Administratorhandbuch für VMware Integrated OpenStack

VMware Integrated OpenStack 3.1

Dieses Dokument unterstützt die aufgeführten Produktversionen sowie alle folgenden Versionen, bis das Dokument durch eine neue Auflage ersetzt wird. Die neuesten Versionen dieses Dokuments finden Sie unter http://www.vmware.com/de/support/pubs.

DE-001582-07

vmware®

Die neueste technische Dokumentation finden Sie auf der VMware-Website unter:

http://www.vmware.com/de/support/

Auf der VMware-Website finden Sie auch die aktuellen Produkt-Updates.

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie Ihre Kommentare und Vorschläge an:

docfeedback@vmware.com

Copyright © 2017 VMware, Inc. Alle Rechte vorbehalten. Informationen zu Copyright und Marken.

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

VMware Global, Inc.
Zweigniederlassung Deutschland
Freisinger Str. 3
85716 Unterschleißheim/Lohhof
Germany
Tel.: +49 (0) 89 3706 17000
Fax: +49 (0) 89 3706 17333
www.vmware.com/de

Inhalt

Über dieses Handbuch

Im *Administratorhandbuch für VMware Integrated OpenStack* erfahren Sie, wie Sie VMware Integrated OpenStack-Cloud-Verwaltungsaufgaben im VMware Integrated OpenStack durchführen. Dazu zählen das Erstellen und Verwalten von Projekten, Benutzerkonten, Typen, Images und Netzwerken.

Zielgruppe

Dieses Handbuch richtet sich an Cloud-Administratoren, die Ressourcen mit einer vollständig in VMware® vSphere® integrierten OpenStack-Bereitstellung erstellen und verwalten möchten. Um diese Verfahren erfolgreich durchzuführen, sollten Sie mit den Komponenten und Funktionen von OpenStack vertraut sein.

VMware Technical Publications – Glossar

VMware Technical Publications enthält ein Glossar mit Begriffen, die Ihnen möglicherweise unbekannt sind. Definitionen von Begriffen, die in der technischen Dokumentation von VMware verwendet werden, finden Sie unter http://www.vmware.com/support/pubs.

Aktualisierte Informationen

Administratorhandbuch für VMware Integrated OpenStack wird mit jeder Produktversion oder bei Bedarf aktualisiert.

Diese Tabelle enthält den Update-Verlauf für *Administratorhandbuch für VMware Integrated OpenStack*.

Revision	Beschreibung
001582-07	■ Die Upgradeverfahren für 3.0 und 3.1 wurden aktualisiert, um während des Updates auf den Übergang vom kompakten zum HA-Modus hinzuweisen. Siehe „Migrieren zur VMware Integrated OpenStack 3.0 oder 3.1-Bereitstellung“, auf Seite 48. ■ Es wurden Verfahren für das Konfigurieren der Profilerstellung für OpenStack-Bereitstellungen hinzugefügt. Siehe „Ablaufverfolgung von OpenStack-Bereitstellungen mithilfe der Profilerstellung“, auf Seite 57. ■ Es wurde ein Verfahren für die Single Sign-On-Integration mit VMware Identity Manager hinzugefügt. Siehe „Konfigurieren von VMware Identity Manager als Single Sign-On-Lösung für OpenStack“, auf Seite 29. ■ Es wurde ein Verfahren für das Konfigurieren von GPU-Passthrough-Geräten für OpenStack-Instanzen hinzugefügt. Siehe „Konfigurieren von GPU-Passthrough-Geräten für OpenStack-Instanzen“, auf Seite 84. ■ Es wurde ein Verfahren zum Ändern des standardmäßigen Adaptertyps durch Ändern des `vmware_adapter_type` hinzugefügt. Siehe „Ändern des Standardadaptertyps für Cinder-Volumes“, auf Seite 89. Es wurde ein Verfahren zur Verwendung der VMware NSX for vSphere -Sicherheitsrichtlinien über Sicherheitsgruppen hinzugefügt. Siehe „Verwenden der VMware NSX for vSphere -Sicherheitsrichtlinien über Sicherheitsgruppen“, auf Seite 66.
001582-06	■ Die Upgrade-Vorgänge wurden aktualisiert. Siehe „Aktualisieren auf VMware Integrated OpenStack 3.0 oder 3.1“, auf Seite 45. ■ Ein Querverweis auf den Abschnitt im Installationshandbuch, in dem die Hardwareanforderungen für den Kompaktmodus beschrieben werden, wurde hinzugefügt. ■ Der Abschnitt über LDAP wurde aktualisiert und beinhaltet nun neue Felder für die LDAP-Konfiguration. Siehe „Verwalten Ihrer Authentifizierungseinstellungen“, auf Seite 24. ■ Der Abschnitt über die Installation von Patches mithilfe des vSphere Web Client wurde aktualisiert. Siehe „Installieren eines Patches mit dem vSphere Web Client“, auf Seite 51. ■ Der Abschnitt über das Erstellen eines neuen Benutzers wurde aktualisiert und enthält nun Informationen über die Standarddomäne. Siehe „Erstellen eines Cloud-Benutzerkontos in OpenStack“, auf Seite 69. ■ Der Abschnitt über das Ändern eines Benutzerkontos wurde aktualisiert und enthält nun Informationen über das Ändern von Kennwörtern. Siehe „Ändern eines Benutzerkontos“, auf Seite 70.

Revision	Beschreibung
001582-05	■ Die CLI-Befehle wurden erweitert und enthalten jetzt neue und verbesserte Fehlerbehebungsfunktionen, einschließlich Befehlen zum Auffinden und Entfernen verwaister Instanzen und verbesserter Protokoll- und Statusberichte. Siehe Kapitel 8, „Befehlsreferenz für die Befehlszeilenschnittstelle von VMware Integrated OpenStack“, auf Seite 117. ■ Es wurde die neue Unterstützung für LBaaS v2.0 dokumentiert. ■ Es wurden Vorgänge für die Anpassung des auf den Dashboard-Seiten angezeigten Logos hinzugefügt. Siehe „Anpassen von Logos und Hintergrund für das Dashboard“, auf Seite 54. ■ Es wurden Vorgänge für das Migrieren von Images zwischen Datenspeichern hinzugefügt. Siehe „Migrieren von Images“, auf Seite 106. ■ Es wurde ein Verfahren zum Hinzufügen von Speicherkapazität zum Computing-Knoten hinzugefügt. Siehe „Hinzufügen von Speicher zum Computing-Knoten“, auf Seite 36. ■ Es wurde ein Verfahren zum Hinzufügen von Speicherkapazität zum Imagedienst-Knoten hinzugefügt. Siehe „Hinzufügen von Speicher zum Imagedienst“, auf Seite 36. ■ Der Sicherungsdienst für Blockspeicher wurde geändert, damit NFS 3.x und NFS 4.1 verarbeitet werden können. Siehe „Konfigurieren des Sicherungsdiensts für Blockspeicher“, auf Seite 37. ■ Es wurde ein Verfahren zum Hinzufügen von VM-Vorlagen als Images hinzugefügt. Siehe „Hinzufügen einer VM-Vorlage als Image“, auf Seite 108. ■ Es wurde ein Verfahren zum Ändern des Standardverhaltens von Nova-Snapshots hinzugefügt. Siehe „Ändern des Standardverhaltens für Nova-Snapshots“, auf Seite 109. ■ Es wurde ein Verfahren zum Ändern des Cinder-Standardverhaltens für Volume-Uploads hinzugefügt. Siehe „Ändern des Cinder-Standardverhaltens für das Hochladen auf Image“, auf Seite 110. ■ Es wurden Verfahren zum Konfigurieren von SR-IOV für Instanzen hinzugefügt. Siehe „Konfigurieren von Single Root I/O Virtualization für Instanzen“, auf Seite 83.
001582-04	■ Die Vorgänge für das Verwalten der Konfiguration Ihrer VMware Integrated OpenStack-Bereitstellung nach der Installation wurden erweitert und umstrukturiert. Siehe „Verwalten Ihrer Bereitstellungskonfiguration“, auf Seite 21. ■ Die Themen zur Verwaltung von Netzwerkeinstellungen wurden erweitert und umstrukturiert. Siehe „Verwalten Ihrer Netzwerkkonfiguration“, auf Seite 30. ■ Es wurden Informationen zur Aktivierung der Hochverfügbarkeit für Edge hinzugefügt. Siehe „Verwalten der Hochverfügbarkeit für NSX Edge-Knoten“, auf Seite 33. ■ Es wurden Informationen zum CLI-Befehl von VMware Integrated OpenStack hinzugefügt. Siehe Kapitel 8, „Befehlsreferenz für die Befehlszeilenschnittstelle von VMware Integrated OpenStack“, auf Seite 117. ■ Vorgänge für das Verwenden der richtlinienbasierten Speicherverwaltung wurden hinzugefügt. Siehe „Festlegen des standardmäßigen Nova-Speichers für OpenStack-Instanzen“, auf Seite 87. ■ Nebenversionen.
001582-03	■ Erweiterte Image-Verwaltungsprozeduren, um nicht unterstützte Quelle-Image-Formate mit einzubeziehen. Siehe „Importieren von Images zum Imagedienst“, auf Seite 95. ■ Der Abschnitt zur Versionsaktualisierung wurde aktualisiert, um das Verfahren zum Hinzufügen des erforderlichen IP-Adressbereichs abzuklären. Siehe „Hinzufügen von IP-Adressen zur Netzwerkkonfiguration“, auf Seite 46. ■ Verfahren für das Verstärken von DRS wurden hinzugefügt, um die Platzierung von OpenStack-Instanzen in vCenter-Hosts zu verwalten. Siehe „Anwenden von VM-Gruppeneinstellungen zu Image-Metadaten“, auf Seite 79. ■ Verfahren für das Angeben von QoS-Ressourcenzuteilungen für Instanzen wurden durch Modifizieren der Metadaten des Quell-Image hinzugefügt. Siehe „Konfigurieren von QoS-Ressourcenzuteilung für Instanzen unter Verwendung von Image-Metadaten“, auf Seite 103. ■ Verfahren für das Angeben von QoS-Ressourcenzuteilungen für Instanzen wurden durch Modifizieren der Metadaten des Typs hinzugefügt. Siehe „Konfigurieren von QoS Ressourcenzuteilung für Instanzen unter Verwendung von Typ-Metadaten“, auf Seite 114. ■ Ein Bereich zur Gastanpassung wurde hinzugefügt. Siehe „Konfigurieren von Images für Windows-Gastanpassung“, auf Seite 101. ■ Nebenversionen.

Revision	Beschreibung
001582-02	■ Für VMware Integrated OpenStack Version 2.0 aktualisiert. ■ Themen zu den Schritten nach der Installation und zu zusätzlichen Komponenten wurden entfernt. Diese sind jetzt im Installations- und Konfigurationshandbuch für VMware Integrated OpenStack enthalten. ■ Es wurden Schritte zum Sichern der VMware Integrated OpenStack-Bereitstellung hinzugefügt. Siehe „Sichern der VMware Integrated OpenStack-Bereitstellung“, auf Seite 39. ■ Es wurden Schritte zum Wiederherstellen der VMware Integrated OpenStack-Bereitstellung aus einer Sicherung hinzugefügt. Siehe „Wiederherstellen von VMware Integrated OpenStack aus einer Sicherung“, auf Seite 40. ■ Zusätzliche Schritte für die Wiederherstellung einzelner OpenStack-Knoten im Falle eines Fehlers. Siehe „Wiederherstellung nach einem Fehler“, auf Seite 41. ■ Zusätzliche Verfahren zum Konfigurieren eines Sicherungsdiensts für Cinder-Datenträger. ■ Nebenversionen.
001582-01	■ Es wurden Schritte zum Verbinden von Datenträgertypen mit einer vorhandenen Speicherrichtlinie hinzugefügt. Siehe „Erstellen eines Datenträgertyps“, auf Seite 90. ■ Die Vorgänge zum Konfigurieren des Objektspeicherknotens wurden erweitert. ■ Nebenversionen.
001582-00	Erstversion.

Grundlegende Informationen zu VMware Integrated OpenStack 1

Mit VMware Integrated OpenStack können Sie OpenStack-Dienste in Ihre vorhandene Implementierung von VMware vSphere einbinden.

Sie stellen VMware Integrated OpenStack über die Integrated OpenStack Manager vApp in vCenter bereit.

Der Integrated OpenStack Manager bietet einen Workflow, der Sie durch den VMware Integrated OpenStack-Bereitstellungsvorgang führt und diesen abschließt. Mit Integrated OpenStack Manager können Sie Ihre Verwaltungs- und Computing-Cluster angeben, Ihr Netzwerk konfigurieren und Ressourcen hinzufügen. Nach der Bereitstellung können Sie Integrated OpenStack Manager verwenden, um Komponenten hinzufügen oder die Konfiguration Ihrer VMware Integrated OpenStack-Cloud-Infrastruktur zu ändern.

VMware Integrated OpenStack 3.x basiert auf der Mitaka-Version von OpenStack.

Dieses Kapitel behandelt die folgenden Themen:

Internationalisierung

VMware Integrated OpenStack 2.0 und höher ist in Englisch und sieben weiteren Sprachen verfügbar: Vereinfachtes Chinesisch, Traditionelles Chinesisch, Japanisch, Koreanisch, Französisch, Deutsch und Spanisch.

Für alle Eingabe- und Benennungskonventionen von OpenStack-Ressourcen (wie Projektnamen, Benutzernamen, Image-Namen usw.) und für die zugrunde liegenden Infrastrukturkomponenten (wie ESXi-Hostnamen, vSwitch-Portgruppennamen, Datencenter-Namen, Datenspeichernamen usw.) müssen ASCII-Zeichen verwendet werden.

OpenStack Foundation Compliance

Jede neue Version von VMware Integrated OpenStack entspricht den neuesten Richtlinien des OpenStack Foundation DefCore Committee.

Das Produkt VMware Integrated OpenStack fungiert als eine OpenStack-unterstützte Plattform™ und gewährt damit bewährte Interoperabilität mit allen anderen OpenStack-unterstützten™ Produkten.

Ausführliche Informationen zur Kompatibilität von VMware Integrated OpenStack mit der OpenStack-unterstützten Plattform™ finden Sie unter http://www.openstack.org/marketplace/distros/distribution/vmware/vmware-integrated-openstack.

VMware Integrated OpenStack -Systemanforderungen

Bevor Sie mit den VMware Integrated OpenStack-Bereitstellungsaufgaben beginnen, muss Ihr System alle Hardware-, Software-, Netzwerk- und Speicheranforderungen erfüllen.

Hardwareanforderungen für VMware Integrated OpenStack

Die Hardwareanforderungen basieren auf der Anzahl der für jede Komponente verwendeten VMs. Beispielsweise werden zwei VMs für den Lastausgleich verwendet, wobei jede VM zwei von den insgesamt vier erforderlichen CPUs benötigt. Die Anforderungen variieren abhängig davon, ob Ihre OpenStack-Bereitstellung Virtual Distributed Switch (VDS) oder VMware NSX for vSphere (NSX) mit der Komponente „Netzwerk“ verwendet.

VMware Integrated OpenStack -Hauptkomponenten

Komponente	VMs	CPU	RAM (GB)	Festplattenspeicher (GB)
Integrated OpenStack Manager	1	2 (2 pro VM)	4 (4 pro VM)	25
Lastausgleichsdienst	2	4 (2 pro VM)	8 (4 pro VM)	40 (20 pro VM)
Datenbankdienst	3	12 (4 pro VM)	48 (16 pro VM)	240 (80 pro VM)
Arbeitsspeicherdienst	2	4 (2 pro VM)	32 (16 pro VM)	40 (20 pro VM)
Nachrichtenwarteschlangen-Dienst	2	8 (4 pro VM)	32 (16 pro VM)	40 (20 pro VM)
Controller	2	16 (8 pro VM)	32 (16 pro VM)	160 (80 pro VM)
Computing-Dienst (Nova-CPU)	1	2 (2 pro VM)	4 (4 pro VM)	20 (20 pro VM)
DHCP-Dienst (nur VDS-Bereitstellungen)	2	8 (4 pro VM)	32 (16 pro VM)	40 (20 pro VM)
GESAMT	15	56	192	605

VMware Integrated OpenStack Anforderungen für den Kompaktmodus

VMware Integrated OpenStack 3.0 unterstützt einen neuen Bereitstellungsmodus: den Kompaktmodus, der mit sehr geringem Hardwareeinsatz ausgeführt werden kann. Weitere Informationen zu den Hardwareanforderungen für den Betrieb im Kompaktmodus finden Sie im *Installations- und Konfigurationshandbuch für VMware Integrated OpenStack*.

NSX -Komponenten

Für NSX-Komponenten sind mehr CPUs, Arbeitsspeicher und Festplattenspeicher erforderlich, wenn sie mit VMware Integrated OpenStack bereitgestellt werden.

Komponente	VMs	CPU	RAM	Festplattenspeicher
NSX Controller	3	12 (4 pro VM)	12 GB (4 pro VM)	60 GB (20 pro VM)
NSX Manager	1	4 (4 pro VM)	12 GB (12 pro VM)	60 GB (60 pro VM)

Komponente	VMs	CPU	RAM	Festplattenspeicher
NSX Edge (siehe Hinweis unten)	Variiert: erstellt nach Bedarf.	1 pro Edge-DHCP-VM 2 pro Edge-Router-VM	512 MB pro Edge-DHCP-VM 1 pro Edge-Router-VM	512 MB pro Edge-DHCP-VM 1 pro Edge-Router-VM
GESAMT	4 plus Edge-Anforderungen	16 plus Edge-Anforderungen	24 GB plus Edge-Anforderungen	120 GB plus Edge-Anforderungen

Wenn Sie ein logisches Subnetz oder einen logischen Router erstellen, wird eine neue Edge-VM dynamisch erstellt, um bei Ausfall eines vorhandenen Edge-Knotens auf diese Anforderung zu reagieren.

Softwareanforderungen für VMware Integrated OpenStack

Bevor Sie mit den VMware Integrated OpenStack-Bereitstellungsaufgaben beginnen, stellen Sie sicher, dass die Softwarekomponenten alle Versionsvoraussetzungen für vSphere, ESXi-Hosts und das NSX-Produkt erfüllen.

Anforderung	Beschreibung
vSphere-Version	■ vSphere 5.5 Update 2 Enterprise Plus ■ vSphere 6 Enterprise Plus
ESXi-Hosts	■ Version 5.5 Update 2 ■ Acht oder mehr logische Prozessoren auf jedem Host. ■ vCenter und alle ESXi-Hosts, die für die VMware Integrated OpenStack-Bereitstellung vorgesehen sind, müssen denselben Network Time Protocol (NTP)-Server verwenden. ■ Stellen Sie sicher, dass die ESXi-Host-Firewalls so konfiguriert sind, dass der Zugriff auf gdbserver zulässig ist. Normalerweise lautet der Portbereich 5900-5964.
NSX	Erkundigen Sie sich bei VMware nach der bevorzugten Version.

Speicheranforderungen für NSX -Bereitstellungen

Die Speicheranforderungen variieren abhängig von der Konfiguration Ihrer Bereitstellung. Datenspeicher können von verschiedenen Knoten und Clustern gemeinsam verwendet werden. Während des Installationsvorgangs können Sie zum Beispiel denselben Datenspeicher für die Computing- und Imagedienst-Knoten angeben.

Informationen zu Speicheranforderungen pro VM in einer typischen VMware Integrated OpenStack-Bereitstellung finden Sie unter „Hardwareanforderungen für VMware Integrated OpenStack“, auf Seite 12.

Speicheranforderungen variieren und richten sich danach, ob Sie die Bereitstellung auf einem NSX- oder VDS-Netzwerk durchführen.

Speicheranforderungen für NSX -Bereitstellungen

NSX Controller-, Manager- und Edge-Knoten wirken sich auf die Speicheranforderungen in einer NSX-Bereitstellung aus.

Cluster	Speicheranforderungen (GB)	Hinweise
Verwaltung	665	Die Berechnung der Speicheranforderung basiert auf den folgenden Knoten: ■ OpenStack Manager (1 Knoten) ■ Lastausgleichsdienste (2 Knoten) ■ Datenbank (3 Knoten) ■ Arbeitsspeicher (2 Knoten) ■ Nachrichtenwarteschlange (2 Knoten) ■ Controller (2 Knoten) ■ NSX Controller (3 Knoten) ■ NSX Manager (1 Knoten)
Computing	20	Wert ist pro Cluster. Jeder Computing-Cluster enthält einen einzelnen Computing-Knoten. Fügen Sie Cluster hinzu, um mehr Kapazität zu erzielen.
NSX Edge	1,5	Wert ist pro Knoten. Die Speicheranforderungen für den NSX Edge-Cluster variieren. Wenn Sie ein logisches Subnetz oder einen logischen Router erstellen, ein vorhandener NSX Edge-Knoten die Anforderung aber nicht erfüllen kann, wird ein zusätzlicher Knoten dynamisch erstellt. **Hinweis** Das Erstellen eines dedizierten Clusters für die NSX Edge-Knoten stellt eine optimale Vorgehensweise dar, um die Leistung zu optimieren. In einer alternativen Bereitstellung können Sie die NSX Edge-Knoten im Verwaltungs-Cluster einbeziehen.

Speicheranforderungen für VDS -Bereitstellungen

DHCP-Knoten wirken sich auf die Speicheranforderungen in einer VDS-Bereitstellung aus.

Cluster	Speicheranforderungen (GB)	Hinweise
Verwaltung	585	Die Berechnung der Speicheranforderung basiert auf den folgenden Dienstknoten: ■ OpenStack Manager (1 Knoten) ■ Lastausgleichsdienste (2 Knoten) ■ Datenbank (3 Knoten) ■ Arbeitsspeicher (2 Knoten) ■ Nachrichtenwarteschlange (2 Knoten) ■ Controller (2 Knoten) ■ DHCP-Controller (2 Knoten)
Computing	20	Wert ist pro Cluster. Jeder Computing-Cluster enthält einen einzelnen Computing-Knoten. Fügen Sie Cluster hinzu, um mehr Kapazität zu erzielen.

Erforderliche NSX -Parameter

Wenn Sie VMware Integrated OpenStack mit NSX für die Netzwerkkomponente bereitstellen, müssen Sie die NSX-Knoten im Voraus konfigurieren.

Wenn Sie VMware Integrated OpenStack installieren, müssen Sie die folgenden Informationen angeben.

Ab VMware Integrated OpenStack 3.1 können Sie bei Verwendung von VMware NSX-T in Ihrer Umgebung die native Unterstützung von DHCP und Metadaten benutzen. Für diese Funktionen müssen Sie ein DHCP-Profil und einen Metadaten-Proxyserver für Ihre NSX-T-Umgebung erstellen.

Eigenschaft	Beschreibung
Benutzername	Benutzername für den Zugriff auf den NSX Manager-Knoten.
Kennwort	Kennwort für den Zugriff auf den NSX Manager-Knoten.
Transportzone	Name der Standardtransportzone.
Edge-Cluster	Der Name des Clusters, der die Edge-Knoten enthält.
Virtual Distributed Switch für Edge-VTEP	Der VDS aus der NSX-Konfiguration.
Portgruppe für externes Netzwerk	Die in einem VLAN speziell für das externe Netzwerk erstellte Portgruppe. Sie haben diese Portgruppe als Teil des Prozesses erstellt, die Bereitstellung von VMware Integrated OpenStack mit NSX vorzubereiten.
(optional nur VMware NSX-T) DHCP-Profil	Für die Verwendung von nativem DHCP konfigurieren Sie ein DHCP-Serverprofil für Ihre NSX-T-Umgebung. Weitere Informationen finden Sie unter *Erstellen eines DHCP-Serverprofils* im *Administratorhandbuch für NSX-T*.
(optional nur VMware NSX-T) Metadaten-Proxyserver	Für die Verwendung der Metadatenunterstützung konfigurieren Sie einen Metadaten-Proxyserver für Ihre NSX-T-Umgebung. Weitere Informationen finden Sie unter *Hinzufügen eines Metadaten-Proxyservers* im *Administratorhandbuch für NSX-T*. Während der Konfiguration verwenden Sie die private ID des Lastausgleichsdiensts Ihrer OpenStack-Bereitstellung als URL für den Nova-Server. Beispiel: *http://load_balancer_private_IP:8775/*. Behalten Sie außerdem den Parameter für den geheimen Schlüssel bei, da Sie ihn während der Bereitstellung von VMware Integrated OpenStack benötigen.

OpenStack-Instanzen in vSphere Web Client

Die in Ihrer VMware Integrated OpenStack-Bereitstellung erstellten VMs werden in Ihrer vCenter-Bestandsliste angezeigt. Viele Beschränkungen beziehen sich darauf, wie Sie mit OpenStack-VMs arbeiten und diese verwalten.

In den meisten Fällen müssen Sie diese VMs nicht im vSphere Web Client, sondern im OpenStack-Dashboard oder an der Befehlszeilenschnittstelle verwalten.

In vSphere unterstützte OpenStack-Funktionen

vSphere unterstützt bestimmte OpenStack-Funktionen.

OpenStack-Funktion	Unterstützt in vSphere
Starten	JA
Neu starten	JA
Beenden	JA
Größe ändern	JA
Sichern	JA
Pausieren	NEIN
Fortsetzen	NEIN
Anhalten	JA
Fortsetzen	JA
Netzwerk einfügen „Netzwerk einfügen“ wird nur unterstützt, wenn die folgenden Bedingungen zutreffen: ■ Mit Nova-Netzwerk im Flat-Modus ■ Mit Debian- oder Ubuntu-basierten virtuellen Maschinen ■ Zur Startzeit	JA

OpenStack-Funktion	Unterstützt in vSphere
Datei einfügen	NEIN
Ausgabe der seriellen Konsole	JA
RDP-Konsole	NEIN
Datenträger anfügen	JA
Datenträger trennen	JA
Live-Migration	JA
Snapshot	JA
iSCSI	JA
Fibre Channel	JA Über vSphere-Datenspeicher unterstützt
Administratorkennwort festlegen	NEIN
Gastinformationen abrufen	JA
Hostinformationen festlegen	JA
Glance-Integration	JA
Dienststeuerung	JA
VLAN-Netzwerk	JA
Flat-Netzwerk	JA
Sicherheitsgruppen	NEIN vSphere Web Client unterstützt Sicherheitsgruppen, wenn das Neutron-Plug-In von VMware NSX for vSphere verwendet wird.
Firewallregeln	NEIN
Routing	JA
Laufwerk konfigurieren	JA
Entfernen oder Host-Wartungsmodus	JA
Datenträgertausch	NEIN
Begrenzung der Datenträgerrate	NEIN

VM-Vorgänge in OpenStack

In der folgenden Tabelle werden VMware Integrated OpenStack- und vSphere-VM-Vorgänge dargestellt. Zudem finden Sie in dieser Tabelle Empfehlungen zur optimalen Durchführung der jeweiligen Vorgänge. Wenn Sie eine VM in VMware Integrated OpenStack erstellen, verwalten Sie diese VM in VMware Integrated OpenStack.

vSphere-Funktion	OpenStack-Gegenstück	Über OpenStack-API offen gelegt	Wo wird dieser Vorgang durchgeführt
Virtuelle Maschine erstellen	Instanz starten	JA	OpenStack-Dashboard
Neu starten	Neu starten	JA	OpenStack-Dashboard oder vSphere Web Client
Löschen	Beenden	JA	OpenStack-Dashboard
Größe ändern	Größe ändern	JA	OpenStack-Dashboard
Pausieren	Pausieren	JA	OpenStack-Dashboard oder vSphere Web Client

vSphere-Funktion	OpenStack-Gegenstück	Über OpenStack-API offen gelegt	Wo wird dieser Vorgang durchgeführt
Fortsetzen	Fortsetzen	JA	OpenStack oder vSphere Web Client
Pausieren	Anhalten	JA	OpenStack-Dashboard
Fortsetzen	Fortsetzen	JA	OpenStack-Dashboard
Ausgabe der seriellen Konsole	Ausgabe der seriellen Konsole	JA	OpenStack-Dashboard oder vSphere Web Client
RDP-Konsole	RDP-Konsole		OpenStack-Dashboard oder vSphere Web Client
Festplatte hinzufügen	Datenträger anfügen	JA	OpenStack-Dashboard
Festplatte entfernen	Datenträger trennen	JA	OpenStack-Dashboard
vMotion	Live-Migration	JA	vSphere Web Client Da OpenStack kein Clusterkonzept aufweist, kann das Migrieren von VMs über OpenStack zu Unterbrechungen führen. Führen Sie VM-Migrationen daher unter Verwendung von vMotion aus.
Snapshot	Snapshot	JA	OpenStack-Dashboard oder vSphere Web Client
Über VMware Tools verfügbare Funktionen.	Gastinformationen abrufen/Hostinformationen abrufen	JA	OpenStack-Dashboard oder vSphere Web Client Für vSphere Web Client ist diese Funktion mit VMware Tools verfügbar.
Verteilte Portgruppen	VLAN-Netzwerk oder Flat-Netzwerk	JA	OpenStack-Dashboard
Über VMware Tools verfügbare Funktion.	Laufwerk konfigurieren	NEIN	OpenStack-Dashboard oder vSphere Web Client Für vSphere Web Client ist diese Funktion mit VMware Tools verfügbar.
VMware Tools in einer VM installieren	VMware Tools in einer VM installieren	NEIN	OpenStack-Dashboard oder vSphere Web Client

Nicht in der OpenStack-API unterstützte vCenter -Funktionen

Zwischen den OpenStack-Funktionen und den vSphere-Funktionen besteht keine direkte Parität. Die OpenStack-API unterstützt die folgenden vCenter-Funktionen nicht.

- Hinzufügen eines Hosts zu einem Cluster

  OpenStack kann in vSphere einem Cluster keinen Host hinzufügen.

- Versetzen eines Hosts in den Wartungsmodus

  Sie versetzen einen Host in den Wartungsmodus, wenn Sie Wartungstätigkeiten ausführen, beispielsweise wenn Sie zusätzlichen Arbeitsspeicher installieren. Ein Host wird in den Wartungsmodus nur auf Benutzeranforderung versetzt bzw. verlässt diesen nur dann. In OpenStack ist diese Funktion nicht vorhanden. Anweisungen zum Wechseln in den Wartungsmodus und zum Verlassen des Wartungsmodus finden Sie in der vSphere-Dokumentation.

- Ressourcenpools

Ein Ressourcenpool in vSphere ist eine logische Abstraktion für die flexible Verwaltung von Ressourcen, wie zum Beispiel CPU und Arbeitsspeicher. OpenStack weist keine entsprechende Funktion auf.

- vSphere-Snapshots

  vCenter unterstützt OpenStack-Snapshots. vSphere-Snapshots sind jedoch eindeutig identifizierbar und werden in der OpenStack-API nicht unterstützt.

Überwachen von OpenStack-Instanzen im vSphere Web Client

Sie können die Instanzaktivität und die Metadaten im vSphere Web Client anzeigen und überwachen.

Voraussetzungen

Stellen Sie sicher, dass VMware Integrated OpenStack bereitgestellt und betriebsbereit ist.

Stellen Sie sicher, dass die Instanzen in VMware Integrated OpenStack von Ihnen oder einem anderen Benutzer gestartet wurden.

Vorgehensweise

1. Wählen Sie im vSphere Web Client die Option **Home > Bestandslisten** aus und klicken Sie auf das Symbol VMware Integrated OpenStack.
2. Erweitern Sie die Ansicht „Bestandsliste“ so, dass die Instanz-VMs im Computing-Cluster sichtbar sind.

   Die Instanz-VMs sind durch Ihre UUIDs gekennzeichnet.
3. Wählen Sie eine Instanz-VM aus und klicken Sie auf die Registerkarte **Übersicht**.

   Auf der Registerkarte **Übersicht** werden die Portlets für die VMs im vSphere Web Client angezeigt. Die Portlets „VM“ und „Tags“ von OpenStack enthalten Details zu den in OpenStack erstellten Instanzen.
4. (Optional) Suchen und überprüfen Sie die Portlets „VM“ und „Tags“ von OpenStack.

   Diese Portlets zeigen Informationen zur ausgewählten Instanz an, einschließlich Instanzeigenschaften wie Name, Mandant, Benutzer, der die Instanz erstellt hat, ursprünglicher Typ usw.
5. (Optional) Verwenden Sie den vSphere Web Client, um OpenStack-Instanzen zu suchen und zu filtern.
   a. Geben Sie im vSphere Web Client-Suchfeld einen der Tag-Werte aus dem Portlet „Tags“ ein.

      Geben Sie zum Beispiel `m1.tiny` für die Suche nach allen Instanzen ein, die mit dem Standardtyp m1.tiny erstellt wurden.

      Die Registerkarte **Verwandte Objekte** wird mit einer Liste aller OpenStack-Instanzen angezeigt, die diesem Suchkriterium entsprechen.

   b. Klicken Sie auf den Namen einer beliebigen Instanz, um die Registerkarte **Übersicht** für diese Instanz zu öffnen.

Programm zur Verbesserung der Benutzerfreundlichkeit

Sie können das Produkt so konfigurieren, dass Daten erfasst werden, die das Programm zur Verbesserung der Benutzerfreundlichkeit von VMware verwenden kann.

Dieses Produkt nimmt am Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) von VMware teil. Einzelheiten zu den im Rahmen des CEIP erfassten Daten sowie zum Zweck der Verwendung durch VMware können im Trust & Assurance Center unter http://www.vmware.com/trustvmware/ceip.html eingesehen werden.

Um dem CEIP für dieses Produkt beizutreten oder es zu verlassen, navigieren Sie in der Benutzeroberfläche zur Seite des Programms zur Verbesserung der Benutzerfreundlichkeit, um Ihre Teilnahme am CEIP zu ändern:

- Während der Produktbereitstellung mit dem Integrated OpenStack Manager ist die Teilnahme am CEIP standardmäßig aktiviert, es sei denn, Sie entschließen sich, nicht daran teilzunehmen.

Navigieren Sie nach der anfänglichen Bereitstellung zur Seite des Programms zur Verbesserung der Benutzerfreundlichkeit, um ggf. Ihre Teilnahme zu ändern.

- Um am CEIP teilzunehmen, navigieren Sie zu **Startseite > Bestandslisten** und klicken Sie auf das Symbol VMware Integrated OpenStack. Klicken Sie auf die Registerkarte **Verwalten** und dann auf die Registerkarte **Einstellungen**. Klicken Sie anschließend auf **Aktivieren**, um am CEIP teilzunehmen.
- Um das CEIP zu verlassen, navigieren Sie zu **Startseite > Bestandslisten** und klicken Sie auf das Symbol VMware Integrated OpenStack. Klicken Sie auf die Registerkarte **Verwalten** und dann auf die Registerkarte **Einstellungen**. Klicken Sie anschließend auf **Deaktivieren**, um das Programm zu verlassen.

Verwalten Ihrer VMware Integrated OpenStack - Bereitstellung

2

Die Verwaltung Ihrer VMware Integrated OpenStack-Bereitstellung umfasst das Ändern von Konfigurationseinstellungen, das Sichern und Wiederherstellen Ihrer OpenStack-Konfiguration und -Daten, das Verwenden von Patches für kleinere Updates sowie das Ausführen von Upgrades auf neuere Versionen.

Dieses Kapitel behandelt die folgenden Themen:

Verwalten Ihrer Bereitstellungskonfiguration

Während des Installations- und Bereitstellungsvorgangs für VMware Integrated OpenStack führen Sie u. a. folgende Aufgaben durch: Konfigurieren der OpenStack-Komponenten, Angabe des Syslog-Servers, Eingabe der Kennwörter für LDAP, NSX und vCenter Server. Nach der Bereitstellung können Sie diese Einstellungen ändern.

Überwachen Ihrer VMware Integrated OpenStack -Bereitstellung

Nach Abschluss der Installation von VMware Integrated OpenStack können Sie die Konfiguration Ihrer Bereitstellung überwachen, einschließlich Datenspeichergrößen, Netzwerkeinstellungen, Metadatendienst usw.

Vorgehensweise

1 Wählen Sie in vCenter die Option **Startseite > VMware Integrated OpenStack** aus.

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

Ändern der Adresse des Syslog-Servers

Die Adresse des Syslog-Servers wird während der Installation konfiguriert, aber Sie können die Konfiguration danach ändern.

Voraussetzungen

Stellen Sie sicher, dass die neue Adresse des Syslog-Servers gültig ist.

Vorgehensweise

1 Wählen Sie in vCenter die Option **Home > VMware Integrated OpenStack > Verwalten** aus.

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

3 Klicken Sie auf **Syslog-Server**.

Im Bereich „Syslog-Server“ wird die aktuelle Konfiguration angezeigt.

4 Klicken Sie auf **Bearbeiten**, um die Adresse des Syslog-Servers zu ändern.

5 Klicken Sie auf **OK**, damit die Änderung wirksam wird.

Es kann einige Minuten dauern, bis der vSphere Web Client die OpenStack-Konfiguration aktualisiert hat.

Aktualisieren von Bereitstellungskennwörtern

Ein Teil der Konfiguration Ihrer VMware Integrated OpenStack-Bereitstellung umfasst Kennwörter, mit denen OpenStack auf Ihren LDAP-Server, NSX, und vCenter Server zugreifen und damit eine Verbindung herstellen kann. Wenn die Anmeldedaten geändert werden, können Sie die Kennworteinstellungen direkt im VMware Integrated OpenStack Manager ändern, um den fortlaufenden Zugriff zu gewährleisten.

Auf der Seite „Kennwort ändern“ werden nur die Textfelder mit den aktualisierten Kennwörtern geändert. Wenn Sie bei einem Kennwort keine Änderung durchführen möchten, lassen Sie das Textfeld leer.

Voraussetzungen

Stellen Sie sicher, dass die angegebenen Kennwörter im Bereich „Kennwörter ändern“ mit den Kennwörtern übereinstimmen, die jeweils für den LDAP-Server, NSX oder vCenter Server konfiguriert wurden.

Vorgehensweise

1 Wählen Sie in vCenter die Option **Home > VMware Integrated OpenStack > Verwalten** aus.

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

3 Klicken Sie auf **Kennwort ändern**.

Der Bereich „Kennwörter ändern“ enthält Textfelder für das Aktualisieren der aktuellen Kennwortkonfigurationen für den LDAP-Server, NSX und vCenter Server.

4 Geben Sie das neue Kennwort ein.

5 Klicken Sie auf **Übernehmen**.

Die Kennworteinstellungen in VMware Integrated OpenStack werden anhand der neuen Werte aktualisiert.

Manage the OpenStack SSL Certificate Configuration

You can add OpenStack SSL certificates in the VMware Integrated OpenStack manager.

You can only import existing CA signed certificates, created from CSRs generated by VMware Integrated OpenStack. You can also create new CSRs to create new CA signed certificates. Using wildcard certificates is not supported.

Procedure

1 In the vSphere Web Client, select **Home > Inventories**, and click the VMware Integrated OpenStack icon.

2 Click the **Manage** tab and click the **Settings** tab.

3 Click **OpenStack SSL Certificate**.

4 Generate a new certificate signing request to create new CA signed certificate.

   a Provide the Organizational Unit, Organizational Name, Locality Name, State Name, and Country Code information as appropriate to your organization.

   b Click **Generate**.

   c Use the generated certificate signing request to create a certificate that is signed by your CA.

5 Import the CA signed certificate.

   a Click **Import**.

   b Browse to and select the CA signed certificate file.

   c Click **OK**.

   The imported certificate is applied.

Konfigurieren der Ceilometer-Komponente

Ceilometer ist die Telemetrie-Komponente von OpenStack, die Daten im Hinblick auf die Nutzung der physischen und virtuellen Ressourcen in Ihrer OpenStack-Bereitstellung sammelt und speichert.

Sie können Ceilometer nach Abschluss der VMware Integrated OpenStack-Bereitstellung aktivieren.

Vorgehensweise

1 Wählen Sie in vCenter die Option **Home > VMware Integrated OpenStack > Verwalten** aus.

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

3 Klicken Sie auf **Ceilometer**.

   Im Fensterbereich „Ceilometer“ werden der aktuelle Status und die Konfiguration angezeigt.

4 Klicken Sie auf **Bearbeiten**, um die Einstellungen zu ändern.

5 Wählen Sie die Option **Ceilometer konfigurieren**.

6 Klicken Sie auf **OK**, um Ceilometer zu konfigurieren.

   Es kann einige Minuten dauern, bis der vSphere Web Client die OpenStack-Konfiguration aktualisiert hat.

Ceilometer wird bei der ersten Konfiguration automatisch aktiviert. Danach zeigen die Ceilometer-Einstellungen nur die Optionen **Aktivieren** und **Deaktivieren** an.

Änderung der Registrierung beim Programm zur Verbesserung der Benutzerfreundlichkeit

Während des Installationsvorgangs können Sie sich beim Programm zur Verbesserung der Benutzerfreundlichkeit von VMware (CEIP, Customer Experience Improvement Program) anmelden. Nach der Installation können Sie diese Konfiguration im VMware Integrated OpenStack Manager ändern.

Dieses Produkt nimmt am Programm zur Verbesserung der Benutzerfreundlichkeit (CEIP) von VMware teil. Einzelheiten zu den im Rahmen des CEIP erfassten Daten sowie zum Zweck der Verwendung durch VMware können im Trust & Assurance Center unter http://www.vmware.com/trustvmware/ceip.html eingesehen werden.

