervisor-Dienste auf Supervisoren verwalten** auf dem Supervisor verfügen, auf dem der Dienst installiert werden soll.

Verfahren

1. Wählen Sie im vSphere Client-Startmenü die Option **Arbeitslastverwaltung** aus.
2. Wählen Sie **Dienste** aus.
3. Wählen Sie **Dienst verwalten** aus.
4. Wählen Sie die neue zu installierende Version und den Supervisor aus, auf dem Sie sie installieren möchten.

   Stellen Sie sicher, dass es sich bei der aktuell installierten Dienstversion auf dem Supervisor um eine ältere Version handelt.



5 Klicken Sie auf **Weiter**.

Kompatibilitätsvorabprüfungen werden durchgeführt, um festzustellen, ob die Supervisor-Dienstversion, die Sie installieren möchten, mit dem Supervisor kompatibel ist. Wenn die Dienstversion mit dem Supervisor kompatibel ist, können Sie mit der Installation fortfahren. Falls die ausgewählte Dienstversion nicht mit dem Supervisor kompatibel ist, werden zwei Arten von Meldungen angezeigt, die die genaue Inkompatibilität beschreiben:

- Warnmeldungen: Sie können die Warnmeldungen überspringen, müssen sie jedoch bestätigen, um mit der Installation fortfahren zu können.
- Fehlermeldungen. Fehlermeldung gibt an, dass die Supervisor-Dienstversion mit dem Supervisor nicht kompatibel ist und nicht installiert werden kann. Im Falle von Fehlermeldungen müssen Sie zuerst die erkannte Inkompatibilität beheben, bevor Sie den Dienst auf dem jeweiligen Supervisor installieren können.

6 Geben Sie im Feld **YAML-Dienstkonfiguration** Konfigurationseigenschaften ein, wenn der Dienst diese erfordert.

7 Zeigen Sie den Installationsfortschritt für den Dienst auf Supervisoren an.

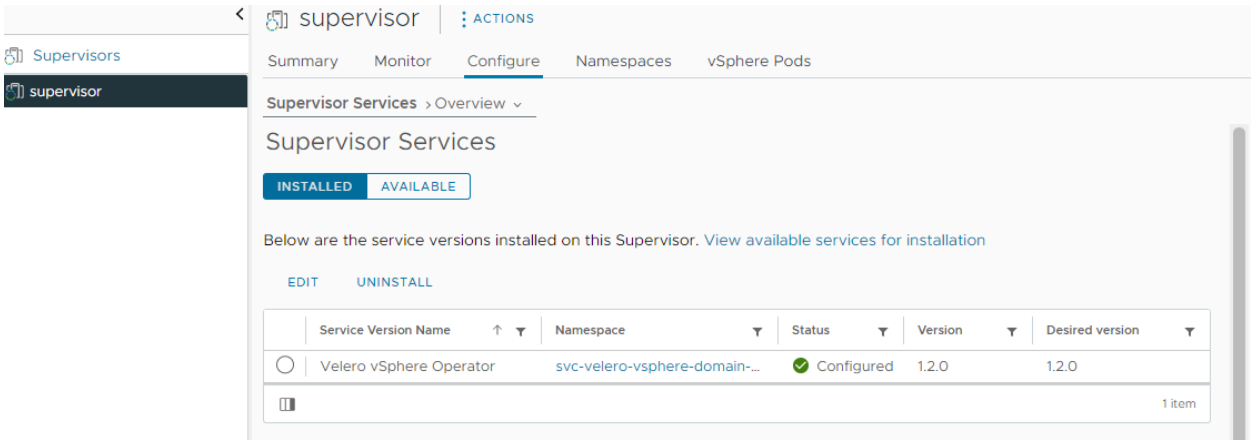
a Wählen Sie die Registerkarte **Supervisoren** und einen Supervisor aus, auf dem Sie den Dienst installieren.

b Klicken Sie auf **Konfigurieren** und dann auf **Supervisor Services > Überblick**.

c Wählen Sie die Registerkarte **Installiert**.

Ergebnisse

Der Supervisor-Dienst befindet sich im Status „Wird konfiguriert“, was bedeutet, dass alle erforderlichen Ressourcen im Supervisor erstellt werden und die Dienst-YAML auf den Cluster angewendet wird. Nachdem die YAML erfolgreich auf den Supervisor mit allen seinen erstellten oder aktualisierten Ressourcen und Namespaces angewendet wurde, wechselt der Dienststatus zu „Konfiguriert“. Der Dienst ist für alle Namespaces in diesem Cluster verfügbar und DevOps-Ingenieure können ihn mit ihren Arbeitslasten verwenden.



Anzeigen der auf einem Supervisor installierten Supervisor-Dienste

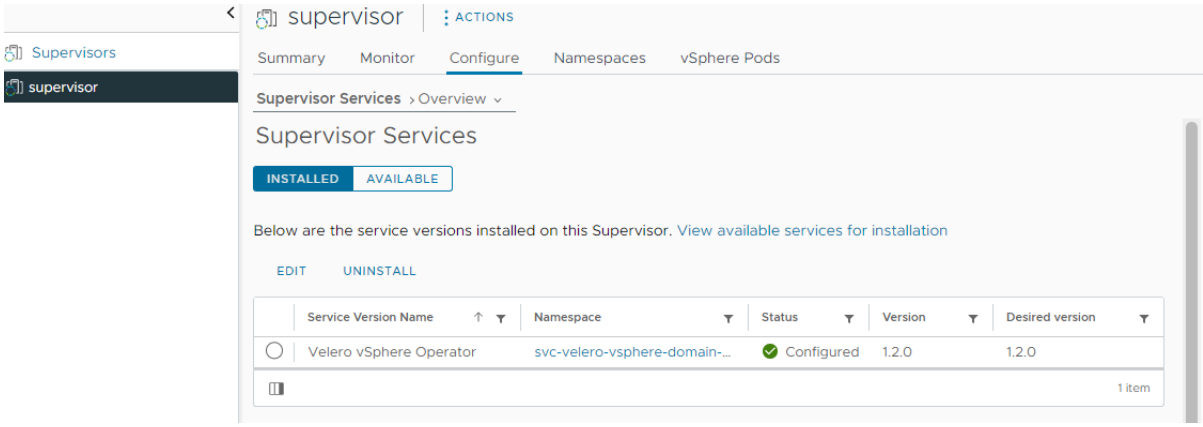
Sie haben die Möglichkeit, die in den Supervisoren in Ihrer vSphere IaaS control plane-Umgebung installierten vSphere-Dienste anzuzeigen. In einem Supervisor installierte Supervisor-Dienste sind für jeden Namespace im Cluster verfügbar.

Voraussetzungen

- Fügen Sie Supervisor-Dienste zu vCenter Server hinzu. Weitere Informationen finden Sie unter Hinzufügen eines Supervisor-Dienst zu vCenter Server.
- Installieren Sie Supervisor-Dienste in Supervisoren. Weitere Informationen finden Sie unter Installieren eines Supervisor-Diensts auf einem Supervisor.

Verfahren

1. Wählen Sie im vSphere Client-Startmenü die Option **Arbeitslastverwaltung** aus.
2. Klicken Sie auf die Registerkarte **Supervisoren** und wählen Sie einen Supervisor aus der Liste aus.
3. Klicken Sie auf die Registerkarte **Konfigurieren** und dann unter **Supervisor-Dienste** auf **Übersicht**.



   - Zeigen Sie auf der Registerkarte **Installiert** die Supervisor-Dienste an, die aktuell im Supervisor installiert sind.
   - Zeigen Sie auf der Registerkarte **Verfügbar** die Supervisor-Dienste an, die für die Installation verfügbar sind.

Nächste Schritte

Über die Registerkarte **Verfügbar** können Sie die Supervisor-Dienste in diesem Supervisor verwalten, Dienste deinstallieren oder neue Dienste installieren.

Deaktivieren eines Supervisor-Dienst oder einer Version davon

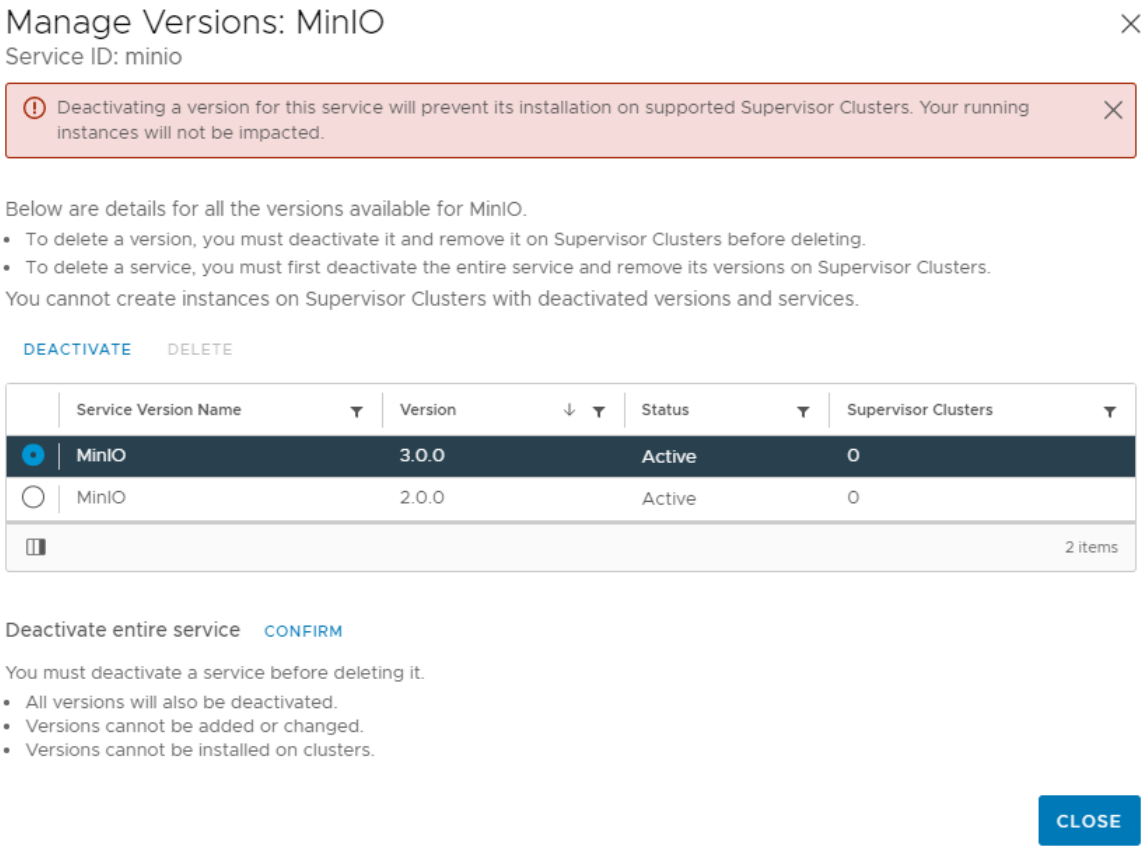
Deaktivieren Sie eine Supervisor-Dienst-Version, wenn Sie sie nicht mehr mit Kubernetes-Arbeitslasten in Ihrer vSphere IaaS control plane-Umgebung verwenden möchten. Eine deaktivierte Dienstversion wird weiterhin auf den Supervisoren ausgeführt, auf denen sie installiert ist, aber Sie können eine deaktivierte Dienstversion nicht auf anderen Supervisoren installieren. Wenn Sie einen gesamten Dienst deaktivieren, werden alle Dienstversionen deaktiviert. Sie können neue Dienstversionen erst wieder hinzufügen oder auf Supervisoren installieren, wenn Sie den Dienst erneut aktivieren.

Voraussetzungen

- Überprüfen Sie, ob Sie auf vCenter Server-Ebene über das Recht **Supervisor-Dienste verwalten** verfügen.

Verfahren

1. Wählen Sie im vSphere Client-Startmenü die Option **Arbeitslastverwaltung** aus.
2. Wählen Sie **Dienste** aus.
3. Klicken Sie auf der Karte „Dienst“ auf **Aktionen > Versionen verwalten**.
   - Um eine Supervisor-Dienst-Version zu deaktivieren, wählen Sie die Version aus und klicken Sie auf **Deaktivieren**.
   - Um den gesamten Dienst zu deaktivieren, klicken Sie neben **Gesamten Dienst deaktivieren** auf **Bestätigen**.



Ergebnisse

Die Dienstversion wird deaktiviert, und eine Installation auf Supervisoren ist nicht mehr möglich.

Aktivieren einer Supervisor-Dienst-Version unter vCenter Server

Sobald eine Supervisor-Dienst-Version deaktiviert wurde, können Sie sie erneut aktivieren, falls Ihr DevOps-Team diese Dienstversion in seinen unter vSphere IaaS control plane ausgeführten Kubernetes-Arbeitslasten verwenden möchte.

- Überprüfen Sie, ob Sie auf dem vCenter Server-System, auf dem der Dienst registriert ist, über das Recht **Supervisor-Dienste verwalten** verfügen.

Verfahren

1. Wählen Sie im vSphere Client-Startmenü die Option **Arbeitslastverwaltung** aus.
2. Wählen Sie **Dienste** aus.
3. Klicken Sie in der Karte Supervisor-Dienst auf **Aktive Versionen**.
4. Wählen Sie **Versionen verwalten** aus.

5 Wählen Sie die Supervisor-Dienst-Version mit dem Status „Deaktiviert“ aus und klicken Sie auf **Erneut aktivieren**.

Deinstallieren eines Supervisor-Dienst von einem Supervisor

Deinstallieren Sie einen Supervisor-Dienst von einem Supervisor, wenn Ihr DevOps-Team den Dienst nicht mehr für seine Kubernetes-Arbeitslasten benötigt, die in der vSphere IaaS control plane-Umgebung ausgeführt werden.

Voraussetzungen

- Überprüfen Sie, ob Sie über das Recht **Supervisor-Dienste verwalten** auf dem vCenter Server-System verfügen, das den Supervisor hostet, auf dem der Dienst installiert ist.

Verfahren

1 Wählen Sie im vSphere Client-Startmenü die Option **Arbeitslastverwaltung** aus.

2 Klicken Sie auf die Registerkarte **Supervisoren** und wählen Sie einen Supervisor aus der Liste aus.

3 Klicken Sie auf die Registerkarte **Konfigurieren** und dann unter **Supervisor-Dienste** auf **Übersicht**.

4 Wählen Sie unter **Installiert** die Supervisor-Dienst-Version aus, die Sie deinstallieren möchten, und klicken Sie auf **Deinstallieren**.

Ergebnisse

Der Supervisor-Dienst wird vom Supervisor deinstalliert. Alle Dienstressourcen und der Dienst-Namespace werden aus dem Supervisor entfernt. Alle verwalteten Instanzen von Diensten, die die vSAN Data Persistence Platform verwenden, werden aus dem Supervisor entfernt.

Löschen einer Supervisor-Dienst-Version

Löschen Sie die Version eines Supervisor-Dienst aus vCenter Server, wenn diese Version veraltet ist und Ihr DevOps-Team sie nicht mehr für die in der vSphere IaaS control plane-Umgebung ausgeführte Kubernetes-Arbeitslast benötigt.

Voraussetzungen

- Achten Sie darauf, dass die Supervisor-Dienst-Version, die Sie löschen möchten, nicht auf Supervisoren installiert ist. Weitere Informationen finden Sie unter Deinstallieren eines Supervisor-Dienst von einem Supervisor.
- Überprüfen Sie, ob Sie auf vCenter Server-Ebene über das Recht **Supervisor-Dienste verwalten** verfügen.

Verfahren

1 Wählen Sie im vSphere Client-Startmenü die Option **Arbeitslastverwaltung** aus.

2 Wählen Sie **Dienste** aus.

3 Klicken Sie auf der Karte „Supervisor-Dienst“ auf **Aktionen > Versionen verwalten**.

4 Wählen Sie die Version aus, die Sie löschen möchten, und klicken Sie auf **Deaktivieren**.

5 Wählen Sie die deaktivierte Version aus und klicken Sie auf **Löschen**.

Löschen eines Supervisor-Diensts

Löschen Sie einen Supervisor-Dienst aus der vSphere IaaS control plane-Umgebung, wenn Ihre DevOps-Ingenieure ihn nicht mehr für ihre Kubernetes-Arbeitslasten benötigen.

Voraussetzungen

- Überprüfen Sie, ob Sie auf dem vCenter Server-System, auf dem der Dienst registriert ist, über das Recht **Supervisor-Dienste verwalten** verfügen.

Verfahren

1 Wählen Sie im vSphere Client-Startmenü die Option **Arbeitslastverwaltung** aus.

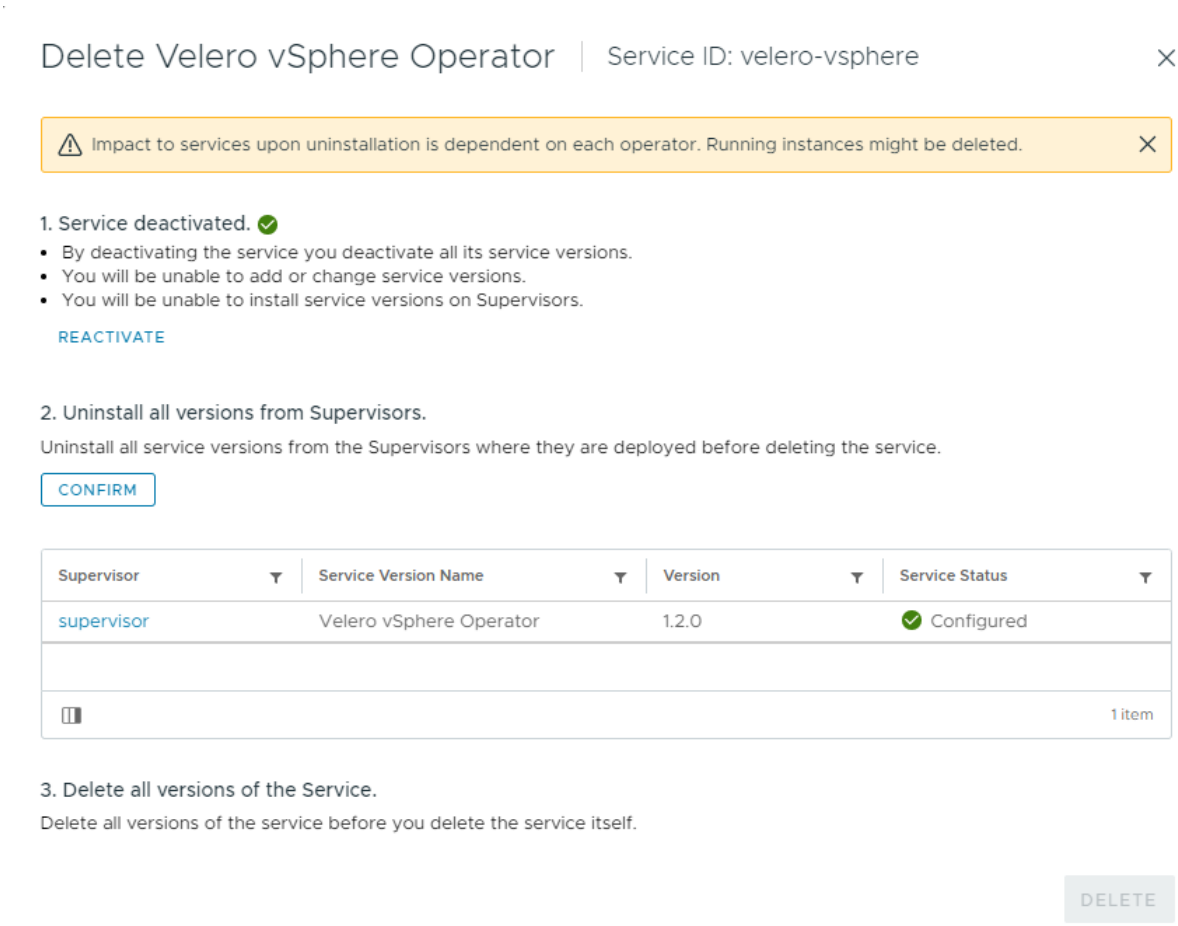
2 Wählen Sie **Dienste** aus.

3 Klicken Sie auf der Karte des Supervisor-Dienst, den Sie entfernen möchten, auf **Aktionen > Löschen**.

4 Bestätigen Sie die Deaktivierung aller derzeit verfügbaren Dienstversionen.

5 Bestätigen Sie die Deinstallation des Diensts von den Supervisoren.

   Das Deinstallieren eines Supervisor-Dienst auf den Supervisoren, auf denen er ausgeführt wird, kann einige Zeit in Anspruch nehmen. Sie können das Dialogfeld schließen, während der Vorgang ausgeführt wird, und es dann erneut öffnen, um mit der nächsten Phase fortzufahren.



6 Bestätigen Sie das Löschen aller verfügbaren Versionen des Diensts.

7 Klicken Sie auf **Löschen**.

Verwenden der vSAN Data Persistence-Plattform mit modernen statusbehafteten Diensten

5

In vSphere IaaS control plane können Sie die vSAN Data Persistence-Plattform für moderne statusbehaftete Dienste verwenden, die persistenten Speicher erfordern. Die Plattform bietet ein Framework, das es Drittanbietern ermöglicht, ihre Dienstanwendungen in die zugrunde liegende vSphere-Infrastruktur zu integrieren.

Informationen vSAN Data Persistence Platform

Die Verwendung von vSAN Data Persistence bietet u. a. die folgenden Vorteile:

Automatische Dienstbereitstellung und Skalierung

Mithilfe des vSphere Client können Administratoren einen modernen statusbehafteten Dienst in einem Supervisor installieren und DevOps-Ingenieuren Zugriff zu dem Dienst-Namespace gewähren. Die DevOps-Ingenieure können Instanzen des statusbehafteten Diensts über Kubernetes-APIs dynamisch per Self-Service bereitstellen.

Mit vCenter Server vernetzte Dienstüberwachung

Partner können Dashboard-Plug-Ins erstellen, die mit vCenter Server vernetzt werden. Mithilfe der Plug-Ins für die Benutzeroberfläche können die vSphere-Administratoren die statusgehafteten Dienste verwalten und überwachen. Darüber hinaus bietet vSAN Funktionen zur Überwachung des Systemzustands und der Kapazität für diese integrierten Drittanbieterdienste.

Optimierte Speicherkonfiguration mit vSAN Direct

vSAN Direct ermöglicht modernen statusbehafteten Diensten, sich direkt mit dem zugrunde liegenden direkt angeschlossenen Speicher für optimierte E/A-Vorgänge und Speichereffizienz zu verbinden.

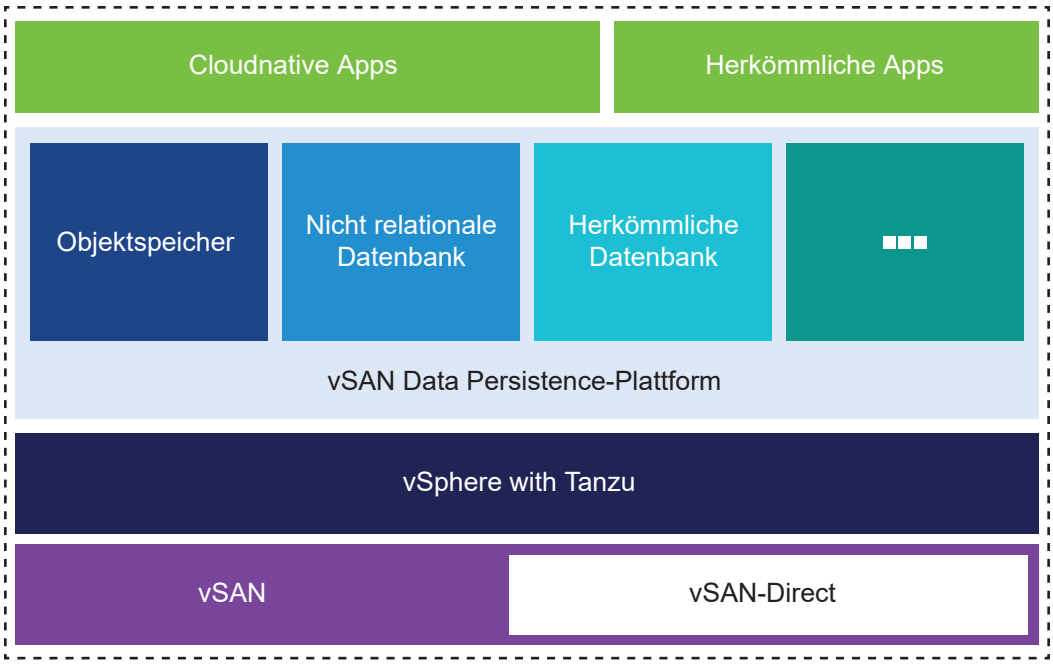
Die-Plattform unterstützt die folgenden Diensttypen:

- Objektspeicher, z. B. MinIO
- NoSQL-Datenbanken, auch nicht relationale Datenbanken genannt
- Herkömmliche Datenbanken

Shared Nothing-Speicher für vSphere

Die meisten modernen statusbehafteten Dienste verfügen über eine Shared Nothing-Architektur (SNA). Sie verbrauchen nicht replizierten lokalen Speicher und bieten ihre eigene Speicherreplizierung, -komprimierung und weitere Datenvorgänge an. Dies führt dazu, dass die Dienste nicht davon profitieren, wenn dieselben Vorgänge vom zugrunde liegenden Speicher ausgeführt werden.

Um eine Duplizierung der Vorgänge zu verhindern, bietet die vSAN Data Persistence-Plattform zwei vSAN-Lösungen mit optimierten Datenpfaden. Der persistente Dienst kann entweder unter vSAN mit der SNA-Speicherrichtlinie oder in einem überwiegend unformatierten lokalen Speicher namens vSAN Direct ausgeführt werden.



vSAN mit SNA-Speicherrichtlinie

Mit dieser Technologie können Sie einen verteilten replizierten vSAN-Datenspeicher mit der lokal auf dem Host vorhandenen vSAN-SNA-Richtlinie verwenden. Dies führt dazu, dass die SNA-Dienstanwendung die Platzierung steuern und die Aufgabe zur Bereitstellung der Datenverfügbarkeit übernehmen kann. Die Technologie macht es für den persistenten Dienst einfach, seine Computing-Instanz und ein Speicherobjekt auf demselben physischen ESXi-Host zu platzieren. Bei der hostlokalen Platzierung ist es möglich, Vorgänge wie die Replizierung auf der Dienstebene und nicht auf der Speicherebene durchzuführen.

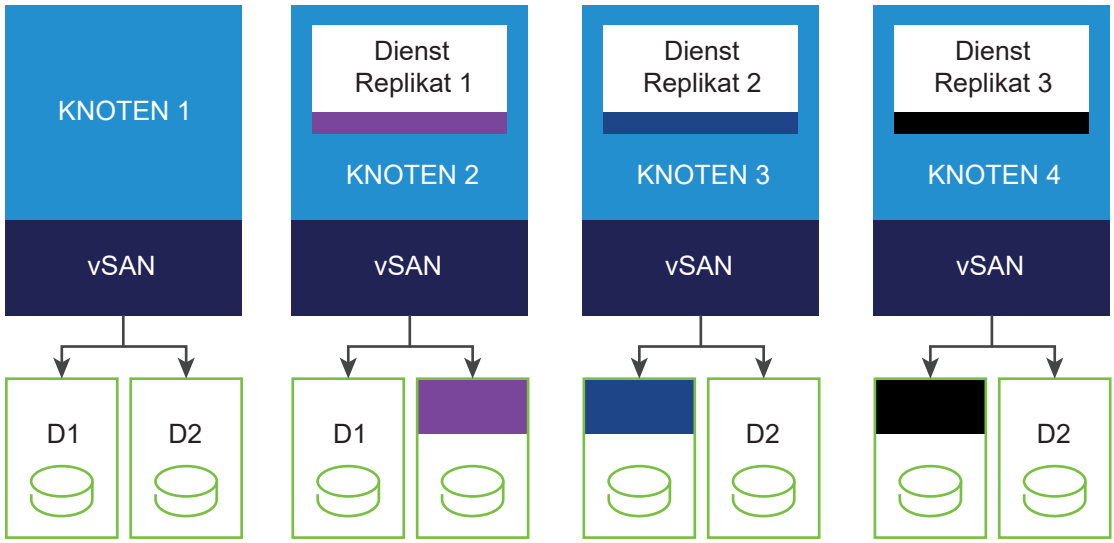
Die Computing-Instanz, z. B. ein Pod, wird zuerst auf einem der Knoten im vSAN-Cluster eingerichtet. Dann werden alle Daten des vSAN-Objekts, das mit der vSAN-SNA-Richtlinie erstellt wurde, automatisch auf demselben Knoten platziert, auf dem der Pod ausgeführt wird.

Das folgende Beispiel veranschaulicht die Speicherbereitstellung einer Anwendung, die die SNA-Speicherklasse für das persistente Volume verwendet. vSAN kann eine beliebige Festplattengruppe auf dem Knoten für die Platzierung des persistenten Volumes auswählen.

Gesamtkopien der Daten = 3

Erwartete Fault Tolerance = 2

Tatsächliche Fehler, die toleriert werden = 2

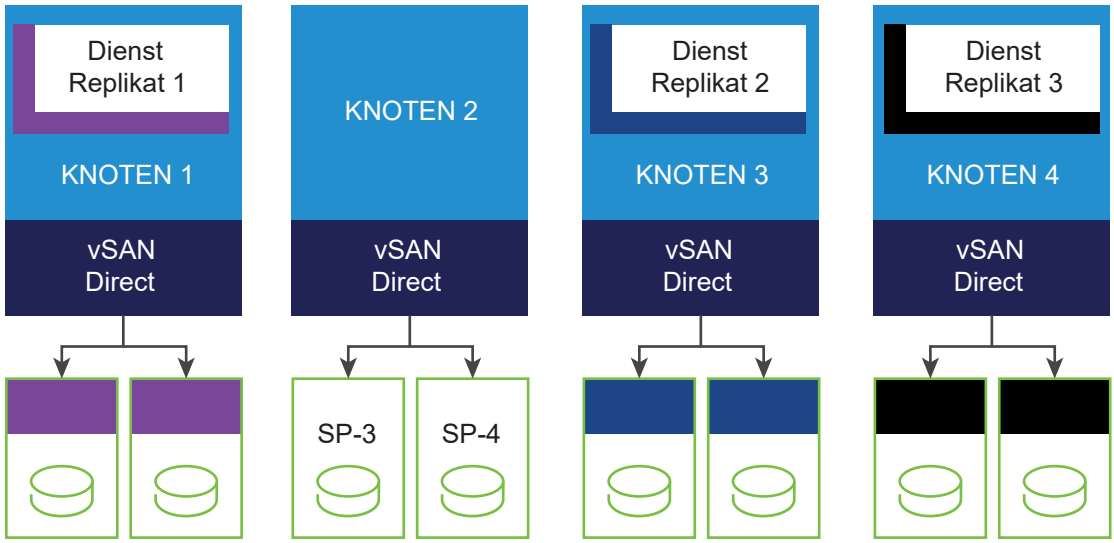


vSAN Direct

Auch wenn vSAN mit der SNA-Speicherrichtlinie Daten lokal auf der Computing-Instanz platzieren kann, besteht ein Overhead eines verteilten vSAN-Datenpfads zwischen der Anwendung und dem physischen Speichergerät. Bei Verwendung von vSAN Direct können die Anwendungen mit statusbehafteten Diensten über einen direkteren Datenpfad, der die leistungsoptimierte Lösung bietet, auf überwiegend unformatierten lokalen Nicht-vSAN-Speicher zugreifen.

Mit vSAN Direct kann der vSphere-Administrator hostlokale Geräte beanspruchen und anschließend die Geräte verwalten und überwachen. vSAN Direct bietet Einblicke in den Gerätezustand, die Leistung und die Kapazität. Auf jedem beanspruchten lokalen Gerät erstellt vSAN Direct einen unabhängigen VMFS-Datenspeicher und stellt ihn als Platzierungswahl für die Anwendung zur Verfügung. Die VMFS-Datenspeicher, die von vSAN Direct verwaltet werden, werden als Speicherpools in Kubernetes angezeigt. Im vSphere Client werden sie als vSAN Direct-Datenspeicher angezeigt.

Nachfolgend sind persistente Volumes dargestellt, die lokal auf vSAN Direct-Festplatten platziert werden.



Verwenden von vSAN mit SNA oder vSAN Direct

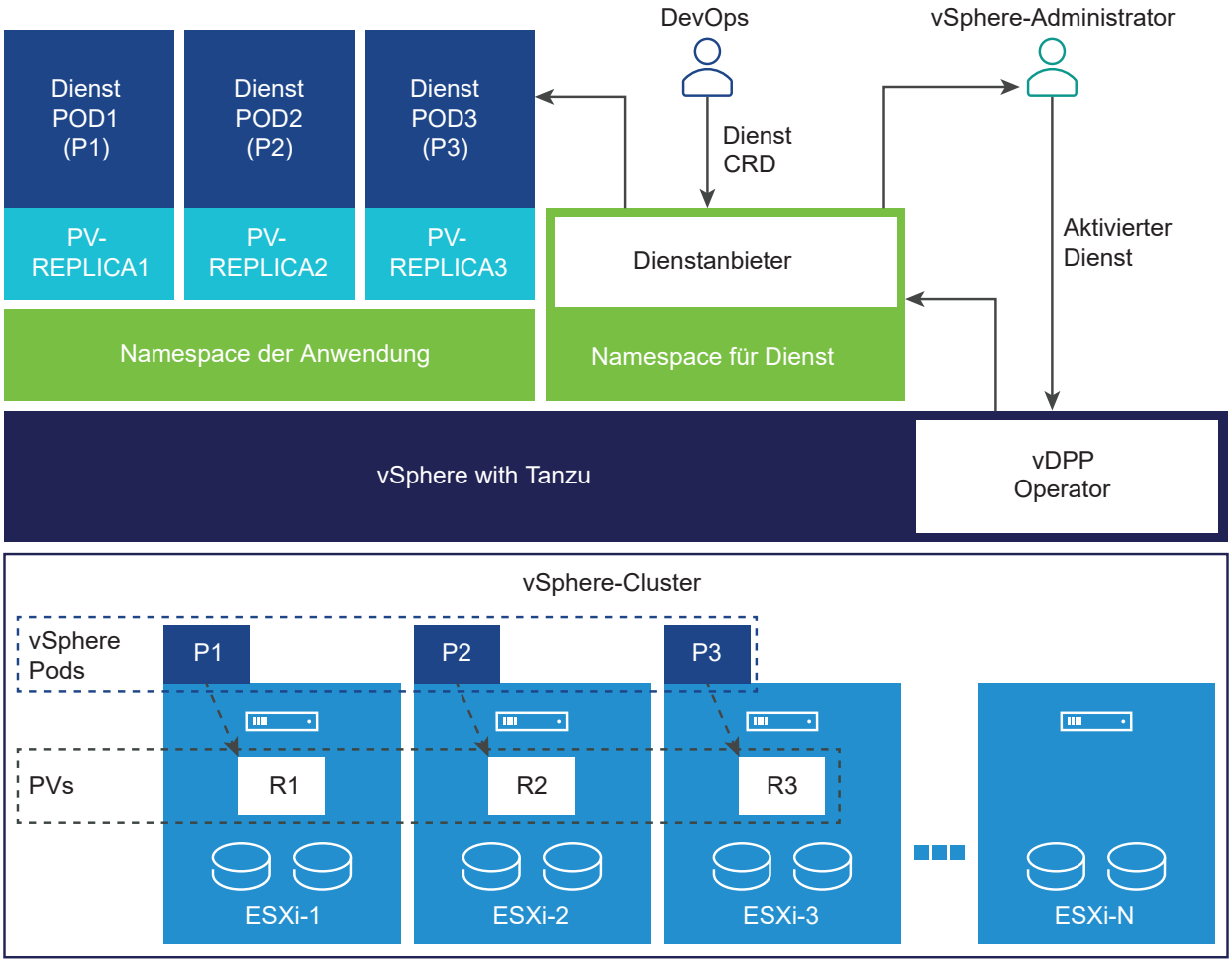
Befolgen Sie diese allgemeinen Empfehlungen, wenn Sie entscheiden, welche Art von vSAN verwendet werden soll.

- Verwenden Sie vSAN mit SNA, wenn Sie möchten, dass die cloudnative statusbehaftete Anwendung die physische Infrastruktur mit anderen regulären VMs oder Kubernetes-Arbeitslasten gemeinsam nutzen soll. Jede Arbeitslast kann ihre eigene Speicherrichtlinie definieren und das Beste aus beidem über einen einzelnen Cluster abrufen.
- Verwenden Sie vSAN Direct, wenn Sie einen dedizierten Hardware-Cluster für die cloudnativen Shared Nothing-Dienste erstellen.

Operator der vSAN Data Persistence-Plattform

Der Operator der vSAN Data Persistence-Plattform (vDPP) ist eine Komponente, die für die Ausführung und Verwaltung von zustandsbehafteten, mit vSphere vernetzten Partnern verantwortlich ist. Der vDPP-Operator stellt dem vSphere-Administrator verfügbare statusbehaftete Dienste zur Verfügung. Wenn der vSphere-Administrator einen persistenten Dienst wie beispielsweise MinIO aktiviert, stellt der vDPP-Operator einen anwendungsspezifischen Operator für den Dienst im Supervisor bereit.

Die anwendungsspezifischen Operatoren werden von einem Drittanbieter bereitgestellt und müssen mit vDPP konform sein. Der Operator bietet in der Regel eine CRD, die eine Self-Service-Schnittstelle für Kubernetes-Benutzer zur Instanziierung von Instanzen bereitstellt. vSphere IaaS control plane verwendet diesen Operator und diese CRD, um neue Dienstinstanzen bereitzustellen und sie über die statusbehaftete Diensteschicht zu verwalten und zu überwachen. Die meisten dieser Operatoren verwenden statusbehaftete Sätze für die Bereitstellung ihrer Instanzen.



Nachdem der vSphere-Administrator einen Dienst aktiviert hat, findet Folgendes statt.

- Der vDPP-Operator aktiviert einen dienstspezifischen Operator.
- Der dienstspezifische Operator registriert das Plug-In für die Benutzeroberfläche.
- Es werden speicheroptimierte Speicherrichtlinien erstellt.

Konfigurationsgrenzwerte für die vSAN Data Persistence-Plattform

VMware stellt im Tool für die Maximalwerte für die VMware-Konfiguration Konfigurationsgrenzwerte bereit.

Maximalwerte für vSAN Data Persistence	Grenzwerte
Maximale Anzahl an persistenten Volumes pro vSAN Data Persistence-Plattform	1000
Maximale Anzahl an persistenten Volumes pro Dienstinstanz auf der vSAN Data Persistence-Plattform	60 bis 80

Lesen Sie als Nächstes die folgenden Themen:

- Aktivieren von statusbehafteten Diensten in vSphere IaaS control plane
- Einrichten eines vSAN Direct-Datenspeichers für statusbehaftete Dienste
- Überwachen von statusbehafteten Diensten in vSphere IaaS control plane
- Überprüfen der für statusbehaftete Dienste verfügbaren Speicherrichtlinien
- Erstellen von benutzerdefinierten Speicherrichtlinien für die vSAN Data Persistence-Plattform

Aktivieren von statusbehafteten Diensten in vSphere IaaS control plane

vSphere IaaS control plane ist mit mehreren Diensten von Drittanbietern kompatibel, die die vSAN Data Persistence-Plattform für ihren Bedarf an persistentem Speicher verwenden. Aktivieren Sie als vSphere-Administrator die Dienste auf vCenter Server. Wenn Sie den statusbehafteten Dienst aktivieren, registrieren Sie den Dienst bei vCenter Server mit der heruntergeladenen YAML-Datei, die den Dienst beschreibt. Installieren Sie den Dienst dann auf Supervisoren, damit Ihre DevOps-Ingenieure ihn in Kubernetes-Arbeitslasten verwenden können.

Voraussetzungen

Erforderliches Recht: **Supervisor-Dienste.Supervisor-Dienste verwalten**

1 Konfigurieren eines dauerhaften Speichers

Mit der vSAN Data Persistence-Plattform können statusbehaftete Dienste vSAN-Speicher in den folgenden beiden Modi verwenden:

- vSAN Direct. Informationen zum Einrichten von vSAN Direct finden Sie unter Erstellen eines vSAN Direct-Datenspeichers.

  Hinweis Für die Festplatten in vSAN Direct-Datenspeicher werden Änderungen des Volume-Zuteilungstyps nicht unterstützt. Nachdem Sie den Volume-Zuteilungstyp für die Festplatten im vSAN Direct-Datenspeicher festgelegt haben, können Sie ihn nicht mehr ändern. Die Änderung des Volume-Zuteilungstyps für die neue Festplatte ist jedoch für Vorgänge wie Klonen und Verlagern zulässig.

- Reguläres vSAN mit SNA-Speicherrichtlinie. Informationen zum Einrichten von vSAN-Speicher finden Sie unter *Verwalten von VMware vSAN*.

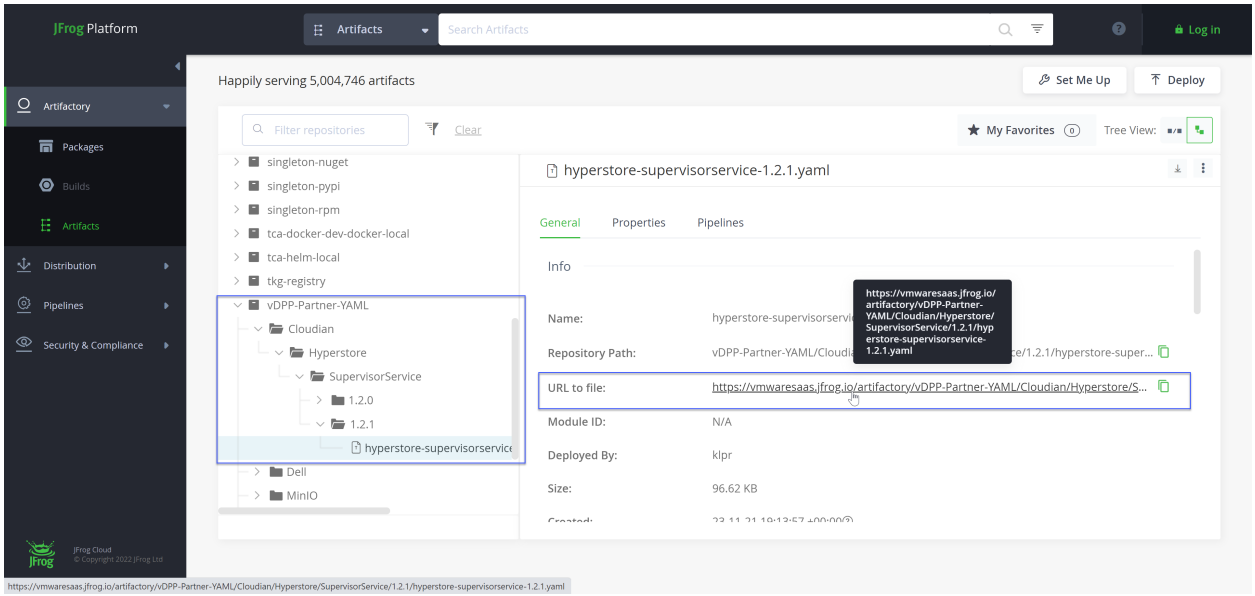
2 Herunterladen der YAML-Dienstdatei

Achten Sie beim Herunterladen der YAML-Dienstdateien aus dem von VMware verwalteten Repository darauf, dass Sie die richtige Dienstversion verwenden, die mit Ihrer Version von vSphere kompatibel ist.

Wenn Sie frühere Versionen von Partnerdiensten, MinIO und Cloudian Hyperstore installiert haben, führen Sie nach dem Upgrade Ihrer vSphere-Umgebung ein Upgrade auf kompatible Versionen durch. Die neueren Versionen der Partneroperatoren beheben bestimmte Probleme und verwenden neue Plattformfunktionen. Weitere Informationen dazu finden Sie in der Partnerdokumentation.

1 Navigieren Sie im https://vmwaresaas.jfrog.io/-Repository zu einem entsprechenden Partnerordner in **Artefakte > vDPP-Partner-YAML**.

2 Klicken Sie auf die URL zur Datei und laden Sie die YAML-Datei herunter.



3 Hinzufügen des Diensts zu vCenter Server

Verwenden Sie die heruntergeladene YAML-Datei für den Partnerdienst.

Weitere Informationen finden Sie unter Hinzufügen eines Supervisor-Dienst zu vCenter Server.

4 Installieren des Diensts auf dem Supervisor

Weitere Informationen finden Sie unter Installieren eines Supervisor-Diensts auf einem Supervisor.

Nachdem Sie den Dienst aktiviert haben, führt die vSAN Data Persistence-Plattform die folgenden Aktionen aus, um die erforderlichen Ressourcen für den Dienst zu erstellen:

- Sie erstellt einen Namespace für diesen Dienst im Supervisor.
- Erstellt Standardspeicherrichtlinien und entsprechende Speicherklassen und weist sie dem Namespace zu.

Die Richtlinien gelten für vSAN Shared-Nothing-Architektur (SNA)- und vSAN Direct-Datenspeicher.

Hinweis Die vSAN Data Persistence-Plattform erstellt Speicherklassen vom Typ „vsan-direct“ und „vsan-sna“ im Namespace automatisch, nachdem der vSphere-Administrator den Dienst aktiviert hat. Nur Anwendungen, die auf dem Supervisor ausgeführt werden, können die Speicherklassen „vsan-direct“ und „vsan-sna“ verwenden. Diese Speicherklassen können nicht innerhalb eines Tanzu Kubernetes Grid-Clusters verwendet werden.

Ab vSphere 7.0 Update 2 ist die vSAN Direct-Speicherrichtlinie funktionsbasiert. Wenn Sie Tag-basierte Richtlinien in vSphere 7.0 Update 1 erstellt haben, werden diese nach einem Upgrade auf vSphere 7.0 Update 2 oder höher automatisch in funktionsbasierte Richtlinien konvertiert.

Wenn Sie benutzerdefinierte Speicherrichtlinien erstellen und sie dem Dienst-Namespace statt dem Standard zuweisen möchten, finden Sie weitere Informationen unter Erstellen einer vSAN Direct-Speicherrichtlinie und vSAN SNA-Speicherrichtlinie erstellen.

- Erstellt DevOps-Rollen, einschließlich der Rollen mit Berechtigungen zum Bearbeiten und Anzeigen.

  Wenn der Dienstoperator bereitgestellt wird, werden seine benutzerdefinierten CRDs im Supervisor installiert. Benutzer mit Bearbeitungsberechtigung können Ressourcen dieser CRDs im Namespace erstellen, lesen, aktualisieren und löschen (CRUD). Benutzer mit Ansichtsberechtigung können Ressourcen dieser CRD nur anzeigen.

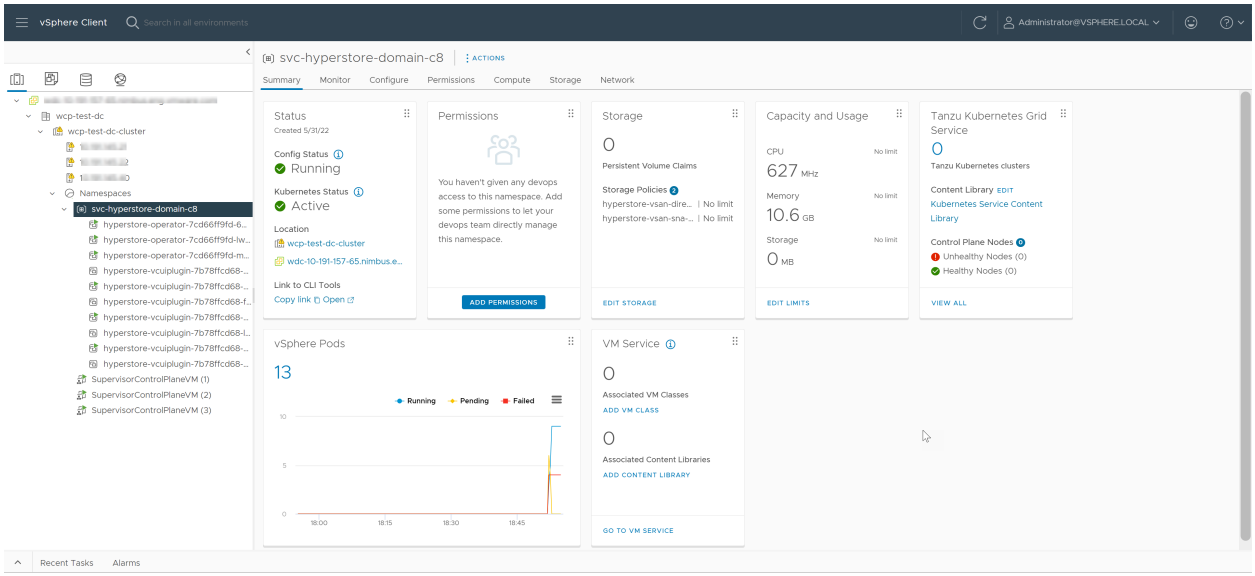
- Wenn der Drittanbieter ein benutzerdefiniertes Benutzeroberflächen-Plug-In bereitgestellt hat, wird es im vSphere Client angezeigt. Der vSphere-Administrator kann das-Plug-In verwenden, um den Dienst zu verwalten.

