

vCenter Server- Konfiguration

Update 3

VMware vSphere 7.0

VMware ESXi 7.0

vCenter Server 7.0

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

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

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

VMware Global, Inc.
Zweigniederlassung Deutschland
Willy-Brandt-Platz 2
81829 München
Germany
Tel.: +49 (0) 89 3706 17 000
Fax: +49 (0) 89 3706 17 333
www.vmware.com/de

Copyright © 2019-2021 VMware, Inc. Alle Rechte vorbehalten. [Urheberrechts- und Markenhinweise](#).

Inhalt

| | |
|---|-----------|
| Informationen zur vCenter Server-Konfiguration | 6 |
| 1 vCenter Server-Konfigurationsübersicht | 7 |
| Was ist mit Platform Services Controller (PSC) geschehen? | 8 |
| 2 Verwenden der vCenter Server-Verwaltungsschnittstelle zum Konfigurieren von vCenter Server | 10 |
| Anmelden bei der vCenter Server-Verwaltungsschnittstelle | 11 |
| Anzeigen des vCenter Server-Systemzustands | 11 |
| Neustarten oder Herunterfahren von vCenter Server | 12 |
| Erstellen eines Support-Pakets | 13 |
| Überwachen der CPU- und Arbeitsspeichernutzung | 13 |
| Überwachen der Festplattennutzung | 13 |
| Überwachen der Netzwerkauslastung | 14 |
| Überwachen der Datenbanknutzung | 14 |
| Aktivieren oder Deaktivieren des SSH- und Bash-Shell-Zugriffs | 15 |
| Konfigurieren der DNS-, IP-Adress- und Proxy-Einstellungen | 16 |
| Neukonfigurieren des primären Netzwerkbezeichners | 18 |
| Bearbeiten der Firewall-Einstellungen | 20 |
| Konfigurieren der Systemzeitzone und Zeitsynchronisierungseinstellungen | 21 |
| Starten, Stoppen und Neustarten von Diensten | 21 |
| Konfigurieren von Aktualisierungseinstellungen | 22 |
| Ändern des Kennworts und der Kennwortablaufestellungen des Root-Benutzers | 23 |
| Weiterleiten von vCenter Server-Protokolldateien an Remote-Syslog-Server | 24 |
| Konfigurieren und Planen von Sicherungen | 25 |
| 3 Verwenden des vSphere Client zur Konfiguration von vCenter Server | 26 |
| Konfigurieren von vCenter Server | 26 |
| Konfigurieren von Lizenzeneinstellungen für vCenter Server | 27 |
| Konfigurieren von Statistikeinstellungen | 27 |
| Konfigurieren von Laufzeiteinstellungen für vCenter Server | 31 |
| Konfigurieren von Benutzerverzeichniseinstellungen | 31 |
| Konfigurieren von Einstellungen für E-Mail-Absender | 32 |
| Konfigurieren von SNMP-Einstellungen | 34 |
| Anzeigen von Porteneinstellungen | 35 |
| Konfigurieren von Zeitüberschreitungseinstellungen | 35 |
| Konfigurieren von Protokollierungsoptionen | 36 |
| Konfigurieren von Datenbankeinstellungen | 37 |

| | |
|---|----|
| Überprüfen von SSL-Zertifikaten für Legacy-Hosts | 38 |
| Konfigurieren von erweiterten Einstellungen | 39 |
| Senden einer Nachricht an andere angemeldete Benutzer | 40 |
| Beitreten oder Verlassen einer Active Directory-Domäne | 40 |
| Hinzufügen eines Benutzers zur Gruppe „SystemConfiguration.BashShellAdministrators“ | 43 |
| Neustart eines Knotens | 43 |
| Anzeigen des Systemzustands von Knoten | 44 |
| Exportieren eines Support-Pakets | 45 |

4 Verwenden der Appliance-Shell zur Konfiguration von vCenter Server 46

| | |
|---|----|
| Zugreifen auf die Appliance-Shell | 46 |
| Aktivieren der Bash-Shell und Zugriff darauf über die Appliance-Shell | 47 |
| Tastenkombinationen für Bearbeitungsbefehle | 47 |
| Anzeigen der Hilfe zu den Plug-Ins und API-Befehlen in der Appliance | 49 |
| Plug-Ins in der vCenter Server-Shell | 49 |
| Durchsuchen der Protokolldateien mit dem showlog-Plug-In | 51 |
| API-Befehle in der Appliance-Shell | 51 |
| Konfigurieren von SNMP für vCenter Server | 57 |
| Konfigurieren des SNMP-Agenten zum Abfragen | 58 |
| Konfigurieren von vCenter Server für SNMP v1 und v2c | 58 |
| Konfigurieren von vCenter Server für SNMP v3 | 60 |
| Konfigurieren des SNMP-Agenten zum Filtern von Benachrichtigungen | 64 |
| Konfiguration der Clientsoftware für die SNMP-Verwaltung | 65 |
| Zurücksetzen der SNMP-Einstellungen auf die Standardeinstellungen | 66 |
| Konfigurieren der Einstellungen für die Uhrzeitsynchronisierung in vCenter Server | 67 |
| Verwenden der Uhrzeitsynchronisierung von VMware Tools | 67 |
| Hinzufügen oder Ersetzen von NTP-Servern in der vCenter Server-Konfiguration | 68 |
| Synchronisieren der Uhrzeit in vCenter Server mit einem NTP-Server | 69 |
| Verwalten lokaler Benutzerkonten in vCenter Server | 69 |
| Benutzerrollen in vCenter Server | 69 |
| Abrufen einer Liste der lokalen Benutzerkonten in vCenter Server | 70 |
| Erstellen eines lokalen Benutzerkontos in vCenter Server | 70 |
| Aktualisieren des Kennworts eines lokalen Benutzers in vCenter Server | 71 |
| Aktualisieren eines lokalen Benutzerkontos in vCenter Server | 71 |
| Löschen eines lokalen Benutzerkontos in vCenter Server | 72 |
| Überwachen von Systemzustand und Statistiken in vCenter Server | 73 |
| Verwenden des vimtop-Plug-In zum Überwachen der Ressourcennutzung von Diensten | 74 |
| Überwachen von Diensten mit vimtop im interaktiven Modus | 74 |
| Befehlszeilenoptionen im interaktiven Modus | 75 |
| Einzeltastenbefehle im interaktiven Modus für vimtop | 75 |

5 Verwenden der Benutzerschnittstelle der direkten Konsole zur Konfiguration von vCenter Server 77

Anmelden bei der Benutzerschnittstelle der direkten Konsole (DCUI) 77

Ändern des Kennworts des Root-Benutzers 78

Konfigurieren des Verwaltungsnetzwerks von vCenter Server 79

Neustarten des Verwaltungsnetzwerks von vCenter Server 80

Aktivieren des Zugriffs auf die Bash-Shell 80

Zugriff auf die Bash-Shell zur Fehlerbehebung 80

Exportieren eines vCenter Server-Support-Pakets zwecks Fehlerbehebung 81

Informationen zur vCenter Server-Konfiguration

vCenter Server-Konfiguration enthält Informationen zur Konfiguration von VMware vCenter[®] Server™.

Zielgruppe

Die vorliegenden Informationen richten sich an Benutzer, die VMware vCenter Server[®] konfigurieren möchten. Die Informationen sind für erfahrene Systemadministratoren bestimmt, die mit der VM-Technologie und Datacenteroperationen vertraut sind.

Wir bei VMware legen Wert auf die Verwendung neutraler Sprache. Um dieses Prinzip bei unseren Kunden und Partnern sowie innerhalb der internen Community zu fördern, erstellen wir Inhalte mit neutraler Sprache.

vSphere Client- und vCenter Server-Verwaltungsschnittstelle

Die Anweisungen in diesem Handbuch spiegeln den vSphere Client, eine HTML5-basierte GUI und die vCenter Server-Verwaltungsschnittstelle wider. Einige zusätzliche Funktionen können anhand der Shell der vCenter Server Appliance und der Benutzerschnittstelle der direkten Konsole durchgeführt werden.

vCenter Server-Konfigurationsübersicht

1

Die vCenter Server wird mit einer vorkonfigurierten virtuelle Maschine bereitgestellt, die für die Ausführung von VMware vCenter Server[®] und zugehörigen Diensten optimiert ist.

Während der Bereitstellung von vCenter Server können Sie eine VMware vCenter[®] Single Sign-On™-Domäne erstellen oder einer bestehenden Domäne beitreten. Weitere Informationen zur Bereitstellung von vCenter Server finden Sie unter *Installation und Einrichtung von vCenter Server*.

Die vCenter Server wird unter VMware ESXi™ 6.0 und höher unterstützt. Das Paket enthält die folgende Software:

- Project Photon OS[®] 3.0
- PostgreSQL-Datenbank
- vCenter Server 7.0 und vCenter Server 7.0-Komponenten
- Notwendige Dienste für die Ausführung von vCenter Server wie beispielsweise vCenter Single Sign-On, License Service und VMware Certificate Authority

Detaillierte Informationen zur Authentifizierung finden Sie unter *vSphere Authentication*.

Die Anpassung der vorkonfigurierten virtuellen Maschine wird bis auf das Hinzufügen von Arbeitsspeicher, CPU und Festplattenspeicher nicht unterstützt.

Für die vCenter Server gibt es die folgenden Standard-Benutzernamen:

- Root-Benutzer mit dem Kennwort, das Sie während der Bereitstellung der virtuellen Appliance festlegen. Sie verwenden den Root-Benutzer, um sich bei der vCenter Server-Verwaltungsschnittstelle und beim vorkonfigurierten Betriebssystem der virtuellen Maschine anzumelden.

Wichtig Das Kennwort für das Root-Konto der vCenter Server läuft standardmäßig nach 365 Tagen ab. Informationen zum Ändern des Root-Kennworts und zum Konfigurieren der Einstellungen für den Kennwortablauf finden Sie unter [Ändern des Kennworts und der Kennwortablaufeinstellungen des Root-Benutzers](#).

- „administrator@ihr_domänenname“, der vCenter Single Sign-On-Benutzer mit dem Kennwort und Domännennamen, den Sie während der Bereitstellung der Appliance festlegen.

Wenn Sie vCenter Server installieren, können Sie die vSphere-Domäne ändern. Verwenden Sie nicht denselben Domännennamen wie bei Ihrem Microsoft Active Directory- oder OpenLDAP-Domännennamen.

Anfänglich hat nur der Benutzer „administrator@*ihr_domänenname*“ die Berechtigung, sich beim vCenter Server-System anzumelden. Standardmäßig ist der Benutzer administrator@*Name_Ihrer_Domäne* Mitglied der Gruppe SystemConfiguration.Administrators. Dieser Benutzer kann eine Identitätsquelle, in der zusätzliche Benutzer und Gruppen definiert sind, zu vCenter Single Sign-On hinzufügen oder er kann den Benutzern und Gruppen Berechtigungen erteilen. Weitere Informationen finden Sie unter *vSphere-Sicherheit*.

Sie können vCenter Server-Einstellungen auf vier Arten konfigurieren:

- Verwenden Sie die vCenter Server-Verwaltungsschnittstelle.
Sie können die Systemeinstellungen wie z. B. Einstellungen für Zugang, Netzwerk, Uhrzeitsynchronisierung und Root-Kennwort bearbeiten. Dies ist die bevorzugte Methode für die Konfiguration von vCenter Server.
- Verwenden Sie den vSphere Client.
Sie können zu den Systemkonfigurationseinstellungen der vCenter Server navigieren und die Bereitstellung mit einer Active Directory-Domäne verbinden. Sie können die in der vCenter Server ausgeführten Dienste verwalten und verschiedene Einstellungen wie beispielsweise Zugriffs-, Netzwerk- und Firewall-Einstellungen ändern.
- Verwenden Sie die Bash-Shell.
Sie können TTY1 zur Anmeldung bei der Konsole verwenden, oder Sie verwenden SSH und führen Konfigurations-, Überwachungs- und Fehlerbehebungsbefehle in der vCenter Server aus.
- Verwenden Sie die Benutzerschnittstelle der direkten Konsole (DCUI).
Sie können TTY2 zur Anmeldung bei der DCUI der vCenter Server verwenden, um das Kennwort des Root-Benutzers zu ändern, die Netzwerkeinstellungen zu konfigurieren oder den Zugriff auf die Bash-Shell oder auf SSH zu aktivieren.

Dieses Kapitel enthält die folgenden Themen:

- [Was ist mit Platform Services Controller \(PSC\) geschehen?](#)

Was ist mit Platform Services Controller (PSC) geschehen?

In vSphere 7.0 werden alle Platform Services Controller-Dienste in vCenter Server konsolidiert.

Ab vSphere 7.0 muss für die Bereitstellung oder das Upgrade von vCenter Server in vSphere 7.0 vCenter Server Appliance verwendet werden. Dies ist eine vorkonfigurierte virtuelle Maschine, die für die Ausführung von vCenter Server optimiert ist. Die neue Version von vCenter Server enthält alle Platform Services Controller-Dienste, wobei die Funktionalität und die Workflows – darunter

Authentifizierung, Zertifikatsverwaltung und Lizenzierung – beibehalten wurden. Es ist nicht mehr erforderlich und auch nicht mehr möglich, eine externe Platform Services Controller-Instanz bereitzustellen und zu verwenden. Alle Platform Services Controller-Dienste sind in vCenter Server konsolidiert, sodass die Bereitstellung und Verwaltung vereinfacht werden.

Da diese Dienste jetzt zu vCenter Server gehören, werden sie nicht mehr als Teil von Platform Services Controller beschrieben. In vSphere 7.0 wurde die Dokumentation *Platform Services Controller-Verwaltung* durch die Dokumentation *vSphere-Authentifizierung* ersetzt. Die neue Publikation enthält vollständige Informationen zur Authentifizierung und Zertifikatsverwaltung. Informationen dazu, wie Sie für vSphere 6.5- und 6.7-Bereitstellungen mithilfe einer vorhandenen externen Platform Services Controller-Instanz und von vCenter Server Appliance ein Upgrade auf bzw. eine Migration zu vSphere 7.0 durchführen, finden Sie in der Dokumentation *vSphere-Upgrade*.

Verwenden der vCenter Server-Verwaltungsschnittstelle zum Konfigurieren von vCenter Server

2

Nachdem Sie vCenter Server bereitgestellt haben, können Sie sich bei der vCenter Server-Verwaltungsschnittstelle anmelden und die Einstellungen bearbeiten.

Informationen zum Patchen von vCenter Server und zum Aktivieren automatischer Suchvorgänge für vCenter Server-Patches finden Sie in der *vSphere-Upgrade*-Dokumentation.

Informationen zum Sichern und Wiederherstellen von vCenter Server finden Sie unter *Installation und Einrichtung von vCenter Server*.

Dieses Kapitel enthält die folgenden Themen:

- Anmelden bei der vCenter Server-Verwaltungsschnittstelle
- Anzeigen des vCenter Server-Systemzustands
- Neustarten oder Herunterfahren von vCenter Server
- Erstellen eines Support-Pakets
- Überwachen der CPU- und Arbeitsspeichernutzung
- Überwachen der Festplattennutzung
- Überwachen der Netzwerkauslastung
- Überwachen der Datenbanknutzung
- Aktivieren oder Deaktivieren des SSH- und Bash-Shell-Zugriffs
- Konfigurieren der DNS-, IP-Adress- und Proxy-Einstellungen
- Neukonfigurieren des primären Netzwerkbezeichners
- Bearbeiten der Firewall-Einstellungen
- Konfigurieren der Systemzeitzone und Zeitsynchronisierungseinstellungen
- Starten, Stoppen und Neustarten von Diensten
- Konfigurieren von Aktualisierungseinstellungen
- Ändern des Kennworts und der Kennwortablaufesinstellungen des Root-Benutzers
- Weiterleiten von vCenter Server-Protokolldateien an Remote-Syslog-Server
- Konfigurieren und Planen von Sicherungen

Anmelden bei der vCenter Server-Verwaltungsschnittstelle

Melden Sie sich bei der vCenter Server-Verwaltungsschnittstelle an, um auf die vCenter Server-Konfigurationseinstellungen zuzugreifen.

Hinweis Die Anmeldesitzung läuft ab, wenn Sie die vCenter Server-Verwaltungsschnittstelle 10 Minuten lang im Leerlauf lassen.

Voraussetzungen

Stellen Sie sicher, dass die vCenter Server erfolgreich bereitgestellt wurde und ausgeführt wird.

Verfahren

1 Navigieren Sie in einem Webbrowser zur vCenter Server-Verwaltungsschnittstelle, <https://Appliance-IP-Adresse-oder-FQDN:5480>.

2 Melden Sie sich als „root“ an.

Das standardmäßige Root-Kennwort ist das Kennwort, das Sie während der Bereitstellung von vCenter Server festlegen.

Anzeigen des vCenter Server-Systemzustands

Sie können die Verwaltungsschnittstelle von vCenter Server verwenden, um den Gesamtsystemzustand von vCenter Server und Benachrichtigungen zum Systemzustand anzuzeigen.

Der allgemeine Systemzustand der vCenter Server basiert auf dem Status der Hardwarekomponenten, wie beispielsweise CPU, Arbeitsspeicher, Datenbank und Speicher. Er basiert zudem auf dem Zustand der Aktualisierungskomponente, die angibt, ob die Softwarepakete laut der letzten Prüfung auf vorhandene Patches aktuell sind.

Wichtig Falls Sie keine regelmäßigen Prüfungen auf verfügbare Patches durchführen, ist der Systemzustand der Aktualisierungskomponente möglicherweise nicht mehr aktuell. Informationen zur Prüfung auf Patches für die vCenter Server und zur Aktivierung von automatischen Prüfungen auf Patches für die vCenter Server finden Sie unter *vSphere-Upgrade*.

Voraussetzungen

Melden Sie sich bei der vCenter Server-Verwaltungsschnittstelle als Root-Benutzer an.

Verfahren

1 Klicken Sie in der vCenter Server-Verwaltungsschnittstelle auf **Übersicht**.

- 2 Zeigen Sie im Fensterbereich „Integritätsstatus“ das Badge „Allgemeiner Zustand“ an.

Tabelle 2-1. Integritätsstatus

| Badge-Symbol | Beschreibung |
|---|---|
|  | Gut. Alle Komponenten befinden sich in einem guten Zustand. |
|  | Warnung. Eine oder mehrere Komponenten sind möglicherweise bald überlastet. Lassen Sie sich die Details im Fensterbereich „Meldungen zum Systemzustand“ anzeigen. |
|  | Alarm. Eine oder mehrere Komponenten sind möglicherweise herabgestuft. Es sind möglicherweise nicht sicherheitsrelevante Patches verfügbar. Lassen Sie sich die Details im Fensterbereich „Meldungen zum Systemzustand“ anzeigen. |
|  | Kritisch. Eine oder mehrere Komponenten befinden sich in einem unbrauchbaren Zustand, und vCenter Server wird möglicherweise bald nicht mehr reagieren. Sicherheits-Patches sind möglicherweise verfügbar. Lassen Sie sich die Details im Fensterbereich „Meldungen zum Systemzustand“ anzeigen. |
|  | Unbekannt. Keine Daten verfügbar. |

Neustarten oder Herunterfahren von vCenter Server

Sie können die vCenter Server-Verwaltungsschnittstelle verwenden, um die ausgeführte virtuelle Maschine neu zu starten oder auszuschalten.

Voraussetzungen

Melden Sie sich bei der vCenter Server-Verwaltungsschnittstelle als Root-Benutzer an.

Verfahren

- 1 Klicken Sie in der vCenter Server-Verwaltungsschnittstelle auf **Übersicht**.
- 2 Klicken Sie im oberen Menübereich auf das Dropdown-Menü **Aktionen**.
- 3 Klicken Sie auf **Neu starten** bzw. **Herunterfahren**, um die virtuelle Maschine neu zu starten bzw. auszuschalten.
- 4 Klicken Sie im Bestätigungsfenster auf **Ja**, um den Vorgang zu bestätigen.

Erstellen eines Support-Pakets

Sie können ein Support-Paket erstellen, das die Protokolldateien für die vCenter Server-Instanz enthält, die in der Appliance ausgeführt wird. Sie können die Protokolldateien lokal auf Ihrem Rechner analysieren oder das Paket an den VMware-Support senden.

Voraussetzungen

Melden Sie sich bei der vCenter Server-Verwaltungsschnittstelle als Root-Benutzer an.

Verfahren

- 1 Klicken Sie in der vCenter Server-Verwaltungsschnittstelle auf **Übersicht**.
- 2 Klicken Sie im oberen Menübereich auf das Dropdown-Menü **Aktionen**.
- 3 Klicken Sie auf **Support-Paket erstellen** und speichern Sie das Paket auf Ihrem lokalen Computer.

Ergebnisse

Das Support-Paket wird als `.tgz`-Datei auf Ihren lokalen Computer heruntergeladen.

Überwachen der CPU- und Arbeitsspeichernutzung

Mit der vCenter Server-Verwaltungsschnittstelle können Sie die gesamte CPU- und Arbeitsspeichernutzung von vCenter Server überwachen.

Voraussetzungen

Melden Sie sich bei der vCenter Server-Verwaltungsschnittstelle als Root-Benutzer an.

Verfahren

- 1 Klicken Sie in der vCenter Server-Verwaltungsschnittstelle auf **Überwachen**.
- 2 Klicken Sie auf der Seite „Überwachen“ auf die Registerkarte **CPU und Arbeitsspeicher**.
- 3 Wählen Sie im Dropdown-Menü **Datumsbereich** den Zeitraum für die Generierung eines Trenddiagramms zur CPU-Nutzung und eines Trenddiagramms zur Arbeitsspeichernutzung aus.
- 4 Zeigen Sie auf die Diagramme, um die CPU- und Arbeitsspeichernutzung an einem bestimmten Datum zu einer bestimmten Uhrzeit anzuzeigen.

Überwachen der Festplattennutzung

Sie können die vCenter Server-Verwaltungsschnittstelle verwenden, um die Festplattennutzung von vCenter Server zu überwachen.

Voraussetzungen

Melden Sie sich bei der vCenter Server-Verwaltungsschnittstelle als Root-Benutzer an.

Verfahren

- 1 Klicken Sie in der vCenter Server-Verwaltungsschnittstelle auf **Überwachen**.
- 2 Klicken Sie auf der Seite „Überwachen“ auf die Registerkarte **Festplatten**.

Ergebnisse

Im Bereich „Festplatten überwachen“ wird eine Festplatte sortierbar nach Name, Partition oder Nutzung angezeigt.

Überwachen der Netzwerkauslastung

Mit der vCenter Server-Verwaltungsschnittstelle können Sie die Netzwerknutzung von vCenter Server am vergangenen Tag, in der vergangenen Woche, im vergangenen Monat oder im vergangenen Quartal überwachen.

Voraussetzungen

Melden Sie sich bei der vCenter Server-Verwaltungsschnittstelle als Root-Benutzer an.

Verfahren

- 1 Klicken Sie in der vCenter Server-Verwaltungsschnittstelle auf **Überwachen**.
- 2 Klicken Sie auf der Seite „Überwachen“ auf die Registerkarte **Netzwerk**.
- 3 Wählen Sie im Dropdown-Menü **Datumsbereich** den Zeitraum für die Generierung des Diagramms zur Netzwerkauslastung aus.
- 4 Wählen Sie in der Tabelle unter dem Diagrammraster ein zu überwachendes Paket oder eine Übertragungsrate in Byte aus.