Vorgehensweise

1 Um am CEIP teilzunehmen, navigieren Sie zu **Startseite > Bestandslisten** und klicken Sie auf das Symbol VMware Integrated OpenStack. Klicken Sie auf die Registerkarte **Verwalten** und dann auf die Registerkarte **Einstellungen**. Klicken Sie anschließend auf **Aktivieren**, um am CEIP teilzunehmen.

2 Um das CEIP zu verlassen, navigieren Sie zu **Startseite > Bestandslisten** und klicken Sie auf das Symbol VMware Integrated OpenStack. Klicken Sie auf die Registerkarte **Verwalten** und dann auf die Registerkarte **Einstellungen**. Klicken Sie anschließend auf **Deaktivieren**, um das Programm zu verlassen.

3 Klicken Sie auf **Programm zur Verbesserung der Benutzerfreundlichkeit**.

Auf der Seite des Programms zur Verbesserung der Benutzerfreundlichkeit wird der aktuelle Status Ihrer Teilnahme am CEIP angezeigt. Ist er aktiviert, nehmen Sie teil. Ist er deaktiviert, nehmen Sie nicht teil.

Verwalten Ihrer Authentifizierungseinstellungen

Ein Teil Ihrer VMware Integrated OpenStack-Bereitstellungskonfiguration umfasst das Einrichten der Authentifizierung. Diese Konfiguration können Sie auch nach der Installation ändern.

Voraussetzungen

Vergewissern Sie sich, dass die neuen LDAP-Einstellungen gültig sind.

Vorgehensweise

1 Wählen Sie in vCenter die Option **Home > VMware Integrated OpenStack > Verwalten** aus.

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

3 Klicken Sie auf **Identitätsquelle konfigurieren**.

Im Fensterbereich wird die aktuelle Konfiguration angezeigt.

4 Legen Sie die VMware Integrated OpenStack-Identitätsquelle fest.

Option	Beschreibung
OpenStack-Administrator	Definieren Sie den Namen für den OpenStack-Administrator. Dies ist der Standardname des Administrators für die Anmeldung beim VMware Integrated OpenStack-Dashboard.
Kennwort des OpenStack-Administrators	Definieren Sie das Kennwort für den OpenStack-Administrator. Dies ist das Standardkennwort des Administrators für die Anmeldung beim VMware Integrated OpenStack-Dashboard.
Kennwort bestätigen	Geben Sie das Kennwort zur Bestätigung erneut ein.

5 Wenn Sie LDAP für Ihre VMware Integrated OpenStack-Bereitstellung verwenden, klicken Sie auf das Pluszeichen (+), um die LDAP-Quelle zu konfigurieren.

Das Dialogfeld „Identitätsquelle hinzufügen“ wird angezeigt.

Option	Beschreibung
Domänenname	Geben Sie den vollständigen Active Directory-Domänennamen an, z. B. vmware.com.
Bind-Benutzer	Geben Sie den Benutzernamen an, um ihn für LDAP-Anforderungen an Active Directory zu binden.
Bind-Kennwort	Geben Sie das Kennwort an, um dem LDAP-Client Zugriff auf den LDAP-Server zu gewähren.
Domänen-Controller	(Optional) VMware Integrated OpenStack wählt automatisch die vorhandenen Active Directory-Domänen-Controller. Sie können jedoch eine Liste mit bestimmten Domänen-Controllern angeben, die verwendet werden sollen. Wählen Sie hierfür die Optionsschaltfläche **Domänen-Controller** aus und geben Sie die IP-Adresse eines oder mehrerer Domänen-Controller ein (durch Kommas getrennt).
Site	(Optional) Optional können Sie die LDAP-Suche auf einen bestimmten Bereitstellungsort in Ihrem Unternehmen begrenzen, z. B. auf sales.vmware.com. Wählen Sie die Optionsschaltfläche **Site** aus und geben Sie den Domänennamen des Ortes ein, an dem gesucht werden soll.
DN der Benutzerstruktur	(Optional) Geben Sie die Basis zum Suchen nach Benutzern ein, z. B. DC=vmware, DC=com. In den meisten Active Directory-Bereitstellungen wird standardmäßig die oberste Ebene der Benutzerstruktur verwendet.
Benutzerfilter	(Optional) Geben Sie einen LDAP-Suchfilter für Benutzer ein. **Wichtig** Wenn Sie VMware Integrated OpenStack 3.0 oder älter verwenden und Ihr Verzeichnis mehr als 1000 Objekte (Benutzer und Gruppen) enthält, müssen Sie einen Filter anwenden, um sicherzustellen, dass weniger als 1000 Objekte zurückgegeben werden. Beispiele von Filtern finden Sie unter https://msdn.microsoft.com/en-us/library/aa746475(v=vs.85).aspx.
Erweiterte Einstellung	Wenn Sie erweiterte LDAP-Einstellungen vornehmen möchten, aktivieren Sie das Kontrollkästchen **Erweiterte Einstellung**.

Wenn Sie das Kontrollkästchen **Erweiterte Einstellung** aktivieren, werden zusätzliche Felder für die LDAP-Konfiguration angezeigt.

Hinweis Wenden Sie sich immer an den LDAP-Administrator, um die korrekten Werte für erweiterte LDAP-Einstellungen zu erhalten, oder verwenden Sie Tools wie ldapsearch oder Apache Directory Studio, um die Einstellungen aufzurufen.

Option	Beschreibung
Verschlüsselung	Wählen Sie im Dropdown-Menü **Keine**, **SSL** oder **StartTLS** aus.
Hostname	Geben Sie den Hostnamen für den LDAP-Server ein.
Port	Geben Sie die Portnummer für Benutzer auf dem LDAP-Server ein.
Benutzerobjektklasse	(Optional) Geben Sie die LDAP-Objektklasse für Benutzer ein.
Attribut der Benutzer-ID	(Optional) Geben Sie das LDAP-Attribut ein, das der Benutzer-ID zugewiesen ist. Beachten Sie, dass dieser Wert kein Attribut mit mehreren Werten sein darf.
Attribut des Benutzernamens	(Optional) Geben Sie das LDAP-Attribut ein, das dem Benutzernamen zugewiesen ist.
Attribut der Benutzer-E-Mail	(Optional) Geben Sie das LDAP-Attribut ein, das der Benutzer-E-Mail-Adresse zugewiesen ist.
Attribut des Benutzerkennworts	(Optional) Geben Sie das LDAP-Attribut ein, das dem Kennwort zugewiesen ist.
Gruppenobjektklasse	(Optional) Geben Sie eine LDAP-Objektklasse für Gruppen ein.

Option	Beschreibung
Attribut der Gruppen-ID	(Optional) Geben Sie das LDAP-Attribut ein, das der Gruppen-ID zugewiesen ist.
Attribut des Gruppennamens	(Optional) Geben Sie das LDAP-Attribut ein, das dem Gruppennamen zugewiesen ist.
Attribut der Gruppenmitglieder	(Optional) Geben Sie das LDAP-Attribut ein, das dem Namen des Gruppenmitglieds zugewiesen ist.
Attribut der Gruppenbeschreibung	(Optional) Geben Sie das LDAP-Attribut ein, das der Gruppenbeschreibung zugewiesen ist.

Abbildung 2-1. Dialogfeld „Identitätsquelle hinzufügen“

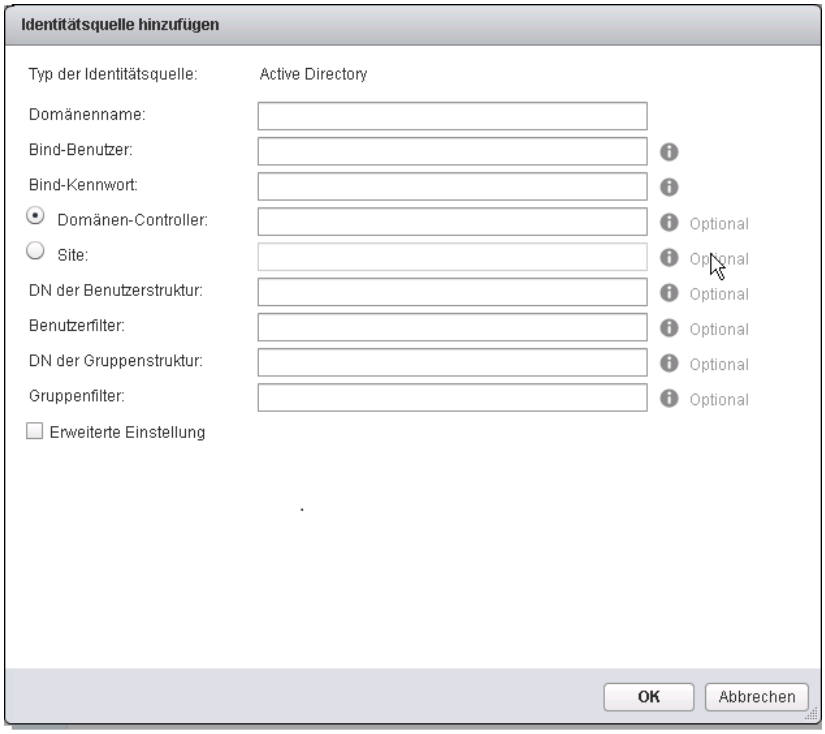
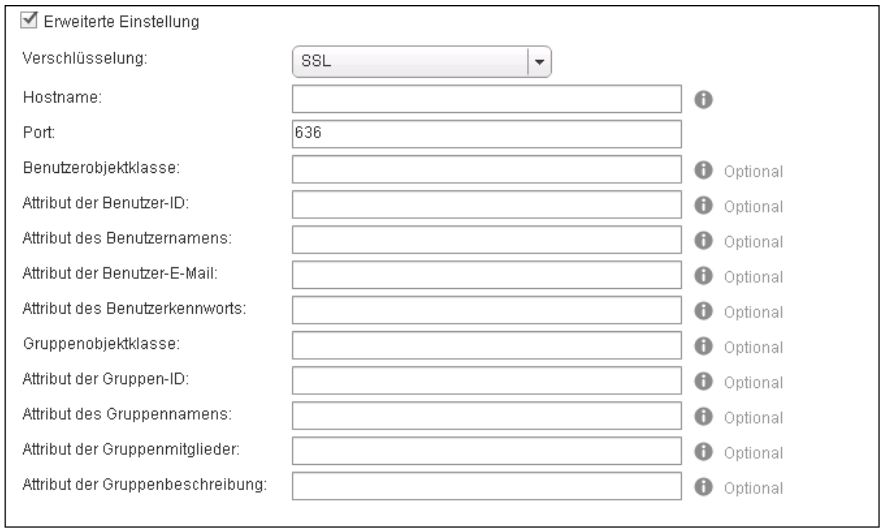


Abbildung 2-2. Erweiterte LDAP-Einstellungen



6 Klicken Sie auf **Speichern**.

Weiter

Für die LDAP-Konfiguration müssen Sie die Standardkonfiguration der OpenStack-Domäne manuell ändern. Siehe „Ändern der Standarddomänenkonfiguration“, auf Seite 27.

Ändern der Standarddomänenkonfiguration

Die Identitätsdienstkomponente (Keystone) gibt keine Benutzer und Gruppen an die Standarddomäne zurück. Mit dem folgenden Verfahren wird die Standardkonfiguration geändert, um sicherzustellen, dass Benutzer mit Administratorrechten auf LDAP-Benutzer zugreifen und sie Rollen in OpenStack zuweisen können.

Voraussetzungen

- Vergewissern Sie sich, dass VMware Integrated OpenStack erfolgreich bereitgestellt wurde.
- Stellen Sie sicher, dass VMware Integrated OpenStack ausgeführt wird.
- Vergewissern Sie sich, dass Active Directory als LDAP-Back-End konfiguriert ist.

Vorgehensweise

1 Melden Sie sich unter Verwendung von SSH bei der VMware Integrated OpenStack-Bereitstellung an.

Dieser Schritt hängt von Ihrem Bereitstellungsmodus ab.

- Wenn Ihre Bereitstellung den Kompaktmodus verwendet, melden Sie sich beim Controller-Knoten an.
- Wenn Ihre Bereitstellung den Hochverfügbarkeitsmodus verwendet, melden Sie sich beim Lastausgleichsdienstknoten an.

2 Wechseln Sie zum Root-Benutzer.

```
sudo su -
```

3 Führen Sie die Datei `cloudadmin_v3.rc` aus.

```
$ source ~/cloudadmin_v3.rc
```

4 Erstellen Sie das anfängliche Projekt in der Standarddomäne in OpenStack.

```
$ openstack --os-identity-api-version 3 --os-username admin \
      --os-user-domain-name local --os-project-name admin --os-password admin \
      --os-region-name nova project create --domain default --description "Demo Project" --
or-show demo
```

Parameter	Beschreibung
`--os-identity-api-version 3`	Gibt die API-Version an, in diesem Fall die Version **3**.
`--os-username admin`	Gibt den Administratorbenutzernamen für die Anmeldung an, in diesem Fall **`admin`**.
`--os-user-domain-name local`	Gibt die Domäne für den angegebenen Benutzer an, in diesem Fall **`local`**.
`--os-project-name admin`	Gibt das OpenStack-Projekt „admin“ an.
`--os-password admin`	Gibt das Administratorkennwort für die Anmeldung an, in diesem Fall **`admin`**.
`--os-region-name nova project create`	Führt den Befehl `nova project create` aus.
`--domain default`	Dieser Befehl gibt die Domäne an, in der das neue Projekt erstellt wird, in diesem Fall die Domäne **`default`**.

Parameter	Beschreibung
`--description "Demo Project"`	Mit diesem Parameter wird das neue Projekt benannt, in diesem Fall **`Demo Project`**.
`--or-show demo`	Erstellt einen Alias für das neue Projekt.

5 Fügen Sie dem neuen Projekt in der Standarddomäne einen Administratorbenutzer hinzu.

```
$ openstack --os-identity-api-version 3 --os-username admin \
      --os-user-domain-name local --os-project-name admin --os-password admin \
      --os-region-name nova role add --project demo --project-domain default \
      --user SOMEUSER@vmware.com --user-domain default admin
```

Parameter	Beschreibung
`--os-identity-api-version 3`	Gibt die API-Version an, in diesem Fall die Version **`3`**.
`--os-username admin`	Gibt den Administratorbenutzernamen für die Anmeldung an, in diesem Fall **`admin`**.
`--os-user-domain-name local`	Gibt die Domäne für den angegebenen Benutzer an, in diesem Fall **`local`**.
`--os-project-name admin`	Gibt das OpenStack-Projekt „admin“ an.
`--os-password admin`	Gibt das Administratorkennwort für die Anmeldung an, in diesem Fall **`admin`**.
`--os-region-name nova role add`	Führt den Befehl `nova role add` aus.
`--project demo`	Gibt das Projekt an, dem der neue Administratorbenutzer hinzugefügt wird.
`--project-domain default`	Gibt die Projektdomäne an.
`--user SOMEUSER@vmware.com`	Gibt den neuen Administratorbenutzer an.
`--user-domain default admin`	Weist den neuen Benutzer der Domäne „default admin“ zu.

Hinweis Wenn Sonderzeichen für die Benutzer-ID verwendet werden, müssen Sie die Keystone-Einstellungen im VMware Integrated OpenStack-Manager ändern.

6 (Optional) Wenn Sonderzeichen für die Administratorbenutzer-ID verwendet werden, müssen Sie die Keystone-Einstellungen im VMware Integrated OpenStack-Manager ändern.

a Wechseln Sie im VMware Integrated OpenStack-Manager in vCenter zu **Verwalten > Einstellungen > Identitätsquelle konfigurieren**.

b Klicken Sie auf **Bearbeiten**.

c Ändern Sie unter „Erweiterte Einstellungen“ den Wert für die Benutzer-ID von **`cn`** in **`userPrincipalName`**.

Nun können Sie sich im VMware Integrated OpenStack-Dashboard mithilfe des Administratorbenutzernamens und -kennworts bei der Standarddomäne anmelden.

Konfigurieren von VMware Identity Manager als Single Sign-On-Lösung für OpenStack

Ab VMware Integrated OpenStack 3.1 können Sie Ihre VMware Integrated OpenStack-Bereitstellungen mit VMware Identity Manager integrieren.

Durch die Integration von VMware Integrated OpenStack mit VMware Identity Manager können Sie mithilfe vorhandener Anmeldedaten auf sichere Weise auf Cloud-Ressourcen wie etwa Server, Volumes und Datenbanken auf verschiedenen Endpoints in mehreren autorisierten Clouds zugreifen. Sie verfügen über einen einzelnen Satz von Anmeldedaten und müssen nicht zusätzliche Identitäten bereitstellen oder mehrere Anmeldungen vornehmen. Die Anmeldedaten werden vom Identitätsanbieter des Benutzers verwaltet.

Voraussetzungen

- Stellen Sie sicher, dass VMware Identity Manager die Version 2.8.0 oder höher aufweist.
- Vergewissern Sie sich, dass Sie sich bei der VMware Identity Manager-Instanz als Administrator authentifizieren können.

Vorgehensweise

1 Implementieren Sie die Datei `custom.yml`.

```
sudo mkdir –p /opt/vmware/vio/custom
sudo cp /var/lib/vio/ansible/custom/custom.yml.sample /opt/vmware/vio/custom/custom.yml
```

2 Bearbeiten Sie die Datei `/opt/vmware/vio/custom/custom.yml` in einem Texteditor, um sie für Ihre Umgebung zu konfigurieren.

a Heben Sie unter `Federation` die Auskommentierung der folgenden Parameter auf und legen Sie Werte für Ihre Umgebung fest.

Das folgende Beispiel veranschaulicht die gängigste Konfiguration mit VMware Identity Manager.

Parameter	Wert
federation_protocol	saml2
federation_idp_id	vidm
federation_idp_name	vIDM SSO
federation_idp_metadata_url	https://*IDP_HOSTNAME*/SAAS/API/1.0/GET/metadata/idp.xml
federation_group	Verbundbenutzer
federation_group_description	Gruppen für alle Verbundbenutzer
vidm_address	*IDP_URL*
vidm_user	*vidm_administrative_user*
vidm_password	*vidm_administrative_user_password*
vidm_insecure	False
vidm_group	ALL USERS

b Speichern Sie die Datei `custom.yml`.

3 Aktivieren Sie die Verbundfunktion mit den Einstellungen, die Sie in der Datei `custom.yml` konfiguriert haben.

```
viocli deployment configure ––tags federation ––limit controller,lb
```

Nachdem der Integrationsvorgang erfolgreich abgeschlossen wurde, wird im VMware Integrated OpenStack-Dashboard das neue Dropdown-Menü **Authentifizieren mit** angezeigt, über das der Benutzer die Authentifizierungsmethode auswählen kann.

4 Bevor ein Benutzer von VMware Identity Manager sich bei VMware Integrated OpenStack anmelden kann, weisen Sie der Gruppe, zu der dieser Benutzer gehört, eine Rolle bzw. ein Projekt zu.

   Möglicherweise müssen Sie in Keystone eine Gruppe erstellen, die einer in VMware Identity Manager vorhandenen Gruppe entspricht, zu der ein Benutzer gehört. Für Benutzer von VMware Identity Manager erstellt Keystone nicht automatisch Gruppen, sondern flüchtige Benutzer. Wenn die Gruppe nicht vorhanden ist, wird der Benutzer Mitglied der Standardgruppe `Federated Users`.

   a Melden Sie sich beim VMware Integrated OpenStack-Dashboard als Administrator an.

   b Klicken Sie unter „Verbund“ auf **Zuordnungen**, um die aktuellen Zuordnungen anzuzeigen.

   c Klicken Sie auf „Bearbeiten“, um eine Zuordnung entsprechend Ihren Bedürfnissen zu konfigurieren.

      Weitere Informationen zu Zuordnungen finden Sie unter Mapping Combinations for Federation (Zuordnungskombinationen für den Verbund) in der OpenStack-Dokumentation.

Verwalten Ihrer Netzwerkkonfiguration

Während der Installation konfigurieren Sie die Neutron-Netzwerkkomponente durch die Angabe von Portgruppen. Nach der Installation können Sie den IP-Bereich erweitern, eine L2-Bridge erstellen oder den DNS der dedizierten Netzwerke ändern.

Hinzufügen von IP-Adressbereichen zu einem Netzwerk

Sie können IP-Adressbereiche zum Verwaltungs- oder API-Zugriff-Netzwerk hinzufügen.

Sie fügen IP-Bereiche üblicherweise als Teil eines Upgrade-Vorgangs hinzu.

Vorgehensweise

1 Wählen Sie im vSphere Web Client die Option **Home > Bestandslisten** aus und klicken Sie auf das Symbol VMware Integrated OpenStack.

2 Klicken Sie auf die Registerkarte **Verwalten** und dann auf die Registerkarte **Netzwerke**.

   Auf der Registerkarte **Netzwerk** werden die Verwaltungs- und API-Netzwerkkonfigurationen einschließlich ihrer IP-Adressbereiche aufgelistet.

3 Erweitern Sie die für das Verwaltungsnetzwerk verfügbaren IP-Adressen.

   a Klicken Sie mit der rechten Maustaste auf den Namen des Verwaltungsnetzwerks in der Liste und wählen Sie **IP-Bereich hinzufügen** aus.

   b Geben Sie den neuen IP-Bereich im Dialogfeld „IP-Bereich hinzufügen“ ein.

      Hinweis Wenn Sie Adressen im Rahmen des Upgrade-Vorgangs hinzufügen, muss der neue IP-Bereich exakt mit der Anzahl von IP-Adressen übereinstimmen, die für das vorhandene Verwaltungsnetzwerk konfiguriert sind. In einer typischen VMware Integrated OpenStack-Bereitstellung erfordert das Verwaltungsnetzwerk beispielsweise einen Mindestbereich von 11 IP-Adressen.

   c Klicken Sie auf **OK**.

4 Erweitern Sie die für das externe Netzwerk verfügbaren IP-Adressen.

a Klicken Sie mit der rechten Maustaste auf den Namen des API-Netzwerks in der Liste und wählen Sie **IP-Bereich hinzufügen** aus.

b Geben Sie den neuen IP-Bereich im Dialogfeld „IP-Bereich hinzufügen“ ein.

Hinweis Wenn Sie Adressen im Rahmen des Upgrade-Vorgangs hinzufügen, muss der neue IP-Bereich exakt mit der Anzahl von IP-Adressen übereinstimmen, die für das vorhandene API-Netzwerk konfiguriert sind. Beispielsweise erfordert in einer typischen VMware Integrated OpenStack-Bereitstellung das API-Netzwerk einen Mindestbereich von 2 IP-Adressen für Version 3.0 und ältere Versionen sowie einen Mindestbereich von 3 IP-Adressen für Version 3.1 und neuere Versionen.

c Klicken Sie auf **OK**.

Ändern der Einstellung für den Standardrouter

Sie können die von NSX verwendete Einstellung für den Standardrouter in der Datei `custom.yml` ändern.

Die Neutron-Konfigurationsdatei enthält einen Parameter, der die standardmäßigen Routertypen festlegt. Beispiel: `tenant_router_types = shared, distributed, exclusive`. Sie können die Datei `custom.yml` ändern, sodass diese Konfiguration mit einer benutzerdefinierten Einstellung überschrieben wird.

Vorgehensweise

1 Implementieren Sie die Datei `custom.yml`.

```
sudo mkdir –p /opt/vmware/vio/custom
sudo cp /var/lib/vio/ansible/custom/custom.yml.sample /opt/vmware/vio/custom/custom.yml
```

2 Öffnen Sie die Datei `/opt/vmware/vio/custom/custom.yml` in einem Texteditor.

3 Heben Sie die Auskommentierung des Parameters `nsxv_tenant_router_types` auf und geben Sie die Routertypen für NSX-Mandanten an.

```
nsxv_tenant_router_types: exclusive, shared, distributed
```

4 Melden Sie sich unter Verwendung von SSH bei VMware Integrated OpenStack Manager an.

5 Wechseln Sie zum Root-Benutzer.

```
sudo su –
```

6 Übertragen Sie die neue Konfiguration auf Ihre VMware Integrated OpenStack-Bereitstellung.

```
viocli deployment configure ––limit controller
```

Ändern der Netzwerk-DNS-Einstellung

Nach der Installation können Sie die DNS-Einstellungen für die Netzwerke ändern, die für die OpenStack-Verwaltung und den API-Zugriff konfiguriert wurden.

Wichtig Durch das Ändern der Netzwerk-DNS-Einstellung kommt es zu einer kurzen Unterbrechung der Netzwerkverbindung.

Vorgehensweise

1 Wählen Sie im vSphere Web Client die Option **Home > Bestandslisten** aus und klicken Sie auf das Symbol VMware Integrated OpenStack.

2 Klicken Sie auf die Registerkarte **Verwalten** und dann auf die Registerkarte **Netzwerke**.

Auf der Registerkarte **Netzwerk** werden die Verwaltungs- und API-Netzwerkkonfigurationen einschließlich ihrer DNS-Adressen aufgelistet.

3 Klicken Sie mit der rechten Maustaste auf den Netzwerknamen, dessen DNS-Einstellung Sie ändern möchten, und wählen Sie **DNS ändern**.

Hinweis Sie können auch das Netzwerk in der Liste auswählen, auf **Alle Aktionen** klicken und die Option **DNS ändern** auswählen.

4 Ändern Sie den DNS und die IP-Adressen des sekundären DNS.

5 Klicken Sie auf **OK**.

Erstellen einer VXLAN/VLAN L2-Bridge

In einer Leaf-and-Spine-Datencenter-Architektur kann der OpenStack Computing-Cluster nicht auf VMs in einem VLAN zugreifen. Sie können diese technische Einschränkung umgehen, indem Sie ein VXLAN-Netzwerk und eine VXLAN/VLAN L2-Bridge erstellen.

Voraussetzungen

Stellen Sie sicher, dass eine VDS-Portgruppe für die VXLAN-Netzwerkkonfiguration verfügbar ist.

Vorgehensweise

1 Melden Sie sich unter Verwendung von SSH als Administrator bei VMware Integrated OpenStack Manager an.

2 Melden Sie sich unter Verwendung von SSH beim controller01-Knoten an.

3 Erstellen Sie das logische L2-Gateway unter Neutron.

- Für VMware Integrated OpenStack-Version 3.0 oder eine ältere Version verwenden Sie den Befehl `neutron-l2gw l2-gateway-create`.

```
neutron-l2gw l2-gateway-create <gateway-name> \
--device name=<device-name1>,interface_names="<interface-name1>[|<seg-id1>]"
```

- Für VMware Integrated OpenStack-Version 3.1 oder eine neuere Version verwenden Sie den Befehl `l2-gateway-create`.

```
l2-gateway-create <gateway-name> \
--device name=<device-name1>,interface_names="<interface-name1>[|<seg-id1>]"
```

Option	Beschreibung
<gateway-name>	Gibt den Namen des neuen Gateways an.
<device-name1>	Gibt den Gerätenamen an. Dies ist ein Dummy-Name. Das NSX Plug-In erstellt einen dedizierten DLR.
<interface-name1>	Gibt die verteilte Portgruppen-MOB-ID als Schnittstellennamen an.
<seg-id1>	Gibt die verteilte Portgruppensegmentierungs-ID an.

Über den Sicherungs-Edge-Pool erstellt NSX einen dedizierten DLR, genannt L2-Bridging-{gateway-id}.

4 Erstellen Sie die logische L2-Gateway-Verbindung unter Neutron.

- Für VMware Integrated OpenStack-Version 3.0 oder eine ältere Version verwenden Sie den Befehl `neutron-l2gw l2-gateway-connection-create`.

```
neutron-l2gw l2-gateway-connection-create <gateway-name/uuid> <network-name/uuid> \
[--default-segmentation-id=<seg-id>]
```

- Für VMware Integrated OpenStack-Version 3.1 oder eine neuere Version verwenden Sie den Befehl `l2-gateway-connection-create`.

```
l2-gateway-connection-create <gateway-name/uuid> <network-name/uuid> \
[--default-segmentation-id=<seg-id>]
```

Option	Beschreibung
<gateway-name/uuid>	Gibt den Namen des vorhandenen Gateways an.
<network-name/uuid>	Gibt den Netzwerknamen an. Dies ist ein Dummy-Name. Das NSX Plug-In erstellt einen dedizierten DLR.
<default-segmentation-id=seg-id1>	Gibt die standardmäßige ID der verteilten Portgruppensegmentierung an.

Dieser Vorgang verbindet das OpenStack-Netzwerk mit dem Anbieter-VLAN-Netzwerk.

Verwalten der Hochverfügbarkeit für NSX Edge-Knoten

Sie können VMware Integrated OpenStack konfigurieren, um sicherzustellen, dass jeder NSX Edge-Knoten für die Hochverfügbarkeit aktiviert ist.

Sie können die Datei `custom.yml` konfigurieren, bevor Sie VMware Integrated OpenStack installieren und bereitstellen. Wenn VMware Integrated OpenStack bereits installiert und bereitgestellt wurde, können Sie jeden ausgeführten NSX Edge-Knoten manuell aktivieren.

Aktivieren der Hochverfügbarkeit für NSX Edge-Knoten vor der Bereitstellung

Bevor Sie VMware Integrated OpenStack installieren, können Sie die Hochverfügbarkeit für NSX Edge-Knoten aktivieren, indem Sie die Datei `custom.yml` ändern.

Voraussetzungen

Vergewissern Sie sich, dass Ihr Edge-Cluster mindestens zwei Hosts aufweist. Ist dies nicht der Fall, erhalten Sie möglicherweise einen Anti-Affinitätsfehler.

Vorgehensweise

1 Implementieren Sie die Datei `custom.yml`.

```
sudo mkdir –p /opt/vmware/vio/custom
sudo cp /var/lib/vio/ansible/custom/custom.yml.sample /opt/vmware/vio/custom/custom.yml
```

2 Bearbeiten Sie die Datei `/opt/vmware/vio/custom/custom.yml`.

a Heben Sie die Auskommentierung des Parameters `nsxv_edge_ha` auf.

b Setzen Sie den Parameter `nsxv_edge_ha` auf **`True`** fest.

```
nsxv_edge_ha: True
```

3 Speichern Sie die Datei `custom.yml`.

Wenn Sie VMware Integrated OpenStack installieren und bereitstellen, wird die Hochverfügbarkeit standardmäßig für alle NSX Edge-Knoten aktiviert.

Aktivieren der Hochverfügbarkeit für NSX Edge-Knoten nach der Bereitstellung

Wenn Sie VMware Integrated OpenStack bereits installiert haben, können Sie die Hochverfügbarkeit für NSX Edge-Knoten aktivieren, indem Sie die Datei `custom.yml` ändern und jeden ausgeführten Edge-Knoten manuell ändern.

Voraussetzungen

Vergewissern Sie sich, dass Ihr Edge-Cluster mindestens zwei Hosts aufweist. Ist dies nicht der Fall, erhalten Sie möglicherweise einen Anti-Affinitätsfehler.

Vorgehensweise

1 Implementieren Sie die Datei `custom.yml`.

```
sudo mkdir –p /opt/vmware/vio/custom
sudo cp /var/lib/vio/ansible/custom/custom.yml.sample /opt/vmware/vio/custom/custom.yml
```

2 Bearbeiten Sie die Datei `/opt/vmware/vio/custom/custom.yml`.

   a Heben Sie die Auskommentierung des Parameters `nsxv_edge_ha` auf.

   b Setzen Sie den Parameter `nsxv_edge_ha` auf **`True`** fest.

   ```
   nsxv_edge_ha: True
   ```

3 Speichern Sie die Datei `custom.yml`.

   Nach dem Ändern und Speichern der Datei `custom.yml` ist die Hochverfügbarkeit für alle NSX Edge-Knoten aktiviert, die nachfolgend von VMware Integrated OpenStack generiert werden.

4 Aktivieren Sie die Hochverfügbarkeit auf allen aktuellen NSX Edge-Knoten manuell.

   a Im VMware Integrated OpenStack-Controller befindet sich eine Liste mit allen aktuellen Edge-Knoten und deren `edge–id`-Werten.

   ```
   sudo –u neutron nsxadmin –r edges –o list
   ```

   b Aktivieren Sie die Hochverfügbarkeit in jedem Edge-Knoten, indem Sie dessen `edge–id`-Wert angeben.

   ```
   sudo –u neutron nsxadmin –r edges –o nsx–update \
   ––property highAvailability=True \
   ––property edge–id=<edge–id>
   ```

   c Wiederholen Sie den vorhergehenden Befehl für jeden Edge-Knoten.

5 Übertragen Sie die neue Konfiguration auf Ihre VMware Integrated OpenStack-Bereitstellung.

```
viocli deployment –v configure
```

Wichtig Dieser Befehl aktualisiert Ihre gesamte Bereitstellung und könnte Vorgänge kurzzeitig unterbrechen.

Deaktivieren des öffentlichen API-Zugriffs

Sie können den Benutzerzugriff auf Ihre VMware Integrated OpenStack-Bereitstellung vorübergehend sperren. Möglicherweise müssen Sie z. B. Wartungsarbeiten durchführen, bei denen der Zugriff für Benutzer gesperrt werden muss, administrativer Zugriff jedoch zugelassen werden soll.

Durch Anpassen der Datei `custom.yml` können Sie den Benutzerzugriff über das öffentliche API-Netzwerk sperren. Wenn Benutzer versuchen, auf OpenStack zuzugreifen, wird ihnen eine Wartungswebseite angezeigt.

Vorgehensweise

1 Falls nicht bereits geschehen, implementieren Sie die Datei `custom.yml`.

```
sudo mkdir –p /opt/vmware/vio/custom
sudo cp /var/lib/vio/ansible/custom/custom.yml.sample /opt/vmware/vio/custom/custom.yml
```

2 Bearbeiten Sie die Datei `custom.yml`, indem Sie die Auskommentierung des `haproxy_custom_maintenance_page`-Parameters aufheben.

```
############################
# haproxy maintenance page
############################
# location of the maintenance page to be displayed when the public VIP is disabled
haproxy_custom_maintenance_page : "/home/viouser/custom/503maintenance.html"
# mail contact for maintenance page.
#haproxy_mailto: test@vmware.com
```

3 Speichern Sie die Datei `custom.yml`.

4 Übertragen Sie die geänderte Konfiguration auf Ihre VMware Integrated OpenStack-Bereitstellung.

```
viocli deployment –v configure ––limit lb
```

5 Um die Sperrung zu entfernen, wiederholen Sie den Vorgang und kommentieren Sie den Parameter `haproxy_custom_maintenance_page` erneut aus.

Hinzufügen von Kapazität in vSphere Web Client

Sie können einer vorhandenen VMware Integrated OpenStack-Bereitstellung Computing-Cluster und Datenspeicher hinzufügen.

Hinzufügen eines neuen Computing-Clusters

Sie können die Anzahl der Computing-Cluster in Ihrer VMware Integrated OpenStack-Bereitstellung erhöhen, um die CPU-Kapazität zu erweitern.

Voraussetzungen

Bereiten Sie einen Cluster mit mindestens einem Host vor.

Vorgehensweise

1 Wählen Sie in vCenter die Option **Home > VMware Integrated OpenStack > Verwalten** aus.

2 Wählen Sie die Registerkarte **Nova Compute** aus.

Auf dieser Registerkarte werden die aktuellen Nova Computing-Cluster und ihr Status angezeigt.

3 Klicken Sie im oberen Bereich auf das grüne Pluszeichen (+).

4 Wählen Sie auf der Seite „Nova-Cluster hinzufügen“ des Dialogfelds „Cluster zu OpenStack hinzufügen“ den Cluster aus, den Sie als eine erforderliche Komponente vorbereitet haben, und klicken Sie auf **Weiter**.

Der von Ihnen ausgewählte Cluster muss mindestens einen Host beinhalten.

5 Wählen Sie auf der Seite „Vorgeschlagene Konfiguration überprüfen“ die vorhandene Verwaltungs-VM aus und klicken Sie auf **Weiter**.

6 Wählen Sie die Datenspeicher für die Mandanten im neuen Cluster aus und klicken Sie auf **Weiter**.

7 Überprüfen Sie die vorgeschlagene Konfiguration und klicken Sie auf **Fertig stellen**.

8 Bestätigen Sie, dass der neue Cluster zur OpenStack-Bereitstellung hinzugefügt wurde.

Der neu hinzugefügte Cluster wird auf der Registerkarte **Nova Compute** angezeigt.

Die OpenStack-Kapazität erhöht sich basierend auf den im zusätzlichen Cluster verfügbaren Ressourcen.

Hinzufügen von Speicher zum Computing-Knoten

Sie können die Anzahl der für den Computing-Knoten in Ihrer VMware Integrated OpenStack-Bereitstellung verfügbaren Datenspeicher erhöhen.

Durch Hinzufügen eines Datenspeichers zum Computing-Knoten wird der Nova-Dienst neu gestartet, wodurch es zu einer vorübergehenden Unterbrechung der OpenStack-Dienste im Allgemeinen kommen kann.

Voraussetzungen

Vergewissern Sie sich, dass Sie Datenspeicher verfügbar haben. Informationen finden Sie in der Dokumentation zu vSphere Web Client.

Vorgehensweise

1 Wählen Sie in vCenter die Option **Home > VMware Integrated OpenStack > Verwalten** aus.

2 Klicken Sie auf die Registerkarte **Nova-Speicher**.

Auf dieser Registerkarte werden die derzeit verfügbaren Datenspeicher, ihr Status und weitere Details angezeigt.

3 Klicken Sie im oberen Bereich auf das grüne Pluszeichen (+).

4 Wählen Sie auf der Seite „Einen Nova-Knoten auswählen“ des Dialogfelds „Nova-Datenspeicher hinzufügen“ den Cluster aus, dem Sie einen Datenspeicher hinzufügen möchten, und klicken Sie auf **Weiter**.

5 Wählen Sie auf der Seite „Nova-Datenspeicher hinzufügen“ mindestens einen Datenspeicher zum Hinzufügen zum Cluster aus und klicken Sie auf **Weiter**.

6 Überprüfen Sie die vorgeschlagene Konfiguration und klicken Sie auf **Fertig stellen**.

Die Speicherkapazität für den ausgewählten Computing-Knoten nimmt entsprechend der Größe des zusätzlichen Datenspeichers zu.

Hinzufügen von Speicher zum Imagedienst

Sie können die Anzahl der für den Imagedienst-Knoten in Ihrer VMware Integrated OpenStack-Bereitstellung verfügbaren Datenspeicher erhöhen.

Durch Hinzufügen eines Datenspeichers zum Imagedienst-Knoten wird der Glance-Dienst neu gestartet, wodurch es zu einer vorübergehenden Unterbrechung der OpenStack-Dienste im Allgemeinen kommen kann.

Voraussetzungen

Vergewissern Sie sich, dass Sie Datenspeicher verfügbar haben. Informationen finden Sie in der Dokumentation zu vSphere Web Client.

Vorgehensweise

1 Wählen Sie in vCenter die Option **Home > VMware Integrated OpenStack > Verwalten** aus.

2 Klicken Sie auf die Registerkarte **Glance-Speicher**.

Auf dieser Registerkarte werden die derzeit verfügbaren Datenspeicher, ihr Status und weitere Details angezeigt.

3 Klicken Sie im oberen Bereich auf das grüne Pluszeichen (+).

4 Wählen Sie auf der Seite „Glance-Datenspeicher hinzufügen“ mindestens einen Datenspeicher zum Hinzufügen zum Cluster aus und klicken Sie auf **Weiter**.

5 Überprüfen Sie die vorgeschlagene Konfiguration und klicken Sie auf **Fertig stellen**.

Die Speicherkapazität für den Imagedienst-Knoten nimmt entsprechend der Größe des zusätzlichen Datenspeichers zu.

Konfigurieren des Sicherungsdiensts für Blockspeicher

Es wird empfohlen, einen Sicherungsdienst für die Blockspeicherkomponente (Cinder) von OpenStack zu konfigurieren, um Datenverlust zu vermeiden. Sie können Cinder so konfigurieren, dass Datenträger entweder auf einem Netzwerkdateisystem (NFS) oder in einem Objektspeicherdienst (Swift) gesichert werden. Bei Swift handelt es sich um einen weiteren OpenStack-Dienst.

Sie konfigurieren einen Sicherungsdienst durch Installieren der in Ihrer VMware Integrated OpenStack 3.0 oder 3.1-Bereitstellung enthaltenen OpenStack Debian-Pakete.

Im Rahmen dieses Verfahrens werden die beiden Controller als controller01 und controller02 bezeichnet.

Voraussetzungen

Vergewissern Sie sich, dass Ihre VMware Integrated OpenStack 3.0 oder 3.1-Bereitstellung installiert ist und ausgeführt wird.

Für Sicherungskonfigurationen mit dem Swift-Dienst:

- Vergewissern Sie sich, dass die Swift-Komponente als Teil Ihrer VMware Integrated OpenStack 3.0 oder 3.1-Bereitstellung installiert ist. Weitere Informationen finden Sie im Installations- und Konfigurationshandbuch für VMware Integrated OpenStack.
- Vergewissern Sie sich, dass die Swift-Komponente bei der Identitätsdienstkomponente (Keystone) registriert ist. Bei Keystone handelt es sich um einen weiteren OpenStack-Dienst. Diese Registrierung ist Teil der Standard-Keystone-Konfiguration. Keystone wird als Teil Ihrer VMware Integrated OpenStack 3.0 oder 3.1-Bereitstellung installiert.