5 Überprüfen der für den Dienst erstellten Ressourcen

Der vSphere-Administrator kann überprüfen, ob alle geeigneten Ressourcen für den Dienst erstellt wurden.

Navigieren Sie zum für den Dienst erstellten Namespace und klicken Sie auf die Registerkarte **Übersicht**.

Auf der Seite „Übersicht“ werden die dem Namespace zugewiesenen Speicherrichtlinien, die auf dem Namespace ausgeführten vSphere Pods usw. angezeigt.



6 Verwalten und Überwachen des Diensts

- Wenn der Drittanbieter ein benutzerdefiniertes Benutzeroberflächen-Plug-In bereitgestellt hat, kann der vSphere-Administrator das Plug-In zur Verwaltung und Überwachung des Diensts verwenden.

  Weitere Informationen finden Sie in der Dokumentation zum Benutzeroberflächen-Plug-In des Drittanbieters.

- Darüber hinaus kann der vSphere-Administrator die Skyline Health-Prüfungen verwenden, um die Dienste zu überwachen. Weitere Informationen hierzu finden Sie unter Überwachen von statusbehafteten Diensten in vSphere IaaS control plane.

- Wenn Sie anstelle der Standard- benutzerdefinierte Speicherrichtlinien erstellen möchten, finden Sie weitere Informationen unter Erstellen von benutzerdefinierten Speicherrichtlinien für die vSAN Data Persistence-Plattform.

7 Starten der Nutzung des Diensts

Der DevOps-Ingenieur verwendet den Befehl `kubectl` für den Zugriff auf den Dienst-Namespace.

Wie Sie überprüfen, ob der für statusbehaftete Dienste verwendete Namespace über geeignete Speicherklassen verfügt, erfahren Sie unter Überprüfen der für statusbehaftete Dienste verfügbaren Speicherrichtlinien.

Sie können die Drittanbieter-CRDs verwenden, um Instanzen des Drittanbieteranwendungsdiensts bereitzustellen. Weitere Informationen finden Sie in der Dokumentation des Drittanbieters.

Einrichten eines vSAN Direct-Datenspeichers für statusbehaftete Dienste

Wenn Sie einen dedizierten Hardwarecluster für statusbehaftete Dienste in vSphere IaaS control plane erstellen möchten, können Sie einen vSAN Direct-Datenspeicher verwenden. vSAN Direct ist hauptsächlich ein Raw-Datenspeicher, den Sie auf nicht beanspruchten Speichergeräten bereitstellen, die lokal auf Ihrem ESXi-Host vorhanden sind.

Markieren von Speichergeräten für vSAN Direct mit Tags

vSAN Direct benötigt einige nicht beanspruchte Festplatten auf jedem ESXi-Host innerhalb eines vSAN-Clusters. In bestimmten Umgebungen beansprucht vSAN jedoch automatisch alle lokalen Speichergeräte auf Ihren Hosts. Sie können die Geräte als für reguläres vSAN ungeeignet und für vSAN Direct verfügbar festlegen.

Verwenden Sie den Befehl `esxcli`, um die Geräte als vSAN Direct zu markieren.

Verfahren

1. Markieren Sie das lokale Speichergerät für vSAN Direct mit Tags.

   ```
   esxcli vsan storage tag add -d diskName -t vsanDirect
   ```

   Beispiel:

   ```
   esxcli vsan storage tag add -d mpx.vmhba0:C0:T1:L0 -t vsanDirect
   ```

   Das Gerät ist für reguläres vSAN nicht geeignet.

2. Entfernen Sie das vSAN Direct-Tag vom Gerät.

   ```
   esxcli vsan storage tag remove -d diskName -t vsanDirect
   ```

   Beispiel:

   ```
   esxcli vsan storage tag remove -d mpx.vmhba0:C0:T1:L0 -t vsanDirect
   ```

Verwenden eines Skripts, um Speichergeräte für vSAN Direct mit Tags zu versehen

Alternativ können Sie das folgende Skript verwenden, um HDD-Geräte, die an Ihren ESXi-Host angehängt sind, mit Tags zu versehen. Nach der Ausführung des Skripts sind die Geräte für reguläres vSAN nicht mehr geeignet und sind für vSAN Direct verfügbar.

```
#!/usr/bin/env python3

# Copyright 2020 VMware, Inc. All rights reserved.

# Abstract
#
#    This script helps manage tagging of Direct Attached HDD disks
#    on ESXi systems for vSAN Direct in preparation for a VCF deployment.
#
```

```
#    It is expected to be used with ESX systems of version 7.0.1 or later.
#

import argparse
from enum import Enum
import logging
import sys
import os
import paramiko
import subprocess
import traceback
import ast
import getpass
from six.moves import input
from distutils.util import strtobool
from argparse import ArgumentParser

class ParseState(Enum):
        OPEN = 0
        DEVICE = 1

class RemoteOperationError(Exception):
    pass

class EsxVersion:

    def __init__(self, major, minor, release):
        self.major = major
        self.minor = minor
        self.release = release

    def __str__(self):
        return '{}.{}.{}'.format(self.major, self.minor, self.release)

    @staticmethod
    def build(str):
        tokens = str.split(b'.',3)
        return EsxVersion(int(tokens[0]), int(tokens[1]), int(tokens[2]))

class StorageDevice:

    def __init__(self, deviceId, isSSD, isVsanDirectEnabled):
        self.deviceId = str(deviceId.decode())
        self.isSSD = isSSD
        self.isVsanDirectCapable = True
        self.isVsanDirectEnabled = isVsanDirectEnabled

    def __str__(self):
        return '{}:\n\tIs SSD: {}\n\tvsanDirect enabled:{}'.format(
                    self.deviceId,
                    self.isSSD,
                    self.isVsanDirectEnabled)

    @staticmethod
    def strToBool(v):
```

```
        return bool(strtobool(str(v.decode())))

    @staticmethod
    def build(deviceId, props):
        vsanDirectEnabled = False
        isLocal = StorageDevice.strToBool(props[b'Is Local'])
        status = props[b'Status']
        isOffline = StorageDevice.strToBool(props[b'Is Offline'])
        isSSD = StorageDevice.strToBool(props[b'Is SSD'])
        isBootDevice = StorageDevice.strToBool(props[b'Is Boot Device'])
        deviceType = props[b'Device Type']
        if deviceType == b'Direct-Access' and isLocal and (not isOffline) and (not
isBootDevice) and status == b'on':
            return StorageDevice(deviceId, isSSD, vsanDirectEnabled)
        else:
            print("Skipping device {}".format(deviceId))
            return None

def parse_arguments():
    """
    Parses the command line arguments to the function
    """
    parser = argparse.ArgumentParser()
    parser.add_argument('--hostname', dest='hostname',
            help='specify hostname for the ESX Server', required=True)
    parser.add_argument('--username', dest='username',
            help='specify username to connect to the ESX Server', required=True)
    parser.add_argument('--password', dest='password',
            help='specify password to connect to the ESX Server', required=False)
    return parser.parse_args()

def get_esx_version(sshClient):
    global logger
    stdin_, stdout_, stderr_ = sshClient.exec_command('vmware -v')
    exit_status = stdout_.channel.recv_exit_status()
    if exit_status != 0:
        logger.error('Command exited with non-zero status: %s' % exit_status)
        logger.error('Error message: %s' % stderr_.read())
        raise RemoteOperationError('Failed to determine ESX version')
    output = stdout_.read()
    tokens = output.split()
    if len(tokens) < 3:
        raise RemoteOperationError('Invalid ESX Version - %s', output)
    return EsxVersion.build(tokens[2])

def check_esx_version(esxVersion):
    return esxVersion.major >= 7 and esxVersion.minor >= 0 and esxVersion.release >= 1

def query_devices(sshClient):
    global logger
    stdin_, stdout_, stderr_ = sshClient.exec_command('esxcli storage core device list')
    exit_status = stdout_.channel.recv_exit_status()
    if exit_status != 0:
        logger.error('Command exited with non-zero status: %s' % exit_status)
        logger.error('Error message: %s' % stderr_.read())
```

```
        raise RemoteOperationError('Failed to query core storage device list')
    output = stdout_.read()
    # Build the device list from the output
    return create_device_list(output)

def create_device_list(str):
    devices = []

    deviceId=""
    deviceProps={}

    parseState = ParseState.OPEN
    for line in str.splitlines():
        if parseState == ParseState.OPEN:
            if line.strip():
                deviceId=line.strip()
                parseState = ParseState.DEVICE
        elif parseState == ParseState.DEVICE:
            if line.strip():
                props = line.strip().split(b':',1)
                deviceProps[props[0]] = props[1].strip()
            else:
                if deviceId:
                    device = StorageDevice.build(deviceId, deviceProps)
                    if device:
                        devices.append(device)
                    else:
                        logger.debug("Skipping device {}".format(deviceId))
                deviceId=""
                deviceProps={}
                parseState = ParseState.OPEN
    if deviceId:
        device = StorageDevice.build(deviceId, deviceProps)
        if device:
            devices.append(device)
    return devices

def tag_device_for_vsan_direct(sshClient, deviceId):
    global logger
    logger.info("Tagging device [{}] for vSAN Direct".format(deviceId))
    command = "esxcli vsan storage tag add -d " + deviceId + " -t vsanDirect"
    stdin_, stdout_, stderr_ = sshClient.exec_command(command)
    exit_status = stdout_.channel.recv_exit_status()
    if exit_status != 0:
        logger.error('Command exited with non-zero status: %s' % exit_status)
        logger.error('Error message: %s' % stderr_.read())
        raise RemoteOperationError('Failed to tag device [{}] for vSAN
Direct'.format(deviceId))
    logger.info('Successfully tagged device [{}] for vSAN Direct'.format(deviceId))

def untag_device_for_vsan_direct(sshClient, deviceId):
    global logger
    logger.info("Untagging device [{}] for vSAN Direct".format(deviceId))
    command = "esxcli vsan storage tag remove -d " + deviceId + " -t vsanDirect"
    stdin_, stdout_, stderr_ = sshClient.exec_command(command)
```

```
    exit_status = stdout_.channel.recv_exit_status()
    if exit_status != 0:
        logger.error('Command exited with non-zero status: %s' % exit_status)
        logger.error('Error message: %s' % stderr_.read())
        raise RemoteOperationError('Failed to untag device [{}] for vSAN
Direct'.format(deviceId))
    logger.info('Successfully untagged device [{}] for vSAN Direct'.format(deviceId))

def get_vsan_info_for_device(sshClient, deviceId):
    global logger
    command = "vdq -q -d {}".format(deviceId)
    stdin_, stdout_, stderr_ = sshClient.exec_command(command)
    exit_status = stdout_.channel.recv_exit_status()
    if exit_status != 0:
        logger.error('Command exited with non-zero status: %s' % exit_status)
        logger.error('Error message: %s' % stderr_.read())
        raise RemoteOperationError('Failed to query vsan direct status on device [%s]' %
deviceId)
    output = stdout_.read()
    return ast.literal_eval(str(output.decode()))

def update_vsan_direct_status(sshClient, devices):
        for device in devices:
            vsanInfo = get_vsan_info_for_device(sshClient, device.deviceId)
            device.isVsanDirectEnabled = vsanInfo[0]['IsVsanDirectDisk'].strip() == "1"
            device.isVsanDirectCapable = vsanInfo[0]['State'].strip() == 'Eligible for use by
VSAN'

def getVsanDirectCapableDevices(devices):
    selectDevices = []
    # Cull devices incapable of vSAN Direct
    for device in devices:
        if device.isVsanDirectCapable:
            selectDevices.append(device)
    return selectDevices

def print_devices(devices):
    print("Direct-Attach Devices:")
    print("======================")
    iDevice = 0
    for device in devices:
        iDevice = iDevice + 1
        print ("{}. {}".format(iDevice, device))
    print("======================")

def tag_devices(sshClient, devices):
    for device in devices:
        tag_device_for_vsan_direct(sshClient, device.deviceId)

def untag_devices(sshClient, devices):
    for device in devices:
        untag_device_for_vsan_direct(sshClient, device.deviceId)

def tag_all_hdd_devices(sshClient, devices):
    hddDevices = []
```

```
    for device in devices:
        if not device.isSSD:
            hddDevices.append(device)
    if len(hddDevices) > 0:
        tag_devices(sshClient, hddDevices)

def show_usage():
    print ("====================================")
    print ("commands: {tag-all-hdd, tag, untag}")
    print ("\ttag <comma separated serial numbers of devices>")
    print ("\tuntag <comma separated serial numbers of devices>")
    print ("\ttag-all-hdd")
    print ("=============")

def main():
    global logger
    logger.info('Tag disks for vSAN Direct')

    try:
        # Parse arguments
        args = parse_arguments()

        # 1. Setup SSH connection to ESX system
        sshClient = paramiko.SSHClient()
        sshClient.load_system_host_keys()
        sshClient.set_missing_host_key_policy(paramiko.AutoAddPolicy())
        passwd = args.password
        if passwd == None:
            passwd = getpass.getpass(prompt='Password: ')
        logger.info('Connecting to ESX System (IP: %s)' % args.hostname)
        sshClient.connect(args.hostname, username=args.username, password=passwd)
        # version check
        esxVersion = get_esx_version(sshClient)
        print('ESX Version on {} is {}'.format(args.hostname, esxVersion))
        logger.info('Checking ESX Version...')
        if not check_esx_version(esxVersion):
            raise Exception('ESX Version must be 7.0.1 or greater')

        print ('This script helps tag direct-attached disks for vSAN Direct on ESX')
        print ('Note: Only disks of type HDD are supported at this time.')
        print ()
        print ("For help, type help")
        show_usage()

        while True:
            # get device list
            print("Querying devices...")
            devices = query_devices(sshClient)
            # update devices with vSAN Direct status
            update_vsan_direct_status(sshClient, devices)
            # cull device list
            selectDevices = getVsanDirectCapableDevices(devices)
            # List the devices for the user to see
            print_devices(selectDevices)
            # find out what the user wants to do to these devices
```

```
            args = input('Command> ').split()
            if len(args) == 0:
                break
            cmd = args[0]
            if cmd == 'q' or cmd == 'quit' or cmd == 'exit':
                break
            elif cmd == 'help':
                show_usage()
            elif cmd == 'tag-all-hdd':
                print("Tagging all HDD devices...")
                tag_all_hdd_devices(sshClient, selectDevices)
            elif cmd == 'tag' or cmd == 'untag':
                chosenDevices = []
                if len(args) > 1:
                    serials = args[1].split(',')
                    for serialStr in serials:
                        serial = int(serialStr)
                        if serial < 1 or serial > len(selectDevices):
                            raise Exception("Error: Serial {} is out of range".format(serial))
                        chosenDevices.append(selectDevices[serial-1])
                if len(chosenDevices) == 0:
                    print("No devices specified")
                    continue
                if cmd == 'tag':
                    print("Tagging devices...")
                    tag_devices(sshClient, chosenDevices)
                else:
                    print("Untagging devices...")
                    untag_devices(sshClient, chosenDevices)
            else:
                print ("Error: Unrecognized command - %s" % cmd)
    except paramiko.ssh_exception.AuthenticationException as e:
        logger.error(e)
        sys.exit(5)
    except Exception as e:
        logger.error('Disk tagging failed with error: %s' % e)
        logger.error(traceback.format_exc())
        sys.exit(1)
    finally:
        # Close SSH client
        try:
            sshClient.close()
        except:
            pass

# Set up logging
logging.basicConfig()
logger = logging.getLogger('tag-disks-for-vsan-direct')

if __name__ == "__main__":
    main()
```

Erstellen eines vSAN Direct-Datenspeichers

Richten Sie als vSphere-Administrator einen vSAN Direct-Datenspeicher ein, der mit Funktionalitäten wie vSAN Data Persistence-Plattform oder VM-Instanzspeicher verwendet werden soll. Verwenden Sie zum Erstellen des Datenspeichers nicht beanspruchte Speichergeräte, die sich auf Ihrem ESXi-Host befinden.

Sie können den vSAN Direct-Datenspeicher erstellen, wenn Sie vSAN für Ihren Supervisor aktivieren. Die folgende Aufgabe zeigt, wie lokale Speichergeräte als vSAN Direct beansprucht werden können, wenn vSAN bereits auf dem Cluster aktiviert ist.

Verfahren

1 Navigieren Sie im vSphere Client zum vSAN-Cluster.

2 Klicken Sie auf die Registerkarte **Konfigurieren**.

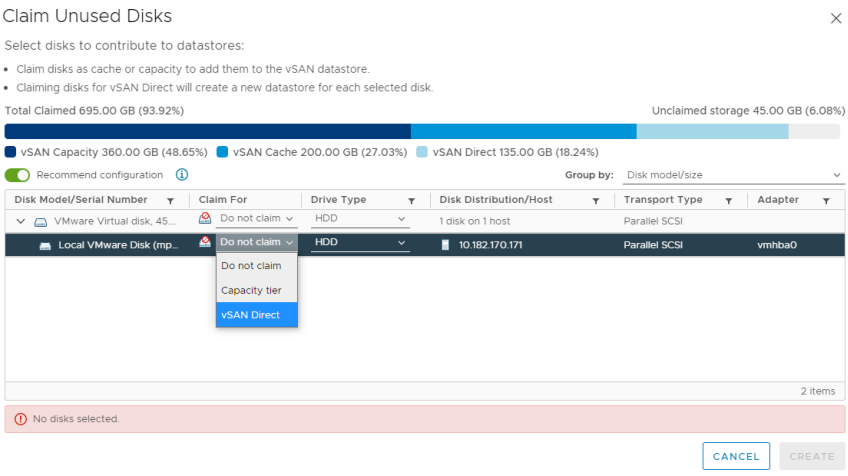
3 Klicken Sie unter vSAN auf **Festplattenverwaltung**.

4 Klicken Sie auf **Ungenutzte Festplatten beanspruchen**.

5 Klicken Sie im Dialogfeld **Unbelegte Festplatten beanspruchen** auf die Registerkarte **vSAN Direkt**.

6 Wählen Sie ein zu beanspruchende Gerät aus und aktivieren Sie ein Kontrollkästchen in der Spalte **Für vSAN Direct beanspruchen**.

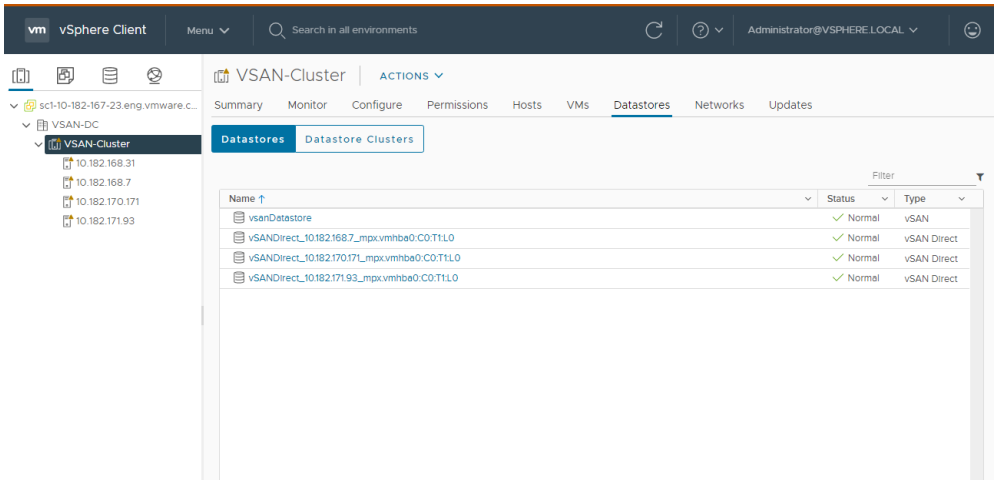
Hinweis Wenn Sie die Geräte für einen regulären vSAN-Datenspeicher beanspruchen, werden diese Geräte nicht auf der Registerkarte **vSAN Direct** angezeigt.



7 Klicken Sie auf **Erstellen**.

Für jedes von Ihnen beanspruchte Gerät erstellt vSAN Direct einen neuen Datenspeicher.

8 Klicken Sie auf die Registerkarte **Datenspeicher**, um alle vSAN Direct-Datenspeicher in Ihrem Cluster anzuzeigen.



Nächste Schritte

Sie können vSAN Direct mit externem Speicher verwenden. Weitere Informationen finden Sie in der Dokumentation zum Thema *Wartung der vSphere IaaS-Steuerungsebene* unter Verwenden eines externen Speichers mit vSAN Direct.

Überwachen von statusbehafteten Diensten in vSphere IaaS control plane

Nachdem Sie integrierte statusbehaftete Drittanbieterdienste aktiviert haben, nutzen Sie die Integritäts- und Kapazitätsüberwachungsfunktionen von vSAN, um den Status anzuzeigen und die Speicherplatznutzung der Dienstobjekte zu analysieren.

Verfahren

1 Navigieren Sie in vSphere Client zum Supervisor.

2 Klicken Sie auf die Registerkarte **Überwachen**.

3 Überwachen Sie virtuelle Objekte, die im Namespace ausgeführt werden, der zum aktivierten Dienst gehört.

   a Klicken Sie unter **vSAN** auf **Virtuelle Objekte**.

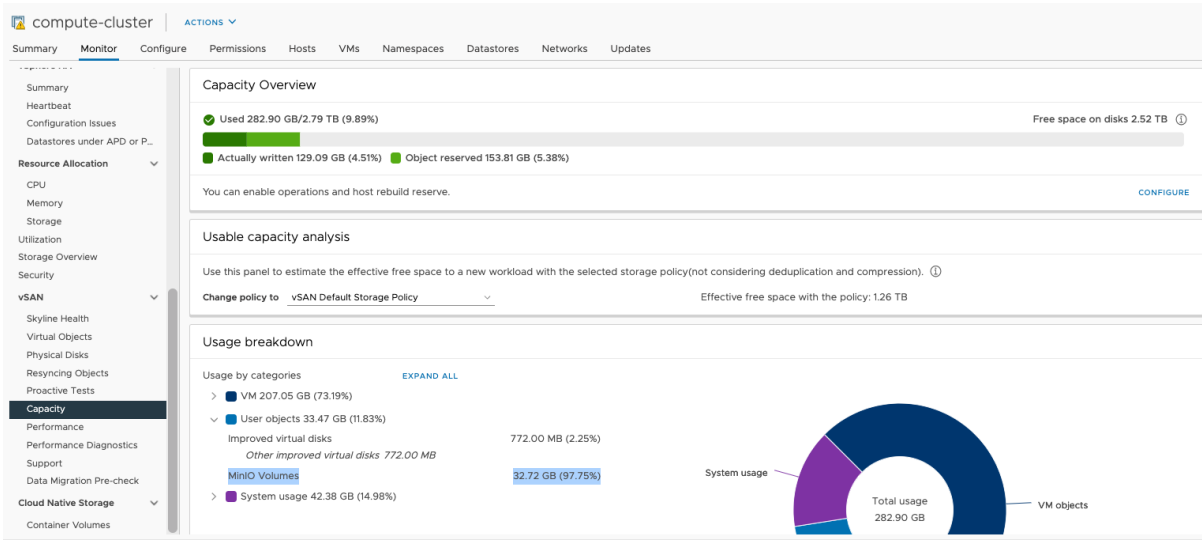
   Sie können die virtuellen Objekte wie z. B. MinIO-Operatorobjekte durchsuchen und deren Status überprüfen.

   b Um die Platzierung des Objekts über die physische Infrastruktur hinweg zu sehen, wählen Sie ein bestimmtes Objekt aus und klicken Sie auf **PLATZIERUNGSDETAILS ANZEIGEN**.

4 Überwachen Sie die Kapazität, die Dienstobjekte verwenden.

a Klicken Sie unter **vSAN** auf **Kapazität**.

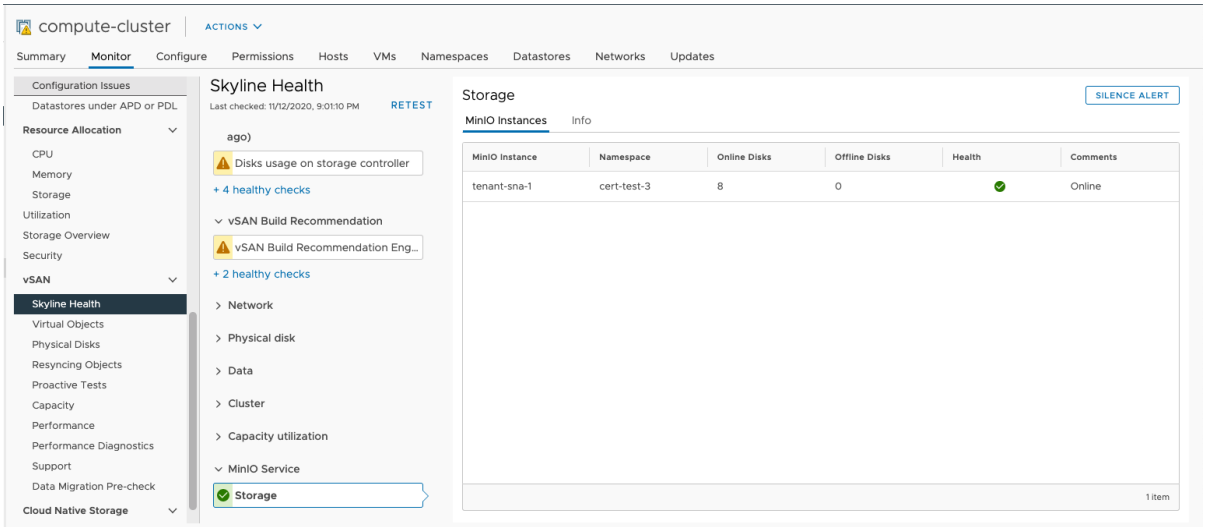
b Zeigen Sie im Bereich **Nutzungsaufschlüsselung** Ihre Dienstobjekte unter **Benutzerobjekte** an.



5 Überwachen Sie den Zustand Ihrer Dienstinstanzen.

a Wählen Sie unter **vSAN** die Option **Skyline Health** aus.

b Wählen Sie die Integritätsprüfung für einen einzelnen Dienst aus, um die detaillierten Informationen anzuzeigen.



Überprüfen der für statusbehaftete Dienste verfügbaren Speicherrichtlinien

Stellen Sie als DevOps Engineer sicher, dass der Namespace, den Sie für zustandsabhängige Dienste in der vSphere IaaS control plane-Umgebung verwenden, über die entsprechenden

Speicherklassen verfügt. Die Speicherklassen können vSAN Shared-Nothing-Architecture (SNA) und vSAN Direct sein.

Die vSAN Data Persistence-Plattform erstellt diese Speicherklassen im Namespace automatisch, nachdem ein vSphere-Administrator den zustandsabhängigen Dienst aktiviert hat. Weitere Informationen hierzu finden Sie unter Aktivieren von statusbehafteten Diensten in vSphere IaaS control plane.

Hinweis Nur Anwendungen, die auf dem Supervisor ausgeführt werden, können die Speicherklassen „vsan-direct“ und „vsan-sna“ verwenden. Diese Speicherklassen können nicht innerhalb eines Tanzu Kubernetes Grid-Clusters verwendet werden.

Neben Standardspeicherklassen können vSphere-Administratoren auch benutzerdefinierte Speicherrichtlinien erstellen und sie dem Namespace zuweisen. Weitere Informationen finden Sie unter Erstellen einer vSAN Direct-Speicherrichtlinie und vSAN SNA-Speicherrichtlinie erstellen.

Verfahren

- Stellen Sie sicher, dass die Speicherrichtlinien, die mit vSAN SNA und vSAN Direct verwendet werden sollen, in Ihrem Namespace verfügbar sind.

```
# kubectl get sc
NAME                        PROVISIONER              RECLAIMPOLICY   VOLUMEBINDINGMODE
ALLOWVOLUMEEXPANSION   AGE
sample-vsan-direct-thick    csi.vsphere.vmware.com   Delete          WaitForFirstConsumer
true                   3m36s
sample-vsan-sna-thick       csi.vsphere.vmware.com   Delete          WaitForFirstConsumer
true                   13m
```

Erstellen von benutzerdefinierten Speicherrichtlinien für die vSAN Data Persistence-Plattform

Wenn Sie einen statusbehafteten Dienst auf einem Supervisor in vSphere IaaS control plane aktivieren, erstellt die vSAN Data Persistence-Plattform Standardspeicherrichtlinien und entsprechende Speicherklassen und weist sie dem Dienst-Namespace zu. Die Richtlinien gelten für vSAN Shared-Nothing-Architektur (SNA)- und vSAN Direct-Datenspeicher. Anstelle der Standardeinstellung können Sie benutzerdefinierte Speicherrichtlinien erstellen.

Befolgen Sie bei der Entscheidung darüber, welcher Datenspeichertyp verwendet werden soll, die folgenden allgemeinen Empfehlungen:

- Verwenden Sie vSAN Direct, wenn Sie einen dedizierten Hardware-Cluster für die cloudnativen Shared Nothing-Dienste erstellen.
- Verwenden Sie vSAN mit SNA, wenn Sie möchten, dass die cloudnative statusbehaftete Anwendung die physische Infrastruktur mit anderen regulären VMs oder Kubernetes-Arbeitslasten gemeinsam nutzen soll. Jede Arbeitslast kann ihre eigene Speicherrichtlinie definieren und das Beste aus beidem über einen einzelnen Cluster abrufen.

Weitere Informationen finden Sie unter Shared Nothing-Speicher für vSphere.

Nachdem Sie die Richtlinie erstellt haben, können Sie sie dem Namespace zuweisen, in dem Ihr zustandsabhängiger Dienst ausgeführt wird. Weitere Informationen finden Sie unter Erstellen und Konfigurieren eines vSphere-Namespace im Supervisor..

Erstellen einer vSAN Direct-Speicherrichtlinie

Wenn Sie vSAN Direct verwenden, erstellen Sie eine Speicherrichtlinie, die mit einem Supervisor-Namespace verwendet werden soll. In dem Namespace, den Sie mit dieser Speicherrichtlinie verknüpfen, können Sie Arbeitslasten ausführen, die mit vSAN Direct kompatibel sind, z. B. statusbehaftete Dienste oder Instanzspeicher-VMs.

Verfahren

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

   a Klicken Sie auf der **Startseite** auf **Richtlinien und Profile**.

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

   c Klicken Sie auf **Erstellen**.

2 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.
Beschreibung	Geben Sie die Beschreibung der Speicherrichtlinie ein.

3 Aktivieren Sie auf der Seite **Richtlinienstruktur** unter **Datenspeicherspezifische Regeln** Regeln für die Platzierung des vSAN Direct-Speichers.

4 Legen Sie vSAN Direct auf der Seite **vSAN Direct-Regeln** als Speicherplatzierungstyp fest.

5 Überprüfen Sie auf der Seite **Speicherkompatibilität** die Liste der vSAN Direct-Datenspeicher, die mit dieser Richtlinie übereinstimmen.

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

   Um Änderungen an Einstellungen vorzunehmen, klicken Sie auf **Zurück**, um wieder zur entsprechenden Seite zu wechseln.

vSAN SNA-Speicherrichtlinie erstellen

Wenn Sie vSAN mit der vSAN Data Persistence-Plattform verwenden, können Sie eine vSAN Shared Nothing Architecture (SNA) für die Verwendung mit dem Namespace erstellen, in dem zustandsabhängige Dienste ausgeführt werden.

Verfahren

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

   a Klicken Sie auf der **Startseite** auf **Richtlinien und Profile**.

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

   c Klicken Sie auf **Erstellen**.

2 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. **`Beispiel SNA Thick`**.
Beschreibung	Geben Sie die Beschreibung der Speicherrichtlinie ein.

3 Aktivieren Sie auf der Seite **Richtlinienstruktur** unter **Datenspeicherspezifische Regeln** Regeln für die Platzierung des vSAN-Speichers.

4 Klicken Sie auf der Seite **vSAN** auf die Registerkarte **Verfügbarkeit** und wählen Sie die folgenden Werte aus. Die Werte gelten nur für SNA-Arbeitslasten auf der vSAN Data Persistence-Plattform. Sie können nicht für die Bereitstellung von VM-Arbeitslasten verwendet werden.

Option	Bezeichnung
Option	Wert
Ausfalltoleranz von Site	**Keine – Standardcluster** **Hinweis** Die vSAN Data Persistence-Plattform unterstützt nur Standardcluster.
Zu tolerierende Ausfälle	**Keine Datenredundanz mit Hostaffinität**

   Für SNA-Arbeitslasten erzwungenes Thick Provisioning ist als Wert für die Objektspeicherplatzreservierung auf der Registerkarte **Erweiterte Richtlinienregeln** ausgewählt. Sie können diesen Wert nicht ändern.

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

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

   Um Änderungen an Einstellungen vorzunehmen, klicken Sie auf **Zurück**, um wieder zur entsprechenden Seite zu wechseln.

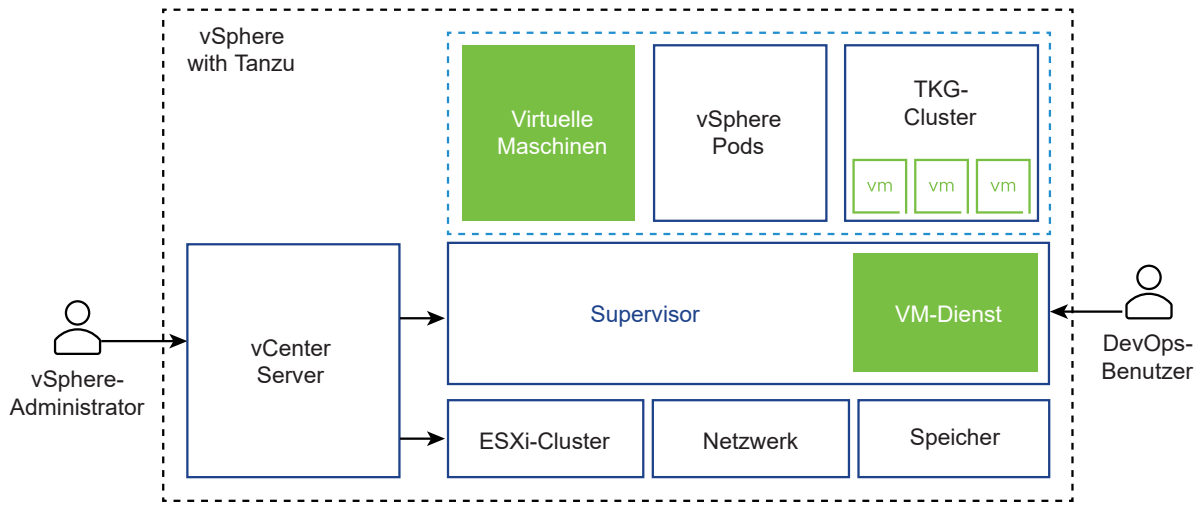
Bereitstellen und Verwalten von virtuellen Maschinen in vSphere IaaS control plane

6

vSphere IaaS control plane bietet eine VM-Service-Funktionalität, die es DevOps-Ingenieuren ermöglicht, neben Containern auch VMs in einer gemeinsamen, freigegebenen Kubernetes-Umgebung bereitzustellen und auszuführen. Sie können den VM-Dienst verwenden, um den Lebenszyklus von virtuellen Maschinen in einem Namespace zu verwalten. Der VM-Dienst verwaltet eigenständige VMs und VMs, die die Tanzu Kubernetes Grid-Cluster bilden.

Der VM-Dienst adressiert die Bedürfnisse von DevOps-Teams, die Kubernetes nutzen, aber bestehende VM-basierte Arbeitslasten haben, die nicht einfach containerisiert werden können. Es hilft Anwendern auch, den Aufwand für die Verwaltung einer Nicht-Kubernetes-Plattform neben einer Container-Plattform zu reduzieren. Wenn Container und VMs auf einer Kubernetes-Plattform ausgeführt werden, können DevOps-Teams ihren Arbeitslastbedarf auf nur einer Plattform konsolidieren.

Hinweis Zusätzlich zu eigenständigen VMs verwaltet der VM-Dienst die VMs, die die Tanzu Kubernetes Grid-Cluster bilden. Informationen über Cluster finden Sie in der Dokumentation zum Thema *Verwenden des TKG-Dienstes mit der vSphere IaaS-Steuerungsebene*.



Jede VM, die über den VM-Dienst bereitgestellt wird, funktioniert als vollständige Maschine, auf der alle Komponenten, einschließlich eines eigenen Betriebssystems, in der vSphere IaaS control plane-Infrastruktur ausgeführt werden. Die VM hat Zugriff auf Netzwerke und Speicher, die ein Supervisor bereitstellt, und wird mithilfe des standardmäßigen Kubernetes-Befehls `kubectl` verwaltet. Die VM wird als vollständig isoliertes System ausgeführt, das immun gegen Störungen durch andere VMs oder Arbeitslasten in der Kubernetes-Umgebung ist.

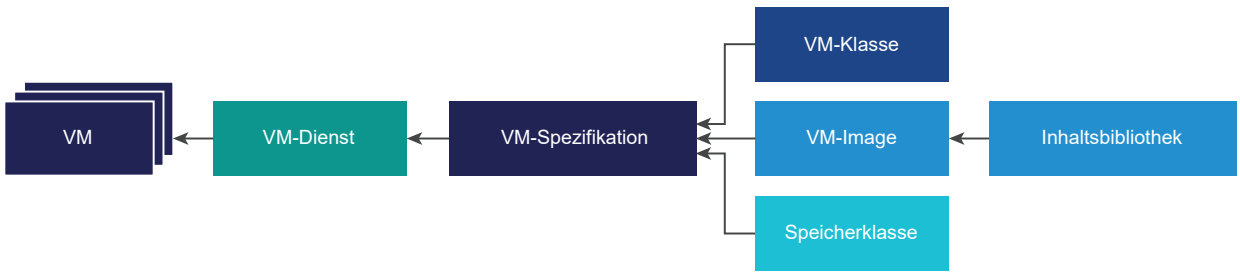
Wann werden virtuelle Maschinen auf einer Kubernetes-Plattform verwendet?

Im Allgemeinen hängt die Entscheidung zum Ausführen von Arbeitslasten in einem Container oder in einer VM von Ihren geschäftlichen Anforderungen und Zielen ab. Zu den Gründen für den Einsatz von VMs zählen unter anderem die folgenden:

- Ihre Anwendungen können nicht containerisiert werden.
- Sie haben spezifische Hardwareanforderungen für Ihr Projekt.
- Anwendungen sind für einen benutzerdefinierten Kernel oder ein benutzerdefiniertes Betriebssystem konzipiert.
- Anwendungen sind besser für die Ausführung in einer VM geeignet.
- Sie wünschen sich ein konsistentes Kubernetes-Erlebnis und möchten Overhead vermeiden. Anstatt separate Infrastruktursätze für Ihre Nicht-Kubernetes- und Container-Plattformen zu betreiben, können Sie diese Stacks konsolidieren und mit einem vertrauten `kubectl`-Befehl verwalten.

Konzepte des VM-Diensts

Um den Status einer VM zu beschreiben, die in einer virtuellen vSphere-Namespace bereitgestellt werden soll, verwenden Sie Parameter wie eine VM-Klasse, ein VM-Image und eine Speicherklasse. Der VM-Service führt dann diese Spezifikationen zusammen, um eigenständige VMs oder VMs, die Tanzu Kubernetes Grid-Cluster unterstützen, zu erstellen.



VM-Dienst

Der VM-Dienst ist eine Komponente von vSphere IaaS control plane, die eine deklarative, Kubernetes-ähnliche API für die Verwaltung von VMs und zugehörigen vSphere-Ressourcen bietet. Der VM-Service ermöglicht es den vSphere-Administratoren, Ressourcen bereitzustellen und Vorlagen wie VM-Klassen und VM-Images für Kubernetes bereitzustellen. DevOps-Ingenieure können diese Ressourcen verwenden, um den gewünschten Zustand einer VM zu beschreiben. Nachdem die DevOps-Ingenieure den VM-Zustand spezifiziert haben, wandelt der VM-Service den gewünschten Zustand in einen realisierten Zustand gegenüber den unterstützenden Infrastrukturressourcen um.

Eine über den VM-Dienst erstellte VM kann nur aus dem Kubernetes-Namespace mit den `kubectl`-Befehlen verwaltet werden. vSphere-Administratoren können die VM nicht von der vSphere Client aus verwalten, können aber ihre Details anzeigen und die von ihr verwendeten Ressourcen überwachen. Weitere Informationen finden Sie unter Überwachen der in vSphere IaaS control plane verfügbaren virtuellen Maschinen.

VM-Klasse

Die VM-Klasse ist eine VM-Spezifikation, mit der eine Gruppe von Ressourcen für eine VM angefordert werden kann. Die VM-Klasse wird von einem vSphere-Administrator kontrolliert und verwaltet und definiert Parameter wie die Anzahl der virtuellen CPUs, die Arbeitsspeicherkapazität und die Reservierungseinstellungen. Die definierten Parameter werden durch die zugrunde liegenden Infrastrukturressourcen eines Supervisors unterstützt und garantiert.

Ein vSphere-Administrator kann benutzerdefinierte VM-Klassen erstellen.

Darüber hinaus bietet die Arbeitslastverwaltung mehrere Standard-VM-Klassen. In der Regel gibt es jeden Standardklassentyp in zwei Editionen: garantiert und bestmöglich. Eine garantierte Edition reserviert vollständig die Ressourcen, die eine VM-Spezifikation anfordert. Für eine bestmögliche Klassenedition gilt dies nicht; das bedeutet, dass die Ressourcen überbelegt werden können. In der Regel wird ein garantierter Typ in einer Produktionsumgebung verwendet.

Beispiele für Standard-VM-Klassen sind die folgenden.

Klasse	CPU	Arbeitsspeicher (GB)	Reservierte CPU und reservierter Arbeitsspeicher
`guaranteed-large`	4	16	Ja
`best-effort-large`	4	16	Nein
`guaranteed-small`	2	4	Ja
`best-effort-small`	2	4	Nein

Der vSphere-Administrator kann eine beliebige Anzahl vorhandener VM-Klassen zuweisen, um sie für DevOps-Ingenieure innerhalb eines bestimmten Namespaces zur Verfügung zu stellen.

Die VM-Klasse bietet eine vereinfachte Erfahrung für die DevOps-Ingenieure. Die DevOps müssen nicht die vollständige Konfiguration jeder VM verstehen, die sie erstellen möchten. Stattdessen können sie eine VM-Klasse aus den verfügbaren Optionen auswählen, und der VM-Dienst verwaltet die VM-Konfiguration.

Auf der Kubernetes-Seite werden die VM-Klassen als `VirtualMachineClass`-Ressourcen angezeigt.

VM-Image

Ein VM-Image ist eine Vorlage, die eine Softwarekonfiguration enthält, einschließlich Betriebssystem, Anwendungen und Daten.

Wenn DevOps-Ingenieure VMs erstellen, können sie Images aus der Inhaltsbibliothek auswählen, die dem Namespace zugeordnet ist. Für die DevOps werden die Images als `VirtualMachineImage` zur Verfügung gestellt.

Ein vSphere-Administrator kann VM-Images erstellen, die mit vSphere IaaS control plane kompatibel sind, und sie in eine Inhaltsbibliothek hochladen.

Inhaltsbibliothek

Ein DevOps-Ingenieur verwendet eine Inhaltsbibliothek als Quelle von Images, um eine VM zu erstellen. Ähnlich wie VM-Klassen kann ein vSphere-Administrator vorhandene Inhaltsbibliotheken einem Namespace oder einem Cluster zuweisen, um sie DevOps-Ingenieuren zur Verfügung zu stellen. Der vSphere-Administrator kann die Namespace-Inhaltsbibliothek auch beschreibbar machen. Mit dieser zusätzlichen Berechtigung können DevOps-Benutzer ihre Images in der Bibliothek veröffentlichen.

Speicherklasse

Der VM-Dienst verwendet Speicherklassen zum Platzieren virtueller Festplatten und zum dynamischen Anhängen persistenter Volumes. Weitere Informationen zu Speicherklassen finden Sie unter Kapitel 8 Verwenden von persistentem Speicher mit Supervisor-Arbeitslasten in vSphere IaaS control plane.

VM-Spezifikation

DevOps-Ingenieure beschreiben den gewünschten Zustand einer VM in einer YAML-Datei, die das VM-Image, die VM-Klasse und die Speicherklasse zusammenführt.

VM-Operator für Kubernetes

Der VM-Operator ermöglicht die Verwaltung virtueller Maschinen mit einer deklarativen API im Kubernetes-Stil.

Ab vSphere 8.0 Update 3 wird der VM-Operator „v1alpha2“ von vSphere IaaS control plane unterstützt. Diese Version bietet unter anderem folgende Funktionen:

- Verbesserte Unterstützung für Bootstrap-Anbieter, einschließlich Unterstützung für Inline-Cloud-Init und Windows.

- Verbesserte Konfiguration des Gastnetzwerks.
- Erweiterte Statusfunktionen.
- Unterstützung für benutzerdefinierte Readiness-Gates.
- Neue VirtualMachineWebConsoleRequest-API.

Abgesehen von neuen v1alpha2-spezifischen API-Änderungen funktionieren die meisten anderen APIs in v1alpha2 zusammen mit v1alpha1. Die meisten Felder in VM-Spezifikationen sind mit v1alpha1 abwärtskompatibel.

Nach der Veröffentlichung von v1alpha2 können Sie weiterhin v1alpha1-Objekte verwenden. Alle v1alpha1-Objekte werden mithilfe von Konvertierungs-Webhooks, die in den VM-Operator integriert sind, automatisch in v1alpha2 umgewandelt.

Informationen zum VM-Operator „v1alpha2“ und den unterstützten Feldern finden Sie unter https://vm-operator.readthedocs.io/en/stable/ref/api/v1alpha2/.

Netzwerk

Der VM-Dienst hat keine spezifischen Anforderungen und basiert auf der netzwerkspezifischen Konfiguration, die in vSphere IaaS control plane zur Verfügung steht. Der VM-Dienst unterstützt beide Netzwerktypen, das vSphere-Netzwerk oder NSX. Wenn VMs bereitgestellt werden, teilt ein verfügbarer Netzwerkanbieter den VMs statische IP-Adressen zu. Weitere Informationen finden Sie unter Supervisor-Netzwerk in der Dokumentation zum Thema *Konzepte und Planung der vSphere IaaS-Steuerungsebene*.

VM-Dienst und Supervisor mit vSphere-Zonen

Wenn Sie VMs auf einem Supervisor mit drei Zonen erstellen, wird die VM-Instanz über alle verfügbaren Zonen hinweg repliziert. Zum Steuern der Platzierung der VMs über die YAML-Datei kann das DevOps-Team die Kubernetes-Bezeichnung `topology.kubernetes.io/zone` verwenden. Beispiel: `topology.kubernetes.io/zone: zone-a02`.

Workflow für die Bereitstellung und Überwachung einer VM

Als vSphere-Administrator legen Sie Leitlinien für die Richtlinie und Governance der VMs fest und stellen VM-Ressourcen wie VM-Klassen und VM-Vorlagen an DevOps-Ingenieure bereit. Nach der Bereitstellung einer VM können Sie sie mithilfe des vSphere Client überwachen.

Schritt	Durchgeführt von	Beschreibung
1	vSphere-Administrator	Erstellen und Verwalten von Inhaltsbibliotheken für eigenständige VMs in vSphere IaaS control plane
2	vSphere-Administrator	Arbeiten mit VM-Klassen in vSphere IaaS control plane Konfigurieren Sie für die Verwendung von NVIDIA vGPU ein PCI-Gerät in der VM-Klasse. Weitere Informationen finden Sie unter Bereitstellen einer VM mit vGPU und anderen PCI-Geräten in vSphere IaaS control plane.