Die Optionen variieren entsprechend Ihren Netzwerkeinstellungen.

Das Netzwerkauslastungsdiagramm wird aktualisiert und zeigt die Auslastung des ausgewählten Elements an.

- 5 Durch Zeigen auf das Netzwerkauslastungsdiagramm werden die Netzwerkauslastungsdaten an einem bestimmten Datum zu einer bestimmten Uhrzeit angezeigt.

Überwachen der Datenbanknutzung

Mit der vCenter Server-Verwaltungsschnittstelle können Sie die Nutzung der eingebetteten Datenbank der vCenter Server nach Datentyp überwachen. Außerdem können Sie Trenddiagramme zur Speichernutzung überwachen und einige der größten Datentypen filtern.

Voraussetzungen

Melden Sie sich bei der vCenter Server-Verwaltungsschnittstelle als Root-Benutzer an.

Verfahren

- 1 Klicken Sie in der vCenter Server-Verwaltungsschnittstelle auf **Überwachen**.
- 2 Klicken Sie auf der Seite „Überwachen“ auf die Registerkarte **Datenbank**, um den belegten und den freien Speicherplatz für die vCenter Server-Datenbank zu überwachen.
- 3 Wählen Sie im Dropdown-Menü **Datumsbereich** den Zeitraum für die Generierung der Trenddiagramme zur Speicherplatznutzung aus.
- 4 Klicken Sie unten im Diagramm auf den Titel einer bestimmten Datenbankkomponente, um diese Komponente in das Diagramm einzuschließen oder daraus auszuschließen.

| Option | Beschreibung |
|---|--|
| Trenddiagramm der Speicherplatznutzung pro Arbeitsplatz | Ermöglicht Ihnen, Trendlinien für Alarme, Ereignisse, Aufgaben und Statistiken auszuwählen und anzuzeigen. |
| Trenddiagramm der Speicherplatznutzung insgesamt | Ermöglicht Ihnen, SEAT-, DB-Protokoll- und Core-Trendlinien anzuzeigen. |

- 5 Durch Zeigen auf das Speicherplatznutzungsdiagramm wird der Datenbank-Nutzungswert an einem bestimmten Datum zu einer bestimmten Uhrzeit angezeigt.

Aktivieren oder Deaktivieren des SSH- und Bash-Shell-Zugriffs

Sie können die vCenter Server-Verwaltungsschnittstelle verwenden, um die Zugriffseinstellungen für die Appliance zu bearbeiten.

Sie können die SSH-Administratoranmeldung bei der Appliance aktivieren oder deaktivieren. Sie können auch den Zugriff auf die Bash-Shell der vCenter Server für ein bestimmtes Zeitintervall aktivieren.

Voraussetzungen

Melden Sie sich bei der vCenter Server-Verwaltungsschnittstelle als Root-Benutzer an.

Verfahren

- 1 Klicken Sie in der vCenter Server-Verwaltungsschnittstelle auf **Zugriff** und anschließend auf **Bearbeiten**.
- 2 Bearbeiten Sie die Zugriffseinstellungen für vCenter Server.

| Option | Beschreibung |
|---------------------------------|--|
| SSH-Anmeldung aktivieren | Aktiviert den SSH-Zugriff auf vCenter Server. |
| DCUI aktivieren | Aktiviert den DCUI-Zugriff auf vCenter Server. |
| Konsolen-CLI aktivieren | Aktiviert den Konsolen-CLI-Zugriff auf die vCenter Server. |
| Bash-Shell aktivieren | Aktiviert den Bash-Shell-Zugriff auf vCenter Server für die angegebene Anzahl von Minuten. |

- 3 Klicken Sie auf **OK**, um die Einstellungen zu speichern.

Konfigurieren der DNS-, IP-Adress- und Proxy-Einstellungen

Sie können die Kombination von statischen und DHCP-IPv4- und -IPv6-Adressen festlegen, die DNS-Einstellungen bearbeiten und die Proxy-Einstellungen für vCenter Server definieren.

Voraussetzungen

- Um die IP-Adresse der Appliance zu ändern, vergewissern Sie sich, dass der Systemname der Appliance ein FQDN ist. Der Systemname wird als primärer Netzwerkbezeichner verwendet. Wenn Sie während der Bereitstellung der Appliance eine IP-Adresse als Systemnamen festlegen, können Sie den primären Netzwerkbezeichner (Primary Network Identifier, PNID) später in einen vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) ändern.

Hinweis Sie können nur die IPv4-IP-Adressen als Systemnamen festlegen. Die IPv4-IP-Adresse muss vor dieser Einstellung aktiviert werden.

- Um einen Dual-Stack-VC wiederherzustellen, sollte der Basis-VC nach der Bereitstellung in Phase 1 wie folgt konfiguriert werden:
 - Wenn die PNID des gesicherten VC in IPv4 aufgelöst wird und IPv4 statisch konfiguriert ist, sollte für den Basis-VC während Phase 1 statisches oder DHCP-IPv4 konfiguriert sein.
 - Wenn die PNID des gesicherten VC in IPv4 aufgelöst wird und IPv4 DHCP konfiguriert ist, sollte für den Basis-VC während Phase 1 DHCP mit IPv4 konfiguriert sein.
 - Wenn die PNID des gesicherten VC in IPv6 aufgelöst wird und IPv6 statisch konfiguriert ist, sollte für den Basis-VC während Phase 1 statisches oder DHCP-IPv6 konfiguriert sein.
 - Wenn die PNID des gesicherten VC in IPv6 aufgelöst wird und für IPv6 DHCP konfiguriert ist, sollte für den Basis-VC während Phase 1 DHCP-IPv6 konfiguriert sein.
- Melden Sie sich bei der vCenter Server-Verwaltungsschnittstelle als Root-Benutzer an.

Verfahren

- 1 Klicken Sie in der vCenter Server-Verwaltungsschnittstelle auf **Netzwerk**.
- 2 Klicken Sie auf der Seite „Netzwerkeinstellungen“ auf **Bearbeiten**.

- 3 Erweitern Sie den Hostnamen und DNS-Abschnitt, um die DNS-Einstellungen zu konfigurieren.

Hinweis Ein gültiger Wert für Hostname ist entweder der FQDN, der in eine aktivierte IP-Adresse aufgelöst wird, oder die IPv4-IP-Adresse.

| Option | Beschreibung |
|---------------------------------------|--|
| DNS-Einstellungen automatisch abrufen | Ruft die DNS-Einstellungen automatisch vom Netzwerk ab. |
| DNS-Einstellungen manuell eingeben | Ermöglicht die manuelle Festlegung der DNS-Adresseinstellungen. Wenn Sie diese Option auswählen, müssen Sie folgende Informationen angeben: <ul style="list-style-type: none"> ■ Die IP-Adresse des bevorzugten DNS-Servers. ■ (Optional) Die IP-Adresse des alternativen DNS-Servers. |

- 4 Klicken Sie auf der Seite „Netzwerkeinstellungen“ auf **Bearbeiten**.
- 5 Erweitern Sie den NICO-Abschnitt, um die Gatewayeinstellungen zu konfigurieren.

Hinweis PNID und Netzwerk-APIs unterstützen nur NICO als primäre Netzwerkkarte.

- 6 Bearbeiten Sie die IPv4-Adresseinstellungen.

| Option | Beschreibung |
|---|---|
| IPv4-Einstellungen aktivieren oder deaktivieren | Aktiviert oder deaktiviert die IPv4-Adresse basierend auf der ausgewählten Umschloption. |
| IPv4-Einstellungen automatisch abrufen | Ruft die IPv4-Adresse für die Appliance automatisch vom Netzwerk ab. |
| IPv4-Einstellungen manuell eingeben | Verwendet eine IPv4-Adresse, die Sie manuell eingerichtet haben. Sie müssen die IP-Adresse, die Länge des Subnetzpräfixes und das Standard-Gateway eingeben. <p>Hinweis Bei statischen IPv4- oder IPv6-Adressen muss der DNS-Server manuell festgelegt werden.</p> |

Hinweis Lösungen von Zweit- und Drittanbietern müssen erneut registriert werden, wenn eine Änderung bei den IPv4- und IPv6-IP-Adressen vorliegt.

- 7 Bearbeiten Sie die IPv6-Adresseinstellungen.

| Option | Beschreibung |
|---|--|
| IPv6-Einstellungen aktivieren oder deaktivieren | Aktiviert oder deaktiviert die IPv6-Adresse basierend auf der ausgewählten Umschloption. |
| IPv6-Adressen automatisch mittels DHCP abrufen | Weist der Appliance mithilfe von DHCP automatisch IPv6-Adressen vom Netzwerk zu. |

| Option | Beschreibung |
|--|--|
| IPv6-Einstellungen automatisch mittels Router-Ankündigung abrufen | Weist der Appliance mithilfe von Router-Ankündigung automatisch IPv6-Adressen vom Netzwerk zu. |
| Statische IPv6-Adressen verwenden | Verwendet statische IPv6-Adressen, die Sie manuell eingerichtet haben. <ol style="list-style-type: none"> 1 Klicken Sie auf das Kontrollkästchen. 2 Geben Sie die IPv6-Adresse und die Länge des Subnetzpräfixes ein. 3 Klicken Sie auf Hinzufügen., um zusätzliche IPv6-Adressen hinzuzufügen. 4 Klicken Sie auf Speichern. <p>Hinweis Bei statischen IPv4- oder IPv6-Adressen muss der DNS-Server manuell festgelegt werden.</p> |

Sie können die Appliance so konfigurieren, dass die IPv6-Einstellungen sowohl über DHCP als auch über die Router-Ankündigung automatisch abgerufen werden. Sie können gleichzeitig eine statische IPv6-Adresse zuweisen.

Hinweis Lösungen von Zweit- und Drittanbietern müssen erneut registriert werden, wenn eine Änderung bei den IPv4- und IPv6-IP-Adressen vorliegt.

- 8 Klicken Sie zum Konfigurieren eines Proxyservers im Abschnitt „Proxy-Einstellungen“ auf **Bearbeiten**.
- 9 Auswählen der zu aktivierenden Proxy-Einstellung

| Option | Beschreibung |
|--------------|--|
| HTTPS | Aktivieren zur Konfiguration der HTTPS-Proxy-Einstellungen. |
| FTP | Aktivieren zur Konfiguration der FTP-Proxy-Einstellungen. Hinweis Stellen Sie sicher, dass ICMP auf dem Proxyserver aktiviert ist. |
| HTTP | Aktivieren zur Konfiguration der HTTP-Proxy-Einstellungen. |

- 10 Geben Sie den Server-Hostnamen oder die IP-Adresse ein.
- 11 Geben Sie den Port ein.
- 12 Geben Sie den Benutzernamen ein (optional).
- 13 Geben Sie das Kennwort ein (optional).
- 14 Klicken Sie auf **Speichern**.

Neukonfigurieren des primären Netzwerkbezeichners

Sie können den vollqualifizierten Domännennamen (Fully Qualified Domain Name, FQDN), die IP-Adresse oder den primären Netzwerkbezeichner (Primary Network Identifier, PNID) des Verwaltungsnetzwerks von vCenter Server ändern.

Voraussetzungen

Der Systemname wird als primärer Netzwerkbezeichner verwendet. Wenn Sie während der Bereitstellung der Appliance eine IP-Adresse als Systemnamen festlegen, können Sie den primären Netzwerkbezeichner (Primary Network Identifier, PNID) später in einen vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) ändern.

Wenn vCenter High Availability (HA) aktiviert ist, müssen Sie die vCenter HA-Einrichtung vor der Neukonfiguration des PNID deaktivieren.

Verfahren

- 1 Melden Sie sich mit Ihren SSO-Administratoranmeldedaten bei der vCenter Server-Verwaltungsschnittstelle an.
- 2 Navigieren Sie in der vCenter Server-Verwaltungsschnittstelle zur Seite **Netzwerk** und klicken Sie auf **Bearbeiten**.
- 3 Wählen Sie die zu ändernde Netzwerkkarte (NIC) aus und klicken Sie auf **Weiter**.
- 4 Ändern Sie im Bereich **Einstellungen bearbeiten** den Hostnamen und geben Sie die neue IP-Adresse an. Klicken Sie auf **Weiter**.
- 5 Geben Sie im Bereich **SSO-Anmeldedaten** die SSO-Administratoranmeldedaten ein. Sie müssen Anmeldedaten vom Typ **administrator@<domain_name>** verwenden.
- 6 Überprüfen Sie im Bereich **Bereit zum Abschließen** Ihre neuen Einstellungen und prüfen Sie das Feld für die Sicherungsbestätigung. Klicken Sie auf **Beenden**.

Der Status der Netzwerkaktualisierung wird in einer Taskleiste angezeigt. Um die Aktualisierung abubrechen, klicken Sie auf **Netzwerkaktualisierung abbrechen**. Wenn die Neukonfiguration des Netzwerks abgeschlossen ist, werden Sie in der Benutzeroberfläche an die neue IP-Adresse umgeleitet.

- 7 Melden Sie sich mit Ihren SSO-Administratoranmeldedaten an, um den Neukonfigurationsvorgang abzuschließen und die Dienste neu zu starten.
- 8 Überprüfen Sie auf der Seite **Netzwerk** den neuen Hostnamen und die IP-Adresse.

Nächste Schritte

- Registrieren Sie alle bereitgestellten Plug-Ins erneut.
- Generieren Sie alle benutzerdefinierten Zertifikate neu.
- Falls vCenter HA aktiviert war, konfigurieren Sie es neu.
- Falls die aktive Domäne aktiviert war, konfigurieren Sie sie neu.
- Falls der hybride Verknüpfungsmodus aktiviert war, konfigurieren Sie die hybride Verknüpfung mit Cloud-vCenter Server neu.

Bearbeiten der Firewall-Einstellungen

Nach der Bereitstellung des vCenter Server können Sie dessen Firewall-Einstellungen bearbeiten und Firewallregeln mit der Verwaltungsschnittstelle erstellen.

Sie können Firewallregeln einrichten, um Datenverkehr zwischen vCenter Server und bestimmten Servern, Hosts oder virtuellen Maschinen zuzulassen oder zu blockieren. Sie können nicht bestimmte Ports, sondern nur den ganzen Datenverkehr blockieren.

Voraussetzungen

Stellen Sie sicher, dass der Benutzer, der sich bei der vCenter Server-Instanz anmeldet, Mitglied der Gruppe „SystemConfiguration.Administrators“ in vCenter Single Sign-On ist.

Verfahren

- 1 Klicken Sie in der vCenter Server-Verwaltungsschnittstelle auf **Firewall**.
- 2 Bearbeiten Sie die Firewall-Einstellungen.

| Befehl | Aktion |
|---------------------|---|
| Hinzufügen | <ol style="list-style-type: none"> a Um eine Firewallregel zu erstellen, klicken Sie auf Hinzufügen. b Wählen Sie eine Netzwerkschnittstelle der virtuellen Maschine aus. c Geben Sie die IP-Adresse des Netzwerks ein, auf das diese Regel angewendet werden soll. Bei der IP-Adresse kann es sich um eine IPv4- oder IPv6-Adresse handeln. d Geben Sie die Länge des Subnetzpräfixes ein. e Wählen Sie im Dropdown-Menü Aktion aus, ob Sie die Verbindung zwischen vCenter Server und dem von Ihnen eingegebenen Netzwerk akzeptieren, ignorieren, ablehnen oder zurücksetzen möchten. f Klicken Sie auf Speichern. |
| Bearbeiten | <ol style="list-style-type: none"> a Wählen Sie eine Regel und klicken Sie auf Bearbeiten. b Bearbeiten Sie die Einstellungen der Regel. c Klicken Sie auf Speichern. |
| Löschen | <ol style="list-style-type: none"> a Wählen Sie eine Regel und klicken Sie auf Löschen. b Klicken Sie bei Aufforderung erneut auf Löschen. |
| Neu anordnen | <ol style="list-style-type: none"> a Wählen Sie eine Regel und klicken Sie auf Neu anordnen. b Wählen Sie im Bereich „Neu anordnen“ die Regel aus, die Sie verschieben möchten. c Klicken Sie auf Nach oben verschieben oder Nach unten verschieben. d Klicken Sie auf Speichern. |

Konfigurieren der Systemzeitzone und Zeitsynchronisierungseinstellungen

Nach der Bereitstellung der vCenter Server können Sie die Einstellungen für die Zeitzone des Systems und für die Uhrzeitsynchronisierung in der vCenter Server-Verwaltungsschnittstelle ändern.

Wenn Sie vCenter Server bereitstellen, verwenden Sie entweder die Uhrzeiteinstellungen des ESXi-Hosts, auf dem vCenter Server ausgeführt wird, oder Sie konfigurieren die Uhrzeitsynchronisierung basierend auf einem NTP-Server. Wenn sich die Uhrzeiteinstellungen in Ihrem vSphere-Netzwerk ändern, können Sie die Einstellungen für die Zeitzone des Systems und für die Uhrzeitsynchronisierung in der Appliance bearbeiten.

Voraussetzungen

Melden Sie sich bei der vCenter Server-Verwaltungsschnittstelle als Root-Benutzer an.

Verfahren

- 1 Klicken Sie in der vCenter Server-Verwaltungsschnittstelle auf **Uhrzeit**.
- 2 Konfigurieren Sie die Einstellungen für die Zeitzone des Systems.
 - a Klicken Sie im Bereich „Zeitzone“ auf **Bearbeiten**.
 - b Wählen Sie im Dropdown-Menü **Zeitzone** einen Standort oder eine Zeitzone aus und klicken Sie auf **Speichern**.
- 3 Konfigurieren Sie die Einstellungen für die Uhrzeitsynchronisierung.
 - a Klicken Sie im Bereich „Uhrzeitsynchronisierung“ auf **Bearbeiten**.
 - b Konfigurieren Sie im Dropdown-Menü **Modus** die Uhrzeitsynchronisierungsmethode.

| Option | Beschreibung |
|--------------------|---|
| Deaktiviert | Keine Uhrzeitsynchronisierung. Verwendet die Einstellungen für die Zeitzone des Systems. |
| Host | Aktiviert die Uhrzeitsynchronisierung von VMware Tools. Verwendet VMware Tools, um die Uhrzeit der Appliance mit der Uhrzeit des ESXi-Hosts zu synchronisieren. |
| NTP | Aktiviert die NTP-Synchronisierung. Sie müssen die IP-Adresse oder den FQDN von mindestens einem NTP-Server eingeben. |

- c Klicken Sie auf **Speichern**.

Starten, Stoppen und Neustarten von Diensten

Sie können die vCenter Server-Verwaltungsschnittstelle verwenden, um den Status der vCenter Server-Komponenten anzuzeigen und die Dienste zu starten, zu beenden und neu zu starten.

Voraussetzungen

Melden Sie sich bei der vCenter Server-Verwaltungsschnittstelle als Root-Benutzer an.

Verfahren

- 1 Klicken Sie in der vCenter Server-Verwaltungsschnittstelle auf **Dienste**.
Auf der Seite „Dienste“ wird eine Tabelle mit installierten Diensten angezeigt, die nach Name, Starttyp, Systemzustand und Status sortiert werden können.
- 2 Wählen Sie einen Dienst aus und klicken Sie auf **STARTUP-TYP ERSTELLEN**, um entweder den manuellen oder den automatischen Start eines Diensts zu konfigurieren.
- 3 Wählen Sie einen Dienst aus und klicken Sie auf **START**, um einen Dienst zu starten.
- 4 Wählen Sie einen Dienst und klicken Sie auf **STOPP** zum Beenden oder auf **NEU STARTEN**, um einen Dienst neu zu starten. Klicken Sie dann auf **OK**.

Warnung Das Stoppen oder der Neustart einiger Dienste führt möglicherweise dazu, dass Funktionen vorübergehend nicht verfügbar sind.

Konfigurieren von Aktualisierungseinstellungen

Sie können die vCenter Server-Verwaltungsschnittstelle verwenden, um Ihre Update-Einstellungen zu konfigurieren und nach neuen Updates zu suchen.

Voraussetzungen

Melden Sie sich bei der vCenter Server-Verwaltungsschnittstelle als Root-Benutzer an.

Verfahren

- 1 Klicken Sie in der vCenter Server-Verwaltungsschnittstelle auf **Aktualisieren**.
- 2 Klicken Sie auf **Einstellungen**, um Ihre Update-Einstellungen zu konfigurieren.
 - a Aktivieren Sie das Kontrollkästchen, um automatisch nach Updates zu suchen.
 - b Legen Sie fest, ob ein Standard- oder ein benutzerdefiniertes Repository verwendet werden soll.
 - c Wenn Sie ein benutzerdefiniertes Repository ausgewählt haben, geben Sie die Repository-URL, den Benutzernamen (optional) und das Kennwort (optional) ein. Klicken Sie auf **Speichern**.
Für die URL werden die Protokolle HTTPS und FTPS unterstützt.
- 3 Um manuell nach Updates zu suchen, klicken Sie auf das Dropdown-Menü **Nach Updates suchen**.
 - a Wählen Sie aus, ob eine **CD-ROM** oder eine **CD-ROM + URL** auf Updates überprüft werden sollen.

Ergebnisse

Die Tabelle „Verfügbare Updates“ zeigt verfügbare Updates an und kann nach Version, Typ, Datum, Neustartanforderung und Schweregrad sortiert werden.

Ändern des Kennworts und der Kennwortablaufeinstellungen des Root-Benutzers

Wenn Sie vCenter Server bereitstellen, legen Sie das anfängliche Kennwort für den Root-Benutzer fest, welches standardmäßig nach 90 Tagen abläuft. Das Root-Kennwort und die Einstellungen für Kennwortablauf können Sie über die vCenter Server-Verwaltungsschnittstelle ändern.

Voraussetzungen

Melden Sie sich bei der vCenter Server-Verwaltungsschnittstelle als Root-Benutzer an.

Verfahren

- 1 Klicken Sie in der vCenter Server-Verwaltungsschnittstelle auf **Verwaltung**.
- 2 Klicken Sie im Abschnitt „Kennwort“ auf **Ändern**.
- 3 Geben Sie das aktuelle Kennwort und das neue Kennwort ein und klicken Sie auf **Speichern**.
- 4 Konfigurieren Sie die Einstellungen für den Kennwortablauf für den Root-Benutzer.
 - a Klicken Sie im Abschnitt „Einstellungen für Kennwortablauf“ auf **Bearbeiten** und wählen Sie die Richtlinie für den Kennwortablauf.

| Option | Beschreibung |
|--------|---|
| Ja | <p>Das Kennwort des Root-Benutzers läuft nach einer bestimmten Anzahl von Tagen ab. Sie müssen die folgenden Informationen angeben:</p> <ul style="list-style-type: none"> ■ Gültigkeit des Root-Kennworts (Tage) Die Anzahl von Tagen, nach der das Kennwort abläuft. ■ E-Mail-Adresse für Warnung zum Ablauf Die E-Mail-Adresse, an die vCenter Server vor dem Ablaufdatum eine Warnmeldung sendet. |
| Nein | Das Kennwort des Root-Benutzers läuft nie ab. |

- b Klicken Sie im Bereich „Einstellungen für Kennwortablauf“ auf **Speichern**, um die neuen Einstellungen für den Kennwortablauf zu übernehmen.

