Sichern und Wiederherstellen 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

Sicherung und Wiederherstellung der vSphere IaaS-Steuerungsebene

Sicherung und Wiederherstellung der vSphere IaaS-Steuerungsebene liefert Informationen zum Sichern und Wiederherstellen der Supervisor-Steuerungsebene sowie der Arbeitslasten, die auf Tanzu Kubernetes Grid-Clustern und vSphere-Pods ausgeführt werden.

Zielgruppe

Diese Informationen richten sich an vSphere-Administratoren und DevOps-Ingenieure, die Arbeitslasten, die auf vSphere IaaS Control Plane ausgeführt werden, sowie den Status der Supervisor-Steuerungsebene sichern und wiederherstellen möchten. Es sind Kenntnisse in den folgenden Bereichen erforderlich:

- vSphere IaaS Control Plane
- vSphere
- Kubernetes
- Velero
- Instanzspeicher

Überlegungen zum Sichern und Wiederherstellen von vSphere IaaS Control Plane

1

Erfahren Sie, wie der Sicherungs- und Wiederherstellungsprozess für vSphere IaaS Control Plane aussieht, und machen Sie sich mit den wichtigsten Überlegungen zur Implementierung Ihrer Sicherungs- und Wiederherstellungsstrategie für vSphere IaaS Control Plane vertraut.

Szenario	Tools	Anmerkungen
Sichern und Wiederherstellen der Supervisor-Steuerungsebene	vCenter Server dateibasierte Sicherung und Wiederherstellung über die Benutzeroberfläche der Arbeitslastverwaltung	Konfigurieren Sie die Sicherung des Status des Supervisoren in vCenter Server als Teil der geplanten dateibasierten Sicherungen in vCenter Server. Später können Sie den Status des Supervisoren in vCenter Server über die Schnittstelle der Arbeitslastverwaltung im vSphere Client wiederherstellen. **Hinweis** Das Wiederherstellen des Zustands des Supervisoren in vCenter Server und das Wiederherstellen des Zustands von vCenter Server sind zwei unterschiedliche Workflows. Das Wiederherstellen von vCenter Server führt nicht zur Wiederherstellung des Supervisoren-Hosts. Weitere Informationen hierzu finden Sie unter Kapitel 2 Sichern und Wiederherstellen der Supervisor-Steuerungsebene.
Sichern und Wiederherstellen von vSphere-Pods	Velero-Plug-In für vSphere	Installieren und Konfigurieren des Plug-Ins im Supervisor. Weitere Informationen hierzu finden Sie unter Kapitel 3 Installieren und Konfigurieren des Velero-Plug-In für vSphere im Supervisor. Weitere Informationen hierzu finden Sie unter Kapitel 6 Sichern und Wiederherstellen von vSphere-Pods mit Velero-Plug-In für vSphere.

Szenario	Tools	Anmerkungen
Sichern Sie statusfreie und statusbehaftete Arbeitslasten auf einem Tanzu Kubernetes Grid-Cluster und stellen Sie sie auf einem Cluster wieder her, der von Tanzu Kubernetes Grid bereitgestellt wird.	Velero-Plug-In für vSphere	Sichern und Wiederherstellen von Kubernetes-Metadaten und dauerhaften Volumes. Sie können Velero-Snapshots (nicht Restic) für dauerhafte Volumes verwenden. Weitere Informationen hierzu finden Sie unter Kapitel 3 Installieren und Konfigurieren des Velero-Plug-In für vSphere im Supervisor. Weitere Informationen finden Sie unter Sichern und Wiederherstellen von TKG 2-Clusterarbeitslasten mit dem Velero-Plug-In für vSphere.
Sichern Sie statusfreie und statusbehaftete Arbeitslasten auf einem Tanzu Kubernetes Grid-Cluster und stellen Sie sie auf einem konformen Kubernetes-Cluster wieder her, der nicht von Tanzu Kubernetes Grid bereitgestellt wird.	Eigenständiges Velero und Restic	Verwenden Sie eigenständiges Velero für die Portabilität. Muss Restic für statusbehaftete Anwendungen enthalten. Weitere Informationen finden Sie unter Installieren und Konfigurieren von eigenständigem Velero und Restic in TKG 2-Clustern auf Supervisor. Weitere Informationen finden Sie unter Sichern und Wiederherstellen von Arbeitslasten für TKG 2-Clusterarbeitslasten auf Supervisor mit eigenständigem Velero und Restic.
vCenter Server-Konfiguration	vCenter Server	Wenn vCenter Server verloren geht, verwenden Sie vCenter Server, um vCenter Server-Objekte zu sichern und wiederherzustellen. Weitere Informationen finden Sie unter Dateibasierte Sicherung und Wiederherstellung von vCenter Server.
NSX	NSX Manager	Lastausgleichs- und Ingress-Dienste hängen von der NSX-Sicherung ab. NSX-T Data Center ermöglicht die produktinterne Sicherung und Wiederherstellung, die die Sicherung und Wiederherstellung der NSX Manager-Knoten und -Objekte unterstützt. Weitere Informationen finden Sie unter Sichern und Wiederherstellen von NSX Manager in der NSX-T-Dokumentation.

Sichern und Wiederherstellen der Supervisor-Steuerungsebene

2

Sie können die Option zum Aufzeichnen des Status des Supervisoren in vCenter Server als Teil der dateibasierten vCenter Server-Sicherungen einbeziehen. Später können Sie die Supervisor-Steuerungsebene aus den erstellten Sicherungsdateien wiederherstellen.

Lesen Sie als Nächstes die folgenden Themen:

- Sichern des Supervisor-Status
- Wiederherstellen der Supervisor-Steuerungsebene

Sichern des Supervisor-Status

Erfahren Sie, wie Sie den Status des Supervisoren in Ihrer Umgebung sichern. Sie können die Sicherung des in vCenter Server verfügbaren Supervisoren als Teil der vCenter Server-dateibasierten Backups einschließen.

Die Sicherungsdateien für die Supervisor-Steuerungsebene erfassen den Status der folgenden Komponenten:

- Den etcd-Status.
- Container-Images, die für Infrastruktur-Pods verwendet werden, um sicherzustellen, dass VMs der Steuerungsebene nach einem vCenter Server-Upgrade wiederhergestellt werden können.
- Das Kubernetes-CA-Zertifikat und den Schlüssel, um sicherzustellen, dass alle Kubernetes-Zertifikate nach einer Wiederherstellung von derselben Zertifizierungsstelle neu generiert werden können. Dadurch wird sichergestellt, dass vSphere-Pods und das Spherelet nach der Wiederherstellung nicht neu konfiguriert werden müssen, um einer neuen Kubernetes-Zertifizierungsstelle zu vertrauen.
- Alle vSphere-Namespaces und den Status aller Kubernetes-Ressourcen, die Arbeitslasten zugeordnet sind, wie z. B. Bereitstellungen, Pods, VMs, TKG-Ressourcen, Ansprüche an dauerhafte Volumes usw.

Weitere Informationen zum vCenter Server-dateibasierten Sichern und Wiederherstellen finden Sie unter Dateibasierte Sicherung und Wiederherstellung von vCenter Server.

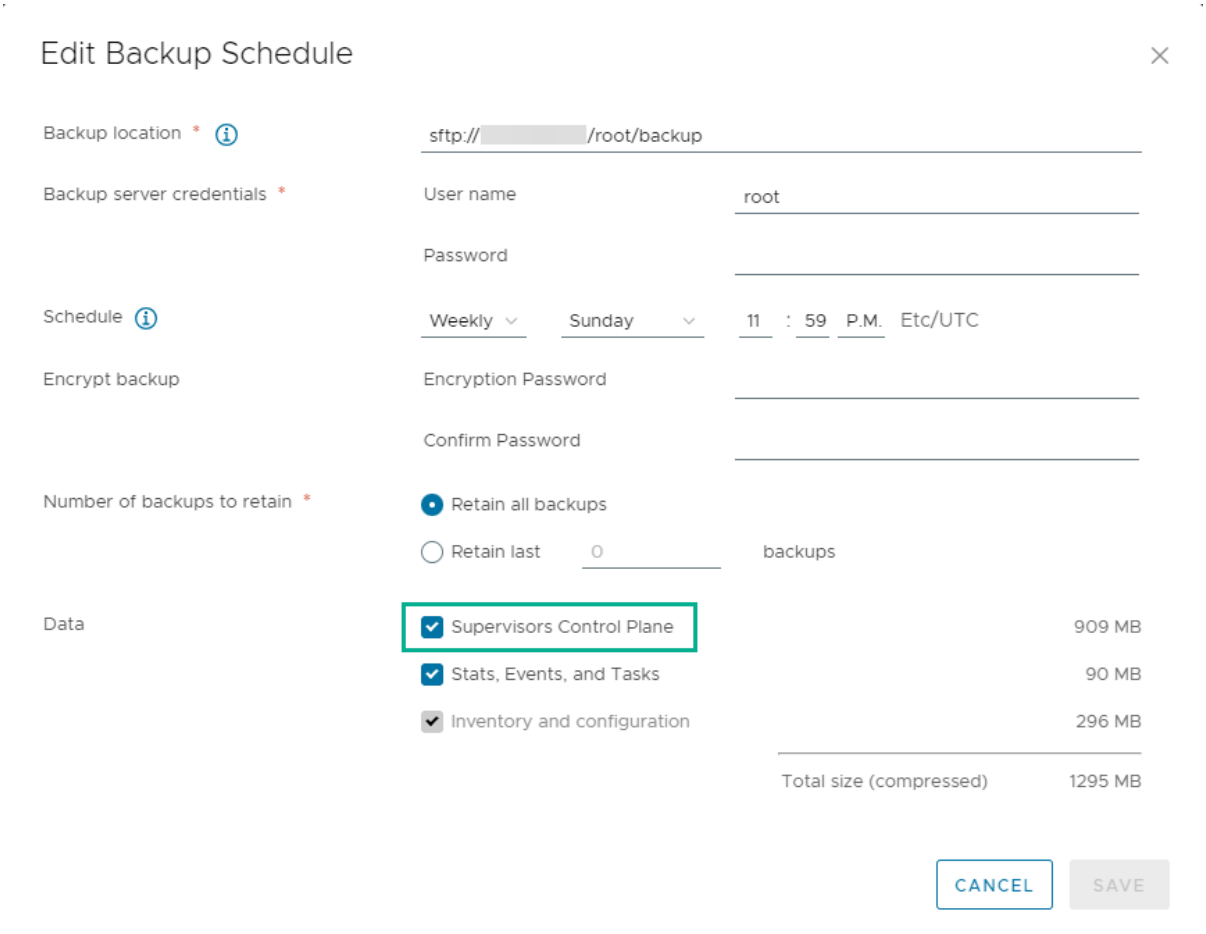
Voraussetzungen

- Sie müssen über einen FTP-, FTPS-, HTTP-, HTTPS-, SFTP-, NFS- oder SMB-Server verfügen und dieser muss mit genügend Festplattenspeicher zum Speichern der Sicherung ausgeführt werden.

Verfahren

1. Gehen Sie im Webbrowser zur vCenter ServerManagement-Schnittstelle, `https://appliance-IP-address-or-FQDN:5480`.
2. Melden Sie sich als „root“ an.
3. Klicken Sie in der vCenter Server-Verwaltungsschnittstelle auf **Sichern**.
4. Klicken Sie auf **Bearbeiten**, wenn bereits ein Sicherungszeitplan vorhanden ist.

   Wenn kein Sicherungszeitplan vorhanden ist, finden Sie unter Dateibasierte Sicherung planen weitere Informationen zum Erstellen eines Sicherungsplans.
5. Wählen Sie im Bereich Sicherungsplan bearbeiten die Option **Supervisor-Steuerungsebene** aus.



Ergebnisse

Der Status aller Supervisoren in vCenter Server wird als Teil der vCenter Server-Sicherungen gesichert.

Wiederherstellen der Supervisor-Steuerungsebene

Sie können das Supervisoren-Steuerungsfenster in vCenter Server aus den Sicherungsdateien des vCenter Server-Systems selbst wiederherstellen.

Hinweis Das Wiederherstellen der Supervisoren-Steuerungsebene in vCenter Server und das Wiederherstellen des Zustands von vCenter Server sind zwei unterschiedliche Workflows. Das Wiederherstellen von vCenter Server führt nicht zur Wiederherstellung der Supervisor-Steuerungsebene.

Voraussetzungen

- Konfigurieren Sie die Aufzeichnung des Supervisor-Status über dateibasierte Sicherungen der vCenter Server Managementschnittstelle.

Verfahren

1. Navigieren Sie im vSphere Client zu **Arbeitslastverwaltung**.
2. Wählen Sie **Supervisoren** und dann **Wiederherstellen** aus.
3. Geben Sie die Backup-Details ein.

Option	Bezeichnung
vCenter	Wählen Sie das vCenter Server-System aus, das den Supervisor verwaltet.
Auswahl der Sicherung	■ Wählen Sie **Backup-Server-Ordner durchsuchen** aus, um die im Root-Ordner des mit diesem vCenter Server-System konfigurierten Backup-Dateiservers gespeicherten Dateien hochzuladen. ■ Wählen Sie **Einzelner Sicherungsspeicherort** aus, um eine bestimmte Sicherungsdatei hochzuladen, und geben Sie dann die URL zu dieser Sicherungsdatei ein. ■ Wählen Sie **Sicherungsort und Benutzername aus vCenter Sicherungszeitplan verwenden** aus, um den Speicherort des Root-Ordners und den Benutzernamen für den Sicherungsspeicherort aufzufüllen, der mit vCenter Server konfiguriert ist.
Speicherort	Geben Sie den Speicherort des Sicherungs-Root-Ordners ein.
Benutzername	Eingeben des Benutzernamens für den Zugriff auf die Sicherungen
Kennwort	Geben Sie das Kennwort für den Benutzernamen ein.

4. Klicken Sie auf **Weiter**.
5. Wählen Sie eine Sicherungsdatei aus und klicken Sie auf **Weiter**, um den Download der Sicherungsdatei zu starten.
6. Wählen Sie den wiederherzustellenden Supervisor aus und klicken Sie auf **Weiter**.

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

Ergebnisse

Der Supervisor wechselt in den Konfigurationszustand zurück und alle gelöschten Steuerungsebenen-VMs haben eine erneute Bereitstellung mit den Daten aus der Sicherungsdatei. Sie können den Prozess überwachen, indem Sie in der Spalte **Konfigurationsstatus** auf **Ansicht** klicken.

Installieren und Konfigurieren des Velero-Plug-In für vSphere im Supervisor

3

Erfahren Sie, wie Sie das Velero-Plug-In für vSphere zur Sicherung und Wiederherstellung von Arbeitslasten auf vSphere-Pods und in TKG-Clustern installieren und konfigurieren.

Überblick

Das Velero-Plug-In für vSphere bietet eine Lösung zum Sichern und Wiederherstellen von vSphere IaaS Control Plane-Arbeitslasten. Nachdem Sie das Velero-Plug-In für vSphere im Supervisor installiert und konfiguriert haben, können Sie TKG-Clusterarbeitslasten und vSphere-Pods sichern und wiederherstellen. Für persistente Arbeitslasten können Sie mit dem Velero-Plug-In für vSphere Snapshots der persistenten Volumes erstellen.

Voraussetzungen:

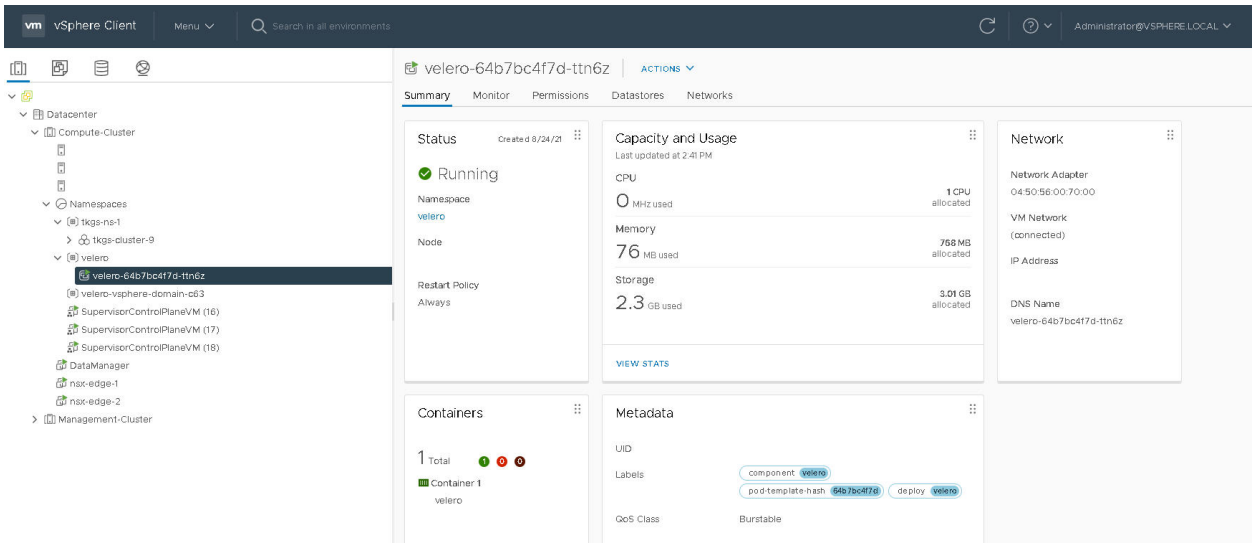
- Supervisor ist aktiviert.
- Ein vSphere-Namespace wird erstellt und konfiguriert.
- Sie müssen Mitglied der vSphere-Administratorrolle sein oder über die folgenden vSphere-Rechte verfügen:
  - **SupervisorServices.Manage**
  - **Namespaces.Manage**
  - **Namespaces.Configure**

  Hinweis Weitere Informationen finden Sie unter Erstellen einer dedizierten Gruppe und Rolle in *Verwenden des TKG-Dienstes mit der vSphere IaaS-Steuerungsebene*.
- Erstellen Sie eine Linux-VM, auf der Sie die Velero-CLI ausführen können. Oder verwenden Sie einen vorhandenen Linux-Jump-Host, über den Sie auf den Supervisor zugreifen können.
- Die Velero-Versionsnummern werden als `X.Y.Z` dargestellt. In der Velero-Kompatibilitätsmatrix finden Sie die spezifischen Versionen, die verwendet werden sollen. Ersetzen Sie sie entsprechend beim Ausführen der Befehle.