Schritt	Durchgeführt von	Beschreibung
3	DevOps-Ingenieur	Bereitstellen einer eigenständigen VM in vSphere IaaS control plane Informationen zu Tanzu Kubernetes Grid-Cluster-VMs finden Sie unter *Verwenden des TKG-Dienstes mit der vSphere IaaS-Steuerungsebene*.
4	vSphere-Administrator	Überwachen der in vSphere IaaS control plane verfügbaren virtuellen Maschinen
5	DevOps-Ingenieur	Verwalten und Veröffentlichen von Inhaltsbibliotheks-Images in vSphere IaaS control plane

Lesen Sie als Nächstes die folgenden Themen:

- Erstellen und Verwalten von Inhaltsbibliotheken für eigenständige VMs in vSphere IaaS control plane
- Arbeiten mit VM-Klassen in vSphere IaaS control plane
- Erstellen und Verwalten von VM-Klassen mithilfe der Datencenter-CLI
- Bereitstellen einer eigenständigen VM in vSphere IaaS control plane
- Bereitstellen einer VM mit vGPU und anderen PCI-Geräten in vSphere IaaS control plane
- Bereitstellen einer VM mit Instanzspeicher in vSphere IaaS control plane
- Bereitstellen von VMs mit konfigurierbaren OVF-Eigenschaften in vSphere IaaS control plane
- Überwachen der in vSphere IaaS control plane verfügbaren virtuellen Maschinen
- Fehlerbehebung bei VMs mithilfe der vSphere VM-Web-Konsole

Erstellen und Verwalten von Inhaltsbibliotheken für eigenständige VMs in vSphere IaaS control plane

Für die Bereitstellung von virtuellen Maschinen in der vSphere IaaS control plane-Umgebung benötigen DevOps-Benutzer Zugriff auf VM-Images oder Vorlagen, die Softwarekonfigurationen enthalten, einschließlich Betriebssystemen, Anwendungen und Daten. Für den Zugriff auf Images konfiguriert ein vSphere-Administrator eine VM-Inhaltsbibliothek und ordnet sie dann dem Namespace zu, in dem die VMs bereitgestellt werden. Ab vSphere 8.0 Update 2 kann der vSphere-Administrator die Inhaltsbibliothek auch auf Supervisor-Ebene zuweisen, damit sie in allen Namespaces zur Verfügung steht.

Erstellen einer Inhaltsbibliothek für eigenständige VMs in vSphere IaaS control plane

Erstellen Sie als vSphere-Administrator eine Inhaltsbibliothek zum Speichern und Verwalten von VM-Vorlagen.

Erstellen einer Inhaltsbibliothek für eigenständige VMs

Sie können eine lokale Inhaltsbibliothek erstellen und sie mit Vorlagen und anderen Dateitypen füllen. Sie können auch eine abonnierte Bibliothek erstellen, um die Inhalte einer bereits vorhandenen veröffentlichten lokalen Bibliothek zu verwenden.

Um die Elemente einer Inhaltsbibliothek zu schützen, können Sie eine OVF-Sicherheitsrichtlinie anwenden. Die OVF-Sicherheitsrichtlinie erzwingt eine strenge Validierung, wenn Sie eine Inhaltsbibliothek bereitstellen oder aktualisieren, Elemente in eine Inhaltsbibliothek importieren oder Vorlagen synchronisieren. Um sicherzustellen, dass die Vorlagen von einem vertrauenswürdigen Zertifikat signiert sind, können Sie das OVF-Signaturzertifikat von einer vertrauenswürdigen Zertifizierungsstelle zu einer Inhaltsbibliothek hinzufügen.

Weitere Informationen zu Inhaltsbibliotheken und VM-Vorlagen in vSphere finden Sie unter Verwenden von in Inhaltsbibliotheken in *vSphere-Administratorhandbuch für virtuelle Maschinen*.

Voraussetzungen

Erforderliche Rechte:

- **Inhaltsbibliothek.Lokale Bibliothek erstellen** oder **Inhaltsbibliothek.Abonnierte Bibliothek erstellen** in der vCenter Server-Instanz, in der Sie die Bibliothek erstellen möchten.
- **Datenspeicher.Speicher zuteilen** auf dem Zieldatenspeicher.

Verfahren

1. Navigieren Sie zur Seite **VM-Dienst**.
   a. Wählen Sie im vSphere Client-Startmenü die Option **Arbeitslastverwaltung** aus.
   b. Klicken Sie auf die Registerkarte **Dienste** und dann auf der Karte **VM-Dienst** auf **Verwalten**.
2. Klicken Sie auf der Seite **VM-Dienst** auf **Inhaltsbibliotheken > Inhaltsbibliothek erstellen**.

   Diese Aktion führt Sie zum Abschnitt „Inhaltsbibliothek“ im vSphere Client.
3. Klicken Sie auf **Erstellen**.

   Der Assistent **Neue Inhaltsbibliothek** wird geöffnet.
4. Geben Sie auf der Seite **Name und Speicherort** einen Namen ein, wählen Sie eine vCenter Server-Instanz für die Inhaltsbibliothek aus und klicken Sie auf **Weiter**.

   Verwenden Sie unbedingt einen informativen Namen für die Inhaltsbibliothek, damit Ihr DevOps-Team diese problemlos finden und auf die Elemente in der Bibliothek zugreifen kann.

5 Wählen Sie auf der Seite **Inhaltsbibliothek konfigurieren** den Typ der zu erstellenden Inhaltsbibliothek aus und klicken Sie auf **Weiter**.

Option	Beschreibung
Lokale Inhaltsbibliothek	Auf eine Inhaltsbibliothek kann nur von derjenigen vCenter Server-Instanz aus zugegriffen werden, in der Sie sie standardmäßig erstellt haben. a (Optional) Um den Inhalt der Bibliothek für andere vCenter Server-Instanzen verfügbar zu machen, wählen Sie **Veröffentlichung aktivieren** aus. b (Optional) Wenn für den Zugriff auf die Inhaltsbibliothek ein Kennwort erforderlich sein soll, wählen Sie **Authentifizierung aktivieren** aus und legen Sie ein Kennwort fest.
Abonnierte Inhaltsbibliothek	Eine abonnierte Inhaltsbibliothek stammt aus einer veröffentlichten Inhaltsbibliothek. Verwenden Sie diese Option, um vorhandene Inhaltsbibliotheken zu nutzen. Sie können die abonnierte Bibliothek mit der veröffentlichten Bibliothek synchronisieren, um aktuelle Inhalte anzuzeigen. Sie können der abonnierten Bibliothek jedoch keine Inhalte hinzufügen oder Inhalte daraus entfernen. Nur ein Administrator der veröffentlichten Bibliothek kann Inhalte der veröffentlichten Bibliothek hinzufügen, ändern oder daraus entfernen. Geben Sie für das Abonnement einer Bibliothek die folgenden Informationen an: a Geben Sie im Textfeld **URL für Abonnement** die URL-Adresse für die veröffentlichte Bibliothek ein. b Wenn die Authentifizierung für die veröffentlichte Bibliothek aktiviert ist, wählen Sie **Authentifizierung aktivieren** aus und geben Sie das Kennwort des Herausgebers ein. c Wählen Sie eine Downloadmethode für den Inhalt der abonnierten Bibliothek aus. ■ Wenn Sie eine lokale Kopie aller Elemente in der veröffentlichten Bibliothek unmittelbar nach dem Abonnieren herunterladen möchten, wählen Sie **sofort** aus. ■ Wenn Sie Speicherplatz sparen möchten, wählen Sie **bei Bedarf** aus. Sie laden nur die Metadaten für die Elemente in der veröffentlichten Bibliothek herunter. Wenn Sie ein Element verwenden müssen, synchronisieren Sie das Element oder die gesamte Bibliothek, um den dazugehörigen Inhalt herunterzuladen. d Akzeptieren Sie den Fingerabdruck des SSL-Zertifikats, wenn Sie dazu aufgefordert werden. Der Fingerabdruck des SSL-Zertifikats wird auf Ihrem System gespeichert, bis Sie die abonnierte Inhaltsbibliothek aus dem Bestand löschen.

6 (Optional) Wählen Sie auf der Seite **Sicherheitsrichtlinie anwenden** die Option **Sicherheitsrichtlinie anwenden** aus und dann **OVF-Standardrichtlinie**.

Für die abonnierte Bibliothek wird diese Option nur angezeigt, wenn die Bibliothek Sicherheitsrichtlinien unterstützt.

Wenn Sie diese Option auswählen, führt das System eine strenge OVF-Zertifikatüberprüfung durch, wenn ein OVF-Element vom lokalen Host in die Bibliothek importiert oder ein Element synchronisiert wird. Die OVF-Elemente, die die Zertifikatvalidierung nicht bestehen, können nicht importiert werden.

Wenn das Element die Validierung während der Synchronisierung nicht besteht, wird es mit dem Tag **Überprüfung fehlgeschlagen** gekennzeichnet. Nur das Element und die Metadaten werden beibehalten, aber nicht die Dateien im Element.

7 Wählen Sie auf der Seite **Speicher hinzufügen** einen Datenspeicher als Speicherort für die Inhalte der Inhaltsbibliothek aus und klicken Sie auf **Weiter**.

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

Auffüllen einer Inhaltsbibliothek mit VM-Images für eigenständige VMs

Nachdem Sie die Inhaltsbibliothek erstellt haben, füllen Sie sie mit VM-Vorlagen im OVA- oder OVF-Format auf. Ihre DevOps-Ingenieure können die Vorlagen verwenden, um neue eigenständige virtuelle Maschinen in der virtuellen vSphere IaaS control plane-Umgebung bereitzustellen.

Zum Auffüllen der Bibliothek können Sie verschiedene Methoden verwenden. In diesem Thema wird erläutert, wie Sie einer lokalen Inhaltsbibliothek Elemente hinzufügen, indem Sie Dateien von Ihrem lokalen Computer oder von einem Webserver importieren. Weitere Informationen zum Auffüllen der Inhaltsbibliothek finden Sie unter Auffüllen der Bibliotheken mit Inhalt in *vSphere-Administratorhandbuch für virtuelle Maschinen*.

Hinweis Es gibt keine Einschränkungen für die von Ihnen verwendeten VM-Images. Wenn Sie einsatzbereite OVA-Images testen möchten, können Sie sie von der Seite Empfohlene Images herunterladen. Beachten Sie, dass diese Images nur für die POC-Verwendung vorgesehen sind. Erstellen Sie in der Produktionsumgebung Images mit den neuesten Patches und erforderlichen Sicherheitseinstellungen, die den Unternehmenssicherheitsrichtlinien folgen.

Voraussetzungen

- Erstellen Sie VM-Images, die mit vSphere IaaS control plane kompatibel sind.

  Die Image-Spezifikation erfordert, dass alle VM-Images VMware Tools oder ein gleichwertiges Open Source-Paket enthalten. Die Images müssen eine der folgenden Optionen verwenden, um ein Bootstrap des Gastbetriebssystems und seines Netzwerk-Stacks durchzuführen. Weitere Informationen finden Sie unter Bootstrap-Anbieter.

  - Linux + Cloud-Init Version 17.9-21.2 mit DataSourceVMwareGuestInfo.
  - Linux + Cloud-Init Version 21.3+
  - Windows + Cloudbase-Init Version 1.1.0+
  - Windows + Sysprep (Systemvorbereitung)

  Informationen zu Cloud-Init finden Sie in der offiziellen Dokumentation unter Der Standard für die Anpassung von Cloud-Instanzen.

Informationen zu Sysprep finden Sie in der offiziellen Dokumentation unter Sysprep-Übersicht.

- Wenn Ihre Bibliothek durch eine Sicherheitsrichtlinie geschützt ist, vergewissern Sie sich, dass alle Bibliothekselemente konform sind. Wenn eine geschützte Bibliothek eine Mischung aus konformen und nicht konformen Elementen enthält, werden den DevOps-Ingenieuren mit `kubectl get virtualmachineimages` keine VM-Images angezeigt.
- Erforderliche Berechtigung: **Inhaltsbibliothek.Bibliothekselement hinzufügen** und **Inhaltsbibliothek.Dateien aktualisieren** auf der Bibliothek.

Verfahren

1. Wählen Sie im vSphere Client-Startmenü die Option **Inhaltsbibliotheken** aus.
2. Klicken Sie mit der rechten Maustaste auf eine lokale Inhaltsbibliothek und wählen Sie **Element importieren**.

   Das Dialogfeld **Bibliothekselement importieren** wird geöffnet.
3. Wählen Sie im Abschnitt **Quelle** die Quelle des Elements aus.

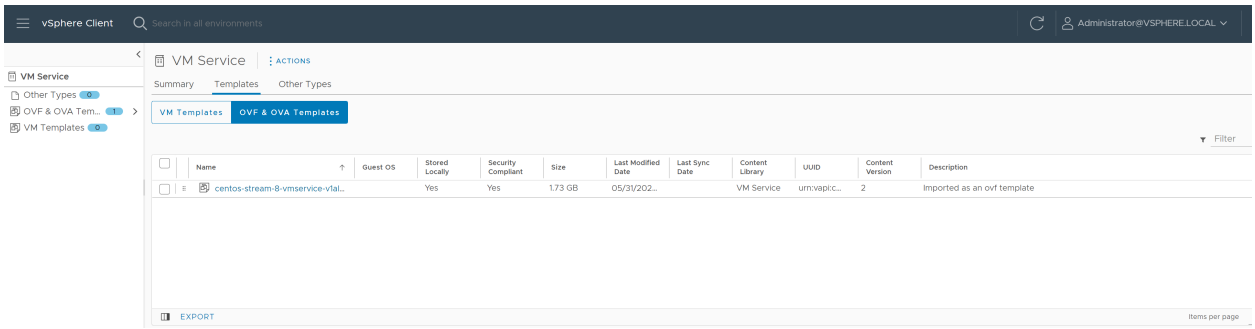
Option	Beschreibung
URL	Geben Sie den Pfad zu dem Webserver ein, auf dem sich das Element befindet. **Hinweis** Sie können entweder eine `.ovf` oder eine `.ova`-Datei importieren. Das resultierende Inhaltsbibliothekselement ist vom Typ „OVF-Vorlage“.
Lokale Datei	Klicken Sie auf **Datei hochladen**, um zu der Datei zu navigieren, die Sie von Ihrem lokalen System importieren möchten. Sie können das Dropdown-Menü verwenden, um Dateien in Ihrem lokalen System zu filtern. **Hinweis** Sie können entweder eine `.ovf` oder eine `.ova`-Datei importieren. Wählen Sie beim Importieren einer OVF-Vorlage zuerst die OVF-Deskriptordatei (`.ovf`) aus. Im nächsten Schritt werden Sie aufgefordert, die anderen Dateien in der OVF-Vorlage auszuwählen, z. B. die `.vmdk`-Datei auszuwählen. Das resultierende Inhaltsbibliothekselement ist vom Typ „OVF-Vorlage“.

   vCenter Server liest und validiert die Manifest- und Zertifikatdateien im OVF-Paket während des Importierens. Eine Warnung wird im Assistenten zum **Importieren von Bibliothekselementen** angezeigt, wenn Probleme mit Zertifikaten bestehen, z. B. wenn vCenter Server ein abgelaufenes Zertifikat erkennt.

   Hinweis vCenter Server liest signierte Inhalte nicht, wenn das OVF-Paket aus einer `.ovf`-Datei von Ihrem lokalen Computer importiert wird.
4. Geben Sie im Abschnitt **Ziel** einen Namen und eine Beschreibung für das Element ein.
5. Klicken Sie auf **Import**.

Ergebnisse

Das Element wird auf der Registerkarte **Vorlagen** oder auf der Registerkarte **Andere Typen** angezeigt.



Hinzufügen und Verwalten von VM-Inhaltsbibliotheken in vSphere IaaS control plane

Nachdem Sie die Inhaltsbibliothek erstellt und mit VM-Vorlagen aufgefüllt haben, verwenden Sie den vSphere Client, um die Bibliothek dem Namespace hinzuzufügen. Durch das Hinzufügen der Bibliothek zum Namespace geben Sie Ihren DevOps-Benutzern Zugriff auf die Bibliothek. Darüber hinaus können Sie die Datencenter-CLI (DCLI)-Befehle verwenden, um dem Namespace eine beschreibbare oder schreibgeschützte Inhaltsbibliothek hinzuzufügen oder um eine schreibgeschützte Bibliothek auf Clusterebene zuzuweisen.

Hinzufügen einer VM-Inhaltsbibliothek zu einem Namespace mit dem vSphere Client

Die Inhaltsbibliothek, die Sie mit dem vSphere Client hinzufügen, ist schreibgeschützt. Die DevOps-Benutzer können auf Images aus dieser Inhaltsbibliothek zugreifen, aber keine VM-Images in dieser Bibliothek veröffentlichen.

Sie können mehrere Inhaltsbibliotheken zu einem einzelnen Namespace hinzufügen. Sie können dieselbe Inhaltsbibliothek verschiedenen Namespaces hinzufügen.

Hinweis Dieses Verfahren gilt nur für Inhaltsbibliotheken für den VM-Dienst. Eine Inhaltsbibliothek für Tanzu Kubernetes Grid muss über die Tanzu Kubernetes Grid-Karte verwaltet werden.

Voraussetzungen

Erforderliche Rechte:

- **Namespaces.Clusterweite Konfiguration ändern**
- **Namespaces.Namespace-Konfiguration ändern**

Verfahren

1 Wechseln Sie in vSphere Client zum Namespace.
   a Wählen Sie im vSphere Client-Startmenü die Option **Arbeitslastverwaltung** aus.
   b Klicken Sie auf die Registerkarte **Namespaces** und klicken Sie dann auf den Namespace.
2 Fügen Sie eine Inhaltsbibliothek hinzu.
   a Klicken Sie auf der Karte **VM-Dienst** auf **Inhaltsbibliothek hinzufügen**.
   b Wählen Sie eine oder mehrere Inhaltsbibliotheken aus und klicken Sie auf **OK**.

Verwalten von VM-Inhaltsbibliotheken in einem Namespace mithilfe des vSphere Client

Nachdem Sie die Bibliothek mit dem Namespace verknüpft haben, können Sie den vSphere Client verwenden, um sie vom Namespace zu entfernen. Sie können auch weitere Bibliotheken hinzufügen.

Das Entfernen einer Inhaltsbibliothek aus einem Namespace wirkt sich nicht auf VMs aus, die zuvor mit den Bibliotheks-Images bereitgestellt wurden.

Hinweis Dieses Verfahren gilt nur für Inhaltsbibliotheken für den VM-Dienst.Tanzu Kubernetes Grid-Inhaltsbibliotheken müssen über die Tanzu Kubernetes Grid-Karte verwaltet werden.

Voraussetzungen

Erforderliche Rechte:

- **Namespaces.Clusterweite Konfiguration ändern**
- **Namespaces.Namespace-Konfiguration ändern**

Verfahren

1 Wechseln Sie in vSphere Client zum Namespace.
   a Wählen Sie im vSphere Client-Startmenü die Option **Arbeitslastverwaltung** aus.
   b Klicken Sie auf die Registerkarte **Namespaces** und klicken Sie dann auf den Namespace.
2 Fügen Sie eine Inhaltsbibliothek hinzu oder entfernen Sie sie.
   a Klicken Sie in der Karte **VM-Dienst** auf **Inhaltsbibliothek verwalten**.
   b Führen Sie einen der folgenden Vorgänge aus.

Option	Bezeichnung
Entfernen einer Inhaltsbibliothek	Heben Sie die Auswahl der Inhaltsbibliothek auf und klicken Sie auf **OK**.
Hinzufügen einer Inhaltsbibliothek	Wählen Sie eine oder mehrere Inhaltsbibliotheken aus und klicken Sie auf **OK**.

Nächste Schritte

OVF-Vorlagen aus der Bibliothek werden im Kubernetes-Namespace als VM-Images verfügbar und können von DevOps zur Eigenwartung von VMs verwendet werden. Weitere Informationen finden Sie unter Bereitstellen einer virtuellen Maschine in vSphere IaaS control plane.

Hinweis Es werden nur OVF-Vorlagen aus der Bibliothek in den Namespaces angezeigt. Andere Inhaltstypen werden im Namespace nicht angezeigt.

Hinzufügen einer VM-Inhaltsbibliothek zu einem Namespace mithilfe der Datencenter-CLI

Als vSphere-Administrator können Sie den Data Center CLI (DCLI)-Befehl verwenden, um die Inhaltsbibliothek einem Namespace zuzuweisen. Beim Zuweisen der Bibliothek können Sie die dem Namespace zugeordnete Bibliothek beschreibbar machen. Wenn die Bibliothek beschreibbar ist, können DevOps-Benutzer neben der Anzeige der Bibliothek und der Images in der Bibliothek auch neue VM-Images darin veröffentlichen.

Mit den DCLI-Befehlen können Sie dem Namespace jeden beliebigen Bibliothekstyp hinzufügen, einschließlich lokaler, veröffentlichter und abonnierter Bibliothekstypen. Es können jedoch nur lokale und veröffentlichte Bibliotheken als beschreibbare Bibliotheken verknüpft werden. Inhaltsbibliotheken und Bibliothekselemente sind nur im zugeordneten Namespace verfügbar.

Verfahren

1. Melden Sie sich bei vCenter Server mit dem Root-Benutzerkonto an.
2. Geben Sie `dcli +i` ein, um DCLI im interaktiven Modus zu verwenden.
3. Rufen Sie die ID der Inhaltsbibliothek ab, die dem Namespace zugeordnet werden soll.

   ```
   dcli > namespacemanagement content library list
   ```
4. Führen Sie den folgenden Befehl aus, um die Inhaltsbibliothek dem Namespace zuzuweisen.

   Der Aktualisierungsvorgang erfolgt nicht inkrementell. Nur die in der Liste angegebenen Bibliotheken werden dem Namespace zugeordnet und die zuvor hinzugefügten Bibliotheken werden entfernt, es sei denn, ihre IDs sind angegeben. Wenn Sie beispielsweise `'[{"content_library": "CLA", "writable": "true"}]'` aktualisieren und später `'[{"content_library": "CLB", "writable": "true"}]'` aktualisieren, wird CLA entfernt und nur CLB wird hinzugefügt. Wenn CLA und CLB zugeordnet werden sollen, müssen Sie beide Bibliotheken angeben: `'[{"content_library": "CLA", "writable": "true"}, {"content_library": "CLB", "writable": "true"}]'`.

   ```
   dcli > namespaces instances update --namespace namespace_name --content-libraries
   '[{"content_library": "content_library_ID", "writable": "true | false"}]'
   ```

   Verwenden Sie die folgenden Argumente:

   - `--namespace` *`namespace_name`* – Name des Namespace.

- `--content_libraries` *`content_library_ID`* `writable: true | false` – ID der Inhaltsbibliothek, die dem Namespace zugeordnet werden soll, und ob die Bibliothek beschreibbar ist oder nicht.

Beispiel:

```
dcli > namespaces instances update --namespace lb-edit-ns --content-libraries
'[{"content_library": "cl-b585915ddxxxxxxxx", "writable": "true"}]'
```

5 Um die Inhaltsbibliothek aus dem Namespace zu löschen, wiederholen Sie den Befehl `namespaces instances update` und entfernen Sie den Eintrag der Inhaltsbibliothek aus der Array-Liste.

Beispiel:

```
dcli > namespaces instances update --namespace lb-edit-ns --content-libraries '[]'
```

Ergebnisse

Die hinzugefügte Inhaltsbibliothek wird in der DevOps-Namespace-Ansicht verfügbar.

Der DevOps-Benutzer kann die folgenden Befehle ausführen, um sicherzustellen, dass die Inhaltsbibliothek hinzugefügt oder gelöscht wurde.

```
kubectl get cl -n lb-edit-ns
   NAMESPACE    NAME                   VSPHERENAME   TYPE    WRITABLE   STORAGETYPE   AGE
   lb-edit-ns   cl-b585915ddxxxxxxxx   Test-ns-cl    Local   true       Datastore     3m9s
kubectl describe cl cl-b585915ddxxxxxxxx -n lb-edit-ns
kubectl get clitem -n lb-edit-ns
```

Hinzufügen einer VM-Inhaltsbibliothek zu Supervisor mithilfe der Datencenter-CLI

Zusätzlich zur Zuweisung der Inhaltsbibliothek auf Namespace-Ebene kann der vSphere Administrator den Datencenter-CLI (DCLI)-Befehl verwenden, um die Bibliothek einem Supervisor-Cluster zuzuordnen. Die Inhaltsbibliothek steht allen Namespaces in Supervisor zur Verfügung.

Sie können alle Typen von Bibliotheken zuordnen, einschließlich lokaler, veröffentlichter und abonnierter Bibliotheken.

Hinweis Die dem Supervisor zugewiesene Inhaltsbibliothek ist schreibgeschützt. Die DevOps-Benutzer können nur aus dieser Inhaltsbibliothek auf VM-Images zugreifen, aber keine VM-Images in dieser Bibliothek veröffentlichen.

Voraussetzungen

Weitere Informationen zu den DCLI-Befehlen finden Sie unter VMware-Datencenter-CLI.

Verfahren

1 Melden Sie sich bei vCenter Server mit dem Root-Benutzerkonto an.

2 Geben Sie `dcli +i` ein, um DCLI im interaktiven Modus zu verwenden.

3 Rufen Sie den Supervisor-Namen und die ID der Inhaltsbibliothek ab, um eine Verbindung mit dem Supervisor herzustellen.

   a Rufen Sie den Supervisor-Namen aus der Cluster-Liste ab.

   Der Befehl listet alle Cluster auf, die in vCenter Server verfügbar sind.

   ```
   dcli > namespacemanagement clusters list
   ```

   b Listet die IDs aller Inhaltsbibliotheken jeglicher Art auf, die in vCenter Server verfügbar sind.

   ```
   dcli > library list
   ```

   c Überprüfen Sie die Details für die jeweilige Bibliothek.

   ```
   dcli > library get --library-id content_library_ID
   ```

4 Ordnen Sie dem Supervisor eine oder mehrere Inhaltsbibliotheken zu.

   Der Aktualisierungsvorgang erfolgt nicht inkrementell. Nur die in der Liste angegebenen Bibliotheken werden dem Namespace zugeordnet und die zuvor hinzugefügten Bibliotheken werden entfernt, es sei denn, ihre IDs sind angegeben. Wenn Sie beispielsweise `'[{"content_library": "CLA", "writable": "true"}]'` aktualisieren und später `'[{"content_library": "CLB", "writable": "true"}]'` aktualisieren, wird CLA entfernt und nur CLB wird hinzugefügt. Wenn CLA und CLB zugeordnet werden sollen, müssen Sie beide Bibliotheken angeben: `'[{"content_library": "CLA", "writable": "true"}, {"content_library": "CLB", "writable": "true"}]'`.

   ```
   dcli > namespacemanagement clusters update --cluster cluster_name --content-libraries
   '[{"content_library": content_library_ID_1}, {"content-library": content_library_ID_2}]'
   ```

   Verwenden Sie die folgenden Argumente:

   - `--cluster cluster_name` – Bezeichner für den Supervisor-Cluster.
   - `--content-libraries content_library_ID` – Eine ID einer Inhaltsbibliothek, die dem Supervisor zugeordnet werden soll. Sie können mehrere IDs auflisten.

     Beispiel:

     ```
     dcli > namespacemanagement clusters update --cluster cluster_name --content-libraries
     '[{"content_library": 535d4b3d-xxxx-xxxx-xxxx-xxxxxxxxxxxx}, {"content-library":
     b5aa7f68-xxxx-xxxx-xxxx-xxxxxxxxxxxx}]'
     ```

5 Stellen Sie sicher, dass die Inhaltsbibliotheken mit dem Cluster verbunden sind.

   ```
   dcli > namespacemanagement clusters get --cluster cluster_name
   ```

   Die Ausgabe muss die IDs der verbundenen Inhaltsbibliotheken enthalten.

6 Um die zugeordnete Inhaltsbibliothek aus dem Cluster zu löschen, wiederholen Sie den Befehl `namespacemanagement clusters update` und entfernen Sie so den Eintrag der Inhaltsbibliothek aus der Array-Liste für die Inhaltsbibliothek.

   Beispiel:

```
dcli > namespacemanagement clusters update --cluster cluster_name --content-libraries '[]'
```

Ergebnisse

Die neu hinzugefügten Inhaltsbibliotheken werden in der DevOps-Clusteransicht verfügbar. Alle Änderungen, die der vSphere Administrator an den Inhaltsbibliotheken vornimmt, werden in der DevOps-Ansicht wiedergegeben. Der DevOps-Benutzer kann die folgenden Befehle ausführen, um die Inhaltsbibliotheken aufzulisten und deren Inhalt zu beschreiben:

- `kubectl get ccl` – Liste aller auf Clusterebene verfügbaren Inhaltsbibliotheken. Die Ausgabe kann der folgenden ähneln.

```
NAME                    VSPHERENAME                          TYPE         STORAGETYPE   AGE
cl-f28af8153fb849bd7    Kubernetes Service Content Library   Subscribed   Datastore     6d5h
cl-knounwp7xxxxxxxxx    Image Registry Content Library       Local        Datastore     6d4h
```

- `kubectl get cclitem` – Liste aller Elemente in den Inhaltsbibliotheken auf Clusterebene.
- `kubectl describe ccl NAME` – Detaillierte Informationen für eine bestimmte Inhaltsbibliothek auf Clusterebene.

Verwalten und Veröffentlichen von Inhaltsbibliotheks-Images in vSphere IaaS control plane

Nachdem ein vSphere-Administrator einem Namespace oder Cluster Inhaltsbibliotheken zugewiesen hat, können DevOps-Benutzer auf die Bibliothek zugreifen und ihre Elemente zum Bereitstellen von VMs aus VM-Images in der Bibliothek verwenden. Wenn die dem Namespace zugewiesene Bibliothek beschreibbar ist, können DevOps-Benutzer mit Bearbeitungsberechtigungen auch die Bibliothekselemente verwalten und neue VM-Images veröffentlichen.

Hinweis Es gibt keine Einschränkungen für die von Ihnen verwendeten VM-Images. Wenn Sie einsatzbereite OVA-Images testen möchten, können Sie sie von der Seite Empfohlene Images herunterladen. Beachten Sie, dass diese Images nur für die POC-Verwendung vorgesehen sind. Erstellen Sie in der Produktionsumgebung Images mit den neuesten Patches und erforderlichen Sicherheitseinstellungen, die den Unternehmenssicherheitsrichtlinien folgen.

Voraussetzungen

Stellen Sie als DevOps-Benutzer sicher, dass sie die folgenden Anforderungen erfüllen:

- Sie verfügen über `Edit`-Berechtigungen für den vSphere Namespace.

- Der vSphere-Administrator hat dem Namespace eine beschreibbare Inhaltsbibliothek zugewiesen. Weitere Informationen hierzu finden Sie unter Hinzufügen einer VM-Inhaltsbibliothek zu Supervisor mithilfe der Datencenter-CLI .
- Die Inhaltsbibliothek ist lokal oder veröffentlicht. abonnierte Bibliotheken können nicht bearbeitet werden.

Verfahren

1 Verwalten Sie die Bibliothekselemente.

a Stellen Sie sicher, dass die Inhaltsbibliotheken im Namespace verfügbar sind.

Hinweis Wenn Sie Bibliothekselemente in der Bibliothek verwalten oder VM-Images in der Bibliothek veröffentlichen möchten, stellen Sie sicher, dass ihr beschreibbarer Status "true" lautet.

```
kubectl get cl -n <namespace-name>
   NAME                   VSPHERENAME   TYPE    WRITABLE   STORAGETYPE   AGE
   cl-b585915ddxxxxxxxx   Test-ns-cl-1  Local   true       Datastore     3m9s
   cl-535d4b3dnxxxyyyyy   Test-ns-cl-1  Local   false      Datastore     3m9s
```

b Überprüfen Sie die Inhalte der Bibliothek.

```
kubectl get clitem -n <namespace-name>
 NAME                 VSPHERENAME     CONTENTLIBRAYREF         TYPE   READY   AGE
 clitem-d2wnmq.....   item 1          cl-b585915ddxxxxxxxx     Ovf    True    26c
 clitem-55088d.....   item 2          cl-b585915ddxxxxxxxx     Ovf    True    26c
 clitem-xyzxyz.....   xyzxyz          cl-535d4b3dnxxxyyyyy     Ovf    True    26c
```

c Löschen Sie ein Image aus der Inhaltsbibliothek.

Hinweis Sie können ein Element nur aus der Bibliothek löschen, die beschreibbar ist und wenn Sie über `Edit`-Berechtigungen oder Berechtigungen einer höheren Ebene verfügen.

Nachdem Sie das clitem gelöscht haben, wird auch die entsprechende vmi-Ressource gelöscht.

```
kubectl delete clitem clitem-55088d.....
 NAME                 VSPHERENAME     CONTENTLIBRAYREF         TYPE   READY   AGE
 clitem-d2wnmq.....   item 1          cl-b585915ddxxxxxxxx     Ovf    True    26c
 clitem-xyzxyz.....   xyzxyz          cl-535d4b3dnxxxyyyyy     Ovf    True    26c
```

d Rufen Sie Image-Details ab.

```
kubectl get vmi -n <namespace-name>
 NAME              PROVIDER-NAME      CONTENT-LIBRAY-NAME    IMAGE-NAME VERSION   OS-
TYPE        FORMAT   AGE
 vmi-d2wnmq.....   clitem-d2wnmq..... cl-b585915ddxxxxxxxx   item 1
ubuntu64guest  ovf      26c
 vmi-55088d.....   clitem-55088d..... cl-b585915ddxxxxxxxx   item 2
otherguest     ovf      26c
```

2 Veröffentlichen Sie ein Image in der Inhaltsbibliothek.

a Erstellen Sie eine YAML-Datei, um eine Quell-VM bereitzustellen.

Stellen Sie sicher, dass imageName in der VirtualMachine-Spezifikation auf eines der VM-Images aus der Inhaltsbibliothek verweist.

Beispiel: `source-vm.yaml`.

```
apiVersion: vmoperator.vmware.com/v1alpha2
kind: VirtualMachine
metadata:
  name: source-vm
  namespace: test-publish-ns
spec:
  className: best-effort-small
  storageClass: wcpglobal-storage-profile
  imageName: vmi-d2wnmq.....
  powerState: poweredOn
  vmMetadata:
    transport: CloudInit
```

b Rufen Sie Informationen über die bereitgestellte VM ab und stellen Sie eine Verbindung zur VM her, um sicherzustellen, dass sie ausgeführt wird.

Sie erhalten eine Ausgabe ähnlich der Folgenden:

```
kubectl get vm -n <namespace-name>
NAME        POWER-STATE   CLASS             IMAGE           PRIMARY-IP        AGE
source-vm   poweredOn     best-effort-small vmi-d2wnmq..... 192.168.000.00   9m32s
```

c Erstellen Sie eine Veröffentlichungsanforderung für ein neues Ziel-Image.

Beispielsweise `vmpub.yaml`. Geben Sie in der Anforderung den Namen der Quell-VM und der Zielinhaltsbibliothek an, in der Sie Ihr Image veröffentlichen möchten. Stellen Sie sicher, dass die Bibliothek beschreibbar ist.

```
apiVersion: vmoperator.vmware.com/v1alpha2
kind: VirtualMachinePublishRequest
metadata:
  name: vmpub-1
  namespace: test-publish-ns
spec:
  source:
    apiVersion: vmoperator.vmware.com/v1alpha2
    kind: VirtualMachine
    name: source-vm # If empty, the name of this VirtualMachinePublishRequest will be
used as the source VM name ("vmpub-1" in this example).
  target:
    item:
      name: publish-image-1 # If empty, the target item name is <source-vm-name>-image
by default
    location:
      apiVersion: imageregistry.vmware.com/v1alpha2
      kind: ContentLibrary
      name: cl-b585915ddxxxxxxxx
```

d Beschreiben Sie die Veröffentlichungsanforderung.

Stellen Sie sicher, dass die Veröffentlichungsanforderung in einem `Ready`-Status befindet, wobei `ImageName` festgelegt ist.

```
kubectl describe vmpub vmpub-1 -n <namespace-name>
==================
Status:
  imageName: vmi-12980cddd...
  ready: true
==================
```

e Stellen Sie sicher, dass das neue Image zur Inhaltsbibliothek hinzugefügt wird, nachdem die Veröffentlichungsanforderung abgeschlossen ist.

```
kubectl get vmi
 NAME              PROVIDER-NAME      CONTENT-LIBRAY-NAME    IMAGE-NAME      VERSION
OS-TYPE        FORMAT   AGE
 vmi-12980cddd..   clitem-12980cddd.. cl-b585915ddxxxxxxxx   publish-image-1
ubuntu64guest  ovf      7m12s
 vmi-d2wnmq.....   clitem-d2wnmq..... cl-b585915ddxxxxxxxx   item 1
ubuntu64guest  ovf      26m
 vmi-55088d.....   clitem-55088d..... cl-b585915ddxxxxxxxx   item 2
otherguest     ovf      26m
```

Sie können dieses neue Image verwenden, um eine neue VM bereitzustellen.

Arbeiten mit VM-Klassen in vSphere IaaS control plane

Für die Selbstverwaltung von VMs in vSphere IaaS control plane müssen DevOps-Benutzer Zugriff auf VM-Klassen haben. Eine VM-Klasse ist eine Vorlage, die CPU, Speicher und Reservierungen für VMs definiert. Mit einer VM-Klasse können Leitlinien für die Richtlinie und die Governance von VMs durch das Vorwegnehmen von Entwicklungsanforderungen und Berücksichtigen von Ressourcenverfügbarkeit und -einschränkungen festgelegt werden.

vSphere IaaS control plane bietet mehrere Standard-VM-Klassen. Ein vSphere-Administrator kann sie in der aktuellen Form verwenden oder benutzerdefinierte VM-Klassen erstellen. Um den DevOps-Benutzern die Klassen zur Verfügung zu stellen, fügt der vSphere-Administrator sie einem Namespace hinzu. Die dem Namespace zugewiesenen VM-Klassen können von eigenständigen VMs und von den VMs verwendet werden, die Tanzu Kubernetes Grid-Cluster bilden.

Erstellen einer benutzerdefinierten VM-Klasse mit dem vSphere Client

Als vSphere-Administrator können Sie verfügbare Standardklassen verwenden. Sie können auch benutzerdefinierte VM-Klassen anstelle der Standardklasse erstellen und sie für die VM-Bereitstellung in einem Namespace verwenden.

Wenn Sie neue Klassen erstellen, sollten Sie die folgenden Aspekte berücksichtigen.

- VM-Klassen, die Sie in einer vCenter Server-Instanz erstellen, stehen allen vCenter Server-Clustern und allen Namespaces in diesen Clustern zur Verfügung.
- VM-Klassen stehen allen Namespaces im vCenter Server zur Verfügung. DevOps-Ingenieure können jedoch nur die VM-Klassen verwenden, die Sie einem bestimmten Namespace zuordnen.

Hinweis Sie können auch VM-Klassen mithilfe des DCLI-Befehls erstellen. Weitere Informationen hierzu finden Sie unter Erstellen und Verwalten von VM-Klassen mithilfe der Datencenter-CLI.

Voraussetzungen

Erforderliche Rechte:

- **Namespaces.Clusterweite Konfiguration ändern**
- **Namespaces.Namespace-Konfiguration ändern**
- **VM-Klassen.VM-Klassen verwalten**

Verfahren

1 Navigieren Sie zur Seite **VM-Dienst**.

   a Wählen Sie im vSphere Client-Startmenü die Option **Arbeitslastverwaltung** aus.

   b Klicken Sie auf die Registerkarte **Dienste** und klicken Sie dann im Bereich **VM-Dienst** auf **Verwalten**.

2 Klicken Sie auf der Seite **VM-Dienst** auf **VM-Klassen** und dann auf **VM-Klasse erstellen**.

3 Geben Sie auf der Seite **Name** den VM-Klassennamen an und klicken Sie auf **Weiter**.

Der Name der VM-Klasse bezeichnet die VM-Klasse. Geben Sie einen eindeutigen DNS-konformen Namen ein, der diesen Anforderungen entspricht:

- Verwenden Sie einen eindeutigen Namen, der die Namen der standardmäßigen oder benutzerdefinierten VM-Klassen in Ihrer Umgebung nicht dupliziert.
- Verwenden Sie eine alphanumerische Zeichenfolge mit einer maximalen Länge von 63 Zeichen.
- Verwenden Sie keine Großbuchstaben oder Leerzeichen.
- Verwenden Sie einen Bindestrich an einer beliebigen Stelle außer als erstes oder letztes Zeichen. Beispiel: `vm-class1`.

Nachdem Sie die VM-Klasse erstellt haben, können Sie ihren Namen nicht mehr ändern.

4 Wählen Sie auf der Seite **Kompatibilität** die Hardwarekompatibilität der VM-Klasse aus und klicken Sie auf **Weiter**.

Weitere Informationen finden Sie unter Virtuelle Maschinenkompatibilität.

Hinweis Sie können die Hardware-Kompatibilität einer VM-Klasse nur während der Erstellung festlegen und später nicht mehr ändern.

5 Behalten Sie auf der Seite **Konfiguration** die Standardwerte bei.

6 Überprüfen Sie auf der Seite **Überprüfen und bestätigen** die Details und klicken Sie auf **Beenden**.

Nächste Schritte

Bearbeiten Sie die VM-Klassenkonfiguration, z. B. VM-Hardware und VM-Optionen.

Bearbeiten einer VM-Klasse mithilfe des vSphere Client

Erfahren Sie, wie Sie eine VM-Klasse nach ihrer Erstellung bearbeiten können. Sie können Hardwareressourcen wie CPU, Arbeitsspeicher und Geräte konfigurieren und VM-Optionen und erweiterte Parameter bearbeiten. Sie können auch Standard-VM-Klassen bearbeiten, die von vSphere IaaS control plane angeboten werden.

Das Bearbeiten einer VM-Klasse führt nicht zur automatischen Neukonfiguration der VMs, die zuvor über diese Klasse bereitgestellt wurden. Wenn beispielsweise ein DevOps-Benutzer einen Tanzu Kubernetes Grid-Cluster mit der VM-Klasse erstellt hat und Sie später die VM-Klassendefinition ändern, bleiben vorhandene Tanzu Kubernetes Grid-VMs davon unberührt. Neue Tanzu Kubernetes Grid-VMs verwenden die geänderte Klassendefinition.

Vorsicht Wenn Sie einen Tanzu Kubernetes Grid-Cluster nach der Bearbeitung einer von diesem Cluster verwendeten VM-Klasse skalieren, verwenden neue Clusterknoten die aktualisierte Klassendefinition, aber vorhandene Clusterknoten verwenden weiterhin die anfängliche Klassendefinition, was zu einer Nichtübereinstimmung führt. Sowohl Steuerungsebenen- als auch Worker-Knoten können skaliert werden. Informationen zur Skalierung finden Sie in *Verwenden des TKG-Dienstes mit der vSphere IaaS-Steuerungsebene* unter Skalieren eines Arbeitslastclusters.

Wenn Sie eine VM-Klasse löschen, wird sie aus allen zugeordneten Namespaces entfernt. DevOps-Benutzer können keine Self-Service-VMs mehr verwenden, die diese VM-Klasse verwenden. VMs, die bereits mit dieser VM-Klasse erstellt wurden, sind davon nicht betroffen.

Voraussetzungen

Erforderliche Rechte:

- **Namespaces.Clusterweite Konfiguration ändern**
- **Namespaces.Namespace-Konfiguration ändern**
- **VM-Klassen.VM-Klassen verwalten**

Verfahren

1. Zeigen Sie im vSphere Client die verfügbaren VM-Klassen an.
   a. Wählen Sie im vSphere Client-Startmenü die Option **Arbeitslastverwaltung** aus.
   b. Klicken Sie auf die Registerkarte **Dienste** und klicken Sie dann auf den Bereich **VM-Dienst**.
   c. Klicken Sie auf der Seite **VM-Dienst** auf **VM-Klassen**.

      Alle standardmäßigen oder vom Benutzer erstellten VM-Klassen werden unter **Verfügbare VM-Klassen angezeigt**.
2. Klicken Sie im Bereich der ausgewählten VM-Klasse auf **Verwalten** und dann auf **Bearbeiten**.

3 Konfigurieren Sie auf der Seite **Virtuelle Hardware** die Hardwareressourcen der VM-Klasse, z. B. Arbeitsspeicher, CPU und verschiedenandere Geräte.

Alle VM-Hardwareeinstellungen werden angewendet, wenn ein DevOps-Benutzer die VM-Klasse einer VM zuweist. So werden beispielsweise die CPU-Konfigurationswerte zu den CPU-Ressourcen, die allen VMs zugewiesen werden, die der Benutzer von DevOps mit Hilfe der VM-Klasse erstellt.

Hinweis Ab vSphere 8.0 Update 2b stellt der Assistent zum Erstellen und Bearbeiten von VM-Klassen beim Festlegen von CPU- und Arbeitsspeicherressourcen von Prozentwerten auf numerische Werte in MB, GB, TB und MHz um. Für alle zuvor erstellten VM-Klassen sehen Sie die CPU- und den Arbeitsspeicherbelegung in Prozenten, aber jetzt können Sie diese Werte in den neuen numerischen Formaten bearbeiten.

VM-Konfigurationsoption	Beschreibung
CPU	Festlegen der CPU-Ressourcen, die für die VM reserviert sind. Weitere Informationen zum Konfigurieren von CPU-Ressourcen finden Sie unter Konfiguration und Beschränkungen der virtuellen CPU und Konfigurieren der CPU-Ressourcen einer virtuellen Maschine.
Arbeitsspeicher	Definiert den für eine VM konfigurierten Arbeitsspeicher in MB, GB oder TB. Weitere Informationen zu VM-Arbeitsspeicherressourcen finden Sie unter Konfiguration des virtuellen Arbeitsspeichers.
Grafikkarte	Konfigurieren Sie 3D-Grafiken, um Windows AERO, CAD, Google Earth und andere 3D-Design-, Modellierungs- und Multimedia-Anwendungen zu nutzen. Weitere Informationen zur Grafikkarteneinstellung finden Sie unter Wie kann ich 3D-Grafiken konfigurieren.
Sicherheitsgeräte	Gewährleisten Sie zusätzliche Sicherheit für die VM-Klasse, indem Sie Software Guard Extensions® (vSGX) konfigurieren. Weitere Informationen finden Sie unter Sichern von virtuellen Maschinen mit Intel Software Guard-Erweiterungen.

4 Klicken Sie in der Option **Virtuelle Hardware** auf **Neues Gerät hinzufügen**, um Geräte zur VM-Klasse hinzuzufügen und zu konfigurieren.

Sie konfigurieren unterschiedliche Geräte für die VM-Klasse, z. B. Speichercontroller, Netzwerkadapter, USB- und PCI-Geräte.

VM-Konfigurationsoption	Beschreibung
RDM-Festplatte	Fügen Sie ein Raw Device Mapping (RDM) hinzu, um die Daten einer virtuellen Maschine direkt auf einer SAN LUN zu speichern anstatt in einer virtuellen Festplattendatei. Weitere Informationen finden Sie unter Hinzufügen einer RDM-Festplatte zu einer virtuellen Maschine.
Host-USB-Gerät	Fügen Sie ein oder mehrere USB-Passthrough-Geräte von einem ESXi-Host zu einer virtuellen Maschine hinzu, wenn die physischen Geräte mit dem Host verbunden sind, auf dem die virtuelle Maschine läuft. Weitere Informationen finden Sie unter Hinzufügen von USB-Geräten eines ESXi-Hosts zu einer virtuellen Maschine.
NVDIMM	Konfigurieren Sie ein virtuelles NVDIMM-Gerät für die VM-Klasse, damit diese den nichtflüchtigen (oder dauerhaften) Computerspeicher verwenden kann. Weitere Informationen finden Sie unter Hinzufügen eines NVDIMM-Geräts zu einer virtuellen Maschine.
CD-/DVD-Laufwerk	Konfigurieren eines CD/DVD-Geräts für die VM-Klasse. Weitere Informationen finden Sie unter Vorgehensweise zum Hinzufügen oder Ändern eines CD- oder DVD-Laufwerks einer virtuellen Maschine.
NVMe -Controller, **SATA -Controller**, **SCSI -Controller**	Konfigurieren von Speichercontrollern für die VM-Klasse. Weitere Informationen finden Sie unter Bedingungen, Einschränkungen und Kompatibilität von SCSI-, SATA- und NVMe-Speichercontrollern.
USB-Controller	Fügen Sie der VM-Klasse einen USB-Controller hinzu, um USB-Passthrough von einem ESXi-Host oder von einem Clientcomputer zu unterstützen. Weitere Informationen finden Sie unter Hinzufügen eines USB-Controllers zu einer virtuellen Maschine.
PCI-Gerät	Konfigurieren Sie VMs für die Verwendung der NVIDIA GRID vGPU-Technologie (virtual GPU), wenn die ESXi-Hosts in Ihrer vSphere IaaS control plane-Umgebung über ein oder mehrere NVIDIA GRID-GPU-Grafikgeräte verfügen. Sie können auch andere PCI-Geräte auf einem ESXi-Host konfigurieren, um sie einer VM im Passthrough-Modus zur Verfügung zu stellen. Wenn Sie diese Option auswählen, ändert sich der Wert für die Reservierung von Arbeitsspeicherressourcen automatisch in 100 %. Weitere Informationen und zusätzliche Anforderungen finden Sie unter Bereitstellen einer VM mit PCI-Geräten in vSphere IaaS control plane.
Watchdog-Timer	Fügen Sie einen virtuellen Watchdog-Timer (VWDT) hinzu, um die Selbstständigkeit in Bezug auf die Systemleistung innerhalb einer virtuellen Maschine sicherzustellen. Weitere Informationen finden Sie unter Vorgehensweise zum Hinzufügen eines virtuellen Watchdog- Timergeräts zu einer virtuellen Maschine.