Für Sicherungskonfigurationen mit der NFS-Freigabe:

- Erstellen Sie einen dedizierten NFS-Freigabeordner zum Speichern der gesicherten Daten.
- Vergewissern Sie sich, dass der Besitzer des NFS-Freigabeordners über dieselbe UID wie Cinder auf den Controllerknoten verfügt. Die Cinder-Standard-UID ist 107. Dieser Wert kann in Ihrer Bereitstellung abweichen.

Vorgehensweise

1 Melden Sie sich unter Verwendung von SSH bei VMware Integrated OpenStack Manager an.

2 Implementieren Sie die Datei `custom.yml`.

```
sudo mkdir –p /opt/vmware/vio/custom
sudo cp /var/lib/vio/ansible/custom/custom.yml.sample /opt/vmware/vio/custom/custom.yml
```

3 Um Swift als Sicherungsdienst zu nutzen, ändern Sie die Datei `/opt/vmware/vio/custom/custom.yml` entsprechend.

   a Heben Sie die Auskommentierung des Parameters `cinder_backup_driver` auf.

   b Legen Sie den Parameter `cinder_backup_driver` auf **`cinder.backup.drivers.swift`** fest.

```
# Driver to use for backups. (string value)
 cinder_backup_driver: cinder.backup.drivers.swift
```

4 Um NFS als Sicherungsdienst zu nutzen, ändern Sie die Datei `/opt/vmware/vio/custom/custom.yml` entsprechend.

   a Heben Sie die Auskommentierung des Parameters `cinder_backup_driver` auf.

   b Legen Sie den Parameter `cinder_backup_driver` auf **`cinder.backup.drivers.nfs`** fest.

   ```
   # Driver to use for backups. (string value)
    cinder_backup_driver: cinder.backup.drivers.nfs
   ```

   c Heben Sie die Auskommentierung des Parameters `cinder_backup_share` auf.

   d Legen Sie den Parameter `cinder_backup_share` auf **`<NFS-Host-IP-Adresse>:<Dateisicherungspfad>`** fest.

   ```
   # NFS share in fqdn:path, ipv4addr:path, or "[ipv6addr]:path"
    # format. (string value)
    cinder_backup_share: <NFS host IP address>:<file backup path>
   ```

   e Wenn die NFS-Freigabe nicht in Version 4.1 vorliegt, müssen Sie die Auskommentierung des Parameters `cinder_backup_mount_options` aufheben und ihn auf Ihre Version von NFS festlegen. Beispiel: **`vers=3`**.

   ```
   # Mount options passed to the NFS client. See NFS man page for
   # details. (string value) 'vers=4' to support version NFS 4
   cinder_backup_mount_options: vers=4
   ```

5 Speichern Sie die Datei `custom.yml`.

6 Übertragen Sie die neue Konfiguration auf Ihre VMware Integrated OpenStack-Bereitstellung.

```
viocli deployment -v configure --limit controller
```

Wichtig Dieser Befehl aktualisiert Ihre gesamte Bereitstellung und könnte Vorgänge kurzzeitig unterbrechen.

Weiter

Vergewissern Sie sich, dass die Cinder-Sicherungskonfiguration ordnungsgemäß funktioniert. Siehe „Sicherstellen, dass der Cinder-Sicherungsdienst ausgeführt wird und betriebsbereit ist“, auf Seite 38.

Sicherstellen, dass der Cinder-Sicherungsdienst ausgeführt wird und betriebsbereit ist

Erstellen und sichern Sie einen Testdatenträger, um sicherzustellen, dass die Cinder-Sicherung richtig konfiguriert ist und ordnungsgemäß funktioniert.

Voraussetzungen

Schließen Sie die Cinder-Sicherungskonfiguration ab. Siehe „Konfigurieren des Sicherungsdiensts für Blockspeicher“, auf Seite 37.

Vorgehensweise

1 Vergewissern Sie sich, dass der Cinder-Sicherungsdienst ausgeführt wird.

```
cinder service-list
```

2 Erstellen Sie einen Testdatenträger.

```
cinder create --display-name <volume name>
```

3 Erstellen Sie eine Sicherung des Testdatenträgers.

```
cinder backup-create --display-name <backup name> <volume name>
```

4 Überprüfen Sie, ob die Sicherungsdatei auf der NFS-Freigabe bzw. im Swift-Dienst erstellt wurde.

Beheben eines Fehlers bei der Cinder-Datenträgersicherung

Während Sie die Cinder-Sicherung auf einer NFS-Freigabe konfigurieren, schlägt der erste Versuch, eine Testsicherung zu erstellen, fehl.

Problem

Wenn Sie die Cinder-Sicherungskonfiguration überprüfen, erhalten Sie einen Fehler beim Erstellen der ersten Sicherung.

Ursache

VMware Integrated OpenStack verfügt nicht über die erforderlichen Berechtigungen zum Schreiben in die NFS-Freigabe.

Lösung

1 Melden Sie sich unter Verwendung von SSH beim controller01-Knoten als Root-Benutzer an.

2 Navigieren Sie zum Mount-Verzeichnis für die Cinder-Sicherungskonfiguration.

```
cd /var/lib/cinder/backup_mount/
```

3 Ändern Sie den Besitzer des Ordners von `root` in `cinder`.

```
chown –R cinder:cinder *
```

Diese Problemumgehung korrigiert die Konfiguration und erteilt der Cinder-Komponente die Berechtigung für den Zugriff auf die NFS-Freigabe.

Sichern der VMware Integrated OpenStack -Bereitstellung

Es wird empfohlen, regelmäßig Sicherungen von OpenStack-Verwaltungsserver und -Datenbank zu erstellen.

Sie führen Sicherungsvorgänge an der Befehlszeilenschnittstelle für den VMware Integrated OpenStack Manager aus.

Voraussetzungen

Sie müssen sich mit Administrator- oder Superuser (sudo)-Rechten anmelden, um Sicherungsvorgänge auszuführen.

Vorgehensweise

1 Melden Sie sich unter Verwendung von SSH bei VMware Integrated OpenStack Manager an.

2 Wechseln Sie zum Root-Benutzer.

```
sudo su –
```

3 (Optional) Wechseln Sie in den ausführlichen Modus.

```
viocli backup <–v | –verbose>
```

4 (Optional) Zeigen Sie die Hilfeoptionen an.

```
viocli backup <–h | –help>
```

5 Verwenden Sie den Befehl `viocli backup mgmt_server <NFS_VOLUME>`, um den OpenStack Management Server zu sichern.

```
viocli backup mgmt_server [–d DEPLOYMENT] <NFS_VOLUME>
```

Option	Beschreibung
–d DEPLOYMENT	Gibt den Namen der zu sichernden VMware Integrated OpenStack-Bereitstellung an.
NFS_VOLUME	Name oder IP-Adresse des NFS-Ziel-Volumes und des Verzeichnisses im Format *remote_host:remote_dir*. Beispiel: 192.168.1.77:/backups

Die Sicherungsdatei wird automatisch mit dem Zeitstempel `vio_ms_JJJJMMTThhmmss` versehen.

6 Sichern Sie die OpenStack-Datenbank.

```
viocli backup openstack_db [–d DEPLOYMENT] <NFS_VOLUME>
```

Option	Beschreibung
–d DEPLOYMENT	Gibt den Namen der zu sichernden VMware Integrated OpenStack-Bereitstellungsdatenbank an.
NFS_VOLUME	Name oder IP-Adresse des NFS-Ziel-Volumes und des Verzeichnisses im Format *remote_host:remote_dir*. Beispiel: 192.168.1.77:/backups

Die Sicherungsdatei wird automatisch mit dem Zeitstempel `vio_os_db_JJJJMMTThhmmss` versehen.

Bei Eintreten eines schwerwiegenden Ereignisses können Sie die neuen Sicherungsdateien verwenden, um die Daten und die Konfiguration Ihrer VMware Integrated OpenStack-Bereitstellung wiederherzustellen.

Wiederherstellen von VMware Integrated OpenStack aus einer Sicherung

Im Falle eines Absturzes können Sie Ihren VMware Integrated OpenStack-Verwaltungsserver und Ihre OpenStack-Datenbank aus einer früheren Sicherung wiederherstellen.

Sie führen Wiederherstellungsvorgänge an der Befehlszeilenschnittstelle für den VMware Integrated OpenStack Manager aus.

Voraussetzungen

Melden Sie sich mit Administrator- oder Superuser (sudo)-Rechten an, um Wiederherstellungsvorgänge auszuführen.

Stellen Sie sicher, dass Sie über Sicherungen des Verwaltungsservers und der Datenbank verfügen. Siehe „Sichern der VMware Integrated OpenStack-Bereitstellung“, auf Seite 39.

Vorgehensweise

1 Melden Sie sich unter Verwendung von SSH bei VMware Integrated OpenStack Manager an.

2 Wechseln Sie zum Root-Benutzer.

```
sudo su –
```

3 (Optional) Wechseln Sie in den ausführlichen Modus.

```
viocli restore <–v | –verbose>
```

4 (Optional) Zeigen Sie die Hilfeoptionen an.

```
viocli restore <–h | –help>
```

5 Stellen Sie den OpenStack Management Server wieder her, wobei PATH den gewünschten Speicherort für die Sicherungsdatei angibt.

```
viocli restore mgmt_server \
[–d DEPLOYMENT] \
<BACKUP_NAME> \
<NFS_VOLUME>
```

Option	Beschreibung
–d DEPLOYMENT	Gibt die Sicherung anhand des bei der Erstellung zugewiesenen Bereitstellungsnamens an.
BACKUP_NAME	Gibt den Zeitstempel der zur Wiederherstellung des Verwaltungsservers zu verwendenden Sicherungsdatei an.
NFS_VOLUME	Gibt den NFS-Host an, auf dem sich die Sicherungsdatei befindet.

6 Stellen Sie die OpenStack-Datenbank wieder her.

```
viocli restore openstack_db \
[–d DEPLOYMENT] \
<BACKUP_NAME> \
<NFS_VOLUME>
```

Option	Beschreibung
–d DEPLOYMENT	Gibt die Sicherung anhand des bei der Erstellung zugewiesenen Bereitstellungsnamens an.
BACKUP_NAME	Gibt den Zeitstempel der zur Wiederherstellung der Datenbank zu verwendenden Sicherungsdatei an.
NFS_VOLUME	Gibt den NFS-Host an, auf dem sich die Sicherungsdatei befindet.

Sie stellen Ihren VMware Integrated OpenStack-Verwaltungsserver und Ihre OpenStack-Datenbank auf dem Stand der Sicherungen wieder her.

Wiederherstellung nach einem Fehler

Im Falle eines Festplattenfehlers oder eines anderen kritischen Problems können Sie die einzelnen Knoten in Ihrer VMware Integrated OpenStack-Bereitstellung über die Befehlszeilenschnittstelle wiederherstellen.

Wenn Sie einen VMware Integrated OpenStack-Knoten wiederherstellen, wird er in den Zustand eines neu bereitgestellten Knotens versetzt. Zum Wiederherstellen eines Datenbankknotens müssen Sie eine Sicherungsdatei wiederherstellen. Siehe „Sichern der VMware Integrated OpenStack-Bereitstellung“, auf Seite 39.

Vorgehensweise

1 Melden Sie sich unter Verwendung von SSH bei VMware Integrated OpenStack Manager an.

2 Wechseln Sie zum Root-Benutzer.

```
sudo su –
```

3 Wechseln Sie in den ausführlichen Modus.

```
viocli recover <–v | –verbose>
```

4 Zeigen Sie die Hilfeoptionen an.

```
viocli recover <–h | –help>
```

5 Führen Sie eine Wiederherstellung der OpenStack-Knoten nach Knoten oder Rolle aus.

a So stellen Sie einen Datenbankknoten wieder her:

```
viocli recover <[–r ROLE –dn BACKUP_NAME]|[–n NODE –dn BACKUP_NAME]> –nfs NFS_VOLUME
```

Option	Beschreibung
–n NODE	Stellt die anhand des VM-Namens angegebenen Datenbankknoten nach Knotennamen wieder her. Sie können mehrere Knoten in einem Befehl angeben. Verwenden Sie den VM-Namen, wie er im VMware Integrated OpenStack-Manager (**VMware Integrated OpenStack > OpenStack-Bereitstellungen > [Bereitstellungsname]**) angezeigt wird. Beispiel: `viocli recover -n VIO–DB–0 VIO–DB–1 VIO–DB–2 -dn vio_os_db_20150830215406 –nfs 10.146.29.123:/backups` Stellt aus der angegebenen NFS-Sicherungsdatei alle genannten Datenbankknoten wieder her: VIO-DB-0, VIO-DB-1 und VIO-DB-2.
–r ROLE	Stellt alle Datenbankknoten in der angegebenen Gruppe wieder her. Sie können mehrere Rollen in einem Befehl angeben. Verwenden Sie den Gruppennamen, wie er im VMware Integrated OpenStack-Manager (**VMware Integrated OpenStack > OpenStack-Bereitstellungen > [Bereitstellungsname]**) angezeigt wird. Beispiel: `viocli recover –r DB –dn vio_os_db_20150830215406 –nfs 10.146.29.123:/backups` Stellt aus der angegebenen NFS-Sicherungsdatei alle Knoten der DB-Knotengruppe wieder her.
–dn BACKUP_NAME	Gibt den Zeitstempel der zur Wiederherstellung der Datenbank zu verwendenden Sicherungsdatei an.
–nfs NFS_VOLUME	Gibt den NFS-Host an, auf dem sich die Sicherungsdatei befindet.

b So stellen Sie einen beliebigen Knoten, der kein Datenbankknoten ist, wieder her:

```
viocli recover <[–r ROLE]|[–n NODE]>
```

Option	Beschreibung
–n NODE	Stellt die anhand des VM-Namens angegebenen Knoten wieder her. Sie können mehrere Knoten in einem Befehl angeben. Verwenden Sie den VM-Namen, wie er im VMware Integrated OpenStack-Manager (**VMware Integrated OpenStack > OpenStack-Bereitstellungen > [Bereitstellungsname]**) angezeigt wird. Beispiel: `viocli recover –n VIO–Controller01` Stellt den VIO-Controller01-Knoten wiederher.
–r ROLE	Stellt alle Knoten in der angegebenen Gruppe wieder her. Sie können mehrere Rollen in einem Befehl angeben. Verwenden Sie den Gruppennamen, wie er im VMware Integrated OpenStack-Manager (**VMware Integrated OpenStack > OpenStack-Bereitstellungen > [Bereitstellungsname]**) angezeigt wird. Beispiel: `viocli recover –r VIO–Controller01`

Option	Beschreibung
	Stellt alle Knoten in der VIO-Controller01-Knotengruppe wiederher.

Tipp Sie können den Befehl `viocli show` verwenden, um alle Knoten und deren Rollen in Ihrer VMware Integrated OpenStack-Bereitstellung aufzulisten.

6 Vergewissern Sie sich, dass der Knoten ausgeführt wird, indem Sie seinen Status im VMware Integrated OpenStack-Manager überprüfen: **VMware Integrated OpenStack > OpenStack-Bereitstellungen > [Bereitstellungsname]**.

Abhängig von Ihrer Bereitstellung kann der Wiederherstellungsvorgang einige Minuten in Anspruch nehmen.

Speicherorte der VMware Integrated OpenStack -Protokolldateien

Wenn Sie technischen Support anfordern, werden Sie möglicherweise gebeten, Protokolldateien bereitzustellen. Die folgenden Tabellen geben den Speicherort der Dateien an und beschreiben deren Zweck.

VMware Integrated OpenStack -Verwaltungsserver-Protokolle

Name und Speicherort	Beschreibung
`/var/log/apache2/access.log`	Protokolliert den Zugriff auf den VMware Integrated OpenStack-Manager.
`/var/log/apache2/error.log`	Protokolliert Zugriffsfehler für den VMware Integrated OpenStack-Manager.
`/var/log/jarvis/ansible.log`	Protokolliert Aktivitäten des Ansible-Dienstes.
`/var/log/jarvis/jarvis.log`	Protokolliert Aktivitäten des Jarvis-Dienstes.
`/var/log/jarvis/pecan.log`	Protokolliert Aktivitäten des Pecan-Frameworkdienstes.
`/var/log/oms/oms.log`	Protokolliert Aktivitäten des VMware Integrated OpenStack-Manager-Dienstes.
`/var/log/oms/register_plugin.log`	Protokolliert Aktivitäten der VMware Integrated OpenStack-Plug-In-Registrierung.
`/var/log/osvmw/osvmw_exceptions.log`	Protokolliert Ausnahmen für den osvmw-Dienst.
`/var/log/osvmw/osvmw.log`	Protokolliert Aktivitäten des osvmw-Dienstes.
`/var/log/viocli/viocli.log`	Protokolliert Aktivitäten des viocli-Dienstes (VMware Integrated OpenStack CLI).
`/var/log/viomon/viomon.log`	Protokolliert Aktivitäten der VMware Integrated OpenStack-Überwachung.
`/var/log/viopatch/*.log`	Protokolliert Upgrade- und Patch-Aktivitäten.
`/var/log/bootsequence.log`	Protokolliert Startaktivitäten.

OpenStack Controller-Protokolle

Name und Speicherort	Beschreibung
`/var/log/apache2/access.log`	Protokolliert Zugriffsaktivitäten für Horizon (VMware Integrated OpenStack-Dashboard).
`/var/log/cinder/cinder_api.log`	Protokolliert Aktivitäten des Cinder-API-Dienstes.
`/var/log/apache2/error.log`	Protokolliert allgemeine Aktivitäten für Horizon (VMware Integrated OpenStack-Dashboard).
`/var/log/cinder/cinder_scheduler.log`	Protokolliert Aktivitäten des Cinder Scheduler-Dienstes.

Name und Speicherort	Beschreibung
/var/log/glance/glance-api.log	Protokolliert Aktivitäten des Glance-API-Dienstes.
/var/log/cinder/cinder-volume.log	Protokolliert Aktivitäten des Cinder-Datenträgerdienstes.
/var/log/glance/glance-registry.log	Protokolliert Aktivitäten des Glance-Registrierungsdienstes.
/var/log/glance/manage.log	Protokolliert allgemeine Aktivitäten des Glance-Dienstes.
/var/log/heat/heat-api-cfn.log	Protokolliert allgemeine Aktivitäten des Heat-Dienstes.
/var/log/heat/heat-api-cloudwatch.log	Protokolliert allgemeine Aktivitäten des Heat-Dienstes.
/var/log/heat/heat-api.log	Protokolliert Aktivitäten des Heat-API-Dienstes.
/var/log/heat/heat-engine.log	Protokolliert Aktivitäten des Heat-Engine-Dienstes.
/var/log/keystone/keystone-manage.log	Protokolliert Aktivitäten des Keystone-Verwaltungsdienstes.
/var/log/keystone/keystone.log	Protokolliert allgemeine Aktivitäten des Keystone-Dienstes.
/var/log/neutron/neutron-server.log	Protokolliert Aktivitäten des Neutron-Serverdienstes.
/var/log/nova/nova-api.log	Protokolliert Aktivitäten des Nova-API-Dienstes.
/var/log/nova/nova-conductor.log	Protokolliert Aktivitäten des Nova-Conductor-Dienstes.
/var/log/nova/nova-consoleauth.log	Protokolliert Aktivitäten des Nova-Consoleauth-Dienstes.
/var/log/nova/nova-manage.log	Protokolliert Aktivitäten des Nova-Verwaltungsdienstes.
/var/log/nova/nova-mksproxy.log	Protokolliert Aktivitäten des Nova-mksproxy-Dienstes.
/var/log/nova/nova-novncproxy.log	Protokolliert Aktivitäten des Nova-novncproxy-Dienstes.
/var/log/nova/nova-scheduler.log	Protokolliert Aktivitäten des Nova-Scheduler-Dienstes.

Datenbankdienst-Protokolle

Name und Speicherort	Beschreibung
/var/log/syslog	Allgemeine Datenbankprotokollierung einschließlich MySQL-Protokollierung.
/var/log/rabbitmq/rabbit@database01.log	Protokolliert allgemeine RabbitMQ-Datenbankaktivitäten.
/var/log/rabbitmq/shutdown_log	Protokolliert Herunterfahraktivitäten des RabbitMQ-Dienstes.
/var/log/rabbitmq/startup_log	Protokolliert Hochfahraktivitäten des RabbitMQ-Dienstes.

Computing- und Loadbalancer-Dienst-Protokolle

Name und Speicherort	Beschreibung
/var/log/haproxy/haproxy.log	Protokolliert Aktivitäten des HAProxy-Dienstes.
/var/log/nova/nova-compute.log	Protokolliert Aktivitäten des Nova Compute-Dienstes.
/var/log/nova/nova-manage.log	Protokolliert Aktivitäten des Nova-Verwaltungsdienstes.
/var/log/ceilometer/ceilometer-agent-compute.log	Protokolliert Aktivitäten des Ceilometer-Agents.

Aktualisieren auf VMware Integrated OpenStack 3.0 oder 3.1

Sie aktualisieren VMware Integrated OpenStack auf VMware Integrated OpenStack 3.0 oder 3.1, indem Sie einen Debian-Patch installieren, VMware Integrated OpenStack 3.0 oder 3.1 separat bereitstellen und anschließend von Ihrer vorhandenen VMware Integrated OpenStack-Bereitstellung auf die neue, aktualisierte Bereitstellung migrieren.

Bei diesem Aktualisierungsvorgang ist vSphere erforderlich, um die vorhandene Bereitstellung und die aktualisierte Bereitstellung verarbeiten zu können. Sie müssen zusätzliche Ressourcen, Datenspeicher, IP-Adressen usw. verfügbar machen, um den Upgrade-Vorgang ausführen zu können. vSphere verwaltet beide Bereitstellungen, bis Sie entscheiden, dass der Upgrade-Vorgang erfolgreich war und kein Rollback auf Ihre vorherige VMware Integrated OpenStack-Bereitstellung durchgeführt werden muss.

Wichtig Das Upgrade behält nur Anpassungen bei, die in der Datei `custom.yml` konfiguriert sind. Änderungen oder Anpassungen, die direkt an der OpenStack-Bereitstellung vorgenommen werden, wie beispielsweise SWIFT, werden nicht übernommen. Der OpenStack-Administrator ist dafür verantwortlich, solche Änderungen nachzuverfolgen und nach dem Upgrade erneut anzuwenden.

Hinweis Wenn Sie ein Upgrade von VMware Integrated OpenStack 2.5.1 durchführen, wird nur das Upgrade auf VMware Integrated OpenStack 3.1 unterstützt.

Voraussetzungen

- Stellen Sie sicher, dass mit Ausnahme der memcache- und RabbitMQ-Knoten alle Knoten übereinstimmende Ressourcen aufweisen. Informationen finden Sie in den Hardwareanforderungen im Installations- und Konfigurationshandbuch für VMware Integrated OpenStack.
- Sichern Sie Ihre aktuelle Bereitstellung. Ausführliche Informationen finden Sie unter „Sichern der VMware Integrated OpenStack-Bereitstellung“, auf Seite 39.
- Um Ihre aktuelle VMware Integrated OpenStack-Konfiguration beizubehalten, exportieren Sie sie aus dem VMware Integrated OpenStack-Manager als Konfigurationsdatei.

Vorgehensweise

1 Hinzufügen von IP-Adressen zur Netzwerkkonfiguration auf Seite 46

Der Upgrade-Vorgang erfordert temporäre IP-Adressen zusätzlich zu Ihrer bestehenden IP-Adresskonfiguration. vSphere stellt ein Tool bereit, mit dem Sie diesen erforderlichen IP-Bereich hinzufügen können.

2 Installieren des Upgrade-Patches für VMware Integrated OpenStack 3.0 oder 3.1 auf Seite 47

Das VMware Integrated OpenStack 3.0 oder 3.1-Upgrade ist ein Debian-Patch. Wenn Sie den Upgrade-Patch installieren, aktualisieren Sie die VMware Integrated OpenStack Manager-vApp.

3 Migrieren zur VMware Integrated OpenStack 3.0 oder 3.1-Bereitstellung auf Seite 48

Nachdem Sie den Upgrade-Patch heruntergeladen und installiert haben, installieren Sie ihn als separate Bereitstellung und migrieren Sie Ihre Daten.

4 Wiederherstellen einer vorherigen VMware Integrated OpenStack-Bereitstellung auf Seite 49

Sie können zu einer vorherigen Version von VMware Integrated OpenStack zurückkehren, indem Sie Ihre vorherige Bereitstellung wiederherstellen.

5 Löschen der älteren VMware Integrated OpenStack-Bereitstellung auf Seite 50

Nachdem das Upgrade auf die VMware Integrated OpenStack 3.0 oder 3.1-Bereitstellung abgeschlossen ist, können Sie die ältere VMware Integrated OpenStack-Bereitstellung löschen. Indem Sie die alte Bereitstellung löschen, geben Sie die von dieser Bereitstellung belegten CPU-, Datenspeicher- und IP-Adressressourcen frei.

Hinzufügen von IP-Adressen zur Netzwerkkonfiguration

Der Upgrade-Vorgang erfordert temporäre IP-Adressen zusätzlich zu Ihrer bestehenden IP-Adresskonfiguration. vSphere stellt ein Tool bereit, mit dem Sie diesen erforderlichen IP-Bereich hinzufügen können.

Sie können den Vorgang für das Hinzufügen von IP-Adressen aus beliebigen Gründen verwenden. Wenn Sie IP-Adressen nicht im Rahmen eines Upgrade-Vorgangs hinzufügen, gilt die spezifische Anzahl der erforderlichen IP-Adressen möglicherweise nicht.

Vorgehensweise

1 Wählen Sie im vSphere Web Client die Option **Home > Bestandslisten** aus und klicken Sie auf das Symbol VMware Integrated OpenStack.

2 Klicken Sie auf die Registerkarte **Verwalten** und dann auf die Registerkarte **Netzwerke**.

Auf der Registerkarte **Netzwerk** werden die Verwaltungs- und API-Netzwerkkonfigurationen einschließlich ihrer IP-Adressbereiche aufgelistet.

3 Erweitern Sie die für das Verwaltungsnetzwerk verfügbaren IP-Adressen.

a Klicken Sie mit der rechten Maustaste auf den Namen des Verwaltungsnetzwerks in der Liste und wählen Sie **IP-Bereich hinzufügen** aus.

b Geben Sie den neuen IP-Bereich im Dialogfeld „IP-Bereich hinzufügen“ ein.

Hinweis Wenn Sie Adressen im Rahmen des Upgrade-Vorgangs hinzufügen, muss der neue IP-Bereich exakt mit der Anzahl von IP-Adressen übereinstimmen, die für das vorhandene Verwaltungsnetzwerk konfiguriert sind. In einer typischen VMware Integrated OpenStack-Bereitstellung erfordert das Verwaltungsnetzwerk beispielsweise einen Mindestbereich von 11 IP-Adressen.

---

c Klicken Sie auf **OK**.

4 Erweitern Sie die für das externe Netzwerk verfügbaren IP-Adressen.

a Klicken Sie mit der rechten Maustaste auf den Namen des API-Netzwerks in der Liste und wählen Sie **IP-Bereich hinzufügen** aus.

b Geben Sie den neuen IP-Bereich im Dialogfeld „IP-Bereich hinzufügen“ ein.

Hinweis Wenn Sie Adressen im Rahmen des Upgrade-Vorgangs hinzufügen, muss der neue IP-Bereich exakt mit der Anzahl von IP-Adressen übereinstimmen, die für das vorhandene API-Netzwerk konfiguriert sind. Beispielsweise erfordert in einer typischen VMware Integrated OpenStack-Bereitstellung das API-Netzwerk einen Mindestbereich von 2 IP-Adressen für Version 3.0 und ältere Versionen sowie einen Mindestbereich von 3 IP-Adressen für Version 3.1 und neuere Versionen.

---

c Klicken Sie auf **OK**.

Weiter

Wenn Sie IP-Adressen im Rahmen des Upgrade-Vorgangs hinzugefügt haben, können Sie nun den Upgrade-Patch abrufen und installieren.

Installieren des Upgrade-Patches für VMware Integrated OpenStack 3.0 oder 3.1

Das VMware Integrated OpenStack 3.0 oder 3.1-Upgrade ist ein Debian-Patch. Wenn Sie den Upgrade-Patch installieren, aktualisieren Sie die VMware Integrated OpenStack Manager-vApp.

Vorgehensweise

1 Laden Sie das Upgrade als Debian-Patch von VMware herunter.

Wenn Sie nicht wissen, wo Sie den Upgrade-Patch abrufen sollen, navigieren Sie zur VMware Integrated OpenStack-Produktseite https://www.vmware.com/products/openstack.

2 Fügen Sie den Upgrade-Patch Ihrer VMware Integrated OpenStack-Installation hinzu.

a Melden Sie sich bei der Konsole für den VMware Integrated OpenStack-Verwaltungsserver an.

b Laden Sie die Debian-Datei für den Patch herunter.

c Fügen Sie den Pfad für den Upgrade-Patch hinzu.

```
viopatch add –l <upgrade patch path>
```

d Vergewissern Sie sich, dass der Upgrade-Patch erfolgreich hinzugefügt wurde.

```
viopatch list
```

Mit diesem Befehl wird eine Liste der verfügbaren Patches mit den jeweiligen Versionsnummern, dem jeweiligen Typ und dem aktuellen Status zurückgegeben. Die Liste gibt den Upgrade-Patch nach Build-Nummer an.

3 Installieren Sie den Upgrade-Patch.

a Stellen Sie sicher, dass der VMware Integrated OpenStack-Dienst entweder ausgeführt wird oder noch nicht bereitgestellt wurde.

Wenn sich der VMware Integrated OpenStack-Dienst in einem anderen Status befindet, schlägt das Upgrade fehl.

b Melden Sie sich beim VMware Integrated OpenStack-Verwaltungsserver an und installieren Sie den Patch.

```
viopatch install –p <upgrade patch name> –v <upgrade patch version>
```

Die Patch-Installation dauert einige Minuten.

4 Führen Sie den Befehl `viocli dbverify` aus, um die VMware Integrated OpenStack-Datenbank auf bekannte Probleme zu überprüfen, wie beispielsweise doppelte oder fehlende Schlüssel, die Probleme beim Upgrade-Vorgang verursachen können.

```
viocli dbverify [–d NAME] [–h] [–v]
```

Weitere Informationen hierzu finden Sie unter „Befehl „viocli dbverify““, auf Seite 118.

Die VMware Integrated OpenStack-vApp wurde nun aktualisiert.

Weiter

Jetzt können Sie die neue VMware Integrated OpenStack-Bereitstellung installieren und bereitstellen.

Migrieren zur VMware Integrated OpenStack 3.0 oder 3.1 -Bereitstellung

Nachdem Sie den Upgrade-Patch heruntergeladen und installiert haben, installieren Sie ihn als separate Bereitstellung und migrieren Sie Ihre Daten.

Wenn Sie ein Upgrade von einer VMware Integrated OpenStack 2.x- oder 3.0-Bereitstellung auf 3.1 durchführen, müssen Sie die öffentlichen VIP-Einstellungen für den Lastausgleichsdienst nicht konfigurieren, da diese Konfiguration nun automatisch erfolgt.

Beim Upgrade-Vorgang können Sie auch von einer 3.0-Bereitstellung im Kompaktmodus auf eine 3.1-HA-Bereitstellung umstellen.

Vorgehensweise

1 Wenn Sie beim vSphere Web Client angemeldet sind, melden Sie sich ab und wieder an.

Dadurch wird die Schnittstelle aktualisiert, sodass Sie über den vSphere Web Client auf den neu installierten Patch zugreifen können.

2 Wählen Sie im vSphere Web Client die Option **Home > Bestandslisten** aus und klicken Sie auf das Symbol VMware Integrated OpenStack.

3 Klicken Sie auf die Registerkarte **Übersicht**, um sich zu vergewissern, dass der VMware Integrated OpenStack-Manager aktualisiert wurde.

Die neue Version wird neben der vApp angezeigt.

4 Klicken Sie auf die Registerkarte **Verwalten** und dann auf die Registerkarte **Upgrades**.

Auf der Registerkarte **Upgrades** wird die aktuelle VMware Integrated OpenStack-Bereitstellung angezeigt.

5 Klicken Sie mit der rechten Maustaste auf den Namen der Bereitstellung und wählen Sie aus dem Popup-Menü die Option **Upgrade** aus.

6 Geben Sie den Namen für die neue Bereitstellung ein.

Dieser Name muss sich vom Namen der vorhandenen Bereitstellung unterscheiden.

7 Wenn Sie von einer 3.0-Bereitstellung im Kompaktmodus auf 3.1 aktualisieren, wählen Sie im Dropdown-Menü **Bereitstellungstyp** den Typ für die aktualisierte Bereitstellung aus.

Wenn VMware Integrated OpenStack 3.0 im Kompaktmodus bereitgestellt wird, können Sie während der Aktualisierung in den HA-Modus wechseln oder den Kompaktmodus beibehalten.

8 Klicken Sie auf **Weiter**.

9 Bei einem Upgrade auf Version 3.0 konfigurieren Sie die öffentlichen VIP-Einstellungen für den Lastausgleichsdienst.

Dieser Wert dient als temporäre VIP-Konfiguration. Wenn Sie von der vorhandenen Bereitstellung zur aktualisierten Bereitstellung migrieren, verwendet die neue Bereitstellung die vorhandene VIP-Konfiguration, und die alte Bereitstellung verwendet die temporäre Bereitstellung.

Option	Beschreibung
Öffentliche virtuelle IP	Dieser Wert sollte sich im selben Subnetz wie das OpenStack-API-Zugriffsnetzwerk und außerhalb des für das OpenStack-API-Zugriffsnetzwerk angegebenen IP-Bereichs befinden.

10 Klicken Sie auf **Weiter**.

11 Überprüfen Sie die Upgradekonfiguration und klicken Sie auf **Fertig stellen**.

Die neue Bereitstellung ist erfolgt, aber sie verwendet eine temporäre öffentliche IP-Adresse. Benutzer können darauf zugreifen, aber nur unter Verwendung dieser temporären öffentlichen VIP. Erst nachdem Sie den folgenden Schritt durchgeführt haben, wird die ursprüngliche öffentliche VIP für die neue Bereitstellung konfiguriert. Auf der Registerkarte **Upgrades** werden jetzt die aktuelle VMware Integrated OpenStack-Bereitstellung und neue Bereitstellungen aufgelistet. Die aktuelle Bereitstellung weist den Status „Wird ausgeführt“ auf, und die neue aktualisierte Bereitstellung weist den Status „Bereitgestellt“ auf.

12 Klicken Sie auf der Registerkarte **Upgrades** mit der rechten Maustaste auf den Namen der alten Bereitstellung und wählen Sie **Daten migrieren** aus.

Wichtig Sie werden aufgefordert, diese Aktion zu bestätigen, weil die VMware Integrated OpenStack-Dienste während der Datenmigration beendet werden und bis zum Abschluss des Upgradevorgangs Ausfallzeiten auftreten.

Wenn der Migrationsvorgang abgeschlossen ist, wird der Status für die aktualisierte Bereitstellung auf der Registerkarte **Upgrades** in „Migriert“ geändert.

13 Klicken Sie auf der Registerkarte **Upgrades** mit der rechten Maustaste auf den Namen der vorherigen Bereitstellung und wählen Sie **Zu neuer Bereitstellung wechseln** aus.

Wenn der Bereitstellungswechsel abgeschlossen ist, wird der Status für die aktualisierte Bereitstellung auf der Registerkarte **Upgrades** in „Wird ausgeführt“ geändert. Die vorherige Bereitstellung weist den Status „Beendet“ auf.

Weiter

Wenn der Bereitstellungsvorgang nicht erfolgreich ist, können Sie Ihre vorherige VMware Integrated OpenStack-Bereitstellung wiederherstellen. Siehe „Wiederherstellen einer vorherigen VMware Integrated OpenStack-Bereitstellung“, auf Seite 49.

Wenn der Bereitstellungsvorgang erfolgreich ist, können Sie die vorherige VMware Integrated OpenStack-Bereitstellung löschen.

Wiederherstellen einer vorherigen VMware Integrated OpenStack - Bereitstellung

Sie können zu einer vorherigen Version von VMware Integrated OpenStack zurückkehren, indem Sie Ihre vorherige Bereitstellung wiederherstellen.

Voraussetzungen

- Vergewissern Sie sich, dass Sie die vorherige VMware Integrated OpenStack-Bereitstellung in Ihrem OpenStack-Manager beibehalten haben.
- Vergewissern Sie sich, dass Sie bereit sind, die in der vorherigen VMware Integrated OpenStack-Bereitstellung ausgeführten Dienste zu beenden.

Vorgehensweise

1 Wählen Sie im vSphere Web Client die Option **Home > Bestandslisten** aus und klicken Sie auf das Symbol VMware Integrated OpenStack.

2 Klicken Sie im Fenster „Bestandslisten“ auf **OpenStack-Bereitstellungen**.

Die aktuelle VMware Integrated OpenStack-Bereitstellung wird im mittleren Fenster angezeigt.

3 Klicken Sie mit der rechten Maustaste auf den Namen der aktuellen Bereitstellung auf der Registerkarte **OpenStack-Bereitstellungen** und wählen Sie **OpenStack-Bereitstellung beenden** aus.

4 Kehren Sie zum VMware Integrated OpenStack-Hauptfenster zurück (**Startseite > Bestandslisten > VMware Integrated OpenStack**).

5 Klicken Sie auf die Registerkarte **Verwalten** und dann auf die Registerkarte **Upgrades**.

Auf der Registerkarte **Upgrades** werden die VMware Integrated OpenStack 3.0 oder 3.1-Bereitstellung und ältere Bereitstellungen aufgelistet.

6 Klicken Sie mit der rechten Maustaste auf den Namen der vorherigen VMware Integrated OpenStack-Bereitstellung und wählen Sie aus dem Popup-Menü die Option **Wiederherstellen** aus.

Wenn die Wiederherstellung Ihrer VMware Integrated OpenStack-Bereitstellung abgeschlossen ist, wird der OpenStack-Dienst neu gestartet.

Löschen der älteren VMware Integrated OpenStack -Bereitstellung

Nachdem das Upgrade auf die VMware Integrated OpenStack 3.0 oder 3.1-Bereitstellung abgeschlossen ist, können Sie die ältere VMware Integrated OpenStack-Bereitstellung löschen. Indem Sie die alte Bereitstellung löschen, geben Sie die von dieser Bereitstellung belegten CPU-, Datenspeicher- und IP-Adressressourcen frei.

Voraussetzungen

Vergewissern Sie sich, dass Ihre aktualisierte VMware Integrated OpenStack 3.0 oder 3.1-Bereitstellung erfolgreich ausgeführt wird und ordnungsgemäß funktioniert. Nachdem Sie eine Bereitstellung gelöscht haben, können Sie sie nicht mehr wiederherstellen.

Vorgehensweise

1 Wählen Sie im vSphere Web Client die Option **Home > Bestandslisten** aus und klicken Sie auf das Symbol VMware Integrated OpenStack.

2 Klicken Sie auf die Registerkarte **Verwalten** und dann auf die Registerkarte **Upgrades**.

Auf der Registerkarte **Upgrades** werden die aktuelle und die alte Version von VMware Integrated OpenStack sowie alte Bereitstellungen angezeigt. Die VMware Integrated OpenStack 3.0 oder 3.1-Bereitstellung weist den Status „Wird ausgeführt“ auf. Die VMware Integrated OpenStack-Bereitstellung weist den Status „Beendet“ auf.

3 Klicken Sie mit der rechten Maustaste auf die ältere VMware Integrated OpenStack-Bereitstellung und wählen Sie aus dem Popup-Menü die Option **Löschen** aus.

4 Bestätigen Sie den Löschvorgang an der Eingabeaufforderung.

Die Bereitstellung wird auf der Registerkarte **Upgrades** bzw. in der Liste **OpenStack-Bereitstellungen** nicht mehr angezeigt.

Aktualisieren Ihrer VMware Integrated OpenStack -Bereitstellung

Sie aktualisieren Ihre VMware Integrated OpenStack-Bereitstellung mit der VMware Integrated OpenStack Manager vApp oder den Befehlen an der Befehlszeilenschnittstelle, um Patches zu installieren und anzuwenden.

Nach der Installation eines Patches können Sie bei Bedarf eine vorherige Version wiederherstellen.

Installieren eines Patches mit dem vSphere Web Client

VMware bietet Updates in Form von Debian-Patches. Patches, die sich nicht auf die Infrastruktur der VMware Integrated OpenStack-Bereitstellung auswirken, können mit der VMware Integrated OpenStack Manager-vApp angewendet werden.

Voraussetzungen

vSphere Web Client

Für einige Patches ist es möglicherweise erforderlich, den VMware Integrated OpenStack-Dienst vor dem Fortfahren herunterzufahren.

Vorgehensweise

1 Laden Sie den Debian-Patch von VMware herunter.

Wenn Sie nicht wissen, wo Sie den Patch abrufen sollen, navigieren Sie zur VMware Integrated OpenStack-Produktseite https://www.vmware.com/products/openstack oder wenden Sie sich an VMware.

2 Übertragen Sie die Patch-Datei auf den Verwaltungsserver.

3 Melden Sie sich am Verwaltungsserver an und geben Sie den folgenden Befehl ein, um die Patch-Datei in das Verwaltungsserver-Repository zu laden:

```
sudo viopatch add –l path/filename.deb
```

filename.deb steht dabei für den Dateinamen der Debian-Patch-Datei.

4 Wählen Sie im vSphere Web Client die Option **Home > Bestandslisten** aus und klicken Sie auf das Symbol VMware Integrated OpenStack.