Der Screenshot zeigt den Endzustand einer Velero-Plug-In für vSphere-Installation.

- Zur Unterstützung der Bereitstellung von vSphere-Pods wird ein NSX-Netzwerk verwendet.

- Eine Datenmanager-VM ist bereitgestellt.
- Der Velero-Operator ist aktiviert und wird im `velero-vsphere-domain-cXX`-Namespace ausgeführt.
- Ein Namespace mit der Bezeichnung `velero` ist konfiguriert..
- Das Velero-Plug-In für vSphere wird als vSphere Pod im `velero` Namespace ausgeführt.



Schritt 0 (Optional): Erstellen eines dedizierten Netzwerks für die Sicherung und Wiederherstellung des Datenverkehrs

Sie können den Sicherungs- und Wiederherstellungsdatenverkehr für Produktionsumgebungen vom Netzwerkdatenverkehr für die vSphere IaaS Control Plane-Verwaltung trennen. Dies ist zwar nicht erforderlich, wird aber empfohlen. Dabei sind zwei Aspekte zu beachten:

- Taggen der ESXi-Hosts für die Unterstützung von Network File Copy (NFC)
- Konfigurieren des Sicherungs- und Wiederherstellungsnetzwerks mit NSX.

Um ESXi-Hosts so zu konfigurieren, dass sie einen Transport von dedizierten Netzwerkblockgeräten (Network Block Device, NBD) unterstützen, fügen Sie auf jedem ESXi-Host im vSphere-Cluster, auf dem Supervisor aktiviert ist, eine VMkernel-NIC hinzu, und legen Sie die `vSphereBackupNFC` auf dieser NIC fest. Wenn das Tag `vSphereBackupNFC` auf den NIC-Typ für einen VMkernel-Adapter angewendet wird, wird der Sicherungs- und Wiederherstellungsdatenverkehr durch die ausgewählte virtuelle NIC geleitet.

Um diese Konfiguration durchzuführen, verwenden Sie das Virtual Disk Development Kit. Weitere Informationen hierzu finden Sie in der NBD-Dokumentation.

Hinweis Wenn die `vSphereBackupNFC` auf der VMkernel-NIC nicht aktiviert ist, wird der Sicherungs- und Wiederherstellungsdatenverkehr nicht auf dem Sicherungs- und Wiederherstellungsnetzwerk gesendet, selbst wenn Sie eines konfigurieren. Ist `vSphereBackupNFC` nicht aktiviert, wird der Datenverkehr über das vSphere-Verwaltungsnetzwerk übertragen.

Sobald das `vSphereBackupNFC`-Tag aktiviert ist, konfigurieren Sie das Sicherungs- und Wiederherstellungsnetzwerk mit NSX, indem Sie den vorhandenen vSphere Distributed Switch (VDS) für den Cluster wie folgt aktualisieren:

- Klicken Sie im vSphere Client auf **Menü > Verwaltung**.
- Wählen Sie den vorhandenen VDS für den Cluster aus.
- Klicken Sie mit der rechten Maustaste auf den VDS und wählen Sie dann **Verteilte Portgruppe > Neue verteilte Portgruppe** aus.
- Erstellen Sie eine neue verteilte Portgruppe mit dem Namen **BackupRestoreNetwork**.
- Fügen Sie der verteilten Portgruppe **BackupRestoreNetwork** einen VMkernel-Adapter hinzu.
- Verbinden Sie alle ESXi-Hosts im vCenter-Cluster, in dem die Arbeitslastverwaltung aktiviert ist, mit der verteilten Portgruppe **BackupRestoreNetwork**.
- Aktivieren Sie das `vSphereBackupNFC`-Tag.

Schritt 1: Erstellen eines S3-kompatiblen Objektspeichers

Zum Sichern und Wiederherstellen persistenter Volumes müssen Sie einen S3-kompatiblen Objektspeicher bereitstellen. Velero unterstützt eine Reihe von Objektspeicher-Anbietern.

Für die Installation des Velero-Plug-In für vSphere müssen Sie die folgenden Informationen über Ihren S3-kompatiblen Objektspeicher bereitstellen:

Datenelement	Beispielwert
s3Url	http://my-s3-store.example.com
aws_access_key_id	ACCESS-KEY-ID-STRING
aws_secret_access_key	SECRET-ACCESS-KEY-STRING

Erstellen Sie eine Datei für geheime Schlüssel mit dem Namen `s3-credentials` und den folgenden Informationen. Beim Installieren des Velero-Plug-In für vSphere werden Sie auf diese Datei verweisen.

```
[default]
aws_access_key_id = ACCESS-KEY-ID-STRING
aws_secret_access_key = SECRET-ACCESS-KEY-STRING
```

MinIO ist ein S3-kompatibler Objektspeicher, der einfach zu installieren und zu verwenden ist. vSphere IaaS Control Plane wird mit einem MinIO-Supervisor-Dienst geliefert, den Sie aktivieren können. Weitere Informationen finden Sie in der Veröffentlichung *Dienste und Arbeitslasten der vSphere IaaS-Steuerungsebene*.

Alternativ können Sie einen MinIO-Server manuell auf einer Linux-VM installieren. Anweisungen finden Sie unter Installieren und Konfigurieren von eigenständigem Velero und Restic in TKG-Clustern.

Schritt 2: Installieren und Konfigurieren des Data Manager

Warnung Der Data Manager ist nur funktionell getestet und nicht dazu gedacht, im großen Umfang zu arbeiten. Er verspricht keine Leistungserwartungen. Er ist nicht dazu gedacht, geschäftskritische Anwendungen in der Produktion zu sichern.

Um die Sicherung und Wiederherstellung mithilfe von Velero-Plug-In für vSphere zu erleichtern, stellen Sie eine oder mehrere Data Manager-VMs bereit, damit Sie Sicherungsdaten von persistenten Volumes im S3-kompatiblen Objektspeicher verschieben können. Bei der Sicherung verschiebt der Data Manager die Volume-Snapshot-Daten vom vSphere-Volume auf den externen persistenten S3-kompatiblen Speicher, und bei der Wiederherstellung verschiebt er jene Daten vom externen S3-kompatiblen Speicher auf ein vSphere-Volume.

Installieren Sie den Data Manager in einer vSphere IaaS Control Plane-Umgebung als VM.

Hinweis Schalten Sie die Data Manager-VM erst ein, nachdem Sie den Velero-vSphere-Operator aktiviert haben.

1. Klicken Sie mit dem vSphere Client mit der rechten Maustaste auf das Datencenter, in dem Supervisor aktiviert ist, und wählen Sie **OVF-Vorlage bereitstellen** aus.
2. Laden Sie die Data Manager-OVA-Datei über die folgende URL auf Ihre lokale Maschine herunter: https://vmwaresaas.jfrog.io/artifactory/Velero-YAML/Velero/DataManager/1.2.0/datamgr-ob-20797900-photon-3-release-1.2.ova.
3. Wählen Sie **Lokale Datei** aus und laden Sie die Data Manager-OVA-Datei auf vCenter Server hoch.
4. Benennen Sie die virtuelle Maschine beispielsweise als **`DataManager`**.
5. Wählen Sie die Computing-Ressource aus, bei der es sich um den vSphere-Cluster handelt, in dem der Supervisor konfiguriert ist.
6. Überprüfen Sie die VM-Bereitstellungsdetails und klicken Sie auf **Weiter**.
7. Akzeptieren Sie die Lizenzvereinbarungen und klicken Sie auf **Weiter**.
8. Wählen Sie den Speicher aus und klicken Sie auf **Weiter**.

9 Wählen Sie das Zielnetzwerk für die Datenmanager-VM aus.

- Klicken Sie auf **BackupRestoreNetwork**, wenn Sie ein dediziertes Sicherungs- und Wiederherstellungsnetzwerk konfiguriert haben.
- Klicken Sie auf **Verwaltungsnetzwerk**, wenn Sie kein dediziertes Sicherungs- und Wiederherstellungsnetzwerk konfiguriert haben.

10 Bestätigen Sie Ihre Auswahl und klicken Sie auf **Beenden**, um den Vorgang abzuschließen.

11 Sie haben die Möglichkeit, den Status der Bereitstellung im Fensterbereich „Kürzlich bearbeitete Aufgaben“ zu überwachen.

Hinweis Wenn Sie eine Fehlermeldung erhalten, dass der „OVF-Deskriptor nicht verfügbar“ ist, verwenden Sie den Chrome-Browser.

12 Konfigurieren Sie nach der Bereitstellung der Data Manager-VM die Eingabeparameter für die VM.

13 Klicken Sie mit der rechten Maustaste auf die VM und wählen Sie **Einstellungen bearbeiten** aus.

14 Wechseln Sie auf der Registerkarte „Virtuelle Hardware“ für das CD/DVD-Laufwerk von **Host-Gerät** zu **Client-Gerät**.

Hinweis Wenn Sie dies nicht tun, können Sie die erforderlichen erweiterten Konfigurationseinstellungen nicht speichern.

15 Wählen Sie auf der Registerkarte **Einstellungen bearbeiten > Erweiterte Parameter** die Optionen **Erweitert > Konfigurationsparameter bearbeiten**.

16 Konfigurieren Sie die Eingabeparameter für jede der folgenden Einstellungen:

Parameter	Wert
`guestinfo.cnsdp.vcUser`	Geben Sie den vCenter Server-Benutzernamen mit den ausreichenden Berechtigungen ein, um VMs bereitzustellen. Wenn Sie keinen Benutzer mit vSphere-Administratorberechtigungen angeben, finden Sie weitere Informationen in der Dokumentation zu vSphere-Berechtigungen. Sie können auch einen dedizierten Benutzer für die Arbeitslastverwaltung anlegen. Weitere Informationen finden Sie unter Erstellen einer dedizierten Gruppe und Rolle in *Verwenden des TKG-Dienstes mit der vSphere IaaS-Steuerungsebene*.
`guestinfo.cnsdp.vcAddress`	Geben Sie die vCenter Server-IP-Adresse oder den FQDN ein.
`guestinfo.cnsdp.vcPasswd`	Geben Sie das vCenter Server-Benutzerkennwort ein.
`guestinfo.cnsdp.vcPort`	Die Standardeinstellung lautet **`443`**. Ändern Sie diesen Wert nicht.

Parameter	Wert
`guestinfo.cnsdp.wcpControlPlaneIP`	Geben Sie die Floating IP-Adresse des Supervisor ein. Rufen Sie diesen Wert ab, indem Sie zum Supervisor in der Arbeitslastverwaltung gehen und **Konfigurieren > Netzwerk > Verwaltungsnetzwerk > Floating IP-Adresse** auswählen
`guestinfo.cnsdp.updateKubectl`	Der Standardwert lautet **`false`**. Ändern Sie diesen Wert nicht.
`guestinfo.cnsdp.veleroNamespace`	Behalten Sie den Standardwert `velero` bei. Später im Prozess werden Sie einen vSphere-Namespace auf dem Supervisor mit dem Namen `velero` erstellen. Diese beiden Namen müssen übereinstimmen.
`guestinfo.cnsdp.datamgrImage`	Wenn nicht konfiguriert (nicht festgelegt), ruft das System standardmäßig das Container-Image aus dem Docker Hub unter `vsphereveleroplugin/data-manager-for-plugin:1.1.0` ab.

17 Klicken Sie auf **OK**, um die Konfiguration zu speichern, und erneut auf **OK**, um die VM-Einstellungen zu speichern.

Hinweis Wenn Sie das CD/DVD-Laufwerk nicht von **Host-Gerät** zu **Client-Gerät** geändert haben, können Sie die Einstellungen nicht speichern. Brechen Sie in diesem Fall den Vorgang ab, wechseln Sie das Laufwerk und wiederholen Sie die erweiterten Konfigurationseinstellungen.

18 Schalten Sie die Data Manager-VM erst ein, nachdem Sie den Velero-vSphere-Operator aktiviert haben (nächster Abschnitt).

Schritt 3 : Installieren des Velero-vSphere-Operator-Diensts auf dem Supervisor

vSphere IaaS Control Plane stellt den Velero-vSphere-Operator als Supervisor-Dienst bereit. Der Velero-vSphere-Operator-Dienst unterstützt in Kombination mit dem Velero-Plug-In für vSphere die Sicherung und Wiederherstellung von Kubernetes-Arbeitslasten, einschließlich Snapshots von persistenten Volumes. Weitere Informationen zu Supervisor-Dienste finden Sie unter Verwalten von Supervisor-Diensten in *Dienste und Arbeitslasten der vSphere IaaS-Steuerungsebene*.

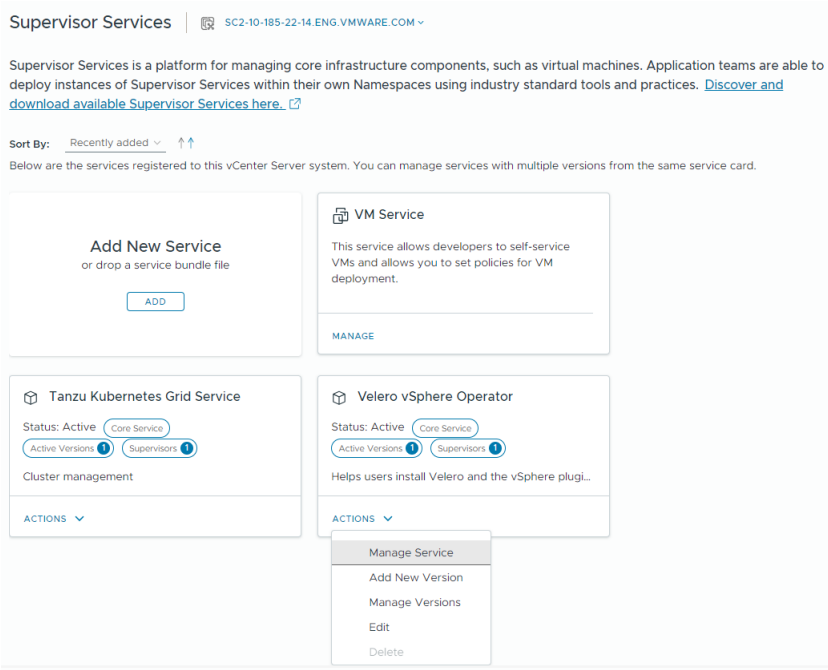
Velero-vSphere-Operator ist ein Kern-Supervisor-Dienst, was bedeutet, dass der Service Operator bei vCenter Server vorregistriert ist. Führen Sie die Schritte aus, um Velero-vSphere-Operator als Dienst auf Supervisor zu installieren.

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

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

3 Wählen Sie oben im Dropdown-Menü das Ziel vCenter Server aus.

4 Klicken Sie auf der Karte „Velero-vSphere-Operator“ auf **Aktionen > Service verwalten**.



5 Wählen Sie den Ziel-Supervisor aus, auf dem Sie den Dienst wiederherstellen möchten, und klicken Sie auf **Weiter**.

6 Klicken Sie auf **Beenden**, um die Installation des Diensts abzuschließen.

Überprüfen Sie den Velero-vSphere-Operator-Dienst auf dem Supervisor und starten Sie die Data Manager-VM.

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

2 Wählen Sie **Dienste** aus.

3 Vergewissern Sie sich, dass der Velero-vSphere-Operator installiert ist und sich im Status **Konfiguriert** befindet.

4 Vergewissern Sie sich auf der Registerkarte **Namespaces**, dass ein neuer vSphere-Namespace-Namespace mit dem Namen `svc-velero-vsphere-domain-xxx` angezeigt wird, wobei `xxx` ein eindeutiges alphanumerisches Token ist. Dies ist der Namespace, der vom System für den Velero-vSphere-Operator erstellt wurde.

Hinweis Sie brauchen diesen Namespace nicht zu konfigurieren und sollten ihn nicht bearbeiten.

5 Suchen Sie in **Host und Cluster** die Data Manager-VM und schalten Sie die VM ein.

Schritt 4 : Erstellen eines vSphere-Namespace für das Velero-Plug-In für vSphere

Erstellen Sie mit dem vSphere Client manuell einen vSphere-Namespace im Supervisor. Dieser vSphere-Namespace ist für das Velero-Plug-In für vSphere erforderlich.

- Benennen Sie den vSphere-Namespace **`velero`**.
- Wählen Sie den Namespace **velero** aus und konfigurieren Sie ihn.
- Geben Sie den Speicher für den Namespace **velero** an.
- Erteilen Sie einem Benutzer mit entsprechenden Rechten die Berechtigung zum Bearbeiten des **velero**-Namespace.