VM-Konfigurationsoption	Beschreibung
Präzisionsuhr	Fügen Sie der VM eine Präzisionsuhr hinzu. Eine Präzisionsuhr ist eine virtuelle Uhr, die eine virtuelle Maschine mit Zugriff auf die Systemzeit des primären ESXi-Hosts bereitstellt. Weitere Informationen finden Sie unter Vorgehensweise zum Hinzufügen einer Präzisionsuhr zu einer virtuellen Maschine.
Serieller Port	Konfigurieren einer Verbindung des virtuellen seriellen Ports mit einem physischen seriellen Port oder einer Datei auf dem Hostcomputer. Weitere Informationen finden Sie unter Ändern der Konfiguration des seriellen Ports..
Instanzspeicher	Konfigurieren des Instanzspeichers für die VM. Zusammen mit dauerhaften Speichervolumes kann eine VM Instanzspeicher verwenden. Im Gegensatz zu dauerhaften Volumes, die getrennt von der VM vorhanden sind, hängen Instanzspeicher-Volumes vom Lebenszyklus einer VM-Instanz ab. Mithilfe der Option **Instanzspeicher** können Sie geeignete Speicherrichtlinien hinzufügen und Volumes für die Verwendung mit der VM konfigurieren. Informationen zu weiteren Anforderungen finden Sie unter Bereitstellen einer VM mit Instanzspeicher in vSphere IaaS control plane.
Netzwerkadapter	Konfigurieren eines Netzwerkadapters für die VM-Klasse. Wenn der DevOps-Benutzer eine VM mit Hilfe der VM-Klasse bereitstellt, kann er für den Adapter ein Arbeitslastnetzwerk für den Adapter angeben. Das Arbeitslastnetzwerk muss für den vSphere-Namespace konfiguriert werden, auf dem die VM läuft. Weitere Informationen zu den unterstützten Adaptertypen finden Sie unter Netzwerkadaptergrundlagen.

5 Auf der Seite **VM-Optionen** können Sie VM-Optionen festlegen oder ändern, um VMware Tools-Skripte auszuführen, den Zugriff von Benutzern auf die Remote-Konsole zu steuern, das Startverhalten zu konfigurieren und vieles mehr.

Weitere Informationen zu den VM-Optionen, die Sie für die VM-Klasse konfigurieren können, finden Sie unter Optionen für virtuelle Maschinen konfigurieren.

6 Auf der Seite **Erweiterte Parameter** können Sie die VM-Konfigurationsparameter ändern oder hinzufügen, indemwenn Sie die Hilfe eines Mitarbeiters des technischen Supports von VMware in Anspruch nehmen. Außerdem können Sie die Anweisungen in der oder VMware-Dokumentation verwendenSie anweist, um einen Parameter hinzuzufügen oder zu ändern, wenn Sieum ein Problem mit dem System zu beheben möchten.

Weitere Informationen zu den erweiterten VM-Parametern finden Sie unter Erweiterte Dateiparameter der virtuellen Maschine konfigurieren.

7 Sobald Sie mit der Bearbeitung der VM-Klasse fertig sind, überprüfen und bestätigen Sie Ihre Änderungen und klicken Sie auf **Beenden**.

Zuordnen einer VM-Klasse zu einem Namespace mit dem vSphere Client

Fügen Sie als vSphere-Administrator eine Standard- oder benutzerdefinierte VM-Klasse zu einem oder mehreren Namespaces auf einem Supervisor hinzu. Wenn Sie einem Namespace eine VM-Klasse hinzufügen, stellen Sie die Klasse den DevOps-Benutzern zur Verfügung, damit sie Self-Service-VMs in der Kubernetes-Namespace-Umgebung starten können. Die VM-Klassen, die Sie dem Namespace zuweisen, werden auch von den VMs verwendet, die Tanzu Kubernetes Grid bilden.

Sie können einem einzelnen Namespace mehrere VM-Klassen hinzufügen. Verschiedene VM-Klassen dienen als Indikatoren für verschiedene Dienstebenen. Wenn Sie mehrere VM-Klassen veröffentlichen, können DevOps-Anwender beim Erstellen und Verwalten von virtuellen Maschinen im Namensraum eine Auswahl zwischen allen benutzerdefinierten und Standardklassen treffen.

Hinweis DevOps-Ingenieure benötigen Zugriff auf VM-Klassen, um einen Tanzu Kubernetes Grid-Cluster in einem neu erstellten Namespace bereitstellen zu können. Als vSphere-Administrator müssen Sie standardmäßige oder benutzerdefinierte VM-Klassen explizit jedem neuen Namespace zuordnen, in dem der Tanzu Kubernetes Grid-Cluster bereitgestellt wird.

Voraussetzungen

Erforderliche Rechte:

- **Namespaces.Clusterweite Konfiguration ändern**
- **Namespaces.Namespace-Konfiguration ändern**
- **VM-Klassen.VM-Klassen verwalten**

Verfahren

1. Wechseln Sie in vSphere Client zum Namespace.
   a. Wählen Sie im vSphere Client-Startmenü die Option **Arbeitslastverwaltung** aus.
   b. Klicken Sie auf die Registerkarte **Namespaces** und klicken Sie dann auf den Namespace.
2. Fügen Sie eine VM-Klasse hinzu.
   a. Klicken Sie im Bereich **VM-Dienst** auf **VM-Klasse hinzufügen**.
   b. Wählen Sie eine oder mehrere VM-Klassen aus und klicken Sie auf **OK**.

Ergebnisse

Die hinzugefügten VM-Klassen stehen im Namespace für die DevOps für Self-Service-VMs zur Verfügung. Diese Klassen können auch von den VMs, die Tanzu Kubernetes Grid-Cluster bilden, verwendet werden.

Verwalten von VM-Klassen in einem Namespace mithilfe des vSphere Client

Nachdem Sie eine VM-Klasse mit einem Namespace verbunden haben, können Sie weitere VM-Klassen hinzufügen oder die Klasse entfernen, um ihre Veröffentlichung im Kubernetes-Namespace rückgängig zu machen.

Voraussetzungen

- Wenn Sie eine VM-Klasse aus einem Namespace entfernen möchten, stellen Sie sicher, dass sie nicht vom Tanzu Kubernetes Grid verwendet wird. Das Entfernen kann sich auf Tanzu Kubernetes Grid-Vorgänge auswirken.
- Erforderliche Rechte:
  - **Namespaces.Clusterweite Konfiguration ändern**
  - **Namespaces.Namespace-Konfiguration ändern**
  - **VM-Klassen.VM-Klassen verwalten**

Verfahren

1. Wechseln Sie in vSphere Client zum Namespace.
   a. Wählen Sie im vSphere Client-Startmenü die Option **Arbeitslastverwaltung** aus.
   b. Klicken Sie auf die Registerkarte **Namespaces** und klicken Sie dann auf den Namespace.
2. Fügen Sie eine VM-Klasse hinzu oder entfernen Sie sie.
   a. Klicken Sie im Bereich **VM** auf **VM-Klasse verwalten**.
   b. Führen Sie einen der folgenden Vorgänge aus.

Option	Bezeichnung
Entfernen einer VM-Klasse	Heben Sie die Auswahl der VM-Klasse auf und klicken Sie auf **OK**.
Hinzufügen einer VM-Klasse	Wählen Sie eine oder mehrere VM-Klassen aus und klicken Sie auf **OK**.

Erstellen und Verwalten von VM-Klassen mithilfe der Datencenter-CLI

Zusätzlich zum vSphere Client können Sie die Data Center CLI (DCLI)-Befehle verwenden, um die VM-Klassen zu erstellen und zu verwalten. Die DCLI-Befehle bieten Ihnen mehr Flexibilität und Zugriff auf VM-Konfigurationsoptionen, die im vSphere Client nicht verfügbar sind.

Voraussetzungen

Melden Sie sich bei vCenter Server mit dem Root-Benutzerkonto an und geben Sie `dcli +i` ein, um die DCLI im interaktiven Modus zu verwenden.

Informationen zu DCLI-Befehlen finden Sie unter Übersicht über die Ausführung von DCLI-Befehlen.

Verfügbare DCLI-Befehle

Befehl	Beschreibung
`namespacemanagement virtualmachineclasses create`	Erstellen Sie ein VM-Klassenobjekt.
`namespacemanagement virtualmachineclasses delete`	Löschen Sie das VM-Klassenobjekt.
`namespacemanagement virtualmachineclasses get`	Gibt Informationen zu einer VM-Klasse zurück.
`namespacemanagement virtualmachineclasses list`	Gibt Informationen zu allen VM-Klassen zurück.
`namespacemanagement virtualmachineclasses update`	Aktualisieren Sie die Konfiguration des VM-Klassenobjekts.

Erstellen einer VM-Klasse mithilfe der Datencenter-CLI

Verwenden Sie als vSphere-Administrator den DCLI-Befehl `com vmware vcenter namespacemanagement virtualmachineclasses create`, um eine VM-Klasse zu erstellen. Sie können VM-Eigenschaften wie CPU, Arbeitsspeicher, Arbeitsspeicherreservierungen, Netzwerkadapter usw. konfigurieren.

Der Befehl übernimmt die folgenden Argumente.

Argument	Beschreibung
-h, --help	Die entsprechende Hilfemeldung wird angezeigt und der Vorgang wird beendet.
--config-spec CONFIG_SPEC	Eine VirtualMachineConfigSpec, die der VM-Klasse (JSON-Eingabe) zugeordnet ist.
--cpu-count CPU_COUNT	Erforderlich. Die Anzahl der für die virtuelle Maschine dieser Klasse konfigurierten CPUs (Ganzzahl).
--cpu-reservation CPU_RESERVATION	Der Prozentsatz der insgesamt verfügbaren CPUs, die für eine virtuelle Maschine reserviert sind (Ganzzahl).
--description DESCRIPTION	Beschreibung für die VM-Klasse (Zeichenfolge).
--devices-dynamic-direct-path-io-devices DEVICES_DYNAMIC_DIRECT_PATH_IO_DEVICES	Liste der dynamischen DirectPath I/O-Geräte (JSON-Eingabe).
--devices-vgpu-devices DEVICES_VGPU_DEVICES	Liste der vGPU-Geräte (JSON-Eingabe).
--id ID	Erforderlich. Bezeichner der Klasse der virtuellen Maschine (Zeichenfolge).
--instance-storage-policy INSTANCE_STORAGE_POLICY	Speicherrichtlinie, die dem Instanzspeicher (Zeichenfolge) entspricht.
--instance-storage-volumes INSTANCE_STORAGE_VOLUMES	Liste der Instanzspeichervolumes (JSON-Eingabe).

Argument	Beschreibung
--memory-mb MEMORY_MB	Erforderlich. Die Arbeitsspeichermenge in MB, die für die virtuelle Maschine dieser Klasse konfiguriert ist (Ganzzahl).
--memory-reservation MEMORY_RESERVATION	Der Prozentsatz des verfügbaren Arbeitsspeichers, der für eine virtuelle Maschine dieser Klasse reserviert ist.

Verwenden Sie die folgenden Beispiele, um VM-Klassen mit unterschiedlichen Eigenschaften zu erstellen.

CPU und Arbeitsspeicher

```
com vmware vcenter namespacemanagement virtualmachineclasses create
--id cpu-mem-class --cpu-count 2 --memory-mb 2048 --config-spec
'{"_typeName":"VirtualMachineConfigSpec","numCPUs":2,"memoryMB":2048}'
```

Das Festlegen von `numCPUs` und `memoryMB` in der Konfigurationsspezifikation ist optional. Wenn Sie diese Eigenschaften festlegen möchten, müssen sie dieselben Werte wie die obligatorischen Werte der vAPI-Felder `--cpu-count` und `--memory-mb` aufweisen.

CPU- und Arbeitsspeicherreservierungen

Wenn Sie eine VM-Klasse mithilfe einer Konfigurationsspezifikation mit CPU- und Arbeitsspeicherreservierung erstellen, ist die Arbeitsspeicherreservierung oder der Arbeitsspeichergrenzwert in MB für `memoryAllocation` und MHz für `cpuAllocation` angegeben.

```
com vmware vcenter namespacemanagement
virtualmachineclasses create --id cpu-res-class-1 --config-
spec '{"_typeName":"VirtualMachineConfigSpec","numCPUs":2,"memoryMB":2048,"cpuAllocation":
{"_typeName":"ResourceAllocationInfo","reservation":200,"limit":200},"memoryAllocation":
{"_typeName":"ResourceAllocationInfo","reservation":200,"limit":200}}' --cpu-count 2 --
memory-mb 2048
```

Netzwerkadapter

Mit dem folgenden Befehl wird ein Netzwerkadapter vom Typ E1000 erstellt.

```
com vmware vcenter namespacemanagement virtualmachineclasses
create --id class-w-e1000 --cpu-count 2 --memory-
mb 2048 --config-spec '{"_typeName":"VirtualMachineConfigSpec","deviceChange":
[{"_typeName":"VirtualDeviceConfigSpec","operation":"add","device":
{"_typeName":"VirtualE1000","key":-100}}]}'
```

vGPUs

In diesen Beispielen erstellt der erste Befehl eine VM-Klasse mit einer vGPU mithilfe des Felds `--devices-vgpu-devices`. Der zweite Befehl erstellt eine VM-Klasse mit einer vGPU mithilfe einer Konfigurationsspezifikation.

```
com vmware vcenter namespacemanagement virtualmachineclasses create --id vmclass-1 --devices-
vgpu-devices '[{"profile_name": "mockup-vmiop-8c"}]' --memory-reservation 100 --cpu-count 2 --
memory-mb 4096
```

```
com vmware vcenter namespacemanagement virtualmachineclasses
create --id vmclass-2 --cpu-count 2 --memory-
mb 4096 --config-spec '{"_typeName":"VirtualMachineConfigSpec","deviceChange":
[{"_typeName":"VirtualDeviceConfigSpec","operation":"add","device":
{"_typeName":"VirtualPCIPassthrough","key":20,"backing":
{"_typeName":"VirtualPCIPassthroughVmiopBackingInfo","vgpu":"mockup-vmiop-8c"}}}]}'
--memory-reservation 100
```

Instanzspeicher

Die folgenden Beispiele erstellen VM-Klassen, die Instanzspeicher verwenden, indem sie die Felder `--instance-storage-volumes` und `--instance-storage-policy` nutzen.

```
com vmware vcenter namespacemanagement virtualmachineclasses create --id vmclass-ist-1
--instance-storage-volumes '[{"size":47}]' --instance-storage-policy "e28d4352-1d1e-431b-
b3f7-528bef5838a0" --cpu-count 2 --memory-mb 4096
```

Das ID-Feld ist in diesem Beispiel eine bekannte virtualDisk-ID, die ein Instanzspeichergerät in den VM-Service-VMs darstellt.

```
com vmware vcenter namespacemanagement virtualmachineclasses create --id vmclass-ist-2 --cpu-
count 2 --memory-mb 2048 --config-spec
'{"_typeName":"VirtualMachineConfigSpec","deviceChange":
[{"_typeName":"VirtualDeviceConfigSpec","operation":"add","fileOperation":"create","device":
{"_typeName":"VirtualDisk","key":0,"backing":
{"_typeName":"VirtualDiskFlatVer2BackingInfo","fileName":"","diskMode":"","thinProvisioned":fa
lse},"capacityInKB":0,"capacityInBytes":49283072,"vDiskId":
{"_typeName":"ID","id":"e28d4352-1d1e-431b-b3f7-528bef5838a0"}},"profile":
[{"_typeName":"VirtualMachineDefinedProfileSpec","profileId":"e28d4352-1d1e-431b-
b3f7-528bef5838a0","profileData":
{"_typeName":"VirtualMachineProfileRawData","extensionKey":"com.vmware.vim.sps"}}]}]}'
```

Aktualisieren einer VM-Klasse mithilfe der Datencenter-CLI

Verwenden Sie als vSphere-Administrator den DCLI-Befehl `com vmware vcenter namespacemanagement virtualmachineclasses update`, um eine VM-Klasse zu ändern.

Verwenden Sie die folgenden Beispiele.

Ändern von CPU und Arbeitsspeicher

```
com vmware vcenter namespacemanagement virtualmachineclasses get --vm-class cpu-mem-class
com vmware vcenter namespacemanagement virtualmachineclasses update --vm-class cpu-mem-class
--cpu-count 4 --memory-mb 4096
```

Ändern von CPU- und Arbeitsspeicherreservierungen

Wenn Sie eine VM-Klasse mithilfe einer Konfigurationsspezifikation mit CPU- und Arbeitsspeicherreservierung erstellen, ist die Arbeitsspeicherreservierung oder der Arbeitsspeichergrenzwert in MB für `memoryAllocation` und MHz für `cpuAllocation` angegeben.

```
com vmware vcenter namespacemanagement virtualmachineclasses get --vm-class cpu-res-class-1
com vmware vcenter namespacemanagement virtualmachineclasses update --vm-class cpu-res-
class-1 --cpu-reservation 100 --memory-reservation 100
com vmware vcenter namespacemanagement virtualmachineclasses get --vm-class cpu-res-class-1
```

Sie können die Konfigurationsspezifikation auch verwenden, um die CPU- und Arbeitsspeicherreservierungen zu aktualisieren. Alle vorhandenen CPU- oder Arbeitsspeicherreservierungen werden überschrieben. Beispiel:

```
com vmware vcenter namespacemanagement virtualmachineclasses update --vm-
class  cpu-res-class-1 --config-spec '{"_typeName":"VirtualMachineConfigSpec","cpuAllocation":
{"_typeName":"ResourceAllocationInfo","reservation":200,"limit":200},"memoryAllocation":
{"_typeName":"ResourceAllocationInfo","reservation":200,"limit":200}}'
```

Hinzufügen von vGPUs

```
com vmware vcenter namespacemanagement virtualmachineclasses get --vm-class class-w-e1000
com vmware vcenter namespacemanagement virtualmachineclasses update --vm-class class-w-e1000
--devices-vgpu-devices '[{"profile_name": "mockup-vmiop-8c"}]'
com vmware vcenter namespacemanagement virtualmachineclasses get --vm-class class-w-e1000
```

```
com vmware vcenter namespacemanagement virtualmachineclasses get --vm-class vmclass-1
com vmware vcenter namespacemanagement virtualmachineclasses update --vm-
class vmclass-1 --config-spec '{"_typeName":"VirtualMachineConfigSpec","deviceChange":
[{"_typeName":"VirtualDeviceConfigSpec","operation":"add","device":
{"_typeName":"VirtualPCIPassthrough","key":20,"backing":
{"_typeName":"VirtualPCIPassthroughVmiopBackingInfo","vgpu":"mockup-
vmiop-8c"}}},{"_typeName":"VirtualDeviceConfigSpec","operation":"add","device":
{"_typeName":"VirtualPCIPassthrough","key":20,"backing":
{"_typeName":"VirtualPCIPassthroughVmiopBackingInfo","vgpu":"mockup-vmiop"}}}]}'
com vmware vcenter namespacemanagement virtualmachineclasses get --vm-class vmclass-1
```

Entfernen von vGPU

```
com vmware vcenter namespacemanagement virtualmachineclasses update --vm-class vmclass-1 --
devices-vgpu-devices '[]'
 com vmware vcenter namespacemanagement virtualmachineclasses get --vm-class vmclass-1
```

Hinzufügen des Instanzspeichers

```
com vmware vcenter namespacemanagement virtualmachineclasses update --vm-class vmclass-1
--instance-storage-volumes '[{"size":47}]' --instance-storage-policy "e28d4352-1d1e-431b-
b3f7-528bef5838a0"
 com vmware vcenter namespacemanagement virtualmachineclasses get --vm-class vmclass-1
```

```
com vmware vcenter namespacemanagement virtualmachineclasses get --vm-class vmclass-ist-2
com vmware vcenter namespacemanagement virtualmachineclasses update --vm-class vmclass-ist-2
--instance-storage-volumes '[{"size":51},{"size":50}]' --instance-storage-policy
"e28d4352-1d1e-431b-b3f7-528bef5838a0"
com vmware vcenter namespacemanagement virtualmachineclasses get --vm-class vmclass-ist-2
com vmware vcenter namespacemanagement virtualmachineclasses update --vm-class vmclass-ist-2
--config-spec '{"_typeName":"VirtualMachineConfigSpec","deviceChange":
[{"_typeName":"VirtualDeviceConfigSpec","operation":"add","fileOperation":"create","device":
{"_typeName":"VirtualDisk","key":0,"backing":
{"_typeName":"VirtualDiskFlatVer2BackingInfo","fileName":"","diskMode":"","thinProvisioned":fa
lse},"capacityInKB":0,"capacityInBytes":52428800,"vDiskId":
{"_typeName":"ID","id":"cc737f33-2aa3-4594-aa60-df7d6d4cb984"}},"profile":
[{"_typeName":"VirtualMachineDefinedProfileSpec","profileId":"e28d4352-1d1e-431b-
b3f7-528bef5838a0","profileData":
{"_typeName":"VirtualMachineProfileRawData","extensionKey":"com.vmware.vim.sps"}}]}]}'
com vmware vcenter namespacemanagement virtualmachineclasses get --vm-class vmclass-ist-2
```

Entfernen des Instanzspeichers

```
com vmware vcenter namespacemanagement virtualmachineclasses update --vm-class vmclass-ist-1
--instance-storage-volumes '[]' --instance-storage-policy ""
com vmware vcenter namespacemanagement virtualmachineclasses get --vm-class vmclass-ist-1
```

Hinzufügen von Netzwerkadaptern

Mit diesem Befehl werden sowohl ein Instanzspeicher als auch eine e1000-Netzwerkkarte zur VM-Klasse hinzugefügt.

```
com vmware vcenter namespacemanagement virtualmachineclasses update --vm-class vmclass-ist-2
--config-spec '{"_typeName":"VirtualMachineConfigSpec","deviceChange":
[{"_typeName":"VirtualDeviceConfigSpec","operation":"add","fileOperation":"create","device":
{"_typeName":"VirtualDisk","key":0,"backing":
{"_typeName":"VirtualDiskFlatVer2BackingInfo","fileName":"","diskMode":"","thinProvisioned":fa
lse},"capacityInKB":0,"capacityInBytes":52428800,"vDiskId":
{"_typeName":"ID","id":"cc737f33-2aa3-4594-aa60-df7d6d4cb984"}},"profile":
[{"_typeName":"VirtualMachineDefinedProfileSpec","profileId":"e28d4352-1d1e-431b-
b3f7-528bef5838a0","profileData":
{"_typeName":"VirtualMachineProfileRawData","extensionKey":"com.vmware.vim.sps"}}]},
{"_typeName":"VirtualDeviceConfigSpec","operation":"add","device":
{"_typeName":"VirtualE1000","key":-100}}]}'
com vmware vcenter namespacemanagement virtualmachineclasses get --vm-class vmclass-ist-2
```

Leere Konfigurationsspezifikation

```
com vmware vcenter namespacemanagement virtualmachineclasses update --vm-class class-w-e1000
--config-spec ''
```

Nächste Schritte

Die VM-Klassen, die Sie mit der DCLI erstellen, werden in vCenter Server verfügbar. Sie können den vSphere Client verwenden, um diese VM-Klassen einem Namespace zuzuweisen. Weitere Informationen hierzu finden Sie unter Zuordnen einer VM-Klasse zu einem Namespace mit dem vSphere Client.

Bereitstellen einer eigenständigen VM in vSphere IaaS control plane

Verwenden Sie als DevOps-Ingenieur den Befehl `kubectl`, um verfügbare VM-Ressourcen zu überprüfen und eine eigenständige Linux- oder Windows VM in einem Namespace auf einem Supervisor bereitzustellen. Wenn die VM ein für vGPU konfiguriertes PCI-Gerät enthält, können Sie nach dem Erstellen und Starten der VM in Ihrer vSphere IaaS control plane-Umgebung den NVIDIA vGPU-Grafiktreiber installieren, um GPU-Vorgänge vollständig zu aktivieren.

Voraussetzungen

Um eine eigenständige VM in vSphere IaaS control plane bereitstellen zu können, muss ein DevOps-Ingenieur Zugriff auf bestimmte VM-Ressourcen haben. Stellen Sie sicher, dass ein vSphere-Administrator diese Schritte durchgeführt hat, um VM-Ressourcen verfügbar zu machen:

- Erstellen Sie einen Namespace und weisen Sie ihm Speicherrichtlinien zu. Weitere Informationen finden Sie unter Erstellen und Konfigurieren eines vSphere-Namespace im Supervisor..
- Erstellen Sie eine Inhaltsbibliothek und ordnen Sie sie dem Namespace zu. Weitere Informationen finden Sie unter Erstellen und Verwalten von Inhaltsbibliotheken für eigenständige VMs in vSphere IaaS control plane.
  - Wenn eine Inhaltsbibliothek durch eine Sicherheitsrichtlinie geschützt ist, müssen alle Bibliothekselemente konform sein. Wenn die geschützte Bibliothek eine Kombination aus konformen und nicht konformen Elementen enthält, werden den DevOps-Ingenieuren über den Befehl `kubectl get virtualmachineimages` keine VM-Images angezeigt.
  - Wenn Sie VMs mit vGPU-Geräten bereitstellen möchten, müssen Sie Zugriff auf Images haben, wobei der Startmodus auf EFI festgelegt ist, z. B. CentOS.
- Ordnen Sie Standard- oder benutzerdefinierte VM-Klassen einem Namespace zu. Weitere Informationen finden Sie unter Arbeiten mit VM-Klassen in vSphere IaaS control plane.

Wenn Sie NVIDIA vGPU oder andere PCI-Geräte für Ihre VMs verwenden möchten, müssen weitere Voraussetzungen erfüllt sein. Weitere Informationen finden Sie unter Bereitstellen einer VM mit PCI-Geräten in vSphere IaaS control plane.

Informationen zum VM-Operator und unterstützten Feldern finden Sie unter Konzepte des VM-Diensts und https://vm-operator.readthedocs.io/en/stable/ref/api/v1alpha2/.

Anzeigen der in einem Namespace verfügbaren VM-Ressourcen in vSphere IaaS control plane

Stellen Sie als DevOps-Ingenieur sicher, dass Sie auf VM-Ressourcen in Ihrem Namespace zugreifen können, und zeigen Sie vm-Klassen und VM-Vorlagen an, die in Ihrer Umgebung verfügbar sind. Sie können auch Speicherklassen und andere Elemente auflisten, die Sie möglicherweise für den Self-Service einer VM benötigen.

Diese Aufgabe umfasst Befehle, mit denen Sie auf Ressourcen zugreifen können, die für eine Bereitstellung einer eigenständigen VM verfügbar sind. Informationen zu den Ressourcen, die für die Bereitstellung von Tanzu Kubernetes Grid-Clustern und VMs erforderlich sind, die die Cluster bilden, finden Sie unter VM-Klassen für Tanzu Kubernetes-Cluster in der Dokumentation zu *Verwenden des TKG-Dienstes mit der vSphere IaaS-Steuerungsebene*.

Verfahren

1 Greifen Sie in der Kubernetes-Umgebung auf Ihren Namespace zu.

Weitere Informationen finden Sie unter Abrufen und Verwenden des Supervisor-Kontexts in vSphere IaaS control plane.

2 Um die in Ihrem Namespace verfügbaren VM-Klassen anzeigen zu können, führen Sie den folgenden Befehl aus.

```
kubectl get virtualmachineclass
```

Sie sehen die folgende Ausgabe.

Hinweis Da der bestmögliche VM-Klassentyp eine Überbelegung von Ressourcen zulässt, ist es möglich, dass keine Ressourcen mehr verfügbar sind, wenn Sie Grenzwerte für den Namespace festgelegt haben, in dem Sie die VMs bereitstellen. Verwenden Sie aus diesem Grund den garantierten VM-Klassentyp in der Produktionsumgebung.

```
NAME                      VIRTUALMACHINECLASS       AGE

best-effort-large         best-effort-large         44m
best-effort-medium        best-effort-medium        44m
best-effort-small         best-effort-small         44m
best-effort-xsmall        best-effort-xsmall        44m
custom                    custom                    44m
```

3 Zum Anzeigen von Details zu einer bestimmten VM-Klasse führen Sie die folgenden Befehle aus:

- `kubectl describe virtualmachineclasses` *name_vm_class*

Wenn eine VM-Klasse ein vGPU-Gerät enthält, können Sie sein Profil unter `spec: hardware: devices: vgpuDevices` anzeigen.

```
......
spec:
  hardware:
    cpus: 4
    devices:
      vgpuDevices:
      - profileName: grid_v100-q4
......
```

- `kubectl get virtualmachineclasses -o wide`

  Wenn die VM-Klasse ein vGPU- oder Passthrough-Gerät enthält, wird es in der Spalte `VGPUDevicesProfileNames` oder `PassthroughDeviceIDs` ausgegeben.

4 Zeigen Sie die VM-Images an.

`kubectl get virtualmachineimages`

Die angezeigte Ausgabe lautet in etwa wie folgt: Der Image-Name, wie z. B. `vmi-xxxxxxxxxxxxx`, wird vom System automatisch generiert.

```
NAME                                                VERSION  OSTYPE                FORMAT
IMAGESUPPORTED  AGE
vmi-xxxxxxxxxxxxx                                            centos8_64Guest       ovf
true            4d3h
```

5 Verwenden Sie den folgenden Befehl, um ein bestimmtes Image zu beschreiben.

`kubectl describe virtualmachineimage vmi-xxxxxxxxxxxxx`

VMs mit vGPU-Geräten erfordern Images, für die als Startmodus EFI festgelegt ist, z. B. CentOS. Sie müssen Zugriff auf diese Images haben.

6 Überprüfen Sie, ob Sie auf Speicherklassen zugreifen können.

`kubectl get resourcequotas`

Weitere Informationen finden Sie unter Anzeigen von Speicherklassen in einem vSphere-Namespace.

```
NAME                        AGE
REQUEST
     LIMIT
my-ns-ubuntu-storagequota   24h   wcpglobal-storage-profile.storageclass.storage.k8s.io/
requests.storage: 0/9223372036854775807
```

Bereitstellen einer virtuellen Maschine in vSphere IaaS control plane

Stellen Sie als DevOps-Ingenieur eine VM und ihr Gastbetriebssystem deklarativ bereit, indem Sie VM-Bereitstellungsspezifikationen in eine Kubernetes-YAML-Datei schreiben.

Voraussetzungen

Wenn Sie NVIDIA vGPU oder andere PCI-Geräte für Ihre VMs verwenden, beachten Sie Folgendes: Bereitstellen einer VM mit PCI-Geräten in vSphere IaaS control plane

Verfahren

1 Bereiten Sie eine VM-YAML-Datei vor.

Geben Sie in der Datei die folgenden Parameter an:

Option	Bezeichnung
apiVersion	Gibt die Version der VM-Dienst-API an. Beispiel: **`vmoperator.vmware.com/v1alpha2`**.
kind	Gibt den Typ der zu erstellenden Kubernetes-Ressource an. Der einzige verfügbare Wert ist **`VirtualMachine`**.
spec.imageName	Gibt den Namen der VM-Image-Ressource im Kubernetes-Cluster an.
spec.storageClass	Gibt die Speicherklasse an, die für den Speicher der dauerhaften Volumes verwendet werden soll.
spec.className	Gibt den Namen der VM-Klasse an, in der die zu verwendenden Einstellungen für die virtuelle Hardware beschrieben werden.
spec.networkInterfaces	Gibt netzwerkbezogene Einstellungen für die VM an. ■ `networkType`. Die Werte für diesen Schlüssel können **`nsx-t`** oder **`vsphere-distributed`** lauten. ■ `networkName`. Legen Sie bei Bedarf einen Namen fest oder behalten Sie den Standardnamen bei.
spec.vmMetadata	Enthält zusätzliche Metadaten, die an die VM übergeben werden sollen. Sie können diesen Schlüssel verwenden, um das Gastbetriebssystem-Image anzupassen und Elemente wie den `hostname` der VM und `user-data` festzulegen, einschließlich Kennwörter, SSH-Schlüssel usw. Weitere Informationen, einschließlich Details zum Bootstrap und zur Anpassung von Windows VMs mithilfe des Microsoft Systemvorbereitungstools (Sysprep), finden Sie unter Anpassung eines Gastbetriebssystems.
topology.kubernetes.io/zone	Steuert die Platzierung der VM auf einem Supervisor mit drei Zonen. Beispiel: `topology.kubernetes.io/zone: zone-a02`.

Die folgende Beispiel-VM-YAML-Datei `my-vm` verwendet CloudInit als Bootstrapping-Methode. Das Beispiel zeigt eine VirtualMachine-Ressource, die Benutzerdaten in einer geheimen Ressource `my-vm-bootstrap-data` angibt. Der geheime Schlüssel wird für das Bootstrap und die Anpassung des Gastbetriebssystems verwendet.

Die Daten im geheimen Schlüssel enthalten die CloudInit cloud-config. Weitere Informationen zum cloud-config-Format finden Sie in der offiziellen Dokumentation Cloud-Konfigurationsbeispiele.

Beispiele mit Sysprep als Bootstrapping-Methode finden Sie unter Sysprep.

```
apiVersion: vmoperator.vmware.com/v1alpha2
kind: VirtualMachine
metadata:
  name:      my-vm
  namespace: my-namespace
spec:
  className:    small
  imageName:    vmi-xxxxxxxxxxxx
  storageClass: iscsi
  vmMetadata:
    transport: CloudInit
    secretName: my-vm-bootstrap-data
```

```
apiVersion: v1
kind: Secret
metadata:
  name:      my-vm-bootstrap-data
  namespace: my-namespace
stringData:
  user-data: |
    #cloud-config
    users:
    - default
    - name: xyz..
      primary_group: xyz..
      groups: users
      ssh_authorized_keys:
      - ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDSL7uWGj...
    runcmd:
    - "ls /"
    - [ "ls", "-a", "-l", "/" ]
    write_files:
    - path: /etc/my-plaintext
      permissions: '0644'
      owner: root:root
      content: |
        Hello, world.
```

Verwenden Sie das folgende Beispiel, wenn Sie eine VM in einer Umgebung mit Zonen bereitstellen.

Um die Werte für *ZONE_NAME* abzurufen, führen Sie den Befehl `kubectl get vspherezones` aus.

```
apiVersion: vmoperator.vmware.com/v1alpha2
kind: VirtualMachine
metadata:
  name: <vm-name>
```

```
  namespace: <vm-ns>
  labels:
    topology.kubernetes.io/zone: ZONE_NAME
...
```

2 Stellen Sie die VM bereit.

```
kubectl apply -f my-vm.yaml
```

3 Stellen Sie sicher, dass die VM erstellt wurde.

```
kubectl get vm
NAME              AGE
my-vm             28s
```

4 Überprüfen Sie die VM-Details und deren Status.

```
kubectl describe virtualmachine my-vm
```

Die Ausgabe lautet in etwa wie folgt: Über die Ausgabe können Sie auch die IP-Adresse der VM abrufen, die in der `Vm Ip` angezeigt wird.

```
Name:         my-vm
Namespace:    my-namespace
API Version:  vmoperator.vmware.com/v1alpha2
Kind:         VirtualMachine
Metadata:
  Creation Timestamp:  2021-03-23T19:07:36Z
  Finalizers:
    virtualmachine.vmoperator.vmware.com
  Generation:  1
  Managed Fields:
 ...
 ...
Status:
  Bios UUID:              4218ec42-aeb3-9491-fe22-19b6f954ce38
  Change Block Tracking:  false
  Conditions:
    Last Transition Time:  2021-03-23T19:08:59Z
    Status:                True
    Type:                  VirtualMachinePrereqReady
  Host:                    10.185.240.10
  Instance UUID:           50180b3a-86ee-870a-c3da-90ddbaffc950
  Phase:                   Created
  Power State:             poweredOn
  Unique ID:               vm-73
  Vm Ip:                   10.161.75.162
Events:                    <none>
...
```

5 Stellen Sie sicher, dass die VM-IP-Adresse erreichbar ist.

```
ping 10.161.75.162
PING 10.161.75.162 (10.161.75.162): 56 data bytes
64 bytes from 10.161.75.162: icmp_seq=0 ttl=59 time=43.528 ms
64 bytes from 10.161.75.162: icmp_seq=1 ttl=59 time=53.885 ms
64 bytes from 10.161.75.162: icmp_seq=2 ttl=59 time=31.581 ms
```

Ergebnisse

Eine über den VM-Dienst erstellte VM kann nur von DevOps aus dem Kubernetes-Namespace verwaltet werden. Der Lebenszyklus kann nicht über den vSphere Client verwaltet werden. vSphere-Administratoren können jedoch die VM und ihre Ressourcen überwachen. Weitere Informationen finden Sie unter Überwachen der in vSphere IaaS control plane verfügbaren virtuellen Maschinen.

Nächste Schritte

Weitere Informationen finden Sie im Blog Introducing Virtual Machine Provisioning.

Bereitstellen einer VM mit vGPU und anderen PCI-Geräten in vSphere IaaS control plane

Wenn ESXi-Hosts in Ihrer vSphere IaaS control plane-Umgebung über ein oder mehrere NVIDIA GRID GPU-Grafikgeräte verfügen, können Sie VMs zur Verwendung der NVIDIA GRID vGPU-Technologie (virtual GPU) konfigurieren. Sie können auch andere PCI-Geräte auf einem ESXi-Host konfigurieren, um sie einer VM im Passthrough-Modus zur Verfügung zu stellen.

Bereitstellen einer VM mit vGPU in vSphere IaaS control plane

NVIDIA GRID GPU-Grafikgeräte sind so konzipiert, dass sie komplexe Grafikvorgänge optimieren und dadurch mit Hochleistung ausgeführt werden können, ohne dabei den Hauptprozessor zu überlasten. NVIDIA GRID vGPU bietet eine beispiellose Grafikleistung, Kosteneffizienz und Skalierbarkeit, indem ein einzelner physischer Grafikprozessor (GPU) von mehreren VMs gemeinsam als separate vGPU-fähige Passthrough-Geräte verwendet wird.

Überlegungen

Wenn Sie NVIDIA vGPU verwenden, gelten die folgenden Bedingungen:

- Drei-Zonen-Supervisor unterstützt keine VMs mit vGPU.
- VMs mit vGPU-Geräten, die vom VM-Dienst verwaltet werden, werden automatisch ausgeschaltet, wenn ein ESXi-Host in den Wartungsmodus wechselt. Dies kann sich vorübergehend auf Arbeitslasten auswirken, die in den VMs ausgeführt werden. Die VMs werden automatisch eingeschaltet, nachdem der Host im Wartungsmodus ausgeführt wurde.
- DRS verteilt vGPU-VMs breit auf die Hosts des Clusters. Weitere Informationen finden Sie unter DRS-Platzierung von vGPU-VMs im Handbuch *Handbuch zur vSphere-Ressourcenverwaltung*.

Anforderungen

Erfüllen Sie zum Konfigurieren von NVIDIA vGPU die folgenden Voraussetzungen:

- Überprüfen Sie im VMware-Kompatibilitätshandbuch, ob ESXi unterstützt wird, und erkundigen Sie sich beim Anbieter, ob der Host die Stromversorgungs- und Konfigurationsanforderungen erfüllt.
- Konfigurieren Sie die Grafikeinstellungen des ESXi-Hosts mit mindestens einem Gerät im Modus **Direkt freigegeben**. Weitere Informationen finden Sie unter Konfigurieren von Hostgrafiken in der Dokumentation zu *Handbuch zur vSphere-Ressourcenverwaltung*.
- Die Inhaltsbibliothek, die Sie für VMs mit vGPU-Geräten verwenden, muss Images enthalten, deren Startmodus auf EFI festgelegt ist, z. B. CentOS.
- Installieren Sie die NVIDIA vGPU-Software. NVIDIA stellt ein vGPU-Softwarepaket bereit, das die folgenden Komponenten enthält.

  Weitere Informationen finden Sie in der entsprechenden Dokumentation zur NVIDIA Virtual GPU-Software.

  - vGPU Manager, den ein vSphere-Administrator auf dem ESXi-Host installiert. Weitere Informationen hierzu finden Sie im VMware-Knowledgebase-Artikel 2033434.
  - Gast-VM-Treiber, den ein DevOps-Ingenieur nach der Bereitstellung und dem Starten der VM in der VM installiert. Weitere Informationen finden Sie unter Installieren des NVIDIA-Gasttreibers in einer VM in vSphere IaaS control plane.

Hinzufügen eines vGPU-Geräts zu einer VM-Klasse mit vSphere Client

Erstellen oder bearbeiten Sie eine vorhandene VM-Klasse, um eine virtuelle NVIDIA GRID GPU (vGPU) hinzuzufügen.

Voraussetzungen

Erforderliche Rechte:

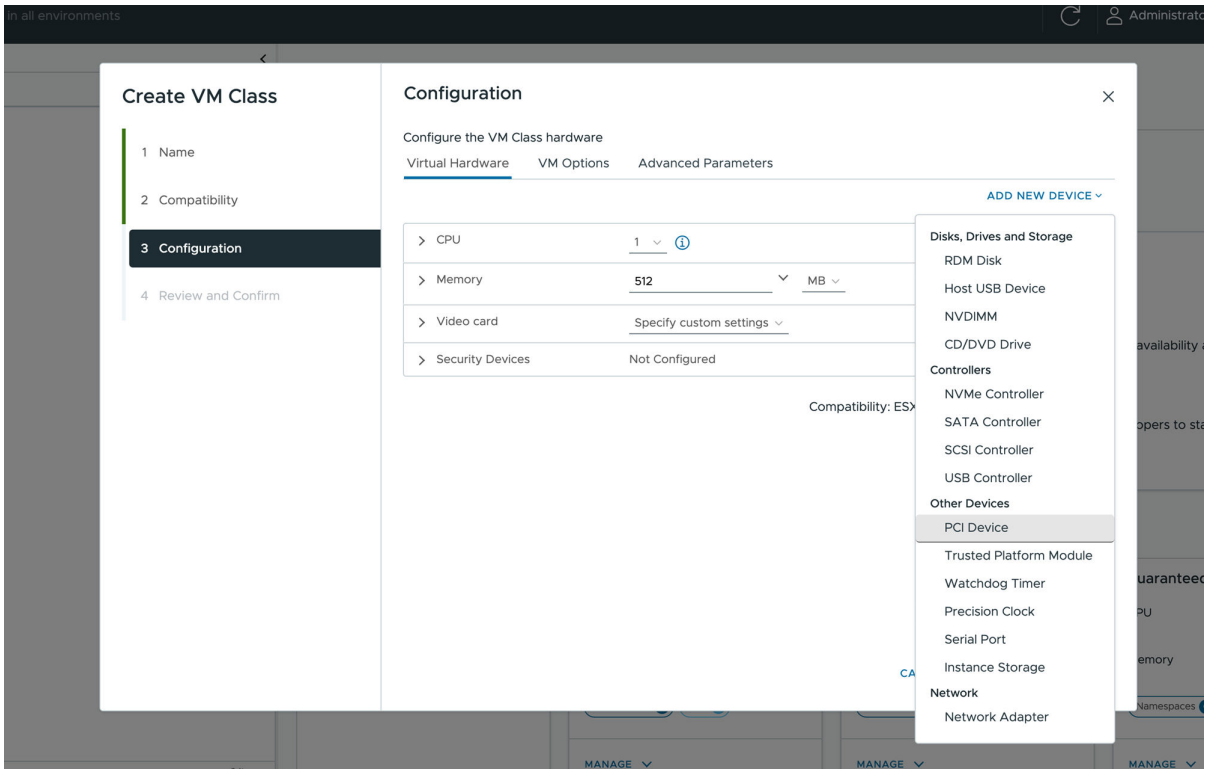
- **Namespaces.Clusterweite Konfiguration ändern**
- **Namespaces.Namespace-Konfiguration ändern**
- **VM-Klassen.VM-Klassen verwalten**

Verfahren

1 Erstellen oder bearbeiten Sie eine vorhandene VM-Klasse.

Option	Aktion
Neue VM-Klasse erstellen	a Wählen Sie im vSphere Client-Startmenü die Option **Arbeitslastverwaltung** aus. b Klicken Sie auf die Registerkarte **Dienste** und klicken Sie dann im Bereich **VM-Dienst** auf **Verwalten**. c Klicken Sie auf der Seite **VM-Dienst** auf **VM-Klassen** und dann auf **VM-Klasse erstellen**. d Führen Sie die angezeigten Anweisungen aus.
Bearbeiten einer VM-Klasse	a Wählen Sie im vSphere Client-Startmenü die Option **Arbeitslastverwaltung** aus. b Klicken Sie auf die Registerkarte **Dienste** und klicken Sie dann im Bereich **VM-Dienst** auf **Verwalten**. c Klicken Sie auf der Seite **VM-Dienst** auf **VM-Klassen**. d Klicken Sie im Bereich der ausgewählten VM-Klasse auf **Verwalten** und dann auf **Bearbeiten**. e Führen Sie die angezeigten Anweisungen aus.

2 Klicken Sie auf der Seite **Konfiguration** auf die Registerkarte **Virtuelle Hardware**, klicken Sie auf **Neues Gerät hinzufügen** und wählen Sie **PCI-Gerät** aus.

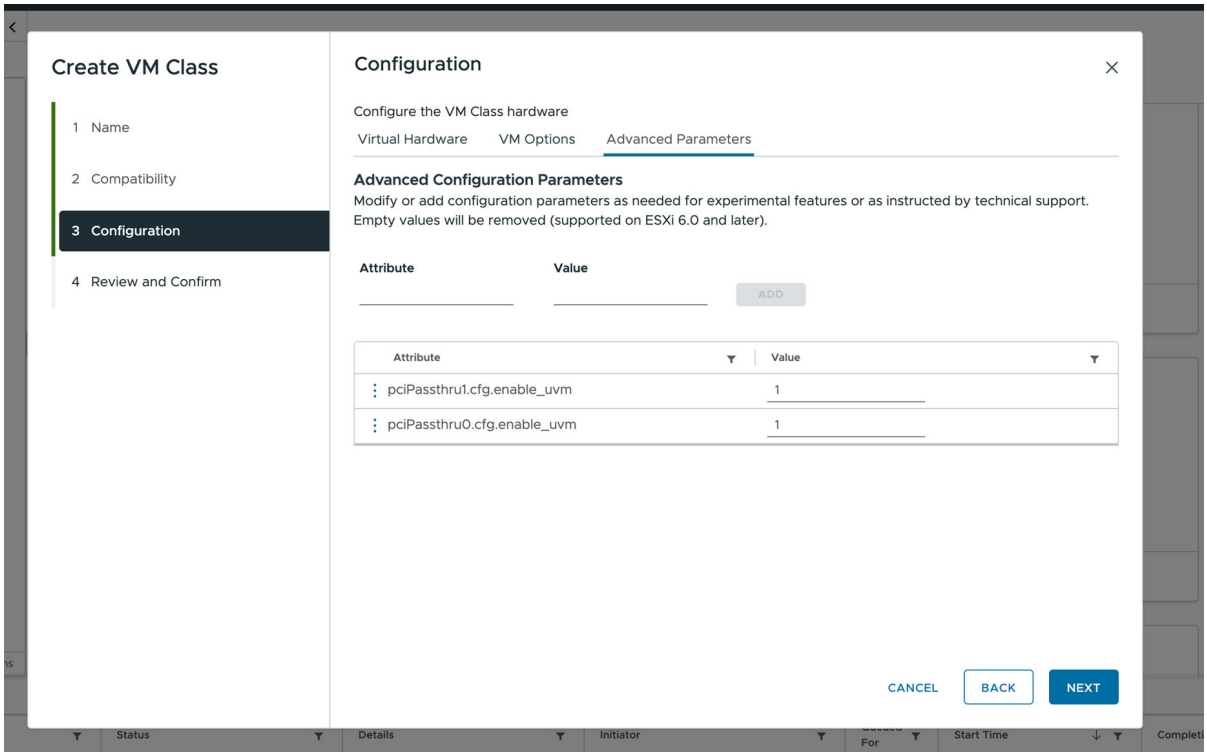


3 Wählen Sie in der Liste der verfügbaren Geräte auf der Seite **Geräteauswahl** die Option „NVIDIA GRID vGPU“ aus und klicken Sie auf **Auswählen**.