5 Klicken Sie auf die Registerkarte **Verwalten** und dann auf die Registerkarte **Updates**.

Auf der Registerkarte **Updates** werden hinzugefügte Patches aufgelistet und es wird angegeben, ob diese installiert wurden.

6 Wählen Sie den Patch aus und klicken Sie auf **Auswählen**.

Der neue Patch wird in der Liste auf der Registerkarte **Updates** angezeigt.

7 Installieren Sie den Patch.

Wenn Sie den Patch mit der VMware Integrated OpenStack Manager-vApp installieren können, wird die Option **Anwenden** in der Spalte „Patch-Aktion“ auf der Registerkarte **Updates** angezeigt.

Wenn die Option **Anwenden** nicht in der Spalte „Patch-Aktion“ angezeigt wird, klicken Sie in der Spalte „Patch-Beschreibung“ auf **Weitere Details**, um auf Anweisungen zum Installieren von Patches über die Befehlszeilenschnittstelle zuzugreifen.

Nach der Patch-Installation ändert sich der Wert in der Spalte „Patch-Status“ auf der Registerkarte **Updates** in „Installiert“.

8 Um das Update abzuschließen, melden Sie sich beim vSphere Web Client ab und erneut an.

Sie können alle angezeigten Fehlermeldungen ignorieren, wenn Sie sich erneut anmelden.

9 Starten Sie alle VMware Integrated OpenStack-Dienste neu.

Installieren eines Patches mit Befehlen an der Befehlszeilenschnittstelle

VMware bietet Updates in Form von Debian-Patches. Patches, die sich auf die Infrastruktur der VMware Integrated OpenStack-Bereitstellung auswirken, müssen über die Befehlskonsole für die VMware Integrated OpenStack Manager-vApp angewendet werden.

Vorgehensweise

1 Laden Sie den Debian-Patch von VMware herunter.

Wenn Sie nicht wissen, wo Sie den Patch abrufen sollen, navigieren Sie zur VMware Integrated OpenStack-Produktseite https://www.vmware.com/products/openstack oder wenden Sie sich an VMware.

2 Fügen Sie den Patch Ihrer VMware Integrated OpenStack-Installation hinzu.

a Melden Sie sich bei der Konsole für den VMware Integrated OpenStack-Verwaltungsserver an.

b Fügen Sie den Patch hinzu.

```
viopatch add –l [path to the debian file]
```

c Bestätigen Sie, dass der Patch erfolgreich hinzugefügt wurde.

```
viopatch list
```

Hiermit wird eine Liste der verfügbaren Patches mit den jeweiligen Versionsnummern, des Typs und des aktuellen Status zurückgegeben. Die Liste gibt den Patch nach Build-Nummer an.

3 Installieren Sie den Patch.

a Stellen Sie sicher, dass der VMware Integrated OpenStack-Dienst entweder ausgeführt wird oder noch nicht bereitgestellt wurde.

Wenn sich der VMware Integrated OpenStack-Dienst in einem anderen Status befindet, schlägt das Upgrade fehl.

b Melden Sie sich beim VMware Integrated OpenStack-Verwaltungsserver an und führen Sie den folgenden Befehl aus:

```
viopatch install –p <upgrade patch name> –v <upgrade patch version>
```

Die Patch-Installation dauert 5 bis 10 Minuten.

4 Um das Update abzuschließen, melden Sie sich beim vSphere Web Client ab und erneut an.

Sie können alle angezeigten Fehlermeldungen ignorieren, wenn Sie sich erneut anmelden.

5 Starten Sie alle VMware Integrated OpenStack-Dienste neu.

Bei Bedarf können Sie die vorherige Version wiederherstellen. Ausführliche Informationen finden Sie unter „Wiederherstellen der Installation eines Patch-Updates“, auf Seite 52.

Informationen zum Beheben von Fehlern bei der Patch-Installation finden Sie unter „Fehlerbehebung bei der Installation des Update-Patches“, auf Seite 53

Wiederherstellen der Installation eines Patch-Updates

Sie können den Zustand vor der Installation eines Patch-Updates wiederherstellen.

Voraussetzungen

Sie können nur eine frühere Version derselben Version wiederherstellen. Sie können zum Beispiel keine 1.0.x-Version einer 2.0-Implementierung wiederherstellen.

Vorgehensweise

1 Melden Sie sich bei der Konsole für den VMware Integrated OpenStack-Verwaltungsserver an.

2 Führen Sie den Deinstallationsbefehl aus.

viopatch uninstall --patch vio-patch-[Versionsnummer] --version [Build-Nummer]

Der Wiederherstellungsvorgang dauert 5 bis 10 Minuten.

3 Starten Sie nach dem Deinstallieren des Patches den vSphere Web Client-Dienst auf dem vCenter Server neu, um ein Downgrade des VMware Integrated OpenStack-Plug-ins durchzuführen.

Fehlerbehebung bei der Installation des Update-Patches

In diesem Abschnitt werden einige häufige Fehler bei der Installation des Update-Patches beschrieben.

Fehlerbehebung beim Fehlschlagen der Installation eines Patch-Updates

Die Patch-Installation ist fehlgeschlagen.

Problem

Nach dem Hinzufügen und Anwenden des Update-Patches schlägt die Installation fehl.

Ursache

Die Bereitstellung von VMware Integrated OpenStack muss ausgeführt werden oder noch nicht begonnen haben.

Lösung

1 Stellen Sie sicher, dass der VMware Integrated OpenStack-Dienst entweder ausgeführt wird oder noch nicht bereitgestellt wurde.

2 Wenn der Dienst ausgeführt wird, stellen Sie sicher, dass alle OpenStack-Verwaltungs-VMs (Datenbank, Lastausgleichsdienst usw.) ebenfalls ausgeführt werden.

Beheben von Fehlern bei der Installation eines Patch-Updates

Sie erhalten eine Fehlermeldung bei der Verwendung von vSphere Web Client zum Hinzufügen eines Patches.

Problem

Die Patch-Installation schlägt mit einer Meldung über einen schwerwiegenden Fehler in vSphere Web Client fehl.

Ursache

Für diesen Update-Typ ist die Verwendung der Befehlszeilenschnittstelle erforderlich, um den Patch hinzuzufügen und zu installieren.

Lösung

- Fügen Sie den Patch unter Verwendung der in „Installieren eines Patches mit Befehlen an der Befehlszeilenschnittstelle“, auf Seite 52 beschriebenen Befehlszeilenschnittstellen-Methode hinzu und installieren Sie ihn.

Anpassen von Logos und Hintergrund für das Dashboard

Standardmäßig werden auf der Anmeldeseite für das VMware Integrated OpenStack-Dashboard das Firmenlogo von VMware und ein weißer Hintergrund angezeigt. Auf allen Seiten im VMware Integrated OpenStack-Dashboard wird das Firmenlogo von VMware oben in der linken Ecke angezeigt. Sie können die Konfiguration Ihrer Bereitstellung so anpassen, dass anstelle der Standard-Grafik das Logo Ihres Unternehmens oder andere Brandings angezeigt werden.

- Die Standardmaße für die Logografik betragen 216 x 35 Pixel. Sie können eine Grafik mit anderen Maßen verwenden, wodurch jedoch u. U. die Darstellung beeinträchtigt wird.
- Die Grafik für den Hintergrund wird in der Mitte der Anmeldeseite angezeigt.

Vorgehensweise

1 Anpassen des Hintergrunds der Anmeldeseite auf Seite 54

Sie können eine benutzerdefinierte Grafik angeben, die auf der Anmeldeseite für das VMware Integrated OpenStack-Dashboard als Hintergrund angezeigt werden soll.

2 Anpassen des Logos der Anmeldeseite auf Seite 55

Sie können das benutzerdefinierte Logo angeben, das auf der Anmeldeseite für das VMware Integrated OpenStack-Dashboard angezeigt werden soll.

3 Anpassen des Logos der Dashboard-Seite auf Seite 56

Sie können das benutzerdefinierte Logo angeben, das oben in der linken Ecke auf jeder Seite im VMware Integrated OpenStack-Dashboard angezeigt wird.

Anpassen des Hintergrunds der Anmeldeseite

Sie können eine benutzerdefinierte Grafik angeben, die auf der Anmeldeseite für das VMware Integrated OpenStack-Dashboard als Hintergrund angezeigt werden soll.

Vorgehensweise

1 Laden Sie Ihre benutzerdefinierte Grafikdatei in das Verzeichnis `/home/viouser/custom/horizon/` in Ihrer VMware Integrated OpenStack-Bereitstellung.

Dies ist das Standardverzeichnis für Grafikdateien im VMware Integrated OpenStack-Dashboard.

2 Öffnen Sie die Datei `/home/viouser/custom/horizon/_styles.scss` in einem Texteditor.

a Heben Sie die Auskommentierung des Parameters `.login-bg` auf.

```
.login-bg {
  height: 100%;
  body {
    background: #1D2226 url("/static/themes/vmware/CUSTOM-BACKGROUND-IMAGE.jpg") repeat-
x 45% 0 !important;
    background-size: 100% auto !important;
    color: black;
  }
```

b Ändern Sie den Parameter `.login-bg` so, dass er auf Ihre benutzerdefinierte Grafikdatei für den Hintergrund verweist.

c Speichern Sie die Datei `_styles.scss`.

3 Implementieren Sie die Datei `custom.yml`.

```
sudo mkdir -p /opt/vmware/vio/custom
sudo cp /var/lib/vio/ansible/custom/custom.yml.sample /opt/vmware/vio/custom/custom.yml
```

4 Öffnen Sie die Datei `/opt/vmware/vio/custom/custom.yml` in einem Texteditor.

   a Heben Sie die Auskommentierung des Parameters auf, mit dem die `custom.yml`-Einstellungen die standardmäßigen Stylesheet-Einstellungen überschreiben können.

   ```
   # overwrite the _styles.scss file in the VMware theme
   horizon_custom_stylesheet: "/home/viouser/custom/horizon/_styles.scss"
   ```

   b Heben Sie die Auskommentierung des Parameters auf, der das benutzerdefinierte Verzeichnis angibt, das die benutzerdefinierte Grafikdatei enthalten soll.

   ```
   # copy all custom images (or other files) to be accessible in horizon
   # IMPORTANT: this line must end with a "/" in order to place the files
   # in the right location for horizon
   horizon_custom_directory: "/home/viouser/custom/horizon/"
   ```

   c Speichern Sie die Datei `custom.yml`.

Ihr benutzerdefiniertes Hintergrundbild wird auf der Anmeldeseite für das Dashboard angezeigt, sobald Sie das nächste Mal eine Sitzung starten.

Anpassen des Logos der Anmeldeseite

Sie können das benutzerdefinierte Logo angeben, das auf der Anmeldeseite für das VMware Integrated OpenStack-Dashboard angezeigt werden soll.

Vorgehensweise

1 Laden Sie Ihre benutzerdefinierte Grafikdatei in das Verzeichnis `/home/viouser/custom/horizon/` in Ihrer VMware Integrated OpenStack-Bereitstellung.

   Dies ist das Standardverzeichnis für Grafikdateien im VMware Integrated OpenStack-Dashboard.

2 Ändern Sie die Datei `/home/viouser/custom/horizon/_styles.scss` in einem Texteditor.

   a Heben Sie die Auskommentierung des Parameters `.login` auf.

   ```
   .login {
       background-image: url(/static/themes/vmware/CUSTOM_LOGIN_PAGE_LOGO.png);
       color: white;
       background-color: black;
   }
   ```

   b Ändern Sie den Parameter `.login` so, dass er auf Ihre benutzerdefinierte Grafikdatei verweist.

   c Speichern Sie die Datei `_styles.scss`.

3 Implementieren Sie die Datei `custom.yml`.

   ```
   sudo mkdir –p /opt/vmware/vio/custom
   sudo cp /var/lib/vio/ansible/custom/custom.yml.sample /opt/vmware/vio/custom/custom.yml
   ```

4 Öffnen Sie die Datei `/opt/vmware/vio/custom/custom.yml` in einem Texteditor.

   a Heben Sie die Auskommentierung des Parameters auf, mit dem die `custom.yml`-Einstellungen die standardmäßigen Stylesheet-Einstellungen überschreiben können.

   ```
   # overwrite the _styles.scss file in the VMware theme
   horizon_custom_stylesheet: "/home/viouser/custom/horizon/_styles.scss"
   ```

   b Heben Sie die Auskommentierung des Parameters auf, der das benutzerdefinierte Verzeichnis angibt, das die benutzerdefinierte Grafikdatei enthalten soll.

   ```
   # copy all custom images (or other files) to be accessible in horizon
   # IMPORTANT: this line must end with a "/" in order to place the files
   # in the right location for horizon
   horizon_custom_directory: "/home/viouser/custom/horizon/"
   ```

   c Speichern Sie die Datei `custom.yml`.

Ihr benutzerdefiniertes Logo wird auf der Anmeldeseite für das Dashboard angezeigt, sobald Sie das nächste Mal eine Sitzung starten.

Anpassen des Logos der Dashboard-Seite

Sie können das benutzerdefinierte Logo angeben, das oben in der linken Ecke auf jeder Seite im VMware Integrated OpenStack-Dashboard angezeigt wird.

Vorgehensweise

1 Laden Sie Ihre benutzerdefinierte Grafikdatei in das Verzeichnis `/home/viouser/custom/horizon/` in Ihrer VMware Integrated OpenStack-Bereitstellung.

   Dies ist das Standardverzeichnis für Grafikdateien im VMware Integrated OpenStack-Dashboard.

2 Ändern Sie die Datei `/home/viouser/custom/horizon/_styles.scss` in einem Texteditor.

   a Heben Sie die Auskommentierung des Parameters `.topbar` auf.

   ```
   .topbar {
     h1.brand a {
       background-image: url(/static/themes/vmware/CUSTOM_PAGE_LOGO.png);
     }
   }
   ```

   b Ändern Sie den Parameter `.topbar` so, dass er auf Ihre benutzerdefinierte Grafikdatei verweist.

   c Speichern Sie die Datei `_styles.scss`.

3 Implementieren Sie die Datei `custom.yml`.

   ```
   sudo mkdir –p /opt/vmware/vio/custom
   sudo cp /var/lib/vio/ansible/custom/custom.yml.sample /opt/vmware/vio/custom/custom.yml
   ```

4 Öffnen Sie die Datei `/opt/vmware/vio/custom/custom.yml` in einem Texteditor.

   a Heben Sie die Auskommentierung des Parameters auf, mit dem die `custom.yml`-Einstellungen die standardmäßigen Stylesheet-Einstellungen überschreiben können.

   ```
   # overwrite the _styles.scss file in the VMware theme
   horizon_custom_stylesheet: "/home/viouser/custom/horizon/_styles.scss"
   ```

   b Heben Sie die Auskommentierung des Parameters auf, der das benutzerdefinierte Verzeichnis angibt, das die benutzerdefinierte Grafikdatei enthalten soll.

   ```
   # copy all custom images (or other files) to be accessible in horizon
   # IMPORTANT: this line must end with a "/" in order to place the files
   # in the right location for horizon
   horizon_custom_directory: "/home/viouser/custom/horizon/"
   ```

   c Speichern Sie die Datei `custom.yml`.

Ihr benutzerdefiniertes Logo wird oben in der linken Ecke auf jeder Seite im Dashboard angezeigt, sobald Sie das nächste Mal eine Sitzung starten.

Ablaufverfolgung von OpenStack-Bereitstellungen mithilfe der Profilerstellung

Mithilfe der VMware Integrated OpenStack-Profilerstellungsfunktion können Sie die Ablaufverfolgung für die OpenStack-Kerndienste aktivieren. Bei aktivierter Funktion erfasst die Ablaufverfolgung die Antwortzeit aller API-, RPC-, Treiber- und Datenbankaufrufe, die Bestandteil eines OpenStack-Vorgangs sind. Sie können die Ablaufverfolgung aktivieren oder deaktivieren, ohne dass Sie OpenStack-Dienste neu starten müssen.

VMware Integrated OpenStack weist zwei Optionen zum Konfigurieren des Profilers auf. Sie können ihn zusammen mit dem Ceilometer-OpenStack-Dienst oder mit vRealize Log Insight verwenden, um Profiler-Ablaufverfolgungsdaten zu speichern.

Vorgehensweise

1 Konfigurieren der Ablaufverfolgung von OpenStack-Diensten auf Seite 57

   Konfigurieren Sie die VMware Integrated OpenStack-Profilerstellungsfunktion, indem Sie Datei `custom.yml` ändern.

2 Verwenden der Ablaufverfolgung von OpenStack-Diensten auf Seite 59

   Verwenden Sie die VMware Integrated OpenStack-Profilerstellung zum Erfassen der Antwortzeit aller API-, RPC-, Treiber- und Datenbankaufrufe, die Bestandteil eines OpenStack-Vorgangs sind.

Konfigurieren der Ablaufverfolgung von OpenStack-Diensten

Konfigurieren Sie die VMware Integrated OpenStack-Profilerstellungsfunktion, indem Sie Datei `custom.yml` ändern.

VMware Integrated OpenStack weist zwei Optionen zum Konfigurieren des Profilers auf. Sie können ihn zusammen mit dem Ceilometer-OpenStack-Dienst oder mit vRealize Log Insight verwenden, um Profiler-Ablaufverfolgungsdaten zu speichern.

Voraussetzungen

- Um vRealize Log Insight zum Speichern von Profiler-Ablaufverfolgungsdaten zu verwenden, stellen Sie sicher, dass Ihre Instanz voll funktionsfähig ist, Version 3.3 oder einer neueren Version entspricht und dass Sie sich mit einem Benutzernamen mit zugewiesener Rolle `USER` authentifizieren können.

- Um den `Ceilometer OpenStack`-Dienst zum Speichern von Profiler-Ablaufverfolgungsdaten zu verwenden, stellen Sie sicher, dass der Dienst ausgeführt wird.

Vorgehensweise

1 Ändern Sie die Datei `custom.yml`, um die Ablaufverfolgung zu aktivieren.

a Falls nicht bereits geschehen, implementieren Sie die Datei `custom.yml`.

```
sudo mkdir –p /opt/vmware/vio/custom
sudo cp /var/lib/vio/ansible/custom/custom.yml.sample /opt/vmware/vio/custom/custom.yml
```

b Bearbeiten Sie die Datei `custom.yml`, indem Sie die Auskommentierung von Parametern aufheben und die Parameter ändern.

- Wenn Sie `Ceilometer OpenStack` verwenden, heben Sie die Auskommentierung der folgenden Parameter auf und ändern Sie die Parameter.

```
os_profiler_enabled: True
os_profiler_hmac_keys: SECRET_KEY
```

- Wenn Sie vRealize Log Insight verwenden, heben Sie die Auskommentierung der folgenden Parameter auf und ändern Sie die Parameter.

```
os_profiler_enabled: True
os_profiler_hmac_keys: SECRET_KEY
os_profiler_connection_string: "loginsight://loginsight_username:password@login-
sight_ip_address"
```

Parameter	Beschreibung
`os_profiler_enabled`	Übernehmen Sie den Standardwert. Mit der Einstellung **`True`** ist die OpenStack-Profilerstellung aktiviert.
`os_profiler_hmac_keys`	Geben Sie den Sicherheitsschlüssel an. Dieser Schlüssel muss immer dann angegeben werden, wenn ein Administrator eine Ablaufverfolgung ausführt.
`os_profiler_connection_string`	Geben Sie die Authentifizierung für den vRealize Log Insight-Server an. Geben Sie dazu den Benutzernamen, das Kennwort und die Adresse der Instanz an.

2 Übertragen Sie die neue Konfiguration auf Ihre VMware Integrated OpenStack-Bereitstellung.

```
viocli deployment configure
```

Hinweis Die Bereitstellung der Konfiguration im Push-Verfahren führt zu einer kurzen Unterbrechung der OpenStack-Dienste.

3 Wenn Sie vRealize Log Insight zum Speichern von Profiler-Ablaufverfolgungsdaten verwenden, legen Sie die Umgebungsvariable `OSPROFILER_CONNECTION_STRING` fest, damit Sie die Verbindungszeichenfolge nicht bei jeder Ausführung von Befehlen mit aktivierter Profilerstellung eingeben müssen.

Sie müssen die Variable auf allen VMware Integrated OpenStack-Controllern festlegen, auf denen Sie Befehle ausführen möchten.

```
export OSPROFILER_CONNECTION_STRING="loginsight://loginsight_username:password@login-
sight_ip_address"
```

Nun können Sie die Profilerstellungsfunktion verwenden.

Verwenden der Ablaufverfolgung von OpenStack-Diensten

Verwenden Sie die VMware Integrated OpenStack-Profilerstellung zum Erfassen der Antwortzeit aller API-, RPC-, Treiber- und Datenbankaufrufe, die Bestandteil eines OpenStack-Vorgangs sind.

VMware Integrated OpenStack unterstützt derzeit die Profilerstellung für Cinder-, Heat-, Glance-, Nova- und Neutron-Befehle.

Voraussetzungen

- Stellen Sie sicher, dass Sie die Umgebungsvariable `OSPROFILER_CONNECTION_STRING` auf dem Controller festgelegt haben, auf dem Sie eine Ablaufverfolgung der OpenStack-Dienste ausführen werden. Weitere Informationen finden Sie unter „Konfigurieren der Ablaufverfolgung von OpenStack-Diensten“, auf Seite 57.

Vorgehensweise

1. Aktivieren Sie die Profilerstellung durch Angeben der Option `profile` für einen bestimmten Befehl und Eingeben des geheimen Schlüssels.

   ```
   cinder --profile YOUR_SECRET_KEY list
   ```

   Die Ausgabe weist einen Befehl auf, den Sie zum Generieren des Profilerstellungsberichts im HTML-Format verwenden.

2. Führen Sie den generierten Befehl aus der Ausgabe aus, um einen Bericht zu generieren, wie beispielsweise `trace.html`.

   ```
   osprofiler trace show --html <UUID>  > trace.html
   ```

   Weitere Informationen zu den verschiedenen Optionen für den Bericht finden Sie in der Hilfe zum Befehl `osprofiler trace show`.

   ```
   osprofiler trace show --help
   ```

Verwalten von OpenStack-Projekten und -Benutzern 3

In VMware Integrated OpenStack verwalten Cloud-Administratoren Berechtigungen über Benutzer-, Gruppen- und Projektdefinitionen. Projekte in OpenStack entsprechen Mandanten in vCloud Suite. Sie können Benutzer und Benutzergruppen zu mehr als einem Projekt zuweisen.

Bevor Sie einen Benutzer erstellen können, müssen Sie mindestens ein Projekt erstellen, dem Sie den Benutzer zuweisen können.

Dieses Kapitel behandelt die folgenden Themen:

Erstellen eines OpenStack-Projekts

Projekte sind die Entsprechung von Mandanten oder Konten. Sie funktionieren als Organisationseinheiten in der Cloud, denen Sie Benutzer zuweisen können.

Voraussetzungen

Stellen Sie sicher, dass Sie beim VMware Integrated OpenStack-Dashboard als Cloud-Administrator angemeldet sind.

Vorgehensweise

1 Wählen Sie das Administratorprojekt aus dem Dropdown-Menü in der Titelleiste aus.

2 Wählen Sie **Administrator > Identität > Projekte** aus.

3 Klicken Sie auf **Projekt erstellen**.

4 Klicken Sie auf die Registerkarte **Projektinformationen** und konfigurieren Sie die Projekteinstellungen.

Einstellung	Beschreibung
Name	Projektname.
Beschreibung	Optionale Beschreibung des neuen Projekts.
Aktiviert	Neue Projekte werden standardmäßig aktiviert. Wenn ein Projekt deaktiviert wird, können Benutzer nicht auf das Projekt zugreifen und keine Startinstanzen für das Projekt verwalten. Zudem kann eine Deaktivierung dazu führen, dass Benutzer sich nicht anmelden können, wenn sie nur diesem Projekt zugewiesen sind.

5 (Optional) Fügen Sie dem Projekt Mitglieder hinzu, indem Sie auf der Registerkarte **Projektmitglieder** vorhandene Cloud-Benutzer auswählen.

6 (Optional) Fügen Sie dem Projekt Mitgliedergruppen hinzu, indem Sie auf der Registerkarte **Projektgruppen** vorhandene Cloud-Benutzergruppen auswählen.

7 Akzeptieren oder ändern Sie auf der Registerkarte **Kontingent** die Kontingenteinstellungen.

   Kontingente sind Grenzwerte für den Betrieb, die Sie konfigurieren können, um die für ein bestimmtes Projekt verfügbaren Systemressourcen festzulegen. Sie können beispielsweise die Cloud-Ressourcen optimieren, indem Sie die für jeden Mandanten zulässige Anzahl von Gigabyte beschränken. Kontingente können auf Projekt- und auf Benutzerebene erzwungen werden.

8 Klicken Sie unten im Fensterbereich auf **Projekt erstellen**.

Das VMware Integrated OpenStack-Dashboard weist dem neuen Projekt eine ID zu und das Projekt wird auf der Seite „Projekte“ aufgelistet.

Ändern eines Projekts

Sie können ein Projekt aktualisieren, um dessen Namen oder Beschreibung zu ändern. Zudem können Sie ein Projekt aktivieren oder vorübergehend deaktivieren.

Wichtig Die Deaktivierung eines Projekts kann negative Auswirkungen haben. Wenn ein Benutzer beispielsweise nur diesem Projekt zugewiesen ist, kann er sich nicht beim VMware Integrated OpenStack-Dashboard anmelden. Auch können die Mitglieder des Projekts nicht auf das Projekt zugreifen. Projektinstanzen werden weiterhin ausgeführt, Sie müssen sie also manuell anhalten oder beenden. Projektdaten werden für den Fall der erneuten Aktivierung des Projekts beibehalten.

Voraussetzungen

Stellen Sie sicher, dass Sie beim VMware Integrated OpenStack-Dashboard als Cloud-Administrator angemeldet sind.

Vorgehensweise

1 Wählen Sie im VMware Integrated OpenStack-Dashboard das Administratorprojekt aus dem Dropdown-Menü in der Titelleiste aus.

2 Wählen Sie **Administrator > Identität > Projekte** aus.

3 Wählen Sie das zu bearbeitende Projekt aus.

4 Wählen Sie in der Spalte „Aktionen“ **Projekt bearbeiten** aus dem Dropdown-Menü aus.

   Im Dialogfeld „Projekt bearbeiten“ können Sie den Namen und die Beschreibung des Projekts ändern und es aktivieren bzw. deaktivieren.

5 Ändern Sie die Projekteinstellungen und klicken Sie auf **Speichern**.

6 (Optional) Um die Benutzerzuweisungen für ein Projekt zu ändern, klicken Sie auf der Seite „Projekte“ für das zu ändernde Projekt auf **Mitglieder verwalten**.

Option	Aktion
Zuweisen eines Benutzers zum aktuellen Projekt	Klicken Sie auf das Pluszeichen (+) für den Benutzer.
Entfernen eines Benutzers aus dem aktuellen Projekt	Klicken Sie auf das Minuszeichen (-) für den Benutzer.

7 Klicken Sie auf **Speichern**.

8 Um ein oder mehrere Projekte zu löschen, kehren Sie zur Seite „Projekte“ zurück und wählen Sie die zu löschenden Projekte aus.

Hinweis Sie können ein gelöschtes Projekt nicht wiederherstellen.

a Klicken Sie auf **Projekte löschen**.

b Bestätigen Sie den Löschvorgang an der Eingabeaufforderung.

Arbeiten mit Sicherheitsgruppen

Eine Sicherheitsgruppe ist eine Gruppe von IP-Filterregeln, die den Netzwerkzugriff definieren und auf alle Instanzen in einem Projekt angewendet werden können. Gruppenregeln sind projektspezifisch. Projektmitglieder können die Standardregeln für ihre Gruppe bearbeiten und neue Regelsätze hinzufügen.

Sie können Sicherheitsgruppen zum Anwenden von IP-Regeln verwenden, indem Sie eine neue Sicherheitsgruppe mit den gewünschten Regeln erstellen oder den Regelsatz in der Standardsicherheitsgruppe ändern.

Hinweis Eine Sicherheitsgruppe kann entweder Regeln oder eine Sicherheitsrichtlinie anwenden, aber nicht beides.

Grundlegende Informationen zur Standardsicherheitsgruppe

Alle Projekte in VMware Integrated OpenStack verfügen über eine Standardsicherheitsgruppe, die für eine Instanz angewendet wird (es sei denn, eine andere Sicherheitsgruppe wurde definiert und angegeben). Wenn keine Änderungen vorgenommen wurden, lässt die Standardsicherheitsgruppe nur ausgehenden Datenverkehr für Ihre Instanz zu, aber keinen eingehenden Datenverkehr. Häufig wird die Standardsicherheitsgruppe bearbeitet, sodass sich Benutzer über den SSH-Zugriff und ICMP-Zugriff anmelden und Instanzen anpingen können.

Erstellen einer Sicherheitsgruppe

Sicherheitsgruppen sind Gruppen von IP-Filterregeln, die den Netzwerkzugriff definieren und auf alle Instanzen in einem Projekt angewendet werden. Sie können diese Regeln in der Sicherheitsgruppe entweder ändern oder eine Sicherheitsgruppe mit benutzerdefinierten Regeln erstellen.

Informationen zum Ändern einer vorhandenen Regel für eine Sicherheitsgruppe finden Sie unter „Ändern der Regeln für eine vorhandene Sicherheitsgruppe“, auf Seite 64.

Vorgehensweise

1 Melden Sie sich beim VMware Integrated OpenStack-Dashboard als ein Cloud-Administrator an.

2 Wählen Sie das Projekt aus dem Dropdown-Menü in der Titelleiste aus.

3 Wählen Sie **Projekt > Berechnen > Zugriff und Sicherheit** aus.

4 Klicken Sie auf die Registerkarte **Sicherheitsgruppen**.

5 Klicken Sie auf **Sicherheitsgruppe erstellen**.

6 Geben Sie einen Namen und eine Beschreibung für die neue Gruppe ein und klicken Sie auf **Sicherheitsgruppe erstellen**.

Die neue Gruppe wird in der Liste auf der Registerkarte **Sicherheitsgruppe** angezeigt.

7 Konfigurieren Sie Regeln für die neue Gruppe.

a Wählen Sie die neue Sicherheitsgruppe aus und klicken Sie auf **Regeln verwalten**.

b Klicken Sie auf **Regel hinzufügen**.

c Wählen Sie im Dropdown-Menü **Regel** die hinzuzufügende Regel aus.

Die nachfolgenden Felder können sich je nach der von Ihnen ausgewählten Regel ändern.

d Falls anwendbar, geben Sie **Eingang** oder **Ausgang** im Dropdown-Menü **Richtung** an.

e Klicken Sie nach Abschluss der Regeldefinition auf **Hinzufügen**.

8 Konfigurieren Sie bei Bedarf weitere Regeln.

9 Klicken Sie auf die Registerkarte **Zugriff und Sicherheit**, um zur Hauptseite zurückzukehren.

Ändern der Regeln für eine vorhandene Sicherheitsgruppe

Sie können eine Sicherheitsgruppe ändern, indem Sie dieser Gruppe zugewiesene Regeln hinzufügen und entfernen. Regeln definieren, welcher Datenverkehr für Instanzen zulässig ist, die der Sicherheitsgruppe zugewiesen sind.

Vorgehensweise

1 Melden Sie sich beim VMware Integrated OpenStack-Dashboard als ein Cloud-Administrator an.

2 Wählen Sie das Projekt aus dem Dropdown-Menü in der Titelleiste aus.

3 Wählen Sie **Projekt > Berechnen > Zugriff und Sicherheit** aus.

4 Klicken Sie auf die Registerkarte **Sicherheitsgruppen**.

5 Wählen Sie die zu ändernde Sicherheitsgruppe aus und klicken Sie auf **Regeln verwalten**.

6 Um eine Regel zu entfernen, wählen Sie die Regel aus und klicken Sie auf **Regel löschen**.

7 Um eine Regel hinzuzufügen, klicken Sie auf **Regel hinzufügen** und wählen Sie die benutzerdefinierte Regel aus dem Dropdown-Menü **Regel** aus.

Option	Beschreibung
Benutzerdefinierte TCP-Regel	Wird für den Austausch von Daten zwischen Systemen und für die Endbenutzerkommunikation verwendet.
Benutzerdefinierte UDP-Regel	Wird für den Austausch von Daten zwischen Systemen verwendet, zum Beispiel auf der Anwendungsebene.
Benutzerdefinierte ICMP-Regel	Wird von Netzwerkgeräten, zum Beispiel Routern, zum Senden von Fehler- oder Überwachungsmeldungen verwendet.
Anderes Protokoll	Sie können eine Regel manuell konfigurieren, wenn das Regelprotokoll nicht in der Liste enthalten ist.

a Wählen Sie in der Dropdown-Liste **Remote** den Eintrag **CIDR** oder **Sicherheitsgruppe** aus.

b Wählen Sie, sofern zutreffend, den Eintrag **Eingang** oder **Ausgang** aus dem Dropdown-Menü **Richtung** aus.

Für TCP- und UDP-Regeln können Sie entweder einen einzelnen Port oder einen Portbereich auswählen. Je nach Auswahl werden unter der Liste „Port öffnen“ verschiedene Felder angezeigt.

c Wählen Sie den erlaubten Zugriffstyp aus.

Option	Beschreibung
CIDR (Classless Inter-Domain Routing)	Beschränkt den Zugriff nur auf IP-Adressen innerhalb des angegebenen Blocks.
Sicherheitsgruppe	Ermöglicht allen Instanzen in der angegebenen Sicherheitsgruppe den Zugriff auf jede andere Gruppeninstanz. In der Ethertyp-Liste können Sie IPv4 oder IPv6 auswählen.

8 Klicken Sie auf **Hinzufügen**.

Die neue Regel wird auf der Seite „Sicherheitsgruppenregeln verwalten“ für die Sicherheitsgruppe angezeigt.

Aktivieren von SSH- und ICMP-Zugriff

Sie können die Standardsicherheitsgruppe ändern, um SSH- und ICMP-Zugriff für Instanzen zu aktivieren. Die Regeln in der Standardsicherheitsgruppe gelten für alle Instanzen im aktuell ausgewählten Projekt.

Vorgehensweise

1 Melden Sie sich beim VMware Integrated OpenStack-Dashboard als ein Cloud-Administrator an.

2 Wählen Sie das Projekt aus dem Dropdown-Menü in der Titelleiste aus.

3 Wählen Sie **Projekt > Berechnen > Zugriff und Sicherheit** aus.

4 Klicken Sie auf die Registerkarte **Sicherheitsgruppen**, wählen Sie die Standardsicherheitsgruppe aus und klicken Sie auf **Regeln verwalten**.

5 Klicken Sie auf **Regel hinzufügen** und konfigurieren Sie die Regeln für den SSH-Zugriff.

Steuerung	Wert
Regel	SSH
Remote	CIDR
CIDR	0.0.0.0/0

Um Anforderungen eines bestimmten IP-Adressbereichs zu akzeptieren, geben Sie den IP-Adressblock im CIDR-Textfeld an.

Der SSH-Port 22 der Instanzen ist jetzt für Anforderungen einer beliebigen IP-Adresse geöffnet.

6 Klicken Sie auf **Hinzufügen**.

7 Klicken Sie auf der Seite „Sicherheitsgruppenregeln verwalten“ auf **Regel hinzufügen** und konfigurieren Sie die Regeln für den ICMP-Zugriff.

Steuerung	Wert
Regel	Alle ICMP
Richtung	Eingang
Remote	CIDR
CIDR	0.0.0.0/0

8 Klicken Sie auf **Hinzufügen**.

Instanzen akzeptieren jetzt alle eingehenden ICMP-Pakete.

Verwenden der VMware NSX for vSphere -Sicherheitsrichtlinien über Sicherheitsgruppen

Mit dieser Funktion wird der Verbrauch der VMware NSX for vSphere -Richtlinie aus der OpenStack-Cloud-Verwaltungsplattform über OpenStack-Sicherheitsgruppen aktiviert. Der NSX-Administrator kann Sicherheitsrichtlinien definieren, die der OpenStack-Cloudadministrator für Cloudbenutzer freigibt. Die Cloudbenutzer können auch ihre eigenen Sicherheitsgruppen mit Regeln definieren, wenn der Cloudadministrator reguläre Sicherheitsgruppen aktiviert. Diese Funktion kann auch von Cloudadministratoren verwendet werden, um Netzwerkdienste von Drittanbietern einzufügen.

Ab VMware Integrated OpenStack 3.1 können Administratoren mit Neutron-Sicherheitsgruppen zwei neue Funktionalitäten verwenden.

Anbietersicherheitsgruppen
Diese Sicherheitsgruppen sind, wenn sie konfiguriert sind, verpflichtend und gelten für alle VMs eines bestimmten Mandanten. Die Sicherheitsgruppen sind auch als Administratorregeln bekannt. Eine Anbietersicherheitsgruppe kann mit einer Richtlinie verbunden werden oder ohne eine Richtlinie vorhanden sein.

Sicherheitsgruppen von NSX Service Composer – Sicherheitsrichtlinie
Weitere Informationen finden Sie im Kapitel *Service Composer* im *VMware NSX for vSphere -Administratorhandbuch*.

Jede Richtlinie von VMware NSX for vSphere kann vom OpenStack-Cloudadministrator als Standardrichtlinie durch Festlegen der Option `nsxv_default_policy_id` in der `custom.yml`-Datei definiert werden. Alle neuen Mandanten verfügen über diese Richtlinie als Standardrichtlinie. Weitere Richtlinien können definiert und als erforderlich oder optional für einen bestimmten Mandanten zugewiesen werden, indem sie entweder mit dem Anbieter oder optionalen Sicherheitsgruppen verbunden werden. Mandantenbenutzer können auch Sicherheitsgruppen mit Regeln erstellen, sie können jedoch keine vom Cloudadministrator festgelegten Sicherheitsgruppen überschreiben.

Nach der Aktivierung von VMware NSX for vSphere -Richtlinien können Cloudadministratoren verschiedene Szenarios konfigurieren.

1. Cloudadministratoren können die Erstellung regulärer Sicherheitsgruppen mit unterschiedlichen Optionen untersagen.
   - Wenn nur eine standardmäßige Sicherheitsgruppe vorhanden ist, ist diese mit der Standardrichtlinie verbunden. Mandanten-VMs werden mit den in der Standardrichtlinie definierten Regeln erzwungen.
   - Wenn der Cloudadministrator eine Sicherheitsgruppe mit einer unterschiedlichen Richtlinie erstellt, können Mandanten-VMs mit dieser Sicherheitsgruppe anstatt der standardmäßigen Sicherheitsgruppe verbunden werden. Nur die in der aktuellen Richtlinie definierten Regeln sind gültig.
   - Wenn zusätzlich zu den Richtlinienregeln Anbietersicherheitsgruppen vorhanden sind, werden Mandanten-VMs auch mit den in den Anbietersicherheitsgruppen definierten Regeln erzwungen.
2. Cloudadministratoren können die Erstellung regulärer Sicherheitsgruppen mit unterschiedlichen Optionen zulassen.
   - Mit benutzerdefinierten regulären Sicherheitsgruppen gestartete VMs werden nur mit den in diesen Sicherheitsgruppen definierten Regeln erzwungen.
   - Wenn zusätzlich zu den Regeln in der regulären Sicherheitsgruppe eine Anbietersicherheitsgruppe vorhanden ist, werden Mandanten-VMs auch mit den in den Anbietersicherheitsgruppen definierten Regeln erzwungen. In diesem Fall haben Regeln der Anbietersicherheitsgruppen Vorrang gegenüber regulären Sicherheitsgruppenregeln. Ebenso haben richtlinienbasierte Regeln Vorrang, wenn Sie richtlinienbasierte Sicherheitsgruppen mit regulären Sicherheitsgruppen verwenden.

- Sie können über Sicherheitsgruppen mit einer Richtlinie oder Regeln verfügen, nicht aber mit beidem.

Verwalten der Sicherheitsgruppen von NSX Service Composer – Sicherheitsrichtlinie über CLI-Befehle

Cloudadministratoren können auch die Verbindung der Sicherheitsgruppenrichtlinie unter Verwendung von CLI-Befehlen über den Integrated OpenStack Manager ändern.

Aktion	Befehlsbeispiel
Ändern der verbundenen Richtlinie für eine Sicherheitsgruppe	`neutron security-group-update --policy=<NSX_Policy_ID> <SECURITY_GROUP_ID>`
Migrieren der vorhandenen Sicherheitsgruppen zu richtlinienbasierten Sicherheitsgruppen unter Verwendung des `nsxadmin`-Hilfsprogramms. **Hinweis** Mit dieser Aktion werden vorhandene, vom Benutzer definierte Regeln gelöscht. Stellen Sie sicher, dass Sie über die entsprechenden Regeln in der Richtlinie verfügen, um eine Netzwerkunterbrechung zu vermeiden.	`nsxadmin -r security-groups -o migrate-to-policy --property policy-id=<NSX_Policy_ID> --property security-group-id=<SECURITY_GROUP_ID>`
Erzwingen von Anbietersicherheitsgruppen auf vorhandenen VM-Ports	`neutron port-update <PORT_ID> --provider-security-groups list=true <SECURITY_GROUP_ID1> <SECURITY_GROUP_ID2>`
Stellen Sie sicher, dass eine neue, auf der NSX-Seite erstellte Richtlinie vor dem Abschnitt mit allen OpenStack-Sicherheitsgruppen platziert wird. Verwenden Sie dazu das `nsxadmin`-Hilfsprogramm. **Hinweis** Wenn mehr als eine richtlinienbasierte Sicherheitsgruppe auf einer VM/auf einem Port erzwungen wird, wird die Reihenfolge, in der die Richtlinienregeln erzwungen werden, vom NSX-Administrator über den Abschnitt „Firewall“ gesteuert.	`sudo -u neutron nsxadmin --config-file /etc/neutron/neutron.conf --config-file /etc/neutron/plugins/vmware/nsxv.ini -r firewall-sections -o nsx-reorder`

- Aktivieren der Sicherheitsrichtlinien von VMware NSX for vSphere in Neutron auf Seite 67

  Sie aktivieren die Sicherheitsrichtlinien von VMware NSX for vSphere in Neutron durch Verändern der `custom.yml`-Datei.