Schritt 5: Erstellen der Velero-Plug-In für vSphere-Configmap

Erstellen Sie eine Configmap für das Velero-Plug-In für vSphere mit der Bezeichnung `velero-vsphere-plugin-config.yaml`.

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: velero-vsphere-plugin-config
data:
  cluster_flavor: SUPERVISOR
```

Wenden Sie die Configmap auf Supervisor an.

```
kubectl apply -n <velero-namespace> -f velero-vsphere-plugin-config.yaml
```

Wenn Sie die Configmap nicht installieren, erhalten Sie folgende Fehlermeldung bei der Installation des Velero-Plug-In für vSphere.

```
Error received while retrieving cluster flavor from config, err: configmaps "velero-vsphere-plugin-config" not found
Falling back to retrieving cluster flavor from vSphere CSI Driver Deployment
```

Schritt 6: Installieren des Velero-Plug-In für vSphere

Sie sind jetzt bereit für die Installation des Velero-Plug-In für vSphere. Laden Sie dazu die **velero-vsphere**-CLI herunter und führen Sie sie aus.

Hinweis Dieses Verfahren erfordert eine Linux-VM. Laden Sie die **velero-vsphere**-Binary auf den Linux-Jump-Host herunter, auf dem Sie die `kubectl-vsphere`- und die `kubectl`-CLI ausführen.

1 Herunterladen der Velero-Plug-In für vSphere-CLI.

Überprüfen Sie die Kompatibilitätsmatrix und laden Sie die Zielversion hier herunter: https://github.com/vmware-tanzu/velero-plugin-for-vsphere/releases.

Hinweis Ersetzen Sie in den folgenden Befehlen `X.Y.Z` durch die Versionen des Velero-CLIs und -Plugins, die Sie heruntergeladen haben.

2 Kopieren Sie die CLI sicher auf den Linux-Jump-Host. Beispiel:

```
pscp -P 22 C:\temp\velero-vsphere-X.Y.Z-linux-amd64.tar.gz ubuntu@10.117.29.131:/home/
ubuntu/tanzu
```

3 Extrahieren Sie die `velero-vsphere`-CLI und machen Sie sie beschreibbar.

```
tar -xf velero-vsphere-X.Y.Z-linux-amd64.tar.gz
chmod +x velero-vsphere
```

4 Fügen Sie die CLI zu Ihrem Pfad hinzu.

```
export PATH="$(pwd)/velero-vsphere-X.Y.Z-linux-amd64:$PATH"
```

5 Erstellen Sie die `s3-credentials`-Datei mit den folgenden Inhalten.

```
aws_access_key_id = ACCESS-KEY-ID-STRING
aws_secret_access_key = SECRET-ACCESS-KEY-STRING
```

6 Rufen Sie die Region, die URL und den Bucket-Namen für Ihren S3-kompatiblen Objektspeicher ab.

7 Melden Sie sich über vSphere-Plug-In für kubectl bei Supervisor an.

8 Führen Sie einen Kontextwechsel zum Supervisor durch.

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

9 Führen Sie den folgenden `velero-vsphere`-CLI-Befehl aus, um das Velero-Plug-In für vSphere in dem von Ihnen erstellten **velero**-Namespace zu installieren.

Exportieren Sie die Werte für AWS-**$BUCKET** und -**$REGION**. Wenn Sie von einer der vorstehenden Anweisungen abgewichen sind, passen Sie auch diese Werte an, z. B. den Namen oder den Speicherort der Geheimschlüssel-Datei, den Namen des manuell erstellten `velero`-Namespace usw.

```
export BUCKET=example-velero-sv && export REGION=us-east-1

./velero-vsphere install \
       --namespace velero \
       --version vX.X.X \
       --provider aws \
       --plugins harbor-repo.vmware.com/velero/velero-plugin-for-aws:vX.Y.Z,harbor-
repo.vmware.com/velero/velero-plugin-for-vsphere:vX.Y.Z \
```

```
        --bucket $BUCKET \
        --secret-file ~/.aws/credentials \
        --snapshot-location-config region=$REGION \
        --backup-location-config region=$REGION
```

Hinweis Beispiel: Die Velero-CLI-Version ist v1.8.1, wenn das Velero-Plug-In für vSphere v1.4.0 verwendet wird.

10 Überprüfen Sie die erfolgreiche Installation des Velero-Plug-In für vSphere.

Bei erfolgreicher Installation sollte die folgende Meldung angezeigt werden:

```
Send the request to the operator about installing Velero in namespace velero
```

Führen Sie den folgenden Befehl aus, um eine weitere Überprüfung durchzuführen. Als Status sollte „Abgeschlossen“ angezeigt werden, dazu die Version.

```
kubectl -n velero get veleroservice default -o json | jq '.status'
```

Erwartetes Ergebnis:

```
{
  "enabled": true,
  "installphase": "Completed",
  "version": "v1.8.1"
}
```

Hinweis Der obige Befehl setzt voraus, dass Sie das `jq`-Dienstprogramm installiert haben, das die JSON-Ausgabe formatiert und an das Terminal sendet. Wenn Sie `jq` nicht installiert haben, installieren Sie es oder entfernen Sie diesen Teil des Befehls (alles nach `json`).

11 Beheben Sie gegebenenfalls Fehler.

Wenn die Installation nicht erfolgreich ist, entfernen Sie die Installation und versuchen Sie es erneut. Um die Installation zu entfernen, führen Sie die Schritte im nächsten Abschnitt in der angegebenen Reihenfolge aus.

Ergänzung: Deinstallieren des Velero-Plug-In für vSphere

Mit den folgenden Schritten deinstallieren Sie das Velero-Plug-In für vSphere.

1 Führen Sie die `velero-vsphere`-CLI aus, um das Velero-Plug-In für vSphere zu deinstallieren.

```
./velero-vsphere uninstall -n velero
```

2 Überprüfen Sie, ob der vSphere Pod mit dem Namen `velero` entfernt wurde.

```
kubectl get pods -n velero
```

Wenn als Pod-Status „Wird beendet“ angezeigt wird, warten Sie, bis er entfernt wurde, bevor Sie fortfahren.

3 Löschen Sie den vSphere Client, und löschen Sie den von Ihnen manuell erstellten vSphere-Namespace mit dem Namen `velero`.

Hinweis Fahren Sie nicht mit dem nächsten Schritt fort, ehe das Löschen des Namespace abgeschlossen ist. Sie können mithilfe von kubectl überprüfen, ob der `velero`-Namespace entfernt wurde (verwenden Sie kubectl aber nicht, um den `velero`-Namespace zu entfernen).

Ergänzung: Installieren des Velero-Plug-In für vSphere in einer Air-Gapped-Umgebung

Wenn Sie das Velero-Plug-In für vSphere in einer Air-Gapped-Umgebung installieren möchten, müssen Sie es mit benutzerdefinierten Images installieren. Sie müssen sicherstellen, dass die passenden Images von `backup-driver` und `data-manager-for-plugin` der angepassten Images in der erwarteten Registrierung verfügbar und über den Kubernetes-Cluster zugänglich sind. In einer Air-Gapped-Umgebung werden angepasste Images aus der privaten Registrierung erwartet, da auf die freigegebenen Images im Docker-Hub nicht zugegriffen werden kann.

Führen Sie zum Installieren des Plug-Ins die folgenden Aufgaben durch:

1 Laden Sie die freigegebenen Images von `velero-plugin-for-vsphere`, `backup-driver` und `data-manager-for-plugin` herunter.

2 Benennen Sie die Images um, indem Sie sie mit passendem `<Registry endpoint and path>` und `<Version tag>` kennzeichnen und in benutzerdefinierte Repositorys hochladen.

3 Installieren Sie das Plug-In mit dem von Ihnen angepassten `velero-plugin-for-vsphere`-Image.

   Wenn Sie Velero-Plug-In für vSphere in einem Vanilla-Cluster installieren, werden zwei zusätzliche Komponenten bereitgestellt, eine `backup-driver`-Bereitstellung und ein `data-manager-for-plugin`-DaemonSet im Hintergrund. In den Supervisor- und Tanzu Kubernetes-Clustern wird lediglich eine `backup-driver`-Bereitstellung zur Verfügung gestellt.

   Wenn Sie das Container-Image von `velero-plugin-for-vsphere` bereitstellen, werden die passenden `backup-driver`- und `data-manager-for-plugin`-Images mithilfe eines Mechanismus zur Image-Analyse analysiert.

   Container-Images werden nach folgendem Muster formalisiert:

   ```
   <Registry endpoint and path>/<Container name>:<Version tag>
   ```

   Wenn Sie das `velero-plugin-for-vsphere`-Container-Image bereitstellen, werden die entsprechenden Images von `backup-driver` und `data-manager-for-plugin` mit passendem `<Registry endpoint and path>` und `<Version tag>` analysiert.

Betrachten Sie beispielsweise das folgende `velero-plugin-for-vsphere`-Container-Image:

```
abc.io:8989/x/y/.../z/velero-plugin-for-vsphere:vX.Y.Z
```

Es wird erwartet, dass die folgenden passenden Images von `backup-driver` und `data-manager-for-plugin` abgerufen werden:

```
abc.io:8989/x/y/.../z/backup-driver:vX.Y.Z
abc.io:8989/x/y/.../z/data-manager-for-plugin:vX.Y.Z
```

4 Führen Sie eine Fehlerbehebung der Installation durch.

Wenn beim Analysieren der passenden Images von `backup-driver` und `data-manager-for-plugin` Probleme oder Fehler auftreten, greift die Installation auf entsprechende Images in den offiziellen `velerovspherepluginn`-Repositorys des Docker-Hubs zurück. Die folgenden Probleme lösen den Fallback-Mechanismus aus:

a Ein unerwarteter Containername wird im benutzerdefinierten `velero-plugin-for-vsphere`-Image in der Benutzereingabe verwendet.

`x/y/velero-velero-plugin-for-vsphere:vX.Y.Z` wird beispielsweise verwendet.

b Der Name der Velero-Bereitstellung wird nicht an `velero` angepasst. Beispiel: Ein Fehler wird ausgelöst, wenn der Name der Velero-Bereitstellung vor der Bereitstellung von Velero auf `velero-server` in der Velero-Datei `manifests` aktualisiert wird.

Der vorhandene Mechanismus zur Analyse von Images in `velero-plugin-for-vsphere` kann die Velero-Bereitstellung nur mit dem festgelegten Namen (`velero`) erkennen.

Sichern und Wiederherstellen von TKG-Dienstclustern und -Arbeitslasten

4

Informationen zum Sichern und Wiederherstellen von TKG-Dienstclustern und -Arbeitslasten finden Sie in diesem Abschnitt.

Lesen Sie als Nächstes die folgenden Themen:

- Überlegungen zur Sicherung und Wiederherstellung von TKG-Dienst-Dienstclustern und -Arbeitslasten
- Sichern und Wiederherstellen von TKG-Cluster-Arbeitslasten mit dem Velero-Plug-In für vSphere
- Sichern und Wiederherstellen von TKG-Cluster-Arbeitslasten Supervisor mit eigenständigem Velero und Restic
- Sichern und Wiederherstellen mithilfe von Velero mit CSI-Snapshot

Überlegungen zur Sicherung und Wiederherstellung von TKG-Dienst-Dienstclustern und -Arbeitslasten

In diesem Abschnitt finden Sie Überlegungen zur Sicherung und Wiederherstellung von Arbeitslasten, die in TKG-Dienst-Clustern ausgeführt werden.

Sichern und Wiederherstellen von TKG-Dienst-Clustern

Zum Sichern und Wiederherstellen von TKG-Dienstclustern sichern Sie die Supervisor-Datenbank. Auf diese Weise können Sie vSphere-Namespaces-Objekte und VMs des TKG-Clusterknotens wiederherstellen.

Sie aktivieren die Supervisor-Sicherung und -Wiederherstellung mithilfe der vCenter Server-Sicherungsfunktion, die über die vCenter Server-Verwaltungsschnittstelle verfügbar ist. Weitere Informationen finden Sie in der Veröffentlichung zur Sicherungswiederherstellung für vSphere IaaS Control Plane.

Hinweis Sie können die Supervisor-Sicherung nur zum Wiederherstellen von TKG-Clusterknoten-VMs verwenden. Sie können die Supervisor-Sicherung nicht zum Wiederherstellen von Arbeitslasten verwenden, die auf TKG-Clustern bereitgestellt werden. Sie müssen Arbeitslasten separat sichern und sie dann wiederherstellen, nachdem der Cluster wiederhergestellt wurde.

Sichern und Wiederherstellen von Arbeitslasten, die auf TKG-Dienst-Clustern ausgeführt werden

In der Tabelle werden die Optionen für das Sichern und Wiederherstellen von statusfreien und statusbehafteten Arbeitslasten behandelt, die in TKG-Clustern ausgeführt werden.

Hinweis Das Sichern und Wiederherstellen eines Kubernetes-Clusters mit eigenständigem Velero ermöglicht Portabilität. Wenn Sie also Clusterarbeitslasten in einem Kubernetes-Cluster wiederherstellen möchten, der nicht vom TKG-Dienst bereitgestellt wurde, sollten Sie eigenständiges Velero verwenden.

Szenario	Tool	Anmerkungen
Sichern Sie statusfreie und statusbehaftete Arbeitslasten in einem TKG-Cluster auf Supervisor und stellen Sie sie in einem TKG-Cluster auf Supervisor wieder her.	Velero-Plug-In für vSphere Weitere Informationen hierzu finden Sie unter Sichern und Wiederherstellen von TKG-Cluster-Arbeitslasten mit dem Velero-Plug-In für vSphere.	Sowohl Kubernetes-Metadaten als auch persistente Volumes können gesichert und wiederhergestellt werden. Velero-Snapshots werden für dauerhafte Volumes mit statusbehafteten Anwendungen verwendet. Erfordert, dass das Velero-Plug-In für vSphere auch auf Supervisor installiert und konfiguriert ist.
Sichern Sie statusfreie und statusbehaftete Arbeitslasten in einem TKG-Cluster auf Supervisor und stellen Sie sie in einem konformen Kubernetes-Cluster wieder her.	Eigenständiges Velero und Restic Siehe Sichern und Wiederherstellen von TKG-Cluster-Arbeitslasten Supervisor mit eigenständigem Velero und Restic. .	Sowohl Kubernetes-Metadaten als auch persistente Volumes können gesichert und wiederhergestellt werden. Restic wird für dauerhafte Volumes mit statusbehafteten Anwendungen verwendet. Verwenden Sie dieses Verfahren, wenn Sie Portabilität benötigen.
Sichern Sie statusfreie und statusbehaftete Arbeitslasten in einem TKG-Cluster auf Supervisor und stellen Sie sie in einem konformen Kubernetes-Cluster wieder her.	Eigenständiges Velero mit CSI-Snapshots Siehe Sichern und Wiederherstellen mithilfe von Velero mit CSI-Snapshot.	Erfordert vSphere 8.0 U2 oder höher und TKr v1.26 oder höher für vSphere 8.0.

Sichern und Wiederherstellen von TKG-Cluster-Arbeitslasten mit dem Velero-Plug-In für vSphere

Dieser Abschnitt enthält Themen zum Sichern und Wiederherstellen von unter Supervisor ausgeführten TKG-Cluster-Arbeitslasten mithilfe des Velero-Plug-In für vSphere.

Installieren und Konfigurieren des Velero-Plug-In für vSphere auf einem TKG-Cluster

Mit dem Velero-Plug-In für vSphere können Sie Arbeitslasten, die in einem TKGS-Cluster ausgeführt werden, sichern und wiederherstellen, indem Sie das Velero-Plug-In für vSphere in dem betreffenden Cluster installieren.

Überblick

Das Velero-Plug-In für vSphere bietet eine Lösung zum Sichern und Wiederherstellen von TKG-Dienst-Clusterarbeitslasten. Für persistente Arbeitslasten können Sie mit dem Velero-Plug-In für vSphere Snapshots der persistenten Volumes erstellen.

Hinweis Wenn Sie Portabilität für die TKG-Dienst-Cluster-Arbeitslasten benötigen, die Sie sichern und wiederherstellen möchten, verwenden Sie nicht das Velero-Plug-In für vSphere. Verwenden Sie für die Kubernetes-Cluster-übergreifende Portabilität eigenständiges Velero mit Restic.

Voraussetzung: Installation des Velero-Plug-In für vSphere im Supervisor

Für die Installation des Velero-Plug-In für vSphere in einem TKGS-Cluster muss das Velero-Plug-In für vSphere im Supervisor installiert sein. Außerdem muss der Supervisor mit NSX-Netzwerk konfiguriert sein. Weitere Informationen finden Sie unter Kapitel 3 Installieren und Konfigurieren des Velero-Plug-In für vSphere im Supervisor.

Speicheranforderung

Zum Sichern eines TKG-Dienst-Clusters benötigen Sie ein Speicher-Backend wie hier beschrieben. Verwenden Sie beim Sichern mehrerer Cluster nicht dasselbe Speicher-Backend für verschiedene Clustersicherungen. Wenn Sie das Speicher-Backend freigeben, werden Sicherungsobjekte synchronisiert. Sie müssen ein anderes Speicher-Backend verwenden, um zu verhindern, dass Daten verloren gehen.

Schritt 1: Installieren der Velero-CLI auf einem Linux-Workstation

Die Velero-CLI ist das Standardtool für die Schnittstelle mit Velero. Die Velero-CLI bietet mehr Funktionen als die Velero-Plug-In für vSphere-CLI (`velero-vsphere`) und ist für die Sicherung und Wiederherstellung von Tanzu Kubernetes-Cluster-Arbeitslasten erforderlich.

Installieren Sie die Velero-CLI auf einer Linux-Workstation. Idealerweise handelt es sich um denselben Jump-Host, in dem Sie zugehörige CLIs für Ihre vSphere IaaS Control Plane-Umgebung ausführen, einschließlich`kubectl`, `kubectl-vsphere`, und `velero-vsphere`.

Die Velero-Versionsnummern werden als `X.Y.Z` dargestellt. In der Velero-Kompatibilitätsmatrix finden Sie die spezifischen Versionen, die verwendet werden sollen. Ersetzen Sie sie entsprechend beim Ausführen der Befehle.

Führen Sie die folgenden Schritte aus, um die Velero-CLI zu installieren.

1 Führen Sie folgende Befehle aus:

```
$ wget https://github.com/vmware-tanzu/velero/releases/download/vX.Y.Z/velero-vX.Y.Z-linux-amd64.tar.gz
$ gzip -d velero-vX.Y.Z-linux-amd64.tar.gz && tar -xvf velero-vX.Y.Z-linux-amd64.tar
$ export PATH="$(pwd)/velero-vX.Y.Z-linux-amd64:$PATH"

$ which velero
/root/velero-vX.Y.Z-linux-amd64/velero
```

2 Überprüfen Sie die Installation der Velero-CLI.