Das Gerät wird auf der Seite „Virtuelle Hardware“ angezeigt.

4 Klicken Sie auf die Registerkarte **Erweiterte Parameter** und legen Sie die Parameter mit den folgenden Attributen und Werten fest.

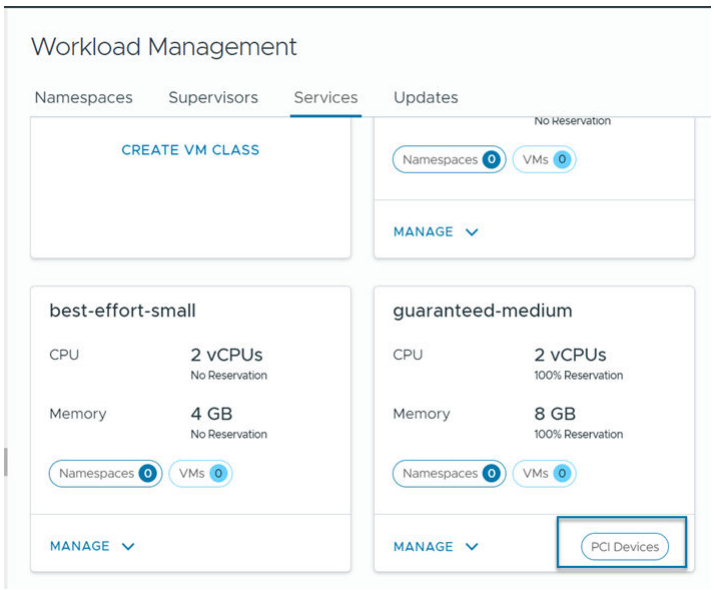
Option	Bezeichnung
Parameter	Wert
pciPassthru0.cfg.enable_uvm	1
pciPassthru1.cfg.enable_uvm	1



5 Überprüfen Sie Ihre Konfiguration und klicken Sie auf **Beenden**.

Ergebnisse

Ein **PCI-Geräte**-Tag im Bereich der VM-Klasse gibt an, dass die VM-Klasse vGPU-fähig ist.



Hinzufügen eines vGPU-Geräts zu einer VM-Klasse mithilfe der Datencenter-CLI

Neben dem vSphere Client können Sie auch den Befehl Data Center CLI (DCLI) verwenden, um vGPUs und erweiterte Konfigurationen hinzuzufügen.

Weitere Informationen zu DCLI-Befehlen finden Sie unter Erstellen und Verwalten von VM-Klassen mithilfe der Datencenter-CLI.

Verfahren

1 Melden Sie sich bei vCenter Server mit dem Root-Benutzerkonto an und geben Sie `dcli +i` ein, um die DCLI im interaktiven Modus zu verwenden.

2 Führen Sie den folgenden Befehl aus, um eine VM-Klasse zu erstellen.

Im folgenden Beispiel enthält die VM-Klasse *my-class* zwei CPUs, 2048 MB Arbeitsspeicher und eine VirtualMachineConfigSpec mit zwei vGPU-Beispielprofilen, nämlich `mockup-vmiop-8c` und `mockup-vmiop`. Die extraConfig-Felder `pciPassthru0.cfg.enable_uvm` und `pciPassthru1.cfg.enable_uvm` sind auf 1 eingestellt.

```
dcli +i +show-unreleased com vmware vcenter namespacemanagement
virtualmachineclasses create --id my-class --cpu-count 2 --memory-
mb 2048 --config-spec '{"_typeName":"VirtualMachineConfigSpec","deviceChange":
[{"_typeName":"VirtualDeviceConfigSpec","operation":"add","device":
{"_typeName":"VirtualPCIPassthrough","key":20,"backing":
{"_typeName":"VirtualPCIPassthroughVmiopBackingInfo","vgpu":"mockup-
vmiop-8c"}}},{"_typeName":"VirtualDeviceConfigSpec","operation":"add","device":
{"_typeName":"VirtualPCIPassthrough","key":20,"backing":
{"_typeName":"VirtualPCIPassthroughVmiopBackingInfo","vgpu":"mockup-
vmiop"}}}],"extraConfig":
[{"_typeName":"OptionValue","key":"pciPassthru0.cfg.enable_uvm","value":
{"_typeName":"string","_value":"1"}},
{"_typeName":"OptionValue","key":"pciPassthru1.cfg.enable_uvm","value":
{"_typeName":"string","_value":"1"}}]}'
```

Installieren des NVIDIA-Gasttreibers in einer VM in vSphere IaaS control plane

Wenn die VM ein für vGPU konfiguriertes PCI-Gerät enthält, installieren Sie nach dem Erstellen und Starten der VM in Ihrer vSphere IaaS control plane-Umgebung den NVIDIA vGPU-Grafiktreiber, um GPU-Vorgänge vollständig zu aktivieren.

Voraussetzungen

- Stellen Sie die VM mit vGPU bereit. Achten Sie darauf, dass die YAML-Datei der VM auf die VM-Klasse mit der vGPU-Definition verweist. Weitere Informationen finden Sie unter Bereitstellen einer virtuellen Maschine in vSphere IaaS control plane.
- Vergewissern Sie sich, dass Sie das vGPU-Softwarepaket von der NVIDIA-Downloadseite heruntergeladen und das Paket dekomprimiert haben und dass die Gastlaufwerkkomponente bereit ist. Informationen finden Sie in der entsprechenden Dokumentation zur NVIDIA Virtual GPU-Software.

  Hinweis Die Version der Treiberkomponente muss der Version des vGPU-Managers entsprechen, die ein vSphere-Administrator auf dem ESXi-Host installiert hat.

Verfahren

1. Kopieren Sie das Linux-Treiberpaket für die NVIDIA vGPU-Software, z. B. `NVIDIA-Linux-x86_64-version-grid.run`, auf die Gast-VM.
2. Beenden Sie alle Anwendungen, bevor Sie versuchen, das Treiberinstallationsprogramm auszuführen.
3. Starten Sie das Installationsprogramm für den NVIDIA vGPU-Treiber.

   ```
   sudo ./NVIDIA-Linux-x86_64-version-grid.run
   ```

4. Akzeptieren Sie die NVIDIA Software-Lizenzvereinbarung und klicken Sie auf **Ja**, um die X-Konfigurationseinstellungen automatisch zu aktualisieren.
5. Stellen Sie sicher, dass der Treiber installiert wurde.

   Beispiel:

   ```
   ~$ nvidia-smi
   Wed May 19 22:15:04 2021
   +-----------------------------------------------------------------------------+
   | NVIDIA-SMI 460.63       Driver Version: 460.63       CUDA Version: 11.2     |
   |-------------------------------+----------------------+----------------------+
   | GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile Uncorr. ECC |
   | Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util  Compute M. |
   |                               |                      |               MIG M. |
   |===============================+======================+======================|
   |   0  GRID V100-4Q        On   | 00000000:02:00.0 Off |                  N/A|
   | N/AN/AP0    N/A/  N/A|    304MiB /  4096MiB |      0%      Default |
   |                               |                      |                  N/A|
   +-------------------------------+----------------------+----------------------+
   ```

```
+-----------------------------------------------------------------------------+
| Processes:                                                                  |
|  GPU   GI   CI        PID   Type   Process name                 GPU Memory |
|        ID   ID                                                  Usage      |
|=============================================================================|
|  No running processes found                                                 |
+-----------------------------------------------------------------------------+
```

Bereitstellen einer VM mit PCI-Geräten in vSphere IaaS control plane

Zusätzlich zu vGPU können Sie auch andere PCI-Geräte auf einem ESXi-Host konfigurieren, um sie einer VM im Passthrough-Modus zur Verfügung zu stellen.

vSphere IaaS control plane unterstützt Dynamic DirectPath I/O-Geräte. Mithilfe von Dynamic DirectPath I/O kann die VM direkt auf die physischen PCI- und PCIe-Geräte zugreifen, die mit einem Host verbunden sind. Sie können Dynamic DirectPath I/O verwenden, um einer VM mehrere PCI-Passthrough-Geräte zuzuweisen. Jedes Passthrough-Gerät kann gemäß seines PCI-Anbieter- und Gerätebezeichners angegeben werden.

Hinweis Wenn Sie Dynamic DirectPath I/O für PCI-Passthrough-Geräte konfigurieren, verbinden Sie die PCI-Geräte mit dem Host und markieren Sie sie als für Passthrough verfügbar. Weitere Informationen finden Sie unter Aktivieren von Passthrough für ein Netzwerkgerät auf einem Host in der Dokumentation zu *vSphere-Netzwerk*.

Bereitstellen einer VM mit Instanzspeicher in vSphere IaaS control plane

Zusammen mit dauerhaften Speichervolumes kann eine VM Instanzspeicher verwenden. Im Gegensatz zu dauerhaften Volumes, die getrennt von der VM vorhanden sind, hängen Instanzspeicher-Volumes vom Lebenszyklus einer VM-Instanz ab. Dieser Speicher befindet sich in der Regel auf Hochgeschwindigkeitsgeräten wie z. B. NVMe, die für den ESXi-Host lokal sind.

Instanzspeicher-Lebenszyklus

Beim Erstellen der VM erstellt das System Instanzspeicher-Volumes und hängt sie an die VM an. Die Daten im Instanzspeicher-Volume bleiben nur während der Lebensdauer der zugehörigen VM-Instanz bestehen. Das Volume wird beim Löschen der VM gelöscht.

VMs mit Instanzspeicher unterstützen den ESXi-Hostwartungsmodus. Die VM wird ausgeschaltet, wenn der ESXi-Host in den Wartungsmodus wechselt, und wieder eingeschaltet, nachdem der Host den Wartungsmodus verlassen hat.

Überlegungen zu Instanzspeicher-VMs

Bei der Verwendung von VMs mit Instanzspeicher sollten Sie die folgenden Punkte beachten:

- Ein Supervisor mit einem VDS-Netzwerk-Stack unterstützt keine Instanzspeicher.
- Drei-Zonen-Supervisor unterstützt keine Instanzspeicher.

- Eine Warnung wird angezeigt, wenn ein vSphere-Administrator eine VM-Klasse mit Instanzspeicher auf einen Namespace anwendet, der über keine für den Instanzspeicher erforderliche geeignete Speicherrichtlinie verfügt.
- VMs mit Instanz-Volumes können nicht auf andere ESXi-Hosts migriert werden.
- Sie können die Instanzspeicher-Volumes nicht bearbeiten, wenn die Volumes bereits verwendet werden.
- Wenn der vSphere-Administrator die Instanz-Speicherrichtlinie nach der VM-Erstellung aus dem Namespace entfernt, wird die VM weiterhin ausgeführt.
- Als DevOps-Ingenieur können Sie keine Instanzspeicherressourcen löschen oder aktualisieren. Sie können das Instanzspeicher-Volume nicht von einer VM-Instanz trennen und an eine andere Instanz anhängen.

Workflow für die Bereitstellung und Überwachung einer Instanzspeicher-VM

Schritt	Durchgeführt von	Beschreibung
1	vSphere-Administrator	Erstellen und Verwalten von Inhaltsbibliotheken für eigenständige VMs in vSphere IaaS control plane
2	vSphere-Administrator	Erstellen Sie einen vSAN Direct-Datenspeicher.
3	vSphere-Administrator	Erstellen Sie eine mit vSAN Direct kompatible Speicherrichtlinie und weisen Sie sie dem Namespace zu.
4	vSphere-Administrator	Erstellen Sie eine Instanzspeicher-VM-Klasse und weisen Sie sie dem Namespace zu.
5	DevOps-Ingenieur	Stellen Sie eine VM mit Instanzspeicher im Namespace bereit.
6	vSphere-Administrator	Überwachen der in vSphere IaaS control plane verfügbaren virtuellen Maschinen

Erstellen eines vSAN Direct-Datenspeichers

Richten Sie als vSphere-Administrator einen vSAN Direct-Datenspeicher ein, der mit Funktionalitäten wie vSAN Data Persistence-Plattform oder VM-Instanzspeicher verwendet werden soll. Verwenden Sie zum Erstellen des Datenspeichers nicht beanspruchte Speichergeräte, die sich auf Ihrem ESXi-Host befinden.

Sie können den vSAN Direct-Datenspeicher erstellen, wenn Sie vSAN für Ihren Supervisor aktivieren. Die folgende Aufgabe zeigt, wie lokale Speichergeräte als vSAN Direct beansprucht werden können, wenn vSAN bereits auf dem Cluster aktiviert ist.

Verfahren

1 Navigieren Sie im vSphere Client zum vSAN-Cluster.

2 Klicken Sie auf die Registerkarte **Konfigurieren**.

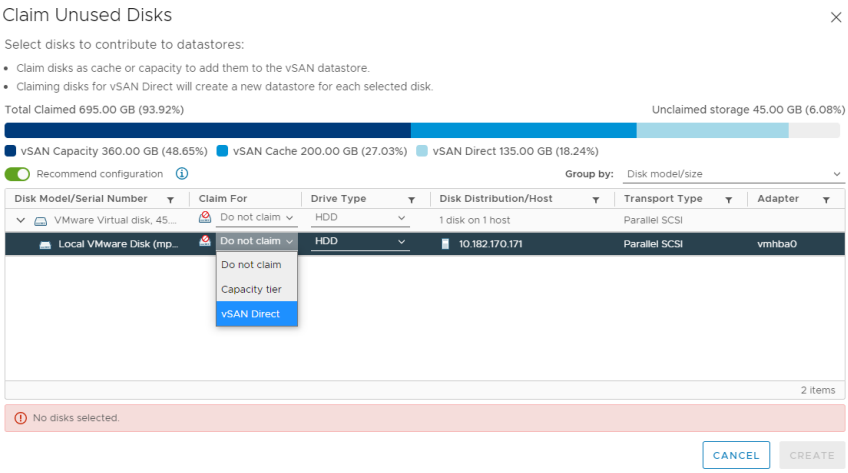
3 Klicken Sie unter vSAN auf **Festplattenverwaltung**.

4 Klicken Sie auf **Ungenutzte Festplatten beanspruchen**.

5 Klicken Sie im Dialogfeld **Unbelegte Festplatten beanspruchen** auf die Registerkarte **vSAN Direkt**.

6 Wählen Sie ein zu beanspruchende Gerät aus und aktivieren Sie ein Kontrollkästchen in der Spalte **Für vSAN Direct beanspruchen**.

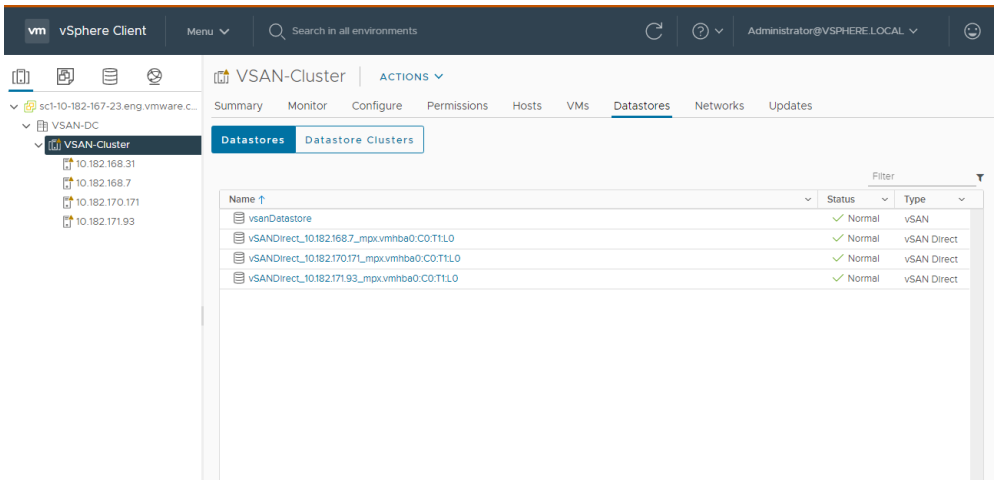
Hinweis Wenn Sie die Geräte für einen regulären vSAN-Datenspeicher beanspruchen, werden diese Geräte nicht auf der Registerkarte **vSAN Direct** angezeigt.



7 Klicken Sie auf **Erstellen**.

Für jedes von Ihnen beanspruchte Gerät erstellt vSAN Direct einen neuen Datenspeicher.

8 Klicken Sie auf die Registerkarte **Datenspeicher**, um alle vSAN Direct-Datenspeicher in Ihrem Cluster anzuzeigen.



Nächste Schritte

Sie können vSAN Direct mit externem Speicher verwenden. Weitere Informationen finden Sie in der Dokumentation zum Thema *Wartung der vSphere IaaS-Steuerungsebene* unter Verwenden eines externen Speichers mit vSAN Direct.

Erstellen einer vSAN Direct-Speicherrichtlinie

Wenn Sie vSAN Direct verwenden, erstellen Sie eine Speicherrichtlinie, die mit einem Supervisor-Namespace verwendet werden soll. In dem Namespace, den Sie mit dieser Speicherrichtlinie verknüpfen, können Sie Arbeitslasten ausführen, die mit vSAN Direct kompatibel sind, z. B. statusbehaftete Dienste oder Instanzspeicher-VMs.

Verfahren

1. Öffnen Sie im vSphere Client den Assistenten **VM-Speicherrichtlinie erstellen**.
   a. Klicken Sie auf der **Startseite** auf **Richtlinien und Profile**.
   b. Klicken Sie unter **Richtlinien und Profile** auf **VM-Speicherrichtlinien**.
   c. Klicken Sie auf **Erstellen**.
2. 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.
Beschreibung	Geben Sie die Beschreibung der Speicherrichtlinie ein.

3. Aktivieren Sie auf der Seite **Richtlinienstruktur** unter **Datenspeicherspezifische Regeln** Regeln für die Platzierung des vSAN Direct-Speichers.
4. Legen Sie vSAN Direct auf der Seite **vSAN Direct-Regeln** als Speicherplatzierungstyp fest.
5. Überprüfen Sie auf der Seite **Speicherkompatibilität** die Liste der vSAN Direct-Datenspeicher, die mit dieser Richtlinie übereinstimmen.
6. Überprüfen Sie auf der Seite **Überprüfen und beenden** die Einstellungen der Speicherrichtlinie und klicken Sie auf **Beenden**.

   Um Änderungen an Einstellungen vorzunehmen, klicken Sie auf **Zurück**, um wieder zur entsprechenden Seite zu wechseln.

Erstellen einer VM-Klasse mit Instanzspeicher

In der VM-Klasse verweisen Sie auf die vSAN Direct-Speicherrichtlinie und legen die Größe der Volumes fest, die für den Instanzspeicher verwendet werden sollen. Nachdem Sie die VM-Klasse erstellt haben, weisen Sie sie dem Namespace zu, den Sie für die Instanzspeicher-VM verwenden möchten.

Voraussetzungen

- Erstellen Sie eine Speicherrichtlinie, die mit dem vSAN Direct-Datenspeicher kompatibel ist.
- Fügen Sie dem Namespace, den Sie für die Instanzspeicher-VM verwenden, die vSAN Direct-Speicherrichtlinie hinzu. Weitere Informationen finden Sie unter Erstellen und Konfigurieren eines vSphere-Namespace im Supervisor..
- Erforderliche Rechte:
  - **Namespaces.Clusterweite Konfiguration ändern**
  - **Namespaces.Namespace-Konfiguration ändern**
  - **VM-Klassen.VM-Klassen verwalten**

Verfahren

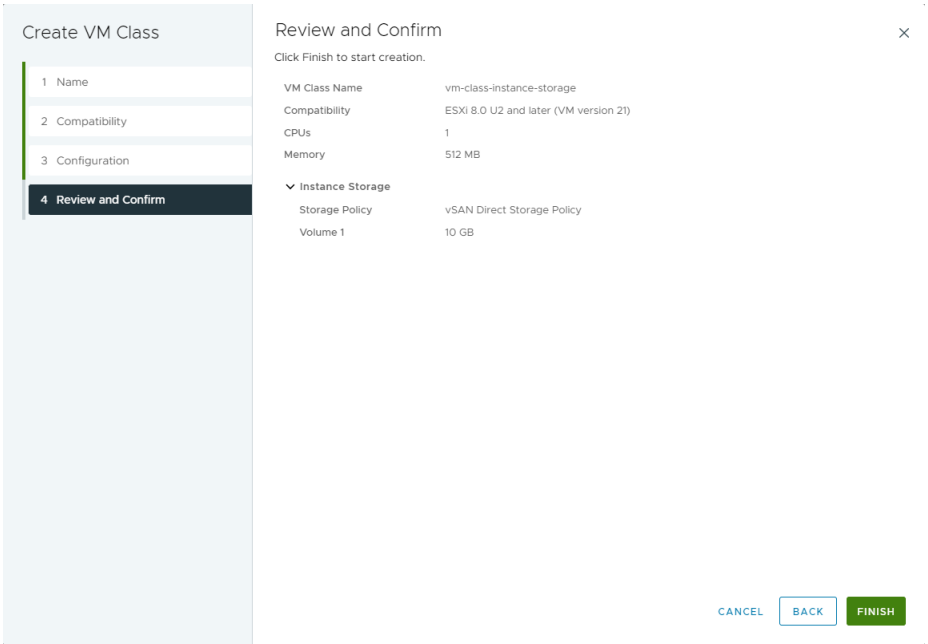
1 Fügen Sie Instanzspeicher hinzu, wenn Sie eine VM-Klasse erstellen oder bearbeiten.

Option	Aktion
VM-Klasse erstellen	a Wählen Sie im vSphere Client-Startmenü die Option **Arbeitslastverwaltung** aus. b Klicken Sie auf die Registerkarte **Dienste** und dann auf der Karte **VM-Dienst** auf **Verwalten**. c Klicken Sie auf der Seite **VM-Dienst** auf **VM-Klasse erstellen**. d Konfigurieren Sie die VM-Klasse nach Bedarf. Weitere Informationen zu den verfügbaren Optionen finden Sie unter Bearbeiten einer VM-Klasse mithilfe des vSphere Client. e Um Instanzspeicher hinzuzufügen, wählen Sie auf der Seite **Konfiguration** die Option **Virtuelle Hardware** und dann **Neues Gerät hinzufügen > Instanzspeicher** aus. Die Option **Instanzspeicher** wird unter „Virtuelle Hardware“ angezeigt.
Vorhandene VM-Klasse bearbeiten	a Wählen Sie im vSphere Client-Startmenü die Option **Arbeitslastverwaltung** aus. b Klicken Sie auf die Registerkarte **Dienste** und klicken Sie dann im Bereich **VM-Dienst** auf **Verwalten**. c Klicken Sie auf der Seite **VM-Dienst** auf **VM-Klassen**. d Klicken Sie auf der Karte einer bestehenden VM-Klasse auf **Verwalten** und dann auf **Bearbeiten**. e Um Instanzspeicher hinzuzufügen, wählen Sie **Virtuelle Hardware** und dann **Neues Gerät hinzufügen > Instanzspeicher** aus. Die Option **Instanzspeicher** wird unter „Virtuelle Hardware“ angezeigt.

2 Erweitern Sie die Option **Instanzspeicher**, um die Instanzspeichereinstellungen zu bearbeiten.

Option	Aktion
Speicherrichtlinie	Wählen Sie die vSAN Direct-Speicherrichtlinie aus.
Volume	Legen Sie die Größe des Volume fest. Sie können mehrere Speichervolumes hinzufügen.

3 Überprüfen Sie auf der Seite **Überprüfen und bestätigen** die Details und klicken Sie auf **Beenden**.



4 Weisen Sie die neu erstellte VM-Klasse dem Namespace zu, den Sie für die Instanzspeicher-VM verwenden.

Weitere Informationen finden Sie unter Zuordnen einer VM-Klasse zu einem Namespace mit dem vSphere Client.

Bereitstellen einer VM mit Instanzspeicher

Stellen Sie als DevOps-Ingenieur sicher, dass Sie auf VM-Ressourcen zugreifen können, die zum Erstellen einer Instanzspeicher-VM erforderlich sind. Verwenden Sie die Ressourcen zum Bereitstellen der VM.

Wenn Sie die Instanzspeicher-VM bereitstellen, befolgen Sie die allgemeinen VM-Bereitstellungsschritte. Weitere Informationen finden Sie unter Bereitstellen einer eigenständigen VM in vSphere IaaS control plane. Dieses Verfahren umfasst zusätzliche spezifische Elemente, die für die Instanzspeicher-VM gelten.

Verfahren

- Überprüfen Sie die folgenden Punkte für die Instanzspeicher-VM:
  - Ihr Namespace enthält die Speicherklasse, die mit dem vSAN Direct-Datenspeicher kompatibel ist.
  - Die Instanzspeicher-VM-Klasse verweist auf diese Speicherklasse.

    Stellen Sie bei der Überprüfung der Details der VM-Klasse des Instanzspeichers sicher, dass sie den Abschnitt `instanceStorage` enthält.

`kubectl describe virtualmachineclasses` *vm-class-instance-storage*

```
apiVersion: vmoperator.vmware.com/v1alpha2
kind: VirtualMachineClass
metadata:
  name: vm-class-instance-storage
spec:
  hardware:
    cpus: 8
    memory: 64Gi
    devices:
...
    instanceStorage:
      storageClass: vsan-direct
      volumes:
      - size: 256Gi
      - size: 512Gi

...
```

- Die VM-YAML-Datei verweist auf die entsprechende Instanzspeicher-VM-Klasse.

Bereitstellen von VMs mit konfigurierbaren OVF-Eigenschaften in vSphere IaaS control plane

Wenn ein DevOps-Ingenieur eine VM in der vSphere IaaS control plane-Umgebung bereitstellt, enthält eine OVF-Vorlage in der Regel hartcodierte Details wie die grundlegende Netzwerkkonfiguration. Sie wissen es jedoch möglicherweise nicht und können den OVF-Eigenschaften der VM, wie z. B. von IPAM bereitgestellte Netzwerkdaten, bestimmte Werte erst zuweisen, nachdem die VM-CR erstellt wurde. Mit der Unterstützung von Vorlagenzeichenfolgen müssen Sie Netzwerkinformationen nicht im Voraus kennen. Sie können Golang-basierte Vorlagen verwenden, um die OVF-Eigenschaftswerte aufzufüllen und den Netzwerk-Stack der VM zu konfigurieren.

Verfahren

1 Stellen Sie sicher, dass Ihre OVF-Datei für alle zu konfigurierenden Eigenschaften den Eintrag `ovf:userConfigurable="true"` enthält.

Mit diesem Eintrag kann das System Platzhalter für Netzwerkwerte wie z. B. Nameserver und Verwaltungs-IPs durch echte Daten ersetzen, nachdem diese erfasst wurden.

Verwenden Sie das folgende Beispiel.

```
<Property ovf:key="hostname" ovf:type="string" ovf:userConfigurable="true"
ovf:value="ubuntuguest">
      <Description>Specifies the hostname for the appliance</Description>
</Property>
<Property ovf:key="nameservers" ovf:type="string" ovf:userConfigurable="true"
ovf:value="1.1.1.1, 1.0.0.1">
```

```
      <Label>2.2. DNS</Label>
      <Description>A comma-separated list of IP addresses for up to three DNS servers</
Description>
</Property>
<Property ovf:key="management_ip" ovf:type="string" ovf:userConfigurable="true">
      <Label>2.3. Management IP</Label>
      <Description>The static IP address for the appliance on the Management Port Group in
CIDR format (Eg. ip/subnet mask bits). This cannot be DHCP.</Description>
</Property>
```

2 Erstellen Sie die VM-YAML-Datei mit Vorlagenzeichenfolgen.

Die Vorlagenzeichenfolgen für Bootstrap-Ressourcen erfassen die Daten, die zum Auffüllen der OVF-Eigenschaftswerte erforderlich sind.

Vorlagenzeichenfolgen können mit einer der folgenden Methoden konfiguriert werden.

- Verwenden Sie vm-operator-api.

  Weitere Informationen finden Sie auf der folgenden Seite in GitHub: https://github.com/vmware-tanzu/vm-operator/blob/main/api/v1alpha2/virtualmachinetempl_types.go.

  Nachfolgend finden Sie eine YAML-Beispieldatei:

```
apiVersion: vmoperator.vmware.com/v1alpha2
kind: VirtualMachine
metadata:
  name: template-vm
  namespace: test-ns
  annotations:
    vmoperator.vmware.com/image-supported-check: disable
spec:
  className: best-effort-xsmall
  imageName: vmi-xxxx0000
  powerState: poweredOn
  storageClass: wcpglobal-storage-profile
  vmMetadata:
    configMapName: template-vm-1
    transport: vAppConfig

---
apiVersion: v1
kind: ConfigMap
metadata:
  name: template-vm-1
  namespace: test-ns
data:
  nameservers: "{{ (index .v1alpha2.Net.Nameservers 0) }}"
  hostname: "{{ .v1alpha2.VM.Name }} "
  management_ip: "{{ (index (index .v1alpha2.Net.Devices 0).IPAddresses 0) }}"
  management_gateway: "{{ (index .v1alpha2.Net.Devices 0).Gateway4 }}"
```

- Verwenden Sie die folgenden Funktionen.

Funktionsname	Signatur	Beschreibung
V1alpha2_FirstIP	func () string	Rufen Sie die erste Nicht-Loopback-IP von der ersten Netzwerkkarte ab.
V1alpha2_FirstIPFromNIC	func (index int) string	Rufen Sie die Nicht-Loopback-IP-Adresse von der ith-Netzwerkkarte ab. Wenn der Index außerhalb des zulässigen Bereichs liegt, wird die Vorlagenzeichenfolge nicht analysiert.
V1alpha2_FormatIP	func (IP string, netmask string) string	Formatieren Sie eine IP-Adresse mit der Netzwerklänge. Eine Netzmaske kann entweder die Länge (z. B. /24) oder die Dezimalschreibweise sein (z. B. 255.255.255.0). Wenn die Eingabenetzmaske ungültig ist oder sich von der Standardmaske unterscheidet, wird sie nicht analysiert.
V1alpha2_FormatNameservers	func (count int, delimiter string) string	Formatieren Sie die erste aufgetretene Anzahl von Namenservern mit einem bestimmten Trennzeichen. Eine negative Zahl als Anzahl bedeutet alle Namenserver.
V1alpha2_IP	func(IP string) string	Formatieren Sie eine statische IP-Adresse mit Standard-Netzmasken-CIDR. Wenn die IP nicht gültig ist, wird die Vorlagenzeichenfolge nicht analysiert.
V1alpha2_IPsFromNIC	func (index int) []string	Listet alle IPs der Ith-Netzwerkkarte auf. Wenn der Index außerhalb des zulässigen Bereichs liegt, wird die Vorlagenzeichenfolge nicht analysiert.

Wenn Sie die Funktionen verwenden, sieht die YAML-Datei wie folgt aus:

```
apiVersion: vmoperator.vmware.com/v1alpha2
kind: VirtualMachine
metadata:
  name: template-vm
  namespace: test-ns
spec:
  className: best-effort-xsmall
  imageName: vmi-xxxx0000
  powerState: poweredOn
  storageClass: wcpglobal-storage-profile
  vmMetadata:
    configMapName: template-vm-2
```

```
    transport: vAppConfig

---
apiVersion: v1
kind: ConfigMap
metadata:
  name: template-vm-2
  namespace: test-ns
data:
  nameservers: "{{ V1alpha2_FormatNameservers 2 \",\" }}"
  hostname: "{{ .v1alpha2.VM.Name }} "
  management_ip: "{{ V1alpha2_FormatIP \"192.168.1.10\" \"255.255.255.0\" }}"
  management_gateway: "{{ (index .v1alpha2.Net.Devices 0).Gateway4 }}"
```

3 Stellen Sie die VM bereit.

```
kubectl apply -f file_name.yaml
```

Nächste Schritte

Wenn die Anpassung fehlschlägt und die VM keine IP-Adresse erhält, überprüfen Sie die VM mithilfe der vSphere VM-Webkonsole. Weitere Informationen hierzu finden Sie unter Fehlerbehebung bei VMs mithilfe der vSphere VM-Web-Konsole.

Überwachen der in vSphere IaaS control plane verfügbaren virtuellen Maschinen

Als vSphere-Administrator verwenden Sie den vSphere Client, um eine VM zu überwachen, die von DevOps in der vSphere IaaS control plane Kubernetes-Umgebung bereitgestellt wurde.

Sie können den VM-Lebenszyklus nicht über den vSphere Client verwalten.

Voraussetzungen

Ein DevOps-Ingenieur hat eine VM bereitgestellt. Siehe *Bereitstellen einer eigenständigen VM in vSphere IaaS control plane*.

Verfahren

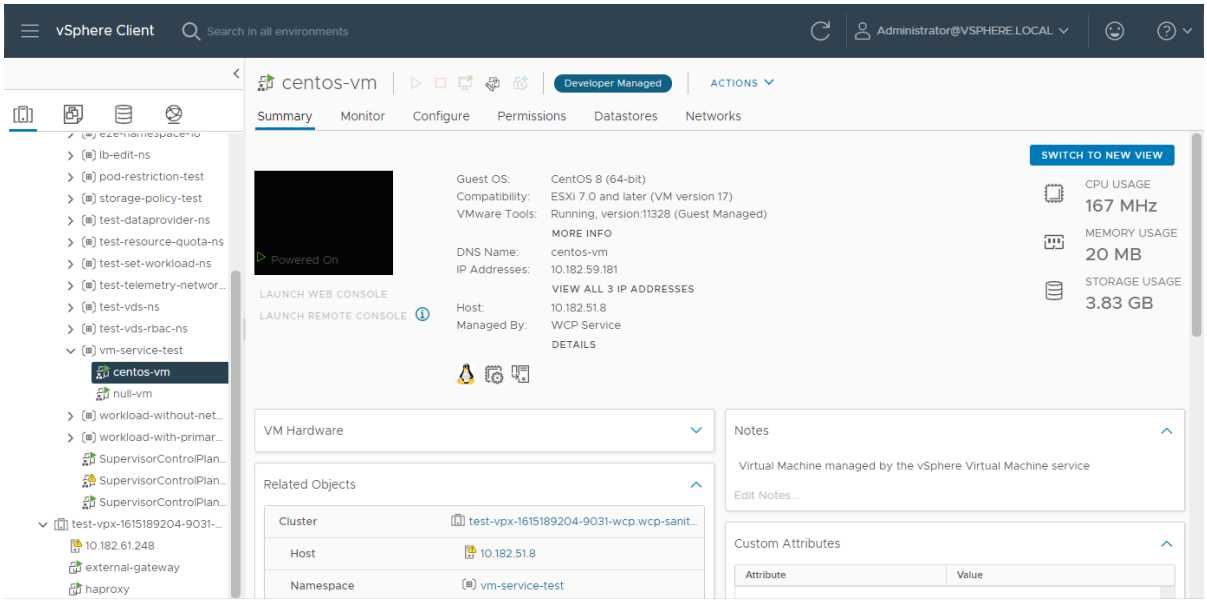
1 Navigieren Sie in vSphere Client zu dem Host-Cluster, für den vSphere IaaS control plane aktiviert ist.

2 Erweitern unter **Namespaces** den Namespace, in dem eine VM bereitgestellt wurde.

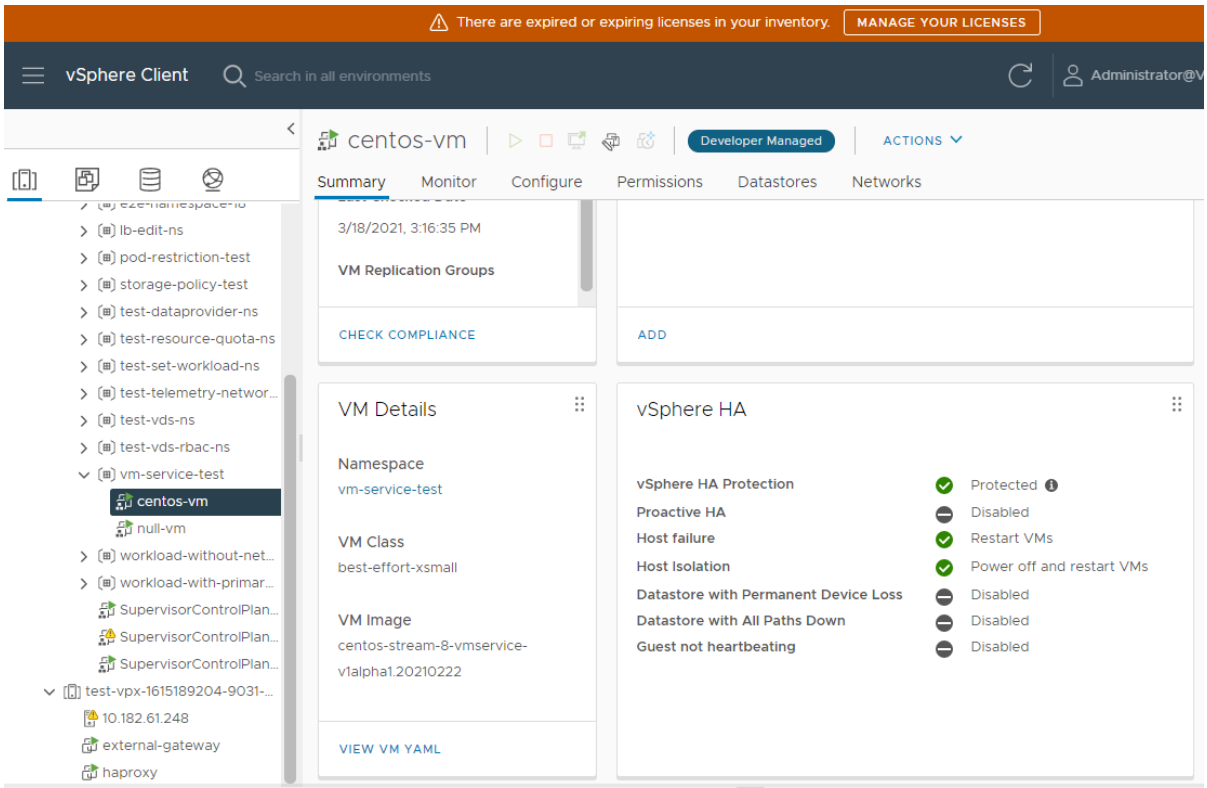
3 Wählen Sie die anzuzeigende VM aus und klicken Sie auf die Registerkarte **Übersicht**.

Vergewissern Sie sich, dass das Tag **Von Entwickler verwaltet** oben auf der Seite **Übersicht** angezeigt wird.

Auf der Seite werden Informationen zur VM angezeigt, einschließlich der jeweiligen Gastbetriebssystem- und IP-Adressen.



4 Klicken Sie oben rechts auf der Seite auf **Zur neuen Ansicht wechseln**, um zusätzliche Details wie die VM-Klasse und das VM-Image sowie den Namespace anzuzeigen, in dem die VM ausgeführt wird.



Fehlerbehebung bei VMs mithilfe der vSphere VM-Web-Konsole

Als DevOps-Techniker können Sie die vSphere VM-Web-Konsole verwenden, um auf problematische VMs zuzugreifen und Fehler zu beheben. Die Verwendung der VM-Web-Konsole kann hilfreich sein, wenn der Zugriff auf VMs nicht über das normale Netzwerk möglich ist, z. B. wenn das Gastbetriebssystem beim ersten Start die korrekten Netzwerkeinstellungen nicht konfigurieren konnte.

Die VM-Webkonsole ist besonders nützlich, wenn Sie VMs mit konfigurierbaren OVF-Eigenschaften bereitstellen. Weitere Informationen finden Sie unter Bereitstellen von VMs mit konfigurierbaren OVF-Eigenschaften in vSphere IaaS control plane.

Voraussetzungen

Verschaffen Sie sich Bearbeitungs- oder Besitzerberechtigungen für den Namespace, in dem die problematische VM bereitgestellt ist. Weitere Informationen finden Sie unter Identitäts- und Zugriffsverwaltung der vSphere IaaS-Steuerungsebene.

Verfahren

1. Greifen Sie in der Kubernetes-Umgebung auf Ihren Namespace zu.

   Weitere Informationen finden Sie unter Abrufen und Verwenden des Supervisor-Kontexts in vSphere IaaS control plane.

2. Stellen Sie sicher, dass die VM bereitgestellt ist.

   ```
   kubectl get vm -n namespace-name
   ```

   Die Ausgabe lautet in etwa wie folgt:

   ```
   NAME      POWERSTATE        AGE
   vm-name   poweredOn         175m
   ```

3. Rufen Sie die URL zur VM-Web-Konsole ab.

   ```
   kubectl vsphere vm web-console vm-name -n namespace-name
   ```

   Hinweis Der Befehl gibt eine authentifizierte URL an die Web-Konsole der VM zurück. Wenn Sie die URL nicht innerhalb eines nicht änderbaren Zeitraums verwenden, der auf zwei Minuten festgelegt ist, läuft die URL ab. Nachdem Sie die URL zum Herstellen einer Verbindung mit der Web-Konsolen-Seite geöffnet haben, wird die Sitzungszeit von WebMKS gesteuert und dauert länger.

4. Klicken Sie auf die URL und führen Sie alle erforderlichen Fehlerbehebungsaktionen für Ihre VM durch.

Bereitstellen von Arbeitslasten in vSphere-Pods

7

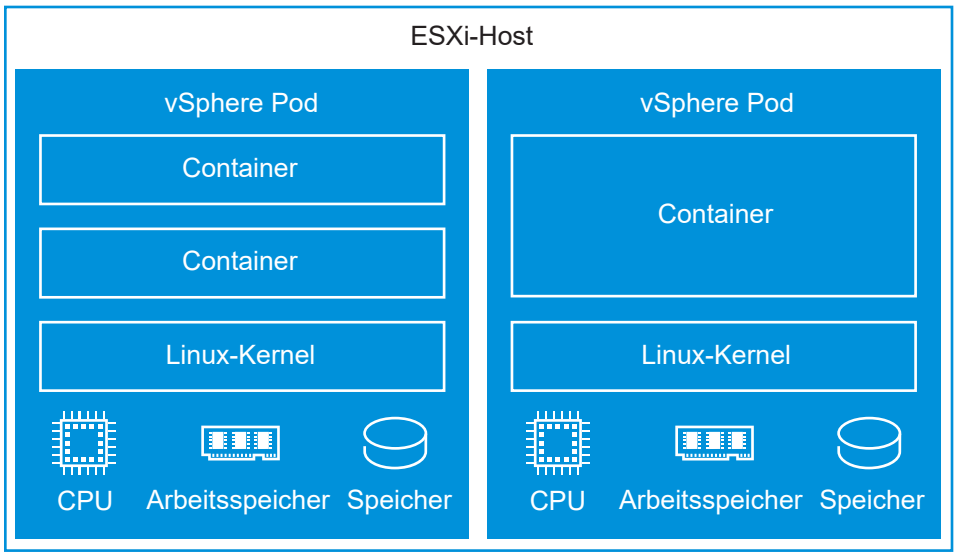
Als DevOps-Ingenieur können Sie den Lebenszyklus von vSphere-Pods innerhalb der Ressourcengrenzen eines auf einem Supervisor ausgeführten vSphere-Namespace bereitstellen und verwalten.

Hinweis Sie können vSphere-Pods nur auf Supervisoren bereitstellen, die mit dem NSX-Netzwerk-Stack konfiguriert sind. Sie können keine vSphere Pods auf Supervisoren bereitstellen, die mit dem VDS-Stack konfiguriert sind. Supervisor-Dienste werden auf beiden Supervisoren unterstützt, die mit NSX oder VDS konfiguriert sind, und sie stellen vSphere-Pods für die eigene Verwendung bereit. Sie können jedoch keine vSphere-Pods für die allgemeine Verwendung auf einem mit VDS konfigurierten Supervisor bereitstellen.

Was ist ein vSphere Pod?

vSphere IaaS control plane führt ein Konstrukt mit dem Namen vSphere Pod ein, das einem Kubernetes-Pod entspricht. Eine vSphere Pod ist eine VM mit einem kleinen Footprint, die einen oder mehrere Linux-Container ausführt. Jede vSphere Pod wird genau für die Arbeitslast angepasst, die sie unterstützt, und weist explizite Ressourcenreservierungen für diese Arbeitslast auf. Sie weist die genaue Menge an Speicherplatz, Arbeitsspeicher und CPU-Ressourcen zu, die für die Ausführung der Arbeitslast erforderlich ist. vSphere-Pods werden nur mit Supervisoren unterstützt, die mit NSX als Netzwerk-Stack konfiguriert sind.

Abbildung 7-1. vSphere-Pods



vSphere-Pods sind Objekte in vCenter Server. Sie ermöglichen die folgenden Funktionen für Arbeitslasten:

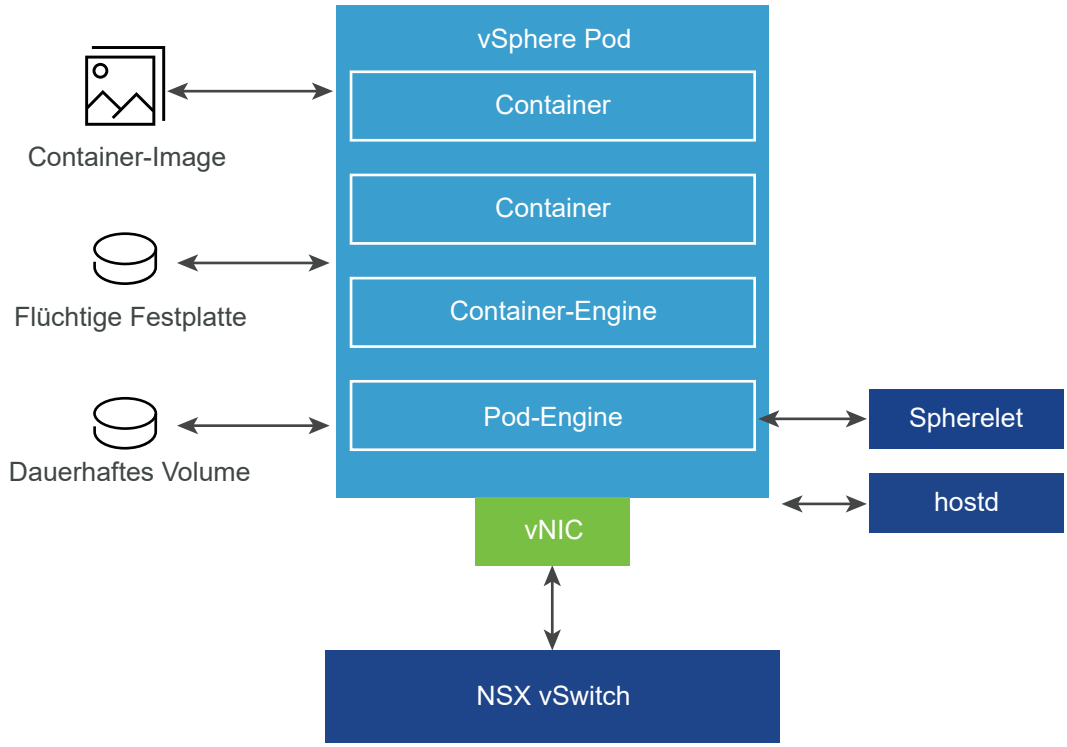
- Starke Isolierung. Ein vSphere Pod wird in gleicher Weise wie eine virtuelle Maschine isoliert. Jeder vSphere Pod hat seinen eigenen Linux-Kernel, der auf dem im Photon OS verwendeten Kernel basiert. Statt dass viele Container einen Kernel teilen, wie in einer Bare-Metal-Konfiguration, hat in einem vSphere Pod jeder Container einen eindeutigen Linux-Kernel.
- Ressourcenverwaltung. vSphere DRS übernimmt die Platzierung von vSphere-Pods im Supervisor.
- Hochleistung. vSphere-Pods erhalten die gleiche Ressourcenisolierung wie VMs und eliminieren Störungen durch benachbarte Elemente, während die schnelle Startzeit und der geringe Overhead von Containern beibehalten werden.
- Diagnose. Als vSphere-Administrator können Sie alle Überwachungs- und Selbstprüfungs-Tools verwenden, die in vSphere für Arbeitslasten verfügbar sind.

vSphere-Pods sind OCI-kompatibel (Open Container Initiative) und können Container von jedem Betriebssystem aus ausführen, solange diese Container ebenfalls OCI-kompatibel sind.

Richtlinien zur Bereitstellung von vSphere-Pods

Stellen Sie vor der Bereitstellung von vSphere-Pods sicher, dass die Umgebung die unterstützten Anforderungen erfüllt.