- Ändern der Sicherheitsrichtlinie in einer Sicherheitsgruppe auf Seite 68

  Sie können die Sicherheitsrichtlinie ändern, die mit einer Sicherheitsgruppe verbunden ist.

Aktivieren der Sicherheitsrichtlinien von VMware NSX for vSphere in Neutron

Sie aktivieren die Sicherheitsrichtlinien von VMware NSX for vSphere in Neutron durch Verändern der `custom.yml`-Datei.

Darüber hinaus müssen Sie die standardmäßige Sicherheitsrichtlinie für die Standardsicherheitsgruppe für einen neuen Mandanten festlegen. Optional können Sie zulassen oder untersagen, dass Mandanten eigene Richtlinien erstellen können.

Vorgehensweise

1 Melden Sie sich beim OpenStack Management Server an.

2 Erstellen Sie die `custom.yml`-Datei, wenn sie nicht vorhanden ist.

```
sudo mkdir -p /opt/vmware/vio/custom
sudo cp /var/lib/vio/ansible/custom/custom.yml.sample
/opt/vmware/vio/custom/custom.yml
```

3 Öffnen Sie die Datei `/opt/vmware/vio/custom/custom.yml` in einem Texteditor.

4 Erstellen Sie Sicherheitsrichtlinien in Neutron unter Verwendung der VIO-Anpassung durch Bearbeiten der `custom.yml`-Datei gemäß Ihrer Konfiguration.

   a Heben Sie die Auskommentierung des Werts `nsxv_use_nsx_policies` auf und ändern Sie ihn zu **`true`**, legen Sie die erforderliche Standardrichtlinie für Mandanten `nsxv_default_policy_id` fest und lassen Sie zu bzw. untersagen Sie, dass Mandanten eigene Richtlinien `nsxv_allow_tenant_rules_with_policy: false` erstellen können, beispielsweise:

```
# Configure neutron security groups to use NSX policies
nsxv_use_nsx_policies: true
# (Optional) If use_nsx_policies is true, this policy will be used as the
# default policy for new tenants.
nsxv_default_policy_id: <YOUR_NSX_POLICY_ID>
# (Optional) If use_nsx_policies is True, this value will determine if the
# tenants can add rules to their security groups.
nsxv_allow_tenant_rules_with_policy: false
```

   b Speichern Sie die Datei `custom.yml`.

5 Übertragen Sie die neue Konfiguration auf Ihre VMware Integrated OpenStack-Bereitstellung.

   Die Aktualisierung der Konfiguration unterbricht kurz die OpenStack-Dienste.

```
viocli deployment configure
```

Ändern der Sicherheitsrichtlinie in einer Sicherheitsgruppe

Sie können die Sicherheitsrichtlinie ändern, die mit einer Sicherheitsgruppe verbunden ist.

Sie führen das Verfahren über einen VMware Integrated OpenStack-Controller aus.

Voraussetzungen

Vorgehensweise

1 Melden Sie sich beim OpenStack Management Server an.

2 Rufen Sie eine Liste der derzeit definierten Sicherheitsgruppen ab.

   Sie benötigen die `id` einer Sicherheitsgruppe, um deren Konfiguration anzuzeigen.

```
neutron-security-group-list
```

3 Rufen Sie die Konfiguration einer Sicherheitsgruppe ab.

   Verwenden Sie die `id` aus dem vorherigen Schritt.

```
neutron-security-group-show <SECURITY_GROUP_ID>
```

   In der Ausgabe können Sie die mit dieser Sicherheitsgruppe verbundene `policy` anzeigen.

4 Tauschen Sie die aktuelle Richtlinie einer Sicherheitsgruppe mit einer anderen Richtlinien aus.

```
neutron security-group-update --policy=<NSX_Policy_ID> <SECURITY_GROUP_ID>
```

Sie haben die verbundene Sicherheitsrichtlinie zu einer bestimmten Sicherheitsgruppe geändert.

Erstellen eines Cloud-Benutzerkontos in OpenStack

Cloud-Benutzer verfügen im Vergleich zu Cloud-Administratoren über einen eingeschränkten Satz an Zugriffsrechten und Berechtigungen. Cloud-Benutzer sind auf die Mandanten beschränkt, denen sie zugewiesen sind. Mandanten werden in OpenStack Projekte genannt. Cloud-Benutzer können unter anderem Instanzen erstellen und verwalten, Datenträger erstellen und verwalten, Netzwerke erstellen und neue Images erstellen.

Voraussetzungen

- Stellen Sie sicher, dass Sie beim VMware Integrated OpenStack-Dashboard als Cloud-Administrator angemeldet sind.
- Stellen Sie sicher, dass ein konfiguriertes OpenStack-Projekt verfügbar ist. Siehe „Erstellen eines OpenStack-Projekts“, auf Seite 61.

VMware Integrated OpenStack unterstützt jetzt Keystone-Backends mit mehreren Domänen:

- Jede Domäne kann ein separates Backend aufweisen.
- Die Domäne *lokal* enthält jetzt die Dienstbenutzer, vioservice-Benutzer und Admin-Benutzer. Diese Domäne wird von SQL unterstützt. Die Domäne *Standard* enthält entweder die Standardbenutzer (bei Verwendung von SQL) oder die LDAP-Benutzer (bei Konfiguration von AD). Der Einfachheit halber ist der Admin-Benutzer auch für die *Standard*-Domäne verfügbar.
- Neben dem Domänenkontext in Horizon müssen Sie auch in der Befehlszeilenschnittstelle eine Domäne angeben, wenn Sie nicht die Standard-Domäne verwenden. OpenStack-Befehlszeilen verwenden standardmäßig immer die Standard-Domäne.
- Beim Anmelden am Dashboard werden Benutzer nun aufgefordert, einen Domänennamen einzugeben. Um sich erfolgreich anzumelden, müssen sie „Standard“ als Domänennamen eingeben.

Vorgehensweise

1 Wählen Sie im VMware Integrated OpenStack-Dashboard das Administratorprojekt aus dem Dropdown-Menü in der Titelleiste aus.

2 Wählen Sie **Administrator > Identitätsfenster > Benutzer** aus.

3 Klicken Sie auf **Benutzer erstellen**.

Das Dialogfeld „Benutzer erstellen“ wird angezeigt.

4 Stellen Sie sicher, dass das Feld „Domänen-ID“ auf Standard eingestellt ist und der Domänenname Standard lautet.

Benutzer müssen den richtigen Domänennamen eingeben, um sich erfolgreich am VMware Integrated OpenStack-Dashboard anzumelden.

5 Konfigurieren Sie die Benutzereinstellungen.

Option	Beschreibung
Benutzername	Cloud-Benutzername.
E-Mail	Gültige E-Mail-Adresse für den neuen Benutzer.
Kennwort/Kennwort bestätigen	Vorläufiges Kennwort für den neuen Benutzer.
Primäres Projekt	Projekt, dem der Benutzer zugewiesen ist. Sie können ein Benutzerkonto nur erstellen, wenn Sie es mindestens einem Projekt zuweisen.

Option	Beschreibung
Rolle	Rolle, der der Benutzer zugewiesen ist. Eine Rolle ist ein Satz an Zugriffsrechten und Berechtigungen. Ein Benutzer mit einer bestimmten Rolle verfügt über die entsprechenden Zugriffsrechte und Berechtigungen.
Aktivieren	Um den Benutzer zu aktivieren, wählen Sie das Kontrollkästchen **Aktivieren** aus. Um den Benutzer zu einem späteren Zeitpunkt zu aktivieren, lassen Sie das Kontrollkästchen **Aktivieren** deaktiviert.

6 Klicken Sie unten im Fensterbereich auf **Benutzer erstellen**.

Das VMware Integrated OpenStack-Dashboard weist dem Benutzer eine ID zu und der Benutzer wird jetzt auf der Seite „Benutzer“ angezeigt.

Ändern eines Benutzerkontos

Als Cloud-Administrator können Sie Benutzerkonten aktivieren, deaktivieren und löschen sowie Kennwörter ändern.

Voraussetzungen

Stellen Sie sicher, dass Sie beim VMware Integrated OpenStack-Dashboard als Cloud-Administrator angemeldet sind.

Vorgehensweise

1 Wählen Sie im VMware Integrated OpenStack-Dashboard das Administratorprojekt aus dem Dropdown-Menü in der Titelleiste aus.

2 Wählen Sie **Identität > Benutzer** aus.

Option	Aktion
Aktivieren oder deaktivieren Sie ein Benutzerkonto.	a Wählen Sie das Benutzerkonto aus, das Sie bearbeiten möchten. b Klicken Sie in der Spalte „Aktionen“ auf **Bearbeiten** und wählen Sie im Dropdown-Menü **Benutzer aktivieren** oder **Benutzer deaktivieren** aus.
Löschen Sie mindestens ein Benutzerkonto.	a Wählen Sie die Benutzerkonten aus, die Sie löschen möchten. b Klicken Sie auf **Benutzer löschen**. c Bestätigen Sie den Löschvorgang an der Eingabeaufforderung.
Ändern Sie ein Kennwort.	a Wählen Sie das Benutzerkonto aus, das Sie bearbeiten möchten. b Klicken Sie in der Spalte „Aktionen“ auf **Bearbeiten** und wählen Sie **Kennwort ändern** aus. c Ändern Sie das Kennwort nach Bedarf.

Arbeiten mit Instanzen in OpenStack 4

Instanzen sind virtuelle Maschinen, die in der Cloud ausgeführt werden.

Als Cloud-Administrator können Sie Instanzen für Benutzer in verschiedenen Projekten verwalten. Sie können einen weichen oder harten Neustart anzeigen, beenden, bearbeiten und ausführen, einen Snapshot von Instanzen erstellen und Instanzen migrieren. Zudem können Sie die Protokolle für Instanzen anzeigen oder eine VNC-Konsole für eine Instanz erstellen.

Informationen zur Verwendung des Dashboards zum Starten von Instanzen als Endbenutzer finden Sie im *Benutzerhandbuch für VMware Integrated OpenStack*.

Dieses Kapitel behandelt die folgenden Themen:

Importieren von VMs aus vSphere in VMware Integrated OpenStack

Sie können VMs aus vSphere in Ihre VMware Integrated OpenStack-Bereitstellung importieren und wie OpenStack-Instanzen verwalten.

Sie importieren VMs über die Datencenter-Befehlszeilenschnittstelle (Datacenter Command Line Interface, DCLI), die sich im selben Paket befindet wie der VMware Integrated OpenStack-Verwaltungsserver und vom Anbieter der VMware Integrated OpenStack-vAPI betrieben wird.

Obwohl importierte VMs zu OpenStack-Instanzen werden, unterscheiden sie sich weiterhin in einigen Punkten:

- Wenn die importierte VM mehrere Festplatten aufweist:
  - Die Erstellung von Nova-Snapshots wird nicht unterstützt.
  - Die Größenanpassung mit Nova wird nicht unterstützt.

- Bestehende Netzwerke werden als Portgruppe vom Typ Anbieternetzwerk importiert. Dabei werden Subnetze mit deaktiviertem DHCP erstellt. Dadurch werden Konflikte zwischen dem DHCP-Knoten in OpenStack und dem externen DHCP-Server vermieden.

  Hinweis Wenn der DHCP-Server bei der Leaseerneuerung nicht dieselbe IP-Adresse behalten kann, wird unter den Instanzinformationen in OpenStack die falsche IP-Adresse angezeigt. Aus diesem Grund empfiehlt es sich, dass Sie statische DHCP-Bindungen auf bestehenden DHCP-Servern verwenden. Zudem empfiehlt es sich, neue OpenStack-Instanzen in den importierten Netzwerken zu starten, da die DHCP-Adresse von dem ggf. vorhandenen externen Server im Konflikt mit OpenStack stehen könnte.

- Beim Typ der importierten VM werden korrekte Werte für CPU und Speicher angezeigt, aber für die Hauptfestplatte werden fälschlicherweise 0 GB angezeigt.

Voraussetzungen

- Vergewissern Sie sich, dass VMware Integrated OpenStack Version 3.0 oder 3.1 ausgeführt wird.
- Vergewissern Sie sich, dass VMware Integrated OpenStack bereitgestellt ist und ausgeführt wird.
- Überprüfen Sie, ob die VMs in dasselbe vCenter importiert werden.
- Der Import von VMs wird mit NSX und dem VDS-Plug-In für Neutron unterstützt.

  Hinweis Wenn Sie VMware Integrated OpenStack 3.0 ausführen, können Sie keine VMs importieren, die durch einen logischen Switch von NSX abgesichert sind. Das Netzwerk-Backing muss eine reguläre, verteilte Portgruppe sein. Diese Funktion wird in VMware Integrated OpenStack 3.1 oder höher unterstützt.

Vorgehensweise

1 Fügen Sie die Cluster, die die zu importierenden VMs enthalten, der VMware Integrated OpenStack-Bereitstellung hinzu.

   a Identifizieren Sie in vSphere Web Client den Cluster, der die zu importierenden VMs enthält.

   b Fügen Sie den Cluster als Nova-Computing-Cluster zur VMware Integrated OpenStack-Bereitstellung hinzu.

   c Wiederholen Sie den Vorgang bei Bedarf für weitere Cluster.

   Nach dem Hinzufügen des Clusters als Nova-Computing-Cluster können Sie die VMs importieren.

2 Melden Sie sich unter Verwendung von SSH bei VMware Integrated OpenStack Manager an.

3 Stellen Sie eine Verbindung mit dem VMware Integrated OpenStack vAPI-Endpoint her.

   Der Endpoint wird lokal ausgeführt.

   ```
   dcli +server http://localhost:9449/api +i
   ```

   Mit diesem Befehl wird eine interaktive Shell (`dcli`) geöffnet.

4 Listen Sie alle Namespaces im vAPI-Anbieter von VMware Integrated OpenStack auf.

   ```
   dcli> com vmware vio
   The vio namespace provides namespaces to manage components related to OpenStack and vSphere
   Available Namespaces:
   vm
   ```

5 (Optional) Listen Sie die Befehle zum Importieren von nicht verwalteten VMs auf.

Nicht verwaltete VMs sind nicht als OpenStack-Instanzen verwaltete VMs in VMware Integrated OpenStack. In diesem Fall enthalten die nicht verwalteten VMs die VMs in dem Cluster, den Sie zum Computing-Knoten hinzugefügt haben.

```
dcli> com vmware vio vm unmanaged
The Unmanaged namespace provides commands to manage virtual machine not under OpenStack
Available Commands:
importall   Imports all unmanaged virtual machines into OpenStack
importvm    Imports given virtual machine into OpenStack
list        Enumerates the list of unmanaged virtual machines
```

6 (Optional) Listen Sie alle nicht verwalteten VMs in einem bestimmten Ziel-Cluster auf, den Sie zum Nova-Computing-Knoten hinzugefügt haben.

```
com vmware vio vm unmanaged list --cluster <vcenter cluster mor-id>
```

7 Importieren Sie VMs in VMware Integrated OpenStack.

Sie können alle VMs oder eine bestimmte VM importieren.

a So importieren Sie alle VMs

```
com vmware vio vm unmanaged importall [-h] --cluster CLUSTER [--tenant-mapping {FOL-
DER,RESOURCE_POOL}] [--root-folder ROOT_FOLDER]
                                                [--root-resource-pool ROOT_RESOURCE_POOL]
```

Option	Beschreibung
--cluster CLUSTER	Legen Sie den Nova-Computing-Cluster fest, in dem sich die VMs befinden.
--tenant-mapping {FOLDER,RESOURCE_POOL}	Legen Sie fest, ob die vSphere-VMs zu OpenStack-Projekten basierend auf ihrer Ordnerposition oder auf Ressourcenpools zugeordnet werden sollen. Dieser Parameter ist optional. Wenn keine Mandantenzuordnung festgelegt ist, werden VMs zu Instanzen im **import_service**-Projekt in OpenStack.
--root-folder ROOT_FOLDER	Wenn Sie alternativ **FOLDER** als `tenant-mapping`-Parameter angegeben haben, können Sie den Namen des Root-Ordners mit den VMs für den Import angeben. ■ Alle VMs im angegebenen Root-Ordner werden importiert, einschließlich der VMs in Unterordnern. ■ Die VMs werden als Instanzen in ein OpenStack-Projekt mit demselben Namen wie der angegebene Root-Ordner importiert. ■ Wenn der Root-Ordner VMs in Unterordnern enthält, werden diese VMs in OpenStack-Projekte mit denselben Namen wie die Unterordner importiert. **Hinweis** Wenn kein Root-Ordner angegeben ist, wird standardmäßig der Name des Ordners auf der obersten Ebene im Cluster verwendet.
--root-resource-pool ROOT_RESOURCE_POOL	Wenn Sie alternativ **RESOURCE_POOL** als `tenant-mapping`-Parameter angegeben haben, können Sie den Namen des Root-Ressourcenpools mit den VMs für den Import festlegen. ■ Alle VMs im angegebenen Root-Ressourcenpool werden importiert, einschließlich der VMs in untergeordneten Ressourcenpools. ■ Die VMs werden als Instanzen in ein OpenStack-Projekt mit demselben Namen wie der angegebene Root-Ressourcenpool importiert. ■ Wenn der Root-Ressourcenpool VMs in untergeordneten Ressourcenpools enthält, werden diese VMs in OpenStack-Projekte mit denselben Namen wie die untergeordneten Ressourcenpools importiert.

b So importieren Sie eine bestimmte VM

```
com vmware vio vm unmanaged importvm [-h] \
     --vm VM [--tenant TENANT] [--nic-mac-address NIC_MAC_ADDRESS] \
     [--nic-ipv4-address NIC_IPV4_ADDRESS]
```

Option	Beschreibung
--vm VM	Geben Sie die **vm-<id>** der zu importierenden VM an. Mit dem Befehl `com vmware vio vm unmanaged list` können Sie die ID-Werte aller zu importierenden VMs anzeigen.
--tenant TENANT	Geben Sie das OpenStack-Projekt an, in dem sich die importierte VM als OpenStack-Instanz befindet. Dieser Parameter ist optional. Wenn kein Wert festgelegt ist, werden VMs zu Instanzen im **import_service**-Projekt in OpenStack.

Option	Beschreibung
`--nic-mac-address` `NIC_MAC_ADDRESS`	Geben Sie alternativ die MAC-Adresse für die Netzwerkkarte (NIC) der VM an. Wenn dieser Wert während des Importvorgangs nicht ermittelt werden kann, schlägt der Import fehl. Über diesen Parameter können Sie die MAC-Adresse der Netzwerkkarte manuell eingeben. **Hinweis** Wenn dieser Wert angegeben ist, müssen Sie auch den Parameter `nic-ipv4-address` angeben.
`--nic-ipv4-address` `NIC_IPV4_ADDRESS`	Geben Sie alternativ die IP-Adresse für die Netzwerkkarte (NIC) der VM an. Wenn dieser Wert während des Importvorgangs nicht ermittelt werden kann, schlägt der Import fehl. Über diesen Parameter können Sie die IP-Adresse der Netzwerkkarte manuell eingeben. **Hinweis** Wenn dieser Wert angegeben ist, müssen Sie auch den Parameter `nic-mac-address` angeben.

8 (Optional) Sie können die Verschiebung und Umbenennung von importierten VMs aktivieren oder deaktivieren, indem Sie die Datei `custom.yml` entsprechend anpassen.

Diese Option ist standardmäßig aktiviert.

a Falls nicht bereits geschehen, implementieren Sie die Datei `custom.yml`.

```
sudo mkdir -p /opt/vmware/vio/custom
sudo cp /var/lib/vio/ansible/custom/custom.yml.sample /opt/vmware/vio/custom/custom.yml
```

b Um die Verschiebung und Umbenennung von importierten VMs zu deaktivieren, heben Sie die Auskommentierung des folgenden Parameters in der Datei `custom.yml` auf.

```
nova_import_vm_relocate: false
```

c Speichern Sie die Datei `custom.yml`.

Erstellen eines Snapshots aus einer Instanz

Mit Snapshots können Sie neue Images aus laufenden Instanzen erstellen.

Sie können ein Snapshot einer Instanz direkt über die Seite „Instanzen“ erstellen.

Vorgehensweise

1 Melden Sie sich beim VMware Integrated OpenStack-Dashboard als ein Cloud-Administrator an.

2 Wählen Sie das Administratorprojekt aus dem Dropdown-Menü in der Titelleiste aus.

3 Wählen Sie **Administrator > Systemfenster > Instanzen** aus.

4 Klicken Sie in der Spalte „Aktionen“ auf **Snapshot erstellen**.

Das Snapshot wird auf der Seite „Images und Snapshots“ angezeigt.

Steuern des Zustands einer Instanz

Als Cloud-Administrator können Sie eine Instanz pausieren, fortsetzen, anhalten, wiederaufnehmen, beenden oder einen weichen bzw. harten Neustart der Instanz durchführen.

Vorgehensweise

1 Melden Sie sich beim VMware Integrated OpenStack-Dashboard als ein Cloud-Administrator an.

2 Wählen Sie das Administratorprojekt aus dem Dropdown-Menü in der Titelleiste aus.

3 Wählen Sie **Administrator > Systemfenster > Instanzen** aus.

4 Wählen Sie die Instanz aus, deren Zustand Sie verwalten möchten.

5 Klicken Sie in der Spalte „Aktionen“ auf **Mehr** und wählen Sie den Zustand aus dem Dropdown-Menü aus.

Als roter Text angezeigte Elemente sind deaktiviert.

Verfolgen der Verwendung von Instanzen

Sie können die Verwendung der Instanzen für jedes Projekt verfolgen. Sie können die monatlichen Kosten verfolgen, indem Sie Metriken wie die Anzahl der VCPUs, Festplatten, RAM und Betriebszeit für Ihre gesamten Instanzen anzeigen.

Vorgehensweise

1 Melden Sie sich beim VMware Integrated OpenStack-Dashboard als ein Cloud-Administrator an.

2 Wählen Sie das Administratorprojekt aus dem Dropdown-Menü in der Titelleiste aus.

3 Wählen Sie **Administrator > Systemfenster > Übersicht** aus.

Auf der Seite „Übersicht“ werden die Nutzungsübersicht und projektspezifische Nutzungsdaten angezeigt. Sie können einen Zeitraum für die Nutzungsdaten angeben. Optional können Sie eine CSV-Übersicht herunterladen.

4 (Optional) Geben Sie einen Zeitraum für die Berichterstellung an und klicken Sie auf **Senden**.

5 (Optional) Klicken Sie auf **CSV-Übersicht herunterladen**, um einen Nutzungsbericht herunterzuladen.

Verwenden von DRS zur Steuerung von OpenStack-Instanzenplatzierung

Als Cloud-Administrator können Sie vSphere-DRS-Einstellungen verwenden, um zu steuern, wie bestimmte OpenStack-Instanzen auf Hosts im Computing-Cluster platziert werden. Modifizieren Sie zusätzlich zur DRS-Konfiguration die Metadaten von Quell-Images in OpenStack, um sicherzustellen, dass von diesen Images erzeugte Instanzen korrekt für die Platzierung identifiziert werden.

Voraussetzungen

- Überprüfen Sie, dass Sie VMware Integrated OpenStack-Version 2.0.x oder höher ausführen.
- Stellen Sie sicher, dass VMware Integrated OpenStack in vSphere ausgeführt wird. Wechseln Sie zu **Home > VMware Integrated OpenStack > OpenStack-Bereitstellungen > [Name der Bereitstellung]**.
- Mindestens eine Dummy-VM im Computing-Cluster, die als Vorlage zur Erstellung einer DRS-VM-Gruppe verwendet wird.

Vorgehensweise

1 Definieren von VM- und Host-Gruppen für das Platzieren von OpenStack-Instanzen auf Seite 77

Erstellen Sie unter vSphere Web Client VM- und Host-Gruppen, die bestimmte OpenStack-Instanzen beinhalten und verwalten.

2 Erstellen einer DRS-Regel für OpenStack-Instanzenplatzierung auf Seite 78

Erstellen Sie im vSphere Web Client eine DRS-Regel zum Verwalten der Verteilung von OpenStack-Instanzen in einer VM-Gruppe für eine bestimmte Host-Gruppe.

3 Anwenden von VM-Gruppeneinstellungen zu Image-Metadaten auf Seite 79

Sie können die Metadaten eines Quell-Image modifizieren, damit Instanzen automatisch in VM-Gruppen platziert werden. VM-Gruppen werden im vSphere Web Client konfiguriert und können weitergehend verwendet werden, um DRS-Regeln anzuwenden.

Definieren von VM- und Host-Gruppen für das Platzieren von OpenStack-Instanzen

Erstellen Sie unter vSphere Web Client VM- und Host-Gruppen, die bestimmte OpenStack-Instanzen beinhalten und verwalten.

Vorgehensweise

1 Melden Sie sich beim vSphere Web Client an.

2 Wechseln Sie zur Ansicht „vCenter-Hosts und -Cluster“.

3 Wählen Sie den für die Anwendung VMware Integrated OpenStack konfigurierten Computing-Cluster aus.

4 Klicken Sie auf die Registerkarte **Verwalten**.

5 Klicken Sie auf **Einstellungen** und dann auf **vSphere DRS**.

6 Überprüfen Sie die folgende Einstellungskonfiguration:

- **DRS** ist aktiviert.
- **DRS Automation** ist auf „Vollautomatisiert“ oder „Teilweise automatisiert“ eingestellt.
- **Power Management** ist ausgeschaltet.

7 Klicken Sie auf **VM/Host-Gruppen**.

8 Erstellen Sie eine VM-Gruppe.

a Klicken Sie auf **Hinzufügen**.

b Geben Sie einen Namen für die neue VM-Gruppe ein.

c Wählen Sie im Dropdown-Menü **Typ** die Option **VM-Gruppe**.

d Klicken Sie auf **Hinzufügen**.

e Wählen Sie auf der Registerkarte **Filter** die Dummy-VM aus, um eine leere VM-Gruppe zu erstellen.

Sie haben die Dummy-VM in einer früheren Aufgabe in diesem Ablauf erstellt.

f Klicken Sie auf **OK**.

9 Erstellen Sie eine Host-Gruppe.

a Klicken Sie auf **Hinzufügen**.

b Geben Sie einen Namen für die neue Host-Gruppe ein.

c Wählen Sie im Dropdown-Menü **Typ** die Option **Host-Gruppe**.

d Klicken Sie auf **Hinzufügen**.

e Fügen Sie auf der Registerkarte **Filter** Mitglieder zur Gruppe hinzu, indem Sie einen oder mehrere Hosts auswählen.

f Klicken Sie auf **OK**.

Beide Gruppen erscheinen nun in der Liste „VM/Host-Gruppen“ auf der Seite „VM/Host“.

Weiter

Sie können nun eine Regel erstellen, die festlegt, wie OpenStack-Instanzen, die zur VM-Gruppe zugewiesen sind, auf die Hosts in der Host-Gruppe verteilt werden. Siehe „Erstellen einer DRS-Regel für OpenStack-Instanzenplatzierung“, auf Seite 78.

Erstellen einer DRS-Regel für OpenStack-Instanzenplatzierung

Erstellen Sie im vSphere Web Client eine DRS-Regel zum Verwalten der Verteilung von OpenStack-Instanzen in einer VM-Gruppe für eine bestimmte Host-Gruppe.

Wenn Sie mit „Definieren von VM- und Host-Gruppen für das Platzieren von OpenStack-Instanzen“, auf Seite 77 fortfahren, so überspringen Sie die Schritte bis Schritt 5.

Voraussetzungen

- Definieren Sie mindestens eine VM-Gruppe.
- Definieren Sie mindestens eine Host-Gruppe.

Siehe „Definieren von VM- und Host-Gruppen für das Platzieren von OpenStack-Instanzen“, auf Seite 77.

Vorgehensweise

1 Melden Sie sich beim vSphere Web Client an.

2 Wechseln Sie zur vCenter-Hosts- und Cluster-Ansicht und wählen Sie den Computing-Cluster aus, der für die VMware Integrated OpenStack-Bereitstellung konfiguriert ist.

3 Klicken Sie auf die Registerkarte **Verwalten** und wechseln Sie zu **Einstellungen > vSphere DRS**.

4 Überprüfen Sie die folgende Einstellungskonfiguration:

- **DRS** ist aktiviert.
- **DRS Automation** ist auf „Vollautomatisiert“ oder „Teilweise automatisiert“ eingestellt.
- **Power Management** ist ausgeschaltet.

5 Klicken Sie auf **VM/Host-Regeln**.

6 Klicken Sie auf **Hinzufügen**.

7 Geben Sie einen Namen für die neue Regel ein und aktivieren bzw. deaktivieren Sie die Option **Regel aktivieren**, um die Regel zu aktivieren bzw. deaktivieren.

8 Wählen Sie im Dropdown-Menü **Typ** die Option **Virtuelle Maschinen zu Hosts** aus.

9 Wählen Sie im Dropdown-Menü **VM-Gruppe** die VM-Gruppe aus, die die OpenStack-Instanzen identifiziert, die Sie platzieren möchten.

10 Wählen Sie die Spezifikation **Muss auf Hosts in der Gruppe ausgeführt werden** aus.

11 Wählen Sie eine Spezifikation für die Regel aus.

Einstellung	Beschreibung
Muss auf Hosts in der Gruppe ausgeführt werden	OpenStack-Instanzen in der angegebenen VM-Gruppe müssen auf Hosts in der angegebenen Host-Gruppe ausgeführt werden.
Sollte auf Hosts in der Gruppe ausgeführt werden	OpenStack-Instanzen in der angegebenen VM-Gruppe sollten – müssen aber nicht – auf Hosts in der angegebenen Host-Gruppe ausgeführt werden.
Darf nicht auf Hosts in der Gruppe ausgeführt werden	OpenStack-Instanzen in der angegebenen VM-Gruppe dürfen niemals auf einem Host in der angegebenen Host-Gruppe ausgeführt werden.
Sollte nicht auf Hosts in der Gruppe ausgeführt werden	OpenStack-Instanzen in der angegebenen VM-Gruppe sollen nicht – können aber – auf Hosts in der angegebenen Host-Gruppe ausgeführt werden.

12 Wählen Sie im Dropdown-Menü **Host-Gruppe** die Host-Gruppe aus, die die Hosts umfasst, auf denen OpenStack-Instanzen platziert werden.

13 Klicken Sie auf **OK**.

Die Regel legt nun fest, dass OpenStack-Instanzen in der angegebenen VM-Gruppe auf Hosts in der angegebenen Host-Gruppe ausgeführt werden müssen.

Weiter

Im VMware Integrated OpenStack-Dashboard können Sie nun die Metadaten für ein bestimmtes Image modifizieren, um sicherzustellen, dass alle von diesem Image erzeugten Instanzen automatisch in die VM-Gruppe mit einbezogen werden und daher der DRS-Regel unterliegen.

Anwenden von VM-Gruppeneinstellungen zu Image-Metadaten

Sie können die Metadaten eines Quell-Image modifizieren, damit Instanzen automatisch in VM-Gruppen platziert werden. VM-Gruppen werden im vSphere Web Client konfiguriert und können weitergehend verwendet werden, um DRS-Regeln anzuwenden.

Voraussetzungen

- Stellen Sie sicher, dass eine VM-Gruppe im vSphere Web Client für den Computing-Cluster konfiguriert ist.
- Stellen Sie sicher, dass der DRS-VM-Gruppenname im vSphere Web Client definiert ist. Siehe „Verwenden von DRS zur Steuerung von OpenStack-Instanzenplatzierung“, auf Seite 76.

Vorgehensweise

1 Melden Sie sich beim VMware Integrated OpenStack-Dashboard als ein Cloud-Administrator an.

2 Wählen Sie das Administratorprojekt aus dem Dropdown-Menü in der Titelleiste aus.

3 Wählen Sie **Admin > System > Images**.

4 Klicken Sie auf das zu ändernde Image.

5 Klicken Sie in der Spalte „Aktionen“ der Image-Auflistung auf den nach unten gerichteten Pfeil und wählen Sie **Metadaten aktualisieren** aus.

6 Fügen Sie die DRS-VM-Gruppen-Metadateneigenschaft zu den Image-Metadaten hinzu.

Das Dialogfeld „Metadaten aktualisieren“ zeigt zwei Spalten an. Die Spalte rechts zeigt die Metadaten-Tags an, die bereits auf das Image angewendet sind, und die Spalte links zeigt verfügbare Metadaten-Tags an, die nach Kategorien (wie Guest Customization, Instance Config Data usw.) gruppiert sind.

a Wählen Sie in der Spalte „Verfügbare Metadaten“ die Eigenschaft **VMware Treiberoptionen > DRS-VM-Gruppe** aus.

b Klicken Sie auf das Pluszeichen (+), um die Eigenschaft zu den Image-Metadaten hinzuzufügen.

Die Metadateneigenschaft **vmware_vm_group** wird in der Spalte „Vorhandene Metadaten“ hervorgehoben.

c Geben Sie den DRS-VM-Gruppennamen für den Metadatenwert so ein, wie er im vSphere Web Client definiert ist.

d Klicken Sie auf das Minus-Zeichen (-), um ein Metadaten-Tag aus der Image-Definition zu entfernen.

7 Klicken Sie auf **Speichern**.

Alle aus diesem Quell-Image erzeugten Instanzen werden automatisch der angegebenen VM-Gruppe in der VMware Integrated OpenStack-Bereitstellung im vCenter zugewiesen.

Verwenden von Affinität und Anti-Affinität zur Platzierung von OpenStack-Instanzen

Der Nova-Scheduler stellt Filter bereit, die Sie verwenden können, um sicherzustellen, dass OpenStack-Instanzen automatisch auf demselben Host (Affinität) oder unterschiedlichen Hosts (Anti-Affinität) gespeichert werden.

Sie wenden die Affinitäts- bzw. Anti-Affinitätsfilter als eine Richtlinie auf eine Servergruppe an. Alle Instanzen, die Mitglieder derselben Gruppe sind, unterliegen denselben Filtern. Wenn Sie eine OpenStack-Instanz erstellen, können Sie die Servergruppe angeben, zu der die Instanz gehören wird und damit auch, welcher Filter angewendet wird.

Sie können diese Konfiguration entweder unter Verwendung der OpenStack-Befehlszeilenschnittstelle oder der ServerGroup-API durchführen. Sie können diese Konfiguration nicht im VMware Integrated OpenStack Horizon-Dashboard durchführen.

Diese Methode der Platzierung von OpenStack-Instanzen ist mandantenbasierend. Affinität und Anti-Affinität bestimmen die Beziehung zwischen Instanzen in derselben Servergruppe. Sie können jedoch nicht die Hosts bestimmen, auf denen sich die Instanzen in vCenter befinden. Unter „Verwenden von DRS zur Steuerung von OpenStack-Instanzenplatzierung“, auf Seite 76 finden Sie eine administratorbasierende Methode, die mehr Kontrolle bietet.

Instanzen unter Verwendung der Befehlszeilenschnittstelle mit einer Affinitäts- oder Anti-Affinitätsrichtlinie erstellen

Sie können unter Verwendung von Affinität oder Anti-Affinität Instanzen platzieren, indem Sie eine Server-Gruppe in OpenStack erstellen und den gewünschten Filter als eine Gruppenrichtlinie anwenden. Alle Instanzen, die Teil der Server-Gruppe sind, unterliegen der Affinitäts- oder Anti-Affinitätsrichtlinie. Sie können diese Konfiguration unter Verwendung der Befehlszeilenschnittstelle durchführen.

Voraussetzungen

- Stellen Sie sicher, dass die vorgesehene Filterkonfiguration mit keiner bestehenden administrativen Konfiguration wie DRS-Regeln, die Instanzenplatzierung auf Hosts verwalten, in Konflikt steht.
- Überprüfen Sie, dass Sie VMware Integrated OpenStack-Version 2.0.x oder höher ausführen.
- Stellen Sie sicher, dass VMware Integrated OpenStack ausgeführt wird.
- Stellen Sie sicher, dass Sie eine Python-Nova-Client-Version 2.17.0.6 oder höher verwenden, wie dies für die ServerGroup API erforderlich ist. Wechseln Sie zu http://docs.openstack.org/user-guide/common/cli_install_openstack_command_line_clients.html.

Vorgehensweise

1 Melden Sie sich unter Verwendung von SSH beim Nova-Client an.

2 (Optional) Rufen Sie die ID des Image ab, das Sie verwenden werden, um die Instanz zu erstellen.

Sie können den Befehl „`nova image-list`“ verwenden, um die Liste verfügbarer Images und derer ID-Werte einzusehen.

3 (Optional) Rufen Sie die ID des Typs ab, die Sie verwenden werden, um die Instanz zu definieren.

Sie können den Befehl „`nova flavor-list`“ verwenden, um die Liste von Typdefinitionen und derer ID-Werte einzusehen.

4 Erstellen Sie eine neue Servergruppe mit der vorgesehenen Richtlinie.

   a Erstellen Sie eine Servergruppe mit der Affinitätsrichtlinie:

   ```
   nova server-group-create --policy affinity <GROUP_NAME>
   ```

   b Erstellen Sie eine Servergruppe mit der Anti-Affinitätsrichtlinie:

   ```
   nova server-group-create --policy anti-affinity <GROUP_NAME>
   ```

   In beiden Fällen gibt die Befehlszeilenschnittstelle die automatisch erzeugte Servergruppen-UUID, den Namen und die Richtlinie zurück.

5 Starten Sie eine neue Instanz unter Verwendung der Flags `--image`, `--flavor` und `--hint`, um die Servergruppen-Affinitätsrichtlinie anzuwenden.

   ```
   nova boot --image IMAGE_ID --flavor FLAVOR_ID --hint group=SERVER_GROUP_UUID INSTANCE_NAME
   ```

6 (Optional) Bestätigen Sie, dass die neue Regel und die Servergruppeninstanzen angezeigt und korrekt in der VMware Integrated OpenStack-Bereitstellung in vCenter ausgeführt werden.

   Die Details werden auf der Seite **Einstellungen > verwalten > VM/Host-Regeln** für den Computing-Cluster angezeigt.

Instanzen unter Verwendung der API mit einer Affinitäts- oder Anti-Affinitätsrichtlinie erstellen

Sie können unter Verwendung von Affinität oder Anti-Affinität Instanzen platzieren, indem Sie eine Server-Gruppe in OpenStack erstellen und den gewünschten Filter als eine Gruppenrichtlinie anwenden. Alle Instanzen, die Teil der Server-Gruppe sind, unterliegen der Affinitäts- oder Anti-Affinitätsrichtlinie. Sie können diese Konfiguration unter Verwendung der ServerGroup-API aus dem Python Nova-Client ausführen.

Voraussetzungen

- Stellen Sie sicher, dass die vorgesehene Anti-Affinität-Filterkonfiguration mit keiner bestehenden administrativen Konfiguration wie DRS-Regeln, die Instanzenplatzierung auf Hosts verwalten, in Konflikt steht.
- Überprüfen Sie, dass Sie VMware Integrated OpenStack-Version 2.0.x oder höher ausführen.
- Stellen Sie sicher, dass VMware Integrated OpenStack ausgeführt wird.
- Stellen Sie sicher, dass Sie eine Python-Nova-Client-Version 2.17.0.6 oder höher verwenden, wie dies für die ServerGroup API erforderlich ist. Wechseln Sie zu http://docs.openstack.org/user-guide/common/cli_install_openstack_command_line_clients.html.

Vorgehensweise

1 Erstellen Sie eine neue Servergruppe mit einer Anti-Affinitätsrichtlinie.

```
POST /v2/TENANT_ID/os-server-groups

{
    "server_group": {
        "name": "SERVER_GROUP_NAME",
        "policies": ["POLICY_TYPE"]
    }
}
```

Option	Beschreibung
TENANT_ID	ID-Wert für den OpenStack-Mandanten.
SERVER_GROUP_NAME	Geben Sie den Namen für die Servergruppe an.
POLICY_TYPE	Geben Sie entweder **`Affinität`** oder **`Anti-Affinität`** an.

2 Starten Sie eine neue Instanz einschließlich des `os:scheduler_hints`-Arguments mit der Servergruppen-ID im `GET /servers`-Befehl.

```
... "os:scheduler_hints": {"group": "SERVER_GROUP_UUID"}
```

3 (Optional) Bestätigen Sie, dass die neue Regel und die Servergruppeninstanzen angezeigt und korrekt in der VMware Integrated OpenStack-Bereitstellung in vCenter ausgeführt werden.

Die Regeldetails werden auf der Seite **Einstellungen > verwalten > VM/Host-Regeln** für den Computing-Cluster angezeigt.

Anwenden von QoS-Ressourcenzuteilung zu bestehenden Instanzen

Sie können QoS-Ressourcenzuteilungseinstellungen auf eine bestehende Instanz anwenden, indem Sie im VMware Integrated OpenStack-Dashboard die Größe der Instanz ändern.