```
velero version

Client:
    Version: vX.Y.Z
```

Schritt 2 : Abrufen der Details des S3-kompatiblen Buckets

Der Einfachheit halber wird in den Schritten davon ausgegangen, dass Sie denselben S3-kompatiblen Objektspeicher verwenden, den Sie beim Installieren des Velero-Plug-In für vSphere im Supervisor konfiguriert haben. In der Produktion können Sie einen separaten Objektspeicher erstellen.

Für die Installation des Velero-Plug-In für vSphere müssen Sie die folgenden Informationen über Ihren S3-kompatiblen Objektspeicher angeben.

Datenelement	Beispielwert
s3Url	`http://my-s3-store.example.com`
aws_access_key_id	ACCESS-KEY-ID-STRING
aws_secret_access_key	SECRET-ACCESS-KEY-STRING

Erstellen Sie eine Datei für geheime Schlüssel mit dem Namen `s3-credentials` und den folgenden Informationen. Beim Installieren des Velero-Plug-In für vSphere werden Sie auf diese Datei verweisen.

```
aws_access_key_id = ACCESS-KEY-ID-STRING
aws_secret_access_key = SECRET-ACCESS-KEY-STRING
```

Schritt 3 Option A: Installieren des Velero-Plug-In für vSphere auf dem TKG-Cluster mithilfe einer Bezeichnung (neue Methode)

Wenn Sie vSphere 8 Update 3 oder höher verwenden, können Sie das Velero-Plug-In für vSphere automatisch in einem TKG-Cluster installieren, indem Sie eine Bezeichnung hinzufügen.

1 Stellen Sie sicher, dass auf den Sicherungsspeicherort zugegriffen werden kann.

2 Stellen Sie sicher, dass der Velero vSphere-Operator-Kern Supervisor-Dienst aktiviert ist.

```
kubectl get ns | grep velero
svc-velero-domain-c9                        Active   18d
```

3 Stellen Sie sicher, dass ein Kubernetes-Namespace mit der Bezeichnung `velero` auf Supervisor erstellt wird.

```
kubectl get ns | grep velero
svc-velero-domain-c9                        Active   18d
velero                                      Active   1s
```

4 Stellen Sie sicher, dass der Velero-Plug-In für vSphere Supervisor-Dienst auf Supervisor aktiviert ist.

```
velero version
Client:
        Version: v1.11.1
        Git commit: bdbe7eb242b0f64d5b04a7fea86d1edbb3a3587c
Server:
        Version: v1.11.1
```

```
kubectl get veleroservice -A
NAMESPACE   NAME      AGE
velero      default   53m
```

```
velero backup-location get
NAME      PROVIDER   BUCKET/PREFIX   PHASE       LAST VALIDATED                  ACCESS
MODE   DEFAULT
default   aws        velero          Available   2023-11-20 14:10:57 -0800 PST
ReadWrite     true
```

5 Aktivieren Sie Velero für den TKG-Zielcluster, indem Sie die Velero-Bezeichnung zum Cluster hinzufügen.

```
kubectl label cluster CLUSTER-NAME --namespace CLUSTER-NS velero.vsphere.vmware.com/
enabled=true
```

Hinweis Die Aktivierung erfolgt über den vSphere-Namespace, wenn der Cluster bereitgestellt wird.

6 Stellen Sie sicher, dass Velero installiert ist und für den Cluster verwendet werden kann.

```
kubectl get ns
NAME                                STATUS   AGE
...
velero                              Active   2m    <--
velero-vsphere-plugin-backupdriver  Active   2d23h
```

```
kubectl get all -n velero
NAME                                READY   STATUS    RESTARTS   AGE
pod/backup-driver-5945d6bcd4-gtw9d  1/1     Running   0          17h
pod/velero-6b9b49449-pq6b4          1/1     Running   0          18h
NAME                              READY   UP-TO-DATE   AVAILABLE   AGE
deployment.apps/backup-driver     1/1     1            1           17h
deployment.apps/velero            1/1     1            1           18h
NAME                                        DESIRED   CURRENT   READY   AGE
replicaset.apps/backup-driver-5945d6bcd4    1         1         1       17h
replicaset.apps/velero-6b9b49449            1         1         1       18h
```

```
velero version
Client:
        Version: v1.11.1
        Git commit: bdbe7eb242b0f64d5b04a7fea86d1edbb3a3587c
Server:
        Version: v1.11.1
```

Schritt 3 Option B: Manuelles Installieren des Velero-Plug-In für vSphere im TKG-Cluster (veraltete Methode)

Sie verwenden die Velero-CLI zum Installieren des Velero-Plug-In für vSphere im TKG-Zielcluster, den Sie sichern und wiederherstellen möchten.

Der Velero-CLI-Kontext folgt automatisch dem `kubectl`-Kontext. Stellen Sie vor der Ausführung von Velero-CLI-Befehlen zur Installation von Velero und des Velero-Plug-In für vSphere auf dem Zielcluster sicher, dass als `kubectl`-Kontext der Zielcluster festgelegt ist.

1 Authentifizieren Sie sich mithilfe des vSphere-Plug-In für kubectl beim Supervisor.

2 Ändern Sie den `kubectl`-Kontext in den TKG-Zielcluster.

```
kubectl config use-context TARGET-TANZU-KUBERNETES-CLUSTER
```

3 Erstellen Sie im TKG-Cluster eine Configmap für das Velero-Plug-In mit der Bezeichnung `velero-vsphere-plugin-config.yaml`.

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: velero-vsphere-plugin-config
data:
  cluster_flavor: GUEST
```

Wenden Sie die Configmap auf den TKG-Cluster an.

```
kubectl apply -n <velero-namespace> -f velero-vsphere-plugin-config.yaml
```

Wenn Sie die Configmap nicht installieren, erhalten Sie folgende Fehlermeldung bei der Installation des Velero-Plug-In für vSphere.

```
Error received while retrieving cluster flavor from config, err: configmaps "velero-
vsphere-plugin-config" not found
Falling back to retrieving cluster flavor from vSphere CSI Driver Deployment
```

4 Führen Sie den folgenden Velero-CLI-Befehl aus, um Velero auf dem Zielcluster zu installieren.

Ersetzen Sie die Platzhalterwerte für die Felder **`BUCKET-NAME`**, **`REGION`** (zwei Instanzen) und **`s3Url`** durch die geeigneten Werte. Wenn Sie von einer der vorstehenden Anweisungen abgewichen sind, passen Sie auch diese Werte an, z. B. den Namen oder den Speicherort der Geheimschlüssel-Datei, den Namen des manuell erstellten `velero`-Namespace usw.

```
./velero install --provider aws \
--bucket BUCKET-NAME \
--secret-file ./s3-credentials \
--features=EnableVSphereItemActionPlugin \
--plugins velero/velero-plugin-for-aws:vX.Y.Z \
--snapshot-location-config region=REGION \
--backup-location-config region=REGION,s3ForcePathStyle="true",s3Url=http://my-s3-
store.example.com
```

5 Installieren Sie das Velero-Plug-In für vSphere auf dem Zielcluster. Der installierte Velero kommuniziert mit dem Kubernetes-API-Server, um das Plug-In zu installieren.

```
velero plugin add vsphereveleroplugin/velero-plugin-for-vsphere:vX.Y.Z
```

Ergänzung: Deinstallieren des Velero-Plug-In für vSphere im TKG-Cluster

Mit den folgenden Schritten deinstallieren Sie das Velero-Plug-In für vSphere.

1 Ändern Sie den `kubectl`-Kontext in den Tanzu Kubernetes-Zielcluster.

```
kubectl config use-context TARGET-TANZU-KUBERNETES-CLUSTER
```

2 Führen Sie zum Installieren des Plug-Ins den folgenden Befehl aus, um den InitContainer von velero-plugin-for-vsphere aus der Velero-Bereitstellung zu entfernen.

```
velero plugin remove vsphereveleroplugin/velero-plugin-for-vsphere:vX.Y.Z
```

3 Um den Vorgang abzuschließen, löschen Sie die Backup-Treiber-Bereitstellung und die zugehörigen CRDs.

```
kubectl -n velero delete deployment.apps/backup-driver
```

```
kubectl delete crds \
backuprepositories.backupdriver.cnsdp.vmware.com \
backuprepositoryclaims.backupdriver.cnsdp.vmware.com \
clonefromsnapshots.backupdriver.cnsdp.vmware.com \
deletesnapshots.backupdriver.cnsdp.vmware.com \
snapshots.backupdriver.cnsdp.vmware.com
```

```
kubectl delete crds uploads.datamover.cnsdp.vmware.com downloads.datamover.cnsdp.vmware.com
```

Sichern und Wiederherstellen von Arbeitslasten im TKG-Cluster mit dem Velero-Plug-In für vSphere

Sie können Arbeitslasten, die in TKG-Clustern auf Supervisor ausgeführt werden, mithilfe des Velero-Plug-In für vSphere sichern und wiederherstellen.

Voraussetzungen

Um TKG-Clusterarbeitslasten mit dem Velero-Plug-In für vSphere zu sichern und wiederherzustellen, müssen Sie zuerst das Velero-Plug-In für vSphere im Zielcluster installieren. Weitere Informationen finden Sie unter Installieren und Konfigurieren des Velero-Plug-In für vSphere auf einem TKG-Cluster.

Sichern einer Arbeitslast

Nachfolgend finden Sie einen Beispielbefehl zum Erstellen einer Velero-Sicherung.

```
velero backup create <backup name> --include-namespaces=my-namespace
```

Die Velero-Sicherung wird als `Completed` gekennzeichnet, nachdem alle lokalen Snapshots erstellt wurden und Kubernetes-Metadaten mit Ausnahme von Volume-Snapshots in den Objektspeicher hochgeladen wurden. Zu diesem Zeitpunkt werden asynchrone Datenverschiebungsaufgaben, d. h. das Hochladen von Volume-Snapshots, weiterhin im Hintergrund ausgeführt und können einige Zeit in Anspruch nehmen. Sie können den Status des Volume-Snapshots überprüfen, indem Sie benutzerdefinierte Snapshot-Ressourcen (Custom Resources, CRs) überwachen.

Snapshots

Snapshots werden zum Sichern persistenter Volumes verwendet. Für jeden Volume-Snapshot wird eine Snapshot-CR im selben Namespace erstellt wie die Anforderung eines dauerhaften Datenträgers (Persistent Volume Claim, PVC), für die ein Snapshot erstellt wird.

Sie können alle Snapshots im PVC-Namespace abrufen, indem Sie den folgenden Befehl ausführen.

```
kubectl get -n <pvc namespace> snapshot
```

Die Definition der benutzerdefinierten Snapshot-Ressource (Custom Resource Definition, CRD) verfügt über eine Reihe von Statusangaben (Phasen) für das Feld „`.status.phase`“, einschließlich:

Snapshot-Status	Beschreibung
Neu	Noch nicht verarbeitet
Snapshotted	Lokaler Snapshot wurde erstellt
SnapshotFailed	Lokaler Snapshot ist fehlgeschlagen
Upload wird durchgeführt ...	Der Snapshot wird hochgeladen
Uploaded	Der Snapshot wird hochgeladen
UploadFailed	Der Snapshot konnte nicht hochgeladen werden
Canceling	Das Hochladen des Snapshots wird abgebrochen
Abgebrochen	Das Hochladen des Snapshots wurde abgebrochen
CleanupAfterUploadFailed	Die Bereinigung des lokalen Snapshots nach dem Hochladen des Snapshots ist fehlgeschlagen

Wiederherstellen einer Arbeitslast

Nachfolgend finden Sie einen Beispielbefehl für die Velero-Wiederherstellung.

```
velero restore create --from-backup <velero-backup-name>
```

Die Velero-Wiederherstellung wird als `Completed` gekennzeichnet, wenn Volume-Snapshots und andere Kubernetes-Metadaten erfolgreich im aktuellen Cluster wiederhergestellt wurden. Zu diesem Zeitpunkt sind alle Aufgaben des vSphere Plug-Ins im Zusammenhang mit dieser Wiederherstellung ebenfalls abgeschlossen. Im Falle einer Velero-Sicherung werden keine asynchronen Datenverschiebungsaufgaben im Hintergrund ausgeführt.

CloneFromSnapshots

Um die Wiederherstellung für jeden Volume-Snapshot durchzuführen, wird eine benutzerdefinierte `CloneFromSnapshot`-Ressource (Custom Resource, CR) im selben Namespace erstellt wie die PVC, für die ursprünglich ein Snapshot erstellt wurde. Sie können alle CloneFromSnapshots im PVC-Namespace abrufen, indem Sie den folgenden Befehl ausführen.

```
kubectl -n <pvc namespace> get clonefromsnapshot
```

Die CloneFromSnapshot-CRD weist einige Schlüsselstatusangaben für das Feld „`.status.phase`“ auf:

Snapshot-Status	Beschreibung
Neu	Das Klonen aus dem Snapshot ist nicht abgeschlossen
InProgress	Der Snapshot des vSphere Volume wird aus dem Remote-Repository heruntergeladen
Abgeschlossen	Das Klonen aus dem Snapshot ist abgeschlossen
Fehlgeschlagen	Das Klonen aus dem Snapshot ist fehlgeschlagen

Sichern und Wiederherstellen von TKG-Cluster-Arbeitslasten Supervisor mit eigenständigem Velero und Restic

Dieser Abschnitt enthält Themen zum Sichern und Wiederherstellen von unter Supervisor ausgeführten TKG-Cluster-Arbeitslasten mit eigenständigem Velero und Restic.

Installieren und Konfigurieren von eigenständigem Velero und Restic in TKG-Clustern

Um Arbeitslasten, die in TKG-Clustern ausgeführt werden, auf Supervisor zu sichern und wiederherzustellen, erstellen Sie einen Datenspeicher und installieren Sie Velero mit Restic im Kubernetes-Cluster.

Überblick

TKG-Cluster werden auf VM-Knoten ausgeführt. Zum Sichern und Wiederherstellen von TKG-Clusterarbeitslasten installieren Sie Velero und Restic im Cluster.

Voraussetzungen

Achten Sie darauf, dass Ihre Umgebung die folgenden Voraussetzungen für die Installation von Velero und Restic zum Sichern und Wiederherstellen von Arbeitslasten auf Tanzu Kubernetes-Clustern erfüllt.

- Eine Linux-VM mit ausreichend Speicherplatz zum Speichern mehrerer Arbeitslastsicherungen. Sie installieren MinIO auf dieser VM.
- Eine Linux-VM, in der die Kubernetes-CLI-Tools für vSphere installiert sind, einschließlich des vSphere-Plug-In für kubectl und kubectl. Sie installieren die Velero-CLI auf dieser Client-VM. Wenn Sie über keine solche VM verfügen, können Sie die Velero CLI lokal installieren, müssen die Installationsschritte jedoch entsprechend anpassen.
- Die Kubernetes-Umgebung verfügt über Internetzugriff und kann von der Client-VM erreicht werden.

Installieren und Konfigurieren des MinIO-Objektspeichers

Velero benötigt einen S3-kompatiblen Objektspeicher als Ziel für Kubernetes-Arbeitslastsicherungen. Velero unterstützt mehrere solcher Objektspeicher-Anbieter. Der Einfachheit halber wird in dieser Anleitung MinIO verwendet. Dabei handelt es sich um einen S3-kompatiblen Speicherdienst, der lokal auf der Objektspeicher-VM ausgeführt wird.

1 Installieren Sie MinIO.

```
wget https://dl.min.io/server/minio/release/linux-amd64/minio
```

2 Erteilen Sie MinIO-Ausführungsberechtigungen.

```
chmod +x minio
```

3 Erstellen Sie ein Verzeichnis auf dem Dateisystem für MinIO.

```
mkdir /DATA-MINIO
```

4 Starten Sie den MinIO-Server.

```
./minio server /DATA-MINIO
```

5 Nach dem Start des MinIO-Servers erhalten Sie wichtige Datenspeicherinstanzdetails, darunter die Endpoint-URL, den AccessKey und den SecretKey. Zeichnen Sie die Endpoint-URL, den AccessKey und den SecretKey in der Tabelle auf.