Abbildung 7-2. vSphere Pod Netzwerk und Speicher



Namespace

Ihre Supervisoren müssen über einen konfigurierten vSphere-Namespace mit Bearbeitungs- oder Besitzerberechtigungen verfügen. Nur Ein-Zonen-Supervisoren mit NSX-Netzwerk unterstützen vSphere-Pods.

Informationen zum Erstellen eines Supervisors finden Sie unter Bereitstellen eines Supervisors für eine Zone mit NSX-Netzwerk.

Informationen zum Erstellen eines Namespace finden Sie unter Erstellen und Konfigurieren eines vSphere-Namespace im Supervisor..

Informationen zum Zuweisen von Berechtigungen finden Sie unter Identitäts- und Zugriffsverwaltung.

Netzwerk

Für Netzwerke nutzen vSphere-Pods die von NSX bereitgestellte Topologie. Weitere Informationen finden Sie unter Supervisor-Netzwerk.

Spherelet ist ein zusätzlicher Prozess, der auf jedem Host erstellt wird. Es handelt sich um ein Kubelet, das nativ auf ESXi portiert wird und dem ESXi-Host ermöglicht, Teil des Kubernetes-Clusters zu werden.

Speicher

vSphere-Pods verwenden drei Speichertypen, je nachdem, welche Objekte gespeichert sind: flüchtige VMDKs, dauerhafte Volume-VMDKs und Container-Image-VMDKs.

Als vSphere-Administrator konfigurieren Sie Speicherrichtlinien für die Platzierung von Container-Image-Cache und flüchtigen VMDKs, wenn Sie die Supervisor aktivieren.

Auf vSphere-Namespace-Ebene konfigurieren Sie Speicherrichtlinien für die Platzierung persistenter Volumes. Weitere Informationen zu den Speicheranforderungen und Konzepten für vSphere IaaS control plane finden Sie unter Kapitel 8 Verwenden von persistentem Speicher mit Supervisor-Arbeitslasten in vSphere IaaS control plane.

Lesen Sie als Nächstes die folgenden Themen:

- Abrufen und Verwenden des Supervisor-Kontexts in vSphere IaaS control plane
- Bereitstellen einer Anwendung auf einem vSphere Pod für einen vSphere-Namespace
- Skalieren einer vSphere Pod-Anwendung
- Bereitstellen eines vertraulichen vSphere Pods
- vSphere Pod-Arbeitslastbereitstellung in vSphere IaaS control plane

Abrufen und Verwenden des Supervisor-Kontexts in vSphere IaaS control plane

Nachdem Sie vom vSphere-Administrator die IP-Adresse der Kubernetes-Steuerungsebene im Supervisor erhalten haben, können Sie sich beim Supervisor anmelden und die Kontexte abrufen, auf die Sie Zugriff haben. In vSphere IaaS control plane entsprechen Kontexte den Namespaces im Supervisor.

Nach der Anmeldung beim Supervisor generiert das vSphere-Plug-In für kubectl den Kontext für den Cluster. In Kubernetes enthält ein Konfigurationskontext einen Cluster, einen 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 vorhandene `kubeconfig`-Datei verfügen, wird sie an jeden Clusterkontext 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

- Rufen Sie Ihre vCenter Single Sign-On-Anmeldedaten ab.
- Rufen Sie die IP-Adresse der Supervisor-Steuerungsebene ab.
- Rufen Sie den Namen des vSphere-Namespace ab.
- Lassen Sie sich bestätigen, dass Sie Berechtigungen des Typs **Bearbeiten** für den vSphere-Namespace haben.

- Laden Sie die Kubernetes-CLI-Tools für vSphere herunter und installieren Sie sie. Informationen finden Sie in der Dokumentation *Installieren und Konfigurieren der vSphere IaaS-Steuerungsebene*.
- 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 finden Sie in der Dokumentation zu *Installieren und Konfigurieren der vSphere IaaS-Steuerungsebene* unter Konfigurieren der sicheren Anmeldung für vSphere IaaS-Steuerungsebenen-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>
```

Beispiel:

```
kubectl vsphere login --server=10.92.42.13 --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

Informationen zum Herstellen einer Verbindung mit einem Tanzu Kubernetes Grid-Cluster finden Sie in *Verwenden des TKG-Dienstes mit der vSphere IaaS-Steuerungsebene* unter Herstellen einer Verbindung mit einem TKG-Cluster als vCenter Single Sign-On-Benutzer.

Bereitstellen einer Anwendung auf einem vSphere Pod für einen vSphere-Namespace

Sie können eine Anwendung auf einem vSphere-Namespace in vSphere IaaS control plane bereitstellen. Sobald die Anwendung bereitgestellt wurde, wird die entsprechende Anzahl von vSphere-Pods im Supervisor innerhalb des Namespace erstellt.

Voraussetzungen

- Bitten Sie den vSphere-Administrator um die IP-Adresse für die Kubernetes-Steuerungsebene im Supervisor.
- Richten Sie Ihr Benutzerkonto in vCenter Single Sign-On ein.
- Stellen Sie mit Ihrem vSphere-Administrator sicher, dass Sie über die Berechtigungen für den Zugriff auf den von Ihnen benötigten Kontext verfügen.

Verfahren

1. Greifen Sie in der Kubernetes-Umgebung auf Ihren Namespace zu.

   Weitere Informationen finden Sie unter Abrufen und Verwenden des Supervisor-Kontexts in vSphere IaaS control plane.

2. Wechseln Sie zu dem Kontext, in dem Sie die Anwendung bereitstellen möchten.

   ```
   kubectl config use-context <namespace>
   ```

3. Stellen Sie die Anwendung bereit.

   ```
   kubectl apply -f <application name>.yaml
   ```

Skalieren einer vSphere Pod-Anwendung

Sie können die Anzahl der Replikate für jede Anwendung, die auf einem Supervisor in einem vSphere IaaS control plane ausgeführt wird, vertikal hoch- und herunterskalieren.

Voraussetzungen

- Bitten Sie den vSphere-Administrator um die IP-Adresse für die Kubernetes-Steuerungsebene im Supervisor.
- Richten Sie Ihr Benutzerkonto in vCenter Single Sign-On ein.

- Stellen Sie mit Ihrem vSphere-Administrator sicher, dass Sie über die Berechtigungen für den Zugriff auf den von Ihnen benötigten Kontext verfügen.

Verfahren

1 Authentifizieren Sie sich beim Supervisor.

```
kubectl vsphere login --server <control plane load balancer IP address> --vsphere-username
<vSphere user account name>
```

2 Skalieren Sie eine Anwendung vertikal hoch oder herunter.

```
kubectl get deployments
kubectl scale deployment <deployment-name> --replicas=<number-of-replicas>
```

Bereitstellen eines vertraulichen vSphere Pods

Mit vSphere IaaS control plane können Sie vertrauliche vSphere-Pods auf einem Supervisor ausführen. Ein vertraulicher vSphere Pod verwendet eine Hardwaretechnologie, mit der der Arbeitsspeicher des Gastbetriebssystem verschlüsselt bleibt und vor dem Zugriff durch den Hypervisor geschützt wird.

Sie können vertrauliche vSphere-Pods erstellen, indem Sie SEV-ES (Secure Encrypted Virtualization-Encrypted State) als zusätzliche Sicherheitserweiterung hinzufügen. SEV-ES verhindert, dass CPU-Register Informationen aus Registern an Komponenten wie den Hypervisor weitergeben. SEV-ES kann auch böswillige Änderungen an einem CPU-Registerzustand erkennen. Weitere Informationen zur Verwendung der SEV-ES-Technologie in der vSphere-Umgebung finden Sie in der Dokumentation zum Thema *vSphere-Sicherheit* unter Sichern von virtuellen Maschinen mit AMD Secure Encrypted Virtualization-Encrypted State.

Voraussetzungen

Um SEV-ES auf einem ESXi zu aktivieren, muss ein vSphere-Administrator die folgenden Richtlinien befolgen:

- Verwenden Sie die Hosts, die die SEV-ES-Funktionalität unterstützen.
- Verwenden Sie ESXi Version von 7.0 Update 2 oder höher.
- Aktivieren Sie SEV-ES in der BIOS-Konfiguration eines ESXi-Systems. In der Systemdokumentation finden Sie weitere Informationen zum Zugriff auf die BIOS-Konfiguration.
- Geben Sie bei Aktivierung von SEV-ES im BIOS einen Wert für die Einstellung **Mindestanzahl SEV-Nicht-ES-ASID** ein, die der Anzahl an SEV-ES-VMs und vertraulichen vSphere-Pods-Host plus eins entspricht. Wenn Sie beispielsweise 100 SEV-ES-VMs und 128 VMs vSphere-Pods ausführen möchten, geben Sie mindestens 229 ein. Sie können eine Einstellung bis zu 500 eingeben.

Verfahren

1 Erstellen Sie eine YAML-Datei, die die folgenden Parameter enthält.

a Aktivieren Sie unter Anmerkungen die Funktion für vertrauliche vSphere-Pods.

```
...
annotations:
        vmware/confidential-pod: enabled
...
```

b Geben Sie Arbeitsspeicherressourcen für Container an.

Stellen Sie sicher, dass Arbeitsspeicheranforderungen und Arbeitsspeichergrenzwerte auf denselben Wert festgelegt werden, wie in diesem Beispiel.

```
resources:
      requests:
        memory: "512Mi"
      limits:
        memory: "512Mi"
```

Verwenden Sie die folgende YAML-Datei als Beispiel:

```
apiVersion: v1
kind: Pod
metadata:
  name: photon-pod
  namespace: my-podvm-ns
  annotations:
    vmware/confidential-pod: enabled
spec:  # specification of the pod's contents
  restartPolicy: Never
  containers:
  - name: photon
    image: wcp-docker-ci.artifactory.eng.vmware.com/vmware/photon:1.0
    command: ["/bin/sh"]
    args:    ["-c", "while true; do echo hello, world!; sleep 1; done"]
    resources:
      requests:
        memory: "512Mi"
      limits:
        memory: "512Mi"
```

2 Melden Sie sich beim Supervisor an.

```
kubectl vsphere login --server=https://<server_adress> --vsphere-username <your user
account name>
```

3 Wechseln Sie zu dem Namespace, in dem Sie die Anwendung bereitstellen möchten.

```
kubectl config use-context <namespace>
```

4 Stellen Sie eine vertrauliche vSphere Pod aus der YAML-Datei bereit:

```
kubectl apply -f <yaml file name>.yaml
```

Hinweis Wenn die vSphere Pod bereitgestellt ist, platziert DRS sie auf dem ESXi-Knoten, der SEV-ES unterstützt. Wenn kein solcher Knoten verfügbar ist, wird die vSphere Pod als fehlgeschlagen gekennzeichnet.

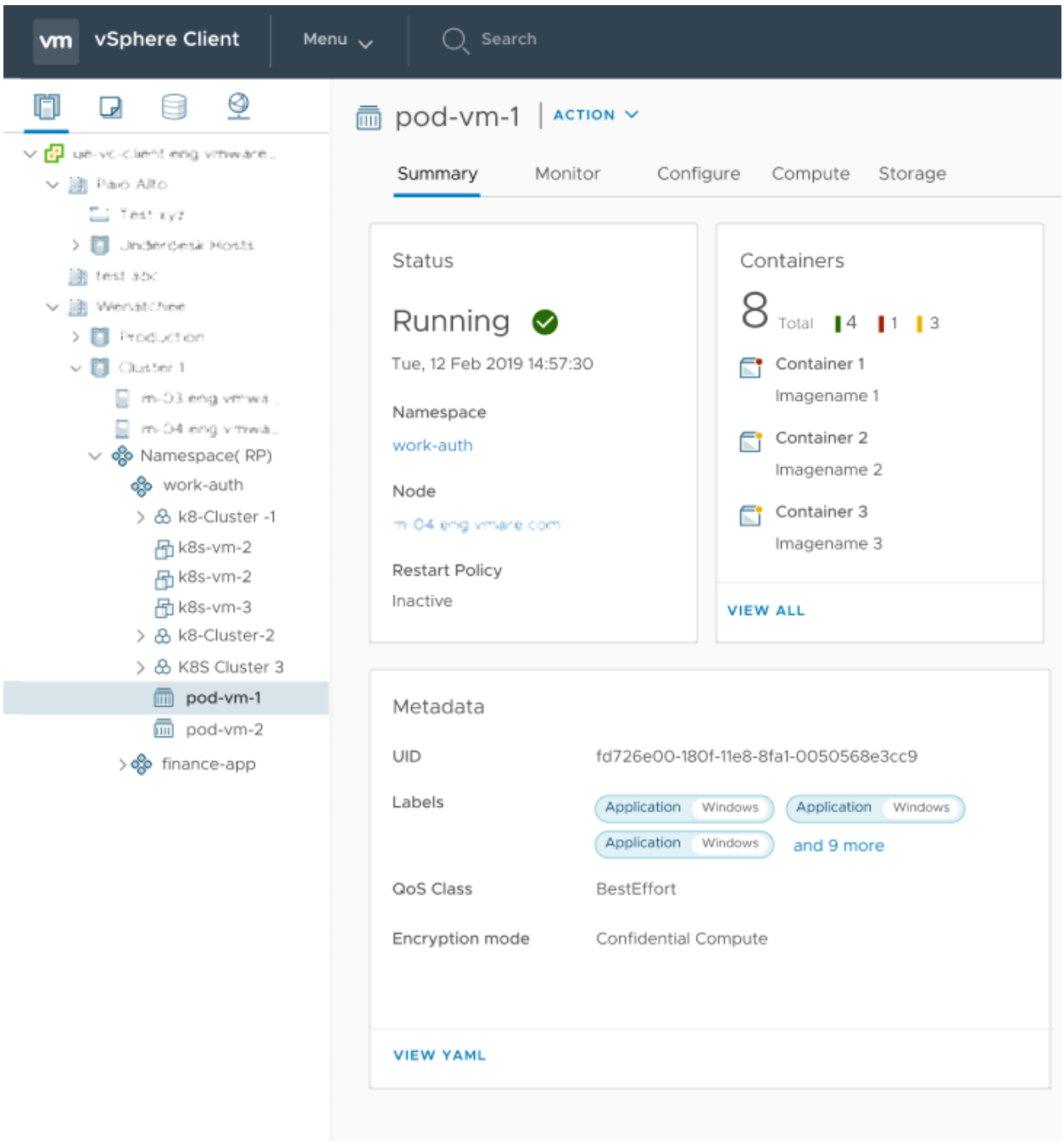
Die gestartete vertrauliche vSphere Pod bietet eine Untesrtützung der Hardware-Arbeitsspeicherverschlüsselung für alle Arbeitslasten, die auf diesem Pod ausgeführt werden.

5 Führen Sie den folgenden Befehl aus, um sicherzustellen, dass die vertrauliche vSphere Pod erstellt wurde.

```
kubectl describe pod/<yaml name>
```

Nächste Schritte

Ein vSphere-Administrator kann die vertrauliche vSphere Pod einsehen. Im vSphere Client wird sie mit dem Tag **Verschlüsselungsmodus: Vertrauliches Berechnen** angezeigt.



vSphere Pod-Arbeitslastbereitstellung in vSphere IaaS control plane

In diesem Beispiel-Lernprogramm wird die Bereitstellung der WordPress-Anwendung mithilfe von vSphere-Pods in der vSphere IaaS control plane-Umgebung beschrieben.

Die WordPress-Bereitstellung umfasst Container für das WordPress-Frontend und das MySQL-Back-End sowie Dienste für beides. Geheimschlüsselobjekte sind ebenfalls erforderlich.

In diesem Lernprogramm wird ein Bereitstellungsobjekt verwendet. In einer Produktionsumgebung sollten Sie normalerweise StatefulSets sowohl für WordPress- als auch für MySQL-Container verwenden.

Voraussetzungen

- Erstellen Sie einen Supervisor für eine Zone mit NSX-Netzwerk. Nur Supervisoren für eine Zone mit NSX unterstützen vSphere-Pods. Weitere Informationen finden Sie unter Bereitstellen eines Supervisors für eine Zone mit NSX-Netzwerk
- Erstellen Sie einen Namespace für die Bereitstellung von vSphere-Pods. Weitere Informationen hierzu finden Sie unter Erstellen und Konfigurieren eines vSphere-Namespace im Supervisor..
- Erstellen Sie eine Speicherrichtlinie, zum Beispiel `vwt-storage-policy`, und weisen Sie sie dem Namespace zu.
- Laden Sie die vSphere Kubernetes-CLI-Tools herunter. Weitere Informationen finden Sie unter Herunterlade und Installieren der Kubernetes-CLI-Tools für vSphere.
- Erstellen Sie die für dieses Lernprogramm erforderlichen YAML-Dateien und überprüfen Sie den Befehlszeilenzugriff auf die Dateien.

Kategorie	Dateien
Speicher	■ mysql-pvc.yaml ■ wordpress-pvc.yaml **Hinweis** Stellen Sie sicher, dass die Dateien auf die richtige Speicherklasse verweisen.
Geheimnisse	■ regcred.yaml ■ mysql-pass.yaml
Dienste	■ mysql-service.yaml ■ wordpress-service.yaml
Bereitstellungen	■ mysql-deployment-vsphere-pod.yaml ■ wordpress-deployment.yaml

WordPress bereitstellen

Verwenden Sie diesen Workflow, um die WordPress-Anwendung mithilfe von vSphere-Pods bereitzustellen.

Teil 1. Zugreifen auf Ihren Namespace

Führen Sie diese Schritte aus, um auf Ihren Namespace zuzugreifen.

Verfahren

1 Melden Sie sich beim Supervisor an.

```
kubectl vsphere login --server=SVC-IP-ADDRESS --vsphere-username wcp-user@vsphere.local
```

2 Führen Sie einen Kontextwechsel zum vSphere-Namespace durch.

```
kubectl config use-context VSPHERE-PODS-NAMESPACE
```

3 Stellen Sie sicher, dass die von Ihnen erstellte Speicherrichtlinie `vwt-storage-policy` im Namespace als Speicherklasse verfügbar ist.

Weitere Informationen hierzu finden Sie unter Anzeigen von Speicherklassen in einem vSphere-Namespace.

Teil 2. WordPress-PVCs erstellen

Verwenden Sie diese Befehle, um WordPress-PVCs zu erstellen.

Verfahren

1 Erstellen Sie die MySQL-PVC.

```
kubectl apply -f mysql-pvc.yaml
```

2 Erstellen Sie die WordPress-PVC.

```
kubectl apply -f wordpress-pvc.yaml
```

3 Verifizieren Sie die PVCs.C

```
kubectl get pvc,pv
```

Teil 3. Geheimnisse erstellen

Der öffentliche Docker-Hub ist die standardmäßige Containerregistrierung für Kubernetes. Docker-Hub schränkt jetzt Image-Abrufe ein. Sie müssen über ein bezahltes Konto verfügen und den Kontoschlüssel zur geheimen YAML im Feld `data.dockerconfigjson` hinzufügen.

Verfahren

1 Erstellen Sie den geheimen Registrierungsschlüssel für Docker-Hub.

```
kubectl apply -f regcred.yaml
```

2 Erstellen Sie den geheimen mysql-Kennwortschlüssel.

Das MySQL-DB-Kennwort ist erforderlich. Innerhalb des geheimen Schlüssels muss das Kennwort base64-codiert sein.

```
kubectl apply -f mysql-pass.yaml
```

3 Verifizieren Sie die Geheimnisse.

```
kubectl get secrets
```

Teil 4. Dienste erstellen

Folgen Sie diesen Schritten, um Dienste zu erstellen.

Verfahren

1 Erstellen Sie den MySQL-Dienst.

```
kubectl apply -f mysql-service.yaml
```

2 Erstellen Sie den WordPress-Service.

```
kubectl apply -f wordpress-service.yaml
```

3 Verifizieren Sie die Dienste.

```
kubectl get services
```

Teil 5. Pod-Bereitstellungen erstellen

Verwenden Sie diese Aufgabe, um Pod-Bereitstellungen zu erstellen.

In diesem Lernprogramm werden Bereitstellungsobjekte verwendet. In einer Produktionsumgebung sollten Sie StatefulSets sowohl für WordPress- als auch für MySQL-Container verwenden.

Verfahren

1 Erstellen Sie die MySQL-Bereitstellung.

```
kubectl apply -f mysql-deployment-vsphere-pod.yaml
```

Hinweis Wenn ein vSphere Pod erstellt wird, erstellt das System eine VM für die Container im Pod. Standardmäßig hat die VM einen RAM-Grenzwert von 512 MB. Der MySQL-Container benötigt mehr Arbeitsspeicher. Die Spezifikation `mysql-deployment-vsphere-pod.yaml` für die Pod-Bereitstellung enthält einen Abschnitt, der den Arbeitsspeicher erhöht, der der vSphere Pod-VM zugewiesen ist. Wenn Sie diesen Abschnitt nicht einschließen, schlägt die Pod-Bereitstellung mit einer Ausnahme aufgrund von nicht genügend Arbeitsspeicher (OOM) fehl. Sie müssen den Arbeitsspeicher nicht erhöhen, wenn Sie einen MySQL-Pod in einem TKG-Cluster bereitstellen.

2 Erstellen Sie die WordPress-Bereitstellung.

```
kubectl apply -f wordpress-deployment.yaml
```

3 Verifizieren Sie die Bereitstellung.

```
kubectl get deployments
```

Teil 6. WordPress testen

Folgen Sie diesen Schritten, um Ihre WordPress-Installation zu testen.

Verfahren

1 Stellen Sie sicher, dass alle Objekte erstellt wurden und ausgeführt werden.

```
kubectl get pv,pvc,secrets,rolebinding,services,deployments,pods
```

2 Rufen Sie die EXTERNAL-IP-Adresse vom WordPress-Dienst ab.

```
kubectl get service wordpress

NAME        TYPE           CLUSTER-IP    EXTERNAL-IP     PORT(S)        AGE
wordpress   LoadBalancer   10.96.9.180   10.197.154.73   80:30941/TCP   87s
```

3 Rufen Sie die EXTERNAL-IP-Adresse auf.

4 Konfigurieren Sie die WordPress-Instanz.

Benutzername: administrator

Kennwort: Verwenden Sie das angegebene sichere Kennwort

Beispiel-YAML-Dateien für die WordPress-Bereitstellung

Verwenden Sie diese Beispiel-YAML-Dateien, wenn Sie die WordPress-Anwendung mit vSphere-Pods bereitstellen.

mysql-pvc.yaml

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: mysql-pvc
  labels:
    app: wordpress
spec:
  accessModes:
    - ReadWriteOnce
  storageClassName: vwt-storage-policy
  resources:
    requests:
      storage: 20Gi
```

wordpress-pvc.yaml

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: wordpress-pvc
  labels:
    app: wordpress
```

```
spec:
  accessModes:
    - ReadWriteOnce
  storageClassName: vwt-storage-policy
  resources:
    requests:
      storage: 20Gi
```

regcred.yaml

```
apiVersion: v1
kind: Secret
metadata:
  name: regcred
data:
  .dockerconfigjson: ewoJImF1dGhzIjog....zZG1KcE5WUmtXRUozWpc
type: kubernetes.io/dockerconfigjson
```

mysql-pass.yaml

```
apiVersion: v1
data:
  password: YWRtaW4=  #admin base64 encoded
kind: Secret
metadata:
  name: mysql-pass
```

mysql-service.yaml

```
apiVersion: v1
kind: Service
metadata:
  name: wordpress-mysql
  labels:
    app: wordpress
spec:
  ports:
    - port: 3306
  selector:
    app: wordpress
    tier: mysql
  clusterIP: None
```

wordpress-service.yaml

```
apiVersion: v1
kind: Service
metadata:
  name: wordpress
  labels:
    app: wordpress
spec:
```

```
  ports:
    - port: 80
  selector:
    app: wordpress
    tier: frontend
  type: LoadBalancer
```

mysql-deployment-vsphere-pod.yaml

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: wordpress-mysql
  labels:
    app: wordpress
spec:
  replicas: 1
  strategy:
    type: Recreate
  selector:
    matchLabels:
      app: wordpress
      tier: mysql
  template:
    metadata:
      labels:
        app: wordpress
        tier: mysql
    spec:
      containers:
      - image: mysql:5.6
        name: mysql
        #increased resource limits required for this pod vm
        #default pod VM RAM is 512MB; MySQL container needs more
        #without extra RAM OOM error prevents deployment
        #extra RAM not required for Kuberentes cluster
        resources:
          limits:
            memory: 1024Mi
            cpu: 1
        env:
        - name: MYSQL_ROOT_PASSWORD
          valueFrom:
            secretKeyRef:
              name: mysql-pass
              key: password
        ports:
        - containerPort: 3306
          name: mysql
        volumeMounts:
        - name: mysql-persistent-storage
          mountPath: /var/lib/mysql
      volumes:
      - name: mysql-persistent-storage
```

```
        persistentVolumeClaim:
          claimName: mysql-pvc
      imagePullSecrets:
      - name: regcred
```

wordpress-deployment.yaml

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: wordpress
  labels:
    app: wordpress
spec:
  selector:
    matchLabels:
      app: wordpress
      tier: frontend
  strategy:
    type: Recreate
  template:
    metadata:
      labels:
        app: wordpress
        tier: frontend
    spec:
      containers:
      - image: wordpress:4.8-apache
        name: wordpress
        env:
        - name: WORDPRESS_DB_HOST
          value: wordpress-mysql
        - name: WORDPRESS_DB_PASSWORD
          valueFrom:
            secretKeyRef:
              name: mysql-pass
              key: password
        ports:
        - containerPort: 80
          name: wordpress
        volumeMounts:
        - name: wordpress-persistent-storage
          mountPath: /var/www/html
      volumes:
      - name: wordpress-persistent-storage
        persistentVolumeClaim:
          claimName: wordpress-pvc
      imagePullSecrets:
      - name: regcred
```

Verwenden von persistentem Speicher mit Supervisor-Arbeitslasten in vSphere IaaS control plane

8

Bestimmte Kubernetes-Arbeitslasten, die mit DevOps in einem Namespace in Supervisor ausführt, benötigen dauerhaften Speicher zum Speichern von Daten. Dauerhafter Speicher kann von vSphere-Pods, Tanzu Kubernetes Grid-Clustern, VMs und anderen Arbeitslasten verwendet werden, die Sie im Namespace ausführen.

Um dem DevOps-Team dauerhaften Speicher zur Verfügung zu stellen, erstellt der vSphere-Administrator Speicherrichtlinien, die verschiedene Speicheranforderungen und Dienstklassen beschreiben. Der Administrator weist anschließend Speicherrichtlinien zu und konfiguriert Speichergrenzwerte auf Namespace-Ebene.

Um zu verstehen, wie vSphere IaaS control plane mit dauerhaftem Speicher funktioniert, machen Sie sich mit den grundlegenden Kubernetes-Konzepten wie Speicherklassen, dauerhaften Volumes und Beanspruchungen dauerhafter Volumes vertraut. Weitere Informationen dazu finden Sie in der Kubernetes-Dokumentation unter https://kubernetes.io/docs/home/.

Informationen zur Integration von vSphere IaaS control plane-Komponenten in Speicher finden Sie unter Supervisor-Speicher in *Konzepte und Planung der vSphere IaaS-Steuerungsebene*.

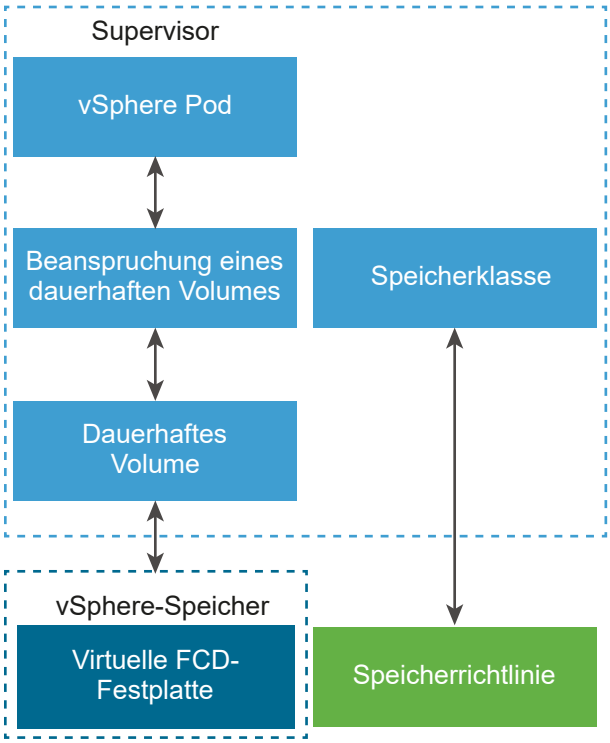
Workflow für dauerhaften Speicher

Der Workflow für die Bereitstellung von persistentem Speicher in vSphere IaaS control plane umfasst in der Regel die folgenden nacheinander erfolgenden Aktionen.

Aktion	Durchgeführt von	Beschreibung
Stellt dem DevOps-Team dauerhafte Speicherressourcen bereit.	vSphere-Administrator	Ein vSphere-Administratoren erstellt Speicherrichtlinien, die unterschiedliche Speicheranforderungen und Dienstklassen beschreiben. Entsprechende Informationen finden Sie in der *Installieren und Konfigurieren der vSphere IaaS-Steuerungsebene* im Thema über das Erstellen von Speicherrichtlinien für die vSphere IaaS-Steuerungsebene. Der Administrator weist die Speicherrichtlinien dann einem Namespace zu und legt Speichergrenzwerte für den Namespace fest. Weitere Informationen hierzu finden Sie unter Erstellen und Konfigurieren eines vSphere-Namespace im Supervisor..
Erstellt Speicherklassen im Namespace	vSphere IaaS control plane	Die Speicherklassen, die den dem Namespace zugewiesenen Speicherrichtlinien entsprechen, werden automatisch in der Kubernetes-Umgebung angezeigt. Wenn der vSphere-Administrator dem Namespace mehrere Speicherrichtlinien zuweist, wird für jede Speicherrichtlinie eine separate Speicherklasse erstellt. Wenn Sie die Tanzu Kubernetes Grid-Cluster verwenden, erbt jeder Cluster Speicherklassen vom Namespace, in dem der Cluster bereitgestellt wird. Das DevOps-Team kann die Speicherklassen für ihre dauerhaften Speicheranforderungen verwenden. Weitere Informationen finden Sie unter Anzeigen von Speicherklassen in einem vSphere-Namespace.

Aktion	Durchgeführt von	Beschreibung
Anforderungen an dauerhafte Speicherressourcen für eine Arbeitslast	DevOps	Das DevOps-Team verwendet die Speicherklassen, um dauerhafte Speicherressourcen für eine Arbeitslast anzufordern. Die Anforderung erfolgt in Form eines Anspruchs für ein dauerhaftes Volume, der auf eine bestimmte Speicherklasse verweist. Weitere Informationen finden Sie unter Bereitstellen eines dynamischen dauerhaften Volumes in vSphere IaaS control plane und Bereitstellen einer eigenständigen VM in vSphere IaaS control plane.
Erstellt ein dauerhaftes Volume-Objekt und eine entsprechende dauerhafte virtuelle Festplatte für eine Arbeitslast.	vSphere IaaS control plane	vSphere IaaS control plane platziert die virtuelle Festplatte in den Datenspeicher, der die in der ursprünglichen Speicherrichtlinie angegebenen Anforderungen und die zugehörige Speicherklasse erfüllt. Die virtuelle Festplatte kann durch eine Arbeitslast gemountet werden.
Überwachen dauerhafter Volumes	vSphere-Administrator	Mithilfe des vSphere Client überwachen vSphere-Administratoren die dauerhaften Volumes und ihre zugrunde liegenden virtuellen Festplatten. Sie können auch die Speicherübereinstimmung und den Systemzustand der dauerhaften Volumes überwachen. Weitere Informationen finden Sie unter Überwachen von dauerhaften Volumes im vSphere Client.

Im Folgenden wird veranschaulicht, wie ein dauerhaftes Volume-Objekt und eine übereinstimmende dauerhafte virtuelle FCD-Festplatte für ein vSphere Pod erstellt werden. Der Anspruch für dauerhaften Speicher verweist auf eine bestimmte Speicherklasse.



Lesen Sie als Nächstes die folgenden Themen:

- Anzeigen von Speicherklassen in einem vSphere-Namespace
- Bereitstellen eines dynamischen dauerhaften Volumes in vSphere IaaS control plane
- Bereitstellen eines statischen persistenten Volumes in vSphere IaaS control plane
- Verwenden des vSAN-Dateidiensts zum Erstellen von ReadWriteMany-Volumes in vSphere IaaS control plane
- Erweiterung von Volumes in vSphere IaaS control plane
- Überwachen von dauerhaften Volumes im vSphere Client
- Überwachen der Volume-Integrität in einem vSphere-Namespace oder Tanzu Kubernetes Grid-Cluster
- Best Practices für die Verwendung von persistentem Speicher auf einem Supervisor mit drei Zonen

Anzeigen von Speicherklassen in einem vSphere-Namespace

Nachdem ein vSphere-Administrator eine Speicherrichtlinie erstellt und dem vSphere-Namespace in vSphere IaaS control plane zugewiesen hat, wird die Speicherrichtlinie als übereinstimmende Kubernetes-Speicherklasse im vSphere-Namespace angezeigt. Sie wird auch auf alle verfügbaren Tanzu Kubernetes Grid-Cluster repliziert. Als DevOps-Ingenieur können Sie sicherstellen, dass die Speicherklasse verfügbar ist.

Ob Sie Befehle ausführen können, hängt von Ihren Berechtigungen ab.

Voraussetzungen

Stellen Sie sicher, dass Ihr vSphere-Administrator eine geeignete Speicherrichtlinie erstellt und dem vSphere-Namespace die Richtlinie zugewiesen hat.

Verfahren

1 Verwenden Sie einen der folgenden Befehle, um zu überprüfen, ob die Speicherklassen verfügbar sind:

- **`kubectl get storageclass`**

  Hinweis Dieser Befehl ist nur für einen Benutzer mit Administratorrechten verfügbar.

  Sie erhalten eine Ausgabe ähnlich der Folgenden: Der Name der Speicherklasse stimmt mit dem Namen der Speicherrichtlinie in vSphere überein.

```
NAME     PROVISIONER              AGE
silver   csi.vsphere.vmware.com   2d
gold     csi.vsphere.vmware.com   1d
```

- **`kubectl describe namespace`** ***`namespace_name`***

  Der Name der Speicherklasse wird in der Ausgabe als Teil des Parameters ***`storageclass_name`*****`.storageclass.storage.k8s.io/requests.storage`** angezeigt. Beispiel:

```
-----------------
Name:                                                                 namespace_name
 Resource                                                              Used  Hard
 --------                                                              ---   ---
 silver.storageclass.storage.k8s.io/requests.storage                   1Gi
9223372036854775807
 gold.storageclass.storage.k8s.io/requests.storage                     0
9223372036854775807
```

2 Führen Sie den folgenden Befehl aus, um die auf dem Namespace verfügbare Menge an Speicherplatz zu überprüfen.

`kubectl describe resourcequotas -namespace` ***`namespace`***

Sie erhalten eine Ausgabe ähnlich der Folgenden:

```
Name:             ns-my-namespace
Namespace:        ns-my-namespace
Resource          Used  Hard
--------          ----  ----
requests.storage  0     200Gi
```

Bereitstellen eines dynamischen dauerhaften Volumes in vSphere IaaS control plane

Statusbehaftete Anwendungen, wie z. B. Datenbanken, speichern Daten zwischen Sitzungen und benötigen dauerhaften Volumes zum Speichern der Daten. Mit vSphere IaaS control plane können Sie dynamisch ein dauerhaftes Volume für Ihre Anwendung bereitstellen.

In der vSphere-Umgebung werden die Objekte eines dauerhaften Volumes von virtuellen Festplatten gesichert, die sich in Datenspeichern befinden. Datenspeicher werden durch Speicherrichtlinien dargestellt. Nachdem der vSphere-Administrator eine Speicherrichtlinie (z. B. **`Gold`**) erstellt und dem Namespace in einem Supervisor zugewiesen hat, wird die Speicherrichtlinie als übereinstimmende Kubernetes-Speicherklasse im vSphere-Namespace und in allen verfügbaren Tanzu Kubernetes Grid-Clustern angezeigt.

Als DevOps-Ingenieur können Sie die Speicherklasse in Ihren Anspruchsspezifikationen für dauerhafte Volumes verwenden. Anschließend können Sie eine Anwendung bereitstellen, die Speicher aus dem Anspruch für dauerhafte Volumes verwendet. In diesem Beispiel wird das dauerhafte Volume für die Anwendung dynamisch erstellt.

Voraussetzungen

Stellen Sie sicher, dass Ihr vSphere-Administrator eine geeignete Speicherrichtlinie erstellt und dem Namespace die Richtlinie zugewiesen hat.

Verfahren

1. Greifen Sie in der vSphere Kubernetes-Umgebung auf Ihren Namespace zu.

   Weitere Informationen hierzu finden Sie unter Abrufen und Verwenden des Supervisor-Kontexts in vSphere IaaS control plane.

2. Stellen Sie sicher, dass die Speicherklassen verfügbar sind.

   Weitere Informationen hierzu finden Sie unter Anzeigen von Speicherklassen in einem vSphere-Namespace.

3 Erstellen Sie einen Anspruch für dauerhafte Volumes.

a Erstellen Sie eine YAML-Datei, die die Konfiguration der Beanspruchung eines dauerhaften Volumes enthält.

In diesem Beispiel verweist die Datei auf die Speicherklasse **`Gold`**.

Um ein persistentes Volume im ReadWriteMany-Modus bereitzustellen, setzen Sie `accessModes` auf `ReadWriteMany`. Weitere Informationen finden Sie unter Verwenden des vSAN-Dateidiensts zum Erstellen von ReadWriteMany-Volumes in vSphere IaaS control plane.

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: my-pvc
spec:
  accessModes:
    - ReadWriteOnce
  storageClassName: gold
  resources:
    requests:
        storage: 3Gi
```

b Wenden Sie die Beanspruchung eines dauerhaften Volumes auf den Kubernetes-Cluster an.

```
kubectl apply -f pvc_name.yaml
```

Dieser Befehl erstellt dynamisch ein dauerhaftes Kubernetes-Volume sowie ein vSphere-Volume mit einer zugrunde liegenden virtuellen Festplatte, die die Speicheranforderungen der Beanspruchung erfüllt.

c Überprüfen Sie den Status der Beanspruchung eines dauerhaften Volumes.

```
kubectl get pvc my-pvc
```

Die Ausgabe zeigt, dass das Volume an Anspruch für dauerhafte Volumes gebunden ist.

```
NAME     STATUS    VOLUME   CAPACITY   ACCESSMODES   STORAGECLASS   AGE
my-pvc   Bound     my-pvc   2Gi        RWO           gold           30s
```

4 Erstellen Sie einen Pod, der das dauerhafte Volume mountet.

a Erstellen Sie eine YAML-Datei, die das dauerhafte Volume enthält.

Die Datei enthält diese Parameter.

```
...
volumes:
    - name: my-pvc
      persistentVolumeClaim:
        claimName: my-pvc
```

b Stellen Sie den Pod aus der YAML-Datei bereit:

```
kubectl create -f pv_pod_name.yaml
```

c Stellen Sie sicher, dass der Pod erstellt wurde.

```
kubectl get pod
```

```
NAME       READY   STATUS    RESTARTS   AGE
pod_name   1/1     Ready     0          40s
```

Ergebnisse

Der von Ihnen konfigurierte Pod verwendet dauerhaften Speicher, der im Anspruch für dauerhafte Volumes beschrieben wird.

Nächste Schritte

Weitere Informationen zum Überwachen des Integritätsstatus des dauerhaften Volumes finden Sie unter Überwachen der Volume-Integrität in einem vSphere-Namespace oder Tanzu Kubernetes Grid-Cluster. Weitere Informationen zum Überprüfen und Überwachen des dauerhaften Volumes im vSphere Client finden Sie unter Überwachen von dauerhaften Volumes im vSphere Client.

Bereitstellen eines statischen persistenten Volumes in vSphere IaaS control plane

Sie können ein Block-Volume statisch in einem Tanzu Kubernetes Grid-Cluster mithilfe einer Beanspruchung eines persistenten Volumes (Persistent Volume Claim, PVC) im Supervisor erstellen.

Die PVC muss die folgenden Bedingungen erfüllen:

- Die PVC ist in demselben Namespace vorhanden, in dem sich der Tanzu Kubernetes Grid-Cluster befindet.
- Die PVC ist nicht mit einem vSphere Pod im Supervisor oder einem Pod in einem anderen Tanzu Kubernetes Grid-Cluster verbunden.

Mit der statischen Bereitstellung können Sie auch eine PVC, der von einem anderen Tanzu Kubernetes Grid-Cluster nicht mehr benötigt wird, in einem neuen Tanzu Kubernetes Grid-Cluster wiederverwenden. Ändern Sie dazu die `Reclaim policy` des persistenten Volumes (PV) im ursprünglichen Tanzu Kubernetes Grid-Cluster in `Retain` und löschen Sie dann die entsprechende PVC.

Führen Sie die folgenden Schritte aus, um eine PVC in einem neuen Tanzu Kubernetes Grid-Cluster statisch zu erstellen, indem Sie die Informationen aus dem übrig gebliebenen zugrunde liegenden Volume verwenden.

Verfahren

1 Notieren Sie sich den Namen der ursprünglichen PVC im Supervisor.

Wenn Sie die PVC von einem alten Tanzu Kubernetes Grid-Cluster wiederverwenden, können Sie den PVC-Namen des `volumeHandle` des alten PV-Objekts im Tanzu Kubernetes Grid abrufen.

2 Erstellen Sie ein PV.

Geben Sie in der YAML-Datei die Werte der folgenden Elemente an:

- Für `storageClassName` können Sie den Namen der Speicherklasse eingeben, der von Ihrer PVC im Supervisor verwendet wird.
- Geben Sie für `volumeHandle` den PVC-Namen ein, den Sie in Schritt 1 abgerufen haben.

Wenn Sie ein Volume von einem anderen Tanzu Kubernetes Grid-Cluster wiederverwenden, löschen Sie die PVC- und PV-Objekte aus dem alten Tanzu Kubernetes Grid-Cluster, bevor Sie ein PV im neuen Tanzu Kubernetes Grid-Cluster erstellen.

Verwenden Sie das folgende YAML-Manifest als Beispiel.

```
apiVersion: v1
kind: PersistentVolume
metadata:
  name: static-tkg-block-pv
  annotations:
    pv.kubernetes.io/provisioned-by: csi.vsphere.vmware.com
spec:
  storageClassName: gc-storage-profile
  capacity:
    storage: 2Gi
  accessModes:
    - ReadWriteOnce
  persistentVolumeReclaimPolicy: Delete
  claimRef:
    namespace: default
    name: static-tkg-block-pvc
  csi:
    driver: "csi.vsphere.vmware.com"
    volumeAttributes:
      type: "vSphere CNS Block Volume"
    volumeHandle: "supervisor-block-pvc-name"  # Enter the PVC name from the Supervisor.
```

3 Erstellen Sie eine PVC, das dem in Schritt 2 erstellten PV-Objekt entspricht.

Legen Sie für `storageClassName` denselben Wert wie im PV fest.

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: static-tkg-block-pvc
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 2Gi
  storageClassName: gc-storage-profile
  volumeName: static-tkg-block-pv
```

4 Stellen Sie sicher, dass die PVC an das von Ihnen erstellte PV gebunden ist.

```
$ kubectl get pv,pvc
 NAME                                   CAPACITY   ACCESS MODES   RECLAIM POLICY
STATUS   CLAIM                          STORAGECLASS         REASON   AGE
 persistentvolume/static-tkg-block-pv    2Gi        RWO            Delete
Bound    default/static-tkg-block-pvc   gc-storage-profile            10s

 NAME                                          STATUS   VOLUME                CAPACITY
ACCESS MODES   STORAGECLASS         AGE
 persistentvolumeclaim/static-tkg-block-pvc   Bound    static-tkg-block-pv   2Gi
RWO            gc-storage-profile   10s
```

Verwenden des vSAN-Dateidiensts zum Erstellen von ReadWriteMany-Volumes in vSphere IaaS control plane

vSphere IaaS control plane unterstützt dauerhafte Volumes im ReadWriteMany-Modus. Mit der ReadWriteMany-Unterstützung kann ein einzelnes Volume von mehreren in einem TKG-Cluster ausgeführten Pods oder Anwendungen gleichzeitig gemountet werden. vSphere IaaS control plane verwendet CNS-Datei-Volumes, die von vSAN Dateifreigaben für die persistenten ReadWriteMany-Volumes gestützt werden. Zum Verwenden von vSAN Freigaben müssen Sie den vSAN-Dateidienst in Ihrer vSAN-Umgebung einrichten und die Unterstützung für Datei-Volumes auf Ihrem Supervisor aktivieren.

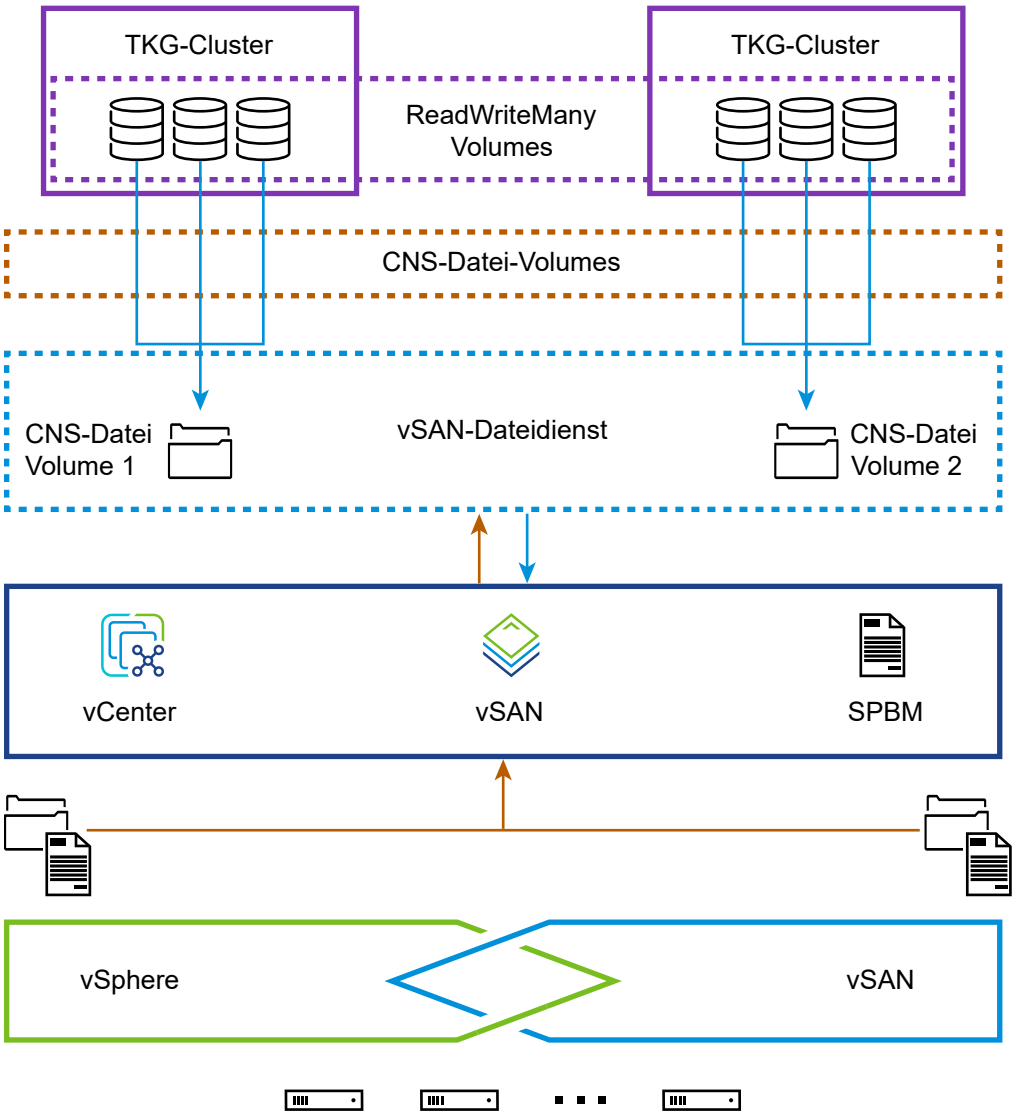
Überlegungen zu Datei-Volumes

Wenn Sie die Unterstützung für Datei-Volumes für dauerhafte Volumes in vSphere IaaS control plane aktivieren, sollten Sie die folgenden Überlegungen beachten.

- Datei-Volumes werden nur für Arbeitslasten im Tanzu Kubernetes Grid-Cluster unterstützt. Sie werden für Arbeitslasten wie vSphere-Pods- und VM-Dienst-VMs im Supervisor-Namespace nicht unterstützt.