Voraussetzungen

- Erfordert einen OpenStack-Typ mit den gewünschten QoS-Ressourcenzuteilungseinstellungen. Siehe „Konfigurieren von QoS Ressourcenzuteilung für Instanzen unter Verwendung von Typ-Metadaten“, auf Seite 114.
- VMware Integrated OpenStack-Version 2.0.x oder höher erforderlich.
- Stellen Sie sicher, dass VMware Integrated OpenStack in vSphere ausgeführt wird.
- Stellen Sie sicher, dass Sie beim VMware Integrated OpenStack-Dashboard als Cloud-Administrator angemeldet sind.

Vorgehensweise

1 Melden Sie sich beim VMware Integrated OpenStack-Dashboard als ein Cloud-Administrator an.

2 Wählen Sie das Administratorprojekt aus dem Dropdown-Menü in der Titelleiste aus.

3 Wählen Sie **Administrator > System > Instanzen** aus.

4 Klicken Sie auf den als Hyperlink hervorgehobenen Namen der Instanz, um auf die Seite der Instanzendetails zuzugreifen.

5 Klicken Sie auf den nach unten gerichteten Pfeil (neben der Schaltfläche **Snapshot erstellen**) und wählen Sie **Größe der Instanz ändern** aus.

6 Öffnen Sie auf der Registerkarte **Typauswahl** die Dropdown-Liste **Neuer Typ** und wählen Sie den Typ mit den gewünschten QoS-Ressourcenzuteilungen aus

7 Klicken Sie auf **Größe ändern**.

Der Prozess der Größenänderung kann einige Minuten in Anspruch nehmen.

Die Instanz unterliegt nun den QoS-Einstellungen, wie diese in den Typ-Metadaten definiert sind.

Konfigurieren von Single Root I/O Virtualization für Instanzen

Sie können Instanzen erstellen, die die SR-IOV-Spezifikation (Single Root I/O Virtualization) verwenden, indem Sie die Metadatenparameter des Typs und des Images ändern, die zum Erstellen der Instanz verwendet werden. SR-IOV ist eine Spezifikation, wodurch ein einzelnes PCIe-Gerät (PCIe, Peripheral Component Interconnect Express) unter einem einzelnen Root-Port als mehrere separate physische Geräte angezeigt wird.

Weitere Informationen zu den Anforderungen und unterstützten Funktionen von SR-IOV finden Sie in der Dokumentation zum vSphere Web Client.

In der folgenden Tabelle werden die Hauptkomponenten von SR-IOV und ihre Rolle beschrieben.

Tabelle 4-1. SR-IOV-Komponenten im Kontext von VMware Integrated OpenStack

Komponente	Rolle
Nova Compute	■ Erfasst die Liste der SR-IOV-Geräte und aktualisiert die Liste der PCI-Gerätespezifikationen. ■ Bettet die Hostobjekt-ID in die Gerätespezifikationen ein.
Nova PCI-Manager	■ Erstellt und pflegt einen Gerätepool mit Adresse, Anbieter-ID, Produkt-ID und Host-ID. ■ Teilt basierend auf PCI-Anforderungen PCI-Geräte Instanzen zu und hebt die Zuteilung auf.
Nova-Planer	■ Plant die Platzierung von Instanzen auf Hosts, die die PCI-Anforderungen erfüllen.
vSphere	■ Verwaltet Hosts in einem dedizierten Computing-Cluster mit SR-IOV-fähigen Netzwerkkarten und Hosts. Ein separater Computing-Cluster wird empfohlen, da DRS-Regeln auf SR-IOV-fähigen Geräten nicht funktionieren.

Voraussetzungen

- Vergewissern Sie sich, dass Ihre Bereitstellung VDS-basiert ist. SR-IOV ist nicht mit NSX kompatibel.
- VMware Integrated OpenStack-Version 2.0.x oder höher erforderlich.
- vSphere-Version 6.0 oder höher erforderlich.

Vorgehensweise

1 Aktivieren von SR-IOV auf Netzwerkadaptern in vSphere auf Seite 84

2 Konfigurieren von GPU-Passthrough-Geräten für OpenStack-Instanzen auf Seite 84

Ab VMware Integrated OpenStack 3.1 können Sie OpenStack-Instanzen, die physische Funktionen der GPU (aktiviert unter Verwendung von Directpath I/O) oder virtuelle Funktionen (SR-IOV) von vSphere verwenden, erstellen.

3 Konfigurieren von Netzwerk-DirectPath I/O-Passthrough für OpenStack-Instanzen auf Seite 85

Ab VMware Integrated OpenStack 3.1 können Sie OpenStack-Instanzen, die physische Funktionen des Netzwerks mit der DirectPath I/O-Technologie von VMware verwenden, erstellen.

4 Ändern von Typ-Metadaten zum Aktivieren von SR-IOV auf Seite 86

Sie müssen die Metadaten für einen Typ ändern, um SR-IOV zu aktivieren. Alle aus einem SR-IOV-fähigen Typ und einem SR-IOV-fähigen Image erstellten Instanzen übernehmen die SR-IOV-Eigenschaft.

5 Ändern von Image-Metadaten zum Aktivieren von SR-IOV auf Seite 87

Sie müssen die Metadaten für ein Image ändern, um SR-IOV zu aktivieren. Alle aus einem SR-IOV-fähigen Typ und einem SR-IOV-fähigen Image erstellten Instanzen übernehmen die SR-IOV-Eigenschaft.

Aktivieren von SR-IOV auf Netzwerkadaptern in vSphere

Vorgehensweise

1 Navigieren Sie im vSphere Web Client zum Host.

2 Erweitern Sie auf der Registerkarte **Konfigurieren** die Option **Netzwerk** und wählen Sie **Physische Adapter** aus.

Sie können sich die SR-IOV-Eigenschaft anzeigen lassen, um zu sehen, ob ein physischer Adapter SR-IOV unterstützt.

3 Wählen Sie den physischen Adapter aus und klicken Sie auf **Adapter-Einstellungen bearbeiten**.

4 Wählen Sie unter SR-IOV aus dem Dropdown-Menü **Status** die Option **Aktiviert** aus.

5 Geben Sie im Textfeld **Anzahl der virtuellen Funktionen** die Anzahl der virtuellen Funktionen ein, die Sie für den Adapter konfigurieren möchten.

6 Klicken Sie auf **OK**.

7 Starten Sie den Host neu.

Da DRS-Regeln auf SR-IOV-fähigen Geräten nicht funktionieren, erstellen Sie einen dedizierten Computing-Cluster für SR-IOV-fähige Hosts und Adapter mit dem Namen vmnics.

Die virtuellen Funktionen werden an dem Netzwerkkartenport aktiv, der durch den Eintrag des physischen Adapters dargestellt wird. Sie werden in der PCI-Geräteliste auf der Registerkarte **Einstellungen** für den Host angezeigt.

Sie können die vCLI-Befehle `esxcli network sriovnic` verwenden, um die Konfiguration von virtuellen Funktionen auf dem Host zu untersuchen.

Weiter

Sie können nun die Typ- und Image-Metadaten im VMware Integrated OpenStack-Dashboard konfigurieren.

Konfigurieren von GPU-Passthrough-Geräten für OpenStack-Instanzen

Ab VMware Integrated OpenStack 3.1 können Sie OpenStack-Instanzen, die physische Funktionen der GPU (aktiviert unter Verwendung von Directpath I/O) oder virtuelle Funktionen (SR-IOV) von vSphere verwenden, erstellen.

Der Verbrauch von GPU- und Passthrough-Funktionen wird durch die Verwendung des entsprechenden Typs erreicht. Ändern Sie die Metadatenparameter des Typs, um die Instanz zu erstellen.

Voraussetzungen

Stellen Sie sicher, dass Sie die folgenden Einstellungen in Ihrer Umgebung ausführen, bevor Sie die GPU-Passthrough-Geräte konfigurieren:

- Aktivieren Sie DirectPath I/O in vSphere. Weitere Informationen finden Sie im Kapitel *DirectPath I/O* in der *VMware vSphere 6.5-Dokumentation*.
- Aktivieren Sie SR-IOV auf GPU-Geräten in den ESXi-Hosts. Weitere Informationen finden Sie unter *Konfigurieren von AMD Multiuser GPU mit vDGA* in der VMware Horizon-Dokumentation.

Vorgehensweise

1 Melden Sie sich beim OpenStack Management Server an.

2 Erstellen Sie die `custom.yml`-Datei, wenn sie nicht vorhanden ist.

```
sudo mkdir –p /opt/vmware/vio/custom
     sudo cp /var/lib/vio/ansible/custom/custom.yml.sample
     /opt/vmware/vio/custom/custom.yml
```

3 Öffnen Sie die Datei `/opt/vmware/vio/custom/custom.yml` in einem Texteditor.

4 Erstellen Sie einen PCI-Alias unter Verwendung der VIO-Anpassung durch Bearbeiten der `custom.yml`-Datei gemäß Ihrer Konfiguration.

   a Bearbeiten Sie den `nova_pci_alias`-Wert zum Erstellen eines PCI-Alias basierend auf `device_type`, `vendor_id` sowie `product_id` und benennen Sie den Alias, beispielsweise:

   ```
   nova_pci_alias: ["product_id": "692f", "vendor_id": "1002", “device_type:” “type–VF”,
   "name": "gpu–vf"}]
   ```

   b Speichern Sie die Datei `custom.yml`.

5 Übertragen Sie die neue Konfiguration auf Ihre VMware Integrated OpenStack-Bereitstellung.

   Die Aktualisierung der Konfiguration unterbricht kurz die OpenStack-Dienste.

   ```
   viocli deployment configure ––tags nova_api_config
   ```

Weiter

„Ändern von Typ-Metadaten zum Aktivieren von SR-IOV“, auf Seite 86.

Konfigurieren von Netzwerk-DirectPath I/O-Passthrough für OpenStack-Instanzen

Ab VMware Integrated OpenStack 3.1 können Sie OpenStack-Instanzen, die physische Funktionen des Netzwerks mit der DirectPath I/O-Technologie von VMware verwenden, erstellen.

Der Verbrauch von DirectPath I/O-Passthrough-Funktionen wird durch die Verwendung des entsprechenden Typs erreicht. Ändern Sie die Metadatenparameter des Typs, um die Instanz zu erstellen.

Voraussetzungen

Stellen Sie sicher, dass Sie die folgenden Einstellungen in Ihrer Umgebung ausführen, bevor Sie die Direct-Path I/O-Passthrough-Geräte konfigurieren:

- Aktivieren Sie DirectPath I/O in vSphere. Weitere Informationen finden Sie im Kapitel *DirectPath I/O* in der *VMware vSphere 6.5-Dokumentation*.

Vorgehensweise

1 Melden Sie sich beim OpenStack Management Server an.

2 Erstellen Sie die `custom.yml`-Datei, wenn sie nicht vorhanden ist.

```
sudo mkdir –p /opt/vmware/vio/custom
     sudo cp /var/lib/vio/ansible/custom/custom.yml.sample
     /opt/vmware/vio/custom/custom.yml
```

3 Öffnen Sie die Datei `/opt/vmware/vio/custom/custom.yml` in einem Texteditor.

4 Erstellen Sie einen PCI-Alias unter Verwendung der VIO-Anpassung durch Bearbeiten der `custom.yml`-Datei gemäß Ihrer Konfiguration.

   a Bearbeiten Sie den `nova_pci_alias`-Wert zum Erstellen eines PCI-Alias basierend auf `device_type`, `vendor_id` sowie `product_id` und benennen Sie den Alias, beispielsweise:

   ```
   nova_pci_alias: [{"device_type": "type–VF", "name": "sriov"}, {"vendor_id":"15b3", "pro–
   duct_id":"1013", "device_type": "type–PF", "name":"fpt"}]
   ```

   b Speichern Sie die Datei `custom.yml`.

5 Übertragen Sie die neue Konfiguration auf Ihre VMware Integrated OpenStack-Bereitstellung.

   Die Aktualisierung der Konfiguration unterbricht kurz die OpenStack-Dienste.

   ```
   viocli deployment configure ––tags nova_api_config
   ```

Weiter

„Ändern von Typ-Metadaten zum Aktivieren von SR-IOV“, auf Seite 86.

Ändern von Typ-Metadaten zum Aktivieren von SR-IOV

Sie müssen die Metadaten für einen Typ ändern, um SR-IOV zu aktivieren. Alle aus einem SR-IOV-fähigen Typ und einem SR-IOV-fähigen Image erstellten Instanzen übernehmen die SR-IOV-Eigenschaft.

Vorgehensweise

1 Melden Sie sich beim VMware Integrated OpenStack-Dashboard als ein Cloud-Administrator an.

2 Wählen Sie das Administratorprojekt aus dem Dropdown-Menü in der Titelleiste aus.

3 Wählen Sie **Administrator > System > Typen** aus.

4 (Optional) Erstellen Sie einen Typ, der für die SR-IOV-Spezifikation dediziert ist.

   Die ursprüngliche Typ-Konfiguration bleibt intakt und für andere Verwendungszwecke verfügbar.

5 Wählen Sie den zu ändernden Typ aus.

6 Klicken Sie in der Spalte „Aktionen“ der Image-Auflistung auf den nach unten gerichteten Pfeil und wählen Sie **Metadaten aktualisieren** aus.

7 Erweitern Sie in der Spalte unter „Verfügbare Metadaten“ die Registerkarte **VMware-Treiberoptionen für Typen**.

   Hinweis Wenn die Registerkarte **VMware-Treiberoptionen für Typen** nicht vorhanden ist, ist die entsprechende Metadateneigenschaft möglicherweise bereits konfiguriert.

8 Klicken Sie auf das Pluszeichen (**+**) neben der Metadateneigenschaft „PCI-Passthrough-Alias“.

   In der Spalte unter „Vorhandene Metadaten“ werden die neu hinzugefügte Metadateneigenschaft und der Standardwert angezeigt. Der numerische Teil steht für die Anzahl der virtuellen Funktionen, die angefordert werden können.

Der PCI-Passthrough-Alias bezieht sich auf eine PCI-Anforderungsspezifikation, die `vendor_id`, `product_id` und `device_type` enthält. In VMware Integrated OpenStack ist der Alias bereits erstellt und bezieht sich auf eine PCI-Anforderungsspezifikation, die zum Zuweisen eines beliebigen Geräts unabhängig von `vendor_id`, `product_id` und `device_type` verwendet werden kann.

9 Erhöhen Sie den numerischen Wert nach Bedarf.

Die maximal zulässige Anzahl virtueller Funktionen ist **`10`**.

10 Klicken Sie auf **Speichern**.

Sie können nun Image-Metadaten ändern, um SR-IOV zu aktivieren.

Ändern von Image-Metadaten zum Aktivieren von SR-IOV

Sie müssen die Metadaten für ein Image ändern, um SR-IOV zu aktivieren. Alle aus einem SR-IOV-fähigen Typ und einem SR-IOV-fähigen Image erstellten Instanzen übernehmen die SR-IOV-Eigenschaft.

Vorgehensweise

1 Melden Sie sich beim VMware Integrated OpenStack-Dashboard als ein Cloud-Administrator an.

2 Wählen Sie das Administratorprojekt aus dem Dropdown-Menü in der Titelleiste aus.

3 Wählen Sie **Admin > System > Images**.

4 (Optional) Erstellen Sie eine Image-Definition, die für die SR-IOV-Spezifikation dediziert ist.

Die ursprüngliche Image-Konfiguration bleibt intakt und für andere Verwendungszwecke verfügbar.

5 Wählen Sie das zu ändernde Image aus.

6 Klicken Sie in der Spalte „Aktionen“ der Image-Auflistung auf den nach unten gerichteten Pfeil und wählen Sie **Metadaten aktualisieren** aus.

7 Erweitern Sie in der Spalte unter „Verfügbare Metadaten“ die Registerkarte **VMware-Treiberoptionen**.

Hinweis Wenn die Registerkarte **VMware-Treiberoptionen** nicht vorhanden ist, ist die entsprechende Metadateneigenschaft möglicherweise bereits konfiguriert.

8 Klicken Sie auf das Pluszeichen (**+**) neben der Metadateneigenschaft „Virtuelle Netzwerkkarte“.

In der Spalte unter „Vorhandene Metadaten“ wird die neu hinzugefügte Metadateneigenschaft als „hw_vif_model“ angezeigt.

9 Wählen Sie in der Dropdown-Liste die Option **VirtualSriovEthernetCard** aus.

10 Klicken Sie auf **Speichern**.

Festlegen des standardmäßigen Nova-Speichers für OpenStack-Instanzen

Um sicherzustellen, dass die über ein Volume gestarteten OpenStack-Instanzen den korrekten Volume-Typ verwenden, können Sie Einstellungen für die richtlinienbasierte Verwaltung, die als „PBM-Richtlinien“ bezeichnet werden, erstellen und anwenden.

Nach der Aktivierung der Speicherrichtlinie in der Datei `custom.yml` wenden Sie die Richtlinie an, indem Sie die Metadaten eines OpenStack-Typs ändern. Alle Instanzen, die unter Verwendung dieses Typs erstellt werden, übernehmen die Konfiguration der Speicherrichtlinie.

Vorgehensweise

1 Implementieren Sie die Datei `custom.yml`.

```
sudo mkdir –p /opt/vmware/vio/custom
sudo cp /var/lib/vio/ansible/custom/custom.yml.sample /opt/vmware/vio/custom/custom.yml
```

2 Bearbeiten Sie die Datei `/opt/vmware/vio/custom/custom.yml`, um die Auskommentierung der PBM-Optionen aufzuheben.

```
############################
# PBM options
############################

# (string) The PBM default policy to use when no policy is associated with a flavor (Mandato–
ry) if nova_pbm_enabled is set to True.
nova_pbm_default_policy: nova

# (boolean) The PBM status. Set this to True to enable storage policies for nova flavors.
nova_pbm_enabled: False
```

3 Setzen Sie den Parameter `nova_pbm_enabled` auf **`True`** fest.

```
nova_pbm_enabled: True
```

4 Speichern Sie die Datei `custom.yml`.

5 Wenden Sie die Richtlinie auf einen OpenStack-Typ als Metadaten an.

   a Melden Sie sich beim VMware Integrated OpenStack-Dashboard als ein Cloud-Administrator an.

   b Wählen Sie das Administratorprojekt aus dem Dropdown-Menü in der Titelleiste aus.

   c Wählen Sie **Administrator > System > Typen** aus.

   d (Optional) Erstellen Sie einen Typ, der für die beabsichtigte Verwendung dieser Metadateneigenschaft charakteristisch ist.

   Erstellen Sie einen benutzerdefinierten Typ, damit dieser die bestimmte Konfiguration enthält. Durch diese Aktion bleibt die ursprüngliche Typ-Konfiguration intakt und für die Erstellung weiterer Instanzen verfügbar.

   e Wählen Sie den zu ändernden Typ aus.

   f Klicken Sie in der Spalte „Aktionen“ der Image-Auflistung auf den nach unten gerichteten Pfeil und wählen Sie **Metadaten aktualisieren** aus.

   g Geben Sie **`vmware:storage_policy`** in das Feld **Benutzerdefiniert** ein.

   h Klicken Sie auf das Pluszeichen (**+**) neben dem Feld **Benutzerdefiniert**.

   In der Spalte unter „Vorhandene Metadaten“ wird die neu hinzugefügte Metadateneigenschaft angezeigt.

   i Geben Sie **`nova`** als Eigenschaftswert für die Metadaten ein.

6 Klicken Sie auf **Speichern**.

Die standardmäßig Nova-Speicherrichtlinie wird auf alle zukünftigen OpenStack-Instanzen angewendet, die mit diesem Typ erstellt werden.

Arbeiten mit Datenträgern und Datenträgertypen in OpenStack 5

Datenträger sind Blockspeichergeräte, die an Instanzen angefügt werden, um einen persistenten Speicher zu ermöglichen.

Als Cloud-Administrator können Sie Datenträger und Datenträgertypen für Benutzer in verschiedenen Projekten verwalten. Sie können Datenträgertypen erstellen und löschen und Datenträger anzeigen und löschen.

Cloud-Benutzer können einen Datenträger jederzeit mit einer laufenden Instanz verbinden oder von dieser trennen und mit einer anderen Instanz verbinden. Informationen zum Verwenden des Dashboards zum Erstellen und Verwalten von Datenträgern als ein Endbenutzer finden Sie im *Benutzerhandbuch für VMware Integrated OpenStack*.

Dieses Kapitel behandelt die folgenden Themen:

Ändern des Standardadaptertyps für Cinder-Volumes

Ab VMware Integrated OpenStack 3.1 können Sie den Standardadaptertyp für neu erstellte Volumes ändern, indem Sie den Parameter `vmware_adapter_type` mithilfe der Datei `custom.yml` ändern.

Leere Volumes werden standardmäßig stets erstellt und einem lsiLogic-Controller hinzugefügt. Wenn ein Volume von einem Image erstellt wird, berücksichtigt Cinder die Eigenschaft `vmware_adaptertype` des Images und erstellt den entsprechenden Controller. Für neu erstellte Volumes legen Sie den Adaptertyp mithilfe des Parameters `cinder_volume_default_adapter_type` in der Datei `custom.yml` unter Verwendung eines der folgenden Werte fest.

Wert	Beschreibung
lsiLogic	Legt „LSI Logic“ als Standardadaptertyp fest
busLogic	Legt „Bus Logic“ als Standardadaptertyp fest
lsiLogicsas	Legt „LSI Logic SAS“ als Standardadaptertyp fest
paraVirtual	Legt „VMware Paravirtual SCSI“ als Standardadaptertyp fest
ide	Legt „IDE“ als Standardadaptertyp fest

Vorgehensweise

1 Implementieren Sie die Datei `custom.yml`.

```
sudo mkdir –p /opt/vmware/vio/custom
sudo cp /var/lib/vio/ansible/custom/custom.yml.sample /opt/vmware/vio/custom/custom.yml
```

2 Öffnen Sie die Datei `/opt/vmware/vio/custom/custom.yml` in einem Texteditor.

a Heben Sie die Auskommentierung des Parameters `cinder_volume_default_adapter_type` auf.

b Ändern Sie die Einstellung mit einem benutzerdefinierten Wert, beispielsweise **`lsiLogicsas`**.

```
############################
# cinder-volume options
############################

# Default volume adapter type; valid values are 'lsiLogic',
# 'busLogic', 'lsiLogicsas', 'paraVirtual' and 'ide'. (string value)
#cinder_volume_default_adapter_type: 'lsiLogicsas'
```

3 Speichern Sie die Datei `custom.yml`.

4 Übertragen Sie die neue Konfiguration auf Ihre VMware Integrated OpenStack-Bereitstellung.

```
viocli deployment configure
```

Hinweis Die Bereitstellung der Konfiguration im Push-Verfahren führt zu einer kurzen Unterbrechung der OpenStack-Dienste.

Erstellen eines Datenträgertyps

Wenn Sie über Cloud-Administratorberechtigungen verfügen, können Sie Blockspeicher-Datenträger und Datenträgertypen für Benutzer verwalten. Nach dem Erstellen eines Datenträgertyps verwenden Sie einen Befehl an der Befehlszeilenschnittstelle, um den Datenträgertyp einer vorhandenen vCenter-speicherbasierten Richtlinie zuzuordnen. Die Speicherrichtlinie definiert einen oder mehrere Datenspeicher für den zu verwendenden Datenträgertyp.

Voraussetzungen

- Stellen Sie sicher, dass die dem Datenträgertyp zuzuordnende Speicherrichtlinie vorhanden ist. Informationen dazu finden Sie in der vSphere-Produktdokumentation.
- Überprüfen Sie den Namen der Speicherrichtlinie. Dieser Wert ist erforderlich, wenn Sie den Befehl an der Befehlszeilenschnittstelle eingeben, um dem Datenträgertyp eine Speicherrichtlinie zuzuordnen.

Vorgehensweise

1 Melden Sie sich beim VMware Integrated OpenStack-Dashboard an.

2 Wählen Sie das Projekt aus dem Dropdown-Menü in der Titelleiste aus.

3 Wählen Sie **Systemfenster > Datenträger** aus.

Auf der Seite „Datenträger“ werden die Datenträger aufgelistet, die konfiguriert und für den aktuellen Benutzer verfügbar sind.

4 Klicken Sie auf die Registerkarte **Datenträgertypen**.

5 Klicken Sie auf **Datenträgertyp erstellen**.

6 Geben Sie einen Namen für den Datenträgertyp ein.

7 Geben Sie eine Beschreibung für den Datenträgertyp ein und klicken Sie auf **Datenträgertyp erstellen**.

8 Ordnen Sie dem Datenträgertyp eine Speicherrichtlinie zu.

a Melden Sie sich bei einem der Controller in VMware Integrated OpenStack an.

b Fügen Sie den cinder-Befehl aus, um dem Datenträgertyp eine Speicherrichtlinie zuzuordnen.

```
cinder type-key name-of-volume-type set vmware:storage_profile=name-of-storage-profile
```

In diesem Beispiel werden die folgenden Parameter und Einstellungen verwendet.

Parameter oder Einstellung	Beschreibung
`name-of-volume-type`	Name des Datenträgertyps, den Sie beim Erstellen des Datenträgertyps festgelegt haben.
`vmware:storage_profile=name-of-storage-profile`	Ordnet die Speicherrichtlinie nach dem in vSphere definierten Namen zu.

9 (Optional) Wenn Sie den Standardadaptertyp überschreiben möchten, ordnen Sie dem Datenträgertyp einen anderen Adaptertyp zu.

```
cinder type-key name-of-volume-type set vmware:adapter_type=name-of-adapter-type
```

Für den Adaptertyp können Sie einen der folgenden Werte auswählen.

Wert	Beschreibung
lsiLogic	Legt „LSI Logic“ als Adaptertyp fest
busLogic	Legt „Bus Logic“ als Adaptertyp fest
lsiLogicsas	Legt „LSI Logic SAS“ als Adaptertyp fest
paraVirtual	Legt „VMware Paravirtual SCSI“ als Adaptertyp fest
ide	Legt „IDE“ als Adaptertyp fest

Löschen eines Datenträgertyps

Als Cloud-Administrator können Sie Datenträger und Datenträgertypen für Benutzer in Projekten verwalten.

Vorgehensweise

1 Melden Sie sich beim VMware Integrated OpenStack-Dashboard an.

2 Wählen Sie das Projekt aus dem Dropdown-Menü in der Titelleiste aus.

3 Wählen Sie **Administrator > Systemfenster > Datenträger** aus.

Auf der Seite „Datenträger“ werden die für den aktuellen Benutzer derzeit konfigurierten und verfügbaren Datenträger aufgelistet.

4 Wählen Sie die zu löschenden Datenträgertypen aus.

5 Klicken Sie auf **Datenträgertypen löschen**.

6 Bestätigen Sie den Löschvorgang an der Eingabeaufforderung.

Migrieren von Datenträgern zwischen Datenspeichern

Sie können Cinder-Datenträger sicher zwischen Datenspeichern migrieren. Damit können Sie Datenspeicher ersetzen, Ressourcen und Kapazität ergänzen und Datenträger erhalten, ohne sie offline zu schalten. Der Prozess zum Migrieren von Datenträgern hängt von mehreren Faktoren ab. Der Prozess ist beispielsweise sehr einfach, wenn der Datenträger nicht an eine Instanz angehängt ist. Wenn ein Datenträger an eine Instanz angehängt ist, müssen Sie die Instanz migrieren.

Hinweis Sie können keinen Datenträger migrieren, an den Snapshots angehängt sind. Sie müssen die Snapshots zunächst trennen.

Migrieren aller Datenträger von einem angegebenen Datenspeicher

Sie können alle Datenträger schnell von einem angegebenen Datenspeicher evakuieren, indem Sie sie automatisch zu anderen Datenspeichern im selben Datenspeicher-Cluster migrieren.

Voraussetzungen

- Vergewissern Sie sich, dass der angegebene Datenspeicher Bestandteil eines Datenspeicher-Clusters ist.
- Vergewissern Sie sich, dass für Storage DRS die Option `Not Automation (Manual Mode)` für den Datenspeicher-Cluster aktiviert ist.
- Vergewissern Sie sich, dass keinerlei Snapshots an die Datenträger angehängt sind. Andernfalls müssen sie zunächst getrennt werden.

Vorgehensweise

1 Melden Sie sich unter Verwendung von SSH bei VMware Integrated OpenStack Manager an.

2 Wechseln Sie zum Root-Benutzer.

```
sudo su –
```

3 Bereiten Sie den Datenträger für die Migration vor.

Mit diesem Schritt werden alle Datenträger auf dem angegebenen Datenspeicher für die Migration vorbereitet.

```
viocli ds–migrate–prep [–d DEPLOYMENT] DC_NAME DS_NAME
```

Option	Beschreibung
–d DEPLOYMENT	Gibt den Namen der VMware Integrated OpenStack-Bereitstellung an.
DC_NAME	Gibt den Namen des Datencenters an.
DS_NAME	Gibt den Namen des Datenspeichers an.

4 Versetzen Sie den Datenspeicher in den Wartungsmodus.

Informationen hierzu finden Sie in der vSphere-Produktdokumentation.

Wenn Sie den Datenspeicher in den Wartungsmodus versetzen, wird der Datenspeicher evakuiert und die Datenträger werden automatisch auf die anderen Datenspeicher im selben Datenspeicher-Cluster migriert.

Migrieren von nicht angehängten Cinder-Datenträgern

Sie können Cinder-Datenträger, die nicht an Instanzen angehängt sind, auf angegebene Zieldatenspeicher migrieren.

Voraussetzungen

Vergewissern Sie sich, dass keinerlei Snapshots an die Datenträger angehängt sind. Andernfalls müssen sie zunächst getrennt werden.

Vorgehensweise

1 Melden Sie sich unter Verwendung von SSH bei VMware Integrated OpenStack Manager an.

2 Wechseln Sie zum Root-Benutzer.

```
sudo su -
```

3 Migrieren Sie den Datenträger.

```
viocli volume-migrate [-d [NAME]] \
                      [--source-dc [SRC_DC_NAME]] [--source-ds [SRC_DS_NAME]] \
                      [--volume-ids [VOLUME_UUIDS]] [--ignore-storage-policy] \
                      DEST_DC_NAME DEST_DS_NAME [-h] [-v]
```

Parameter	Obligatorisch oder Optional	Beschreibung
`-d, --deployment` *NAME*	Automatisch	Name der Bereitstellung, in welche die Volumes migriert werden. Wird automatisch angewendet. Der Standardwert ist der Name der aktuellen Bereitstellung.
`--source-dc` *SRC_DC_NAME*	Obligatorisch, außer wenn VOLUME_UUIDS angegeben ist.	Identifiziert das Quelldatencenter. Wird mit dem Parameter `--source-ds` zur eindeutigen Identifizierung des Datenspeichers verwendet.
`--source-ds` *SRC_DS_NAME*	Obligatorisch, außer wenn VOLUME_UUIDS angegeben ist.	Wird mit dem Parameter `--source-dc` zur eindeutigen Identifizierung des Datenspeichers verwendet. Beim folgenden Befehl werden beispielsweise alle Volumes von Datenspeicher DS-01 in Datencenter DC-01 zu Datenspeicher DS-02 in Datencenter DC-02 migriert. `viocli volume-migrate --source-dc DC-01 --source-ds DS-01 DC-02 DS-02`
`--volume-ids` *VOLUME_UUIDS*	Obligatorisch, außer wenn SRC_DC_NAME und SRC_DS_NAME angegeben sind.	Migriert mindestens ein durch den UUID-Wert festgelegtes einzelnes Volume. Trennen Sie die UUIDs durch Kommas, wenn Sie mehr als ein Volume angeben möchten. Beim folgenden Befehl werden beispielsweise zwei Volumes, die durch ihre UUID-Werte festgelegt sind, zu Datenspeicher DS-01 in Datencenter DC-01 migriert. `viocli volume-migrate --volume-ids 25e121d9-1153-4d15-92f8-c92c10b4987f, 4f1120e1-9ed4-421a-b65b-908ab1c6bc50 DC-01 DS-01`
`--ignore-storage-policy`	Optional	Ignoriert die Überprüfung der Einhaltung von Speicherrichtlinien. Fügen Sie diesen Parameter hinzu, um das Fehlschlagen der Migration zu verhindern, wenn das migrierte Volume eine Speicherrichtlinie enthält, die mit dem Zieldatenspeicher nicht übereinstimmt.
DEST_DC_NAME	Obligatorisch	Gibt das Zieldatencenter an.

Parameter	Obligatorisch oder Optional	Beschreibung
DEST_DS_NAME	Obligatorisch	Gibt den Zieldatenspeicher an.
`-h, --help`	Optional	Zeigt die Verwendung und Argumente für diesen Befehl an.
`-v, --verbose`	Optional	Der ausführliche Modus wird gestartet.

Migrieren von angehängten Cinder-Datenträgern

Um einen angehängten Cinder-Datenträger auf einen anderen Datenspeicher zu migrieren, müssen Sie die virtuelle Maschine der entsprechenden Instanz migrieren, an die der Datenträger angehängt ist.

Voraussetzungen

Vergewissern Sie sich, dass keinerlei Snapshots an die Datenträger angehängt sind. Andernfalls müssen sie zunächst getrennt werden.

Vorgehensweise

1 Melden Sie sich unter Verwendung von SSH bei VMware Integrated OpenStack Manager an.

2 Wechseln Sie zum Root-Benutzer.

```
sudo su -
```

3 Bereiten Sie den Datenträger für die Migration vor.

Mit diesem Schritt werden alle Datenträger auf dem angegebenen Datenspeicher für die Migration vorbereitet.

```
viocli ds-migrate-prep [-d DEPLOYMENT] DC_NAME DS_NAME
```

Option	Beschreibung
`-d DEPLOYMENT`	Gibt den Namen der VMware Integrated OpenStack-Bereitstellung an.
`DC_NAME`	Gibt den Namen des Datencenters an.
`DS_NAME`	Gibt den Namen des Datenspeichers an.

4 Melden Sie sich beim vSphere Web Client an.

5 Suchen Sie die virtuelle Maschine, die der Nova-Instanz entspricht, an die der Datenträger angehängt ist.

6 Verwenden Sie die Funktion Storage vMotion in vSphere Web Client, um die virtuelle Maschine auf einen anderen Datenspeicher zu migrieren.

Weitere Informationen zur Verwendung von Storage vMotion finden Sie in der vSphere-Produktdokumentation.

Verwalten von Images für den Imagedienst 6

Im OpenStack-Kontext ist ein Image eine Datei, die eine virtuelle Festplatte enthält, über die Sie ein Betriebssystem auf einer VM installieren können. Sie können eine Instanz in Ihrer OpenStack-Cloud mit einem der verfügbaren Images erstellen. Die Imagedienstkomponente von VMware Integrated OpenStack unterstützt nativ die in den Formaten ISO, OVA und VMDK gepackten Images.

Wenn Sie über vorhandene Images in vSphere verfügen, die Sie in OpenStack verwenden möchten, können Sie sie in eines der unterstützten Formate exportieren und zum Imagedienst hochladen. Wenn Sie ein Image in einem nicht unterstützten Format abrufen, können Sie es während des Importprozesses konvertieren. Die Formate RAW, QCOW2, VDI und VHD werden nicht unterstützt.

Dieses Kapitel behandelt die folgenden Themen:

Importieren von Images zum Imagedienst

Sie können Befehlszeilenschnittstellenbefehle oder das VMware Integrated OpenStack-Dashboard zum Importieren von Images verwenden.

Voraussetzungen

Um einen erfolgreichen Import zu gewährleisten, stellen Sie sicher, dass das Image in einem der nativen unterstützten Image-Formate (ISO, OVA, VMDK) oder in einem Format vorliegt, das während des Importprozesses konvertiert werden kann (RAW, QCOW2, VDI, VHD).

Vorgehensweise

1 Images unter Verwendung des Horizon-Dashboard importieren auf Seite 96

  Sie können Images direkt in das VMware Integrated OpenStack-Horizon-Dashboard importieren.

2 Images in unterstützten Formaten unter Verwendung der Befehlszeilenschnittstelle importieren auf Seite 97

Sie können Images zur Verwendung in Instanzen verfügbar machen, indem Sie Images in den Image-dienst-Datenspeicher importieren.

3 Importieren von Images in nicht unterstützten Formaten unter Verwendung der Befehlszeilenschnittstelle auf Seite 98

Sie können Images in nicht unterstützten Image-Formaten wie RAW, QCOW2, VDI oder VHD importieren, indem Sie das Tool `glance-import` in der Befehlszeilenschnittstelle verwenden. Dieses Tool konvertiert automatisch das Quell-Image in das VMDK-Format.

Images unter Verwendung des Horizon-Dashboard importieren

Sie können Images direkt in das VMware Integrated OpenStack-Horizon-Dashboard importieren.

Voraussetzungen

- Stellen Sie sicher, dass das Image im Format ISO, VMDK, OVA, RAW, QCOW2, VDI oder VHD gepackt ist.
- Wenn das Format des Quell-Image RAW, QCOW2, VDI oder VHD ist, muss das Quell-Image auf einem Server ohne Anmeldedaten gehostet werden, damit einfache HTTP-Anforderungen zulässig sind.

Vorgehensweise

1 Melden Sie sich beim VMware Integrated OpenStack-Dashboard als ein Cloud-Administrator an.

2 Wählen Sie das Administratorprojekt aus dem Dropdown-Menü in der Titelleiste aus.

3 Wählen Sie **Administrator > Systemfenster > Images** aus.

4 Klicken Sie auf der Seite „Images“ auf **Image erstellen**.

5 Konfigurieren Sie das Image.

Option	Aktion
Name	Geben Sie einen Namen für das neue Image ein.
Beschreibung	(Optional) Geben Sie eine Beschreibung für das neue Image ein.
Image-Quelle	Wählen Sie die Image-Quelle aus. Wenn das Format des Quell-Image RAW, QCOW2, VD oder VHD ist, müssen Sie die Option „Image-Speicherort“ auswählen.
Festplattenformat	Wählen Sie das Festplattenformat aus.
Festplattentyp	Wählen Sie den Festplattentyp aus. Images in den Formaten RAW, QCOW2, VDI und VHD werden automatisch geprüft, damit deren Eigenschaften während des Importprozesses erfasst und in das VMDK-Format konvertiert werden.
Adaptertyp	Wählen Sie den Adaptertyp aus.
Architektur	Übernehmen Sie den Standardwert.
Typ des Betriebssystems	Wählen Sie den Betriebssystemtyp aus.
Mindestgröße der Festplatte (GB)	Geben Sie die Mindestgröße der Festplatte für das Image in GB an.
Mindestarbeitsspeicher (GB)	Geben Sie den Mindestarbeitsspeicher für das Image an.
Öffentlich	Wählen Sie diese Option aus, damit das Image allen Mandanten angezeigt wird und diesen zur Verfügung steht.
Geschützt	Wählen Sie diese Option aus, damit das Image nicht gelöscht werden kann.

6 Klicken Sie auf **Image erstellen**.

Die Seite „Images“ enthält nun das neu hinzugefügte Image.

Das Image kann jetzt in OpenStack-Instanzen bereitgestellt werden.

Images in unterstützten Formaten unter Verwendung der Befehlszeilenschnittstelle importieren

Sie können Images zur Verwendung in Instanzen verfügbar machen, indem Sie Images in den Imagedienst-Datenspeicher importieren.

Um ein Image in einem nicht unterstützten Format wie RAW, QCOW2, VDI oder VHD zu importieren, siehe „Importieren von Images in nicht unterstützten Formaten unter Verwendung der Befehlszeilenschnittstelle“, auf Seite 98.

Voraussetzungen

- Stellen Sie sicher, dass Sie mindestens einen Imagedienst-Datenspeicher konfiguriert haben.
- Rufen Sie das Image ab, zum Beispiel `ubuntuLTS-sparse.vmdk`.
- Stellen Sie sicher, dass die Images im ISO-, VMDK- oder OVA-Format gepackt sind.

Vorgehensweise

1 Melden Sie sich beim OpenStack-Verwaltungs-Cluster als Benutzer mit Administratorrechten an, um das Image in die Imagedienst-Komponente hochzuladen.

2 Führen Sie den `glance image-create`-Befehl aus, um das Image abzurufen, zu definieren und zu importieren.

```
glance  --os-auth-token $token --os-image-url http://123.456.7.8:9292 \
        image-create name="ubuntu-sparse" \
        disk_format=vmdk \
        container_format=bare \
        --visibility="public" \
        --property vmware_adaptertype="lsiLogicsas" \
        --property vmware_disktype="sparse" \
        --property vmware_ostype="ubuntu64Guest" < ubuntuLTS-sparse.vmdk
```

In diesem Beispiel werden die folgenden Parameter und Einstellungen verwendet.

Parameter oder Einstellung	Beschreibung
`--os-image-url http://123.456.7.8:9292`	Die URL des Quell-Images.
`name="ubuntu-sparse"`	Der Name des Quell-Images, in diesem Fall **`ubuntu-sparse`**.
`disk_format=vmdk`	Das Festplattenformat des Quell-Images. Sie können ISO, VMDK oder OVA angeben.
`container_format=bare`	Das Containerformat gibt an, ob das Image-Format Metadaten über die tatsächliche virtuelle Maschine enthält. Da die Containerformat-Zeichenfolge derzeit nicht von Glance verwendet wird, wird empfohlen, für diesen Parameter **`bare`** anzugeben.
`--visibility="public"`	Die Datenschutzeinstellung für das Image in OpenStack. Mit dem Wert **`public`** ist das Image für alle Benutzer verfügbar. Mit dem Wert **`private`** ist das Image nur für den aktuellen Benutzer verfügbar.