Der Abschnitt „Einstellungen für Kennwortablauf“ zeigt das neue Ablaufdatum an.

Weiterleiten von vCenter Server-Protokolldateien an Remote-Syslog-Server

Sie können die vCenter Server-Protokolldateien an einen Remote-Syslog-Server weiterleiten, um Ihre Protokolle zu analysieren.

Hinweis ESXi kann so konfiguriert werden, dass Protokolldateien an vCenter Server gesendet werden, statt auf einer lokalen Festplatte konfiguriert zu werden. Die empfohlene maximale Anzahl unterstützter Hosts, von denen Protokolle erfasst werden, ist 30. Informationen zum Konfigurieren der ESXi-Protokollweiterleitung finden Sie unter <http://kb.vmware.com/s/article/2003322>. Diese Funktion ist für kleinere Umgebungen mit statusfreien ESXi-Hosts vorgesehen. Verwenden Sie für alle anderen Fälle einen dedizierten Protokollserver. Wenn Sie vCenter Server zum Empfangen von ESXi-Protokolldateien verwenden, wird die Leistung von vCenter Server möglicherweise beeinträchtigt.

Voraussetzungen

Melden Sie sich bei der vCenter Server-Verwaltungsschnittstelle als Root-Benutzer an.

Verfahren

- 1 Wählen Sie in der vCenter Server-Verwaltungsschnittstelle die Option **Syslog-Konfiguration** aus.
- 2 Klicken Sie im Abschnitt „Weiterleitungskonfiguration“ auf **Konfigurieren**, wenn Sie keine Remote-Syslog-Hosts konfiguriert haben. Klicken Sie auf **Bearbeiten**, wenn Sie Hosts bereits konfiguriert haben.
- 3 Geben Sie im Bereich „Weiterleitungskonfiguration erstellen“ die Serveradresse des Zielhosts ein. Maximal drei Zielhosts werden unterstützt.
- 4 Wählen Sie im Dropdown-Menü **Protokoll** das zu verwendende Protokoll aus.

| Menüelement | Beschreibung |
|-------------|--|
| TLS | Transport Layer Security |
| TCP | Transmission Control Protocol |
| RELP | Reliable Event Logging Protocol (Protokoll für die zuverlässige Ereignisprotokollierung) |
| UDP | User Datagram Protocol |

- 5 Geben Sie in das Textfeld **Port** die für die Kommunikation mit dem Zielhost zu verwendende Portnummer ein.
- 6 Klicken Sie im Bereich „Weiterleitungskonfiguration erstellen“ auf **Hinzufügen**, um einen anderen Remote-Syslog-Server einzugeben.
- 7 Klicken Sie auf **Speichern**.
- 8 Stellen Sie sicher, dass der Remote-Syslog-Server Nachrichten empfängt.

- 9 Klicken Sie im Abschnitt „Weiterleitungskonfiguration“ auf **Testnachricht senden**.
- 10 Vergewissern Sie sich, dass die Testnachricht auf dem Remote-Syslog-Server empfangen wurde.

Die neuen Konfigurationseinstellungen werden im Abschnitt „Weiterleitungskonfiguration“ angezeigt.

Konfigurieren und Planen von Sicherungen

Sie können die Verwaltungsschnittstelle von vCenter Server verwenden, um einen Sicherungsspeicherort festzulegen, einen Sicherungszeitplan zu erstellen und Sicherungsaktivitäten zu überwachen.

Voraussetzungen

Melden Sie sich bei der vCenter Server-Verwaltungsschnittstelle als Root-Benutzer an.

Verfahren

- 1 Klicken Sie in der vCenter Server-Verwaltungsschnittstelle auf **Sichern**.
- 2 Um einen Sicherungszeitplan zu erstellen, klicken Sie auf **Konfigurieren**. Um einen vorhandenen Sicherungszeitplan zu bearbeiten, klicken Sie auf **Bearbeiten**.
 - a Geben Sie im Fenster **Sicherungszeitplan** den Sicherungsspeicherort ein und verwenden Sie dafür das Format **protocol://server-address[:port-number]/folder/subfolder**.

Zu den unterstützten Protokollen für die Sicherung gehören FTPS, HTTPS, SFTP, FTP, NFS, SMB und HTTP.
 - b Geben Sie den Benutzernamen und das Kennwort für den Sicherungsserver ein.
 - c Geben Sie die Uhrzeit und die Häufigkeit für die Sicherungen ein.
 - d (Optional) Geben Sie ein Verschlüsselungskennwort für die Sicherungen ein.
 - e Geben Sie die Anzahl an Sicherungen an, die beibehalten werden sollen.
 - f Geben Sie die Datentypen an, die gesichert werden sollen.
- 3 Um eine manuelle Sicherung einzuleiten, klicken Sie auf **Jetzt sichern**.

Ergebnisse

Informationen für geplante und manuelle Sicherungen werden in der Tabelle **Aktivität** angezeigt.

Verwenden des vSphere Client zur Konfiguration von vCenter Server

3

Sie können einige Konfigurationsvorgänge über die vSphere Client durchführen, z. B. das Hinzufügen der Appliance zu einer Active Directory-Domäne, Netzwerkvorgänge und andere Einstellungen.

Dieses Kapitel enthält die folgenden Themen:

- Konfigurieren von vCenter Server
- Beitreten oder Verlassen einer Active Directory-Domäne
- Hinzufügen eines Benutzers zur Gruppe „SystemConfiguration.BashShellAdministrators“
- Neustart eines Knotens
- Anzeigen des Systemzustands von Knoten
- Exportieren eines Support-Pakets

Konfigurieren von vCenter Server

Sie können vCenter Server von der vSphere Client- und von der vCenter Server-Verwaltungsschnittstelle aus konfigurieren.

Was Sie tun können, hängt von Ihrer Bereitstellung ab.

Lokale Bereitstellung von vCenter Server

Sie können viele der vCenter Server-Einstellungen ändern, einschließlich derjenigen, die sich auf die Lizenzierung, Statistikerfassung und Protokollierung beziehen.

Bereitstellung von vCenter Server in VMware Cloud on AWS

Instanzen von vCenter Server werden von VMware vorab konfiguriert, wenn Sie ein SDDC erstellen. Sie können die Konfigurationseinstellungen und erweiterte Einstellungen einsehen. Zudem haben Sie die Möglichkeit, eine Meldung des Tages festzulegen.

Detaillierte Informationen zum Konfigurieren von vCenter Server finden Sie im *vCenter Server-Konfiguration-Handbuch*.

Konfigurieren von Lizenzeinstellungen für vCenter Server

Sie müssen nach Ablauf des Testzeitraums oder der Gültigkeit der derzeit zugewiesenen Lizenz einem vCenter Server-System eine Lizenz zuweisen. Wenn Sie für vCenter Server-Lizenzen in „Customer Connect“ ein Upgrade durchführen, sie kombinieren oder teilen, müssen Sie die neuen Lizenzen vCenter Server-Systemen zuweisen und die alten Lizenzen entfernen.

Voraussetzungen

- Um Lizenzen in der vSphere-Umgebung anzeigen und verwalten zu können, benötigen Sie die Berechtigung **Globale.Lizenzen** im vCenter Server-System, in dem vSphere Client ausgeführt wird.

Verfahren

- 1 Navigieren Sie im vSphere Client zur vCenter Server-Instanz.
- 2 Wählen Sie die Registerkarte **Konfigurieren** aus.
- 3 Wählen Sie unter **Einstellungen** die Option **Lizenzierung**.
- 4 Klicken Sie auf **Lizenz zuweisen**.
- 5 Wählen Sie im Dialogfeld **Lizenz zuweisen** die durchzuführende Aufgabe aus.
 - ◆ Wählen Sie im vSphere Client eine vorhandene oder eine neu erstellte Lizenz aus.

| Aufgabe | Schritte |
|---|---|
| Vorhandene Lizenz auswählen | Wählen Sie eine vorhandene Lizenz aus der Liste aus und klicken Sie auf OK . |
| Wählen Sie eine neu erstellte Lizenz aus | <ol style="list-style-type: none"> a Klicken Sie auf die Registerkarte Neue Lizenz. b Geben Sie im Dialogfeld Lizenz zuweisen einen Lizenzschlüssel ein bzw. kopieren und fügen Sie ihn dort ein. Klicken Sie anschließend auf OK. c Geben Sie einen Namen für die neue Lizenz ein und klicken Sie auf OK. Informationen über das Produkt, die Produktfunktionen, die Kapazität und der Ablaufzeitraum werden auf der Seite angezeigt. d Klicken Sie auf OK. e Wählen Sie im Dialogfeld Lizenz zuweisen die neu erstellte Lizenz aus und klicken Sie auf OK. |

Ergebnisse

Die Lizenz wird dem vCenter Server-System zugewiesen und eine Instanz aus der Lizenzkapazität wird dem vCenter Server-System zugeteilt.

Konfigurieren von Statistikeinstellungen

Konfigurieren Sie Erfassungsintervalle für Statistiken, um das Verfahren zum Aufzeichnen von statistischen Daten festzulegen. Sie können über Befehlszeilen-Überwachungsdiagrammprogramme oder durch die Ansicht von Leistungsdiagrammen im vSphere Client auf die gespeicherten statistischen Informationen zugreifen.

Konfigurieren von Intervallen für die Statistikerfassung im vSphere Client

Über Intervalle für die Statistikerfassung werden die Häufigkeit, mit der statistische Abfragen durchgeführt werden, sowie der Zeitraum, für den statistische Daten in der Datenbank gespeichert werden, und der erfasste Typ der statistischen Daten festgelegt. Sie können die erfassten Statistiken über die Leistungsdiagramme im vSphere Client oder über die Überwachungsdienstprogramme anzeigen, die in der Befehlszeile ausgeführt werden.

Hinweis Es sind nicht alle Intervallattribute konfigurierbar.

Voraussetzungen

Erforderliche Berechtigung: **Leistung.Intervalle ändern**

Verfahren

- 1 Navigieren Sie im vSphere Client zur vCenter Server-Instanz.
- 2 Wählen Sie die Registerkarte **Konfigurieren** aus.
- 3 Wählen Sie unter **Einstellungen** die Option **Allgemein** aus.
- 4 Klicken Sie auf **Bearbeiten**.
- 5 Um ein Statistikintervall zu aktivieren oder zu deaktivieren, aktivieren bzw. deaktivieren Sie das Kontrollkästchen für dieses Intervall.
- 6 Um einen Attributwert eines Statistikintervalls zu ändern, wählen Sie im Dropdown-Menü einen Wert aus.
 - a Wählen Sie unter **Intervalldauer** das Zeitintervall aus, in dem die statistischen Daten erfasst werden.
 - b Wählen Sie im Feld **Speichern für** aus, wie lange die archivierten Statistiken in der Datenbank aufbewahrt werden.
 - c Wählen Sie unter **Statistikebene** eine neue Ebene für die Erfassung von Statistiken aus.

Je niedriger die Ebene ist, desto weniger statistische Leistungsindikatoren werden verwendet. Ebene 4 verwendet alle Statistikzähler. Es ist empfehlenswert, diese Ebene nur für das Debuggen auszuwählen.

Die Statistikebene muss dem für das vorangegangene Statistikintervall festgelegten Wert für die Statistikebene entsprechen oder darunter liegen. Bei dieser Anforderung handelt es sich um eine vCenter Server-Abhängigkeit.

7 (Optional) Schätzen Sie für „Datenbankgröße“ die Auswirkungen der Statistikeinstellungen auf die Datenbank ein.

a Geben Sie die Anzahl für **Physische Hosts** ein.

b Geben Sie die Anzahl für **Virtuelle Maschinen** ein.

Der geschätzte erforderliche Speicherplatz und die Anzahl an erforderlichen Datenbankzeilen wird berechnet und angezeigt.

c Nehmen Sie bei Bedarf Änderungen an den Einstellungen für die Statistikerfassung vor.

8 Klicken Sie auf **Speichern**.

Beispiel: Beziehungen zwischen den Standardeinstellungen für Statistikintervalle

- Stichproben, die alle 5 Minuten erfasst und für einen Tag gespeichert werden.
- Stichproben, die alle 30 Minuten erfasst und für eine Woche gespeichert werden.
- Stichproben, die alle 2 Stunden erfasst und für einen Monat gespeichert werden.
- Stichproben, die an einem Tag erfasst und für ein Jahr gespeichert werden.

Für alle Statistikintervalle gilt die Standardebene 1. Verwendet werden die Zähler „Clusterdienste“, „CPU“, „Festplatte“, „Arbeitsspeicher“, „Netzwerk“, „System“ und „VM-Vorgänge“.

Datenerfassungsebenen

Jedes Erfassungsintervall hat eine Standarderfassungsebene, die festlegt, welche Menge an Daten gesammelt werden und welche Leistungsindikatoren in Diagrammen angezeigt werden können. Erfassungsebenen werden auch als Statistikebenen bezeichnet.

Tabelle 3-1. Statistikebenen

| Level | Metriken | Best Practice |
|---------|--|---|
| Ebene 1 | <ul style="list-style-type: none"> ■ Clusterdienste (VMware Distributed Resource Scheduler) – alle Metriken ■ CPU – CPU-Reservierungen, MHz (Gesamt), Nutzung (Durchschnitt), MHz-Nutzung ■ Festplatte – Kapazität, maximale Gesamtlatenz, bereitgestellt, nicht freigegeben, Nutzung (Durchschnitt), verwendet ■ Arbeitsspeicher – Belegt, Arbeitsspeicherreservierungen, Overhead, Datenabruftrate bei Einlagerung, Auslagerungsrate, verwendeter Auslagerungsspeicher, MB (Gesamt), Nutzung (Durchschnitt), vmmemctl (Balloon) ■ Netzwerk – Nutzung (Durchschnitt), IPv6 ■ System – Taktsignal, Betriebszeit ■ Betriebsvorgänge virtueller Maschinen – numChangeDS, numChangeHost, numChangeHostDS | <p>Verwendung für Langzeit-Leistungsüberwachung, wenn Gerätestatistiken nicht erforderlich sind.</p> <p>Ebene 1 ist die standardmäßige Erfassungsebene für alle Erfassungsintervalle.</p> |
| Ebene 2 | <ul style="list-style-type: none"> ■ Metriken der Ebene 1 ■ CPU – im Leerlauf, reservierte Kapazität ■ Festplatte – alle Metriken, mit Ausnahme der Anzahl der Lesevorgänge und der Schreibvorgänge. ■ Arbeitsspeicher – alle Metriken, mit Ausnahme des verwendeten Arbeitsspeichers und der Rollup-Mindestwerte und -Maximalwerte. ■ Betriebsvorgänge virtueller Maschinen – alle Metriken | <p>Verwendung für Langzeit-Leistungsüberwachung, wenn Gerätestatistiken nicht erforderlich sind, Sie jedoch nicht nur die grundlegenden Statistiken erstellen möchten.</p> |
| Ebene 3 | <ul style="list-style-type: none"> ■ Metriken der Ebene 1 und der Ebene 2 ■ Metriken für alle Indikatoren, mit Ausnahme der Rollup-Mindestwerte und -Maximalwerte. ■ Gerätemetriken | <p>Verwendung für Kurzzeit-Leistungsüberwachung, nachdem Probleme aufgetreten oder wenn Gerätestatistiken erforderlich sind.</p> |
| Ebene 4 | Alle vom vCenter Server unterstützten Metriken, auch für jene mit maximalen und minimalen Rollup-Werten. | <p>Verwendung für Kurzzeit-Leistungsüberwachung, nachdem Probleme aufgetreten oder wenn Gerätestatistiken erforderlich sind.</p> |

Hinweis Wenn die Statistikebenen (Ebene 3 oder Ebene 4) über den Standardwert hinaus verwendet werden, kann dies dazu führen, dass es bei einem bestimmten vpxd-Prozess zu Speicherzuwächsen kommt, wenn die Statistikinformationen nicht so schnell wie erforderlich in der Datenbank gespeichert werden können. Wenn der Nutzungsgrenzwert dieser Statistikebenen nicht genau überwacht wird, kann dies zu übermäßigen Speicherzuwächsen beim vpxd-Dienst und somit zu einem Systemabsturz führen.

Für den Fall, dass der Administrator eine dieser Ebenen anhebt, muss der Administrator die Größe des vpxd-Prozesses überwachen und sicherstellen, dass nach der Änderung kein grenzenloses Wachstum stattfindet.

Konfigurieren von Laufzeiteinstellungen für vCenter Server

Sie können die vCenter Server-ID, die verwaltete Adresse und den Namen ändern. Sie müssen möglicherweise Änderungen vornehmen, wenn Sie mehrere vCenter Server-Systeme in derselben Umgebung ausführen.

Voraussetzungen

Erforderliche Berechtigung: **Global.Einstellungen**

Verfahren

- 1 Navigieren Sie im vSphere Client zur vCenter Server-Instanz.
- 2 Wählen Sie die Registerkarte **Konfigurieren** aus.
- 3 Wählen Sie unter **Einstellungen** die Option **Allgemein** aus.
- 4 Klicken Sie auf **Bearbeiten**.
- 5 Wählen Sie im Dialogfeld „vCenter Server-Einstellungen bearbeiten“ **Laufzeiteinstellungen** aus.
- 6 Geben Sie unter **Eindeutige vCenter Server-ID** eine eindeutige ID ein.

Sie können diesen Wert im Zahlenbereich von 0 bis 63 festlegen, um jedes vCenter Server-System in einer gemeinsamen Umgebung zu kennzeichnen. Standardmäßig wird ein willkürlicher ID-Wert generiert.
- 7 Geben Sie im Feld **Verwaltete Adresse von vCenter Server** die Systemadresse von vCenter Server ein.

Die Adresse kann IPv4, IPv6, ein vollqualifizierter Domänenname, eine IP-Adresse oder ein anderes Adressformat sein.
- 8 Geben Sie unter **Name von vCenter Server** den Namen des vCenter Server-Systems ein.

Wenn Sie den DNS-Namen von vCenter Server ändern, können Sie dieses Textfeld verwenden, um den vCenter Server-Namen entsprechend zu ändern.
- 9 Klicken Sie auf **Speichern**.

Nächste Schritte

Wenn Sie Änderungen an der eindeutigen ID des vCenter Server-Systems vorgenommen haben, ist ein Neustart des vCenter Server-Systems erforderlich, damit diese Änderungen wirksam werden.

Konfigurieren von Benutzerverzeichniseinstellungen

Sie können einige der Möglichkeiten konfigurieren, anhand derer vCenter Server mit dem Benutzerverzeichnisserver interagiert, der als Identitätsquelle dient.

Für vCenter Server-Versionen vor vCenter Server 5.0 gelten diese Einstellungen für eine Active Directory-Instanz, die vCenter Server zugeordnet ist. Für vCenter Server 5.0 und höher gelten diese Einstellungen für vCenter Single Sign On-Identitätsquellen.

Voraussetzungen

Erforderliche Berechtigung: **Global.Einstellungen**

Verfahren

- 1 Navigieren Sie im vSphere Client zur vCenter Server-Instanz.
- 2 Wählen Sie die Registerkarte **Konfigurieren** aus.
- 3 Wählen Sie unter **Einstellungen** die Option **Allgemein** aus.
- 4 Klicken Sie auf **Bearbeiten**.
- 5 Wählen Sie im Fenster „Allgemeine vCenter-Einstellungen bearbeiten“ das Verzeichnis **Benutzerverzeichnis**.
- 6 Geben Sie im Feld **Benutzerverzeichnis - Zeitüberschreitung** das Zeitüberschreitungsintervall in Sekunden für die Verbindungsherstellung mit dem Verzeichnisserver ein.
- 7 Aktivieren Sie das Kontrollkästchen **Abfragegrenze**, um eine Größe der Abfragegrenze festzulegen.
- 8 Geben Sie im Feld **Größe der Abfragegrenze** die Anzahl der Benutzer und Gruppen ein, für die Sie Berechtigungen für die untergeordneten Bestandslistenobjekte des vCenter Server-Systems zuweisen können.

Hinweis Sie können im Dialogfeld „Berechtigung hinzufügen“ Benutzern und Gruppen Berechtigungen zuweisen. Das Dialogfeld wird angezeigt, wenn Sie für ein vSphere-Bestandslistenobjekt auf **Berechtigungen hinzufügen** in **Verwalten > Berechtigungen** für ein vSphere-Bestandslistenobjekt klicken.

- 9 Klicken Sie auf **SPEICHERN**.

Konfigurieren von Einstellungen für E-Mail-Absender

Sie müssen die E-Mail-Adresse des Absenderkontos konfigurieren, um vCenter Server-Vorgänge zu verwenden, wie z. B. das Senden von E-Mail-Benachrichtigungen als Alarmaktionen. Sie können E-Mail-Warnungen oder -Alarmlisten mithilfe des anonymen oder Authentifizierungsmodus senden.

Voraussetzungen

Erforderliche Berechtigung: **Global.Einstellungen**

SMTP-Authentifizierung ist verfügbar für:

- Ausschließlich für vSphere 7.0 Update 1 und höhere Versionen.
- Ausschließlich für Office 365-Postfachbenutzer.

- Der SMTP-Mail-Sender sollte die grundlegenden Anforderungen für SMTP-Authentifizierung erfüllen, die im Microsoft-Dokument [Anforderung an die Übermittlung von SMTP AUTH-Clients](#) beschrieben werden.

Verfahren

- 1 Navigieren Sie im vSphere Client zur vCenter Server-Instanz.
- 2 Wählen Sie die Registerkarte **Konfigurieren** aus.
- 3 Wählen Sie unter **Einstellungen** die Option **Allgemein** aus.
- 4 Klicken Sie auf **Bearbeiten**.
- 5 Wählen Sie **E-Mail** aus und geben Sie die Einstellungen ein, die vCenter Server zum Senden von E-Mail-Warnungen verwenden soll.
- 6 Geben Sie im Textfeld **E-Mail-Server** die SMTP-Serverinformationen ein.

Der SMTP-Server ist der DNS-Name oder die IP-Adresse des SMTP-Gateways, das für das Versenden von E-Mail-Nachrichten verwendet werden soll.

- Für den anonymen Versand von E-Mails können Sie beliebige SMTP-Serverinformationen als Namen des E-Mail-Servers eingeben.
 - Für SMTP-Authentifizierung müssen Sie den Namen des E-Mail-Servers als `smtp.office365.com` eingeben, es sei denn, Sie verfügen über eine angepasste Konfiguration. Verwenden Sie die IP-Adresse nicht als E-Mail-Server, da die IP-Adresse für SMTP-Authentifizierung nicht unterstützt wird.
- 7 Geben Sie im Textfeld **E-Mail-Absender** die Informationen des Absenderkontos ein.
Das Absenderkonto ist die E-Mail-Adresse des Absenders.
Für SMTP-Authentifizierung müssen Sie im Textfeld **E-Mail-Absender** den Namen eines gültigen SMTP-Kontos eingeben.

Hinweis Sie müssen die vollständige E-Mail-Adresse sowie den Domännennamen eingeben.

Beispiel: ***mail_server@example.com***

- 8 Klicken Sie auf **SPEICHERN**.
- 9 Dieser Schritt ist ausschließlich für SMTP-Authentifizierung anwendbar.
Sie müssen die SMTP-Benutzereinstellungen wie folgt konfigurieren:
 - a Wählen Sie die Registerkarte **Konfigurieren** aus.
 - b Klicken Sie auf **Erweiterte Einstellungen**.