Datenspeicher-Metadaten	Wert
Endpoint-URL	
AccessKey	
SecretKey	

6 Navigieren Sie zum MinIO-Datenspeicher, indem Sie einen Browser öffnen und darin die Endpoint-URL des MinIO-Servers aufrufen.

7 Melden Sie sich beim MinIO-Server an und geben Sie den AccessKey und SecretKey an.

8 Um MinIO als Dienst zu aktivieren, konfigurieren Sie MinIO für den automatischen Start, indem Sie das `minio.service`-Skript herunterladen.

```
curl -O https://raw.githubusercontent.com/minio/minio-service/master/linux-systemd/
minio.service
```

9 Bearbeiten Sie das `minio.service`-Skript und fügen Sie den folgenden Wert für `ExecStart` hinzu.

```
ExecStart=/usr/local/bin/minio server /DATA-MINIO path
```

10 Speichern Sie das überarbeitete Skript.

11 Konfigurieren Sie den MinIO-Dienst, indem Sie die folgenden Befehle ausführen.

```
cp minio.service /etc/systemd/system
cp minio /usr/local/bin/
systemctl daemon-reload
systemctl start minio
systemctl status minio
systemctl enable minio
```

12 Erstellen Sie einen MinIO-Bucket für die Sicherung und Wiederherstellung, indem Sie den MinIO-Browser starten und sich bei Ihrem Objektspeicher anmelden.

13 Klicken Sie auf das Symbol für „Bucket erstellen“.

14 Geben Sie den Bucket-Namen ein, z. B.: `my-cluster-backups`.

15 Überprüfen Sie, ob der Bucket erstellt wurde.

16 Standardmäßig ist ein neuer MinIO-Bucket schreibgeschützt. Für die Sicherung und Wiederherstellung mit eigenständigem Velero muss der MinIO-Bucket über Lese- und Schreibberechtigung verfügen. Um die Lese- und Schreibberechtigung für den Bucket zu aktivieren, wählen Sie den Bucket aus und klicken Sie auf den Link mit der Ellipse (...).

17 Klicken Sie auf **Richtlinie bearbeiten**.

18 Ändern Sie die Richtlinie in **Lesen und Schreiben**.

19 Klicken Sie auf **Hinzufügen**.

20 Klicken Sie auf das X, um das Dialogfeld zu schließen.

Installieren der Velero-CLI

Installieren Sie die Velero-CLI auf dem VM-Client oder auf Ihrem lokalen Computer.

Die für diese Dokumentation verwendete Version ist *Velero 1.9.7 für Tanzu Kubernetes Grid 2.2.0*.

1 Laden Sie Velero von der Tanzu Kubernetes Grid-Produkt-Download-Seite im VMware Customer Connect-Portal herunter.

Hinweis Sie müssen die von VMware signierte Velero-Binärdatei verwenden, um Unterstützung von VMware zu erhalten.

2 Öffnen Sie eine Befehlszeile und wechseln Sie zum Velero-CLI-Download.

3 Entpacken Sie die Download-Datei. Beispiel:

```
gunzip velero-linux-vX.X.X_vmware.1.gz
```

4 Überprüfen Sie, ob die Velero-Binärdatei vorhanden ist.

```
ls -l
```

5 Erteilen Sie der Velero-CLI Ausführungsberechtigungen.

```
chmod +x velero-linux-vX.X.X_vmware.1
```

6 Machen Sie die Velero-CLI global verfügbar, indem Sie sie in den Systempfad verschieben:

```
cp velero-linux-vX.X.X_vmware.1 /usr/local/bin/velero
```

7 Überprüfen Sie die Installation.

```
velero version
```

Installieren von Velero und Restic auf dem Tanzu Kubernetes-Cluster

Der Velero CLI-Kontext folgt automatisch dem kubectl-Kontext. Legen Sie den kubectl-Kontext fest, bevor Sie Velero-CLI-Befehle zum Installieren von Velero und Restic auf dem Zielcluster ausführen.

1 Rufen Sie den Namen des MinIO-Buckets ab. Beispiel: `my-cluster-backups`.

2 Rufen Sie den AccessKey und den SecretKey für den MinIO-Bucket ab.

3 Legen Sie den Kontext für den Kubernetes-Zielcluster so fest, dass die Velero-CLI weiß, an welchem Cluster gearbeitet werden soll.

```
kubectl config use-context tkgs-cluster-name
```

4 Erstellen Sie eine Geheimschlüsseldatei mit dem Namen `credentials-minio`. Aktualisieren Sie die Datei mit den von Ihnen erfassten MinIO-Serveranmeldedaten. Beispiel:

```
aws_access_key_id = 0XXNO8JCCGV41QZBV0RQ
aws_secret_access_key = clZ1bf8Ljkvkmq7fHucrKCkxV39BRbcycGeXQDfx
```

Hinweis Wenn Sie eine Fehlermeldung vom Typ „Fehler beim Abrufen eines Sicherungsspeichers“ mit der Beschreibung „NoCredentialProviders: keine gültigen Anbieter in Kette“ erhalten, platzieren Sie die Zeile `[default]` am Anfang der Anmeldedatendatei. Beispiel:

```
[default]
aws_access_key_id = 0XXNO8JCCGV41QZBV0RQ
aws_secret_access_key = clZ1bf8Ljkvkmq7fHucrKCkxV39BRbcycGeXQDfx
```

5 Speichern Sie die Datei und stellen Sie sicher, dass die Datei vorhanden ist.

```
ls
```

6 Führen Sie den folgenden Befehl aus, um Velero und Restic auf dem Kubernetes-Zielcluster zu installieren. Ersetzen Sie beide URLs durch die URL Ihrer MinIO-Instanz.

```
velero install \
--provider aws \
--plugins velero/velero-plugin-for-aws:v1.0.0 \
--bucket tkgs-velero \
--secret-file ./credentials-minio \
--use-volume-snapshots=false \
--use-restic \
--backup-location-config \
region=minio,s3ForcePathStyle="true",s3Url=http://10.199.17.63:9000,publicUrl=http://
10.199.17.63:9000
```

7 Überprüfen Sie die Installation von Velero und Restic.

```
kubectl logs deployment/velero -n velero
```

8 Überprüfen Sie den `velero`-Namespace.

```
kubectl get ns
```

9 Überprüfen Sie die `velero`- und `restic`-Pods.

```
kubectl get all -n velero
```

Fehlerbehebung bei Restic-DaemonSet (falls erforderlich)

Um das Restic-DaemonSet mit drei Pods auf einem Kubernetes-Cluster auszuführen, müssen Sie möglicherweise die Restic-DaemonSet-Spezifikation aktualisieren und den hostPath ändern. Weitere Informationen zu diesem Problem finden Sie unter Restic-Integration in der Velero-Dokumentation.

1 Überprüfen Sie das Restic-DaemonSet mit drei Pods.

```
kubectl get pod -n velero
```

Wenn sich die Pods im Status „CrashLoopBackOff“ befinden, bearbeiten Sie sie wie folgt.

2 Führen Sie den Befehl `edit` aus.

```
kubectl edit daemonset restic -n velero
```

3 Ändern Sie den hostPath von `/var/lib/kubelet/pods` zu `/var/vcap/data/kubelet/pods`.

```
- hostPath:
    path: /var/vcap/data/kubelet/pods
```

4 Speichern Sie die Datei.

5 Überprüfen Sie das Restic-DaemonSet mit drei Pods.

```
kubectl get pod -n velero
```

```
NAME                       READY   STATUS    RESTARTS   AGE
restic-5jln8               1/1     Running   0          73s
restic-bpvtq               1/1     Running   0          73s
restic-vg8j7               1/1     Running   0          73s
velero-72c84322d9-le7bd    1/1     Running   0          10m
```

Anpassen der Velero-Speichergrenzwerte (bei Bedarf)

Wenn Ihre Velero-Sicherung für viele Stunden den Status `status=InProgress` zurückgibt, sollten Sie die Grenzwerte und die Speichereinstellungen für Anforderungen erhöhen.

1 Führen Sie den folgenden Befehl aus.

```
kubectl edit deployment/velero -n velero
```

2 Ändern Sie die Grenzwerte und die Speichereinstellungen für Anforderungen von der Standardeinstellung von `256Mi` bzw. `128Mi` zu `512Mi` bzw. `256Mi`.

```
ports:
- containerPort: 8085
  name: metrics
  protocol: TCP
resources:
  limits:
    cpu: "1"
    memory: 512Mi
  requests:
    cpu: 500m
    memory: 256Mi
terminationMessagePath: /dev/termination-log
terminationMessagePolicy: File
```

Sichern und Wiederherstellen von Clusterarbeitslasten mit eigenständigem Velero und Restic

Sie können Arbeitslasten, die in TKG-Clustern ausgeführt werden, mithilfe von eigenständigem Velero und Restic sichern und wiederherstellen. Dieses Verfahren ist eine Alternative zur Verwendung des eingebetteten Velero-Plug-In für vSphere. Eigenständiges Velero wird hauptsächlich verwendet, wenn Sie Portabilität benötigen. Restic ist für statusbehaftete Arbeitslasten erforderlich.

Voraussetzungen

Zum Sichern und Wiederherstellen von Arbeitslasten in einem TKG-Cluster mit eigenständigem Velero und Restic müssen Sie die eigenständige Version von Velero und Restic im Zielcluster installieren. Wenn die Wiederherstellung in einem separaten Zielcluster durchgeführt werden soll, müssen Velero und Restic ebenfalls im Zielcluster installiert sein. Weitere Informationen finden Sie unter Installieren und Konfigurieren von eigenständigem Velero und Restic in TKG-Clustern.

Sichern einer statusfreien Anwendung, die auf einem TKG-Cluster ausgeführt wird

Zum Sichern einer statusfreien Anwendung, die auf einem TKG-Cluster ausgeführt wird, müssen Sie Velero verwenden.

Dieses Beispiel zeigt, wie Sie eine statusfreie Beispielanwendung mit dem `--include namespaces`-Tag sichern und wiederherstellen, wobei sich alle Anwendungskomponenten in diesem Namespace befinden.

```
velero backup create example-backup --include-namespaces example-backup
```

Sie sollten folgende Meldung sehen:

```
Backup request "example-backup" submitted successfully.
Run `velero backup describe example-backup` or `velero backup logs example-backup` for more
details.
```

Überprüfen Sie die erstellte Sicherung.

```
velero backup get
```

```
velero backup describe example-backup
```

Überprüfen Sie den Velero-Bucket im S3-kompatiblen Objektspeicher, z. B. auf dem MinIO-Server.

Velero schreibt einige Metadaten in benutzerdefinierte Kubernetes-Ressourcendefinitionen (Custom Resource Definitions, CRDs).

```
kubectl get crd
```

Mit den Velero-CRDs können Sie bestimmte Befehle ausführen, wie z. B.:

```
kubectl get backups.velero.io -n velero
```

```
kubectl describe backups.velero.io guestbook-backup -n velero
```

Wiederherstellen einer statusfreien Anwendung, die auf einem TKG-Cluster ausgeführt wird

Zum Wiederherstellen einer statusfreien Anwendung, die auf einem TKG-Cluster ausgeführt wird, müssen Sie Velero verwenden.

Um die Wiederherstellung einer Beispielanwendung zu testen, löschen Sie sie.

Löschen Sie den Namespace:

```
kubectl delete ns guestbook
namespace "guestbook" deleted
```

Stellen Sie die App wieder her:

```
velero restore create --from-backup example-backup
```

Sie sollten folgende Meldung sehen:

```
Restore request "example-backup-20200721145620" submitted successfully.
Run `velero restore describe example-backup-20200721145620` or `velero restore logs example-
backup-20200721145620` for more details.
```

Überprüfen Sie, ob die App wiederhergestellt wurde:

```
velero restore describe example-backup-20200721145620
```

Führen Sie zur Überprüfung die folgenden Befehle aus:

```
velero restore get
```

```
kubectl get ns
```

```
kubectl get pod -n example
```

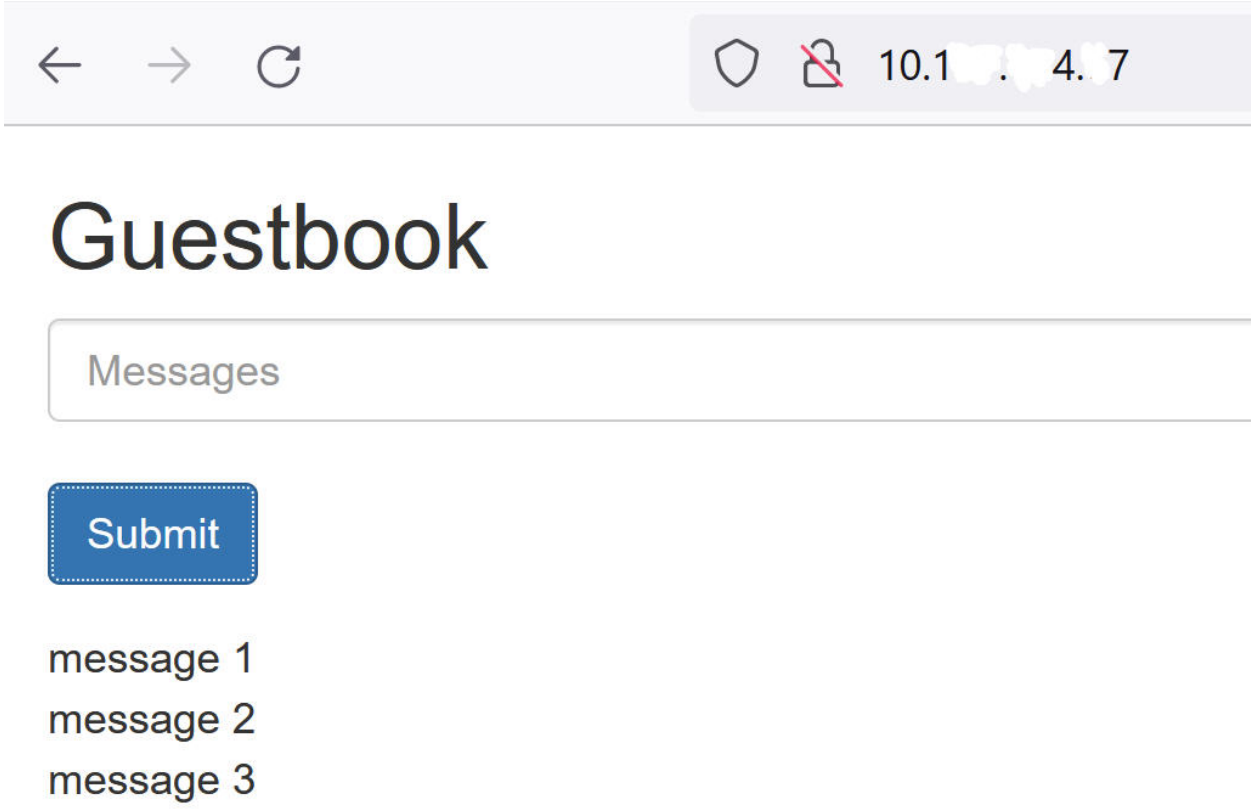
```
kubectl get svc -n example
```

Sichern einer statusbehafteten Anwendung, die auf einem TKG-Cluster ausgeführt wird

Zum Sichern einer statusbehafteten Anwendung, die auf einem TKG-Cluster ausgeführt wird, müssen sowohl die Metadaten als auch die Daten der Anwendung gesichert werden, die auf einem persistenten Volume gespeichert sind. Dazu benötigen Sie Velero und Restic.

Für dieses Beispiel verwenden wir die Guestbook-Anwendung. Dabei wird davon ausgegangen, dass Sie die Guestbook-Anwendung in einem TKG-Cluster bereitgestellt haben. Weitere Informationen finden Sie unter #unique_17.

Zur Veranschaulichung der statusbehafteten Sicherung und Wiederherstellung senden Sie irgendeine Nachricht über die Frontend-Seite an die Guestbook-Anwendung, damit die Nachrichten dauerhaft gespeichert werden. Beispiel:



Dieses Beispiel zeigt, wie Sie die Guestbook-App mit dem `--include namespace`-Tag und Pod-Anmerkungen sichern und wiederherstellen.

Hinweis In diesem Beispiel werden Anmerkungen verwendet. Für Velero Version 1.5 und höher sind jedoch keine Anmerkungen mehr erforderlich. Um keine Anmerkungen zu verwenden, können Sie beim Erstellen der Sicherung die Option `--default-volumes-to-restic` verwenden. Dadurch werden automatisch alle PVs mit Restic gesichert. Weitere Informationen hierzu finden Sie unter https://velero.io/docs/v1.5/restic/.

Um den Sicherungsvorgang zu starten, rufen Sie die Namen der Pods ab:

```
kubectl get pod -n guestbook
```

Beispiel:

```
kubectl get pod -n guestbook

NAME                                          READY   STATUS    RESTARTS   AGE
guestbook-frontend-deployment-85595f5bf9-h8cff  1/1     Running             0          55m
guestbook-frontend-deployment-85595f5bf9-lw6tg  1/1     Running             0          55m
guestbook-frontend-deployment-85595f5bf9-wpqc8  1/1     Running             0          55m
redis-leader-deployment-64fb8775bf-kbs6s        1/1     Running             0          55m
redis-follower-deployment-84cd76b975-jrn8v      1/1     Running             0          55m
redis-follower-deployment-69df9b5688-zml4f      1/1     Running             0          55m
```

Die persistenten Volumes werden an die Redis-Pods angehängt. Da wir diese statusbehafteten Pods mit Restic sichern, müssen wir den statusbehafteten Pods mit dem Namen `volumeMount` Anmerkungen hinzufügen.