Parameter oder Einstellung	Beschreibung	
`--property vmware_adapter_type="lsiLogicsas"`	Während des Imports wird die VMDK-Festplatte geprüft, um ihre Adaptertypeigenschaft zu erfassen. Sie haben zudem die Möglichkeit, den `vmware_adaptertype` zu verwenden, um den Adaptertyp anzugeben. **Hinweis** Wenn Sie eine Festplatte mit dem Adaptertyp paraVirtual oder LSI Logic SAS verwenden, wird empfohlen, diesen Parameter zu verwenden. Beispiele: `vmware_adaptertype= lsiLogicsas` oder `vmware_adaptertype= paraVirtual`.	
`--property vmware_disk_type="sparse"`	Während des Imports wird der VMDK-Festplattentyp geprüft, um die Festplattentypeigenschaft zu erfassen. Sie haben zudem die Möglichkeit, den Festplattentyp mithilfe der Eigenschaft `vmware_disktype` anzugeben.	
	sparse	Diese Festplattentypeigenschaft gilt für monolithische Sparse-Festplatten.
	preallocated	Diese Festplattentypeigenschaft gilt für VMFS-Flat-Festplatten wie zum Beispiel Thick, Zeroedthick oder Eagerzeroedthick. Sollte keine angegeben sein, so ist dies die Standardeigenschaft.
	streamOptimized	Diese Festplattentypeigenschaft gilt für monolithische Sparse-Festplatten, die für Streaming optimiert sind. Sie können Festplatten mit geringem Rechenaufwand dynamisch in und aus diesem Format konvertieren.
`--property vmware_os_type="ubuntu64Guest"`	Der Name der Image-Datei, nachdem diese in den Imagedienst importiert wurde. Im obigen Beispiel lautet der daraus resultierende Name `ubuntuLTS-sparse.vmdk`.	

3 (Optional) Bestätigen Sie in der Computing-Komponente, dass das Image erfolgreich importiert wurde.

```
$ glance image-list
```

Der Befehl gibt eine Liste aller Images zurück, die im Imagedienst verfügbar sind.

Importieren von Images in nicht unterstützten Formaten unter Verwendung der Befehlszeilenschnittstelle

Sie können Images in nicht unterstützten Image-Formaten wie RAW, QCOW2, VDI oder VHD importieren, indem Sie das Tool `glance-import` in der Befehlszeilenschnittstelle verwenden. Dieses Tool konvertiert automatisch das Quell-Image in das VMDK-Format.

Sie können auch das Tool `glance-import` verwenden, um Images in den unterstützten Formaten OVA und VMDK zu importieren.

Voraussetzungen

- Stellen Sie sicher, dass das Image im Format RAW, QCOW2, VDI oder VHD gepackt ist.
- Stellen Sie sicher, dass das Image auf einem Server ohne Anmeldedaten gehostet ist, damit einfache HTTP-Anforderungen zulässig sind.
- Stellen Sie sicher, dass der VMware Integrated OpenStack-Controller auf den gehosteten Server zugreifen kann, auf dem das Image gespeichert ist.

Vorgehensweise

1 Melden Sie sich unter Verwendung von SSH bei VMware Integrated OpenStack Manager an.

2 Verwenden Sie in VMware Integrated OpenStack Manager SSH, um sich beim controller01-Knoten anzumelden.

3 Wechseln Sie zum Root-Benutzer.

```
sudo su –
```

4 Führen Sie die Datei `cloudadmin.rc` aus.

```
source cloudadmin.rc
```

5 Konfigurieren Sie den controller01-Knoten so, dass die interne VIP verwendet wird.

```
export OS_AUTH_URL=http://INTERNAL_VIP:35357/v2.0
```

6 Führen Sie den Befehl `glance–import` aus, um das Image zu importieren.

```
glance–import image_name image_format image_http_url
```

Parameter	Beschreibung
image-name	Geben Sie den Namen für das Image an, so wie er im Imagedienst erscheinen wird.
image_format	Geben Sie das Format der Quell-Image-Datei an. Images, die nicht im Format VMDK vorliegen, werden automatisch in das VMDK-Format konvertiert. Die folgenden Formate werden unterstützt: ■ VMDK ■ OVA ■ RAW ■ QCOW2 ■ VDI ■ VHD
image_http-url	Geben Sie den HTTP-Speicherort der Quell-Image-Datei an.

Beispiel:

```
glance–import cirros–img qcow2 https://launchpad.net/cirros/trunk/0.3.0/+download/cir–
ros–0.3.0–x86_64–disk.img
```

Die Befehlszeilenschnittstelle zeigt die Aufgabeninformationen und den Status, einschließlich der Aufgaben-ID und Image-ID.

```
Created import task with id 5cdc4a04–5c68–4b91–ac44–37da07ec82ec
Waiting for Task 5cdc4a04–5c68–4b91–ac44–37da07ec82ec to finish.
Current Status.. SUCCESS
Image cirros–img created with ID: 2120de75–0717–4d61–b5d9–2e3f16e79edc
```

7 (Optional) Bestätigen Sie, dass die Aufgabe zum Importieren erfolgreich abgeschlossen wurde.

Wenn das Image groß ist und viel Zeit benötigt, können Sie das Hilfsprogramm sicher beenden ohne den Vorgang zu beeinträchtigen und den Aufgabenstatus später überprüfen.

Hinweis Sie müssen die Aufgaben-ID kennen, um den Status überprüfen zu können.

```
glance ––os–image–api–version 2 task–show <task_id>
```

Beispiel:

```
glance ––os–image–api–version 2 task–show 5cdc4a04–5c68–4b91–ac44–37da07ec82ec
+------------+----------------------------------------------------------------------------+
| Property   | Value                                                                      |
+------------+----------------------------------------------------------------------------+
| created_at | 2015–10–15T21:20:59Z                                                       |
```

```
| expires_at | 2015-10-17T21:21:14Z                                                          |
| id         | 5cdc4a04-5c68-4b91-ac44-37da07ec82ec                                          |
| input      | {"image_properties": {"container_format": "bare", "name": "cirros-img"},      |
|            | "import_from_format": "qcow2", "import_from": "https://launchpad.net/         |
|            | cirros/trunk/0.3.0/+download/cirros-0.3.0-x86_64-disk.img"}                   |
| message    |                                                                               |
| owner      | def459fd05d7490e9fda07dbe6ee2d76                                              |
| result     | {"image_id": "2120de75-0717-4d61-b5d9-2e3f16e79edc"}                          |
| status     | success                                                                       |
| type       | import                                                                        |
| updated_at | 2015-10-15T21:21:14Z                                                          |
+------------+-------------------------------------------------------------------------------+
```

8 (Optional) Bestätigen Sie, dass der Import erfolgreich war.

Sie müssen die durch den Befehl glance-import erzeugte Image-ID kennen, um den Import zu bestätigen.

```
glance image-show <image_id>
```

Der Befehl gibt Details zum angegebenen Image zurück.

9 (Optional) Bestätigen Sie, dass das Image im Imagedienst enthalten ist.

```
glance image-list
```

Der Befehl gibt eine Liste aller Images zurück, die im Imagedienst verfügbar sind.

Ändern der Image-Einstellungen

Nach dem Laden eines Images können Sie die Image-Einstellungen, wie beispielsweise den Namen und die Beschreibung des Images sowie die öffentlichen und geschützten Einstellungen, ändern.

Vorgehensweise

1 Melden Sie sich beim VMware Integrated OpenStack-Dashboard als ein Cloud-Administrator an.

2 Wählen Sie das Administratorprojekt aus dem Dropdown-Menü in der Titelleiste aus.

3 Wählen Sie **Administrator > Systemfenster > Images** aus.

4 Wählen Sie das zu bearbeitende Image aus.

5 Klicken Sie in der Spalte „Aktionen“ auf **Images bearbeiten**.

6 Ändern Sie die Einstellungen nach Bedarf.

7 Klicken Sie auf **Image aktualisieren**.

Die Seite „Images“ wird erneut mit den geänderten Informationen angezeigt.

Ändern der Image-Ressourcen-Metadaten

Nachdem ein Image geladen wurde, können Sie die Image-Ressourcenmetadateneinstellungen durch Hinzufügen bzw. Entfernen von Metadaten-Tags für die Image-Definition modifizieren. Image-Ressourcenmetadaten können Endbenutzern dabei helfen, die Art eines Image zu bestimmen. Dies wird von zugeordneten OpenStack-Komponenten und Treibern verwendet, die an den Imagedienst gekoppelt sind.

Sie können Metadatendefinitionen auf der Seite „Metadaten-Definitionen“ verwalten, die sich unter **Admin > System > Metadatendefinitionen** befindet.

Vorgehensweise

1 Melden Sie sich beim VMware Integrated OpenStack-Dashboard als ein Cloud-Administrator an.

2 Wählen Sie das Administratorprojekt aus dem Dropdown-Menü in der Titelleiste aus.

3 Wählen Sie **Admin > System > Images**.

4 Klicken Sie auf das zu ändernde Image.

5 Klicken Sie in der Spalte „Aktionen“ der Image-Auflistung auf den nach unten gerichteten Pfeil und wählen Sie **Metadaten aktualisieren** aus.

6 Ändern Sie die Einstellungen nach Bedarf.

Das Dialogfeld „Metadaten aktualisieren“ verfügt über zwei Spalten. Rechts werden die Metadaten-Tags angezeigt, die bereits auf das Image angewendet werden. Die linke Spalte zeigt verfügbare Metadaten-Tags an, die nach Kategorie (wie Guest Customization, Instance Config Data usw.) gruppiert sind.

a Klicken Sie auf das Pluszeichen (+), um ein Metadaten-Tag zur Image-Definition hinzuzufügen.

Das Element wird in die Spalte „Vorhandene Metadaten“ verschoben und hervorgehoben.

b Geben Sie, sofern zutreffend, den Metadatenwert in das bereitgestellte Feld ein.

c Klicken Sie auf das Minus-Zeichen (-), um ein Metadaten-Tag aus der Image-Definition zu entfernen.

7 Klicken Sie auf **Speichern**.

Konfigurieren von Images für Windows-Gastanpassung

Sie können Images für Windows-Gastanpassung direkt im VMware Integrated OpenStack-Dashboard konfigurieren, indem Sie die Gast-Anpassungsmetadaten auf das Glance-Image anwenden, das verwendet wird, um eine Instanz zu erstellen.

Die Funktion „Windows-Gastanpassung“ stellt eine Alternative zur Cloud-Init-basierenden Methode zur Aktivierung von Gastanpassung bereit. Verwenden Sie nicht die Funktion VMware Integrated OpenStack-Windows-Gastanpassung, wenn ein Image zurzeit Cloud-Init verwendet.

Voraussetzungen

- Stellen Sie sicher, dass Sie beim VMware Integrated OpenStack-Dashboard als Cloud-Administrator angemeldet sind.
- Stellen Sie sicher, dass ein entsprechendes Windows-Betriebssystem-Image im Glance-Imagedienst verfügbar ist.
- Stellen Sie sicher, dass die korrekten Versionen des Tools „Microsoft System Preparation“ (sysprep) für jedes Gastbetriebssystem, das Sie anpassen möchten, in vSphere installiert sind. Siehe Installieren des Tools „Microsoft Sysprep“ in der vSphere-Produktdokumentation.
- Stellen Sie sicher, dass VMware Tools auf dem Quell-Image installiert ist.
- Stellen Sie sicher, dass die Image-Festplattentypeigenschaft den Image-Festplattentyp vor dem Import korrekt widerspiegelt.

  Dies gilt nur für Images, die zu Glance in VMware Integrated OpenStack-Versionen vor 2.0 importiert wurden. In Version 2.0.x und höher werden Image-Eigenschaften automatisch während des Glance-Importprozesses geprüft.

Vorgehensweise

1 Melden Sie sich beim VMware Integrated OpenStack-Dashboard als ein Cloud-Administrator an.

2 Wählen Sie das Administratorprojekt aus dem Dropdown-Menü in der Titelleiste aus.

3 (Optional) Zeigen Sie eine Vorschau der Gastanpassungsoptionen-Metadatendefinition an.

   a Wählen Sie **Admin > System > Metadatendefinitionen**.

   b Klicken Sie auf **Gastanpassungsoptionen**.

   c Klicken Sie auf die Registerkarte **Inhalte**.

   Sie können die Metadatendefinitionen nur im VMware Integrated OpenStack-Dashboard anzeigen. Sie können die Metadaten nicht ändern.

4 Wählen Sie **Admin > System > Images**.

5 Suchen Sie das zu ändernde Windows-Image.

6 Klicken Sie in der Spalte „Aktionen“ der Image-Auflistung auf den nach unten gerichteten Pfeil und wählen Sie **Metadaten aktualisieren** aus.

7 Erweitern Sie in der Spalte unter „Verfügbare Metadaten“ die Registerkarte **Gastanpassungsoptionen**.

Hinweis Ist die Registerkarte **Gastanpassungsoptionen** nicht verfügbar, sind die entsprechenden Metadateneigenschaften möglicherweise bereits konfiguriert.

8 Klicken Sie auf das Pluszeichen (+) neben der Gastanpassungsoption, die Sie hinzufügen möchten.

Tipp Sie können alle Optionen gleichzeitig hinzufügen, indem Sie das Pluszeichen (+) auf der oberen Registerkarte **Gastanpassungsoptionen** anklicken.

In der Spalte unter „Vorhandene Metadaten“ werden die neu hinzugefügten Metadateneigenschaften angezeigt.

Hinweis Sie müssen unter Umständen in dieser Spalte nach unten blättern, um die neu hinzugefügten Metadateneigenschaften einzusehen.

9 Konfigurieren Sie die Metadateneigenschaften.

Metadateneigenschaft	Beschreibung
Zählung Automatische Anmeldung	Wendet die Metadateneigenschaft `windows_logon_count` an. Geben Sie an, wie oft eine Anmeldung am Computer automatisch als Administrator erfolgen kann. Normalerweise ist dieser Wert auf „1“ eingestellt. Sie können den Wert jedoch erhöhen, sollte Ihre Konfiguration mehrere Neustarts erfordern. Dieser Wert kann durch die Liste mit Befehlen festgelegt werden, die durch den `GuiRunOnce`-Befehl ausgeführt werden.
Automatische Anmeldung	Wendet die Metadateneigenschaft `windows_auto_logon` an. Ist dies ausgewählt, wird die VM automatisch als Administrator angemeldet.
Maximale Anzahl an Verbindungen	Wendet die Metadateneigenschaft `windows_max_connect` an. Geben Sie die Anzahl an Client-Lizenzen für den Windows-Server, der installiert wird, ein. **Hinweis** Diese Eigenschaft wird nur angewendet, wenn die nachfolgend beschriebene `windows_license_mode`-Metadateneigenschaft auf `PerServer` eingestellt ist.
Produktschlüssel	Wendet die Metadateneigenschaft `windows_product_key` an. Geben Sie eine gültige Seriennummer ein, die in der Antwortdatei enthalten ist, wenn die Miniinstallation ausgeführt wird. **Hinweis** Diese Seriennummer wird ignoriert, wenn das ursprüngliche Gastbetriebssystem unter Verwendung einer Volumenlizenz-CD installiert wurde.

Metadateneigenschaft	Beschreibung
Serverlizenzierungsmodus	Wendet die Metadateneigenschaft `windows_license_mode` an. Wählen Sie den Lizenzierungsmodus aus, der Ihrem Quell-Image entspricht: `PerServer` oder `PerSeat`.
Windows-Arbeitsgruppe, der beigetreten werden soll	Wendet die Metadateneigenschaft `windows_join_workgroup` an. Wählen Sie die Arbeitsgruppe aus, der die VM beitreten sollte.

10 Klicken Sie auf **Speichern**.

Die Image-Metadaten werden nun für Windows-Gastanpassung konfiguriert und auf alle zukünftigen VMs angewendet, die über dieses Image erstellt werden.

Konfigurieren von QoS-Ressourcenzuteilung für Instanzen unter Verwendung von Image-Metadaten

Sie können die QoS-Ressourcenzuteilungen wie Grenzwerte, Reservierungen und Anteile für CPU, RAM, Datenträger-IOPS und virtuelle Netzwerkschnittstelle (VIF) steuern, indem Sie die Metadaten des zur Erstellung der Instanz verwendeten Quell-Image ändern. Alle nachfolgend erstellten Instanzen, die den Typ verwenden, erben die Metadateneinstellungen.

QoS-Ressourcenzuteilung für eine Instanz kann auch durch Typ-Metadaten angegeben werden. Im Falle eines Konflikts übersteuert die Image-Metadatenkonfiguration die Typ-Metadatenkonfiguration. Siehe „Konfigurieren von QoS Ressourcenzuteilung für Instanzen unter Verwendung von Typ-Metadaten“, auf Seite 114.

Voraussetzungen

- VMware Integrated OpenStack-Version 2.0.x oder höher erforderlich.
- vSphere-Version 6.0 oder höher erforderlich.
- Stellen Sie sicher, dass VMware Integrated OpenStack in vSphere ausgeführt wird.
- Stellen Sie sicher, dass Sie beim VMware Integrated OpenStack-Dashboard als Cloud-Administrator angemeldet sind.

Vorgehensweise

1 Melden Sie sich beim VMware Integrated OpenStack-Dashboard als ein Cloud-Administrator an.

2 Wählen Sie das Administratorprojekt aus dem Dropdown-Menü in der Titelleiste aus.

3 Wählen Sie **Admin > System > Images**.

4 Klicken Sie auf das zu ändernde Image.

5 Klicken Sie in der Spalte „Aktionen“ der Image-Auflistung auf den nach unten gerichteten Pfeil und wählen Sie **Metadaten aktualisieren** aus.

6 Erweitern Sie in der Spalte unter „Verfügbare Metadaten“ die Registerkarte **VMware Kontingent**.

Hinweis Ist die Registerkarte **VMware Kontingent** nicht verfügbar, sind die entsprechenden Metadateneigenschaften möglicherweise bereits konfiguriert.

7 Klicken Sie auf das Pluszeichen (+) neben der Metadateneigenschaft „VMware Kontingent“, die Sie hinzufügen möchten.

Tipp Sie können alle Optionen gleichzeitig hinzufügen, indem Sie auf das Pluszeichen (+) auf der Registerkarte **VMware Kontingent** klicken.

In der Spalte unter „Vorhandene Metadaten“ werden die neu hinzugefügten Metadateneigenschaften angezeigt.

8 Konfigurieren Sie die Metadateneigenschaften.

Metadateneigenschaft	Beschreibung
Kontingent: CPU-Grenzwert	Wendet die Metadateneigenschaft `quota_cpu_limit` an. Gibt den oberen Grenzwert für CPU-Zuweisung in MHz an. Dieser Parameter stellt sicher, dass die Instanz niemals mehr als den definierten Betrag an CPU-Zuweisung verwendet. Geben Sie **`0`** für unbegrenzte CPU-Zuweisung ein.
Kontingent: CPU-Reservierung	Wendet die Metadateneigenschaft `quota_cpu_reservation` an. Gibt die garantierte minimale CPU-Reservierung in MHz an. Dieser Parameter stellt sicher, dass die Instanz über den reservierten Betrag an CPU-Zyklen während des Ressourcenkonflikts verfügt.
Kontingent: Ebene CPU-Anteile	Wendet die Metadateneigenschaft `quota_cpu_shares_level` an. Gibt Ebene der Anteile an, die mit dem im Voraus definierten numerischen Wert von Anteilen verknüpft ist. Wenn die **`benutzerdefinierte`** Ebene ausgewählt ist, müssen Sie die Metadateneigenschaft `quota_cpu_shares_value` mit einbeziehen. Siehe „Kontingent: Wert CPU-Anteile“ nachfolgend.
Kontingent: Wert CPU-Anteile	Wendet die Metadateneigenschaft `quota_cpu_shares_value` an. Gibt die Anzahl der Anteile an, die der Instanz zugeteilt wurden. Wenden Sie diese Eigenschaft nur an, wenn Sie die Metadateneigenschaft `quota_cpu_shares_level` auf **`benutzerdefiniert`** einstellen. Anderenfalls wird diese Eigenschaft ignoriert.
Kontingent: Datenträger-E/A-Grenzwert	Wendet die Metadateneigenschaft `quota_disk_io_limit` an. Gibt den oberen Grenzwert für Datenträgertransaktionen in E/A-Operationen pro Sekunde (IOPS) in Sekunden an. Dieser Parameter stellt sicher, dass die Instanz niemals mehr als den definierten Betrag an Datenträger-IOPS verwendet, und dieser Parameter kann verwendet werden, um einen Grenzwert für die Datenträgerperformance der Instanz durchzusetzen. Geben Sie **`0`** für unbegrenzte IOPS ein.
Kontingent: Datenträger-E/A-Reservierung	Wendet die Metadateneigenschaft `quota_disk_io_reservation` an. Gibt die garantierten minimalen Datenträgertransaktionen in E/A-Operationen pro Sekunde (IOPS) in Sekunden an. Dieser Parameter stellt sicher, dass die Instanz den reservierten Betrag an Datenträger-IOPS während des Ressourcenkonflikts erhält.
Kontingent: Ebene Datenträger-E/A-Anteile	Wendet die Metadateneigenschaft `quota_disk_io_shares_level` an. Gibt Ebene der Anteile an, die mit dem im Voraus definierten numerischen Wert von Anteilen verknüpft ist. Wenn die **`benutzerdefinierte`** Ebene ausgewählt ist, müssen Sie die Metadateneigenschaft `quota_disk_io_shares_share` mit einschließen (Kontingent: Wert Datenträger-E/A-Anteile).
Kontingent: Wert Datenträger-E/A-Anteile	Wendet die Metadateneigenschaft `quota_disk_io_shares_share` an. Gibt die Anzahl der Anteile an, die der Instanz zugeteilt wurden. Wenden Sie diese Eigenschaft nur an, wenn Sie die Metadateneigenschaft `quota_disk_io_shares_level` auf **`benutzerdefiniert`** einstellen. Anderenfalls wird diese Eigenschaft ignoriert.

Metadateneigenschaft	Beschreibung
Kontingent: Grenzwert Arbeitsspeicher	Wendet die Metadateneigenschaft `quota_memory_limit` an. Gibt den oberen Grenzwert für Arbeitsspeicherzuweisung in MB an. Dieser Parameter stellt sicher, dass die Instanz niemals mehr als den definierten Betrag an Arbeitsspeicher verwendet. Geben Sie **0** für unbegrenzte Arbeitsspeicherzuteilung ein.
Kontingent: Reservierung Arbeitsspeicher	Wendet die Metadateneigenschaft `quota_memory_reservation` an. Gibt das garantierte Minimum der Arbeitsspeicherreservierung in MB an. Dieser Parameter stellt sicher, dass die Instanz den reservierten Betrag an Arbeitsspeicher während des Ressourcenkonflikts erhält.
Kontingent: Ebene Anteile Arbeitsspeicher	Wendet die Metadateneigenschaft `quota_memory_shares_level` an. Gibt Ebene der Anteile an, die mit dem im Voraus definierten numerischen Wert von Anteilen verknüpft ist. Wenn die **benutzerdefinierte** Ebene ausgewählt ist, müssen Sie die Metadateneigenschaft `quota_memory_shares_share` mit einschließen (Kontingent: Wert Anteile Arbeitsspeicher).
Kontingent: Wert Anteile Arbeitsspeicher	Wendet die Metadateneigenschaft `quota_memory_shares_share` an. Gibt die Anzahl der Anteile an, die der Instanz zugeteilt wurden. Wenden Sie diese Eigenschaft nur an, wenn Sie die Metadateneigenschaft `quota_memory_shares_level` auf **benutzerdefiniert** einstellen. Anderenfalls wird diese Eigenschaft ignoriert.
Kontingent: VIF-Grenzwert	Wendet die Metadateneigenschaft `quota_vif_limit` an. Gibt den oberen Grenzwert für VIF-Bandbreite in Mbit/s an. Dieser Parameter stellt sicher, dass VIF niemals mehr als den definierten Betrag an Bandbreite verwendet. Geben Sie **0** für unbegrenzte Bandbreitenzuteilung ein.
Kontingent: VIF-Reservierung	Wendet die Metadateneigenschaft `quota_vif_reservation` an. Gibt die garantierte minimale Bandbreite für VIF in Mbit/s an. Dieser Parameter stellt sicher, dass der virtuelle Adapter in der Instanz den reservierten Betrag an Bandbreite während des Ressourcenkonflikts erhält. Wenn die Instanz weniger als den reservierten Betrag verwendet, ist der Rest für andere virtuelle Adapter verfügbar.
Kontingent: Ebene VIF-Anteile	Wendet die Metadateneigenschaft `quota_vif_shares_level` an. Gibt Ebene der Anteile an, die mit dem im Voraus definierten numerischen Wert von Anteilen verknüpft ist. Wenn die **benutzerdefinierte** Ebene ausgewählt ist, müssen Sie die Metadateneigenschaft `quota_vif_shares_share` mit einschließen (Kontingent: Wert Anteile VIF).
Kontingent: Wert VIF-Anteile	Wendet die Metadateneigenschaft `quota_vif_shares_share` an. Für den Fall, dass „benutzerdefiniert“ verwendet wird, ist dies die Anzahl der Anteile.

9 Klicken Sie auf **Speichern**.

Die Image-Metadaten sind nun für Grenzwerte, Reservierungen und Anteile für CPU, IOPS, Arbeitsspeicher und Netzwerkbandbreite konfiguriert. Diese Konfiguration wird auf alle zukünftigen OpenStack-Instanzen angewendet, die mit diesem Image erstellt werden.

Löschen eines vorhandenen Images

Ein Image wird dauerhaft gelöscht und kann nicht wiederhergestellt werden. Sie müssen über Administratorberechtigungen verfügen, um ein Image zu löschen.

Vorgehensweise

1 Melden Sie sich beim VMware Integrated OpenStack-Dashboard als ein Cloud-Administrator an.

2 Wählen Sie das Administratorprojekt aus dem Dropdown-Menü in der Titelleiste aus.

3 Wählen Sie **Administrator > Systemfenster > Images** aus.

4 Wählen Sie mindestens ein zu löschendes Image aus.

5 Klicken Sie auf **Images löschen**.

6 Bestätigen Sie den Löschvorgang, wenn Sie dazu aufgefordert werden.

Migrieren von Images

Sie können Images zwischen Datenspeichern migrieren, ohne dass dabei die UUID oder Metadaten verloren bzw. geändert werden.

Bei diesem Vorgang müssen Sie den Images-Ordner aus dem aktuellen Datenspeicher in einen Offline-Datenspeicher kopieren und die Image-Speicherortkonfiguration des Imagedienstes ändern.

Vorgehensweise

1 Kopieren des Images-Ordners in den neuen Datenspeicher auf Seite 106

Kopieren Sie den Images-Ordner einschließlich des Ordnernamens und relativen Pfads in den neuen Datenspeicher.

2 Aktualisieren der Speicherortdaten von migrierten Images auf Seite 107

Nachdem Sie den Images-Ordner in einen Datenspeicher kopiert haben, müssen Sie die Speicherorteinstellung für jedes Image dem neuen Datenspeicher entsprechend aktualisieren.

Kopieren des Images-Ordners in den neuen Datenspeicher

Kopieren Sie den Images-Ordner einschließlich des Ordnernamens und relativen Pfads in den neuen Datenspeicher.

Voraussetzungen

Vergewissern Sie sich, dass sowohl der aktuelle Datenspeicher als auch der Zieldatenspeicher verfügbar sind.

Vorgehensweise

1 Melden Sie sich unter Verwendung von SSH bei demjenigen ESXi-Host an, auf den der aktuelle Imagedienst-Datenspeicher gemountet wird.

2 Wechseln Sie zum Root-Benutzer.

```
sudo su –
```

3 Suchen Sie den Images-Ordner.

Der Images-Ordner hat normalerweise den Namen `images` und befindet sich auf der obersten Ebene.

4 Kopieren Sie den Images-Ordner mithilfe des Befehls `cp` oder `scp` für Linux in den neuen Datenspeicher.

Wichtig Wenn Sie den Ordner in den neuen Datenspeicher kopieren, behalten Sie sowohl den Namen des Images-Ordners als auch den relativen Pfad bei.

Weiter

Sie müssen nun die Images-Daten bearbeiten und den neuen Speicherort entsprechend aktualisieren. Ausführliche Informationen finden Sie unter „Aktualisieren der Speicherortdaten von migrierten Images“, auf Seite 107.

Aktualisieren der Speicherortdaten von migrierten Images

Nachdem Sie den Images-Ordner in einen Datenspeicher kopiert haben, müssen Sie die Speicherorteinstellung für jedes Image dem neuen Datenspeicher entsprechend aktualisieren.

Voraussetzungen

- Stellen Sie sicher, dass der Images-Ordner in den neuen Datenspeicher kopiert wurde.
- Stellen Sie sicher, dass der Name des Images-Ordners und der relative Pfad im neuen Datenspeicher exakt mit denen im vorherigen Datenspeicher übereinstimmen.
- Stellen Sie sicher, dass Sie die Image-ID-Werte der Images kennen, die Sie aktualisieren möchten.

Vorgehensweise

1 Wiederholen Sie diesen Vorgang für alle Images, die migriert werden sollen.

2 Melden Sie sich unter Verwendung von SSH als Administrator bei VMware Integrated OpenStack Manager an.

3 Melden Sie sich unter Verwendung von SSH beim controller01-Knoten an.

4 Wechseln Sie zum Root-Benutzer.

```
sudo su –
```

5 Führen Sie die Datei `cloudadmin.rc` aus.

```
source cloudadmin.rc
```

6 (Optional) Zeigen Sie eine Liste mit Images an.

```
glance image–list
```

7 (Optional) Ermitteln Sie den Speicherort eines bestimmten Images.

Hinweis Um das Image angeben zu können, müssen Sie über die Image-ID verfügen.

```
glance ––os–image–api–version 2 image–show <image_id>
```

Der Image-Speicherort ist die URL, die durch den Parameter `locations` angegeben wird.

```
vsphere://<vcenter_ip>/folder/<image_folder_name>/<image_id>dcPath=<path_to_datacenter>&dsNa–
me=<old_datastore_name>
```

Beispiel:

```
vsphere://10.20.123.456/folder/images/6c4a7e0d–65e7–4f3c–9dde–0de75f729a0c
?dcPath=Datacenter1&dsName=old_ds
```

8 Aktualisieren Sie die Speicherort-URL des Images dem Zieldatenspeicher entsprechend, um die Migration eines einzelnen Images abzuschließen.

a Fügen Sie den neuen Speicherort zur Image-Konfiguration hinzu.

```
glance --os-image-api-version 2 location-add <image_id> --url <new_url>
```

Option	Beschreibung
image_id	Gibt das Image an, das geändert werden soll.
new_url	Die neue URL entspricht der vorherigen URL, außer wenn das Argument `dsName` den Namen des neuen Datenspeichers angibt. `vsphere://<vcenter_ip>/folder/<image_folder_name>/<image_id>dcPath=<path_to_datacenter>&dsName=<new_datastore_name>`

Wenn der Befehl eine Meldung `400 Bad Request: Invalid Location` zurückgibt, stellen Sie sicher, dass der Dateipfad des Images auf dem Zieldatenspeicher korrekt ist.

b Entfernen Sie den alten Speicherort aus der Image-Konfiguration.

```
glance --os-image-api-version 2 location-delete <image_id> --url <old_url>
```

c Zeigen Sie die Image-Informationen nochmals an, um sicherzustellen, dass der Parameter `locations` den neuen Datenspeicher korrekt angibt.

```
glance --os-image-api-version 2 image-show <image_id>
```

Das Image wurde erfolgreich migriert.

Hinzufügen einer VM-Vorlage als Image

Sie können Ihrer VMware Integrated OpenStack-Bereitstellung vorhandene VM-Vorlagen als Glance-Images hinzufügen. Dies ermöglicht Benutzern, Instanzen zu starten, startfähige Blockspeichervolumes zu erstellen und andere für Glance-Images verfügbare Funktionen zu nutzen.

Voraussetzungen

- Vergewissern Sie sich, dass sich die Vorlage der vorhandenen VMs im selben vCenter befindet wie Ihre VMware Integrated OpenStack-Bereitstellung.
- Stellen Sie sicher, dass folgende Voraussetzungen erfüllt sind.
  - Die VM-Vorlage verfügt nicht über mehrere Festplatten.
  - Die VM-Vorlage verfügt über kein CD-ROM-Laufwerk.
  - Die VM-Vorlage verfügt über kein Diskettenlaufwerk.

Vorgehensweise

1 Bereiten Sie die VM-Vorlage vor.

Konfigurieren Sie die Metadateneinstellungen nach Bedarf.

- Der Parameter `vmware_ostype` ist für Windows-Images notwendig, für Linux-Images jedoch optional.
- Der Parameter `hw_vif_model` wird zur Festlegung eines NIC-Typs empfohlen. Bestätigen Sie den korrekten NIC-Typ für diese Image-Vorlage, bevor Sie diese Einstellung festlegen. Wenn diese Einstellung z. B. nicht festgelegt ist, wird die Instanz standardmäßig mit der Netzwerkkarte E1000 bereitgestellt. Um zu gewährleisten, dass eine andere Netzwerkkarte bereitgestellt wird, legen Sie diese Einstellung entsprechend fest.

  Beispiel: Die Metadatendefinition zum Bereitstellen der Netzwerkkarte VMXNET3 lautet **`hw_vif_model=VirtualVmxnet3`**.

- Die folgenden Metadaten-Einstellungen sind nicht erforderlich.
  - `vmware_adaptertype`
  - `vmware_disktype`

2 Melden Sie sich beim OpenStack Management-Cluster an.

3 Führen Sie den `glance`-Befehl aus, um das Image abzurufen, zu definieren und zu importieren.

```
glance image-create --name <NAME> \
       --disk-format vmdk --container-format bare
       --property vmware_ostype=ubuntu64Guest
                            --property hw_vif_model=VirtualVmxnet3

glance location-add <glance_image_UUID> --url "vi://<vcenter-host>/<datacenter-path>/vm/<sub-
folders>/<template_name>"
```

Der Befehl `location-add` für den Speicherort verweist auf den Bestandspfad für die VM-Vorlage und kann sich entweder auf die VM oder den Host beziehen. Beispiel:

```
"vi://<datacenter-path>/vm/<template_name>"
or
"vi://<datacenter-path>/host/<host_name>/<template_name>"
```

Die Schlüsselwörter `vm` und `host` im Bestandspfad stehen für die Hierarchien **Ansicht 'VM und Vorlagen'** und **Ansicht 'Host und Cluster'** in Ihrem vSphere Web Client.

Ändern des Standardverhaltens für Nova-Snapshots

Standardmäßig sind Nova-Snapshots Glance-Images, die in dem für VMware Integrated OpenStack konfigurierten vCenter als VM-Vorlagen gespeichert und organisiert sind. Sie können dieses Verhalten so ändern, dass Snapshots stattdessen als Stream-optimierte VMDK-Festplatten gespeichert werden.

Vor VMware Integrated OpenStack 2.5 bestand das Standardverhalten darin, dass Nova-Snapshots als Stream-optimierte VMDK-Festplatten gespeichert wurden. Mit diesem Verfahren können Sie den Standard vor Version 2.5 wiederherstellen.

Vorgehensweise

1 Implementieren Sie die Datei `custom.yml`.

```
sudo mkdir -p /opt/vmware/vio/custom
sudo cp /var/lib/vio/ansible/custom/custom.yml.sample /opt/vmware/vio/custom/custom.yml
```

2 Öffnen Sie die Datei `/opt/vmware/vio/custom/custom.yml` in einem Texteditor.

a Heben Sie die Auskommentierung des Parameters `nova_snapshot_format` auf.

b Ändern Sie die Einstellung in **`streamOptimized`**.

```
##############################
# Glance Template Store
# options that affect the use of glance template store
##############################
#glance_default_store: vi
nova_snapshot_format: streamOptimized
#cinder_image_format: template
```

3 Speichern Sie die Datei `custom.yml`.

4 Übertragen Sie die neue Konfiguration auf Ihre VMware Integrated OpenStack-Bereitstellung.

```
viocli deployment configure
```

Hinweis Die Bereitstellung der Konfiguration im Push-Verfahren führt zu einer kurzen Unterbrechung der OpenStack-Dienste.

Ändern des Cinder-Standardverhaltens für das Hochladen auf Image

Standardmäßig erstellt die Blockspeicherfunktion „Hochladen auf Image“ ein Glance-Image von einem als VM-Vorlage gespeicherten und organisierten Cinder-Volume. Sie können dieses Verhalten so ändern, dass die Images stattdessen als Stream-optimierte VMDK-Festplatten gespeichert werden.

Vor VMware Integrated OpenStack 3.0 oder 3.1 bestand das Standardverhalten darin, dass die Glance-Images als Stream-optimierte VMDK-Festplatten gespeichert wurden. Mit diesem Verfahren können Sie den Standard vor Version 3.0 oder 3.1 wiederherstellen.

Vorgehensweise

1 Implementieren Sie die Datei `custom.yml`.

```
sudo mkdir –p /opt/vmware/vio/custom
     sudo cp /var/lib/vio/ansible/custom/custom.yml.sample
     /opt/vmware/vio/custom/custom.yml
```

2 Öffnen Sie die Datei `/opt/vmware/vio/custom/custom.yml` in einem Texteditor.

   a Heben Sie die Auskommentierung des Parameters `cinder_image_format` auf.

   b Ändern Sie die Einstellung in **`streamOptimized`**.

```
##############################
# Glance Template Store
# options that affect the use of glance template store
##############################
#glance_default_store: vi
#nova_snapshot_format: template
cinder_image_format: streamOptimized
```

3 Speichern Sie die Datei `custom.yml`.

4 Übertragen Sie die neue Konfiguration auf Ihre VMware Integrated OpenStack-Bereitstellung.

```
viocli deployment configure
```

Hinweis Die Bereitstellung der Konfiguration im Push-Verfahren führt zu einer kurzen Unterbrechung der OpenStack-Dienste.

Arbeiten mit Typen 7

In OpenStack ist ein Typ eine voreingestellte Konfiguration, die das Computing, den Arbeitsspeicher und die Speicherkapazität einer Instanz definiert. Wenn Sie eine Instanz erstellen, konfigurieren Sie den Server durch die Auswahl eines Typs. Administrative Benutzer können Typen erstellen, bearbeiten und löschen.

Löschen Sie keine Standardtypen.

Dieses Kapitel behandelt die folgenden Themen:

Konfigurationen für Standardtypen

Die OpenStack-Bereitstellung bietet fünf Standardtypen von sehr klein bis sehr groß.

Name	vCPUs	RAM (MB)	Festplatte (GB)
m1.tiny	1	512	1
m1.small	1	2048	20
m1.medium	2	4096	40
m1.large	4	8192	80
m1.xlarge	8	16384	160

Erstellen eines Typs

Administratoren können benutzerdefinierte Typen erstellen.

Voraussetzungen

Stellen Sie sicher, dass Sie beim VMware Integrated OpenStack-Dashboard als Cloud-Administrator angemeldet sind.

Vorgehensweise

1 Wählen Sie im VMware Integrated OpenStack-Dashboard das Administratorprojekt aus dem Dropdown-Menü in der Titelleiste aus.

2 Wählen Sie **Administrator > Systemfenster > Typen** aus.

3 Klicken Sie auf **Typ erstellen**.

4 Konfigurieren Sie im Dialogfeld „Typ erstellen“ den neuen Typ.

Parameter	Beschreibung
Name	Name für den Typ.
ID	Ganzzahl oder UUID4-Wert für die Angabe des Typs. Wenn dieser Parameter leer gelassen wird oder einen Wert von **`auto`** aufweist, generiert OpenStack automatisch eine UUID.
VCPUs	Anzahl der virtuellen CPUs, die eine aus diesem Typ erstellte Instanz verwendet.
RAM (MB)	RAM (in Megabyte) für aus diesem Typ erstellten virtuellen Maschinen.
Root-Festplatte (GB)	Festplatte (in Gigabyte) für die Root-Partition (/) in aus diesem Typ erstellten Instanzen.
Flüchtige Festplatte (GB)	Festplattenspeicher (in Gigabyte) zur Verwendung für die flüchtige Partition. Falls nicht angegeben, lautet der Standardwert 0. Flüchtige Festplatten bieten lokalen Festplattenspeicher, der mit dem Lebenszyklus einer VM-Instanz verknüpft ist. Wenn eine VM beendet wird, gehen alle Daten auf der flüchtigen Festplatte verloren. Flüchtige Festplatten sind nicht in Snapshots enthalten.
Swap-Festplatten (MB)	Zu verwendender Swap-Speicher (in Megabyte) Falls nicht angegeben, lautet der Standardwert 0.

5 Klicken Sie unten im Dialogfeld auf **Typ erstellen**, um den Vorgang abzuschließen.

6 (Optional) Geben Sie an, welche Projekte auf die aus bestimmten Typen erstellten Instanzen zugreifen können.

   a Klicken Sie auf der Seite „Typ“ in der Spalte „Aktionen“ der Instanz auf **Typ bearbeiten**.

   b Klicken Sie im Dialogfeld „Typ bearbeiten“ auf die Registerkarte **Typzugriff**.

   c Verwenden Sie die Steuerelemente zum Wechseln, um die Projekte auszuwählen, auf die die Instanz zugreifen kann.

   d Klicken Sie auf **Speichern**.