- c Klicken Sie auf **EINSTELLUNGEN BEARBEITEN** und geben Sie die folgenden Werte für die Konfigurationsparameter ein:

| Name | Wert |
|--------------------|---|
| mail.smtp.username | Name eines gültigen SMTP-Kontos. Hinweis Dieser Kontoname muss mit dem im Textfeld E-Mail-Absender bereitgestellten Kontonamen übereinstimmen, um E-Mails mithilfe von SMTP-Authentifizierung in Schritt 7 senden zu können. |
| mail.smtp.password | Kennwort des gültigen SMTP-Kontos. Hinweis Das Kennwort ist aktuell nicht maskiert und wird angezeigt. Sie müssen einen dedizierten SMTP-E-Mail-Benutzer verwenden, bis die Maskierung in den kommenden Versionen verfügbar ist. |
| mail.smtp.port | 587 |

- d Klicken Sie auf **SPEICHERN**.

Nächste Schritte

Sie können die folgenden Schritte ausführen, um die E-Mail-Einstellungen zu testen:

- 1 Erstellen Sie einen Alarm, der durch eine Benutzeraktion ausgelöst wird.
Die Benutzeraktion kann beispielsweise darin bestehen, eine virtuelle Maschine auszuschalten.
- 2 Stellen Sie sicher, dass Sie eine E-Mail erhalten, wenn der Alarm ausgelöst wird.

Konfigurieren von SNMP-Einstellungen

Sie können bis zu vier Empfänger für das Empfangen von SNMP-Traps vom vCenter Server konfigurieren. Geben Sie für jeden Empfänger einen Hostnamen, einen Port und eine Community an.

Voraussetzungen

Erforderliche Berechtigung: **Global.Einstellungen**

Verfahren

- 1 Navigieren Sie im vSphere Client zur vCenter Server-Instanz.
- 2 Wählen Sie die Registerkarte **Konfigurieren** aus.
- 3 Wählen Sie unter **Einstellungen** die Option **Allgemein** aus.
- 4 Klicken Sie auf **Bearbeiten**.
- 5 Wählen Sie **SNMP-Empfänger**.
- 6 Aktivieren Sie das Kontrollkästchen **Empfänger 1 aktivieren**.

- 7 Geben Sie unter **Primäre Empfänger-URL** den Hostnamen oder die IP-Adresse des SNMP-Empfängers ein.
- 8 Geben Sie im Feld **Empfängerport** die Portnummer des Empfängers ein.
Bei der Portnummer muss es sich um einen Wert zwischen 1 und 65535 handeln.
- 9 Geben Sie im Feld **Community-String** den Community-Bezeichner ein.
- 10 Um Alarme an mehrere Empfänger zu senden, aktivieren Sie die zusätzlichen **Empfänger aktivieren**-Kontrollkästchen und geben Sie für diese Empfänger den Hostnamen, die Portnummer und den Community-Bezeichner ein.
- 11 Klicken Sie auf **Speichern**.

Anzeigen von Porteinstellungen

Sie können die vom Webservice für die Kommunikation mit anderen Anwendungen verwendeten Ports anzeigen. Sie können diese Porteinstellungen nicht konfigurieren.

Der Webservice wird im Rahmen der Installation von VMware vCenter Server installiert. Der Webservice ist eine erforderliche Komponente für Drittanbieteranwendungen, die die VMware SDK-Anwendungsprogrammierschnittstelle (API) verwenden. Weitere Informationen zum Installieren des Webservices finden Sie in der Dokumentation *Installation und Einrichtung von vCenter Server*.

Verfahren

- 1 Navigieren Sie im vSphere Client zur vCenter Server-Instanz.
- 2 Wählen Sie die Registerkarte **Konfigurieren** aus.
- 3 Wählen Sie unter **Einstellungen** die Option **Allgemein** aus.
- 4 Klicken Sie auf **Bearbeiten**.
- 5 Wählen Sie **Ports** aus.
Die vom Webservice verwendeten Ports werden angezeigt.
- 6 Klicken Sie auf **Speichern**.

Konfigurieren von Zeitüberschreitungseinstellungen

Sie können die Zeitüberschreitungsintervalle für vCenter Server-Vorgänge konfigurieren. Diese Intervalle geben den Zeitraum an, nach dessen Ablauf bei vSphere Client eine Zeitüberschreitung eintritt.

Voraussetzungen

Erforderliche Berechtigung: **Global.Einstellungen**

Verfahren

- 1 Navigieren Sie im vSphere Client zur vCenter Server-Instanz.

- 2 Wählen Sie die Registerkarte **Konfigurieren** aus.
- 3 Wählen Sie unter **Einstellungen** die Option **Allgemein** aus.
- 4 Klicken Sie auf **Bearbeiten**.
- 5 Wählen Sie **Zeitüberschreitungseinstellungen**.
- 6 Geben Sie im Feld **Normal** das Zeitüberschreitungsintervall für normale Vorgänge in Sekunden ein.
Legen Sie für diesen Wert nicht Null (0) fest.
- 7 Geben Sie unter **Lang** das Zeitüberschreitungsintervall für lange Vorgänge in Minuten ein.
Legen Sie für diesen Wert nicht Null (0) fest.
- 8 Klicken Sie auf **Speichern**.
- 9 Starten Sie das vCenter Server-System neu, damit die Änderungen wirksam werden.

Konfigurieren von Protokollierungsoptionen

Sie können den Umfang der Angaben konfigurieren, die vCenter Server in den Protokolldateien erfasst.

Voraussetzungen

Erforderliche Berechtigung: **Global.Einstellungen**

Verfahren

- 1 Navigieren Sie im vSphere Client zur vCenter Server-Instanz.
- 2 Wählen Sie die Registerkarte **Konfigurieren** aus.
- 3 Wählen Sie unter **Einstellungen** die Option **Allgemein** aus.
- 4 Klicken Sie auf **Bearbeiten**.
- 5 Wählen Sie **Protokolleinstellungen**.
- 6 Wählen Sie die Protokollierungsoptionen aus.

| Option | Beschreibung |
|--------------------------------|--|
| Keine | Schaltet die Protokollierung aus |
| Error | Zeigt nur Protokolleinträge für Fehler an |
| Warnung | Zeigt Protokolleinträge für Fehler und Warnungen an |
| Info | Zeigt Protokolleinträge für Informationen, Fehler und Warnungen an |
| Ausführlich | Zeigt ausführliche Protokolleinträge für Informationen, Fehler und Warnungen an |
| Ausführlich (erweitert) | Zeigt erweiterte ausführliche Protokolleinträge für Informationen, Fehler, Warnungen und ausführliche Protokolleinträge an |

7 Klicken Sie auf **SPEICHERN**.

Ergebnisse

Änderungen an den Protokolleinstellungen werden sofort wirksam. Es ist kein Neustart des vCenter Server-Systems erforderlich.

Konfigurieren von Datenbankeinstellungen

Sie können die maximale Anzahl von Datenbankverbindungen konfigurieren, die gleichzeitig bestehen können. Damit das Wachstum der vCenter Server-Datenbank begrenzt und Speicherplatz eingespart wird, können Sie die Datenbank so konfigurieren, dass Informationen zu Aufgaben oder Ereignissen regelmäßig verworfen werden.

Hinweis Verwenden Sie nicht die Optionen zur Datenbankaufbewahrung, wenn Sie den vollständigen Verlauf der Aufgaben und Ereignisse für Ihren vCenter Server aufbewahren möchten.

Verfahren

- 1 Navigieren Sie im vSphere Client zur vCenter Server-Instanz.
- 2 Wählen Sie die Registerkarte **Konfigurieren** aus.
- 3 Wählen Sie unter **Einstellungen** die Option **Allgemein** aus.
- 4 Klicken Sie auf **Bearbeiten**.
- 5 Klicken Sie im Fenster „Allgemeine vCenter-Einstellungen bearbeiten“ auf **Datenbank**.
- 6 Geben Sie in das Feld **Maximale Verbindungen** die erforderliche Anzahl an Verbindungen ein.

Hinweis Ändern Sie diesen Wert nur dann, wenn bei Ihrem System eines der folgenden Probleme vorliegt.

- Wenn Ihr vCenter Server-System viele Vorgänge häufig ausführt und die Leistung kritisch ist, erhöhen Sie die Anzahl der Verbindungen.
 - Wenn die Datenbank freigegeben ist und die Verbindungen zur Datenbank kostenintensiv sind, verringern Sie die Anzahl der Verbindungen.
-

- 7 Aktivieren Sie die Option **Aufgabenbereinigung**, damit vCenter Server die aufbewahrten Aufgaben in regelmäßigen Abständen löscht.
- 8 (Optional) Geben Sie im Feld **Aufgabenaufbewahrung (Tage)** einen Wert (in Tagen ein).
Die Informationen zu den auf diesem vCenter Server-System ausgeführten Aufgaben werden nach der angegebenen Anzahl an Tagen verworfen.
- 9 Aktivieren Sie die Option **Ereignisbereinigung**, damit vCenter Server die aufbewahrten Ereignisse in regelmäßigen Abständen bereinigt.

- 10 (Optional) Geben Sie im Feld **Ereignisaufbewahrung (Tage)** einen Wert (in Tagen ein).

Die Informationen zu den Ereignissen für dieses vCenter Server-System werden nach der angegebenen Anzahl an Tagen verworfen.

Hinweis Überwachen der vCenter Server-Datenbanknutzung und -Festplattenpartition in der vCenter Server-Verwaltungsschnittstelle.

Warnung Die Erhöhung der Ereignisaufbewahrung auf mehr als 30 Tage führt zu einer erheblichen Zunahme der vCenter-Datenbankgröße und kann den vCenter Server zum Herunterfahren bringen. Stellen Sie sicher, dass Sie die vCenter-Datenbank entsprechend vergrößern.

- 11 Starten Sie den vCenter Server neu, um die Änderungen manuell anzuwenden.
- 12 Klicken Sie auf **SPEICHERN**.

Überprüfen von SSL-Zertifikaten für Legacy-Hosts

Sie können vCenter Server so konfigurieren, dass er die SSL-Zertifikate von Hosts überprüft, zu denen er eine Verbindung herstellt. Wenn Sie diese Einstellung konfigurieren, führen vCenter Server und vSphere Client Überprüfungen für gültige SSL-Zertifikate durch, bevor für Vorgänge, wie das Hinzufügen eines Hosts oder das Erstellen einer Remotekonsolenverbindung zu einer virtuellen Maschine, eine Verbindung mit einem Host hergestellt wird.

Die Verbindung zwischen vCenter Server 5.1 bzw. vCenter Server 5.5 und den ESXi-Hosts erfolgt immer über SSL-Fingerabdruckzertifikate. Ab vCenter Server 6.0 werden die SSL-Zertifikate standardmäßig von der VMware-Zertifizierungsstelle (VMCA) signiert. Sie können aber auch Zertifikate einer Drittanbieter-Zertifizierungsstelle verwenden. Der Fingerabdruckmodus wird nur für Legacy-Hosts unterstützt.

Verfahren

- 1 Navigieren Sie im vSphere Client zur vCenter Server-Instanz.
- 2 Wählen Sie die Registerkarte **Konfigurieren** aus.
- 3 Wählen Sie unter **Einstellungen** die Option **Allgemein** aus.
- 4 Klicken Sie auf **Bearbeiten**.
- 5 Wählen Sie **SSL-Einstellungen**.
- 6 Ermitteln Sie den Fingerabdruck jedes Legacy-Hosts, der eine Validierung erfordert.
 - a Melden Sie sich an der direkten Konsole an.
 - b Wählen Sie **Support-Informationen anzeigen** im Menü **Systemanpassung** aus.
Der Fingerabdruck wird in der Spalte auf der rechten Seite angezeigt.
- 7 Vergleichen Sie den Fingerabdruck, den Sie vom Host abgerufen haben, mit dem Fingerabdruck, der im Dialogfeld „SSL-Einstellungen“ von vCenter Server aufgeführt ist.

- 8 Sofern die Fingerabdrücke übereinstimmen, markieren Sie das Kontrollkästchen für den Host. Hosts, die nicht ausgewählt sind, werden getrennt, nachdem Sie auf **Speichern** geklickt haben.
- 9 Klicken Sie auf **Speichern**.

Konfigurieren von erweiterten Einstellungen

Sie können unter **Erweiterte Einstellungen** die vCenter Server-Konfigurationsdatei `vpxd.cfg` ändern.

Sie können **Erweiterte Einstellungen** verwenden, um Einträge zur Datei `vpxd.cfg` hinzuzufügen. Sie können sie jedoch nicht bearbeiten oder löschen. VMware empfiehlt Ihnen, dass Sie nur dann Änderungen an diesen Einstellungen vornehmen, wenn Sie vom technischen Support von VMware dazu aufgefordert werden oder wenn Sie die entsprechenden Anweisungen in der VMware-Dokumentation befolgen.

Voraussetzungen

Erforderliche Berechtigung: **Global.Einstellungen**

Verfahren

- 1 Navigieren Sie im vSphere Client zur vCenter Server-Instanz.
- 2 Wählen Sie die Registerkarte **Konfigurieren** aus.
- 3 Klicken Sie auf **Erweiterte Einstellungen**.
- 4 Klicken Sie auf **Einstellungen bearbeiten**.
- 5 Geben Sie im Feld **Name** einen Namen für die Einstellung ein. Namen müssen mit „config“ beginnen. Beispiel: `config.log`.
- 6 Geben Sie im Feld **Wert** den Wert für die angegebene Einstellung ein.
- 7 Klicken Sie auf **Hinzufügen**.
- 8 Klicken Sie auf **Speichern**.

Ergebnisse

Bei neu hinzugefügten erweiterten Einstellungen wird `config.` an die Einstellungsschlüssel in der Datei `vpxd.cfg` angehängt. Beispiel:

```
config.example.setting = exampleValue
```

Nächste Schritte

Viele Änderungen an erweiterten Einstellungen erfordern einen Neustart des vCenter Server-Systems. Nehmen Sie Kontakt zum technischen Support von VMware auf, um zu ermitteln, ob nach Ihren Änderungen ein Neustart erforderlich ist.

Senden einer Nachricht an andere angemeldete Benutzer

Administratoren können Nachrichten an Benutzer senden, die aktuell bei einem vCenter Server-System angemeldet sind. In solchen Nachrichten können Wartungszeiträume angekündigt oder die Benutzer dazu aufgefordert werden, sich vorübergehend abzumelden.

Verfahren

- 1 Navigieren Sie im vSphere Client zur vCenter Server-Instanz.
- 2 Klicken Sie auf **Konfigurieren**.
- 3 Wählen Sie **Einstellungen > Meldung des Tages** und klicken Sie auf **Bearbeiten**.
- 4 Geben Sie eine Nachricht ein und klicken Sie auf **OK**.

Ergebnisse

Die Nachricht wird in jeder aktiven Benutzersitzung am oberen Rand des vSphere Client angezeigt.

Beitreten oder Verlassen einer Active Directory-Domäne

Sie können vCenter Server zu einer Active Directory-Domäne hinzufügen. Sie können die Benutzer und Gruppen aus dieser Active Directory-Domäne an Ihre vCenter Single Sign-On-Domäne anhängen. Sie können die Active Directory-Domäne verlassen.

Wichtig Das Hinzufügen von vCenter Server zu einer Active Directory-Domäne mit einem schreibgeschützten Domänencontroller (RODC) wird nicht unterstützt. Sie können vCenter Server nur zu einer Active Directory-Domäne mit einem beschreibbaren Domänencontroller hinzufügen.

Wenn Sie Berechtigungen konfigurieren möchten, damit Benutzer und Gruppen aus einem Active Directory auf die vCenter Server-Komponenten zugreifen können, müssen Sie die vCenter Server-Instanz zur Active Directory-Domäne hinzufügen.

Um beispielsweise einem Active Directory-Benutzer die Anmeldung bei der vCenter Server-Instanz durch Verwendung des vSphere Client zu ermöglichen, müssen Sie die vCenter Server-Instanz der Active Directory-Domäne hinzufügen und diesem Benutzer die Rolle des Administrators zuweisen.

Voraussetzungen

- Stellen Sie sicher, dass der Benutzer, der sich bei der vCenter Server-Instanz anmeldet, Mitglied der Gruppe „SystemConfiguration.Administrators“ in vCenter Single Sign-On ist.
- Stellen Sie sicher, dass der Systemname der Appliance ein FQDN ist. Wenn Sie bei der Bereitstellung der Appliance eine IP-Adresse als einen Systemnamen festlegen, können Sie vCenter Server nicht zu einer Active Directory-Domäne hinzufügen.

Verfahren

- 1 Verwenden Sie vSphere Client, um sich als „administrator@*your_domain_name*“ bei der vCenter Server-Instanz anzumelden.
- 2 Wählen Sie im Menü vSphere Client die Option **Verwaltung** aus.
- 3 Wählen Sie **Single Sign On > Konfiguration**.
- 4 Klicken Sie auf die Registerkarte **Identitätsanbieter** und wählen Sie **Active Directory-Domäne** als Identitätsanbieterartyp aus.
- 5 Klicken Sie auf **AD BEITRETEN**.
- 6 Geben Sie im Fenster „Active Directory-Domäne beitreten“ die folgenden Details an.

| Option | Beschreibung |
|---------------------------------|---|
| Domäne | Active Directory-Domänenname, z. B. mydomain.com. Geben Sie in diesem Textfeld keine IP-Adresse an. |
| Organisationseinheit (optional) | Der LDAP-FQDN der vollständigen Organisationseinheit (OU), wie z. B. OU=Engineering,DC=mydomain,DC=com. Wichtig Verwenden Sie dieses Feld nur, wenn Sie mit LDAP vertraut sind. |
| Benutzername | Benutzername im UPN-Format (User Principal Name), z. B. „jchin@mydomain.com“. Wichtig Ein kompatibles Anmeldenamensformat, z. B. DOMAIN\UserName, wird nicht unterstützt. |
| Kennwort | Das Kennwort des Benutzers. |

Hinweis Starten Sie den Knoten neu, um die Änderungen zu übernehmen.

- 7 Klicken Sie auf **BEITRETEN**, um die vCenter Server zur Active Directory-Domäne hinzuzufügen.
Der Vorgang wird erfolgreich automatisch ausgeführt und anstelle der Schaltfläche „AD beitreten“ wird nun die Schaltfläche „AD verlassen“ angezeigt.
- 8 (Optional) Um die Active Directory-Domäne zu verlassen, klicken Sie auf **AD VERLASSEN**.
- 9 Starten Sie den vCenter Server neu, um die Änderungen anzuwenden.

Wichtig Wenn Sie den vCenter Server nicht neu starten, treten bei Verwendung des vSphere Client möglicherweise Probleme auf.

- 10 Wählen Sie die Registerkarte **Identitätsquellen** aus und klicken Sie auf **HINZUFÜGEN**.
 - a Wählen Sie im Fenster „Identitätsquelle hinzufügen“ die Option **Active Directory (Integrierte Windows-Authentifizierung)** als Identitätsquellentyp aus.

- b Geben Sie die Identitätsquelleneinstellungen der hinzugefügten Active Directory-Domäne ein und klicken Sie auf **HINZUFÜGEN**.

Tabelle 3-2. Hinzufügen von Einstellungen der Identitätsquelle

| Textfeld | Beschreibung |
|---------------------------|---|
| Domänenname | Vollqualifizierter Domänenname (FDQN) der Domäne. Geben Sie in diesem Textfeld keine IP-Adresse an. |
| Maschinenkonto verwenden | Wählen Sie diese Option aus, um das Konto der lokalen Maschine als SPN zu verwenden. Mit dieser Option geben Sie nur den Domännennamen an. Verwenden Sie diese Option nicht, wenn Sie diese Maschine voraussichtlich umbenennen werden. |
| SPN (Dienstprinzipalname) | Wählen Sie diese Option aus, wenn Sie die lokale Maschine voraussichtlich umbenennen werden. Sie müssen einen SPN, einen Benutzer, der sich mit der Identitätsquelle authentifizieren kann, und ein Kennwort für den Benutzer angeben. |
| Dienstprinzipalname | Der SPN, mit dem Kerberos den Active Directory-Dienst identifiziert. Schließen Sie die Domäne in den Namen ein, wie z. B. „STS/example.com“. Möglicherweise müssen Sie <code>setspn -S</code> ausführen, um den gewünschten Benutzer hinzuzufügen. Weitere Informationen zu <code>setspn</code> finden Sie in der Microsoft-Dokumentation. Der SPN muss innerhalb der Domäne eindeutig sein. Durch Ausführen von <code>setspn -S</code> wird sichergestellt, dass keine Duplikate erstellt werden. |
| Benutzername | Der Name eines Benutzers, der sich mit dieser Identitätsquelle authentifizieren kann. Verwenden Sie das E-Mail-Adressformat wie z. B. „jchin@mydomain.com“. Den Benutzerprinzipalnamen können Sie mit dem Active Directory-Dienstschnittstellen-Editor (ADSI Edit) überprüfen. |
| Kennwort | Das Kennwort für den Benutzer, der für die Authentifizierung mit dieser Identitätsquelle verwendet wird. Dies ist der Benutzer, der im UPN (Benutzerprinzipalnamen) angegeben ist. Schließen Sie den Domännennamen ein, wie z. B. „jdoe@example.com“. |

Ergebnisse

Auf der Registerkarte **Identitätsquellen** wird die hinzugefügte Active Directory-Domäne angezeigt.

Nächste Schritte

Sie können Berechtigungen konfigurieren, damit Benutzer und Gruppen aus der hinzugefügten Active Directory-Domäne auf die vCenter Server-Komponenten zugreifen können. Informationen zum Verwalten von Berechtigungen finden Sie in der Dokumentation *vSphere-Sicherheit*.

Hinzufügen eines Benutzers zur Gruppe „SystemConfiguration.BashShellAdministrators“

Um den Zugriff auf die Appliance-Bash-Shell mit vSphere Client aktivieren zu können, muss der Benutzer, mit dem Sie sich anmelden, ein Mitglied der Gruppe „SystemConfiguration.BashShellAdministrators“ sein. Diese Gruppe ist standardmäßig leer, und Benutzer müssen manuell hinzugefügt werden.

Voraussetzungen

Überprüfen Sie, dass der Benutzer, den Sie für die Anmeldung bei der vCenter Server-Instanz verwenden, Mitglied der SystemConfiguration.Administrators-Gruppe in der vCenter Single Sign-On-Domäne ist.

Verfahren

- 1 Verwenden Sie vSphere Client, um sich als „administrator@*your_domain_name*“ bei der vCenter Server-Instanz anzumelden.

Die Adresse ist vom Typ „http://*appliance-IP-adresse-oder-FQDN*/ui“.

- 2 Wählen Sie im Menü vSphere Client die Option **Verwaltung** aus.
- 3 Wählen Sie **Single Sign On > Benutzer und Gruppen** aus.
- 4 Klicken Sie auf die Registerkarte **Gruppen** und wählen Sie **SystemConfiguration.BashShellAdministrators** aus den Optionen in der Spalte Gruppenname aus.
- 5 Klicken Sie auf **BEARBEITEN**.
- 6 Wählen Sie zum Hinzufügen von Mitgliedern im Fenster **Gruppe bearbeiten** die Domäne aus dem Dropdown-Menü aus und suchen Sie dann nach den erforderlichen Benutzern.
- 7 Klicken Sie auf **SPEICHERN**.