Sie müssen den `volumeMount` kennen, um den statusbehafteten Pod mit Anmerkungen zu versehen. Führen Sie folgenden Befehl aus, um den `mountName` abzurufen.

```
kubectl describe pod redis-leader-deployment-64fb8775bf-kbs6s -n guestbook
```

In den Ergebnissen sehen Sie `Containers.leader.Mounts: /data` aus `redis-leader-data`. Dieses letzte Token ist der `volumeMount`-Name, der für die Annotation des Leader-Pods verwendet werden soll. Für den Follower ist dies `redis-follower-data`. Sie können den `volumeMount`-Namen auch aus der Quell-YAML abrufen.

Versehen Sie jeden Redis-Pod mit Anmerkungen, z. B.:

```
kubectl -n guestbook annotate pod redis-leader-64fb8775bf-kbs6s backup.velero.io/backup-
volumes=redis-leader-data
```

Sie sollten folgende Meldung sehen:

```
pod/redis-leader-64fb8775bf-kbs6s annotated
```

Überprüfen Sie die Anmerkungen:

```
kubectl -n guestbook describe pod redis-leader-64fb8775bf-kbs6s | grep Annotations
Annotations:  backup.velero.io/backup-volumes: redis-leader-data
```

```
kubectl -n guestbook describe pod redis-follower-779b6d8f79-5dphr | grep Annotations
Annotations:  backup.velero.io/backup-volumes: redis-follower-data
```

Führen Sie die Velero-Sicherung durch:

```
velero backup create guestbook-backup --include-namespaces guestbook
```

Sie sollten folgende Meldung sehen:

```
Backup request "guestbook-backup" submitted successfully.
Run `velero backup describe guestbook-pv-backup` or `velero backup logs guestbook-pv-backup`
for more details.
```

Überprüfen Sie die erstellte Sicherung.

```
velero backup get

NAME                   STATUS      ERRORS   WARNINGS   CREATED
EXPIRES   STORAGE LOCATION   SELECTOR
guestbook-backup       Completed   0        0          2020-07-23 16:13:46 -0700 PDT
29d       default            <none>
```

Überprüfen Sie die Sicherungsdetails.

```
velero backup describe guestbook-backup --details
```

Beachten Sie, dass Sie mit Velero andere Befehle ausführen können, wie z. B.:

```
kubectl get backups.velero.io -n velero

NAME               AGE
guestbook-backup   4m58s
```

Und:

```
kubectl describe backups.velero.io guestbook-backup -n velero
```

Wiederherstellen einer statusbehafteten Anwendung, die auf einem TKG 2.0-Cluster ausgeführt wird

Zum Wiederherstellen einer statusbehafteten Anwendung, die auf einem TKG-Cluster ausgeführt wird, müssen sowohl die Metadaten als auch die Daten der Anwendung wiederhergestellt werden, die auf einem persistenten Volume gespeichert sind. Dazu benötigen Sie Velero und Restic.

In diesem Beispiel wird davon ausgegangen, dass Sie die statusbehaftete Guestbook-Anwendung wie im vorherigen Abschnitt beschrieben gesichert haben.

Um die Wiederherstellung der statusbehafteten Anwendung zu testen, löschen Sie ihren Namespace:

```
kubectl delete ns guestbook
namespace "guestbook" deleted
```

Überprüfen Sie, ob die Anwendung gelöscht wurde:

```
kubectl get ns
kubectl get pvc,pv --all-namespaces
```

Verwenden Sie die folgende Befehlssyntax, um eine Anwendung von der Sicherung wiederherzustellen.

```
velero restore create --from-backup <velero-backup-name>
```

Beispiel:

```
velero restore create --from-backup guestbook-backup
```

Sinngemäß sollten Meldungen wie die folgenden angezeigt werden:

```
Restore request "guestbook-backup-20200723161841" submitted successfully.
Run `velero restore describe guestbook-backup-20200723161841` or `velero restore logs
guestbook-backup-20200723161841` for more details.
```

Überprüfen Sie, ob die statusbehaftete Guestbook-Anwendung wiederhergestellt wurde:

```
velero restore describe guestbook-backup-20200723161841

Name:         guestbook-backup-20200723161841
Namespace:    velero
Labels:       <none>
Annotations:  <none>

Phase:  Completed

Backup:  guestbook-backup

Namespaces:
  Included:  all namespaces found in the backup
  Excluded:  <none>

Resources:
  Included:        *
  Excluded:        nodes, events, events.events.k8s.io, backups.velero.io,
restores.velero.io, resticrepositories.velero.io
  Cluster-scoped:  auto

Namespace mappings:  <none>

Label selector:  <none>

Restore PVs:  auto

Restic Restores (specify --details for more information):
  Completed:  3
```

Führen Sie den folgenden zusätzlichen Befehl aus, um die Wiederherstellung zu überprüfen:

```
velero restore get

NAME                                BACKUP                STATUS      ERRORS   WARNINGS
CREATED                         SELECTOR
guestbook-backup-20200723161841     guestbook-backup      Completed   0        0
2021-08-11 16:18:41 -0700 PDT   <none>
```

Überprüfen Sie, ob der Namespace wiederhergestellt wurde:

```
kubectl get ns

NAME              STATUS   AGE
default           Active   16d
guestbook         Active   76s
...
velero            Active   2d2h
```

Überprüfen Sie, ob die Anwendung wiederhergestellt wurde:

```
vkubectl get all -n guestbook

NAME                                 READY   STATUS    RESTARTS   AGE
pod/frontend-6cb7f8bd65-h2pnb        1/1     Running   0          6m27s
pod/frontend-6cb7f8bd65-kwlpr        1/1     Running   0          6m27s
pod/frontend-6cb7f8bd65-snwl4        1/1     Running   0          6m27s
pod/redis-leader-64fb8775bf-kbs6s    1/1     Running   0          6m28s
pod/redis-follower-779b6d8f79-5dphr 1/1     Running   0          6m28s
pod/redis-follower-899c7e2z65-8apnk 1/1     Running   0          6m28s

NAME                                  TYPE           CLUSTER-IP       EXTERNAL-IP
PORT(S)        AGE
service/guestbook-frontend            LoadBalancer   10.10.89.59      10.19.15.99
80:31513/TCP   65s
service/redis-follower                ClusterIP      10.111.163.189   <none>
6379/TCP       65s
service/redis-leader                  ClusterIP      10.111.70.189    <none>
6379/TCP       65s

NAME                                           READY   UP-TO-DATE   AVAILABLE   AGE
deployment.apps/guestbook-frontend-deployment   3/3     3            3           65s
deployment.apps/redis-follower-deployment       1/2     2            1           65s
deployment.apps/redis-leader-deployment         1/1     1            1           65s

NAME                                                    DESIRED   CURRENT   READY   AGE
replicaset.apps/guestbook-frontend-deployment-56fc5b6b47   3         3         3       65s
replicaset.apps/redis-follower-deployment-6fc9cf5759       2         2         1       65s
replicaset.apps/redis-leader-deployment-7d89bbdbcf         1         1         1       65s
```

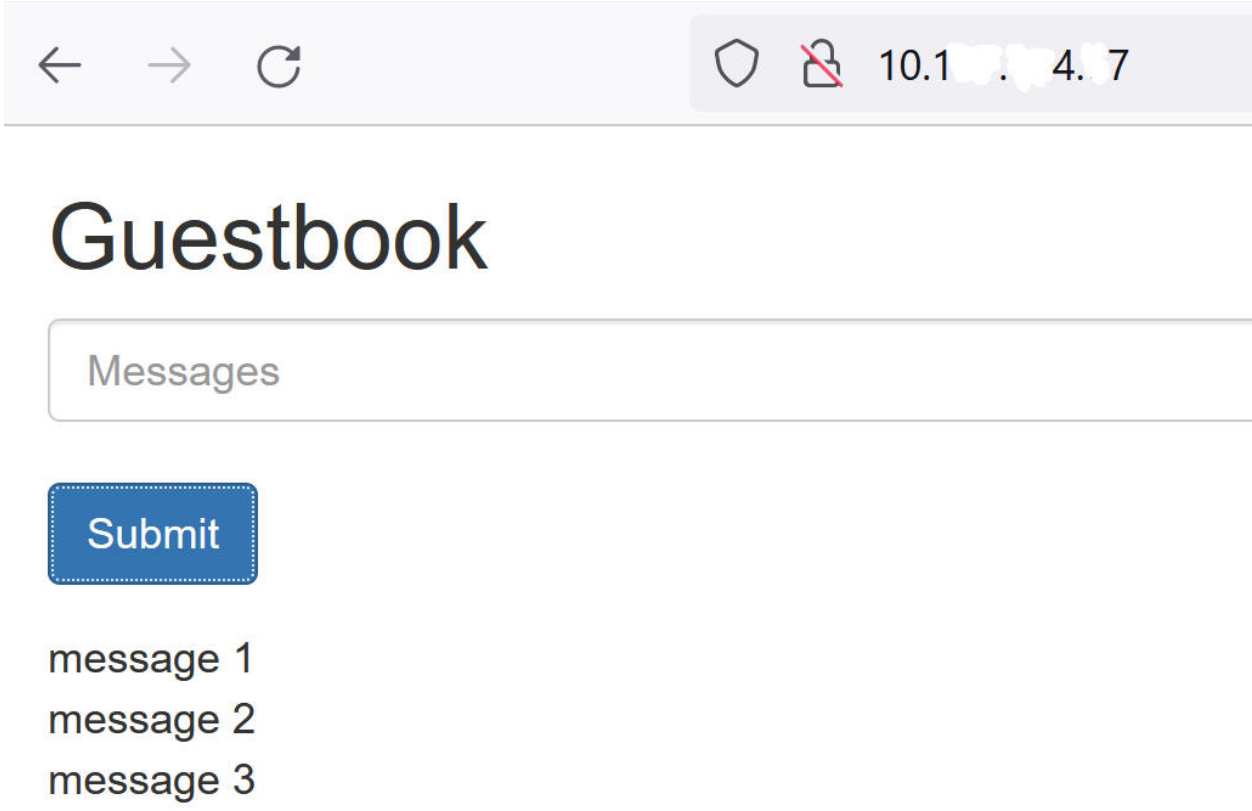
Überprüfen Sie, ob die persistenten Volumes wiederhergestellt wurden:

```
kubectl get pvc,pv -n guestbook

NAME                                       STATUS
VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   AGE
persistentvolumeclaim/redis-leader-claim   Bound    pvc-a2f6e6d4-42db-4fb8-
a198-5379a2552509   2Gi        RWO            thin-disk      2m40s
persistentvolumeclaim/redis-follower-claim Bound    pvc-55591938-921f-452a-
b418-2cc680c0560b   2Gi        RWO            thin-disk      2m40s

NAME                                                       CAPACITY   ACCESS MODES   RECLAIM
POLICY   STATUS   CLAIM                                STORAGECLASS   REASON   AGE
persistentvolume/pvc-55591938-921f-452a-b418-2cc680c0560b   2Gi        RWO
Delete           Bound    guestbook/redis-follower-claim    thin-disk               2m40s
persistentvolume/pvc-a2f6e6d4-42db-4fb8-a198-5379a2552509   2Gi        RWO
Delete           Bound    guestbook/redis-leader-claim      thin-disk               2m40s
```

Öffnen Sie zum Schluss das Guestbook-Frontend über die externe IP des Guestbook-Frontend-Diensts und überprüfen Sie, ob die Nachrichten, die Sie zu Beginn des Lernprogramms gesendet haben, wiederhergestellt wurden. Beispiel:



Sichern und Wiederherstellen mithilfe von Velero mit CSI-Snapshot

Sie können Velero mit CSI-Snapshot verwenden, um von CSI erstellte persistente Volumes für Arbeitslasten zu sichern und wiederherzustellen, die in auf Supervisor bereitgestellten TKG-Clustern ausgeführt werden.

Anforderungen

Beachten Sie die folgenden Anforderungen:

- vSphere 8.0 U2 oder höher
- Tanzu Kubernetes-Version v1.26.5 für vSphere 8.x oder höher
- Persistente Volumes, die mithilfe von CSI-Treibern erstellt wurden, die Volume-Snapshot unterstützen

Achtung Die Verwendung von Velero mit CSI-Snapshot ist nur für dauerhafte Volumes verfügbar, die mithilfe von CSI-Treibern erstellt wurden, die Volume-Snapshots unterstützen. Weitere Informationen finden Sie unter Erstellen von Snapshots in einem TKG-Cluster in *Verwenden des TKG-Dienstes mit der vSphere IaaS-Steuerungsebene*.

Prozedur

Sie können Velero mit CSI-Snapshot (Container Storage Interface) zum Sichern und Wiederherstellen von Arbeitslasten verwenden, die auf TKGS-Clustern ausgeführt werden. Der Velero node-agent ist ein DaemonSet, das Module hostet, um die konkreten Aufgaben der Sicherung und Wiederherstellung mithilfe von CSI-Snapshot-Datenverschiebungen abzuschließen. Weitere Informationen finden Sie unter Unterstützung von Container Storage Interface Snapshots in Velero.

1 Erstellen Sie einen S3-kompatiblen Speicherort, z. B. MinIO oder einen AWS S3-Bucket.

   Im folgenden Beispiel wird ein AWS S3-Bucket verwendet.

   Informationen zur Verwendung von MinIO finden Sie unter Installieren und Konfigurieren des MinIO-Objektspeichers.

2 Installieren Sie die Velero-CLI auf dem Clusterclient, auf dem Sie kubectl ausführen.

   Laden Sie ihn von https://github.com/vmware-tanzu/velero/releases herunter.

   Weitere Informationen finden Sie in den Installationsanweisungen unter einem der folgenden Links:

   - Schritt 1: Installieren der Velero-CLI auf einem Linux-Workstation
   - Installieren der Velero-CLI
   - https://velero.io/docs/v1.12/basic-install/#install-the-cli

3 Stellen Sie eine Verbindung zu dem TKG-Dienst-Cluster her, in dem Sie die Velero-Sicherung testen möchten.

   Weitere Informationen finden Sie unter Herstellen einer Verbindung mit einem TKG-Cluster als vCenter Single Sign-On-Benutzer mit Kubectl.

4 Installieren Sie Velero mit dem Velero-CLI-Plug-In im Cluster.

   Ab Velero v1.14 wird das Velero-CSI-Plug-In mit Velero zusammengeführt. Wenn Sie demnach Velero v1.14 oder höher installieren, müssen Sie das Velero-CSI-Plug-In nicht separat installieren. Wenn Sie es dennoch tun, kann der Velero-Pod nicht gestartet werden.

   Beispiel: Mithilfe des folgenden Befehls wird Velero mit einem AWS S3-Speicher-Backend und der zugehörigen Anmeldedatendatei installiert. Da es sich um Velero v1.14 handelt, müssen Sie das Velero-CSI-Plug-In nicht separat installieren.

```
velero install \
    --provider aws \
    --plugins velero/velero-plugin-for-aws:v1.14 \
    --bucket velero-cpe-backup-bucket \
    --secret-file ./cloud-credential \
    --use-volume-snapshots=true \
    --features=EnableCSI --use-node-agent
```

Zum Installieren einer früheren Velero-Version müssen Sie das Velero-CSI-Plug-In ebenfalls installieren. Beispiel:

```
velero install \
    --provider aws \
    --plugins velero/velero-plugin-for-aws:v1.9.0,velero/velero-plugin-for-csi:v0.7.0 \
    --bucket velero-cpe-backup-bucket \
    --secret-file ./cloud-credential \
    --use-volume-snapshots=true \
    --features=EnableCSI --use-node-agent
```

Sichern und Wiederherstellen von VM-Dienst-VMs in vSphere IaaS Control Plane

5

Als vSphere-Administrator verwenden Sie Backup-Partnerlösungen, die auf VMware vSphere Storage APIs – Data Protection (VADP) basieren, um automatisch eine Sicherung, vollständige Wiederherstellung und Registrierung einer VM-Dienst-VM auf einem Supervisor durchzuführen. Wenn die automatische Registrierung aufgrund von Problemen mit der zugrunde liegenden Infrastruktur fehlschlägt, können Sie die Probleme beheben und dann die `registerVM`-API manuell aufrufen, um die VM erneut zu registrieren.

Sichern einer VM-Dienst-VM

In vSphere IaaS Control Plane können Sie automatische Sicherungen von VM-Dienst-VMs über eine Backup-Partnerlösung wie Veeam durchführen, die VMware vSphere Storage APIs – Data Protection verwendet.

In der Regel nutzt ein vSphere-Administrator die Partnerlösung, um die folgenden Aufgaben auszuführen:

- Einrichten der Sicherungsinfrastruktur, einschließlich der Installation von Sicherungssoftware und der Konfiguration von Sicherungsspeichern und Repositorys.
- Erstellen einer Sicherungsaufgabe für eine VM oder eine Gruppe von VMs.
- Initiieren von Sicherungen durch Auslösen des Auftrags.

Wenn sie ausgelöst wird, sichert die Partnersoftware die Konfiguration, die Daten und den Kubernetes-Status der VM.

In der Regel umfasst die Sicherung die folgenden Elemente:

- Die in vCenter Server gespeicherte VM-Konfiguration.
- Die VMX-Datei.
- Inhalte von VM-Datenfestplatten, die statisch oder FCDs sein können.

Bei VM-Dienst-VMs umfasst die Sicherung auch den Kubernetes-Status der VM sowie weitere Ressourcen, die für das Bootstrap der virtuellen Maschine bei der Wiederherstellung erforderlich sind.