7 (Optional) Ändern Sie die Einstellungen eines bestimmten Typs.

   a Klicken Sie auf der Seite „Typ“ in der Spalte „Aktionen“ der Instanz auf **Typ bearbeiten**.

   b Ändern Sie im Dialogfeld „Typ bearbeiten“ die Einstellungen auf der Registerkarte **Typinformationen** oder **Typzugriff**.

   c Klicken Sie auf **Speichern**.

Löschen eines Typs

Sie können die Anzahl und Vielfalt von Typen verwalten, indem Sie unter anderem doppelte Vorkommen oder diejenigen löschen, die den Anforderungen der Benutzer nicht mehr entsprechen.

Hinweis Das Löschen eines Typs kann nicht rückgängig gemacht werden. Löschen Sie keine Standardtypen.

Voraussetzungen

Sie müssen als Cloud-Administrator beim VMware Integrated OpenStack-Dashboard angemeldet sein, um diese Aufgabe durchzuführen.

Vorgehensweise

1 Wählen Sie im VMware Integrated OpenStack-Dashboard das Administratorprojekt aus dem Dropdown-Menü in der Titelleiste aus.

2 Wählen Sie **Administrator > Systemfenster > Typen** aus.

3 Wählen Sie die zu löschenden Typen aus.

4 Klicken Sie auf **Typen löschen**.

5 Bestätigen Sie den Löschvorgang an der Eingabeaufforderung.

Ändern von Typ-Metadaten

Sie können die Metadaten eines Typs ändern, sodass Eigenschaften zu allen nachfolgend erstellten Instanzen, die den Typ verwenden, dynamisch hinzugefügt werden.

Sie können auch Image-Metadaten verwenden, um viele Einstellungen von Typ-Metadaten anzugeben. Wenn ein Konflikt auftritt, setzt die Image-Metadatenkonfiguration die Typ-Metadatenkonfiguration außer Kraft.

Voraussetzungen

- VMware Integrated OpenStack-Version 2.0.x oder höher erforderlich.
- vSphere-Version 6.0 oder höher erforderlich.
- Stellen Sie sicher, dass VMware Integrated OpenStack in vSphere ausgeführt wird.
- Stellen Sie sicher, dass Sie beim VMware Integrated OpenStack-Dashboard als Cloud-Administrator angemeldet sind.

Vorgehensweise

1 Melden Sie sich beim VMware Integrated OpenStack-Dashboard als ein Cloud-Administrator an.

2 Wählen Sie das Administratorprojekt aus dem Dropdown-Menü in der Titelleiste aus.

3 Wählen Sie **Administrator > System > Typen** aus.

4 (Optional) Erstellen Sie einen Typ, der für die beabsichtigte Verwendung der Metadatenanwendung charakteristisch ist.

Erstellen Sie einen benutzerdefinierten Typ, damit dieser die bestimmte Konfiguration enthält. Mit dem benutzerdefinierten Typ bleibt die ursprüngliche Typ-Konfiguration intakt und für die Erstellung weiterer Instanzen verfügbar.

5 Wählen Sie den zu ändernden Typ aus.

6 Klicken Sie in der Spalte „Aktionen“ der Image-Auflistung auf den nach unten gerichteten Pfeil und wählen Sie **Metadaten aktualisieren** aus.

7 Klicken Sie auf das Pluszeichen (+) neben den hinzuzufügenden Metadateneigenschaften.

In der Spalte unter „Vorhandene Metadaten“ werden die neu hinzugefügten Metadateneigenschaften angezeigt.

8 Konfigurieren Sie die Metadateneigenschaften.

Je nach Fall müssen Sie eine Option aus einer Dropdown-Liste auswählen oder einen Zeichenfolgenwert eingeben.

9 Klicken Sie auf **Speichern**.

Die neu hinzugefügten Typ-Metadateneigenschaften sind nun konfiguriert. Diese Konfiguration wird auf alle zukünftigen OpenStack-Instanzen angewendet, die mit diesem Typ erstellt werden.

Konfigurieren von QoS Ressourcenzuteilung für Instanzen unter Verwendung von Typ-Metadaten

Sie können die QoS-Ressourcenzuteilungen wie Grenzwerte, Reservierungen und Anteile für CPU, RAM, Datenträger-IOPS und virtuelle Netzwerkschnittstelle (VIF) steuern, indem Sie die Metadaten des zur Erstellung der Instanz verwendeten Typs ändern. Alle nachfolgend erstellten Instanzen, die den Typ verwenden, erben die Metadateneinstellungen.

QoS-Ressourcenzuteilung kann auch durch Image-Metadaten angegeben werden. Im Falle eines Konflikts übersteuert die Image-Metadatenkonfiguration die Typ-Metadatenkonfiguration. Siehe „Konfigurieren von QoS-Ressourcenzuteilung für Instanzen unter Verwendung von Image-Metadaten“, auf Seite 103.

Voraussetzungen

- VMware Integrated OpenStack-Version 2.0.x oder höher erforderlich.
- vSphere-Version 6.0 oder höher erforderlich.
- Stellen Sie sicher, dass VMware Integrated OpenStack in vSphere ausgeführt wird.
- Stellen Sie sicher, dass Sie beim VMware Integrated OpenStack-Dashboard als Cloud-Administrator angemeldet sind.

Vorgehensweise

1. Melden Sie sich beim VMware Integrated OpenStack-Dashboard als ein Cloud-Administrator an.
2. Wählen Sie das Administratorprojekt aus dem Dropdown-Menü in der Titelleiste aus.
3. Wählen Sie **Administrator > System > Typen** aus.
4. (Optional) Erstellen Sie einen Typ, der für den Satz an QoS-Ressourcenzuteilungen spezifisch ist.

   Sie müssen einen benutzerdefinierten Typ erstellen, damit dieser die bestimmte Konfiguration enthält. Damit bleibt die ursprüngliche Typ-Konfiguration intakt und für andere Einsätze verfügbar.
5. Wählen Sie den zu ändernden Typ aus.
6. Klicken Sie in der Spalte „Aktionen“ der Image-Auflistung auf den nach unten gerichteten Pfeil und wählen Sie **Metadaten aktualisieren** aus.
7. Erweitern Sie in der Spalte unter „Verfügbare Metadaten“ die Registerkarte **VMware Kontingent**.

   Hinweis Ist die Registerkarte „VMware Kontingent“ nicht verfügbar, sind die entsprechenden Metadateneigenschaften möglicherweise bereits konfiguriert.
8. Klicken Sie auf das Pluszeichen (+) neben der Metadateneigenschaft „VMware Kontingent“, die Sie hinzufügen möchten.

Tipp Sie können alle Optionen gleichzeitig hinzufügen, indem Sie auf das Pluszeichen (+) auf der Registerkarte „VMware Kontingent“ klicken.

In der Spalte unter „Vorhandene Metadaten“ werden die neu hinzugefügten Metadateneigenschaften angezeigt.

9 Konfigurieren Sie die Metadateneigenschaften.

Metadateneigenschaft	Beschreibung
Kontingent: CPU-Grenzwert	Wendet die Metadateneigenschaft `quota:cpu_limit` an. Gibt den oberen Grenzwert für CPU-Zuweisung in MHz an. Dieser Parameter stellt sicher, dass die Instanz niemals mehr als den definierten Betrag an CPU-Zuweisung verwendet. Geben Sie **`0`** für unbegrenzte CPU-Zuweisung ein.
Kontingent: CPU-Reservierung	Wendet die Metadateneigenschaft `quota:cpu_reservation` an. Gibt die garantierte minimale CPU-Reservierung in MHz an. Dieser Parameter stellt sicher, dass die Instanz über den reservierten Betrag an CPU-Zyklen während des Ressourcenkonflikts verfügt.
Kontingent: Ebene CPU-Anteile	Wendet die Metadateneigenschaft `quota:cpu_shares_level` an. Gibt Ebene der Anteile an, die mit dem im Voraus definierten numerischen Wert von Anteilen verknüpft ist. Wenn die **`benutzerdefinierte`** Ebene ausgewählt ist, müssen Sie die Metadateneigenschaft `quota:cpu_shares_value` mit einbeziehen. Siehe „Kontingent: Wert CPU-Anteile“ nachfolgend.
Kontingent: Wert CPU-Anteile	Wendet die Metadateneigenschaft `quota:cpu_shares_value` an. Gibt die Anzahl der Anteile an, die der Instanz zugeteilt wurden. Wenden Sie diese Eigenschaft nur an, wenn Sie die Metadateneigenschaft `quota:cpu_shares_level` auf **`benutzerdefiniert`** einstellen. Anderenfalls wird diese Eigenschaft ignoriert.
Kontingent: Datenträger-E/A-Grenzwert	Wendet die Metadateneigenschaft `quota:disk_io_limit` an. Gibt den oberen Grenzwert für Datenträgertransaktionen in E/A-Operationen pro Sekunde (IOPS) in Sekunden an. Dieser Parameter stellt sicher, dass die Instanz niemals mehr als den definierten Betrag an Datenträger-IOPS verwendet, und dieser Parameter kann verwendet werden, um einen Grenzwert für die Datenträgerperformance der Instanz durchzusetzen. Geben Sie **`0`** für unbegrenzte IOPS ein.
Kontingent: Datenträger-E/A-Reservierung	Wendet die Metadateneigenschaft `quota:disk_io_reservation` an. Gibt die garantierten minimalen Datenträgertransaktionen in E/A-Operationen pro Sekunde (IOPS) in Sekunden an. Dieser Parameter stellt sicher, dass die Instanz den reservierten Betrag an Datenträger-IOPS während des Ressourcenkonflikts erhält.
Kontingent: Ebene Datenträger-E/A-Anteile	Wendet die Metadateneigenschaft `quota:disk_io_shares_level` an. Gibt Ebene der Anteile an, die mit dem im Voraus definierten numerischen Wert von Anteilen verknüpft ist. Wenn die **`benutzerdefinierte`** Ebene ausgewählt ist, müssen Sie die Metadateneigenschaft `quota:disk_io_shares_share` mit einschließen (Kontingent: Wert Datenträger-E/A-Anteile).
Kontingent: Wert Datenträger-E/A-Anteile	Wendet die Metadateneigenschaft `quota:disk_io_shares_share` an. Gibt die Anzahl der Anteile an, die der Instanz zugeteilt wurden. Wenden Sie diese Eigenschaft nur an, wenn Sie die Metadateneigenschaft `quota:disk_io_shares_level` auf **`benutzerdefiniert`** einstellen. Anderenfalls wird diese Eigenschaft ignoriert.
Kontingent: Grenzwert Arbeitsspeicher	Wendet die Metadateneigenschaft `quota:memory_limit` an. Gibt den oberen Grenzwert für Arbeitsspeicherzuweisung in MB an. Dieser Parameter stellt sicher, dass die Instanz niemals mehr als den definierten Betrag an Arbeitsspeicher verwendet. Geben Sie **`0`** für unbegrenzte Arbeitsspeicherzuteilung ein.
Kontingent: Reservierung Arbeitsspeicher	Wendet die Metadateneigenschaft `quota:memory_reservation` an. Gibt das garantierte Minimum der Arbeitsspeicherreservierung in MB an. Dieser Parameter stellt sicher, dass die Instanz den reservierten Betrag an Arbeitsspeicher während des Ressourcenkonflikts erhält.

Metadateneigenschaft	Beschreibung
Kontingent: Ebene Anteile Arbeitsspeicher	Wendet die Metadateneigenschaft `quota:memory_shares_level` an. Gibt Ebene der Anteile an, die mit dem im Voraus definierten numerischen Wert von Anteilen verknüpft ist. Wenn die **`benutzerdefinierte`** Ebene ausgewählt ist, müssen Sie die Metadateneigenschaft `quota:memory_shares_share` mit einschließen (Kontingent: Wert Anteile Arbeitsspeicher).
Kontingent: Wert Anteile Arbeitsspeicher	Wendet die Metadateneigenschaft `quota:memory_shares_share` an. Gibt die Anzahl der Anteile an, die der Instanz zugeteilt wurden. Wenden Sie diese Eigenschaft nur an, wenn Sie die Metadateneigenschaft `quota:memory_shares_level` auf **`benutzerdefiniert`** einstellen. Anderenfalls wird diese Eigenschaft ignoriert.
Kontingent: VIF-Grenzwert	Wendet die Metadateneigenschaft `quota:vif_limit` an. Gibt den oberen Grenzwert für VIF-Bandbreite in Mbit/s an. Dieser Parameter stellt sicher, dass VIF niemals mehr als den definierten Betrag an Bandbreite verwendet. Geben Sie **`0`** für unbegrenzte Bandbreitenzuteilung ein.
Kontingent: VIF-Reservierung	Wendet die Metadateneigenschaft `quota:vif_reservation` an. Gibt die garantierte minimale Bandbreite für VIF in Mbit/s an. Dieser Parameter stellt sicher, dass der virtuelle Adapter in der Instanz den reservierten Betrag an Bandbreite während des Ressourcenkonflikts erhält. Wenn die Instanz weniger als den reservierten Betrag verwendet, ist der Rest für andere virtuelle Adapter verfügbar.
Kontingent: Ebene VIF-Anteile	Wendet die Metadateneigenschaft `quota:vif_shares_level` an. Gibt Ebene der Anteile an, die mit dem im Voraus definierten numerischen Wert von Anteilen verknüpft ist. Wenn die **`benutzerdefinierte`** Ebene ausgewählt ist, müssen Sie die Metadateneigenschaft `quota:vif_shares_share` mit einschließen (Kontingent: Wert Anteile VIF).
Kontingent: Wert VIF-Anteile	Wendet die Metadateneigenschaft `quota:vif_shares_share` an. Für den Fall, dass „benutzerdefiniert“ verwendet wird, ist dies die Anzahl der Anteile.

10 Klicken Sie auf **Speichern**.

Die Typ-Metadaten sind nun für Grenzwerte, Reservierungen und Anteile für CPU, IOPS, Arbeitsspeicher und Netzwerkbandbreite konfiguriert. Diese Konfiguration wird auf alle zukünftigen OpenStack-Instanzen angewendet, die mit diesem Typ erstellt werden.

Befehlsreferenz für die Befehlszeilenschnittstelle von VMware Integrated OpenStack

8

Der CLI-Befehl von VMware Integrated OpenStack weist spezifische Anforderungen an die Syntax auf.

Dieses Kapitel behandelt die folgenden Themen:

Befehl „viocli backup“

Verwenden Sie den Befehl `viocli backup`, um eine Sicherung der Verwaltungsserver-Daten oder der OpenStack-Datenbank zu erstellen. Bei diesem Befehl muss ein NFS-Server verfügbar sein, damit die VMware Integrated OpenStack-Befehlszeile gemountet werden kann.

Der Befehl `viocli backup` verwendet die folgende Syntax.

```
viocli backup mgmt_server [-d NAME] NFS_VOLUME [-h] [-v]
viocli backup openstack_db [-d NAME] NFS_VOLUME [-h] [-v]
```

Parameter	Obligatorisch oder Optional	Beschreibung
`-d, --deployment` *NAME*	Automatisch	Name der zu verwendenden Bereitstellung. Wird automatisch angewendet. Der Standardwert ist der Name der aktuellen Bereitstellung.
NFS_VOLUME	Obligatorisch	Name oder IP-Adresse des NFS-Ziel-Volumes und des Verzeichnisses im Format *remote_host:remote_dir*. Beispiel: 192.168.1.77:/backups
`-h, --help`	Optional	Die Verwendung und Argumente für diesen Befehl werden angezeigt.
`-v, --verbose`	Optional	Der ausführliche Modus wird gestartet.

Die Sicherungsdatei des Verwaltungsservers von VMware Integrated OpenStack wird mit dem Zeitstempel `vio_ms_yyyymmddhhmmss` versehen. Die Sicherungsdatei des Datenbank von VMware Integrated OpenStack wird mit dem Zeitstempel `vio_os_db_yyyymmddhhmmss` versehen.

Befehl „viocli dbverify“

Verwenden Sie den Befehl `viocli dbverify`, um die VMware Integrated OpenStack-Datenbank auf bekannte Probleme zu überprüfen, wie beispielsweise doppelte oder fehlende Schlüssel, die Probleme beim Upgrade-Vorgang verursachen können.

Der Befehl `viocli dbverify` verwendet die folgende Syntax.

```
viocli dbverify [-d NAME] [-h] [-v]
```

Parameter	Obligatorisch oder Optional	Beschreibung
`-d, --deployment` *NAME*	Automatisch	Name der zu verwendenden Bereitstellung. Wird automatisch angewendet. Der Standardwert ist der Name der aktuellen Bereitstellung.
`-h, --help`	Optional	Die Verwendung und Argumente für diesen Befehl werden angezeigt.
`-v, --verbose`	Optional	Der ausführliche Modus wird gestartet.

Befehl „viocli deployment“

Verwenden Sie den Befehl `viocli deployment`, um Ihre VMware Integrated OpenStack-Bereitstellung zu verwalten.

Der Befehl `viocli deployment` verwendet die folgende Syntax.

```
viocli deployment ACTION [-d NAME] [-p] [-h] [-v]
```

Parameter	Obligatorisch oder Optional	Beschreibung	
`ACTION` Verwenden Sie eines der folgenden Positionsargumente: ■ `start` ■ `stop` ■ `pause` ■ `resume` ■ `configure` ■ `cert-req-create` ■ `cert-update` ■ `getlogs` ■ `status`	Obligatorisch	**`start`**	Die Bereitstellung wird gestartet.
		`stop`	Die Bereitstellung wird beendet.
		`pause`	Die Bereitstellung wird angehalten.
		`resume`	Die angehaltene Bereitstellung wird fortgesetzt.
		`configure`	Die gesamte Bereitstellung wird neu konfiguriert.
		`cert-req-create`	Es wird eine Anforderung für eine Zertifikatssignierung für eine Zertifizierungsstelle erstellt.
		`cert-update`	VMware Integrated OpenStack wird mit dem bereitgestellten Zertifikat aktualisiert.
		`getlogs`	Es werden Protokolldateien für die aktuelle Bereitstellung generiert, einschließlich der von Ansible ausgeführten Befehle und der entsprechenden Ausgabe. Protokolldateien werden in `/var/log/viocli/viocli.log` geschrieben und nach jeweils 100 MB rotiert, wobei maximal sieben Mal rotiert wird.
		`status`	Es werden Berichte zu den folgenden möglichen Problemen generiert: ■ Synchronisierungsfehler zwischen dem Verwaltungsserver und den OpenStack-Knoten, einschließlich des Zeitpunkts des Auftretens, des betroffenen Knotens und des Grundes für den Status „Fehlgeschlagen“. ■ Verbindungen zu OpenStack-Vorgängen und durchschnittliche Verbindungsanzahl. ■ Getrennte Netzwerkverbindungen, einschließlich des Zeitpunkts des Auftretens, Hostnamens und Ports mit der fehlgeschlagenen Verbindung, oder des Einzelhosts (sofern vorhanden). ■ Probleme mit der OpenStack-Datenbank, einschließlich des Zeitpunkts des Auftretens, des Status „Fehlgeschlagen“ oder „Erfolgreich“, des Grunds für den Fehler (sofern vorhanden) und der aktuellen Größe des Datenbankclusters. ■ Fehlende Vorgänge, einschließlich des Zeitpunkts des Auftretens, betroffenen Knotens, Status und des Grunds für den Fehler (sofern vorhanden).
`-d, --deployment` *NAME*	Automatisch	Name der zu verwendenden Bereitstellung. Wird automatisch angewendet. Der Standardwert ist der Name der aktuellen Bereitstellung.	
`-p, --progress`	Optional	Der Fortschritt beim aktuellen Aktualisierungsvorgang wird angezeigt.	
`-h, --help`	Optional	Die Verwendung und Argumente für diesen Befehl werden angezeigt.	
`-v, --verbose`	Optional	Der ausführliche Modus wird gestartet.	

Befehl „viocli ds-migrate-prep“

Verwenden Sie den Befehl `viocli ds-migrate-prep`, um einen Datenspeicher auf die Wartung vorzubereiten. Mit dem Befehl `viocli ds-migrate-prep` können Sie sicherstellen, dass der angegebene Datenspeicher in Ihrer VMware Integrated OpenStack-Bereitstellung keine beschädigten Verweise enthält.

Der Befehl `viocli ds-migrate-prep` verwendet die folgende Syntax.

```
viocli ds-migrate-prep [-d NAME] DC_NAME DS_NAME [-h] [-v]
```

Parameter	Obligatorisch oder Optional	Beschreibung
`-d, --deployment` *NAME*	Automatisch	Name der zu verwendenden Bereitstellung. Wird automatisch angewendet. Der Standardwert ist der Name der aktuellen Bereitstellung.
DC_NAME	Obligatorisch	Gibt Datencenter nach Namen an.
DS_NAME	Obligatorisch	Gibt Datenspeicher nach Namen an.
`-h, --help`	Optional	Die Verwendung und Argumente für diesen Befehl werden angezeigt.
`-v, --verbose`	Optional	Der ausführliche Modus wird gestartet.

Der Befehl „viocli epops“

Verwenden Sie den Befehl `viocli epops`, um den Endpoint Operations Management Agent zu verwalten.

VMware Integrated OpenStack wurde mit vRealize Operations Manager 6.2.1 getestet.

Der Befehl `viocli Endpoint Operations` verwendet die folgende Syntax.

```
viocli epops ACTION [-d NAME] [-h] [-v]
```

Parameter	Obligatorisch oder Optional	Beschreibung	
`ACTION` Verwenden Sie eines der folgenden Positionsargumente: ■ `install` ■ `uninstall` ■ `config` ■ `start` ■ `stop`	Obligatorisch	**`install`**	Installiert den Endpoint Operations Management Agent.
		`uninstall`	Deinstalliert den Endpoint Operations Management Agent.
		`config`	Konfiguriert den Endpoint Operations Management Agent.
		`start`	Startet den Endpoint Operations Management Agent.
		`stop`	Beendet den Endpoint Operations Management Agent.
`-d, --deployment` *NAME*	Automatisch	Name der zu verwendenden Bereitstellung. Wird automatisch angewendet. Der Standardwert ist der Name der aktuellen Bereitstellung.	
`-h, --help`	Optional	Die Verwendung und Argumente für diesen Befehl werden angezeigt.	
`-v, --verbose`	Optional	Der ausführliche Modus wird gestartet.	

Befehl `viocli inventory-admin`

Verwenden Sie den Befehl `viocli inventory-admin`, um die Computing- und Blockspeicher-Bestandslisten mit der vSphere-Bestandsliste zu vergleichen und um verwaiste Objekte zu ermitteln und zu entfernen. Verwaiste Instanzen sind Instanzen, die in OpenStack und vSphere nicht über entsprechende VMs verfügen.

Der Befehl `viocli inventory-admin` erfasst vCenter- und OpenStack-Anmeldedaten aus internen Bestandslisten. Für diesen Befehl müssen Sie das OpenStack-Administratorkennwort eingeben. Wenn Sie das Kennwort nicht jedes Mal eingeben möchten, legen Sie die Umgebungsvariable OS_PASSWORD fest.

Der Befehl `viocli inventory-admin` verwendet die folgende Syntax.

```
viocli inventory-admin SHOW_ACTION [-d NAME] [--json] \
       [--pretty] [--all] [--no-grace-period] \
       [--force] [-h] [-v]

viocli inventory-admin CLEAN_ACTION [-d NAME] [--json] \
       [--pretty] [--all] [--no-grace-period] \
       [--force] [-h] [-v]
```

Parameter	Obligatorisch oder Optional	Beschreibung	
`SHOW_ACTION` Verwenden Sie eines der folgenden Positionsargumente: ■ `show-instances` ■ `show-instance-vms` ■ `show-shadow-vms`	Obligatorisch	**`show-instances`**	Es werden verwaiste OpenStack-Instanzen angezeigt.
		`show-instance-vms`	Es werden verwaiste vSphere-Instanzen angezeigt.
		`show-shadow-vms`	Es werden verwaiste Volume-Schatten-VMs angezeigt. Hierbei handelt es sich um Volume-VMs, die über keine entsprechenden Blockspeicher-Volumes in der OpenStack-Datenbank verfügen.
`CLEAN_ACTION` Verwenden Sie eines der folgenden Positionsargumente: ■ `clean-instances` ■ `clean-instance-vms` ■ `clean-shadow-vms`	Obligatorisch	**`clean-instances`**	Es werden verwaiste OpenStack-Instanzen entfernt.
		`clean-instance-vms`	Es werden verwaiste vSphere-Instanzen entfernt.
		`clean-shadow-vms`	Es werden verwaiste Volume-Schatten-VMs entfernt. Hierbei handelt es sich um Volume-VMs, die über keine entsprechenden Blockspeicher-Volumes in der OpenStack-Datenbank verfügen.
`-d, --deployment` *NAME*	Automatisch	Name der zu verwendenden Bereitstellung. Wird automatisch angewendet. Der Standardwert ist der Name der aktuellen Bereitstellung.	
`--json`	Optional	Die Ausgabe wird im JSON-Format zurückgegeben. Dies ist das Standardformat, wenn der Befehl nicht interaktiv verwendet wird.	
`--pretty`	Optional	Die Ausgabe wird im für Benutzer lesbaren Format zurückgegeben. Dies ist das Standardformat, wenn der Befehl interaktiv verwendet wird.	
`--all`	Optional	Alle Objekte werden angezeigt. Beim Standard werden nur verwaiste Objekte angezeigt.	
`--no-grace-period`	Optional	Die Standardeinstellung für die Toleranzperiode wird deaktiviert. Wenn keine Toleranzperiode festgelegt wird, ignoriert dieser Befehl alle Objekte, die in den letzten 30 Minuten erstellt oder geändert wurden.	
`-f, --force`	Optional	Der Vorgang wird ohne Bestätigungsanforderung ausgeführt.	

Parameter	Obligatorisch oder Optional	Beschreibung
`-h, --help`	Optional	Die Verwendung und Argumente für diesen Befehl werden angezeigt.
`-v, --verbose`	Optional	Der ausführliche Modus wird gestartet.

Befehl „viocli recover“

Verwenden Sie den Befehl `viocli recover`, um einen Knoten oder eine Knotengruppe wiederherzustellen. Da die meisten OpenStack-Knoten statusfrei sind, können Sie diese ohne Sicherung wiederherstellen. Bei OpenStack-Datenbankknoten müssen Sie über eine Sicherungsdatei verfügen. Ein NFS-Pfad ist erforderlich. Verwenden Sie den Befehl `viocli show`, um eine detaillierte Liste mit OpenStack-Knoten in Ihrer Bereitstellung anzuzeigen.

Der Befehl `viocli recover` verwendet die folgende Syntax.

```
viocli recover [-d [NAME]] <-r ROLE1,ROLE2... | -n NODE1,NODE2...> \
               [-dn BACKUP_NAME] [-nfs NFS_VOLUME] [-h] [-v]
```

Parameter	Obligatorisch oder Optional	Beschreibung
`-d, --deployment` *NAME*	Automatisch	Name der Bereitstellung, in der die wiederherzustellenden Knoten enthalten sind. Wird automatisch angewendet. Der Standardwert ist der Name der aktuellen Bereitstellung.
`-r, --role` *ROLLE*	Obligatorisch, außer wenn KNOTEN angegeben ist.	Stellt alle Knoten wiederher, die einer bestimmten Rolle zugewiesen sind. Sie können mehrere Rollen in einem Befehl angeben. Sie können auch den Parameter `-n, --node` an denselben Befehl anhängen, um zusätzliche Knoten wiederherzustellen, die dieser Rolle zugewiesen sind. Verwenden Sie den Gruppennamen, wie er im VMware Integrated OpenStack Manager angezeigt wird. Um den Gruppennamen anzuzeigen, wählen Sie **VMware Integrated OpenStack > OpenStack-Bereitstellungen > [Bereitstellungsname]**. Die gültigen Rollennamen sind: **`ComputeDriver`**, **`Controller`**, **`DB`**, **`LoadBalancer`**. Beispiel: Mit dem folgenden Befehl werden die Knoten in der DB-Knotengruppe aus der angegebenen NFS-Sicherungsdatei wiederhergestellt. `viocli recover -r DB -dn vio_os_db_20150830215406 -nfs 10.146.29.123:/backups`
`-n, --node` *KNOTEN*	Obligatorisch, außer wenn ROLLE angegeben ist.	Stellt einen bestimmten Knoten wiederher. Sie können mehrere Knoten in einem Befehl angeben. Verwenden Sie den VM-Namen, wie er im VMware Integrated OpenStack Manager angezeigt wird. Um den Namen anzuzeigen, wählen Sie **VMware Integrated OpenStack > OpenStack-Bereitstellungen > [Bereitstellungsname]**. Beispiel: Mit dem folgenden Befehl werden die angegebenen Datenbankknoten (VIO-DB-0, VIO-DB-1 und VIO-DB-2) aus der angegebenen NFS-Sicherungsdatei wiederhergestellt. `viocli recover -n VIO-DB-0 VIO-DB-1 VIO-DB-2 -dn vio_os_db_20150830215406 -nfs 10.146.29.123:/backups`
`-dn, --dir-name` *BACKUP_NAME*	Obligatorisch für die Wiederherstellung einer OpenStack-Datenbank.	Gibt den Zeitstempel der Sicherungsdatei an, die zur Wiederherstellung der Datenbank verwendendet werden soll.

Parameter	Obligatorisch oder Optional	Beschreibung	
Verwenden Sie für die Wiederherstellung einer Datenbank eines der folgenden Positionsargumente: ■ *DIR_NAME* ■ *NFS_VOLUME*	Obligatorisch für die Wiederherstellung einer OpenStack-Datenbank.	***DIR_NAME***	Name des NFS-Verzeichnisses, in dem die Sicherungsdatei der Datenbank enthalten ist.
		NFS_VOLUME	Name oder IP-Adresse des NFS-Ziel-Volumes und des Verzeichnisses, in dem die Sicherungsdatei der Datenbank enthalten ist. Verwenden Sie das folgende Format: *remote_host:remote_dir*. Beispiel: `192.168.1.77:/backups`.
`-h, --help`	Optional	Die Verwendung und Argumente für diesen Befehl werden angezeigt.	
`-v, --verbose`	Optional	Der ausführliche Modus wird gestartet.	

Befehl „viocli restore“

Verwenden Sie den Befehl `viocli restore`, um eine Bereitstellung aus einer Sicherungsdatei wiederherzustellen, die zuvor mithilfe des `viocli backup`-Befehls erstellt wurde. Sie können eine Sicherung der Verwaltungsserver-Daten oder der OpenStack-Datenbank wiederherstellen.

Der Befehl `viocli restore` verwendet die folgende Syntax.

```
viocli restore mgmt_server [-d [NAME]] <DIR_NAME | NFS_VOLUME> [-h] [-v]
viocli restore openstack_db [-d [NAME]] <DIR_NAME | NFS_VOLUME> [-h] [-v]
```

Parameter	Obligatorisch oder Optional	Beschreibung	
`-d, --deployment` *NAME*	Automatisch	Name der zu verwendenden Bereitstellung. Wird automatisch angewendet. Der Standardwert ist der Name der aktuellen Bereitstellung.	
Verwenden Sie eines der folgenden Positionsargumente: ■ *DIR_NAME* ■ *NFS_VOLUME*	Obligatorisch	***DIR_NAME***	Name des NFS-Verzeichnisses, in dem die Sicherungsdatei enthalten ist.
		NFS_VOLUME	Name oder IP-Adresse des NFS-Ziel-Volumes und des Verzeichnisses im Format *remote_host:remote_dir*. Beispiel: 192.168.1.77:/backups.
`-h, --help`	Optional	Die Verwendung und Argumente für diesen Befehl werden angezeigt.	
`-v, --verbose`	Optional	Der ausführliche Modus wird gestartet.	

Die Sicherungsdatei des Verwaltungsservers von VMware Integrated OpenStack wird mit dem Zeitstempel `vio_ms_yyyymmddhhmmss` versehen. Die Sicherungsdatei des Datenbank von VMware Integrated OpenStack wird mit dem Zeitstempel `vio_os_db_yyyymmddhhmmss` versehen.

Befehl „viocli rollback“

Verwenden Sie den Befehl `viocli rollback`, um bei einem aktuellen Upgrade ein Rollback auf VMware Integrated OpenStack durchzuführen. Verwenden Sie den VMware Integrated OpenStack Manager in vSphere Web Client, um das Rollback durchzuführen.

Der Befehl `viocli rollback` verwendet die folgende Syntax.

```
viocli rollback [-d NAME] [-p] [-h] [-v] [-f]
```

Parameter	Obligatorisch oder Optional	Beschreibung
`-d, --deployment` *NAME*	Automatisch	Name der zu verwendenden Bereitstellung. Wird automatisch angewendet. Der Standardwert ist der Name der aktuellen Bereitstellung.
`-p, --progress`	Optional	Der Fortschritt beim aktuellen Aktualisierungsvorgang wird angezeigt.
`-h, --help`	Optional	Zeigt die Verwendung und Argumente für diesen Befehl an.
`-v, --verbose`	Optional	Der ausführliche Modus wird gestartet.
`-f, --force`	Optional	Der Vorgang wird ohne Bestätigungsanforderung ausgeführt.

Befehl „viocli services“

Verwenden Sie den Befehl `viocli services`, um OpenStack-Dienste zu starten oder zu beenden. Der Unterschied zwischen `viocli deployment stop` und `viocli services stop` liegt darin, dass bei Ersterem der gesamte Cluster einschließlich virtueller Maschinen beendet wird. Bei Letzterem werden nur die Dienste beendet, die auf den virtuellen Maschinen im Cluster ausgeführt werden.

Der Befehl `viocli services` verwendet die folgende Syntax.

```
viocli services ACTION [-d NAME] [-h] [-v]
```

Parameter	Obligatorisch oder Optional	Beschreibung	
`ACTION` Verwenden Sie eines der folgenden Positionsargumente: ■ `start` ■ `stop`	Obligatorisch	**`start`** **`stop`**	Die Bereitstellung wird gestartet. Die Bereitstellung wird beendet.
`-d, --deployment` *NAME*	Automatisch	Name der zu verwendenden Bereitstellung. Wird automatisch angewendet. Der Standardwert ist der Name der aktuellen Bereitstellung.	
`-h, --help`	Optional	Zeigt die Verwendung und Argumente für diesen Befehl an.	
`-v, --verbose`	Optional	Der ausführliche Modus wird gestartet.	

Befehl „viocli show“

Verwenden Sie den Befehl `viocli show`, um eine Liste mit Knoten in einer VMware Integrated OpenStack-Bereitstellung anzuzeigen, oder um detaillierte Informationen zur Bestandsliste einer Bereitstellung zu erhalten.

Der Befehl `viocli show` verwendet die folgende Syntax.

```
viocli show [-p] [-i] [-d NAME] [-h] [-v]
```

Parameter	Obligatorisch oder Optional	Beschreibung
`-p, --inventory-path`	Optional	Zeigt den Pfad der Bestandsliste an, der für die aktuelle Bereitstellung verwendet wird.
`-i, --inventory`	Optional	Zeigt den Inhalt der Bestandslistendatei an, der für die aktuelle Bereitstellung verwendet wird.

Parameter	Obligatorisch oder Optional	Beschreibung
`-d, --deployment` *NAME*	Automatisch	Name der zu verwendenden Bereitstellung. Wird automatisch angewendet. Der Standardwert ist der Name der aktuellen Bereitstellung.
`-h, --help`	Optional	Zeigt die Verwendung und Argumente für diesen Befehl an.
`-v, --verbose`	Optional	Der ausführliche Modus wird gestartet.

Befehl „viocli upgrade“

Verwenden Sie den Befehl `viocli upgrade`, um Upgrades von bzw. auf Hauptversionen von VMware Integrated OpenStack durchzuführen. Verwenden Sie den VMware Integrated OpenStack Manager in vSphere Web Client, um das Upgrade durchzuführen.

Der Befehl `viocli upgrade` verwendet die folgende Syntax.

```
viocli upgrade [-d NAME] [-n NEW_DEPLOYMENT_NAME] \
               [--public-vip PUBLIC_VIP] [--internal-vip INTERNAL_VIP] \
               [-p] [-h] [-v] [-f]
```

Parameter	Obligatorisch oder Optional	Beschreibung
`-d, --deployment` *NAME*	Automatisch	Name der zu verwendenden Bereitstellung. Wird automatisch angewendet. Der Standardwert ist der Name der aktuellen Bereitstellung.
`-n, --new-deployment` *NEUER_BEREITSTELLUNGS-NAME*	Obligatorisch	Name der Upgrade-Bereitstellung.
`--public-vip` *ÖFFENTLI-CHE_VIP*	Obligatorisch	Temporäre öffentliche VIP-Adresse, die der neuen Bereitstellung zugewiesen wurde.
`--internal-vip` *INTER-NE_VIP*	Obligatorisch	Temporäre private VIP-Adresse, die der neuen Bereitstellung zugewiesen wurde.
`-p, --progress`	Optional	Der Fortschritt beim aktuellen Aktualisierungsvorgang wird angezeigt.
`-h, --help`	Optional	Die Verwendung und Argumente für diesen Befehl werden angezeigt.
`-v, --verbose`	Optional	Der ausführliche Modus wird gestartet.
`-f, --force`	Optional	Der Vorgang wird ohne Bestätigungsanforderung ausgeführt.

Befehl „viocli volume-migrate“

Verwenden Sie den Befehl `viocli volume-migrate`, um nicht verbundene Volumes von einem Datenspeicher auf einen anderen zu migrieren.

- Die Migration eines Volumes schlägt fehl, wenn es sich um ein angehängtes Volume handelt.

  Migrieren Sie in diesem Fall die entsprechende Instanz. Angehängte Volumes werden mit der Instanz migriert.

  Hinweis Entsprechende Volume-Schatten-VMs werden nicht migriert. Wenn Sie eine Volume-Schatten-VM migrieren möchten, führen Sie den Befehl „Befehl „viocli ds-migrate-prep““, auf Seite 120 aus und migrieren Sie die Schatten-VM anschließend mithilfe des vSphere Web Client.

- Die Migration eines Volumes schlägt fehl, wenn das Volume eine Speicherrichtlinie aufweist, die der Zieldatenspeicher nicht erfüllt.

  Durch das Hinzufügen des Parameters `--ignore-storage-policy` können Sie die Migration erzwingen. Der Befehl gibt eine Warnung aus, wenn die Speicherrichtlinie bei einer Migration zu einem nicht übereinstimmenden Datenspeicher ignoriert wird.

Der Befehl `viocli volume-migrate` verwendet die folgende Syntax.

```
viocli volume-migrate [-d [NAME]] \
                      [--source-dc [SRC_DC_NAME]] [--source-ds [SRC_DS_NAME]] \
                      [--volume-ids [VOLUME_UUIDS]] [--ignore-storage-policy] \
                      DEST_DC_NAME DEST_DS_NAME [-h] [-v]
```

Parameter	Obligatorisch oder Optional	Beschreibung
`-d, --deployment` *NAME*	Automatisch	Name der Bereitstellung, in welche die Volumes migriert werden. Wird automatisch angewendet. Der Standardwert ist der Name der aktuellen Bereitstellung.
`--source-dc` *SRC_DC_NAME*	Obligatorisch, außer wenn VOLUME_UUIDS angegeben ist.	Identifiziert das Quelldatencenter. Wird mit dem Parameter `--source-ds` zur eindeutigen Identifizierung des Datenspeichers verwendet.
`--source-ds` *SRC_DS_NAME*	Obligatorisch, außer wenn VOLUME_UUIDS angegeben ist.	Wird mit dem Parameter `--source-dc` zur eindeutigen Identifizierung des Datenspeichers verwendet. Beim folgenden Befehl werden beispielsweise alle Volumes von Datenspeicher DS-01 in Datencenter DC-01 zu Datenspeicher DS-02 in Datencenter DC-02 migriert. `viocli volume-migrate --source-dc DC-01 --source-ds DS-01 DC-02 DS-02`
`--volume-ids` *VOLUME_UUIDS*	Obligatorisch, außer wenn SRC_DC_NAME und SRC_DS_NAME angegeben sind.	Migriert mindestens ein durch den UUID-Wert festgelegtes einzelnes Volume. Trennen Sie die UUIDs durch Kommas, wenn Sie mehr als ein Volume angeben möchten. Beim folgenden Befehl werden beispielsweise zwei Volumes, die durch ihre UUID-Werte festgelegt sind, zu Datenspeicher DS-01 in Datencenter DC-01 migriert. `viocli volume-migrate --volume-ids 25e121d9-1153-4d15-92f8-c92c10b4987f, 4f1120e1-9ed4-421a-b65b-908ab1c6bc50 DC-01 DS-01`
`--ignore-storage-policy`	Optional	Ignoriert die Überprüfung der Einhaltung von Speicherrichtlinien. Fügen Sie diesen Parameter hinzu, um das Fehlschlagen der Migration zu verhindern, wenn das migrierte Volume eine Speicherrichtlinie enthält, die mit dem Zieldatenspeicher nicht übereinstimmt.
DEST_DC_NAME	Obligatorisch	Gibt das Zieldatencenter an.
DEST_DS_NAME	Obligatorisch	Gibt den Zieldatenspeicher an.
`-h, --help`	Optional	Zeigt die Verwendung und Argumente für diesen Befehl an.
`-v, --verbose`	Optional	Der ausführliche Modus wird gestartet.

Index

W

Z