Neustart eines Knotens

In vSphere Client können Sie einen Knoten im vCenter Server neu starten.

Voraussetzungen

Überprüfen Sie, dass der Benutzer, den Sie für die Anmeldung bei der vCenter Server-Instanz verwenden, Mitglied der SystemConfiguration.Administrators-Gruppe in der vCenter Single Sign-On-Domäne ist.

Verfahren

- 1 Verwenden Sie vSphere Client, um sich als „administrator@*your_domain_name*“ bei der vCenter Server-Instanz anzumelden.
- 2 Klicken Sie auf der Startseite des vSphere Client auf **Verwaltung > Bereitstellung > Systemkonfiguration**.
- 3 Wählen Sie unter „Systemkonfiguration“ einen Knoten aus der Liste aus.
- 4 Klicken Sie auf **KNOTEN NEU STARTEN**.

Anzeigen des Systemzustands von Knoten

Im vSphere Client können Sie den Systemzustand der vCenter Server-Knoten einsehen.

vCenter Server-Instanzen und -Maschinen, die vCenter Server-Dienste ausführen, werden als Knoten betrachtet. Mit grafischen Badges wird der Systemzustand von Knoten angegeben.

Voraussetzungen

Überprüfen Sie, dass der Benutzer, den Sie für die Anmeldung bei der vCenter Server-Instanz verwenden, Mitglied der SystemConfiguration.Administrators-Gruppe in der vCenter Single Sign-On-Domäne ist.

Verfahren

- 1 Verwenden Sie vSphere Client, um sich als „administrator@*your_domain_name*“ bei der vCenter Server-Instanz anzumelden.
Die Adresse ist vom Typ „http://*appliance-IP-adresse-oder-FQDN*/ui“.
- 2 Wählen Sie im Menü vSphere Client die Option **Verwaltung** aus.
- 3 Wählen Sie **Bereitstellung > Systemkonfiguration** aus.
- 4 Wählen Sie einen Knoten aus, um dessen Systemzustand anzuzeigen.

Tabelle 3-3. Systemzustände

| Badge-Symbol | Beschreibung |
|---|---|
|  | Gut. Der Systemzustand des Objekts ist normal. |
|  | Warnung. Bei dem Objekt treten einige Probleme auf. |

Tabelle 3-3. Systemzustände (Fortsetzung)

| Badge-Symbol | Beschreibung |
|---|---|
|  | Kritisch. Das Objekt funktioniert möglicherweise nicht ordnungsgemäß oder wird bald nicht mehr funktionieren. |
|  | Unbekannt. Für dieses Objekt sind keine Daten verfügbar. |

Exportieren eines Support-Pakets

Sie können ein Support-Paket exportieren, das die Protokolldateien für ein bestimmtes Produkt enthält, das in vCenter Server enthalten ist.

Voraussetzungen

Stellen Sie sicher, dass der Benutzer, der sich bei der vCenter Server-Instanz anmeldet, Mitglied der Gruppe „SystemConfiguration.Administrators“ in vCenter Single Sign-On ist.

Verfahren

- 1 Verwenden Sie vSphere Client, um sich als „administrator@*your_domain_name*“ bei der vCenter Server-Instanz anzumelden.

Die Adresse ist vom Typ „http://*appliance-IP-adresse-oder-FQDN*/ui“.

- 2 Klicken Sie auf der Startseite vom vSphere Client auf **Verwaltung > Bereitstellung > Systemkonfiguration**.
- 3 Wählen Sie einen Knoten aus der Liste aus und klicken Sie auf **Support-Paket exportieren**.
- 4 Erweitern Sie im Fenster **Support-Paket exportieren** die Strukturen, um die in der Appliance ausgeführten Dienste anzuzeigen, und deaktivieren Sie die Dienste, für die Sie keine Protokolldateien exportieren möchten.

Standardmäßig sind alle Dienste aktiviert. Wenn Sie das Supportpaket exportieren und an den VMware-Support senden möchten, lassen Sie alle Kontrollkästchen aktiviert. Die Dienste sind in zwei Kategorien unterteilt: eine Kategorie für die Cloud-Infrastruktur, die die Dienste von bestimmten Produkten in der Appliance enthält, und eine Kategorie für die virtuelle Appliance, die bestimmte Dienste für die Appliance und das vCenter Server-Produkt enthält.

- 5 Klicken Sie auf **Support-Paket exportieren** und speichern Sie das Paket auf Ihrem lokalen Computer.

Ergebnisse

Damit haben Sie das Support-Paket auf Ihrem Computer gespeichert und können es analysieren.

Verwenden der Appliance-Shell zur Konfiguration von vCenter Server

4

Über die Appliance-Shell können Sie auf alle API-Befehle und Plug-Ins von vCenter Server zur Überwachung, Fehlerbehebung und Konfiguration der Appliance zugreifen.

Sie können alle Befehle in der Appliance-Shell mit oder ohne das `pi`-Schlüsselwort ausführen.

Dieses Kapitel enthält die folgenden Themen:

- Zugreifen auf die Appliance-Shell
- Aktivieren der Bash-Shell und Zugriff darauf über die Appliance-Shell
- Tastenkombinationen für Bearbeitungsbefehle
- Anzeigen der Hilfe zu den Plug-Ins und API-Befehlen in der Appliance
- Plug-Ins in der vCenter Server-Shell
- Durchsuchen der Protokolldateien mit dem `showlog`-Plug-In
- API-Befehle in der Appliance-Shell
- Konfigurieren von SNMP für vCenter Server
- Konfigurieren der Einstellungen für die Uhrzeitsynchronisierung in vCenter Server
- Verwalten lokaler Benutzerkonten in vCenter Server
- Überwachen von Systemzustand und Statistiken in vCenter Server
- Verwenden des `vimtop`-Plug-In zum Überwachen der Ressourcennutzung von Diensten

Zugreifen auf die Appliance-Shell

Um auf die Plug-Ins zugreifen zu können, die sich in der Appliance befinden, und die API-Befehle anzuzeigen und zu verwenden, greifen Sie zunächst auf die Appliance-Shell zu.

Verfahren

- 1 Greifen Sie auf die Appliance-Shell zu.
 - Wenn Sie direkten Zugriff auf die Appliance-Konsole haben, drücken Sie `Alt+F1`.
 - Wenn Sie eine Remoteverbindung herstellen möchten, verwenden Sie SSH oder eine andere Remotekonsolenverbindung, um eine Sitzung mit der Appliance zu starten.

- 2 Geben Sie einen Benutzernamen und ein Kennwort ein, die von der Appliance erkannt werden.

Ergebnisse

Sie sind bei der Appliance-Shell angemeldet und sehen eine Begrüßungsnachricht.

Aktivieren der Bash-Shell und Zugriff darauf über die Appliance-Shell

Wenn Sie sich bei der Appliance als Benutzer in der Superadministratorenrolle anmelden, können Sie den Zugriff auf die Bash-Shell der Appliance für andere Benutzer aktivieren. Der Root-Benutzer hat standardmäßig Zugriff auf die Bash-Shell der Appliance.

Die Bash-Shell der Appliance ist standardmäßig für den Root-Benutzer aktiviert

Verfahren

- 1 Greifen Sie auf die Appliance-Shell zu und melden Sie sich als Benutzer mit Superadministratorrolle an.
Der Standardbenutzer mit einer Superadministratorrolle ist „root“.
- 2 Wenn Sie den Zugriff auf die Bash-Shell für andere Benutzer aktivieren möchten, führen Sie den folgenden Befehl aus.

```
shell.set --enabled true
```

- 3 Führen Sie `shell` oder `pi shell` aus, um auf die Bash-Shell zuzugreifen.

Tastenkombinationen für Bearbeitungsbefehle

Sie können verschiedene Tastenkombinationen verwenden, um Befehle an der Bash-Shell der Appliance einzugeben und zu bearbeiten.

Tabelle 4-1. Tastenkombinationen und Funktion

| Tastenkombination | Details |
|---|--|
| Registerkarte | Vervollständigt den aktuellen Befehl. Wenn Sie einen Teil des Befehlsnamens eingeben und die Tabulatortaste drücken, vervollständigt das System den Befehlsnamen. Um die Befehle anzuzeigen, die einer eingegebenen Zeichenfolge entsprechen, geben Sie ein Zeichen ein und drücken die Tabulatortaste. |
| Eingabetaste (an der Befehlszeile) | Führt den eingegebenen Befehl aus. |
| Eingabetaste (bei der Anzeige von Mehr) | Zeigt die nächste Seite der Ausgabe an. |
| Lösch- oder Rücktaste | Löscht das Zeichen links vom Cursor. |

Tabelle 4-1. Tastenkombinationen und Funktion (Fortsetzung)

| Tastenkombination | Details |
|-------------------------------|---|
| Pfeil nach links oder Strg+B | Bewegt den Cursor um ein Zeichen nach links. Wenn Sie einen Befehl eingeben, der über eine Zeile hinausgeht, können Sie die Pfeiltaste nach links oder die Tasten Strg-B drücken, um zum Anfang des Befehls zurückzukehren. |
| Pfeil nach rechts oder Strg+F | Bewegt den Cursor um ein Zeichen nach rechts. |
| Esc, B | Verschiebt den Cursor um ein Wort zurück. |
| Esc, F | Verschiebt den Cursor um ein Wort nach vorne. |
| Strg+A | Verschiebt den Cursor zum Anfang der Befehlszeile. |
| Strg+E | Verschiebt den Cursor zum Ende der Befehlszeile. |
| Strg+D | Löscht das vom Cursor ausgewählte Zeichen. |
| Strg+W | Löscht das Wort neben dem Cursor. |
| Strg+K | Löscht den folgenden Teil der Zeile. Wenn Sie Strg+K drücken, wird die ganze Eingabe ab der Cursorposition bis zum Ende der Befehlszeile gelöscht. |
| Strg+U oder Strg+X | Löscht den vorherigen Teil der Zeile. Wenn Sie Strg+U drücken, wird die ganze Eingabe ab Beginn der Befehlszeile bis zur Cursorposition gelöscht. |
| Strg+T | Wechselt die Position des Zeichens links vom Cursor mit der des Zeichens, an dem der Cursor steht. |
| Strg+R oder Strg+L | Zeigt die Systemeingabeaufforderung und Befehlszeile an. |
| Strg+V oder Esc, Q | Fügt einen Code ein, um dem System anzugeben, dass die folgende Tastenkombination wie eine Befehlseingabe behandelt werden muss, nicht wie eine Bearbeitungstaste. |
| Pfeil nach oben oder Strg+P | Ruft Befehle aus dem Verlaufspuffer erneut auf, beginnend mit dem neuesten Befehl. |
| Pfeil nach unten oder Strg+N | Kehrt zu den neuesten Befehlen im Verlaufspuffer zurück, nachdem Sie die Pfeiltaste nach oben oder Strg+P zum erneuten Aufrufen von Befehlen verwendet haben. |
| Strg+Y | Ruft den neuesten Eintrag im Löschpuffer erneut auf. Der Löschpuffer enthält die letzten 10 abgeschnittenen oder gelöschten Elemente. |
| Esc, Y | Ruft den nächsten Eintrag im Löschpuffer erneut auf. Der Löschpuffer enthält die letzten 10 abgeschnittenen oder gelöschten Elemente. Drücken Sie zunächst Strg+Y, um den neuesten Eintrag erneut aufzurufen, und dann Esc, Y bis zu neun Mal, um die weiteren Einträge im Puffer aufzurufen. |
| Esc, C | Zeigt das Zeichen, auf dem sich der Cursor befindet, in Großschreibung an. |
| Esc, U | Ändert die Schreibung aller Zeichen des Worts, auf dem sich der Cursor befindet, zu Großschreibung. |
| Esc, L | Ändert die großgeschriebenen Buchstaben eines Worts ab der Cursorposition bis zum Ende des Worts zu Kleinschreibung. |

Anzeigen der Hilfe zu den Plug-Ins und API-Befehlen in der Appliance

Über die Appliance-Shell können Sie auf die Plug-Ins und API-Befehle von vCenter Server zugreifen. Sie können die Plug-Ins und Befehle verwenden, um die Appliance zu überwachen, zu konfigurieren und Fehler zu beheben.

Mit der Tabulatortaste können Sie API-Befehle, Plug-In-Namen und API-Parameter automatisch vervollständigen. Für Plug-In-Parameter wird die automatische Vervollständigung nicht unterstützt.

Verfahren

- Greifen Sie auf die Appliance-Shell zu und melden Sie sich an.
- Wenn Sie Hilfe zu den Plug-Ins erhalten möchten, führen Sie den Befehl `help pi list` oder den Befehl `? pi list` aus.

Eine Liste aller Plug-Ins in der Appliance wird angezeigt.
- Wenn Sie Hilfe zu den API-Befehlen erhalten möchten, führen Sie den Befehl `help api list` oder den Befehl `? api list` aus.

Eine Liste aller API-Befehle in der Appliance wird angezeigt.
- Hilfe zu einem bestimmten API-Befehl erhalten Sie, indem Sie den Befehl `help api api_name` oder den Befehl `? api api_name` ausführen.

Um beispielsweise Hilfe zum Befehl `com.vmware.appliance.version1.timesync.set` zu erhalten, führen Sie `help api timesync.set` oder `? api timesync.set` aus.

Plug-Ins in der vCenter Server-Shell

Die Plug-Ins in der vCenter Server ermöglichen den Zugriff auf verschiedene Verwaltungstools. Die Plug-Ins sind in der Befehlszeilenschnittstelle (CLI) selbst enthalten. Bei diesen Plug-Ins handelt es sich um eigenständige Linux- oder VMware-Dienstprogramme, die nicht von einem VMware-Dienst abhängig sind.

Tabelle 4-2. In der vCenter Server verfügbare Plug-Ins

| Plug-In | Beschreibung |
|------------------------------------|---|
| <code>com.vmware.clear</code> | Ein Plug-In zum Löschen des Terminalbildschirms. |
| <code>com.vmware.cmsso-util</code> | Ein Plug-In, das Sie zum Koordinieren von Änderungen an der PNID und dem Maschinenzertifikat, zum Aufheben der Registrierung eines Knotens im Komponentenmanager, für vCenter Single Sign-On und zur Neukonfiguration von vCenter Server verwenden. |
| <code>com.vmware.dcli</code> | vAPI-basierter CLI-Client |

Tabelle 4-2. In der vCenter Server verfügbare Plug-Ins (Fortsetzung)

| Plug-In | Beschreibung |
|---|---|
| <code>com.vmware.nslookup</code> | Ein Plug-In zum Abfragen des Domain Name System (DNS), um Domännennamen oder IP-Adresszuordnungen bzw. einen sonstigen spezifischen DNS-Datensatz zu erhalten. |
| <code>com.vmware.pgrep</code> | Ein Plug-In für die Suche nach allen benannten Prozessen. |
| <code>com.vmware.pgtop</code> | Ein Plug-In für die Überwachung der PostgreSQL-Datenbank. |
| <code>com.vmware.ping</code> | Ein Plug-In zum Pingen eines Remotehosts. Akzeptiert dieselben Argumente wie <code>bin/ping</code> . |
| <code>com.vmware.ping6</code> | Ein Plug-In zum Pingen eines Remotehosts. Akzeptiert dieselben Argumente wie <code>bin/ping6</code> . |
| <code>com.vmware.portaccess</code> | Ein Plug-In für die Fehlerbehebung des Portzugriffs auf einen Host. |
| <code>com.vmware.ps</code> | Ein Plug-In für die Anzeige von Statistiken zu laufenden Prozessen. |
| <code>com.vmware.rvc</code> | Ruby vSphere Console |
| <code>com.vmware.service-control</code> | Ein Plug-In zum Verwalten von VMware-Diensten. |
| <code>com.vmware.shell</code> | Ein Plug-In, das den Zugriff auf die Bash-Shell der Appliance ermöglicht. |
| <code>com.vmware.showlog</code> | Ein Plug-In zum Durchsuchen der Protokolldateien. |
| <code>com.vmware.shutdown</code> | Ein Plug-In zum Neustarten oder Herunterfahren der Appliance. |
| <code>com.vmware.software-packages</code> | Ein Plug-In zum Aktualisieren der Softwarepakete in der Appliance. |
| <code>com.vmware.support-bundle</code> | Ein Plug-In zum Erstellen eines Pakets auf dem lokalen Dateisystem und Exportieren an ein Linux-Remotesystem. Wenn Sie das Plug-In zusammen mit dem <code>stream</code> -Befehl verwenden, wird das Supportpaket nicht auf dem lokalen Dateisystem erstellt, sondern direkt an das Linux-Remotesystem exportiert. |
| <code>com.vmware.top</code> | Ein Plug-In, das Prozessinformationen anzeigt. Akzeptiert dieselben Argumente wie <code>/usr/bin/top/</code> . |
| <code>com.vmware.tracepath</code> | Ein Plug-In, das den Pfad zu einem Netzwerkhost verfolgt. Akzeptiert dieselben Argumente wie <code>/sbin/tracepath</code> . |
| <code>com.vmware.tracepath6</code> | Ein Plug-In, das den Pfad zu einem Netzwerkhost verfolgt. Akzeptiert dieselben Argumente wie <code>/sbin/tracepath6</code> . |
| <code>com.vmware.updatemgr-util</code> | Ein Plug-In zum Konfigurieren von VMware Update Manager. |

Tabelle 4-2. In der vCenter Server verfügbare Plug-Ins (Fortsetzung)

| Plug-In | Beschreibung |
|---|--|
| <code>com.vmware.vcenter-restore</code> | Ein Plug-In zum Wiederherstellen von vCenter Server. |
| <code>com.vmware.vimtop</code> | Ein Plug-In für die Anzeige einer Liste der vSphere-Dienste und deren Ressourcennutzung. |

Durchsuchen der Protokolldateien mit dem showlog-Plug-In

Sie können die Protokolldateien in vCenter Server durchsuchen, um sie auf Fehler zu prüfen.

Verfahren

- 1 Greifen Sie auf die Appliance-Shell zu und melden Sie sich an.
- 2 Geben Sie den `showlog`-Befehl ein, fügen Sie ein Leerzeichen hinzu, und drücken Sie die Tabulatortaste, um alle Inhalte des Ordners `/var/log` anzuzeigen.
- 3 Führen Sie den Befehl zum Anzeigen der Firstboot-Protokolldateien aus.

```
showlog /var/log/firstboot/cloudvm.log
```

API-Befehle in der Appliance-Shell

Anhand der API-Befehle in vCenter Server können Sie verschiedene Verwaltungsaufgaben durchführen. Die API-Befehle werden vom Appliance-Verwaltungsdienst bereitgestellt. Sie können die Uhrzeitsynchronisierungseinstellungen bearbeiten, Prozesse und Dienste überwachen, die SNMP-Einstellungen einrichten usw.

Tabelle 4-3. Verfügbare API-Befehle in vCenter Server

| API-Befehl | Beschreibung |
|---|---|
| <code>com.vmware.appliance.health.applmgmt.get</code> | Ruft den Zustand des applmgmt-Diensts ab. |
| <code>com.vmware.appliance.health.databasestorage.get</code> | Ruft den Zustand des Datenbankspeichers ab. |
| <code>com.vmware.appliance.health.load.get</code> | Ruft den Zustand der CPU-Last ab. |
| <code>com.vmware.appliance.health.mem.get</code> | Ruft den Zustand des Arbeitsspeichers ab. |
| <code>com.vmware.appliance.health.softwarepackages.get</code> | Ruft den Zustand der Systemaktualisierung ab. |
| <code>com.vmware.appliance.health.storage.get</code> | Ruft den allgemeinen Speicherzustand ab. |
| <code>com.vmware.appliance.health.swap.get</code> | Ruft den Auslagerungszustand ab. |
| <code>com.vmware.appliance.health.system.get</code> | Ruft den Systemzustand ab. |

Tabelle 4-3. Verfügbare API-Befehle in vCenter Server (Fortsetzung)

| API-Befehl | Beschreibung |
|--|--|
| <code>com.vmware.appliance.health.system.lastcheck</code> | Ruft die Uhrzeit der letzten Zustandsprüfung ab. |
| <code>com.vmware.appliance.monitoring.list</code> | Ruft eine Liste der überwachten Elemente ab. |
| <code>com.vmware.appliance.monitoring.get</code> | Ruft Informationen zum überwachten Element ab. |
| <code>com.vmware.appliance.monitoring.query</code> | Fragt eine Reihe von Werten für die überwachten Elemente ab. |
| <code>com.vmware.appliance.recovery.backup.job.cancel</code> | Bricht einen Sicherungsjob nach ID ab. |
| <code>com.vmware.appliance.recovery.backup.job.create</code> | Startet einen Sicherungsjob. |
| <code>com.vmware.appliance.recovery.backup.job.get</code> | Ruft den Status des Sicherungsjobs nach ID ab. |
| <code>com.vmware.appliance.recovery.backup.job.list</code> | Ruft eine Liste der Sicherungsjobs ab. |
| <code>com.vmware.appliance.recovery.backup.parts.list</code> | Ruft eine Liste der vCenter Server-Komponenten ab, die in eine Sicherungsaufgabe einbezogen werden können. |
| <code>com.vmware.appliance.recovery.backup.parts.get</code> | Ruft detaillierte Informationen für ein Sicherungsteil ab. |
| <code>com.vmware.appliance.recovery.backup.validate</code> | Validiert Parameter für einen Sicherungsjob, ohne den Job zu starten. |
| <code>com.vmware.appliance.recovery.restore.job.cancel</code> | Bricht einen Wiederherstellungsjob ab. |
| <code>com.vmware.appliance.recovery.restore.job.create</code> | Startet einen Wiederherstellungsjob. |
| <code>com.vmware.appliance.recovery.restore.job.get</code> | Ruft den Status des Wiederherstellungsjobs ab. |
| <code>com.vmware.appliance.recovery.restore.validate</code> | Validiert Wiederherstellungsparameter für einen Wiederherstellungsjob, ohne den Job zu starten. |
| <code>com.vmware.appliance.system.uptime.get</code> | Ruft die Systembetriebszeit ab. |
| <code>com.vmware.appliance.version1.access.consolecli.get</code> | Ruft Informationen über den Status der konsolenbasiert gesteuerten CLI ab (TTY1). |
| <code>com.vmware.appliance.version1.access.consolecli.set</code> | Legt den Aktivierungsstatus der konsolenbasiert gesteuerten CLI fest (TTY1). |