Weitere Informationen zu VMware vSphere Storage APIs – Data Protection und zur Verwendung der Partnersicherungslösungen finden Sie im Knowledge Base-Artikel 1021175 und in Ihrer Partnerdokumentation.

Wiederherstellen einer VM-Dienst-VM

Bei Bedarf kann der vSphere-Administrator die Sicherung verwenden, um die VM wiederherzustellen. Er kann beispielsweise eine VM wiederherstellen, die ausgefallen ist.

vSphere IaaS Control Plane unterstützt nur die vollständige VM-Wiederherstellung, bei der eine gesamte VM aus einer Sicherungsdatei in den aktuellen Zustand der ursprünglichen VM wiederhergestellt wird.

Um diese Art der Wiederherstellung durchzuführen, ist darauf zu achten, dass die ursprüngliche VM auf dem Supervisor und in vSphere nicht vorhanden ist. Wenn sie noch vorhanden ist, verwenden Sie den Befehl `kubectl delete vm` im Supervisor, bevor Sie den Wiederherstellungsauftrag auslösen.

Nachdem Sie den Wiederherstellungsvorgang über die Sicherungssoftware ausgelöst haben, erstellt die Sicherungssoftware die VM im Ressourcenpool und Ordner neu, die während der Wiederherstellung angegeben wurden. Die VM kann mit demselben oder einem anderen VM-Namen wiederhergestellt werden.

Wenn der Vorgang erfolgreich war, erkennt und registriert vSphere IaaS Control Plane automatisch die wiederhergestellte VM auf dem Supervisor in demselben vSphere-Namespace, in dem sie ursprünglich erstellt wurde. Während des Wiederherstellungsvorgangs wird eine VirtualMachine-Ressource auf dem Supervisor erstellt. Gegebenenfalls werden außerdem alle zusätzlichen Ressourcen erstellt, wie z. B. ein geheimer Schlüssel zum Bootstrap der VM oder PersistentVolumeClaims für zusätzliche Volumes, die von der virtuellen Maschine verwendet werden.

Weitere Informationen über geheime Schlüssel finden Sie in der Kubernetes-Dokumentation unter https://kubernetes.io/docs/concepts/configuration/secret/. Informationen zu persistenten Volumes finden Sie unter https://kubernetes.io/docs/concepts/storage/persistent-volumes/.

Leitlinien und Überlegungen

Beachten Sie beim Wiederherstellen der VM Folgendes:

- Bevor Sie mit dem Wiederherstellungsvorgang beginnen, führen Sie die folgenden Schritte aus:
  - Stellen Sie sicher, dass die ursprüngliche VM aus dem Supervisor und aus vSphere entfernt wurde. Wenn sie noch vorhanden ist, verwenden Sie den Befehl `kubectl delete vm` im Supervisor, um sie zu löschen.

- Stellen Sie sicher, dass die zugrunde liegende Infrastruktur zwischen Sicherung und Wiederherstellung nicht geändert wurde. Stellen Sie sicher, dass alle geeigneten Ressourcen, die die ursprüngliche VM verwendet hat, wie z. B. VM-Klassen und Speicherrichtlinien, auf dem Ziel-vSphere-Namespace intakt sind.

  Andernfalls schlägt die automatische Registrierung der VM mit einer Fehlermeldung fehl.

- Die wiederhergestellte VM ist auf demselben Ziel-vSphere-Namespace registriert, in dem sie ursprünglich erstellt wurde.
- Zielressourcenpool und Ordnername müssen mit denen identisch sein, in denen die ursprüngliche VM vorhanden war.
- Der Name der wiederhergestellten VM kann mit dem ursprünglichen VM-Namen identisch sein. Sie können auch einen anderen VM-Namen verwenden.

Lesen Sie als Nächstes die folgenden Themen:

- Manuelles Registrieren einer VM-Dienst-VM

Manuelles Registrieren einer VM-Dienst-VM

Wenn die automatische Registrierung der VM aus irgendeinem Grund nicht erfolgreich ist, erhalten Sie eine Fehlermeldung, die Sie über die genauen Probleme informiert, die den Fehler verursachen. Nachdem Sie die Probleme behoben haben, können Sie die `registerVM`-API aufrufen und die moID der VM verwenden, um die VM manuell zu registrieren.

Im folgenden Beispiel werden die Datencenter CLI(DCLI)-Befehle zum Registrieren der VM verwendet.

Verfahren

1 Rufen Sie die moID der zu registrierenden VM ab.

```
# dcli com vmware vcenter vm list
```

Die moID, auch als MORef-ID bezeichnet, setzt sich aus dem VM-Präfix zusammen, gefolgt von einer numerischen ID, z. B. vm-123456.

2 Registrieren Sie die VM manuell.

```
# dcli com vmware vcenter namespaces instances registervm --namespace my-namespace --vm
vm-123456 +username my-username +password my-password
```

Der Befehl gibt eine Aufgabe zurück, die ähnlich wie die folgende aussieht:

```
task-637:6b051692-7aff-4d59-8a3f-699d114d37e3
```

3 Verwenden Sie den VAPI-Aufgabendienst, um den Status der Aufgabe abzurufen.

```
# dcli com vmware cis tasks get --task task-637:6b051692-7aff-4d59-8a3f-699d114d37e3
+username my-username +password my-password
```

Der Befehl gibt den Status der Aufgabe und etwaige Fehlermeldungen zurück, wenn der Vorgang fehlschlägt.

Sichern und Wiederherstellen von vSphere-Pods mit Velero-Plug-In für vSphere

6

Mit dem Velero-Plug-In für vSphere können Sie Arbeitslasten, die auf vSphere-Pods ausgeführt werden, sichern und wiederherstellen.

Überblick

Mit dem Velero-Plug-In für vSphere können Sie Arbeitslasten, die auf vSphere-Pods ausgeführt werden, im Supervisor sichern und wiederherstellen. Sie können sowohl statusfreie als auch statusbehaftete Anwendungen, die auf vSphere-Pods ausgeführt werden, sichern und wiederherstellen. Für statusbehaftete Anwendungen verwenden Sie das Velero-Plug-In für vSphere, um Snapshots der persistenten Volumes (PVs) zu erstellen.

Hinweis Zum Sichern und Wiederherstellen von vSphere-Pods können Sie eigenständiges Velero nicht zusammen mit Restic verwenden. Stattdessen müssen Sie das auf dem Supervisor installierte Velero-Plug-In für vSphere verwenden.

Voraussetzungen

Bevor Sie vSphere-Pods sichern und wiederherstellen können, müssen Sie das Velero-Plug-In für vSphere installieren und konfigurieren. Weitere Informationen finden Sie unter #unique_20.

Hinweis Das Velero-Plug-In für vSphere führt keine Sicherung und Wiederherstellung des Zustands des Supervisors durch.

Sicherung eines vSphere Pods

Führen Sie den folgenden Befehl aus, um einen statusfreien vSphere Pod zu sichern:

```
velero backup create <backup name> --include-namespaces=my-namespace
```

Die Sicherung wird als `Completed` gekennzeichnet, nachdem alle lokalen Snapshots erstellt und Kubernetes-Metadaten in den Objektspeicher hochgeladen wurden. Die Sicherung von Volume-Snapshots erfolgt jedoch asynchron und kann weiterhin im Hintergrund durchgeführt werden. Es kann einige Zeit dauern, bis der Vorgang abgeschlossen ist.

Sie können den Status von Volume-Snapshots überprüfen, indem Sie benutzerdefinierte Snapshot- und Upload-Ressourcen überwachen.

Snapshot-CRD

Für jeden Volume-Snapshot wird eine benutzerdefinierte Snapshot-Ressource im selben Namespace erstellt wie die PVC, für die ein Snapshot erstellt wird. Sie können alle Snapshots im PVC-Namespace abrufen, indem Sie den folgenden Befehl ausführen.

```
kubectl get -n <pvc namespace> snapshot
```

Die Snapshot-CRD weist mehrere Statusangaben (Phasen) für das Feld „`status.phase`“ auf, einschließlich:

Zustand	Beschreibung
Neu	Noch nicht verarbeitet
Snapshotted	Lokaler Snapshot wurde erstellt
SnapshotFailed	Lokaler Snapshot ist fehlgeschlagen
Upload wird durchgeführt ...	Snapshot wird hochgeladen
Uploaded	Snapshot wurde hochgeladen
UploadFailed	Snapshot konnte nicht hochgeladen werden
Canceling	Hochladen des Snapshots wird abgebrochen
Abgebrochen	Hochladen des Snapshots wurde abgebrochen
CleanupAfterUploadFailed	Bereinigung des lokalen Snapshots nach dem Hochladen des Snapshots fehlgeschlagen

Hochladen einer CRD

Für jeden Volume-Snapshot, der in den Objektspeicher hochgeladen werden soll, wird eine benutzerdefinierte Upload-Ressource im selben Namespace wie Velero erstellt. Sie können alle Uploads im Velero-Namespace abrufen, indem Sie den folgenden Befehl ausführen.

```
kubectl get -n <velero namespace> upload
```

Die Upload-CRD verfügt über mehrere Statusangaben (Phasen) für das Feld „`status.phase`“, einschließlich:

Zustand	Beschreibung
Neu	Noch nicht verarbeitet
InProgress	Upload wird ausgeführt
UploadError	Upload fehlgeschlagen
CleanupFailed	Löschen des lokalen Snapshots nach dem Hochladen fehlgeschlagen Vorgang wird wiederholt

Zustand	Beschreibung
Canceling	Upload wird abgebrochen Kann vorkommen, wenn `velero backup delete` aufgerufen wird, während der Snapshot hochgeladen wird
Abgebrochen	Upload wurde abgebrochen

Wenn beim Hochladen Fehler auftreten, werden die Uploads in regelmäßigen Abständen erneut versucht. Dabei wechselt ihr Status wieder zu InProgress. Nachdem ein Upload erfolgreich abgeschlossen wurde, bleibt sein Datensatz für einen bestimmten Zeitraum bestehen und wird schließlich entfernt.

Wiederherstellen eines vSphere Pods

Führen Sie die folgenden Schritte aus, um eine vSphere Pod-Arbeitslast wiederherzustellen, die mit dem Velero-Plug-In für vSphere gesichert wurde.

1 Erstellen Sie einen vSphere-Namespace für die Arbeitslast, die Sie wiederherstellen möchten.

2 Konfigurieren Sie die Speicherrichtlinie für den Namespace.

3 Führen Sie den folgenden Velero-Befehl aus, um die Arbeitslast wiederherzustellen:

```
velero restore create --from-backup backup-name
```

Die Velero-Wiederherstellung wird als `Completed` gekennzeichnet, wenn Volume-Snapshots und andere Kubernetes-Metadaten erfolgreich im aktuellen Cluster wiederhergestellt wurden. Zu diesem Zeitpunkt sind alle Aufgaben des vSphere Plug-Ins im Zusammenhang mit dieser Wiederherstellung ebenfalls abgeschlossen. Im Falle einer Velero-Sicherung werden keine asynchronen Datenverschiebungsaufgaben im Hintergrund ausgeführt.

Bevor die Velero-Wiederherstellung als `Completed` gekennzeichnet wird, können Sie den Status der Volume-Wiederherstellung überprüfen, indem Sie die CloneFromSnapshot/Download-CRs wie folgt überwachen.

CloneFromSnapshots-CRD

Um die Wiederherstellung für jeden Volume-Snapshot durchzuführen, wird eine benutzerdefinierte CloneFromSnapshot-Ressource (Custom Resource, CR) im selben Namespace erstellt wie die PVC, für die ursprünglich ein Snapshot erstellt wurde. Sie können alle CloneFromSnapshots im PVC-Namespace abrufen, indem Sie den folgenden Befehl ausführen.

```
kubectl -n <pvc namespace> get clonefromsnapshot
```

Die CloneFromSnapshot-CRD weist mehrere Statusangaben (Phasen) für das Feld „`status.phase`“ auf, einschließlich:

Zustand	Beschreibung
Neu	Das Klonen aus dem Snapshot ist nicht abgeschlossen
Abgeschlossen	Das Klonen aus dem Snapshot ist abgeschlossen
Fehlgeschlagen	Klonen aus Snapshot fehlgeschlagen

Herunterladen einer CRD

Bei jeder Wiederherstellung eines Volume-Snapshots, der aus dem Objektspeicher heruntergeladen werden soll, wird eine Download-CR im selben Namespace wie Velero erstellt. Sie können alle Downloads im Velero-Namespace abrufen, indem Sie den folgenden Befehl ausführen.

```
kubectl -n <velero namespace> get download
```

Die Download-CRD weist mehrere Statusangaben (Phasen) für das Feld „`status.phase`“ auf, einschließlich:

Status	Beschreibung
Neu	Noch nicht verarbeitet
InProgress	Download läuft
Abgeschlossen	Download abgeschlossen
Wiederholen	Es wird erneut versucht, den Download auszuführen. Wenn während des Downloads von Sicherungsdaten ein Fehler auftritt, wird ein neuer Download-Versuch durchgeführt.
Fehlgeschlagen	Download ist fehlgeschlagen

Fehlerbehebung beim Sichern und Wiederherstellen der vSphere IaaS Control Plane

7

Informationen zur Fehlerbehebung bei Problemen im Zusammenhang mit der Sicherung und Wiederherstellung der vSphere IaaS Control Plane.

Lesen Sie als Nächstes die folgenden Themen:

- Bereinigen verwaister Objekte nach der Wiederherstellung des Supervisor aus einer Sicherung

Bereinigen verwaister Objekte nach der Wiederherstellung des Supervisor aus einer Sicherung

Nachdem Sie den Supervisor aus einer Sicherung wiederhergestellt haben, werden alle nach der Sicherung erstellten K8s-Ressourcen nach Abschluss der Wiederherstellung gelöscht. Wenn einige dieser Ressourcen mit Objekten verknüpft waren, wie z. B. VMs oder Festplatten, gelten sie in vCenter Server als verwaist. Sie müssen eine Bereinigung der verwaisten Objekte aus vCenter Server durchführen.

Verfahren

1 Listet alle VMs für einen vSphere-Namespace auf.

a Rufen Sie `folderMoId` für den vSphere-Namespace ab, indem Sie folgenden Befehl auf einer Supervisor-VM der Steuerungsebene ausführen:

```
root@421c9fa40208448fecc15d277bdca66d [ ~ ]# kubectl get availabilityzone -o json
{
    "apiVersion": "v1",
    "items": [
        {
            "apiVersion": "topology.tanzu.vmware.com/v1alpha1",
            "kind": "AvailabilityZone",
            "metadata": {
                ...
            },
            "spec": {
                "clusterComputeResourceMoIDs": [
                    "domain-c50"
                ],
                "clusterComputeResourceMoId": "domain-c50",
                "namespaces": {
                    "pod-ns": {
                        "folderMoId": "group-v81", <--- this is the folderMoId that
you need for next step
                        ...
                    },
                    "vmsvc-ns": {
                        "folderMoId": "group-v83", <--- this is the folderMoId that
you need for next step
                        ...
                    }
                }
            }
        }
    ],
    "kind": "List",
    "metadata": {
        "resourceVersion": ""
    }
}
```

b Listen Sie alle vorhandenen VMs im vSphere-Namespace auf, indem Sie folgenden DCLI-Befehl ausführen:

Im Beispiel wird der Namespace `pod-ns` verwendet

```
root@sc2-10-186-199-30 [ ~ ]# dcli +i +username 'Administrator@vsphere.local'
+password <password>
Welcome to VMware Datacenter CLI (DCLI)

usage: <namespaces> <command>
```

```
To auto-complete and browse DCLI namespaces:   [TAB]
If you need more help for a command:           vcenter vm get --help
If you need more help for a namespace:         vcenter vm --help
To execute dcli internal command: env
For detailed information on DCLI usage visit:  http://vmware.com/go/dcli

dcli> com vmware vcenter vm list --folders group-v81
|---------------|-----|----------------------------------------|-----------|---------|
|memory_size_MiB|vm   |name                                    |power_state|cpu_count|
|---------------|-----|----------------------------------------|-----------|---------|
|512            |vm-84|deployment-before-backup-778449d88d-c9gnc|POWERED_ON |1        |
|512            |vm-85|deployment-before-backup-778449d88d-4jtqj|POWERED_ON |1        |
|512            |vm-86|deployment-before-backup-778449d88d-tqwbh|POWERED_ON |1        |
|512            |vm-91|deployment-after-backup-778449d88d-khkxx |POWERED_OFF|1        |
|512            |vm-92|deployment-after-backup-778449d88d-7dgcc |POWERED_OFF|1        |
|512            |vm-93|deployment-after-backup-778449d88d-sxbcf |POWERED_OFF|1        |
|---------------|-----|----------------------------------------|-----------|---------|
```

.