- Wenn Sie ein RWX-Volume in Kubernetes anfordern, erstellt der vSAN-Dateidienst eine NFS-basierte Dateifreigabe der angeforderten Größe und der entsprechenden SPBM-Richtlinie. Pro RWX-Volume wird eine vSAN-Dateifreigabe erstellt. VMware unterstützt 100 Freigaben pro vSAN-Dateidienstcluster. Entsprechend können Sie über maximal 100 RWX-Volumes verfügen.
- Verwenden Sie bei TKG-Clustern die TKr-Version 1.22 oder höher.

  Weitere Informationen finden Sie in den Versionshinweisen zu den VMware Tanzu Kubernetes-Versionen.
- Wenn Sie die Unterstützung von Dateivolumes für vSphere IaaS control plane aktivieren, beachten Sie die potenziellen Sicherheitsschwächen:
  - Die Volumes werden ohne Verschlüsselung gemountet. Auf die unverschlüsselten Daten kann zugegriffen werden, während die Daten über das Netzwerk übertragen werden.
  - Zugriffssteuerungslisten (Access Control Lists, ACLs) werden für die Dateifreigaben verwendet, um den Dateifreigabezugriff innerhalb eines Supervisor-Namespace zu isolieren. Möglicherweise besteht das Risiko eines IP-Spoofing.
- Befolgen Sie diese Richtlinien für Netzwerke:
  - Wenn Sie NSX für Netzwerke in vSphere IaaS control plane verwenden, stellen Sie sicher, dass für den Supervisor-Namespace der NAT-Modus aktiviert ist. Weitere Informationen finden Sie unter Erstellen und Konfigurieren eines vSphere-Namespace im Supervisor..
  - Achten Sie darauf, dass der vSAN-Dateidienst aus dem Arbeitslastnetzwerk routingfähig ist und dass zwischen dem Arbeitslastnetzwerk und den IP-Adressen des vSAN-Dateidiensts keine NAT erfolgt.
  - Verwenden Sie den allgemeinen DNS-Server für den vSAN-Dateidienst und vSphere IaaS control plane.
- Wenn Sie die Unterstützung für Datei-Volumes aktiviert haben und sie später deaktivieren, bleiben vorhandene persistente ReadWriteMany-Volumes, die Sie im Cluster bereitgestellt haben, davon unberührt und können nicht verwendet werden. Sie können keine neuen persistenten ReadWriteMany-Volumes erstellen.



Workflow für die Aktivierung der Unterstützung für Datei-Volumes für persistente Volumes

Befolgen Sie diesen Vorgang, um die Unterstützung für Datei-Volumes zu aktivieren.

1 Ein vSphere-Administrator richtet einen vSAN-Cluster mit konfiguriertem vSAN-Dateidienst ein.

- Entsprechende Informationen finden Sie im Thema über das Aktivieren des vSAN-Dateidiensts und im Thema über das Konfigurieren des Dateidiensts.
- Informationen zu bestimmten Einstellungen in der Umgebung mit vSAN Stretched Cluster finden Sie im Thema über den vSAN-Dateidienst mit Stretched Cluster.

2 Ein vSphere-Administrator aktiviert Unterstützung für Datei-Volumes auf dem Supervisor.

Weitere Informationen finden Sie in der Dokumentation zum Thema *Installieren und Konfigurieren der vSphere IaaS-Steuerungsebene* unter Ändern der Speichereinstellungen auf dem Supervisor.

3 Ein DevOps-Ingenieur stellt ein persistentes Volume bereit und konfiguriert den PVC-`accessMode` als `ReadWriteMany`.

Mehrere Pods können mit derselben PVC bereitgestellt werden.

Beispiel:

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: my-pvc
spec:
  accessModes:
    - ReadWriteMany
  storageClassName: gold
  resources:
    requests:
        storage: 3Gi
```

Erweiterung von Volumes in vSphere IaaS control plane

Als DevOps-Ingenieur können Sie ein dauerhaftes Block-Volume nach seiner Erstellung erweitern. In vSphere IaaS control plane wird die Erweiterung von Offline- und Online-Volumes von beiden Clustertypen, Tanzu Kubernetes Grid und Supervisoren, unterstützt.

Hinweis Sie können nur persistente Block-Volumes erweitern. Derzeit unterstützt vSphere IaaS control plane keine Volume-Erweiterung für ReadWriteMany-Volumes.

Standardmäßig ist `allowVolumeExpansion` bei Speicherklassen, die in der vSphere IaaS control plane-Umgebung angezeigt werden, auf `true` festgelegt. Dieser Parameter ermöglicht die Konfiguration der Größe eines Online- oder Offline-Volumes.

Ein Volume gilt als offline, wenn es nicht mit einem Knoten oder Pod verbunden ist. Ein Online-Volume ist ein Volume, das auf einem Knoten oder Pod verfügbar ist.

Der Grad der Unterstützung der Volume-Erweiterungsfunktion ist abhängig von der vSphere-Version. Sie können Volumes, die in früheren Versionen von vSphere erstellt wurden, erweitern, wenn Sie ein Upgrade Ihrer vSphere-Umgebung auf entsprechende Versionen durchführen, die Erweiterungen unterstützen.

Beachten Sie beim Erweitern der Volumes Folgendes:

- Sie können die Volumes bis zu den durch Speicherkontingente festgelegten Grenzwerten erweitern. vSphere IaaS control plane unterstützt aufeinanderfolgende Skalierungsanforderungen für ein Beanspruchungsobjekt eines persistenten Volumes.

- Alle Arten von Datenspeichern, einschließlich VMFS, vSAN, vSAN Direct, vVols und NFS, unterstützen die Volumeerweiterung.
- Sie können Volumeerweiterungen für Bereitstellungen oder eigenständige Pods durchführen.
- Sie können die Größe von statisch bereitgestellten Volumes in einem Supervisor und in einem Tanzu Kubernetes Grid-Cluster ändern, wenn den Volumes Speicherklassen zugewiesen sind.
- Sie können Volumes, die als Teil eines StatefulSet erstellt werden, nicht erweitern, wenn Sie die StatefulSet-Definition verwenden. Derzeit unterstützt Kubernetes diese Funktion nicht. Dies führt dazu, dass Versuche, die Volumes durch Erhöhen der Speichergröße in der StatefulSet-Definition zu erweitern, fehlschlagen.
- Wenn eine virtuelle Festplatte, die ein Volume-Backing erstellt, über Snapshots verfügt, kann deren Größe nicht geändert werden.
- vSphere IaaS control plane unterstützt keine Volumeerweiterung für strukturbasierte oder migrierte Volumes.

Erweitern eines persistenten Volumes im Offline-Modus

Ein Volume gilt als offline, wenn es nicht mit einem Knoten oder Pod verbunden ist. Beide Clustertypen, Cluster Supervisoren und Tanzu Kubernetes Grid, unterstützen Offline-Volume-Erweiterungen.

Voraussetzungen

Aktualisieren Sie Ihre vSphere-Umgebung auf eine geeignete Version, die Erweiterungen von Offline-Volumes unterstützt.

Verfahren

1 Erstellen Sie eine Beanspruchung eines persistenten Volumes (Persistent Volume Claim, PVC) mit einer Standardspeicherklasse.

   a Definieren Sie das PVC mithilfe des folgenden YAML-Manifests als Beispiel.

   Im Beispiel beträgt die Größe des angeforderten Speichers 1 Gi.

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: example-block-pvc
spec:
  accessModes:
  - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: example-block-sc
```

   b Wenden Sie das PVC auf den Kubernetes-Cluster an.

```
kubectl apply -f example-block-pvc.yaml
```

2 Patchen Sie das PVC, um es zu vergrößern.

   Wenn das MATERIAL nicht an einen Knoten angehängt ist oder von einem Pod verwendet wird, verwenden Sie den folgenden Befehl zum Patchen von PVC. In diesem Beispiel beträgt die angeforderte Speichererhöhung 2 Gi.

```
kubectl patch pvc example-block-pvc -p '{"spec": {"resources": {"requests": {"storage":
"2Gi"}}}}'
```

   Diese Aktion löst eine Erweiterung in dem Volume aus, das mit dem PVC verknüpft ist.

3 Vergewissern Sie sich, dass das Volume größer geworden ist.

```
kubectl get pv
NAME                                        CAPACITY ACCESS MODES RECLAIM POLICY STATUS
CLAIM                         STORAGECLASS           REASON AGE
pvc-9e9a325d-ee1c-11e9-a223-005056ad1fc1   2Gi            RWO         Delete     Bound
default/example-block-pvc   example-block-sc              6m44s
```

Hinweis Die Größe des PVC bleibt unverändert, bis das PVC von einem Pod verwendet wird.

Das folgende Beispiel zeigt, dass sich die PVC-Größe nicht geändert hat. Wenn Sie das PVC beschreiben, sehen Sie, dass die Bedingung `FilesystemResizePending` auf das PVC angewendet ist.

```
kubectl get pvc
NAME                STATUS VOLUME                                      CAPACITY ACCESS
MODES   STORAGECLASS       AGE
example-block-pvc   Bound  pvc-9e9a325d-ee1c-11e9-a223-005056ad1fc1   1Gi
RWO       example-block-sc   6m57s
```

4 Erstellen Sie einen Pod zur Verwendung des PVC.

Wenn das PVC vom Pod verwendet wird, wird das Dateisystem erweitert.

5 Vergewissern Sie sich, dass die PVC-Größe geändert wurde.

```
kubectl get pvc
NAME                STATUS VOLUME                                     CAPACITY ACCESS MODES
STORAGECLASS     AGE
example-block-pvc   Bound  pvc-24114458-9753-428e-9c90-9f568cb25788   2Gi         RWO
example-block-sc 2m12s
```

Die Bedingung `FilesystemResizePending` wurde aus dem PVC entfernt. Volume-Erweiterung ist abgeschlossen.

Nächste Schritte

Ein vSphere-Administrator kann die neue Volume-Größe im vSphere Client sehen. Weitere Informationen hierzu finden Sie unter Überwachen von dauerhaften Volumes im vSphere Client.

Erweitern eines persistenten Volumes im Online-Modus

Ein Online-Volume ist ein Volume, das auf einem Knoten oder Pod verfügbar ist. Als DevOps Engineer können Sie ein persistentes Onlineblock-Volume erweitern. Die Erweiterung von Online-Volumes wird sowohl von Supervisoren- als auch von Tanzu Kubernetes Grid-Clustern unterstützt.

Voraussetzungen

Aktualisieren Sie Ihre vSphere-Umgebung auf eine geeignete Version, die die Erweiterung von Online-Volumes unterstützt.

Verfahren

1 Suchen Sie für die Skalierung nach einer Anforderung von persistenten Datenträgern.

```
$ kubectl get pv,pvc,pod
NAME                                                        CAPACITY   ACCESS MODES
RECLAIM POLICY   STATUS      CLAIM               STORAGECLASS   REASON   AGE
persistentvolume/pvc-5cd51b05-245a-4610-8af4-f07e77fdc984   1Gi        RWO
Delete           Bound       default/block-pvc   block-sc                 4m56s

NAME                                STATUS   VOLUME
CAPACITY   ACCESS MODES   STORAGECLASS   AGE
persistentvolumeclaim/block-pvc   Bound    pvc-5cd51b05-245a-4610-8af4-f07e77fdc984
1Gi        RWO            block-sc       5m3s

NAME            READY   STATUS    RESTARTS   AGE
pod/block-pod   1/1     Running   0          26s
```

Beachten Sie, dass die Speichergröße, die das Volume verwendet, 1 Gi beträgt.

2 Patchen Sie das PVC, um es zu vergrößern.

Erhöhen Sie den Wert für die Größe beispielsweise auf 2 Gi.

```
$ kubectl patch pvc block-pvc -p '{"spec": {"resources": {"requests": {"storage":
"2Gi"}}}}'
persistentvolumeclaim/block-pvc edited
```

Diese Aktion löst eine Erweiterung in dem Volume aus, das mit dem PVC verknüpft ist.

3 Stellen Sie sicher, dass sowohl die PVC- als auch die PV-Größe erhöht wurde.

```
$ kubectl get pvc,pv,pod
NAME                                STATUS   VOLUME
CAPACITY   ACCESS MODES   STORAGECLASS   AGE
persistentvolumeclaim/block-pvc   Bound    pvc-5cd51b05-245a-4610-8af4-f07e77fdc984
2Gi        RWO            block-sc       6m18s

NAME                                                        CAPACITY   ACCESS MODES
RECLAIM POLICY   STATUS      CLAIM               STORAGECLASS   REASON   AGE
persistentvolume/pvc-5cd51b05-245a-4610-8af4-f07e77fdc984   2Gi        RWO
Delete           Bound       default/block-pvc   block-sc                 6m11s

NAME            READY   STATUS    RESTARTS   AGE
pod/block-pod   1/1     Running   0          101s
```

Nächste Schritte

Ein vSphere-Administrator kann die neue Volume-Größe im vSphere Client sehen. Weitere Informationen hierzu finden Sie unter Überwachen von dauerhaften Volumes im vSphere Client.

Überwachen von dauerhaften Volumes im vSphere Client

Wenn DevOps-Ingenieure eine statusbehaftete Anwendung mit einem Anspruch für dauerhafte Volumes bereitstellen, erstellt vSphere IaaS control plane ein dauerhaftes Volume-Objekt und eine passende dauerhafte virtuelle Festplatte. Als vSphere-Administrator können Sie Details des dauerhaften Volumes im vSphere Client überprüfen. Sie können auch die Speicherübereinstimmung und den Systemzustand des Volumes überwachen.

Verfahren

1 Navigieren Sie im vSphere Client zu dem Namespace, der über dauerhafte Volumes verfügt.

   a Wählen Sie im vSphere Client-Startmenü die Option **Arbeitslastverwaltung** aus.

   b Klicken Sie auf die Registerkarte **Namespaces** und wählen Sie einen Namespace aus der Liste aus.

2 Klicken Sie auf die Registerkarte **Speicher** und dann auf **Anforderungen von dauerhaften Datenträgern**.

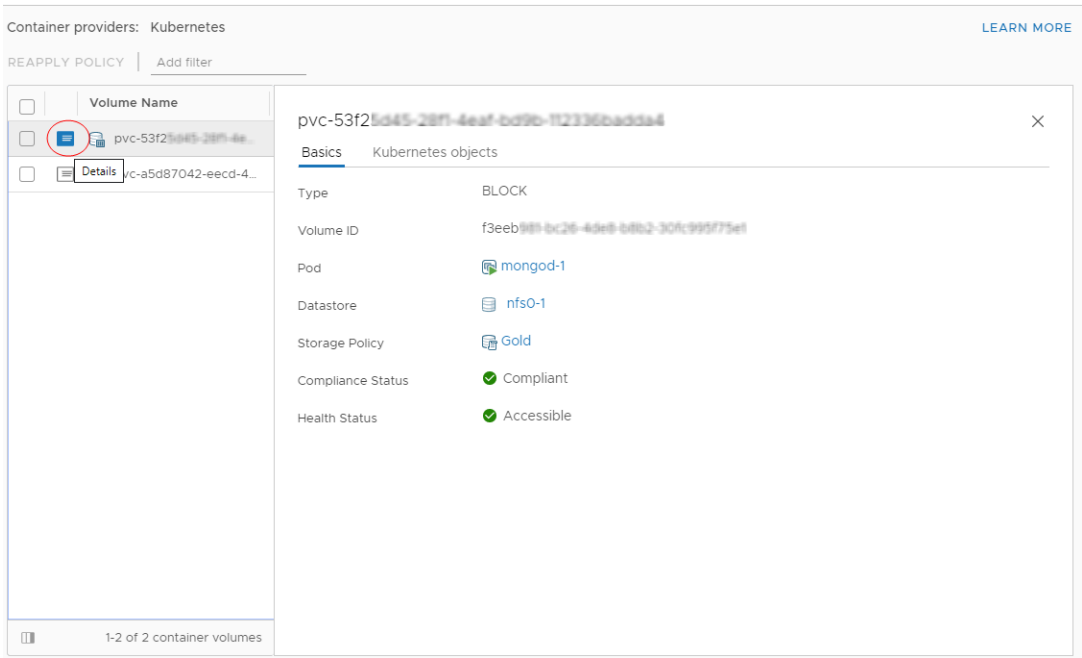
   Der vSphere Client listet alle Objekte mit Ansprüchen für dauerhafte Volumes sowie entsprechende im Namespace verfügbare Volumes auf.

3 Klicken Sie zum Anzeigen der Details eines Anspruchs für ein ausgewähltes dauerhaftes Volume in der Spalte **Name des dauerhaften Volumes** auf den Namen des Volumes.

4 Überprüfen Sie auf der Seite **Container-Volumes** den Integritätsstatus und die Speicherrichtlinienübereinstimmung des Volumes.

a Klicken Sie auf das Symbol **Details** und wechseln Sie zwischen den Registerkarten **Grundlagen** und **Kubernetes-Objekte**, um zusätzliche Informationen für das dauerhafte Kubernetes-Volume anzuzeigen.

Informationen zum Überwachen des Integritätsstatus des Volumes mithilfe des Befehls `kubectl` finden Sie unter Überwachen der Volume-Integrität in einem vSphere-Namespace oder Tanzu Kubernetes Grid-Cluster.



b Überprüfen Sie den Integritätsstatus des Volumes.

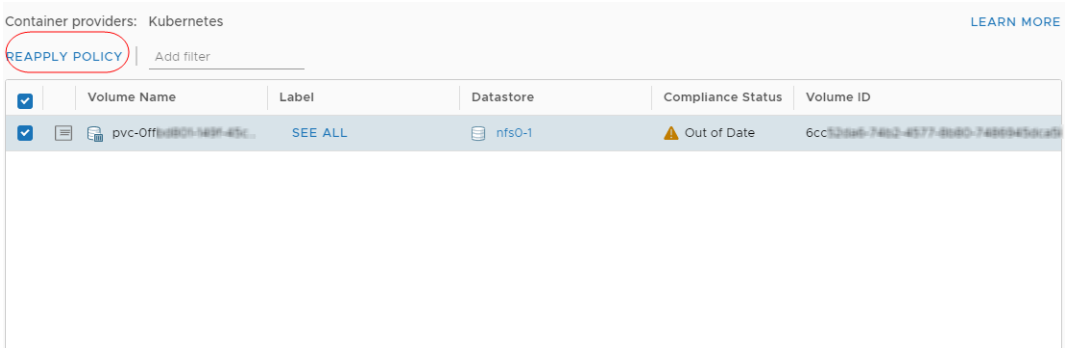
Integritätsstatus	Beschreibung
Verfügbar	Auf das dauerhafte Volume kann zugegriffen werden, und es steht zur Verwendung zur Verfügung.
Kein Zugriff	Auf das dauerhafte Volume kann nicht zugegriffen werden, und es kann nicht verwendet werden. Auf das dauerhafte Volume kann nicht zugegriffen werden, wenn der Datenspeicher, auf dem das Volume gespeichert wird, nicht von den Hosts erreicht werden kann, die eine Verbindung zum Datenspeicher herstellen.

c Überprüfen Sie den Status der Speicherübereinstimmung.

Einer der folgenden Werte wird in der Spalte **Übereinstimmungsstatus** angezeigt.

Übereinstimmungsstatus	Beschreibung
Übereinstimmung	Der Datenspeicher, in dem sich die zugrunde liegende virtuelle Festplatte des Volumes befindet, enthält die von der Richtlinie benötigten Speicherfunktionen.
Veraltet	Dieser Status gibt an, dass die Richtlinie bearbeitet wurde, die neuen Anforderungen aber nicht an den Datenspeicher weitergegeben wurden. Zum Übermitteln der Änderungen wenden Sie die Richtlinie erneut auf das veraltete Volume an.
Nicht übereinstimmend	Der Datenspeicher unterstützt festgelegte Speicheranforderungen, kann jedoch zurzeit nicht die Speicherrichtlinie erfüllen. Der Status kann z. B. in „Keine Übereinstimmung“ wechseln, wenn physische Ressourcen für den Datenspeicher nicht verfügbar sind. Sie können die Übereinstimmung des Datenspeichers wiederherstellen, indem Sie Änderungen an der physischen Konfiguration Ihres Hostclusters vornehmen, indem Sie Hosts oder Festplatten beispielsweise zum Cluster hinzufügen. Wenn weitere Ressourcen die Speicherrichtlinie erfüllen, ändert sich der Status in „Übereinstimmung“.
Nicht anwendbar	Die Speicherrichtlinie verweist auf Datenspeicherkapazitäten, die vom Datenspeicher nicht unterstützt werden.

d Wenn der Übereinstimmungsstatus auf „Veraltet“ gesetzt ist, wählen Sie das Volume aus und klicken Sie auf **Richtlinie erneut anwenden**.



Der Status wird in „Übereinstimmung“ geändert.

Überwachen der Volume-Integrität in einem vSphere-Namespace oder Tanzu Kubernetes Grid-Cluster

Bei Verwendung von vSphere IaaS control plane können Sie den Integritätsstatus eines dauerhaften Volumes in einem gebundenen Zustand überprüfen.

Für jedes persistente Volume in einem gebundenen Zustand wird der Integritätsstatus im Feld `Annotations: volumehealth.storage.kubernetes.io/messages:` der Beanspruchung eines dauerhaften Volumes angezeigt, das an das dauerhafte Volume gebunden ist. Es gibt zwei mögliche Werte für den Integritätsstatus.

Integritätsstatus	Beschreibung
Verfügbar	Auf das dauerhafte Volume kann zugegriffen werden, und es steht zur Verwendung zur Verfügung.
Kein Zugriff	Auf das dauerhafte Volume kann nicht zugegriffen werden, und es kann nicht verwendet werden. Auf das dauerhafte Volume kann nicht zugegriffen werden, wenn der Datenspeicher, auf dem das Volume gespeichert wird, nicht von den Hosts erreicht werden kann, die eine Verbindung zum Datenspeicher herstellen.

Weitere Informationen zum Überwachen des Volume-Integritätsstatus im vSphere Client finden Sie unter Überwachen von dauerhaften Volumes im vSphere Client.

Verfahren

1 Greifen Sie in der vSphere IaaS control plane-Umgebung auf Ihren Namespace zu.

2 Erstellen Sie einen Anspruch für dauerhafte Volumes.

a Erstellen Sie eine YAML-Datei, die die Konfiguration der Beanspruchung eines dauerhaften Volumes enthält.

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: my-pvc
spec:
  accessModes:
    - ReadWriteOnce
  storageClassName: gold
  resources:
    requests:
        storage: 2Gi
```

b Wenden Sie die Beanspruchung eines dauerhaften Volumes auf den Kubernetes-Cluster an.

```
kubectl apply -f pvc_name.yaml
```

Dieser Befehl erstellt ein dauerhaftes Kubernetes-Volume sowie ein vSphere-Volume mit einer zugrunde liegenden virtuellen Festplatte, die die Speicheranforderungen des Anspruchs erfüllt.

c Überprüfen Sie, ob die Beanspruchung eines dauerhaften Volumes an ein Volume gebunden ist.

```
kubectl get pvc my-pvc
```

Die Ausgabe zeigt, dass sich die Beanspruchung eines dauerhaften Volumes und das Volume im gebundenen Zustand befinden.

```
NAME     STATUS    VOLUME   CAPACITY   ACCESSMODES   STORAGECLASS   AGE
my-pvc   Bound     my-pvc   2Gi        RWO           gold           30s
```

3 Überprüfen Sie den Integritätsstatus des Volumes.

Führen Sie den folgenden Befehl aus, um die Volume-Integritätsanmerkung der Beanspruchung eines persistenten Volumes zu überprüfen, die an das dauerhafte Volume gebunden ist.

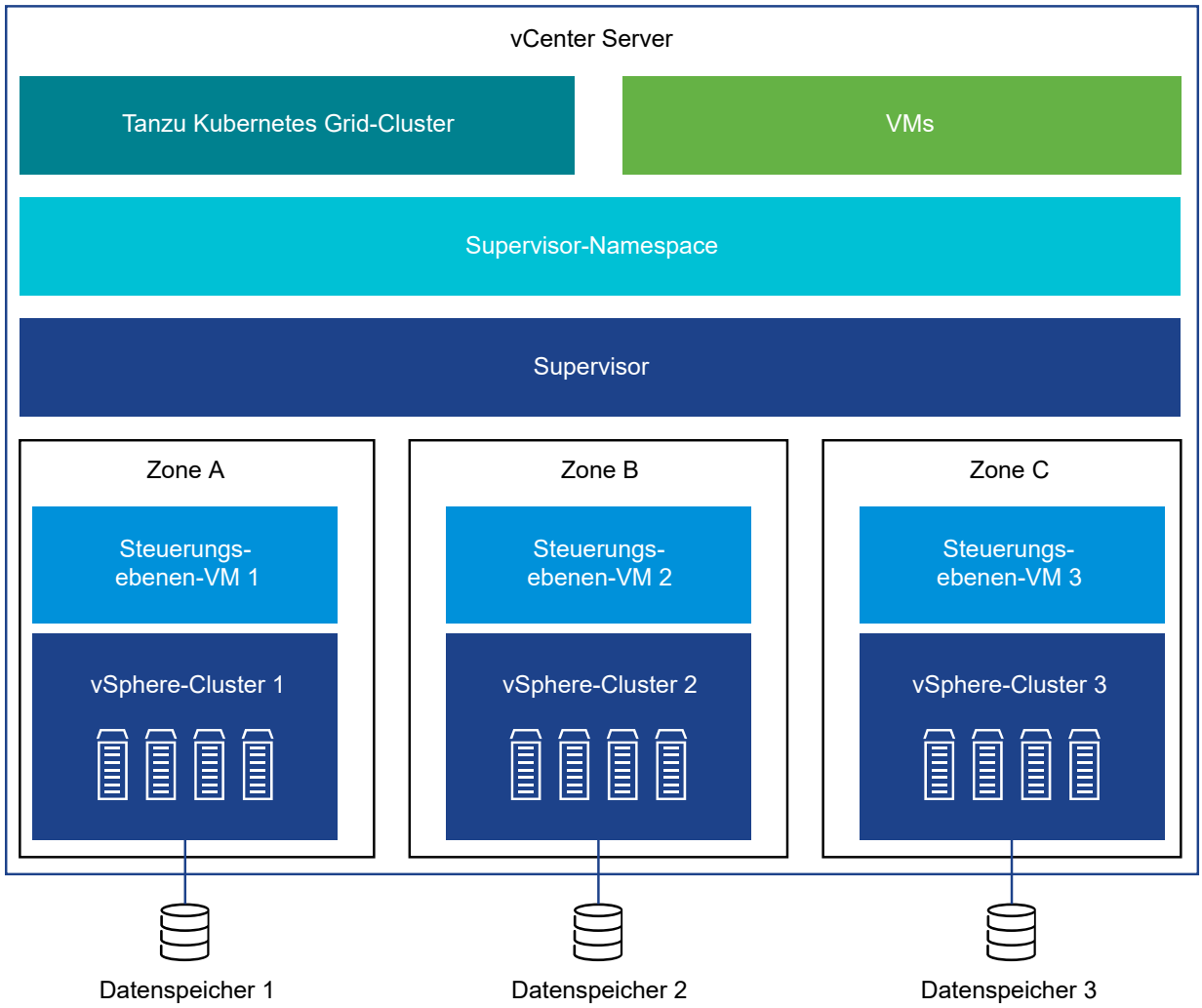
```
kubectl describe pvc my-pvc
```

In der folgenden Beispielausgabe weist das Feld `volumehealth.storage.kubernetes.io/messages` den Integritätsstatus als „Verfügbar“ aus.

```
Name:          my-pvc
Namespace:     test-ns
StorageClass:  gold
Status:        Bound
Volume:        my-pvc
Labels:        <none>
Annotations:   pv.kubernetes.io/bind-completed: yes
               pv.kubernetes.io/bound-by-controller: yes
               volume.beta.kubernetes.io/storage-provisioner: csi.vsphere.vmware.com
               volumehealth.storage.kubernetes.io/messages: accessible
Finalizers:    [kubernetes.io/pvc-protection]
Capacity:      2Gi
Access Modes:  RWO
VolumeMode:    Filesystem
```

Best Practices für die Verwendung von persistentem Speicher auf einem Supervisor mit drei Zonen

Ein Supervisor mit drei Zonen in vSphere IaaS control plane unterstützt den zonenspezifischen Speicher, bei dem ein Datenspeicher von allen Hosts in einer einzelnen Zone gemeinsam genutzt wird.



Beachten Sie Folgendes bei der Vorbereitung von Speicherressourcen für den Supervisor mit drei Zonen:

- Der Speicher in allen drei Zonen muss nicht vom gleichen Typ sein. Ein einheitlicher Speicher in allen drei Clustern bietet jedoch eine konsistente Leistung.
- Verwenden Sie für den Namespace auf dem Supervisor mit drei Zonen eine Speicherrichtlinie, die mit dem freigegebenen Speicher in jedem der Cluster kompatibel ist. Die Speicherrichtlinie muss topologiefähig sein.
- Entfernen Sie keine Topologieeinschränkungen aus der Speicherrichtlinie, nachdem Sie sie dem Namespace zugewiesen haben.
- Mounten Sie keine Zonendatenspeicher in anderen Zonen.
- Folgendes unterstützt ein Supervisor mit drei Zonen nicht:
  - Zonenübergreifende Volumes
  - vSAN File-Volumes (ReadWriteMany-Volumes)

- Bereitstellung statischer Volumes mithilfe der Volume-Registrierungs-API
- Arbeitslasten, die die vSAN Data Persistence-Plattform verwenden
- vSphere Pod
- vSAN Stretched Cluster
- VMs mit vGPU und Instanzspeicher

Erstellen einer Speicherrichtlinie für einen Supervisor mit drei Zonen

Um dauerhaften Speicher verwenden zu können, müssen Workloads, die auf dem Supervisor mit drei Zonen ausgeführt werden, Zugriff auf Speicherklassen mit Zonentopologie haben. Um diese Speicherklassen verfügbar zu machen, erstellt der vSphere-Administrator topologiefähige Speicherrichtlinien und weist sie dem Namespace zu.

Der Namespace auf dem Supervisor mit drei Zonen verhindert, dass Sie Speicherrichtlinien zuweisen können, die nicht topologiefähig sind.

Informationen zum Aktivieren des Supervisor mit drei Zonen finden Sie unter Aktivieren eines Supervisors für drei Zonen.

Verfahren

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

   a Klicken Sie auf der **Startseite** auf **Richtlinien und Profile**.

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

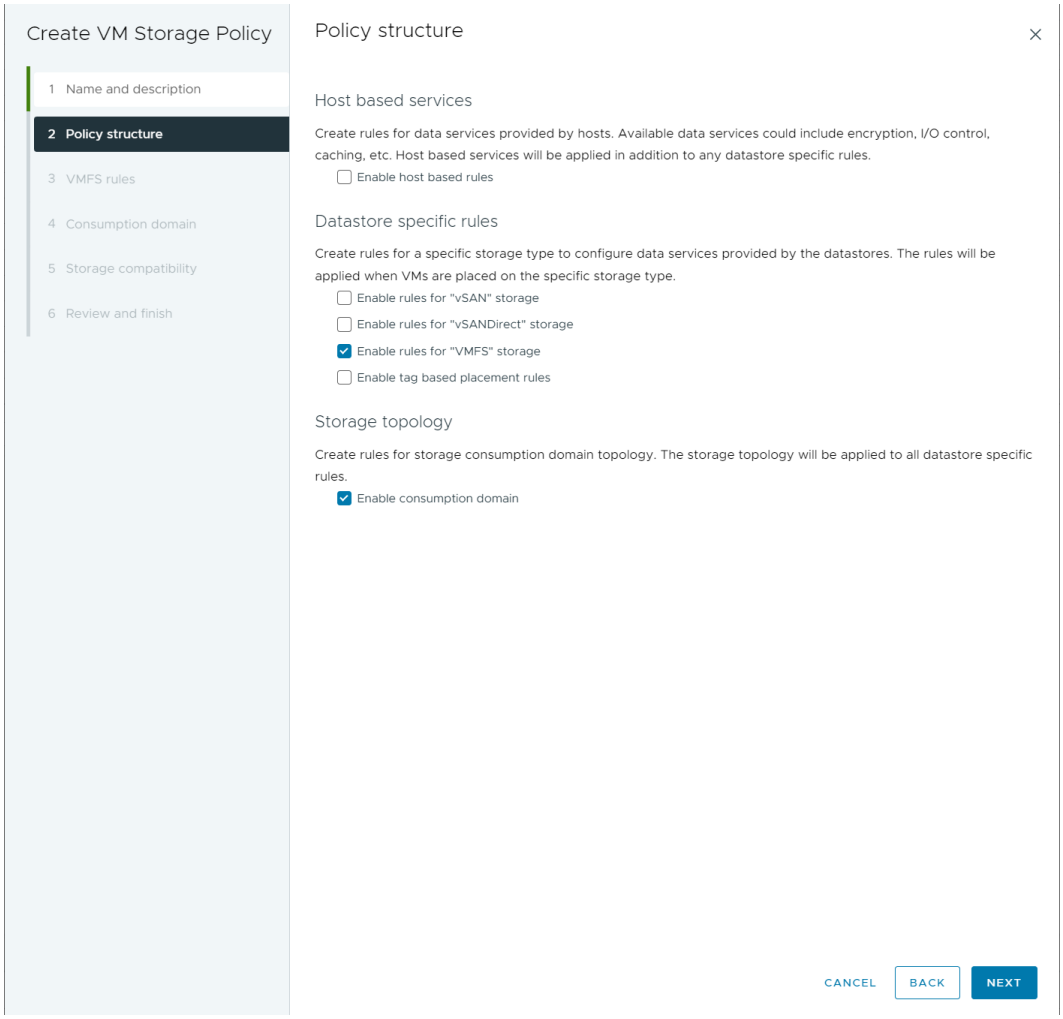
   c Klicken Sie auf **Erstellen**.

2 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.
Beschreibung	Geben Sie die Beschreibung der Speicherrichtlinie ein.

3 Folgen Sie den Eingabeaufforderungen auf der Seite **Richtlinienstruktur**.

4 Wählen Sie unter **Speichertopologie** die Option **Verbrauchsdomäne aktivieren** aus und folgen Sie den Eingabeaufforderungen auf der Seite **Verbrauchsdomäne**.



5 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.

Erstellen einer PVC auf einem Supervisor mit drei Zonen

Wenn Sie eine dynamische Beanspruchung eines dauerhaften Volumes (Persistent Volume Claim, PVC) auf einem Supervisor mit drei Zonen erstellen, können Sie angeben, in welchen Zonen das Volume bereitgestellt werden soll.

Verfahren

- Verwenden Sie zum Steuern der PVC-Zonenplatzierung die Kubernetes-Anmerkung `csi.vsphere.volume-requested-topology` in der YAML-Datei für Ihre PVC.

  Vorsicht Dieser Parameter ist erforderlich, wenn Sie eine PVC direkt auf dem Supervisor erstellen. Fügen Sie jedoch keine Zonenanmerkungen in die PVC ein, die Sie für einen Tanzu Kubernetes Grid-Cluster erstellen. Wenn Sie dies tun, funktioniert die PVC nicht.