Tabelle 4-3. Verfügbare API-Befehle in vCenter Server (Fortsetzung)

| API-Befehl | Beschreibung |
|---|--|
| <code>com.vmware.appliance.version1.access.dcu.get</code> | Ruft Informationen über den Status der Benutzerschnittstelle der direkten Konsole (Direct Console User Interface, DCUI TTY2) fest. |
| <code>com.vmware.appliance.version1.access.dcu.set</code> | Legt den Aktivierungsstatus der Direct Console User Interface (DCUI TTY2) fest. |
| <code>com.vmware.appliance.version1.access.shell.get</code> | Ruft Informationen zum Status der Bash-Shell ab, greift also auf die Bash-Shell von innerhalb der gesteuerten CLI zu. |
| <code>com.vmware.appliance.version1.access.shell.set</code> | Legt den Aktivierungsstatus der Bash-Shell fest, greift also auf die Bash-Shell von innerhalb der gesteuerten CLI zu. |
| <code>com.vmware.appliance.version1.access.ssh.get</code> | Ruft den Aktivierungsstatus der SSH-basiert gesteuerten CLI ab. |
| <code>com.vmware.appliance.version1.access.ssh.set</code> | Legt den Aktivierungsstatus der SSH-basiert gesteuerten CLI fest. |
| <code>com.vmware.appliance.version1.localaccounts.user.add</code> | Erstellt ein neues lokales Benutzerkonto. |
| <code>com.vmware.appliance.version1.localaccounts.user.delete</code> | Löscht ein lokales Benutzerkonto. |
| <code>com.vmware.appliance.version1.localaccounts.user.get</code> | Ruft die Informationen des lokalen Benutzerkontos ab. |
| <code>com.vmware.appliance.version1.localaccounts.user.list</code> | Listet lokale Benutzerkonten auf. |
| <code>com.vmware.appliance.version1.localaccounts.user.password.update</code> | Aktualisiert das Kennwort eines angemeldeten Benutzers oder des Benutzers, den Sie im <code>username</code> -Parameter angeben. |
| <code>com.vmware.appliance.version1.localaccounts.user.set</code> | Aktualisiert Eigenschaften des lokalen Benutzerkontos wie Rolle, vollständiger Name, aktivierter Status und Kennwort. |
| <code>com.vmware.appliance.version1.monitoring.snmp.disable</code> | Beendet einen aktivierten SNMP-Agenten. |
| <code>com.vmware.appliance.version1.monitoring.snmp.enable</code> | Startet einen deaktivierten SNMP-Agenten. |
| <code>com.vmware.appliance.version1.monitoring.snmp.get</code> | Gibt eine SNMP-Agentenkonfiguration zurück. |
| <code>com.vmware.appliance.version1.monitoring.snmp.hash</code> | Generiert lokalisierte Schlüssel für sichere SNMPv3-Kommunikationen. |

Tabelle 4-3. Verfügbare API-Befehle in vCenter Server (Fortsetzung)

| API-Befehl | Beschreibung |
|--|--|
| <code>com.vmware.appliance.version1.monitoring.snmp.limits</code> | Ruft Informationen zu SNMP-Beschränkungen ab. |
| <code>com.vmware.appliance.version1.monitoring.snmp.reset</code> | Setzt Einstellungen auf Werkseinstellungen zurück. |
| <code>com.vmware.appliance.version1.monitoring.snmp.set</code> | Legt die SNMP-Konfiguration fest. |
| <code>com.vmware.appliance.version1.monitoring.snmp.stats</code> | Generiert einen Diagnosebericht für den SNMP-Agenten. |
| <code>com.vmware.appliance.version1.networking.dns.domains.add</code> | Fügt Domänen zu DNS-Suchdomänen hinzu. |
| <code>com.vmware.appliance.version1.networking.dns.domains.list</code> | Ruft eine Liste der DNS-Suchdomänen ab. |
| <code>com.vmware.appliance.version1.networking.dns.domains.set</code> | Legt DNS-Suchdomänen fest. |
| <code>com.vmware.appliance.version1.networking.dns.hostname.get</code> | Ruft den vollqualifizierten Domänennamen ab. |
| <code>com.vmware.appliance.version1.networking.dns.hostname.set</code> | Legt den vollqualifizierten Domänennamen fest. |
| <code>com.vmware.appliance.version1.networking.dns.servers.add</code> | Fügt einen DNS-Server hinzu. Diese Methode schlägt fehl, wenn Sie DHCP verwenden. |
| <code>com.vmware.appliance.version1.networking.dns.servers.get</code> | Ruft die DNS-Serverkonfiguration ab. |
| <code>com.vmware.appliance.version1.networking.dns.servers.set</code> | Legt die DNS-Serverkonfiguration fest. Wenn der Host zum Abrufen der DNS-Server und des Hostnamens per DHCP konfiguriert ist, wird eine DHCP-Aktualisierung erzwungen. |
| <code>com.vmware.appliance.version1.networking.firewall.addr.inbound.add</code> | Fügt eine Firewall-Regel hinzu, um Zugriff von einer eingehenden IP-Adresse zuzulassen oder zu verweigern. |
| <code>com.vmware.appliance.version1.networking.firewall.addr.inbound.delete</code> | Löscht eine spezifische Regel an einer bestimmten Position oder löscht alle Regeln. |
| <code>com.vmware.appliance.version1.networking.firewall.addr.inbound.list</code> | Ruft eine sortierte Liste der eingehenden IP-Adressen ab, die von einer Firewall-Regel zugelassen oder verweigert werden. |
| <code>com.vmware.appliance.version1.networking.interfaces.get</code> | Ruft Informationen über eine bestimmte Netzwerkschnittstelle ab. |
| <code>com.vmware.appliance.version1.networking.interfaces.list</code> | Ruft eine Liste der verfügbaren Netzwerkschnittstellen ab, einschließlich der noch nicht konfigurierten Schnittstellen. |

Tabelle 4-3. Verfügbare API-Befehle in vCenter Server (Fortsetzung)

| API-Befehl | Beschreibung |
|---|--|
| <code>com.vmware.appliance.version1.networking.ipv4.get</code> | Ruft die IPv4-Netzwerkconfiguration für Schnittstellen ab. |
| <code>com.vmware.appliance.version1.networking.ipv4.list</code> | Ruft die IPv4-Netzwerkconfiguration für alle konfigurierten Schnittstellen ab. |
| <code>com.vmware.appliance.version1.networking.ipv4.renew</code> | Erneuert die IPv4-Netzwerkconfiguration an Schnittstellen. Wenn die Schnittstelle für die Verwendung von DHCP für die IP-Adressenzuweisung konfiguriert ist, wird die Lease der Schnittstelle verlängert. |
| <code>com.vmware.appliance.version1.networking.ipv4.set</code> | Legt die IPv4-Netzwerkconfiguration für eine Schnittstelle fest. |
| <code>com.vmware.appliance.version1.networking.ipv6.get</code> | Ruft die IPv6-Netzwerkconfiguration für Schnittstellen ab. |
| <code>com.vmware.appliance.version1.networking.ipv6.list</code> | Ruft die IPv6-Netzwerkconfiguration für alle konfigurierten Schnittstellen ab. |
| <code>com.vmware.appliance.version1.networking.ipv6.set</code> | Legt die IPv6-Netzwerkconfiguration für eine Schnittstelle fest. |
| <code>com.vmware.appliance.version1.networking.routes.add</code> | Fügt statische Routing-Regeln hinzu. Ein Ziel/Präfix des Typs „0.0.0.0/0“ (für IPv4) oder „::/0“ (für IPv6) bezieht sich auf das Standardgateway. |
| <code>com.vmware.appliance.version1.networking.routes.delete</code> | Löscht statische Routing-Regeln. |
| <code>com.vmware.appliance.version1.networking.routes.list</code> | Ruft die Routing-Tabelle ab. Ein Ziel/Präfix des Typs „0.0.0.0/0“ (für IPv4) oder „::/0“ (für IPv6) bezieht sich auf das Standardgateway. |
| <code>com.vmware.appliance.version1.ntp.get</code> | Ruft NTP-Konfigurationseinstellungen ab. Wenn Sie den <code>timesync.get</code> -Befehl ausführen, können Sie die aktuelle Uhrzeitsynchronisierungsmethode (anhand von NTP oder VMware Tools) abrufen. Der <code>ntp.get</code> -Befehl gibt immer die NTP-Serverinformationen zurück, selbst wenn die Uhrzeitsynchronisierungsmethode nicht auf NTP festgelegt ist. Wenn die Uhrzeitsynchronisierungsmethode nicht für die Verwendung von NTP festgelegt ist, wird der NTP-Status als heruntergefahren angezeigt. |

Tabelle 4-3. Verfügbare API-Befehle in vCenter Server (Fortsetzung)

| API-Befehl | Beschreibung |
|--|--|
| <code>com.vmware.appliance.version1.ntp.server.add</code> | Fügt NTP-Server hinzu. Dieser Befehl fügt der Konfiguration NTP-Server hinzu. Wenn die Uhrzeitsynchronisierung NTP-basiert ist, wird der NTP-Daemon neu gestartet, um die neuen NTP-Server zu laden. Andernfalls fügt der Befehl einfach Server zur NTP-Konfiguration hinzu. |
| <code>com.vmware.appliance.version1.ntp.server.delete</code> | Löscht NTP-Server. Dieser Befehl löscht NTP-Server aus der Konfiguration. Wenn die Uhrzeitsynchronisierung NTP-basiert ist, wird der NTP-Daemon neu gestartet, um die neue NTP-Konfiguration zu laden. Andernfalls löscht der Befehl einfach Server aus der NTP-Konfiguration. |
| <code>com.vmware.appliance.version1.ntp.server.set</code> | Legt NTP-Server fest. Dieser Befehl löscht alte NTP-Server aus der Konfiguration und richtet die Eingabe-NTP-Server in der Konfiguration ein. Wenn die Uhrzeitsynchronisierung anhand von NTP festgelegt wird, wird der NTP-Daemon neu gestartet, um die neue NTP-Konfiguration zu laden. Andernfalls ersetzt dieser Befehl nur die Server in der NTP-Konfiguration durch die als Eingabe bereitgestellten NTP-Server. |
| <code>com.vmware.appliance.version1.resources.cpu.stats.get</code> | Ruft CPU-Statistiken ab. |
| <code>com.vmware.appliance.version1.resources.load.health.get</code> | Ruft den Lastzustand ab. |
| <code>com.vmware.appliance.version1.resources.load.stats.get</code> | Ruft Lastdurchschnittswerte ab (in Intervallen von 1, 5 und 15 Minuten). |
| <code>com.vmware.appliance.version1.resources.mem.health.get</code> | Ruft den Zustand des Arbeitsspeichers ab. |
| <code>com.vmware.appliance.version1.resources.mem.stats.get</code> | Ruft Arbeitsspeicherstatistiken ab. |
| <code>com.vmware.appliance.version1.resources.net.stats.get</code> | Ruft Netzwerkstatistiken ab. |
| <code>com.vmware.appliance.version1.resources.net.stats.list</code> | Ruft Netzwerkstatistiken für alle laufenden Schnittstellen ab. |
| <code>com.vmware.appliance.version1.resources.processes.stats.list</code> | Ruft Statistiken aller Prozesse ab. |
| <code>com.vmware.appliance.version1.resources.softwarepackages.health.get</code> | Ruft den Zustand der Update-Komponente ab. |

Tabelle 4-3. Verfügbare API-Befehle in vCenter Server (Fortsetzung)

| API-Befehl | Beschreibung |
|---|--|
| <code>com.vmware.appliance.version1.resources.storage.health.get</code> | Ruft Speicherzustandsstatistiken ab. |
| <code>com.vmware.appliance.version1.resources.storage.stats.list</code> | Ruft Speicherstatistiken für jede logische Festplatte ab. |
| <code>com.vmware.appliance.version1.resources.swap.health.get</code> | Ruft den Auslagerungszustand ab. |
| <code>com.vmware.appliance.version1.resources.swap.stats.get</code> | Ruft Auslagerungsstatistiken ab. |
| <code>com.vmware.appliance.version1.resources.system.health.get</code> | Ruft den Gesamtzustand des Systems ab. |
| <code>com.vmware.appliance.version1.resources.system.stats.get</code> | Ruft den Systemstatus ab. |
| <code>com.vmware.appliance.version1.services.list</code> | Ruft die Liste aller bekannten Dienste ab. |
| <code>com.vmware.appliance.version1.services.restart</code> | Startet einen Dienst neu. |
| <code>com.vmware.appliance.version1.services.status.get</code> | Ruft den Status eines Dienstes ab. |
| <code>com.vmware.appliance.version1.services.stop</code> | Beendet einen Dienst. |
| <code>com.vmware.appliance.version1.system.storage.list</code> | Ruft die Festplatten-Partitions-Zuordnung ab. |
| <code>com.vmware.appliance.version1.system.storage.resize</code> | Ändert die Größe aller Partitionen auf 100 Prozent der Festplattengröße. |
| <code>com.vmware.appliance.version1.system.time.get</code> | Ruft die Systemzeit ab. |
| <code>com.vmware.appliance.version1.system.update.get</code> | Ruft die URL-basierte Patch-Konfiguration ab. |
| <code>com.vmware.appliance.version1.system.update.set</code> | Legt die URL-basierte Patch-Konfiguration fest. |
| <code>com.vmware.appliance.version1.system.version.get</code> | Ruft die Version der Appliance ab. |
| <code>com.vmware.appliance.version1.timesync.get</code> | Ruft die Uhrzeitsynchronisierungskonfiguration ab. |
| <code>com.vmware.appliance.version1.timesync.set</code> | Legt die Uhrzeitsynchronisierungskonfiguration fest. |

Konfigurieren von SNMP für vCenter Server

vCenter Server enthält einen SNMP-Agent, der Trap-Benachrichtigungen senden und GET-, GETBULK- und GETNEXT-Anforderungen empfangen kann.

Mit den Shell-API-Befehlen der Appliance können Sie den SNMP-Agent der vCenter Server aktivieren und konfigurieren. Sie konfigurieren den Agenten unterschiedlich, je nachdem, ob Sie SNMP v1/v2c oder SNMP v3 verwenden möchten.

SNMP v3-Berichte werden nicht unterstützt. vCenter Server unterstützt nur Benachrichtigungen wie v1- und v2c-Traps sowie v3-Traps mit allen Sicherheitsstufen.

Konfigurieren des SNMP-Agenten zum Abfragen

Wenn Sie den SNMP-Agenten für vCenter Server zum Abfragen konfigurieren, kann es Anforderungen von Clientsystemen für die SNMP-Verwaltung, wie z. B. GET-, GETNEXT- und GETBULK-Anforderungen, überwachen und darauf reagieren.

Der eingebettete SNMP-Agent überwacht standardmäßig den UDP-Port 161 für Abfrageanforderungen von Verwaltungssystemen. Sie können den `snmp.set --port`-Befehl zum Konfigurieren eines alternativen Ports verwenden. Um Konflikte zwischen dem Port für den SNMP-Agenten und den Ports für andere Dienste zu vermeiden, verwenden Sie einen UDP-Port, der nicht in `/etc/services` definiert ist.

Verfahren

- 1 Greifen Sie auf die Appliance-Shell zu und melden Sie sich als Benutzer mit Administrator- oder Superadministratorrolle an.

Der Standardbenutzer mit der Superadministratorrolle ist „root“.

- 2 Führen Sie den `snmp.set --port`-Befehl aus, um den Port zu konfigurieren.

Führen Sie beispielsweise folgenden Befehl aus:

```
snmp.set --port port
```

Hier ist *port* der Port für den eingebetteten SNMP-Agenten, der zum Überwachen der Abfragen verwendet werden soll.

Wichtig Der angegebene Port darf nicht bereits von anderen Diensten verwendet werden. Verwenden Sie IP-Adressen aus dem dynamischen Bereich ab Port 49152.

- 3 (Optional) Wenn der SNMP-Agent nicht aktiviert ist, können Sie ihn durch Ausführen des Befehls `snmp.enable` aktivieren.

Konfigurieren von vCenter Server für SNMP v1 und v2c

Wenn Sie den SNMP-Agenten der vCenter Server für SNMP v1 und v2c konfigurieren, unterstützt der Agent das Senden von Benachrichtigungen und das Empfangen von GET-Anforderungen.

In SNMP v1 und v2c sind Community-Strings Namespaces, die ein oder mehrere verwaltete Objekte enthalten. Namespaces können zwar zur Authentifizierung verwendet werden, aber damit wird der Datenaustausch nicht gesichert. Verwenden Sie zum Sichern der Datenübertragung SNMP v3.

Verfahren

1 Konfigurieren von SNMP-Communitys

Um den SNMP-Agenten für vCenter Server zum Senden und Empfangen von SNMP v1- und v2c-Meldungen zu aktivieren, müssen Sie mindestens eine Community für den Agenten konfigurieren.

2 Konfigurieren des SNMP-Agenten zum Senden von v1- oder v2c-Benachrichtigungen

Sie können den SNMP-Agenten für vCenter Server zum Senden von Benachrichtigungen für virtuelle Maschinen und Umgebungen an Verwaltungssysteme verwenden.

Konfigurieren von SNMP-Communitys

Um den SNMP-Agenten für vCenter Server zum Senden und Empfangen von SNMP v1- und v2c-Meldungen zu aktivieren, müssen Sie mindestens eine Community für den Agenten konfigurieren.

Eine SNMP-Community definiert eine Gruppe von Geräten und Verwaltungssystemen. Nur Geräte und Verwaltungssysteme, die Mitglieder derselben Community sind, können SNMP-Meldungen austauschen. Ein Gerät oder Verwaltungssystem kann Mitglied in mehreren Communitys sein.

Verfahren

- 1 Greifen Sie auf die Appliance-Shell zu und melden Sie sich als Benutzer mit Administrator- oder Superadministratorrolle an.

Der Standardbenutzer mit der Superadministratorrolle ist „root“.

- 2 Führen Sie den Befehl `snmp.set --communities` aus, um eine SNMP-Community zu konfigurieren.

Wenn Sie z. B. Communitys für Netzwerkbetriebszentren im öffentlichen Bereich, im Osten und im Westen konfigurieren möchten, führen Sie folgenden Befehl aus:

```
snmp.set --communities public,eastnoc,westnoc
```

Jedes Mal, wenn Sie eine Community unter Verwendung dieses Befehls angeben, überschreiben die von Ihnen angegebenen Einstellungen die vorherige Konfiguration.

Trennen Sie zum Angeben von mehreren Communitys die Namen durch ein Komma.

Konfigurieren des SNMP-Agenten zum Senden von v1- oder v2c-Benachrichtigungen

Sie können den SNMP-Agenten für vCenter Server zum Senden von Benachrichtigungen für virtuelle Maschinen und Umgebungen an Verwaltungssysteme verwenden.

Zum Senden von SNMP v1- und v2c-Benachrichtigungen mithilfe des SNMP-Agenten müssen Sie die Zieladresse (Empfänger), die Unicast-Adresse, die Community und optional einen Port konfigurieren. Wenn Sie keinen Port angeben, sendet der SNMP-Agent Benachrichtigungen standardmäßig an den UDP-Port 162 auf dem Zielverwaltungssystem.

Verfahren

- 1 Greifen Sie auf die Appliance-Shell zu und melden Sie sich als Benutzer mit Administrator- oder Superadministratorrolle an.

Der Standardbenutzer mit der Superadministratorrolle ist „root“.

- 2 Führen Sie den `snmp.set --targets`-Befehl aus:

```
snmp.set --targets target_address@port/community
```

Hier sind *target_address*, *port* und *community* die Adresse des Zielsystems, die Portnummer, an die die Benachrichtigungen gesendet werden sollen, und der Name der Community. Der Portwert ist optional. Wenn Sie keinen Port angeben, wird der Standardport 161 verwendet.

Jedes Mal, wenn Sie ein Ziel unter Verwendung dieses Befehls angeben, überschreiben die von Ihnen angegebenen alle vorher angegebenen Einstellungen. Trennen Sie zum Angeben von mehreren Zielen diese durch ein Komma.

Führen Sie z. B. den folgenden Befehl aus, um die Ziele „192.0.2.1@678/targetcommunity“ und „2001:db8::1/anothercom“ zu konfigurieren:

```
snmp.set --targets 192.0.2.1@678/targetcommunity,2001:db8::1/anothercom
```

- 3 (Optional) Wenn der SNMP-Agent nicht aktiviert ist, können Sie ihn durch Ausführen des Befehls `snmp.enable` aktivieren.
- 4 (Optional) Um ein Test-Trap zu senden, um sicherzustellen, dass der Agent richtig konfiguriert ist, führen Sie den Befehl `snmp.test` aus.

Der Agent sendet eine `warmStart`-Trap an das konfigurierte Ziel.

Konfigurieren von vCenter Server für SNMP v3

Wenn Sie den SNMP-Agenten für SNMP v3 konfigurieren, unterstützt der Agent das Senden von Traps. SNMP v3 bietet zudem eine höhere Sicherheit als v1 und v2c, einschließlich der kryptographischen Authentifizierung und Verschlüsselung.

SNMP v3-Berichte werden nicht unterstützt. vCenter Server unterstützt nur Benachrichtigungen wie v1/v2c-Traps und v3-Traps mit allen Sicherheitsstufen.

Verfahren

1 Konfigurieren der SNMP-Engine-ID

Jeder SNMP v3-Agent verfügt über eine Engine-ID, die als eindeutiger Bezeichner für den Agenten dient. Die Engine-ID wird mit einer Hashing-Funktion verwendet, um lokalisierte Schlüssel für die Authentifizierung und Verschlüsselung der SNMP v3-Meldungen zu generieren.

2 Konfigurieren der SNMP-Authentifizierung und der Datenschutzprotokolle

SNMP v3 unterstützt optional die Authentifizierungs- und Datenschutzprotokolle.

3 Konfigurieren der SNMP-Benutzer

Sie können bis zu fünf Benutzer konfigurieren, die auf die SNMP v3-Informationen zugreifen können. Benutzernamen dürfen nicht länger als 32 Zeichen sein.

4 Konfigurieren der SNMP v3-Ziele

Konfigurieren Sie SNMP v3-Ziele, damit der SNMP-Agent SNMP v3-Traps senden kann.

Konfigurieren der SNMP-Engine-ID

Jeder SNMP v3-Agent verfügt über eine Engine-ID, die als eindeutiger Bezeichner für den Agenten dient. Die Engine-ID wird mit einer Hashing-Funktion verwendet, um lokalisierte Schlüssel für die Authentifizierung und Verschlüsselung der SNMP v3-Meldungen zu generieren.

Wenn Sie keine Engine-ID angeben, bevor Sie den SNMP-Agenten aktivieren, wird eine Engine-ID generiert, wenn Sie den eigenständigen SNMP-Agenten aktivieren.

Verfahren

- 1 Greifen Sie auf die Appliance-Shell zu und melden Sie sich als Benutzer mit Administrator- oder Superadministratorrolle an.

Der Standardbenutzer mit der Superadministratorrolle ist „root“.

- 2 Führen Sie den `snmp.set --engineid`-Befehl aus, um das Ziel zu konfigurieren.

Führen Sie beispielsweise folgenden Befehl aus:

```
snmp.set --engineid 80001adc802417e202b8613f5400000000
```

Hier ist „80001adc802417e202b8613f5400000000“ die ID, eine hexadezimale Zeichenfolgen mit einer Länge von 5 bis 32 Zeichen.

Konfigurieren der SNMP-Authentifizierung und der Datenschutzprotokolle

SNMP v3 unterstützt optional die Authentifizierungs- und Datenschutzprotokolle.

Die Authentifizierung dient dem Sicherstellen der Identität der Benutzer. Der Datenschutz ermöglicht die Verschlüsselung von SNMP v3-Nachrichten, um die Vertraulichkeit der Daten sicherzustellen. Die Datenschutzprotokolle bieten ein höheres Maß an Sicherheit als SNMP v1 und v2c, die dazu Community-Strings verwenden.

Sowohl die Authentifizierung als auch der Datenschutz sind optional. Allerdings müssen Sie die Authentifizierung aktivieren, um den Datenschutz aktivieren zu können.