2 Suchen Sie nach verwaisten Namespaces und bereinigen Sie sie.

Wenn ein Namespace nach der Erstellung einer Supervisor-Sicherung gelöscht wird, wird dieser Namespace nach der Wiederherstellung des Supervisor als Kubernetes-Ressource neu erstellt. Sie müssen diese K8s-Ressource löschen.

a Suchen Sie nach dem verwaisten Namespace, indem Sie alle Namespaces in vCenter Server auflisten.

```
dcli> com vmware vcenter namespaces instances list
```

b Listen Sie alle Namespace-K8s-Ressourcen auf.

```
root@423f9d75bef000dc828a535c6ac0bd4b [ ~ ]# k get ns -A
```

a Suchen Sie nach Unterschieden zwischen den Objekten, die sich aus Schritt A und Schritt B ergeben haben, und bereinigen Sie verwaiste Namespace-K8s-Ressourcen.

```
root@423f9d75bef000dc828a535c6ac0bd4b [ ~ ]# k delete ns test-set-workload-ns
namespace "test-set-workload-ns" deleted
```

3 Suchen Sie nach verwaisten VMs, die mit `VirtualMachine`-Ressourcen verknüpft sind, und bereinigen Sie sie.

Bei `VirtualMachine`-Kubernetes-Ressourcen, die nach der Supervisor-Sicherung erstellt werden, kommt es zu verwaisten VMs, sobald der Supervisor aus dieser Sicherung wiederhergestellt wird. Sie müssen diese verwaisten VMs aus der vCenter Server-Bestandsliste löschen.

a Suchen Sie nach verwaisten VMs, die mit `VirtualMachine`-Ressourcen verknüpft sind.

In den folgenden Schritten wird der Namespace `vmsvc-ns` als Beispiel verwendet.

1 Listen Sie alle VMs in der vCenter Server-Bestandsliste auf. Im Beispiel „snipped“ werden alle VMs in vCenter Server aufgelistet, da `group-96` mit dem Namespace `vmsvc-ns` verknüpft ist.

```
dcli> com vmware vcenter vm list --folders group-v96
|---------------|------|------------|-----------|---------|
|memory_size_MiB|vm    |name        |power_state|cpu_count|
|---------------|------|------------|-----------|---------|
|2048           |vm-104|vmsvc-after |POWERED_ON |2        |
|2048           |vm-97 |vmsvc-before|POWERED_ON |2        |
|---------------|------|------------|-----------|---------|
```

2 Listen Sie alle `VirtualMachine`-K8s-Ressourcen auf. Führen Sie `kubectl get` aus, um Ressourcendetails auf einer der Steuerungsebenen-VMs abzurufen, und suchen Sie in der Ausgabe nach `uniqueID`. In diesem Beispiel wird die mit K8s-Ressourcen verknüpfte VM-Liste mit der Bezeichnung `vm-97` verwendet.

```
root@42344b596f57bfcf9441179fa1ed1a5c [ ~ ]# k get vm -n vmsvc-ns -o json
{
    "apiVersion": "v1",
    "items": [
        {
            "apiVersion": "vmoperator.vmware.com/v1alpha1",
            "kind": "VirtualMachine",
            ...
            "uniqueID": "vm-97",
...
}
```

3 Vergleichen Sie die beiden Listen, die sich aus den obigen Schritten ergeben haben.

- Die VM-Liste in vCenter Server: `<vm-104, vm-97>`
- Die mit K8s-Ressourcen verknüpfte VM-Liste: `<vm-97>`

Folglich lautet die Liste der verwaisten VMs: `<vm-104>`.

b Bereinigen Sie die verwaisten VMs.

```
dcli> com vmware vcenter vm power stop --vm vm-104
dcli> com vmware vcenter vm delete --vm vm-104
```

4 Suchen Sie nach verwaisten VMs, die mit Pod-Ressourcen verknüpft sind, und bereinigen Sie sie.

Pod-K8s-Ressourcen, die nach der Supervisor-Sicherung erstellt werden, führen zu verwaisten VMs im vCenter Server, nachdem Supervisor wiederhergestellt wurde. Führen Sie die Schritte aus, um nach ihnen zu suchen und sie zu bereinigen.

In den Beispielen wird der Namespace `pod-ns` verwendet.

a Listen Sie alle VMs in der vCenter Server-Bestandsliste auf.

In diesem Beispiel ist die VM-Gruppe `group-v83` mit dem Namespace `pod-ns` verknüpft. Die VM-Liste lautet `vm-88`, `vm-89`, `vm-90`, `vm-101`, `vm-102` und `vm-103`.

```
dcli> com vmware vcenter vm list --folders group-v83
|---------------|------|----------------------------------------|-----------|---------
|
|memory_size_MiB|vm    |name                                    |power_state|
cpu_count|
|---------------|------|----------------------------------------|-----------|---------
|
|512            |vm-101|deployment-after-backup-778449d88d-ldvn8 |POWERED_OFF|1
|
|512            |vm-102|deployment-after-backup-778449d88d-v29dd |POWERED_OFF|1
|
|512            |vm-103|deployment-after-backup-778449d88d-zdbl9 |POWERED_OFF|1
|
|512            |vm-88 |deployment-before-backup-778449d88d-fgq5b|POWERED_ON |1
|
|512            |vm-89 |deployment-before-backup-778449d88d-mp7td|POWERED_ON |1
|
|512            |vm-90 |deployment-before-backup-778449d88d-cjhq6|POWERED_ON |1
|
|---------------|------|----------------------------------------|-----------|---------
|
```

b Listen Sie K8s-Ressourcen auf.

Führen Sie `kubectl get` aus, um Ressourcendetails auf einer der Steuerungsebenen-VMs abzurufen, und suchen Sie in der Ausgabe nach `vmware-system-vm-moid`. Die mit K8s-Ressourcen verknüpfte VM-Liste lautet `vm-88`, `vm-89` `vm-90`.

```
root@42344b596f57bfcf9441179fa1ed1a5c [ ~ ]# k get pod -n pod-ns -o json
{
    "apiVersion": "v1",
    "items": [
        {
            "apiVersion": "v1",
            "kind": "Pod",
            "metadata": {
                "annotations": {
                    ...
                    "vmware-system-vm-moid": "vm-90:5a5198fc-c5cb-4b89-
a70f-331025b40539",
                    ...
                },
                    ...
                    "vmware-system-vm-moid": "vm-88:5a5198fc-c5cb-4b89-
a70f-331025b40539",
                    ...
```

```
                    "vmware-system-vm-moid": "vm-89:5a5198fc-c5cb-4b89-
a70f-331025b40539",
                    ...
}
```

c Vergleichen Sie die beiden Listen, die sich aus den obigen Schritten ergeben haben.

- Die VM-Liste in vCenter Server lautet: `<vm-88, vm-89, vm-90, vm-101, vm-102, vm-103>`
- Die mit K8s-Ressourcen verknüpfte VM-Liste lautet: `<vm-88, vm-89, vm-90>`

Folglich lautet die Liste der verwaisten VMs: `<vm-101, vm-102, vm-103>`

d Bereinigen Sie verwaiste VMs.

```
dcli> com vmware vcenter vm delete --vm vm-101
dcli> com vmware vcenter vm delete --vm vm-102
dcli> com vmware vcenter vm delete --vm vm-103
```

5 Suchen Sie nach verwaisten VMs und Ressourcenpools, die mit Tanzu Kubernetes Grid-Clustern verknüpft sind, und bereinigen Sie sie.

Tanzu Kubernetes Grid-Cluster, die nach der Supervisor-Sicherung erstellt werden, führen ebenfalls zu verwaisten VMs im vCenter Server, nachdem Supervisor wiederhergestellt wurde.

Hinweis Wenn nach der Wiederherstellung beim Erstellen von TKG-Clustern Probleme auftreten, müssen Sie verwaiste VMs bereinigen, indem Sie den Anweisungen im aktuellen Schritt folgen.

a Suchen Sie nach der Liste der verwaisten Tanzu Kubernetes Grid-Cluster.

Verwenden Sie kubectl, um die K8s-Ressourcenliste des Tanzu Kubernetes Grid-Clusters auf einer der Steuerungsebenen-VMs abzurufen: `<test-cluster, test-cluster-e2e-script, tkc-before-backup>`.

```
root@4239f4159c7063d5608cf3fc0bdd532e [ ~ ]# k get tkc -A
NAMESPACE             NAME                      CONTROL PLANE   WORKER   TKR
NAME                   AGE   READY   TKR COMPATIBLE   UPDATES AVAILABLE
selfservice-tkc-ns    test-cluster              1               1        v1.23.8---
vmware.3-tkg.1   19h   True    True
test-gc-e2e-demo-ns   test-cluster-e2e-script   3               1        v1.23.8---
vmware.3-tkg.1   18h   False   True
tkc-ns                tkc-before-backup         3               1        v1.23.8---
vmware.3-tkg.1   16h   True    True
```

Verwenden Sie die DCLI, um alle mit dem Namespace oder Tanzu Kubernetes Grid-Cluster verknüpften Ressourcenpools abzurufen. Rufen Sie anschließend die Liste des Tanzu Kubernetes Grid-Clusters in vCenter Server ab: `<test-cluster, test-cluster-e2e-script, tkc-before-backup, tkc-after-backup>`

```
dcli> com vmware vcenter resourcepool list
|----------------------|-------------|
|name                  |resource_pool|
|----------------------|-------------|
|Resources             |resgroup-10  |
|Resources             |resgroup-23  |
|Namespaces            |resgroup-56  |
|selfservice-tkc-ns    |resgroup-62  | <--- this is a namespace
|test-cluster          |resgroup-66  | <--- Tanzu Kubernetes Grid cluster
|test-gc-e2e-demo-ns   |resgroup-70  | <--- this is a namespace
|test-cluster-e2e-script|resgroup-74  | <--- Tanzu Kubernetes Grid cluster
|tkc-ns                |resgroup-80  | <--- this is a namespace
|tkc-before-backup     |resgroup-89  | <--- Tanzu Kubernetes Grid cluster
|tkc-after-backup      |resgroup-96  | <--- Tanzu Kubernetes Grid cluster
|----------------------|-------------|
```

b Vergleichen Sie die beiden Listen aus den obigen Schritten. Die Liste des verwaisten Tanzu Kubernetes Grid-Clusters lautet: `<tkc-after-backup>`

c Bereinigen Sie VMs, die mit dem verwaisten Tanzu Kubernetes Grid-Cluster verknüpft sind.

Rufen Sie mithilfe der DCLI alle VMs ab, die mit dem verwaisten Tanzu Kubernetes Grid-Cluster verknüpft sind, indem Sie den verknüpften Ressourcenpool `<resgroup-96>` verwenden:

```
dcli> com vmware vcenter vm list --resource-pools resgroup-96
|---------------|------|----------------------------------------------|-----------|---
------|
|memory_size_MiB|vm    |name                                          |power_state|
cpu_count|
|---------------|------|----------------------------------------------|-----------|---
------|
|2048           |vm-100|tkc-after-backup-zlcdm-wk5xf                  |POWERED_ON |
2        |
|2048           |vm-101|tkc-after-backup-zlcdm-76q4h                  |POWERED_ON |
2        |
|2048           |vm-98 |tkc-after-backup-zlcdm-9fv2w                  |POWERED_ON |
2        |
|2048           |vm-99 |tkc-after-backup-workers-4hdqb-657fb58d45-d7pqg|POWERED_ON |
2        |
|---------------|------|----------------------------------------------|-----------|---
------|
```

Löschen Sie dann die VMs nacheinander:

```
dcli> com vmware vcenter vm power stop --vm vm-100
dcli> com vmware vcenter vm delete --vm vm-100
```

d Bereinigen Sie den Ressourcenpool, der mit dem verwaisten Tanzu Kubernetes Grid-Cluster verknüpft ist.

```
<dcli> com vmware vcenter resourcepool delete --resource-pool resgroup-96
```

Sie können den verwaisten Ressourcenpool auch aus dem vSphere Client löschen.

6 Suchen Sie nach verwaisten FCDs (First Class Disks), die dauerhaften Volumes (Permanent Volumes, PVs) zugeordnet sind, und bereinigen Sie sie.

PV-K8s-Ressourcen, die nach der Supervisor-Sicherung erstellt werden, führen zu verwaisten FCDs im vCenter Server, nachdem Supervisor wiederhergestellt wurde. Führen Sie die Schritte aus, um nach ihnen zu suchen und sie zu bereinigen.

a Suchen Sie nach verwaisten FCDs, die mit PVs verknüpft sind.

1 Installieren Sie „govc“ zur Verwendung bei der Suche nach verwaisten FCDs. Bei „govc“ handelt es sich um eine benutzerfreundliche Alternative zur CLI, die sich hervorragend zur Automatisierung von Aufgaben eignet.

```
curl -L -o - "https://github.com/vmware/govmomi/releases/latest/download/govc_$
(uname -s)_$(uname -m).tar.gz" | tar -C /usr/local/bin -xvzf - govc
```

Weitere Installationsoptionen finden Sie unter https://github.com/vmware/govmomi/tree/main/govc#installation.

2 Führen Sie das folgende Bash-Skript zum Auflisten von PVs aus, die auf dem Supervisor vorhanden sind.

```
#!/bin/bash

export GOVC_INSECURE=1
export GOVC_USERNAME='Administrator@vsphere.local'
export GOVC_PASSWORD=<password>
export GOVC_URL=https://<vc ip>/sdk

# datastore path example - /test-vpx-1688432886-30489-wcp.wcp-sanity/datastore/
sharedVmfs-0
govc volume.ls -l -ds=<datastore path>
```

Ergebnis:

```
peiyangs@peiyangs-a01 govc % sudo bash orphanedPV.sh
590c8e31-f5bf-4179-9250-5cdd66bf591c
pvc-843c932b-8974-475d-8f8a-9b165137169d    1.0GB   KUBERNETES
vSphereSupervisorID-7f88d7b3-12ac-4fcf-a101-b80eb76becdf
37f8ad5b-dfe6-465b-b0f0-11591a2968dc    pvc-77c42590-
f0b0-457f-9743-6a3ebca55078    1.0GB   KUBERNETES
vSphereSupervisorID-7f88d7b3-12ac-4fcf-a101-b80eb76becdf
28a265b8-2e6b-421c-b16d-046ffc7aeea7    pvc-1b88c923-4354-4537-a7cb-
a8a6d763d5e7    1.0GB   KUBERNETES  vSphereSupervisorID-7f88d7b3-12ac-4fcf-a101-
b80eb76becdf
```

3 Führen Sie das folgende Bash-Skript aus, um alle Festplatten in vCenter Server aufzulisten:

```
#!/bin/bash

export GOVC_INSECURE=1
```

```
export GOVC_USERNAME='Administrator@vsphere.local'
export GOVC_PASSWORD=<password>
export GOVC_URL=https://<vc ip>/sdk

# datastore path example - /test-vpx-1688432886-30489-wcp.wcp-sanity/datastore/
sharedVmfs-0
govc disk.ls -l -ds=<datastore path>
```

Ergebnis:

```
peiyangs@peiyangs-a01 govc % sudo bash orphanedPV.sh
28a265b8-2e6b-421c-b16d-046ffc7aeea7  pvc-1b88c923-4354-4537-a7cb-a8a6d763d5e7
1.0G    Jul  4 02:33:27 <--- this is the disk correspondings to PV
37f8ad5b-dfe6-465b-b0f0-11591a2968dc  pvc-77c42590-f0b0-457f-9743-6a3ebca55078
1.0G    Jul  4 02:32:41 <--- this is the disk correspondings to PV
3a7517c2-f8c2-46a9-b0d5-18c665759311  vmware-sv-img-cache-domain-c50
26.0M   Jul  4 02:36:41
590c8e31-f5bf-4179-9250-5cdd66bf591c  pvc-843c932b-8974-475d-8f8a-9b165137169d
1.0G    Jul  4 02:30:45 <--- this is the disk correspondings to PV
68ba220c-0f83-49eb-b77a-d60471e24844  pvc-92f83ae0-7c2d-46d9-ab85-19858462ddd1
5.0G    Jul  4 18:27:02 <--- this is the disk correspondings to PV
72dbe8c5-a3b5-4298-8203-ea1cb86116e6  vmware-sv-img-cache-domain-c50
3.0M    Jul  4 02:38:39
79e233a6-0134-40e7-8ba8-3133442324f9  vmware-sv-img-cache-domain-c50
195.0M  Jul  4 18:26:12
a1a0a9d7-0baf-4592-9041-8c0feb960246  vmware-sv-img-cache-domain-c50
7.0M    Jul  4 02:35:37
cec2af09-80af-4086-a069-34140e2480dc  vmware-sv-img-cache-domain-c50
193.0M  Jul  4 02:31:12
```

4 Vergleichen Sie die beiden Listen aus den obigen Schritten.

- Die Liste der PVs: `<590c8e31-f5bf-4179-9250-5cdd66bf591c, 37f8ad5b-dfe6-465b-b0f0-11591a2968dc, 28a265b8-2e6b-421c-b16d-046ffc7aeea7>`
- Die Liste der FCDs: `<590c8e31-f5bf-4179-9250-5cdd66bf591c, 37f8ad5b-dfe6-465b-b0f0-11591a2968dc, 28a265b8-2e6b-421c-b16d-046ffc7aeea7, 68ba220c-0f83-49eb-b77a-d60471e24844>`

Zu den verwaisten FCDs gehören: `<68ba220c-0f83-49eb-b77a-d60471e24844>`

b Löschen Sie die verwaisten FCDs.

Löschen Sie mithilfe von „govc“ die verwaisten FCDs. Beispielskript:

```
#!/bin/bash

export GOVC_INSECURE=1
export GOVC_USERNAME='Administrator@vsphere.local'
export GOVC_PASSWORD=<password>
export GOVC_URL=https://<vc ip>/sdk
```

```
# datastore path example - /test-vpx-1688432886-30489-wcp.wcp-sanity/datastore/
sharedVmfs-0
govc disk.rm -ds=<datastore path> 68ba220c-0f83-49eb-b77a-d60471e24844
```

Ergebnis:

```
peiyangs@peiyangs-a01 govc % sudo bash orphanedPV.sh
[06-07-23 11:36:27] Deleting 68ba220c-0f83-49eb-b77a-d60471e24844...OK
```