  ```
  apiVersion: v1
  kind: PersistentVolumeClaim
  metadata:
    name: svcpvc4
    annotations:
      csi.vsphere.volume-requested-topology: '[{"topology.kubernetes.io/zone":"zone-1"},
  {"topology.kubernetes.io/zone":"zone-2"},{"topology.kubernetes.io/zone":"zone-3"}]'
  spec:
    accessModes:
      - ReadWriteOnce
    resources:
      requests:
        storage: 10Mi
    storageClassName: zonal2
  ```

  Wenn Sie alle drei Zonen angeben, wird das Volume entweder in zone-1, zone-2 oder zone-3 erstellt.

Nächste Schritte

Informationen zum Bereitstellen von statusbehafteten Anwendungen in Tanzu Kubernetes Grid-Clustern finden Sie unter Bereitstellen einer StatefulSet-Anwendung über vSphere Zonen mit einem Volume-Anhang mit später Bindung.

Installieren und Konfigurieren von Harbor und Contour in vSphere IaaS control plane

9

Erfahren Sie, wie Sie Harbor und Contour als Supervisor-Dienste in Ihrer vSphere IaaS control plane-Umgebung bereitstellen und konfigurieren. Harbor ist eine cloudnative Open Source-Registrierung, die Sie mit Ihren Arbeitslasten verwenden können, welche auf vSphere IaaS control plane ausgeführt werden. Contour ist ein Ingress-Controller für Kubernetes, der durch Bereitstellung des Envoy-Proxys als Reverse-Proxy und Lastausgleichsdienst funktioniert. Contour unterstützt sofort einsatzbereite, dynamische Konfigurationsaktualisierungen unter Beibehaltung eines schlanken Profils.

Sie können Contour als Supervisor-Dienst als Ingress-Controller für Ihre Anwendungen verwenden. Contour ist auch eine Voraussetzung für die Ausführung des Harbor-Supervisor-Dienst.

Hinweis Supervisor-Dienste werden auf Einzelcluster-Supervisoren unterstützt, die entweder auf VDS- oder NSX-Netzwerk-Stacks ausgeführt werden. Sie können Supervisor-Dienste nicht auf Supervisoren mit drei Zonen bereitstellen.

Harbor als Supervisor-Dienst bietet die folgenden Möglichkeiten und Funktionen:

- Die neueste Version der Open-Source-Registrierung von Harbor.
- Zugriff auf Harbor mit den Admin- und Root-Konten.
- Vollständige Funktionsparität mit der Upstream-Harbor-Registrierung.
- Zugriff auf Harbor über Ingress (Contour) mithilfe von DNS.

Hinweis Bei der Bereitstellung erstellen die Harbor- und Contour-Supervisor-Dienste vSphere-Pods in den für diese Dienste erstellten vSphere-Namespaces. Diese vSphere-Pods werden für die Funktion der Dienste benötigt. Sie können keine vSphere-Pods außerhalb von Supervisor-Dienste auf einem Supervisor bereitstellen, der auf dem VDS-Netzwerk-Stack oder einem Supervisor mit drei Zonen ausgeführt wird. Sie können vSphere-Pods nur für die allgemeine Verwendung auf einem Supervisor mit einem einzelnen Custer bereitstellen, der mit NSX bereitgestellt wurde.

Lesen Sie als Nächstes die folgenden Themen:

- Installieren von Contour als Supervisor-Dienst in vSphere IaaS control plane
- Installieren und Konfigurieren von Harbor auf einem Supervisor in vSphere IaaS control plane

- Migrieren von Images aus der eingebetteten Registrierung zu Harbor in vSphere IaaS control plane

Installieren von Contour als Supervisor-Dienst in vSphere IaaS control plane

Erfahren Sie, wie Sie Contour als Supervisor-Dienst auf den Supervisoren in Ihrer vSphere IaaS control plane-Umgebung installieren. Nach der Installation können Sie Contour als Ingress-Controller für Ihre Anwendungen verwenden. Contour ist auch eine Voraussetzung für die Ausführung von Harbor als Supervisor-Dienst.

Voraussetzungen

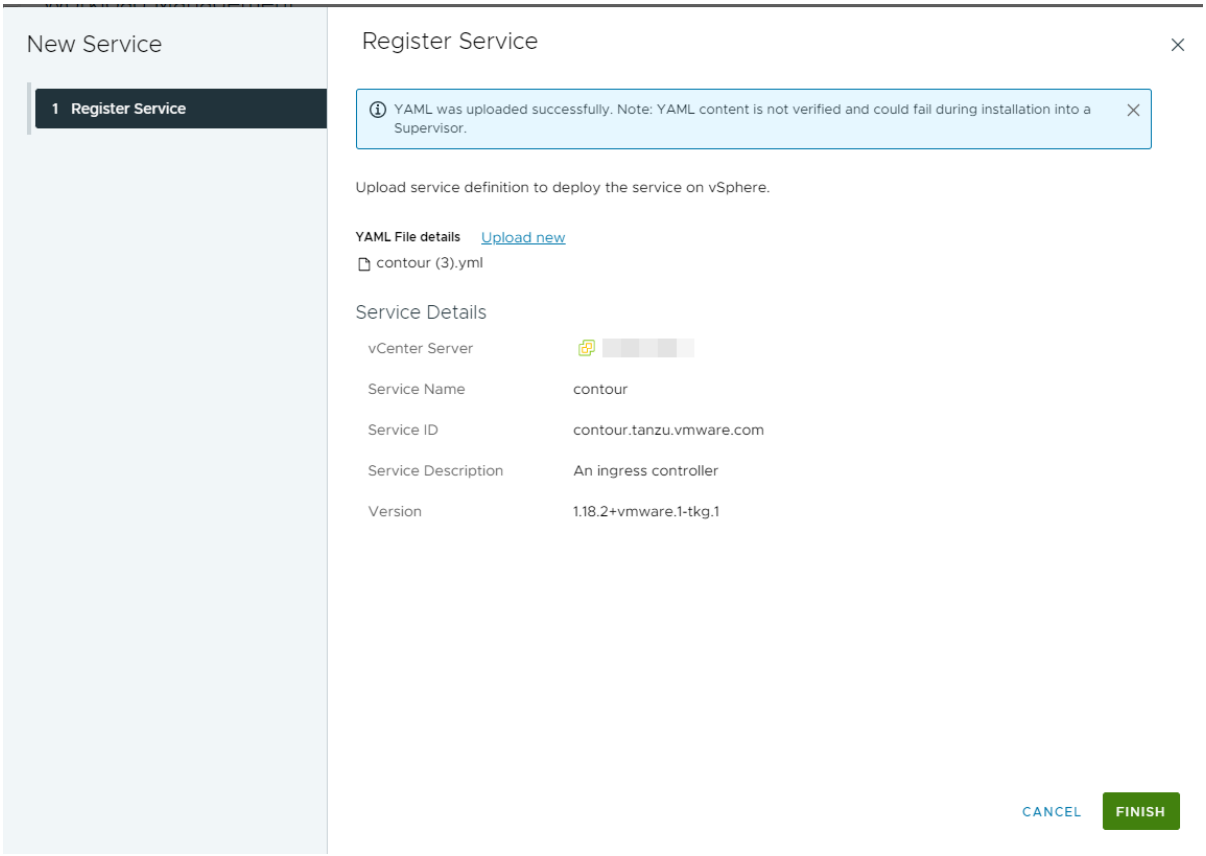
- Überprüfen Sie, ob Sie auf dem vCenter Server-System, dem Sie die Dienste hinzufügen, über die Berechtigung **Supervisor-Dienste verwalten** verfügen.
- Stellen Sie sicher, dass Sie auf vCenter Server 8.0a oder höher aktualisiert haben. Contour- und Harbor-Supervisor-Dienste werden mit vCenter Server 8.0a und höher unterstützt.

Verfahren

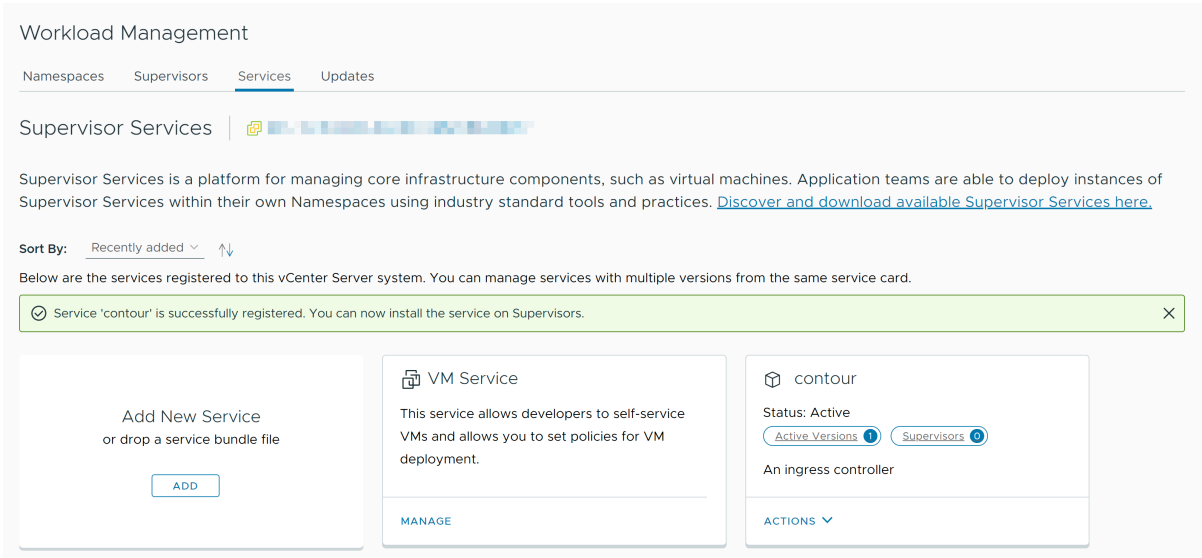
1. Wechseln Sie zum Abschnitt Contour-Versionen des Repositorys Supervisor-Services und laden Sie die folgenden Dateien herunter:
   - Die Contour-Dienstdefinition, der Link lautet `Contour vX.X.X.`. Beispiel: `Contour 1.18.2`
   - Die Contour-Konfigurationsdatei, der Link lautet `values for vX.X.X`. Beispiel: `values 1.18.2`

   Die sich ergebenden Dateien lauten:
   - `contour.yml`
   - `contour-data-values.yml`
2. Navigieren Sie im vSphere Client zu **Arbeitslastverwaltung** und wählen Sie **Dienste** aus.

3 Stellen Sie den Dienste-Operator von Contour bereit, indem Sie auf **Neuen Dienst hinzufügen** klicken und die Dienstdefinition `contour.yml` hochladen.



Wenn der Contour-Operator erfolgreich bereitgestellt wurde, wird seine Dienstkarte auf der Registerkarte **Services** angezeigt.



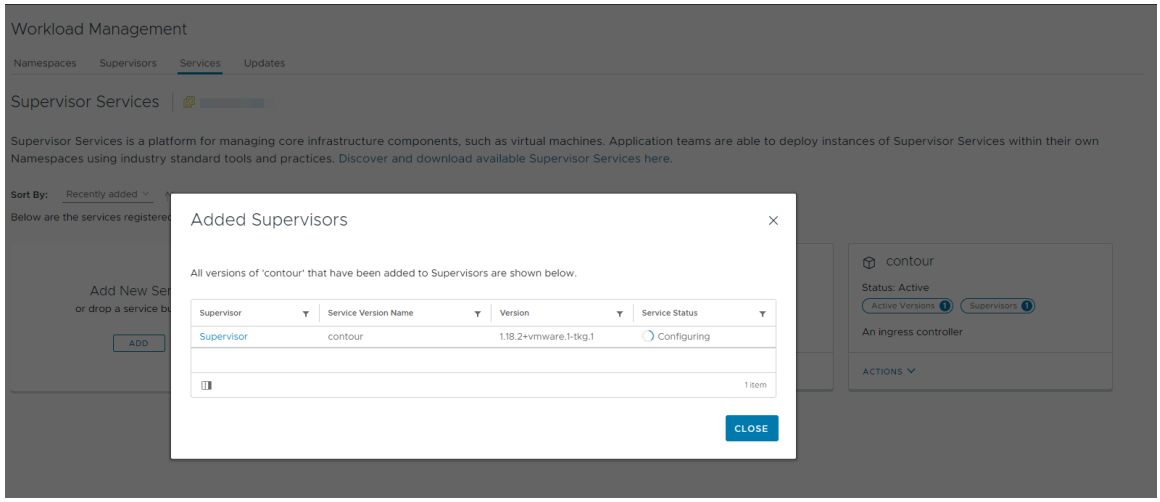
4 Nachdem der Contour-Operator bereitgestellt wurde, können Sie den Supervisor-Dienst auf Supervisoren installieren.

a Wählen Sie auf der Dienstkarte **Contour** die Option **Aktionen > Auf Supervisoren installieren** aus.

b Wählen Sie einen Supervisor aus und kopieren Sie in **YAML-Dienstkonfiguration** den Inhalt der Datei `contour-data-values.yml` und fügen Sie ihn ein, ohne die Standardwerte zu ändern.

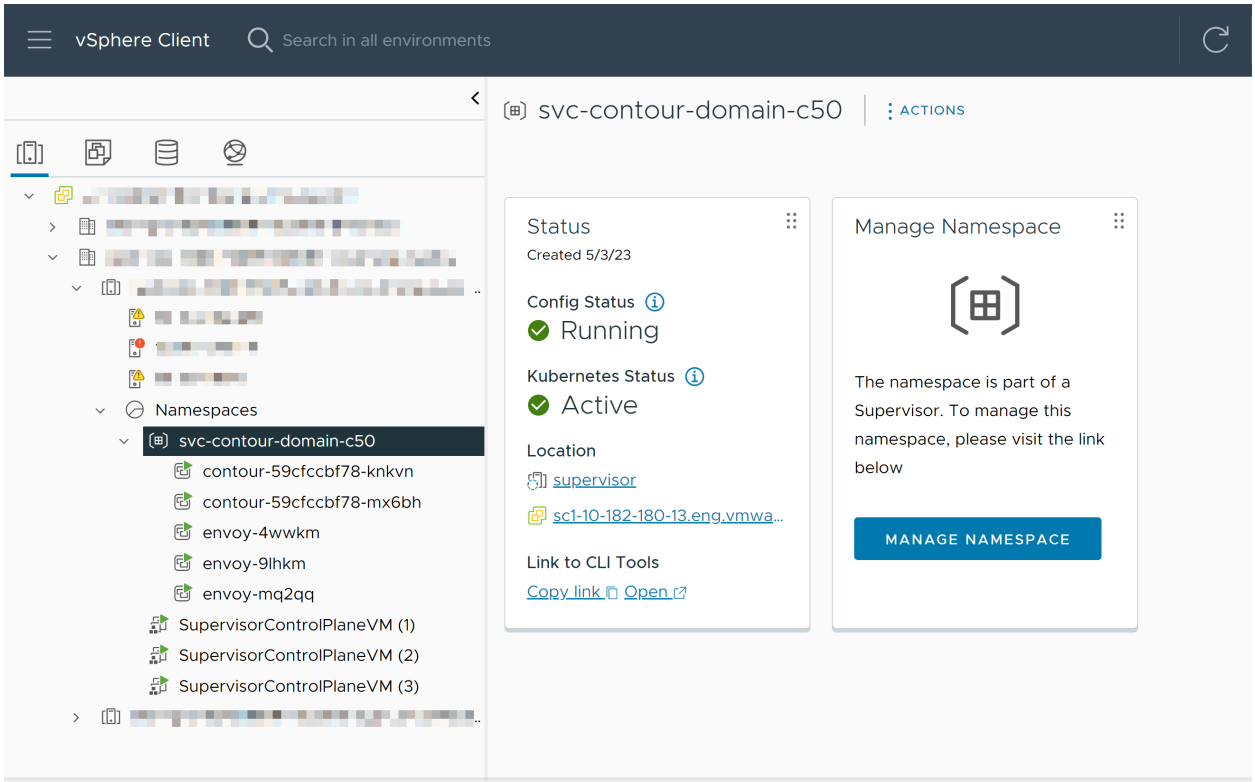
c Klicken Sie auf **OK**.

Sobald die Installation beginnt, können Sie sie verfolgen, indem Sie auf das Feld **Supervisoren** auf der Karte des Contour-Diensts klicken. Es kann einige Sekunden dauern, bis die Zahl neben **Supervisoren** ansteigt. Der Dienst befindet sich im Konfigurationszustand, bis der gewünschte Zustand erreicht ist. Wenn der gewünschte Zustand erreicht ist, ändert sich der Status des Diensts zu „Wird ausgeführt“.

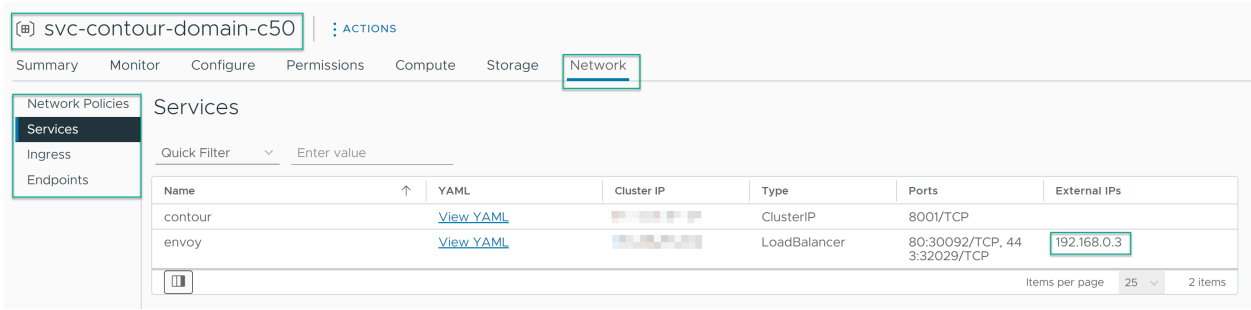


Ergebnisse

Nach der Installation von Contour werden ein für die Dienstinstanz erstellter vSphere-Namespace sowie die entsprechenden vSphere-Pods bereitgestellt:



Sie können auch die IP-Adresse des Envoy-Diensts anzeigen, die Sie Domänennamen in einem externen DNS-Server zuordnen können, der mit dem Supervisor konfiguriert ist. Sie können die Zuordnungen verwenden, um Ingress für Ihre Anwendungen über Contour bereitzustellen. Sie können die Envoy-IP-Adresse über die Option **Netzwerk** des Contour vSphere-Namespace anzeigen:



Nächste Schritte

Wenn Sie Harbor als Supervisor-Dienst verwenden möchten, um eine Registrierung für Ihre Arbeitslasten bereitzustellen, können Sie den Dienst installieren und für die Verwendung mit Ihren Arbeitslasten konfigurieren. Weitere Informationen finden Sie unter Installieren und Konfigurieren von Harbor auf einem Supervisor in vSphere IaaS control plane.

Installieren und Konfigurieren von Harbor auf einem Supervisor in vSphere IaaS control plane

Erfahren Sie, wie Harbor als Supervisor-Dienst installiert und konfiguriert wird. Sie können Harbor dann als Registrierung für Arbeitslasten verwenden, die auf Tanzu Kubernetes Grid-Clustern und vSphere-Pods ausgeführt werden. Harbor benötigt Contour als Ingress-Controller. Installieren Sie daher zuerst den Contour Supervisor-Dienst dann Harbor.

Installieren von Harbor als Supervisor-Dienst

Sie installieren Harbor als Supervisor-Dienst über die Option **Arbeitslastverwaltung** im vSphere Client.

Voraussetzungen

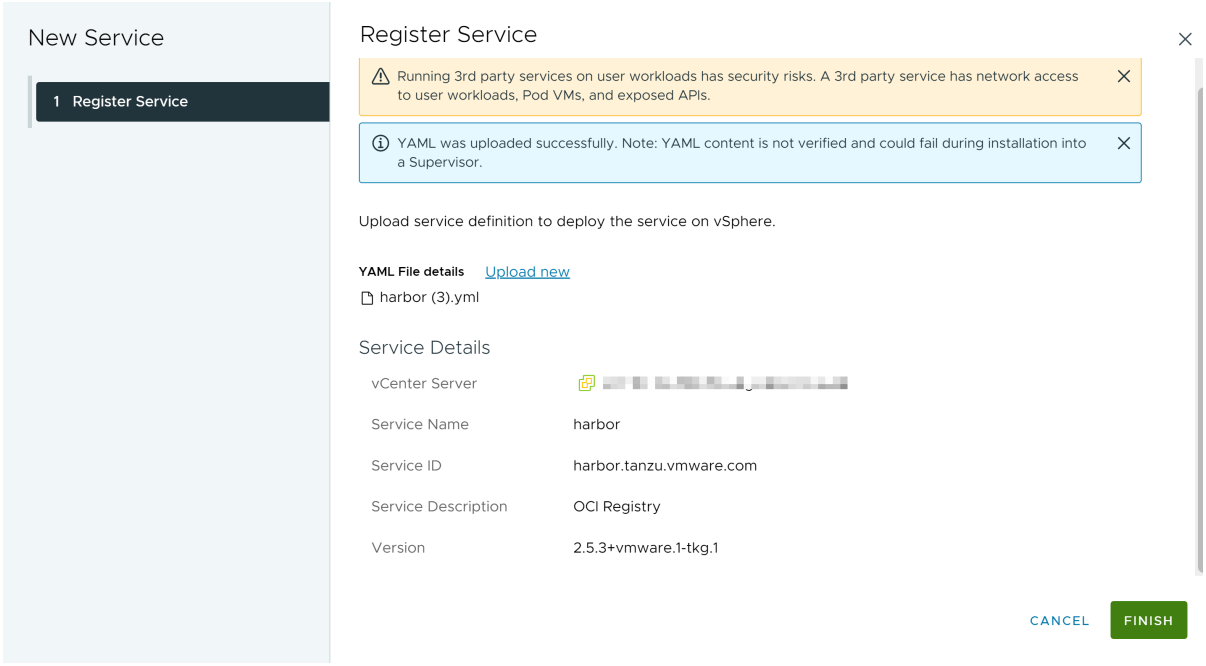
- Stellen Sie sicher, dass Sie auf vCenter Server 8.0a oder höher aktualisiert haben. Contour- und Harbor-Supervisor-Dienste werden mit vCenter Server 8.0a und höher unterstützt.
- Überprüfen Sie, ob Sie auf dem vCenter Server-System, dem Sie die Dienste hinzufügen, über die Berechtigung **Supervisor-Dienste verwalten** verfügen.
- Installieren Sie Contour als Supervisor-Dienst auf demselben Supervisor, in dem Sie Harbor installieren möchten. Weitere Informationen hierzu finden Sie unter Installieren von Contour als Supervisor-Dienst in vSphere IaaS control plane.
- Weisen Sie einen FQDN für den Zugriff auf die Harbor-Administrator-Benutzeroberfläche zu.

Verfahren

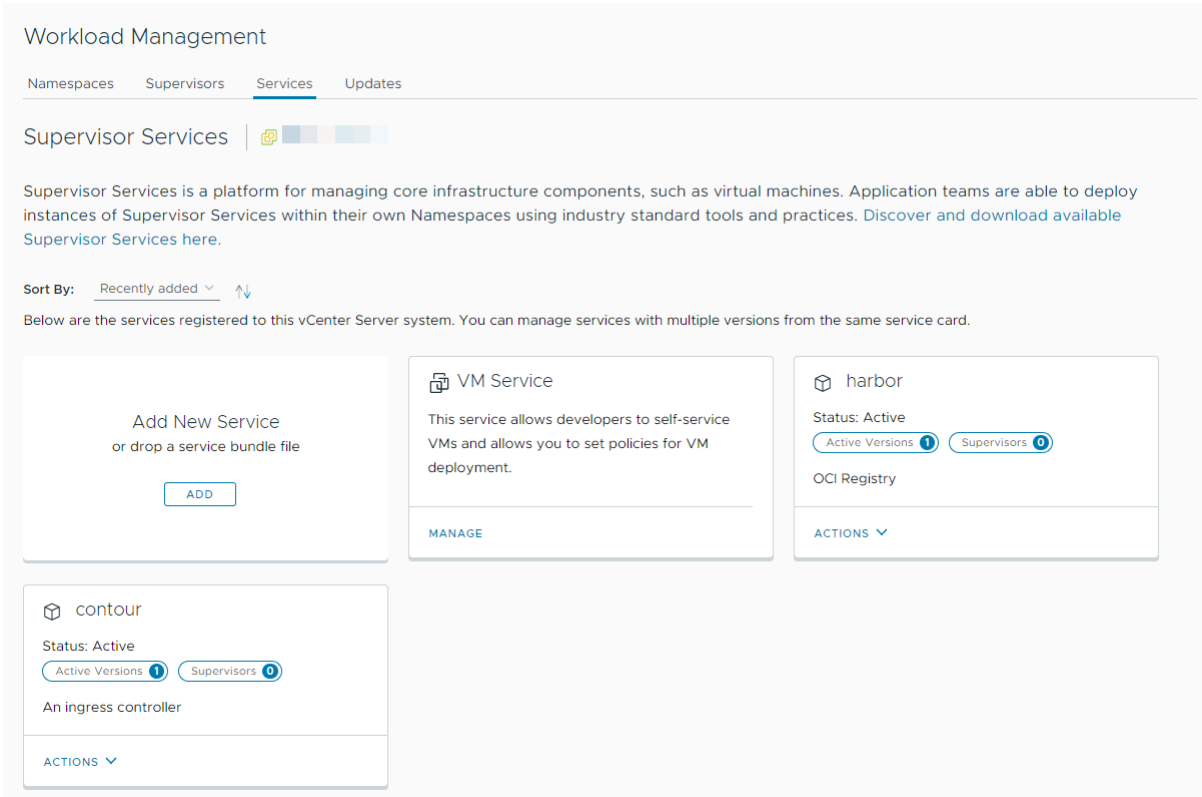
1. Navigieren Sie zum Abschnitt Harbor Versions des Repositorys Supervisor-Services und laden Sie die folgenden Dateien herunter:
   - Die Harbor-Dienstdefinition, der Link lautet `Harbor vX.X.X.`. Beispiel `Harbor 2.5.3`
   - Die Harbor-Konfigurationsdatei, der Link lautet `values for vX.X.X`. Beispiel: `values 2.5.3`

   Die Dateien sehen wie folgt aus:
   - `harbor.yml`
   - `harbor-data-values.yml`
2. Navigieren Sie im vSphere Client zu **Arbeitslastverwaltung** und wählen Sie **Dienste** aus.

3 Stellen Sie den Harbor-Operator bereit, indem Sie auf **Neuen Dienst hinzufügen klicken** und die Dienstdefinition `harbor.yml` hochladen.



Sobald der Harbor-Operator bereitgestellt wurde, wird er auf der Registerkarte **Dienste** angezeigt:



4 Jetzt, da der Harbor-Operator bereitgestellt ist, können Sie den Supervisor-Dienst auf demselben Supervisor installieren, auf dem Contour ausgeführt wird.

a Öffnen Sie die Datei `harbor-data-values.yml` und bearbeiten Sie die Eigenschaften nach Bedarf.

Eigenschaft	Wert	Beschreibung

`hostname: myharbor.com`
 	
`https: 443`
	FQDN	Ändern Sie den FQDN, den Sie für den Zugriff auf die Harbor-Administrator-Benutzeroberfläche festgelegt haben.

`tlsCertificate:`
`tlsSecretLabels:`
`{"managed-by": "vmware-vRegistry"}`
	Hinweis Nicht ändern	Dieser Wert ist erforderlich, damit die TKG-Integration funktioniert.

`harborAdminPassword:` `Harbor12345`	Er kann optional geändert werden.	Das Harbor-Kennwort wird bei der Installation verwendet. Sie können es über die Harbor-Administrator-Benutzeroberfläche ändern, sobald der Dienst installiert wurde.
`secretKey:` `0123456789ABCDEF`	Folge von 16 Zeichen	Der für die Verschlüsselung verwendete geheime Schlüssel. Muss eine Folge von 16 Zeichen sein.
`database:` `password: change-it`	Ein sicheres Kennwort	Ein anfängliches Kennwort für die Postgres-Datenbank.

`core:`
`replicas:`
`secret: change-it`
`xsrfKey:`
`0123456789ABCDEF0123456789ABCDEF`
`jobservice:`
`replicas: 1`
`secret: change-it`
`registry:`
`replicas:`
`secret: change-it`
	Zeichenfolgen für die geheimen Schlüssel und eine XSRF-Schlüsselzeichenfolge mit 32 Zeichen	Ändern Sie diese Option, um Ihre eigenen geheimen Schlüssel einzurichten.

`persistence:`
`persistentVolumeClaim:`
`registry:`
 	
`storageClass: "insert-storage-class-name-here"`
`subPath: ""`
`accessMode: ReadWriteOnce`
`size: 10Gi`
`jobservice:`
	Name der Speicherklasse	Die Speicherrichtlinien, die als Speicherklassen für die Bereitstellung von PVCs verwendet werden, in der Harbor-Registrierung, dem Auftragsdienst, der Datenbank usw.
		Legen Sie alle Eigenschaften auf vorhandene Speicherrichtlinien fest, die in Ihrer Umgebung verfügbar sind. Ändern Sie den Namen der Speicherrichtlinie in einen gültigen

Eigenschaft	Wert	Beschreibung

`storageClass: "insert-storage-class-name-here"`
`subPath: ""`
`accessMode: ReadWriteOnce`
`size: 1Gi`
`database:`
 	
`storageClass: "insert-storage-class-name-here"`
`subPath: ""`
`accessMode: ReadWriteOnce`
`size: 1Gi`
`redis:`
 	
`storageClass: "insert-storage-class-name-here"`
`subPath: ""`
`accessMode: ReadWriteOnce`
`size: 1Gi`
`trivy:`
 	
`storageClass: "insert-storage-class-name-here"`
`subPath: ""`
`accessMode: ReadWriteOnce`
`size: 5Gi`
		Speicherklassennamen, indem Sie auch alle Großbuchstaben durch Kleinbuchstaben ersetzen und alle „_“-Symbole und Leerzeichen durch einen Bindestrich „-“ ersetzen. Ändern Sie beispielsweise **`Harbor-Speicherrichtlinie`** in **`harbor-storage-policy`**.

`network:` `ipFamilies: ["IPv4"]`	**Hinweis** Nicht ändern	IPv6 wird nicht unterstützt.

b Gehen Sie zurück zu **Arbeitslastverwaltung > Dienste** und wählen Sie auf der Dienstkarte **Harbor** die Option **Aktionen > Auf Supervisoren installieren** aus.

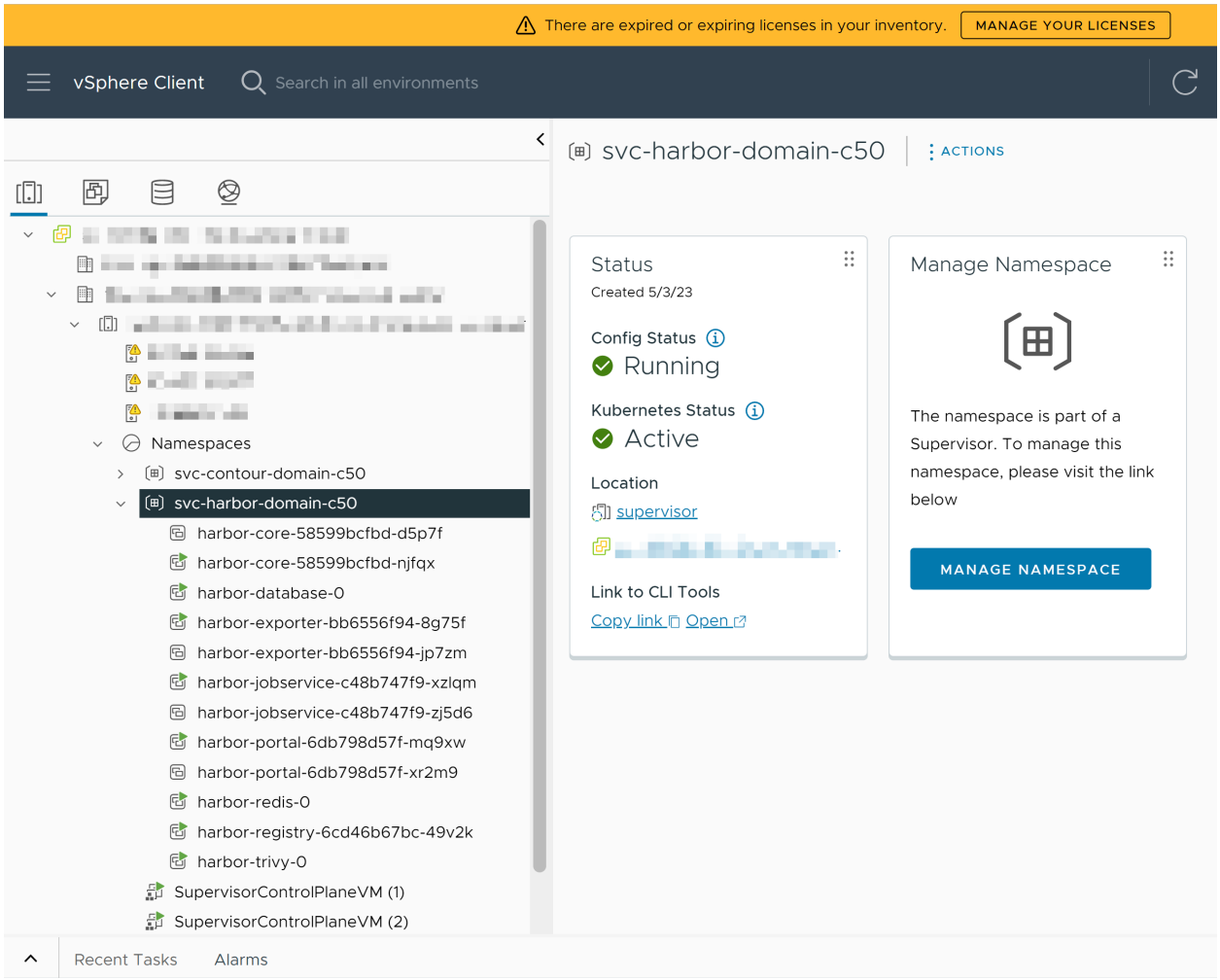
c Wählen Sie den Supervisor aus, auf dem Contour ausgeführt wird, und kopieren Sie in **YAML-Dienstkonfiguration** den Inhalt der geänderten Datei `harbor-data-values.yml` und fügen Sie ihn ein.

d Klicken Sie auf **OK**.

Sobald die Installation beginnt, können Sie sie verfolgen, indem Sie auf das Feld **Supervisoren** auf der Karte des Harbor-Diensts klicken. Es kann einige Sekunden dauern, bis die Zahl neben **Supervisoren** ansteigt. Der Dienst befindet sich im Konfigurationszustand, bis der gewünschte Zustand erreicht ist. Wenn der gewünschte Zustand erreicht ist, ändert sich der Status des Diensts zu „Wird ausgeführt“.

Ergebnisse

Sie können den vSphere-Namespace und die vSphere-Pods, die für Harbor erstellt wurden, in der Ansicht **Hosts und Cluster** anzeigen.

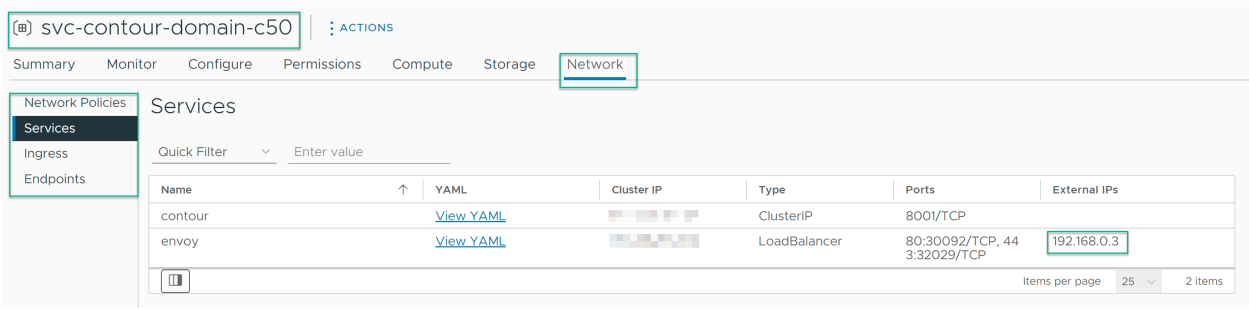


Zuordnen des Harbor-FQDN zur IP-Adresse des Envoy-Ingress

Nachdem Harbor erfolgreich installiert wurde, schließen Sie einen Datensatz der Harbor-FQDN-Zuordnung zur IP-Adresse des Envoy-Ingress in einen externen DNS-Server ein, der mit dem Supervisor konfiguriert ist.

Tanzu Kubernetes Grid-Cluster, vSphere-Pods und der Supervisor müssen den Harbor-FQDN auflösen können, um Images aus der Registrierung abrufen zu können.

Navigieren Sie zum Auffinden der IP-Adresse des Envoy-Ingress zum Contour-Namespace, wählen Sie **Netzwerk** und dann **Dienste** aus:



Einrichten einer Vertrauensstellung mit dem Supervisor-Dienst von Harbor

Nach der Installation von Harbor müssen Sie eine Vertrauensstellung zwischen dem Supervisor und Harbor konfigurieren, um Harbor als Registrierung für vSphere-Pods zu verwenden. Für Tanzu Kubernetes Grid-Cluster, die sich auf demselben Supervisor wie Harbor befinden, wird automatisch eine Vertrauensstellung zwischen Harbor und dem Dienst hergestellt. Um Harbor als Registrierung für Tanzu Kubernetes Grid-Cluster zu verwenden, die auf verschiedenen Supervisoren ausgeführt werden, müssen Sie eine Vertrauensstellung zwischen Harbor und diesen Tanzu Kubernetes Grid-Clustern konfigurieren.

Herstellen einer Vertrauensstellung zwischen Harbor und dem Supervisor

So stellen Sie eine Vertrauensstellung zwischen Harbor und dem Supervisor her:

1 Extrahieren Sie das Harbor-CA-Zertifikat aus der Benutzeroberfläche von Harbor oder mithilfe des geheimen TLS-Schlüssels auf der Steuerungsebene vom Supervisor. Sie können die Harbor-Datei `ca.cert` in der Harbor-Administratorbenutzeroberfläche unter **Administration > Configuration > Registry Root Certificate > Download** abrufen.

2 Fügen Sie das Harbor-CA-Zertifikat zum `image-fetcher-ca-bundle` ConfigMap im `kube-system`-Namespace hinzu. Sie müssen mit einem vCenter Single Sign-On-Administratorkonto angemeldet sein und über die Berechtigung zum Bearbeiten von `image-fetcher-ca-bundle` verfügen.

   a Konfigurieren Sie die Umgebungsvariable KUBE_EDITOR wie hier beschrieben:

   b Bearbeiten Sie die ConfigMap mit dem folgenden Befehl:

   ```
   kubectl edit configmap image-fetcher-ca-bundle -n kube-system
   ```

   c Hängen Sie den Inhalt der Harbor-Datei `ca.cert` an die ConfigMap unterhalb des vorhandenen Supervisor-Zertifikats an. Ändern Sie das Supervisor-Zertifikat auf keinen Fall.

   ```
   apiVersion: v1
   data:
     ca-bundle: |-
       -----BEGIN CERTIFICATE-----
       MIIC/jCCAeagAwIBAgIBADANBgkqhkiG9w0BAQsFADAVMRMwEQYDVQQDEwprdWJl
   ```

```
    ...
    qB72tWi8M5++h2RGcVash0P1CUZOHkpHxGdUGYv1Z97Wl89dT2OTn3iXqn8d1JAK
    aF8=
    -----END CERTIFICATE-----
    -----BEGIN CERTIFICATE-----
    MIIDKDCCAhCgAwIBAgIQBbUsj7mqXXC5XRhqqU3GiDANBgkqhkiG9w0BAQsFADAU
    ...
    5q7y87vOLTr7+0MG4O01zK0dJYx2jVhZlsuduMYpfqRLLewVl0eGu/6vr2M=
    -----END CERTIFICATE-----
kind: ConfigMap
metadata:
  creationTimestamp: "2023-03-15T14:28:34Z"
  name: image-fetcher-ca-bundle
  namespace: kube-system
  resourceVersion: "713"
  uid: 6b7611a0-25fa-40f7-b4f5-e2a13bd0afe3
```

d Speichern Sie die an der Datei vorgenommenen Änderungen. Als Ergebnis meldet kubectl:

```
configmap/image-fetcher-ca-bundle bearbeitet
```

Einrichten einer Vertrauensstellung zwischen Harbor und Tanzu Kubernetes Grid-Clustern mit anderen Supervisoren als Harbor

Tanzu Kubernetes Grid-Cluster, die auf anderen Supervisoren als dem ausgeführt werden, auf dem Harbor installiert ist, müssen über Netzwerkkonnektivität mit Harbor verfügen. Diese Tanzu Kubernetes Grid-Cluster müssen den Harbor-FQDN auflösen können.

Um eine Vertrauensstellung zwischen Harbor und den Tanzu Kubernetes Grid-Clustern herzustellen, extrahieren Sie das Harbor-CA-Zertifikat aus der Benutzeroberfläche von Harbor oder mithilfe des geheimen TLS-Schlüssels auf der Supervisor-Steuerungsebene. Führen Sie dann die unter Integrieren eines TKG 2-Clusters mit einer privaten Containerregistrierung aufgeführten Schritte aus.

Migrieren von Images aus der eingebetteten Registrierung zu Harbor in vSphere IaaS control plane

Wenn Sie die eingebettete Harbor-Registrierung mit Ihrem Supervisor verwenden, können Sie die Images aus der eingebetteten Registrierung zur Harbor-Registrierung migrieren, die Sie als Supervisor-Dienst installiert haben.

Voraussetzungen

- Stellen Sie sicher, dass die Supervisor-Dienste Contour und Harbor auf dem Supervisor installiert sind.
- Stellen Sie sicher, dass das DNS, das Sie mit Ihrem Supervisor verwenden, den Harbor-FQDN enthält, der der Ingress-IP des Envoy-Diensts zugeordnet ist.

- Stellen Sie sicher, dass zwischen dem Supervisor und Harbor eine Vertrauensstellung besteht. Wenn Images von Tanzu Kubernetes Grid-Clustern referenziert werden, die auf anderen Supervisoren als Harbor ausgeführt werden, stellen Sie bitte sicher, dass zwischen diesen Tanzu Kubernetes Grid-Clustern eine Vertrauensstellung besteht.

Verfahren

1 Melden Sie sich beim Supervisor als vCenter Single Sign-On-Benutzer an.

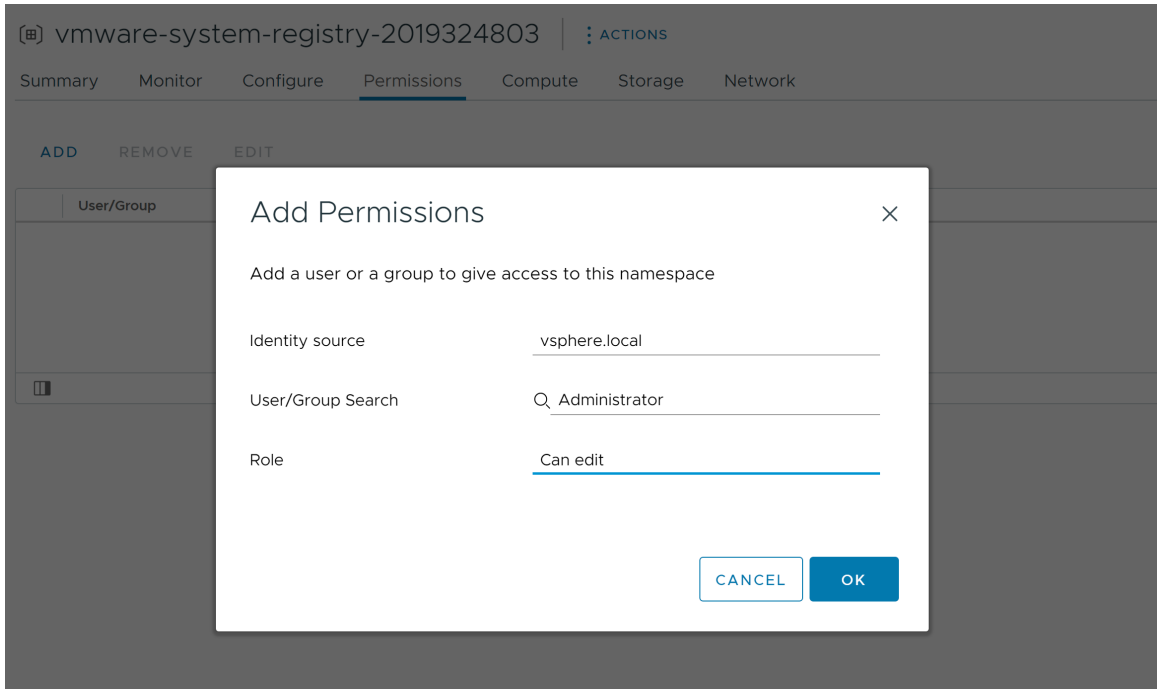
2 Richten Sie den Netzwerkzugriff auf den Supervisor-Dienst von Harbor ein.

   a Erstellen Sie eine Netzwerkrichtlinien-CRD mit dem Namen `allow-all-egress-harbor-supervisor-service` im Dienst-Namespace von Harbor, der beispielsweise `svc-harbor-domain-c9` benannt werden kann.

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: allow-all-egress-harbor-supervisor-service
  namespace: svc-harbor-domain-c9
spec:
  podSelector:
    matchLabels:
      app: harbor
  egress:
  - {}
```

3 Greifen Sie auf die geheimen Schlüssel der eingebetteten Registrierung zu, sodass Sie die Registrierung später als Replizierungs-Endpoint zu Harbor hinzufügen können.

a Gewähren Sie Ihrem vCenter Single Sign-On-Administratorbenutzer im eingebetteten Registrierungs-Namespace Bearbeitungsberechtigungen, die beispielsweise `vmware-system-registry-437393318` benannt werden können.



b Greifen Sie über den eingebetteten Registrierungs-Namespace auf die geheimen Schlüssel zu.

```
# kubectl get secrets -n vmware-system-registry-437393318 harbor-437393318-controller-
registry -o yaml
apiVersion: v1
data:
  harborAdminPassword: UDNSak4wQk5VbFlrY1VZeVprUmpKQT09
  harborAdminUsername: WVdSdGFXND0=
  harborPostgresPassword: TlRoS1ZHeEFLa1lrVkdjaGN6aGtXZz09
kind: Secret
...
```

c Entschlüsseln Sie den Benutzernamen und das Kennwort.

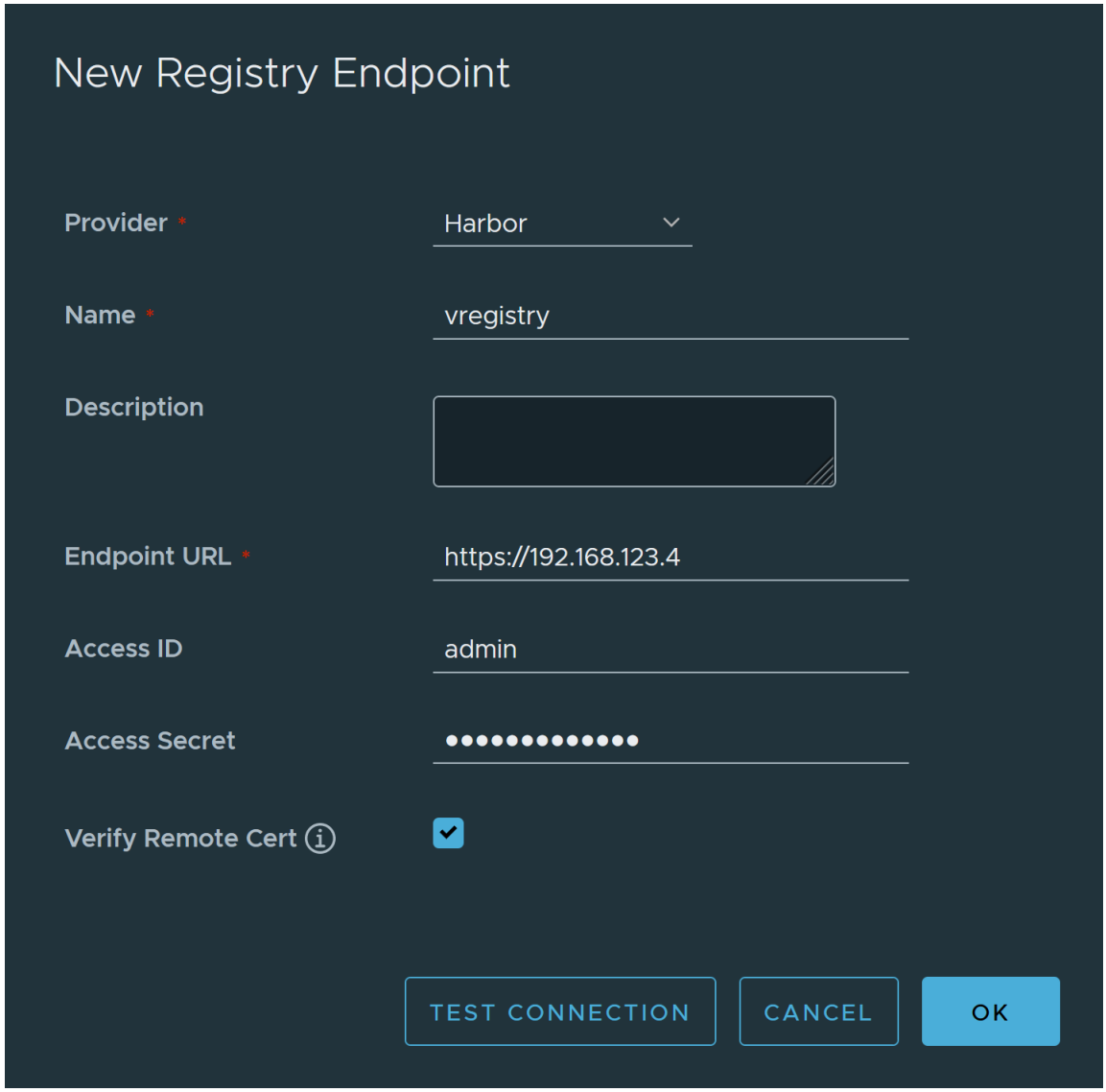
```
# echo 'WVdSdGFXND0=' | base64 -d | base64 -d
admin

# echo 'UDNSak4wQk5VbFlrY1VZeVprUmpKQT09' | base64 -d | base64 -d
?tc7@MRV$qF2fDc$
```

4 Fügen Sie einen Replizierungs-Endpoint und eine Replizierungsregel für die eingebettete Registrierung zum Supervisor-Dienst von Harbor hinzu.

a Melden Sie sich als Root-Benutzer bei der Benutzeroberfläche des Supervisor-Dienst von Harbor an.

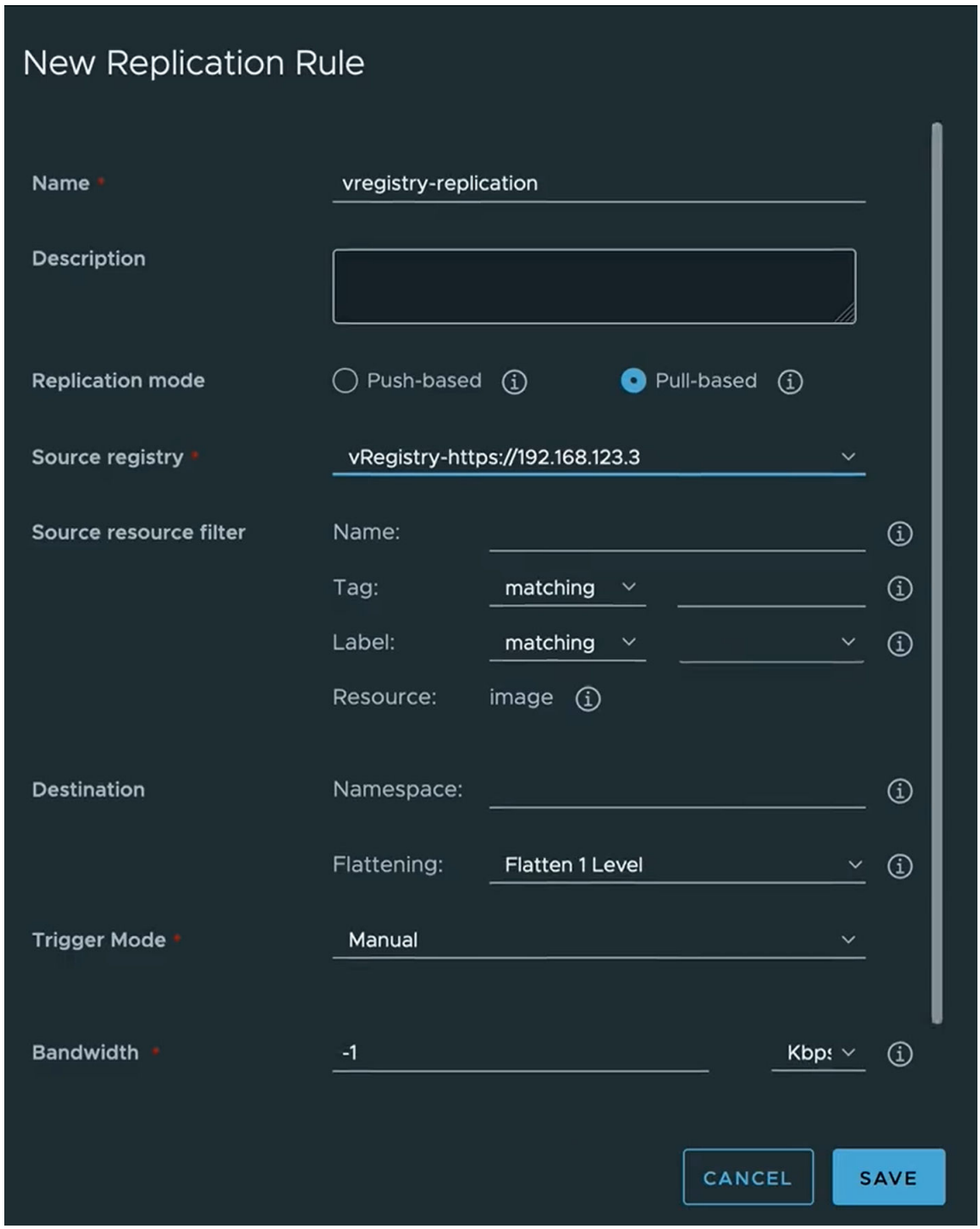
b Klicken Sie auf **Registrierungen** und dann auf **Neuer Endpoint**.



c Wählen Sie die Registerkarte **Replizierungen** aus und klicken Sie auf **Neue Replizierungsregel**.

Geben Sie die folgenden Einstellungen ein und behalten Sie für den Rest die Standardwerte bei:

- **Name** – Geben Sie einen Namen für die Regel an.
- **Replizierungsmodus** – Wählen Sie **Pull-basiert** aus.
- **Quellregistrierung** – Wählen Sie den Registrierungs-Endpoint aus, den Sie hinzugefügt haben.



d Klicken Sie auf **Speichern**.

5 Wählen Sie die neu erstellte Replizierungsregel aus und klicken Sie auf **Replizieren**.

Ergebnisse

Der Inhalt der eingebetteten Registrierung wird in die Harbor-Registrierung repliziert.

Bereitstellen von Supervisor-Dienste in einer Air-Gapped-Umgebung durch Abrufen von Images von einem Proxy

10

Sie können Supervisor-Dienste in einer Air-Gapped-Umgebung bereitstellen, um in einem Intranet private Containerregistrierungen zu nutzen.

Supervisor-Dienste sind Kubernetes-Operatoren, die als Sammlungen von Kubernetes-YAML-Manifesten und Container-Images gespeichert werden und Ressourcen über mehrere Namespaces hinweg bereitstellen können. Dies erfordert eine Reihe von Registrierungsangaben, die für Supervisor üblich sind. Die Bereitstellung von Supervisor-Dienste-Container-Images aus einem privaten Image erfordert das Konfigurieren der Vertrauensstellung und die Authentifizierung für den Supervisor, sofern die private Registrierung eine selbstsignierte Zertifizierungsstelle verwendet und/oder eine Authentifizierung für Image-Abrufe erfordert. Wenn die private Registrierung ein von einer öffentlichen Zertifizierungsstelle signiertes TLS-Zertifikat verwendet, ist keine Konfiguration der Zertifizierungsstelle erforderlich.

Sie können alle Supervisor-Dienste bereitstellen, die entweder über einen Proxy oder aus einer privaten Registrierung in einer Air-Gapped-Umgebung abgerufen werden. Einen vollständigen Satz der Supervisor-Dienste finden Sie unter https://vsphere-tmm.github.io/Supervisor-Services/.

Führen Sie die folgenden Schritte aus:

1 Verlagern Sie die Supervisor-Dienste in eine private Containerregistrierung.

2 Installieren und verwenden Sie die in einer privaten Container-Image-Registrierung gehosteten Supervisor-Dienste.

Lesen Sie als Nächstes die folgenden Themen:

- Verlagern der Supervisor-Dienste in eine private Registrierung
- Installieren und Verwenden des Supervisor-Diensts

Verlagern der Supervisor-Dienste in eine private Registrierung

Verlagern Sie die Supervisor-Dienste in eine private Containerregistrierung.

Voraussetzungen

Stellen Sie sicher, dass Sie über eine private Container-Image-Registrierung verfügen.

Verfahren

1 Installieren Sie das Carvel-Dienstprogramm `imgpkg`.

a Installieren von `imgpkg`

```
wget -O- https://carvel.dev/install.sh > install.sh
sudo bash install.sh
```

b Überprüfen Sie die Installation.

```
imgpkg version
```

Weitere Informationen zum Carvel-Dienstprogramm `imgpkg` finden Sie unter https://carvel.dev/imgpkg/docs/v0.42.x/install/.

2 Rufen Sie das YAML-Manifest für Ihren Dienst ab.

Suchen Sie das `imgpkg`-Paket:

Im Folgenden finden Sie ein Contour-Beispiel:

```
template:
  spec:
    fetch:
    - imgpkgBundle:
        image: projects.registry.vmware.com/tkg/packages/standard/contour:v1.24.4_vmware.1-tkg.1
```

3 Laden Sie ein TAR dieses `imgpkg`-Pakets herunter.

```
imgpkg copy -b projects.registry.vmware.com/tkg/packages/standard/contour:v1.24.4_vmware.1-tkg.1 --to-tar contour-v1.24.4.tar --cosign-signatures
```

Wichtig Sie müssen den Befehl `copy` und nicht die Befehle `push` und `pull` verwenden, um die Images zu verlagern, da sie nicht alle referenzierten Images abrufen.

4 Laden Sie das `imgpkg`-Paket in Ihre private Container-Image-Registrierung hoch.

```
imgpkg copy --tar contour-v1.24.4.tar --to-repo ${registry_url}/contour --cosign-signatures
```

Hinweis `imgpkg` berücksichtigt die Vertrauenseinstellungen des Systems und die Docker-Konfiguration für die Authentifizierung. Wenn Ihre Registrierung eine Authentifizierung erfordert, melden Sie sich zuerst mit dem Docker-CLI-Befehl `docker login ${registry_url}` an.

5 Aktualisieren Sie die YAML-Datei für den Supervisor-Dienst mit der neuen URL für das `imgpkg`-Paket.

Beispiel:

```
template:
  spec:
    fetch:
    - imgpkgBundle:
        image: n.n.n.n/contour:v1.24.4_vmware.1-tkg.1
```

Installieren und Verwenden des Supervisor-Diensts

Nachdem Sie die Supervisor-Dienste in eine private Container-Image-Registrierung verlagert haben, können Sie sie installieren und verwenden.

Fügen Sie zum Verwenden des Supervisor-Diensts zunächst die private Registrierung hinzu, und registrieren und installieren Sie dann die Supervisor-Dienst.

Voraussetzungen

Überprüfen Sie, ob Sie auf dem vCenter Server-System, dem Sie den Dienst hinzufügen, über das Recht **Supervisor-Dienste verwalten** verfügen.

Verfahren

1 Fügen Sie die private Registrierung hinzu.

   a Wählen Sie im vSphere Client-Startmenü die Option **Arbeitslastverwaltung** aus.

   b Klicken Sie auf die Registerkarte **Supervisoren** und wählen Sie einen Supervisor aus der Liste aus.

   c Klicken Sie auf die Registerkarte **Configure** (Konfigurieren) und dann auf **Container Registries** (Containerregistrierungen) und dann **Add** (Hinzufügen).

   d Geben Sie einen Namen für Ihre private Registrierung und optional die Zertifizierungsstelle, den Benutzernamen und das Kennwort ein.

2 Fügen Sie vCenter Server den Supervisor-Dienst hinzu.

   a Wählen Sie im vSphere Client-Startmenü die Option **Arbeitslastverwaltung** aus.

   b Wählen Sie **Dienste** aus.

   c Wählen Sie oben im Dropdown-Menü ein vCenter Server-System aus.

   d Ziehen Sie die YAML-Datei des Diensts auf die Karte **Neuen Dienst hinzufügen** und legen Sie sie dort ab.

3 Installieren des Supervisor-Dienst

   a Wählen Sie im vSphere Client-Startmenü die Option **Arbeitslastverwaltung** aus.

   b Wählen Sie **Dienste** aus.

c Klicken Sie auf der Karte des Supervisor-Dienst, den Sie entfernen möchten, auf **Aktionen > Auf Supervisoren installieren**.

d Wählen Sie den Supervisor aus, in dem Sie den Dienst installieren möchten.

e Geben Sie im Feld **YAML-Dienstkonfiguration** Konfigurationseigenschaften ein, wenn der Dienst diese erfordert.

Geben Sie die Eigenschaften `registryName`, `registryUsername` und `registryPasswd` ein, wenn der Supervisor-Dienst das `SupervisorServiceDefinition`-Format aufweist und die Registrierung eine Authentifizierung erfordert.