Die Authentifizierungs- und Datenschutzprotokolle von SNMP v3 sind lizenzierte vSphere-Funktionen und stehen in einigen vSphere-Editionen möglicherweise nicht zur Verfügung.

Verfahren

- 1 Greifen Sie auf die Appliance-Shell zu und melden Sie sich als Benutzer mit Administrator- oder Superadministratorrolle an.

Der Standardbenutzer mit der Superadministratorrolle ist „root“.

- 2 (Optional) Führen Sie den `snmp.set --authentication`-Befehl aus, um die Authentifizierung zu konfigurieren.

Führen Sie beispielsweise folgenden Befehl aus:

```
snmp.set --authentication protocol
```

Hier muss *protocol* entweder **none** (keine Authentifizierung), **SHA1** oder **MD5** sein.

- 3 (Optional) Führen Sie den `snmp.set --privacy`-Befehl aus, um das Datenschutzprotokoll zu konfigurieren.

Führen Sie beispielsweise folgenden Befehl aus:

```
snmp.set --privacy protocol
```

Hier muss *protocol* entweder **none** (kein Datenschutz) oder **AES128** sein.

Konfigurieren der SNMP-Benutzer

Sie können bis zu fünf Benutzer konfigurieren, die auf die SNMP v3-Informationen zugreifen können. Benutzernamen dürfen nicht länger als 32 Zeichen sein.

Im Rahmen der Konfiguration eines Benutzers generieren Sie Hash-Werte für die Authentifizierung und den Datenschutz auf Basis der Kennwörter des Benutzers für die Authentifizierung und den Datenschutz und der Engine-ID des SNMP-Agenten. Wenn Sie die Engine-ID, das Authentifizierungsprotokoll oder das Datenschutzprotokoll nach dem Konfigurieren der Benutzer ändern, sind die Benutzer nicht mehr gültig und müssen neu konfiguriert werden.

Voraussetzungen

- Vergewissern Sie sich, dass Sie die Authentifizierungs- und Datenschutzprotokolle konfiguriert haben, bevor Sie Benutzer konfigurieren.

- Prüfen Sie, ob Sie die Authentifizierungs- und Datenschutzkennwörter für jeden Benutzer kennen, den Sie konfigurieren möchten. Kennwörter müssen mindestens acht Zeichen lang sein. Speichern Sie diese Kennwörter in Dateien auf dem Hostsystem.

Verfahren

- 1 Greifen Sie auf die Appliance-Shell zu und melden Sie sich als Benutzer mit Administrator- oder Superadministratorrolle an.

Der Standardbenutzer mit der Superadministratorrolle ist „root“.

- 2 Wenn Sie Authentifizierung oder Datenschutz verwenden, rufen Sie die Hash-Werte für Authentifizierung und Datenschutz für den Benutzer ab, indem Sie den Befehl `snmp.hash --auth_hash --priv_hash` ausführen.

Führen Sie beispielsweise folgenden Befehl aus:

```
snmp.hash --auth_hash secret1 --priv_hash secret2
```

Hier ist *secret1* der Pfad zu der Datei, die das Kennwort für die Benutzerauthentifizierung enthält, und *secret2* der Pfad zu der Datei, die das Kennwort für den Datenschutz des Benutzers enthält. Alternativ dazu können Sie das Flag `--raw_secret` angeben und den booleschen Parameter auf *true* setzen.

Die Hash-Werte für die Authentifizierung und den Datenschutz werden angezeigt.

- 3 Konfigurieren Sie den Benutzer, indem Sie `snmp.set --user` ausführen.

Führen Sie beispielsweise folgenden Befehl aus:

```
snmp.set --user userid/authhash/privhash/security
```

Der Befehl umfasst die folgenden Parameter.

| Parameter | Beschreibung |
|-----------------|---|
| <i>userid</i> | Ersetzen Sie diesen Platzhalter durch den Benutzernamen. |
| <i>authhash</i> | Ersetzen Sie diesen Platzhalter durch den Hash-Wert für die Authentifizierung. |
| <i>privhash</i> | Ersetzen Sie diesen Platzhalter durch den Hash-Wert für den Datenschutz. |
| <i>security</i> | Ersetzen Sie dies durch die Stufe der für diesen Benutzer aktivierten Sicherheit, die auth (nur für Authentifizierung), priv (für Authentifizierung und Datenschutz) oder none (keine Authentifizierung und kein Datenschutz) sein kann. |

Konfigurieren der SNMP v3-Ziele

Konfigurieren Sie SNMP v3-Ziele, damit der SNMP-Agent SNMP v3-Traps senden kann.

Sie können zusätzlich zu einem Maximum von drei SNMP v1- oder v2c-Zielen maximal bis zu drei SNMP v3-Ziele konfigurieren.

Um ein Ziel zu konfigurieren, müssen Sie Folgendes angeben: einen Hostnamen oder eine IP-Adresse des Systems, das die Traps empfängt, einen Benutzernamen, eine Sicherheitsstufe und ob Traps gesendet werden sollen. Die Sicherheitsstufe kann **none** (keine Sicherheit), **auth** (nur Authentifizierung) oder **priv** (Authentifizierung und Datenschutz) sein.

Verfahren

- 1 Greifen Sie auf die Appliance-Shell zu und melden Sie sich als Benutzer mit Administrator- oder Superadministratorrolle an.

Der Standardbenutzer mit der Superadministratorrolle ist „root“.

- 2 Führen Sie den Befehl `snmp.set --v3targets` aus, um das SNMP v3-Ziel einzurichten.

Führen Sie beispielsweise folgenden Befehl aus:

```
snmp.set --v3targets hostname@port/userid/secLevel/trap
```

Der Befehl umfasst die folgenden Parameter.

| Parameter | Beschreibung |
|-----------------|--|
| <i>hostname</i> | Ersetzen Sie diesen Platzhalter durch den Hostnamen oder die IP-Adresse des Verwaltungssystems, das die Traps erhält. |
| <i>port</i> | Ersetzen Sie diesen Platzhalter durch den Port des Verwaltungssystems, das die Traps erhält. Wenn Sie keinen Port angeben, wird der Standardport 161 verwendet. |
| <i>userid</i> | Ersetzen Sie „Benutzer-ID“ durch den Benutzernamen. |
| <i>secLevel</i> | Ersetzen Sie diesen Platzhalter entweder durch none , auth oder priv , um die Ebene der Authentifizierung und des Datenschutzes anzugeben, die Sie konfiguriert haben. Verwenden Sie auth , wenn Sie nur die Authentifizierung konfiguriert haben, priv , wenn Sie die Authentifizierung und den Datenschutz konfiguriert haben, und none , wenn Sie keine der beiden Optionen konfiguriert haben. |

- 3 (Optional) Wenn der SNMP-Agent nicht aktiviert ist, können Sie ihn durch Ausführen des Befehls `snmp.enable` aktivieren.
- 4 (Optional) Um ein Test-Trap zu senden, um sicherzustellen, dass der Agent richtig konfiguriert ist, führen Sie den Befehl `snmp.test` aus.

Der Agent sendet eine `warmStart`-Trap an das konfigurierte Ziel.

Konfigurieren des SNMP-Agenten zum Filtern von Benachrichtigungen

Sie können den eingebetteten SNMP-Agenten für vCenter Server zum Herausfiltern von Benachrichtigungen konfigurieren, wenn Sie nicht möchten, dass Ihre SNMP-Verwaltungssoftware diese Benachrichtigungen erhält.

Verfahren

- 1 Greifen Sie auf die Appliance-Shell zu und melden Sie sich als Benutzer mit Administrator- oder Superadministratorrolle an.

Der Standardbenutzer mit der Superadministratorrolle ist „root“.

- 2 Führen Sie den `snmp.set --notraps`-Befehl aus, um Traps zu filtern.

- Um bestimmte Traps zu filtern, führen Sie folgenden Befehl aus:

```
snmp.set --notraps oid_list
```

Hier ist *oid_list* eine kommagetrennte Liste von Objekt-IDs für die zu filternden Traps. Diese Liste ersetzt alle Objekt-IDs, die zuvor mit diesem Befehl angegeben wurden.

- Um alle Trap-Filter zu löschen, führen Sie folgenden Befehl aus:

```
snmp.set --notraps reset
```

- 3 (Optional) Wenn der SNMP-Agent nicht aktiviert ist, können Sie ihn durch Ausführen des Befehls `snmp.enable` aktivieren.

Ergebnisse

Die durch die angegebenen Objekt-IDs identifizierten Traps werden aus der Ausgabe des SNMP-Agenten herausgefiltert und nicht an die SNMP-Verwaltungssoftware weitergeleitet.

Konfiguration der Clientsoftware für die SNMP-Verwaltung

Nachdem Sie vCenter Server für das Senden von Traps konfiguriert haben, müssen Sie Ihre Clientsoftware für die Verwaltung konfigurieren, um diese Traps empfangen und interpretieren zu können.

Sie müssen zum Konfigurieren Ihrer Clientsoftware für die Verwaltung die Communitys für das verwaltete Gerät angeben, die Porteinstellungen konfigurieren und die MIB-Dateien von VMware laden. Spezielle Anweisungen für diese Schritte finden Sie in der Dokumentation Ihres Verwaltungssystems.

Voraussetzungen

Laden Sie die VMware MIB-Dateien von <https://kb.vmware.com/s/article/1013445> herunter

Verfahren

- 1 Geben Sie in Ihrer Verwaltungssoftware die vCenter Server-Instanz als SNMP-basiertes, verwaltetes Gerät an.
- 2 Wenn Sie SNMP v1 oder v2c verwenden, richten Sie die entsprechenden Community-Namen in der Verwaltungssoftware ein.

Diese Namen müssen mit den für den SNMP-Agenten auf vCenter Server eingerichteten Communitys übereinstimmen.

- 3 Wenn Sie SNMP v3 verwenden, konfigurieren Sie Benutzer sowie Authentifizierungs- und Datenschutzprotokolle, damit diese den auf vCenter Server konfigurierten Protokollen entsprechen.
- 4 Wenn Sie den SNMP-Agenten zum Senden von Traps an einen Port auf dem Verwaltungssystem konfiguriert haben, der nicht der Standard-UDP-Port 162 ist, konfigurieren Sie die Clientverwaltungssoftware zum Überwachen des von Ihnen konfigurierten Ports.
- 5 Laden Sie die VMware-MIBs in die Verwaltungssoftware, damit die symbolischen Namen für die vCenter Server-Variablen angezeigt werden können.

Um Lookup-Fehler zu vermeiden, laden Sie diese MIB-Dateien in der folgenden Reihenfolge, bevor Sie weitere MIB-Dateien laden:

- a VMWARE-ROOT-MIB.mib
- b VMWARE-TC-MIB.mib
- c VMWARE-PRODUCTS-MIB.mib

Ergebnisse

Die Verwaltungssoftware kann jetzt Traps von vCenter Server empfangen und interpretieren.

Zurücksetzen der SNMP-Einstellungen auf die Standardeinstellungen

Die SNMP-Einstellungen können auf die Standardeinstellungen zurückgesetzt werden. Auch die Werte von Argumenten können auf die entsprechenden Standardwerte zurückgesetzt werden.

Sie können ein bestimmtes Argument, z. B. Communitys oder Ziele, zurücksetzen. Sie können auch die SNMP-Konfiguration auf die Standardeinstellungen zurücksetzen.

Verfahren

- 1 Greifen Sie auf die Appliance-Shell zu und melden Sie sich als Benutzer mit Administrator- oder Superadministratorrolle an.

Der Standardbenutzer mit der Superadministratorrolle ist „root“.

- 2 Zum Zurücksetzen bestimmter Argumente führen Sie den Befehl `snmp.set --arguments reset` aus.

Um beispielsweise die konfigurierten Communitys zurückzusetzen, verwenden Sie folgenden Befehl:

```
snmp.set --communities reset
```

- 3 Um die gesamte SNMP-Konfiguration auf die Standardeinstellungen zurückzusetzen, führen Sie den Befehl `snmp.reset` aus.

Konfigurieren der Einstellungen für die Uhrzeitsynchronisierung in vCenter Server

Sie können die Einstellungen für die Uhrzeitsynchronisierung in vCenter Server nach der Bereitstellung ändern.

Wenn Sie vCenter Server bereitstellen, können Sie für die Uhrzeitsynchronisierung entweder einen NTP-Server oder VMware Tools auswählen. Wenn sich die Uhrzeiteinstellungen in Ihrem vSphere-Netzwerk ändern, können Sie vCenter Server bearbeiten und die Uhrzeitsynchronisierungseinstellungen anhand der Befehle in der Appliance-Shell konfigurieren.

Wenn Sie die regelmäßige Uhrzeitsynchronisierung aktivieren, legt VMware Tools die Uhrzeit des Gastbetriebssystems auf die Uhrzeit des Hostcomputers fest.

Nach der Uhrzeitsynchronisierung prüft VMware Tools minütlich, ob die Uhrzeit auf dem Gastbetriebssystem mit der Uhrzeit auf dem Host übereinstimmt. Ist dies nicht der Fall, wird die Uhrzeit auf dem Gastbetriebssystem wieder mit der Uhrzeit auf dem Host synchronisiert.

Native Uhrzeitsynchronisierungssoftware wie Network Time Protocol (NTP) ist normalerweise genauer als die regelmäßige Uhrzeitsynchronisierung von VMware Tools und daher vorzuziehen. Sie können nur eine Form der regelmäßigen Uhrzeitsynchronisierung in vCenter Server verwenden. Wenn Sie sich für die native Uhrzeitsynchronisierungssoftware entscheiden, wird die regelmäßigen Uhrzeitsynchronisierung durch VMware Tools für vCenter Server deaktiviert und umgekehrt.

Verwenden der Uhrzeitsynchronisierung von VMware Tools

Sie können vCenter Server für die Verwendung der Uhrzeitsynchronisierung von VMware Tools einrichten.

Verfahren

- 1 Greifen Sie auf die Appliance-Shell zu und melden Sie sich als Benutzer mit Administrator- oder Superadministratorrolle an.

Der Standardbenutzer mit der Superadministratorrolle ist „root“.

- 2 Führen Sie den Befehl aus, um auf VMware Tools basierte Uhrzeitsynchronisierung zu aktivieren.

```
timesync.set --mode host
```

- 3 (Optional) Führen Sie den Befehl aus, um zu überprüfen, ob Sie die Uhrzeitsynchronisierung von VMware Tools erfolgreich angewendet haben.

```
timesync.get
```

Der Befehl gibt zurück, dass sich die Uhrzeitsynchronisierung im Host-Modus befindet.

Ergebnisse

Die Uhrzeit der Appliance wird mit der Uhrzeit des ESXi-Hosts synchronisiert.

Hinzufügen oder Ersetzen von NTP-Servern in der vCenter Server-Konfiguration

Wenn Sie die vCenter Server für die Verwendung der NTP-basierten Uhrzeitsynchronisierung einrichten möchten, müssen Sie zuerst die NTP-Server zur vCenter Server-Konfiguration hinzufügen.

Verfahren

- 1 Greifen Sie auf die Appliance-Shell zu und melden Sie sich als Benutzer mit Administrator- oder Superadministratorrolle an.

Der Standardbenutzer mit der Superadministratorrolle ist „root“.

- 2 Fügen Sie der vCenter Server-Konfiguration NTP-Server hinzu, indem Sie den folgenden `ntp.set`-Befehl ausführen.

```
ntp.set --servers IP-addresses-or-host-names
```

In diesem Befehl ist *IP-addresses-or-host-names* eine kommagetrennte Liste der IP-Adressen oder Hostnamen der NTP-Server.

Dieser Befehl entfernt die aktuellen NTP-Server (sofern vorhanden) und fügt der Konfiguration die neuen NTP-Server hinzu. Wenn die Uhrzeitsynchronisierung auf einem NTP-Server basiert, wird der NTP-Daemon neu gestartet, um die neuen NTP-Server erneut zu laden. Andernfalls ersetzt dieser Befehl die aktuellen NTP-Server in der NTP-Konfiguration durch die neuen NTP-Server, die Sie angeben.

- 3 (Optional) Führen Sie den folgenden Befehl aus, um zu überprüfen, ob Sie die neuen NTP-Konfigurationseinstellungen erfolgreich angewendet haben.

```
ntp.get
```

Der Befehl gibt eine durch Leerzeichen getrennte Liste der Server zurück, die für die NTP-Synchronisierung konfiguriert sind. Bei aktivierter NTP-Synchronisierung gibt der Befehl zurück, dass die NTP-Konfiguration den Status „Erreichbar“ aufweist. Falls die NTP-Synchronisierung deaktiviert ist, gibt der Befehl zurück, dass die NTP-Konfiguration den Status „Nicht erreichbar“ aufweist.

- 4 (Optional) Führen Sie den folgenden Befehl aus, um zu überprüfen, ob der NTP-Server erreichbar ist.

```
ntp.test --servers IP-addresses-or-host-names
```

Der Befehl gibt den Status der NTP-Server zurück.

Nächste Schritte

Bei deaktivierter NTP-Synchronisierung können Sie die Zeitsynchronisierungseinstellungen auf dem vCenter Server auf Basis eines NTP-Servers konfigurieren. Weitere Informationen hierzu finden Sie unter [Synchronisieren der Uhrzeit in vCenter Server mit einem NTP-Server](#).

Synchronisieren der Uhrzeit in vCenter Server mit einem NTP-Server

Sie können die Uhrzeitsynchronisierungseinstellungen in vCenter Server so konfigurieren, dass sie auf einem NTP-Server basieren.

Voraussetzungen

Richten Sie in der vCenter Server-Konfiguration mindestens einen NTP-Server (Network Time Protocol) ein. Weitere Informationen hierzu finden Sie unter [Hinzufügen oder Ersetzen von NTP-Servern in der vCenter Server-Konfiguration](#).

Verfahren

- 1 Greifen Sie auf die Appliance-Shell zu und melden Sie sich als Benutzer mit Administrator- oder Superadministratorrolle an.

Der Standardbenutzer mit der Superadministratorrolle ist „root“.

- 2 Führen Sie den Befehl aus, um NTP-basierte Uhrzeitsynchronisierung zu aktivieren.

```
timesync.set --mode NTP
```

- 3 (Optional) Führen Sie den Befehl aus, um zu überprüfen, ob Sie die NTP-Synchronisierung erfolgreich angewendet haben.

```
timesync.get
```

Der Befehl gibt zurück, dass sich die Uhrzeitsynchronisierung im NTP-Modus befindet.

Verwalten lokaler Benutzerkonten in vCenter Server

Wenn Sie sich bei der Appliance-Shell als Superadministrator anmelden, können Sie die lokalen Benutzerkonten in vCenter Server durch Ausführen von Befehlen in der Appliance-Shell verwalten. Der Standardbenutzer mit einer Superadministratorrolle ist „root“.

Benutzerrollen in vCenter Server

vCenter Server umfasst drei Hauptbenutzerrollen.

Die lokalen Benutzer von vCenter Server haben Berechtigungen, verschiedene Aufgaben durchzuführen. In vCenter Server sind drei Benutzerrollen verfügbar:

Operator

Lokale Benutzer mit der Operator-Benutzerrolle können die vCenter Server-Konfiguration lesen.

Administrator

Lokale Benutzer mit der Administrator-Benutzerrolle können vCenter Server konfigurieren.

Super Administrator

Lokale Benutzer mit der Super Administrator-Benutzerrolle können vCenter Server konfigurieren, die lokalen Konten verwalten und die Bash-Shell verwenden.

Abrufen einer Liste der lokalen Benutzerkonten in vCenter Server

Sie können die Liste der lokalen Benutzerkonten anzeigen, um zu entscheiden, welches Benutzerkonto über die Appliance-Shell verwaltet werden soll.

Verfahren

- 1 Greifen Sie auf die Appliance-Shell zu und melden Sie sich als Benutzer mit Superadministratorrolle an.

Der Standardbenutzer mit einer Superadministratorrolle ist „root“.

- 2 Führen Sie den Befehl `localaccounts.user.list` aus.

Eine Liste der lokalen Benutzer wird angezeigt. Die Informationen zu einem Benutzer enthalten den Benutzernamen, den Status, die Rolle, den Kennwortstatus, den vollständigen Namen und die E-Mail-Adresse.

Hinweis Die Liste der lokalen Benutzer enthält nur die lokalen Benutzer, deren Standard-Shell eine Appliance-Shell ist.

Erstellen eines lokalen Benutzerkontos in vCenter Server

Sie können ein neues lokales Benutzerkonto erstellen.

Informationen zu den Benutzerrollen erhalten Sie unter [Benutzerrollen in vCenter Server](#).

Verfahren

- 1 Greifen Sie auf die Appliance-Shell zu und melden Sie sich als Benutzer mit Superadministratorrolle an.

Der Standardbenutzer mit einer Superadministratorrolle ist „root“.

- 2 Führen Sie den Befehl `localaccounts.user.add --role --username --password` aus.

Um beispielsweise das lokale Benutzerkonto namens „test“ mit der Benutzerrolle „operator“ hinzuzufügen, verwenden Sie folgenden Befehl:

```
localaccounts.user.add --role operator --username test --password
```

Die Rolle kann **operator**, **admin** oder **superAdmin** lauten.

Sie können auch ein lokales Benutzerkonto einrichten und eine E-Mail-Adresse und den vollständigen Namen des Benutzers angeben. Um beispielsweise das lokale Benutzerkonto „test1“ mit der Benutzerrolle „operator“, dem vollständigen Namen „TestName“ und der E-Mail-Adresse „test1@mymail.com“ hinzuzufügen, verwenden Sie folgenden Befehl::

```
localaccounts.user.add --role operator --username test1 --password --fullname TestName --
email test1@mymail.com
```

Leerzeichen in vollständigen Namen sind nicht zulässig.

- 3 Geben Sie bei Aufforderung das Kennwort des neuen lokalen Benutzers ein und bestätigen Sie es.

Ergebnisse

Sie haben nun einen neuen lokalen Benutzer in der Appliance erstellt.

Aktualisieren des Kennworts eines lokalen Benutzers in vCenter Server

Sie können das Kennwort eines lokalen Benutzers in vCenter Server aus Sicherheitsgründen aktualisieren.

Verfahren

- 1 Greifen Sie auf die Appliance-Shell zu und melden Sie sich als Benutzer mit Superadministratorrolle an.

Der Standardbenutzer mit einer Superadministratorrolle ist „root“.

- 2 Führen Sie den Befehl `localaccounts.user.password.update --username user name --password aus`.

Um beispielsweise das Kennwort eines Benutzers mit dem Benutzernamen „test“ zu ändern, führen Sie den folgenden Befehl aus:

```
localaccounts.user.password.update --username test --password
```

- 3 Geben Sie ein neues Kennwort ein und bestätigen Sie es bei Aufforderung.

Aktualisieren eines lokalen Benutzerkontos in vCenter Server

Ein bestehendes lokales Benutzerkonto kann in vCenter Server aktualisiert werden.

Informationen zu den Benutzerrollen erhalten Sie unter [Benutzerrollen in vCenter Server](#).

Verfahren

- 1 Greifen Sie auf die Appliance-Shell zu und melden Sie sich als Benutzer mit Superadministratorrolle an.

Der Standardbenutzer mit einer Superadministratorrolle ist „root“.

2 Mit dem Befehl `localaccounts.user.set --username` aktualisieren Sie einen bestehenden lokalen Benutzer.

- Um die Rolle des lokalen Benutzers zu aktualisieren, verwenden Sie folgenden Befehl:

```
localaccounts.user.set --username user name --role new role
```

user name ist hierbei der Name des Benutzers, den Sie bearbeiten möchten, und *new role* die neue Rolle. Die Rolle kann **operator**, **admin** oder **superAdmin** lauten.

- Um die E-Mail-Adresse des lokalen Benutzers zu aktualisieren, verwenden Sie folgenden Befehl:

```
localaccounts.user.set --username user name --email new email address
```

user name ist hierbei der Name des Benutzers, den Sie bearbeiten möchten, und *new email address* die neue E-Mail-Adresse.

- Um den vollständigen Namen des lokalen Benutzers zu aktualisieren, verwenden Sie folgenden Befehl:

```
localaccounts.user.set --username user name --fullname new full name
```

user name ist hierbei der Name des Benutzers, den Sie bearbeiten möchten, und *new full name* der neue vollständige Name.

- Um den Status des lokalen Benutzers zu aktualisieren, verwenden Sie folgenden Befehl:

```
localaccounts.user.set --username user name --status new status
```

user name ist hierbei der Name des Benutzers, den Sie bearbeiten möchten, und *new status* der neue Status. Der Status kann entweder **disabled** (deaktiviert) oder **enabled** (aktiviert) lauten.

Löschen eines lokalen Benutzerkontos in vCenter Server

Sie können ein lokales Benutzerkonto in vCenter Server löschen.

Verfahren

- 1 Greifen Sie auf die Appliance-Shell zu und melden Sie sich als Benutzer mit Superadministratorrolle an.

Der Standardbenutzer mit einer Superadministratorrolle ist „root“.

- 2 Führen Sie den Befehl `localaccounts.user.delete --username aus`.

Um beispielsweise den Benutzer mit dem Benutzernamen „test“ zu löschen, führen Sie den folgenden Befehl aus:

```
localaccounts.user.delete --username test
```

Der Benutzer wird gelöscht.

Überwachen von Systemzustand und Statistiken in vCenter Server

Sie können den Hardwarezustand von vCenter Server mit den API-Befehlen in der Appliance-Shell überwachen. Sie können auch den Systemstatus der Update-Komponente auf Informationen zu verfügbaren Patches überwachen.

Sie können den Status von Hardwarekomponenten anzeigen, wie z. B. Arbeitsspeicher, CPU, Speicher und Netzwerk, sowie die Update-Komponente, die anzeigt, ob die Softwarepakete entsprechend der letzten Überprüfung auf verfügbare Patches aktuell sind.

Ein bestimmter Systemzustand kann durch die Farben grün, gelb, orange, rot oder grau angezeigt werden. Weitere Informationen finden Sie unter [Anzeigen des vCenter Server-Systemzustands](#).

Eine vollständige Liste der API-Befehle, die Sie zum Überwachen von Statistiken und des Status des vCenter Server-Systems verwenden können, finden Sie unter [API-Befehle in der Appliance-Shell](#).

Verfahren

- 1 Greifen Sie auf die Appliance-Shell zu und melden Sie sich an.

Der Benutzer, dessen Name zum Anmelden verwendet wird, kann ein Benutzer mit einer Operator-, Administrator- oder Superadministratorrolle sein.

- 2 Zeigen Sie den Systemzustand einer bestimmten Komponente an.

- Führen Sie zum Anzeigen des Arbeitsspeicherzustands in vCenter Server den Befehl `mem.health.get aus`.
- Führen Sie zum Anzeigen des Speicherzustands in vCenter Server den Befehl `storage.health.get aus`.
- Führen Sie zum Anzeigen des Auslagerungszustands in vCenter Server den Befehl `swap.health.get aus`.

- Führen Sie zum Anzeigen des Zustands der Update-Komponente in vCenter Server den Befehl `softwarepackages.health.get` aus.

Wichtig Falls Sie keine regelmäßigen Prüfungen auf verfügbare Patches durchführen, ist der Systemzustand der Aktualisierungskomponente möglicherweise nicht mehr aktuell. Informationen zur Prüfung auf Patches für die vCenter Server und zur Aktivierung von automatischen Prüfungen auf Patches für die vCenter Server finden Sie unter *vSphere-Upgrade*.

- Führen Sie zum Anzeigen des Gesamtstatus des vCenter Server-Systems den Befehl `health.system.get` aus.

- 3 Führen Sie zum Anzeigen der Statistiken einer bestimmten Hardwarekomponente den jeweiligen Befehl aus.

Beispiel: Zum Anzeigen der Speicherstatistik für jede logische Festplatte führen Sie den Befehl `storage.stats.list` aus.

Verwenden des `vimtop`-Plug-In zum Überwachen der Ressourcennutzung von Diensten

Sie können das `vimtop`-Dienstprogramm-Plug-In verwenden, um vSphere-Dienste zu überwachen, die in der vCenter Server ausgeführt werden.

`vimtop` ist ein ähnliches Tool wie `esxtop`, das in der Umgebung der vCenter Server ausgeführt wird. Wenn Sie die textbasierte Schnittstelle von `vimtop` in der Appliance-Shell verwenden, können Sie allgemeine Informationen über die vCenter Server sowie eine Liste der vSphere-Dienste und deren Ressourcennutzung anzeigen.

- [Überwachen von Diensten mit `vimtop` im interaktiven Modus](#)

Mit dem `vimtop`-Plug-In können Sie Dienste in Echtzeit überwachen.

- [Befehlszeilenoptionen im interaktiven Modus](#)

Sie können verschiedene Befehlszeilenoptionen verwenden, wenn Sie den Befehl `vimtop` für den Zugriff auf das Plug-In im interaktiven Modus ausführen.

- [Einzeltastenbefehle im interaktiven Modus für `vimtop`](#)

Bei der Ausführung im interaktiven Modus erkennt `vimtop` mehrere Einzeltastenbefehle.

Überwachen von Diensten mit `vimtop` im interaktiven Modus

Mit dem `vimtop`-Plug-In können Sie Dienste in Echtzeit überwachen.

Die Standardansicht des interaktiven `vimtop`-Modus besteht aus den Übersichtstabellen und der Haupttabelle. Sie können im interaktiven Modus Eintastenbefehle verwenden, um die Ansicht von Prozessen zu Festplatten oder dem Netzwerk zu wechseln.

Verfahren

- 1 Melden Sie sich über eine SSH-Clientanwendung bei der Shell der vCenter Server an.
- 2 Führen Sie den Befehl `vimtop` aus, um im interaktiven Modus auf das Plug-In zuzugreifen.

Befehlszeilenoptionen im interaktiven Modus

Sie können verschiedene Befehlszeilenoptionen verwenden, wenn Sie den Befehl `vimtop` für den Zugriff auf das Plug-In im interaktiven Modus ausführen.

Tabelle 4-4. Befehlszeilenoptionen im interaktiven Modus

| Option | Beschreibung |
|-------------------------------------|---|
| <code>-h</code> | Gibt Hilfe für die Befehlszeilenoptionen von <code>vimtop</code> aus. |
| <code>-v</code> | Gibt die Versionsnummer von <code>vimtop</code> aus. |
| <code>-c <i>Dateiname</i></code> | Lädt eine benutzerdefinierte <code>vimtop</code> -Konfigurationsdatei. Wenn die Option <code>-c</code> nicht verwendet wird, lautet die Standardkonfigurationsdatei <code>/root/vimtop/vimtop.xml</code> . Mit dem interaktiven Einzeltastenbefehl <code>w</code> können Sie eine eigene Konfigurationsdatei mit einem anderen Dateinamen und Pfad erstellen. |
| <code>-n <i>Anzahl</i></code> | Legt die Anzahl der durchgeführten Iterationen fest, bevor <code>vimtop</code> den interaktiven Modus verlässt. <code>vimtop</code> aktualisiert die Anzeige <i>Anzahl</i> Mal und wird geschlossen. Der Standardwert ist 10000. |
| <code>-p / -d<i>Sekunden</i></code> | Legt den Aktualisierungszeitraum in Sekunden fest. |

Einzeltastenbefehle im interaktiven Modus für vimtop

Bei der Ausführung im interaktiven Modus erkennt `vimtop` mehrere Einzeltastenbefehle.

Alle Bereiche im interaktiven Modus erkennen die in der folgenden Tabelle aufgeführten Befehle.

Tabelle 4-5. Einzeltastenbefehle im interaktiven Modus

| Tastennamen | Beschreibung |
|----------------|--|
| <code>h</code> | Zeigt ein Hilfemenü für den aktuellen Fensterbereich mit einer Zusammenfassung der Befehle sowie den Status des sicheren Modus. |
| <code>i</code> | Blendet die oberste Zeile im Übersichtsfensterbereich des <code>vimtop</code> -Plug-In ein oder aus. |
| <code>t</code> | Blendet den Abschnitt „Aufgaben“ ein oder aus, der Informationen im Übersichtsfensterbereich über die derzeit in der vCenter Server-Instanz ausgeführten Aufgaben anzeigt. |
| <code>m</code> | Blendet den Abschnitt „Arbeitsspeicher“ im Übersichtsfensterbereich ein oder aus. |
| <code>f</code> | Blendet den Abschnitt „CPU“ ein oder aus, der im Übersichtsfensterbereich Informationen über alle verfügbare CPUs anzeigt. |
| <code>g</code> | Blendet den Abschnitt „CPUs“ ein oder aus, der im Übersichtsfensterbereich Informationen über die obersten 4 physischen CPUs anzeigt. |
| Leertaste | Aktualisiert sofort den aktuellen Fensterbereich. |

Tabelle 4-5. Einzeltastenbefehle im interaktiven Modus (Fortsetzung)

| Tastennamen | Beschreibung |
|-----------------------------|--|
| a | Hält die angezeigten Informationen über die Ressourcennutzung der Dienste in den aktuellen Fensterbereichen an. |
| r | Aktualisiert die angezeigten Informationen über die Ressourcennutzung der Dienste in den aktuellen Fensterbereichen. |
| s | Legt das Aktualisierungsintervall fest. |
| q | Beendet den interaktiven Modus des <code>vimtop</code> -Plug-Ins. |
| k | Zeigt die Ansicht „Festplatten“ im Hauptfensterbereich an. |
| ein | Wechselt im Hauptfensterbereich in die Ansicht „Netzwerk“. |
| Esc | Löscht die Auswahl oder kehrt zur Ansicht für Prozesse im Hauptfensterbereich zurück. |
| Eingabetaste | Wählt einen Dienst aus, um zusätzliche Details anzuzeigen. |
| n | Blendet die Namen der Kopfzeilen im Hauptfensterbereich ein oder aus. |
| u | Blendet die Maßeinheiten der Kopfzeilen im Hauptfensterbereich ein oder aus. |
| Pfeil nach links, rechts | Wählt Spalten aus. |
| Pfeil nach oben, unten | Wählt Zeilen aus. |
| <,> | Verschiebt eine ausgewählte Spalte. |
| Löschen | Entfernt die ausgewählte Spalte. |
| c | Fügt der aktuellen Ansicht im Hauptfensterbereich eine Spalte hinzu. Mit der Leertaste werden Spalten der angezeigten Liste hinzugefügt oder daraus entfernt. |
| a | Sortiert die ausgewählte Spalte in aufsteigender Reihenfolge. |
| d | Sortiert die ausgewählte Spalte in absteigender Reihenfolge. |
| z | Löscht die Sortierreihenfolge für alle Spalten. |
| l | Legt die Breite für die ausgewählte Spalte fest. |
| B | Setzt die Spaltenbreiten auf ihre Standardwerte zurück. |
| + | Erweitert das ausgewählte Element. |
| - | Reduziert das ausgewählte Element. |
| w | Schreibt die aktuelle Einrichtung in eine <code>vimtop</code> -Konfigurationsdatei. Der Standarddateiname ist derjenige, der von der Option <code>-c</code> angegeben wird, bzw. <code>/root/vimtop/vimtop.xml</code> , wenn die Option <code>-c</code> nicht verwendet wird. Sie können auch einen anderen Dateinamen an der Befehlszeileneingabe eingeben, die vom Befehl <code>w</code> generiert wird. |

Verwenden der Benutzerschnittstelle der direkten Konsole zur Konfiguration von vCenter Server

5

Nach der Bereitstellung von vCenter Server können Sie die Netzwerkeinstellungen neu konfigurieren und den Zugriff auf die Bash-Shell zur Fehlerbehebung aktivieren. Für den Zugriff auf die Benutzerschnittstelle der direkten Konsole (Direct Console User Interface, DCUI) müssen Sie sich als Root-Benutzer anmelden.

Die Startseite der DCUI enthält einen Link zum Support-Paket der vCenter Server. Der Link zum Support-Paket weist folgendes Format auf: <https://Appliance-Hostname:443/appliance/support-bundle>.

Dieses Kapitel enthält die folgenden Themen:

- Anmelden bei der Benutzerschnittstelle der direkten Konsole (DCUI)
- Ändern des Kennworts des Root-Benutzers
- Konfigurieren des Verwaltungsnetzwerks von vCenter Server
- Neustarten des Verwaltungsnetzwerks von vCenter Server
- Aktivieren des Zugriffs auf die Bash-Shell
- Zugriff auf die Bash-Shell zur Fehlerbehebung
- Exportieren eines vCenter Server-Support-Pakets zwecks Fehlerbehebung

Anmelden bei der Benutzerschnittstelle der direkten Konsole (DCUI)

Die Benutzerschnittstelle der direkten Konsole (Direct Console User Interface, DCUI) ermöglicht mithilfe textbasierter Menüs die lokale Interaktion mit vCenter Server.

Verfahren

- 1 Navigieren Sie im vSphere Client zum Host und klicken Sie auf **Konfigurieren > Dienste**. Bestätigen Sie, dass die Dienste für SSH und die Benutzeroberfläche der direkten Konsole aktiv sind.
- 2 Öffnen Sie einen SSH-Client und stellen Sie eine Verbindung zum vCenter Server her.

- 3 Melden Sie sich mit dem Root-Konto an.
- 4 Geben Sie **DCUI** ein, um die Benutzeroberfläche der direkten Konsole zu starten.
- 5 Klicken Sie in das Konsolenfenster und drücken Sie F2, um das System anzupassen.
- 6 Geben Sie das Kennwort des Root-Benutzers ein und drücken Sie die Eingabetaste.

Wichtig Nachdem Sie das dritte Mal ungültige Anmeldedaten eingegeben haben, wird das Root-Konto fünf Minuten lang gesperrt.

Ergebnisse

Sie haben sich bei der DCUI angemeldet. Sie können das Kennwort des Root-Benutzers ändern, die Netzwerkeinstellungen bearbeiten und den Zugriff auf die Bash-Shell der vCenter Server Appliance aktivieren.

Ändern des Kennworts des Root-Benutzers

Sie können das Kennwort des Root-Benutzers ändern, um den nicht autorisierten Zugriff auf die Benutzerschnittstelle der direkten Konsole (Direct Console User Interface, DCUI) der vCenter Server zu verhindern.

Das Standardkennwort des Root-Benutzers ist für die vCenter Server-Instanz das Kennwort, das Sie während der Bereitstellung eingeben.

Wichtig Das Kennwort für das Root-Konto von vCenter Server läuft nach 90 Tagen ab. Sie können die Ablaufzeit für ein Konto ändern, indem Sie sich als Root-Benutzer bei der vCenter Server-Bash-Shell anmelden und `chage -M number_of_days -W warning_until_expiration user_name` ausführen. Um die Ablaufzeit des Root-Kennworts auf unendlich zu verlängern, führen Sie den Befehl `chage -M -1 -E -1 root` aus.

Verfahren

- 1 Melden Sie sich bei der Benutzerschnittstelle der direkten Konsole an.
- 2 Wählen Sie **Kennwort konfigurieren** aus und drücken Sie die Eingabetaste.
- 3 Geben Sie das alte Kennwort des Root-Benutzers ein und drücken Sie die Eingabetaste.
- 4 Richten Sie das neue Kennwort ein und drücken Sie die Eingabetaste.
- 5 Drücken Sie die Esc-Taste wiederholt, bis Sie zurück zum Hauptmenü der Benutzerschnittstelle der direkten Konsole gelangt sind.

Ergebnisse

Damit haben Sie das Kennwort des Root-Benutzers der Appliance geändert.

Konfigurieren des Verwaltungsnetzwerks von vCenter Server

Die vCenter Server-Instanz kann Netzwerkeinstellungen von einem DHCP-Server abrufen oder statische IP-Adressen verwenden. Die Netzwerkeinstellungen von vCenter Server können Sie über die Benutzerschnittstelle der direkten Konsole (Direct Console User Interface, DCUI) ändern. Sie können die IPv4-, IPv6- und DNS-Konfiguration ändern.

Voraussetzungen

Um die IP-Adresse der vCenter Server-Instanz zu ändern, vergewissern Sie sich, dass der Systemname ein FQDN ist. Wenn Sie bei der Bereitstellung eine IP-Adresse als einen Systemnamen festlegen, können Sie die IP-Adresse nach der Bereitstellung nicht mehr ändern. Der Systemname wird immer als primärer Netzwerkbezeichner verwendet.

Verfahren

- 1 Melden Sie sich bei der Benutzerschnittstelle der direkten Konsole von vCenter Server an.
- 2 Wählen Sie **Verwaltungsnetzwerk konfigurieren** und drücken Sie die Eingabetaste.
- 3 Ändern Sie die IPv4-Einstellungen über **IP-Konfiguration**.

| Option | Beschreibung |
|--|--|
| Dynamische IP-Adresse und Netzwerkkonfiguration verwenden | Ruft Netzwerkeinstellungen von einem DHCP-Server ab, falls ein solcher Server in Ihrem Netzwerk verfügbar ist. |
| Statische IP-Adresse und Netzwerkkonfiguration festlegen | Legt die statische Netzwerkkonfiguration fest. |

- 4 Ändern Sie die IPv6-Einstellungen über **IPv6-Konfiguration**.

| Option | Beschreibung |
|---|---|
| IPv6 aktivieren | Aktiviert oder deaktiviert IPv6 |
| Statusorientierte DHCP-Konfiguration verwenden | Verwendet einen DHCP-Server zum Abrufen von IPv6-Adressen und Netzwerkeinstellungen. |
| Statusfreie ICMP-Konfiguration verwenden | Verwendet eine SLAAC (Stateless Address Autoconfiguration) zum Abrufen von IPv6-Adressen und Netzwerkeinstellungen. |

- 5 Ändern Sie die DNS-Einstellungen über **DNS-Konfiguration**.

| Option | Beschreibung |
|---|--|
| DNS-Serveradresse und Hostname automatisch abrufen | Ruft die DNS-Serveradresse und den Hostnamen automatisch ab. Verwenden Sie diese Option, wenn die IP-Einstellungen automatisch von einem DHCP-Server abgerufen werden. |
| Folgende DNS-Serveradresse und folgenden Hostnamen verwenden | Legt die statische IP-Adresse und den Hostnamen für den DNS-Server fest. |

- 6 Legen Sie benutzerdefinierte DNS-Suffixe über **Benutzerdefinierte DNS-Suffixe** fest.
Falls Sie keine Suffixe angeben, wird ein Standardsuffix vom Namen der lokalen Domäne abgeleitet.
- 7 Drücken Sie die Esc-Taste wiederholt, bis Sie zurück zum Hauptmenü der Benutzerschnittstelle der direkten Konsole gelangt sind.

Neustarten des Verwaltungsnetzwerks von vCenter Server

Starten Sie das Verwaltungsnetzwerk von vCenter Server neu, um die Netzwerkverbindung wiederherzustellen.

Verfahren

- 1 Melden Sie sich bei der Benutzerschnittstelle der direkten Konsole (Direct Console User Interface, DCUI) von vCenter Server an.
- 2 Wählen Sie **Verwaltungsnetzwerk neu starten** aus und drücken Sie die Eingabetaste.
- 3 Drücken Sie F11.

Aktivieren des Zugriffs auf die Bash-Shell

Mit der Benutzerschnittstelle der direkten Konsole (Direct Console User Interface, DCUI) können Sie den lokalen Zugriff und den Remotezugriff auf die Bash-Shell aktivieren. Wenn der Bash-Shell-Zugriff über die DCUI aktiviert wird, ist der Zugriff 3.600 Sekunden lang möglich.

Verfahren

- 1 Melden Sie sich bei der Benutzerschnittstelle der direkten Konsole (Direct Console User Interface, DCUI) von vCenter Server an.
- 2 Wählen Sie **Fehlerbehebungsoptionen** und drücken Sie die Eingabetaste.
- 3 Wählen Sie im Menü „Optionen für den Fehlerbehebungsmodus“ entweder Bash-Shell oder SSH aus.
- 4 Drücken Sie die Eingabetaste, um den Dienst zu starten.
- 5 Drücken Sie die Esc-Taste wiederholt, bis Sie zurück zum Hauptmenü der Benutzerschnittstelle der direkten Konsole gelangt sind.

Nächste Schritte

Greifen Sie auf die Bash-Shell der vCenter Server zwecks Fehlerbehebung zu.

Zugriff auf die Bash-Shell zur Fehlerbehebung

Melden Sie sich bei der Bash-Shell nur zur Fehlerbehebung an.

Verfahren

- 1 Greifen Sie mithilfe einer der folgenden Methoden auf die Shell zu.
 - Drücken Sie Alt+F1, wenn Sie direkten Zugriff auf die vCenter Server-Instanz haben.
 - Wenn Sie eine Remoteverbindung herstellen möchten, verwenden Sie SSH oder eine andere Remote-Konsolenverbindung, um eine Sitzung zu starten.
- 2 Geben Sie einen Benutzernamen und ein Kennwort ein.
- 3 Geben Sie in der Shell den Befehl `pi shell` oder `shell` ein, um auf die Bash-Shell zuzugreifen.

Exportieren eines vCenter Server-Support-Pakets zwecks Fehlerbehebung

Sie können das Support-Paket der vCenter Server-Instanz in der Appliance zwecks Fehlerbehebung mithilfe der im DCUI-Startbildschirm angezeigten URL exportieren.

Sie können auch das Support-Paket aus der Bash-Shell der vCenter Server Appliance abrufen, indem Sie das Skript `vc-support.sh` ausführen.

Das Support-Paket wird im `.tgz`-Format exportiert.

Verfahren

- 1 Melden Sie sich bei der Windows-Hostmaschine an, auf die Sie das Paket herunterladen möchten.
- 2 Öffnen Sie einen Webbrowser und geben Sie die in der DCUI angezeigte URL des Support-Pakets ein:

`https://appliance-fully-qualified-domain-name:443/appliance/support-bundle`

- 3 Geben Sie den Benutzernamen und das Kennwort des Root-Benutzers ein.
- 4 Drücken Sie die **Eingabetaste**.

Das Support-Paket wird als `.tgz`-Datei auf Ihre Windows-Maschine heruntergeladen.

- 5 (Optional) Analysieren Sie die Datei `firstbootStatus.json`, um festzustellen, welches firstboot-Skript fehlgeschlagen ist.

Wenn Sie das Skript `vc-support.sh` in der Bash-Shell der vCenter Server Appliance ausgeführt haben, führen Sie zum Prüfen der Datei `firstbootStatus.json` folgenden Befehl aus:

```
cat /var/log/firstboot/firstbootStatus.json
```