



# Monitoring und Reporting

## SnapCenter Plug-in for VMware vSphere 4.9

NetApp  
July 23, 2024

# Inhalt

- Monitoring und Reporting ..... 1
  - Zeigt Statusinformationen an ..... 1
  - Überwachen von Jobs ..... 3
  - Job-Protokolle herunterladen ..... 3
  - Aufrufen von Berichten ..... 4
  - Generieren Sie ein Support Bundle aus dem SnapCenter Plug-in für VMware vSphere ..... 7
  - Generieren Sie ein Support-Bundle über die Wartungskonsole ..... 8
  - Prüfprotokolle ..... 9

# Monitoring und Reporting

## Zeigt Statusinformationen an

Sie können Statusinformationen im vSphere-Client-Dashboard anzeigen. Die Statusinformationen werden einmal pro Stunde aktualisiert.

### Schritte

1. Klicken Sie im linken Navigator-Bereich des vSphere-Clients auf **Dashboard**, wählen Sie einen vCenter-Server aus, und klicken Sie dann im Dashboard auf die Registerkarte **Status**.
2. Zeigen Sie eine Übersicht Statusinformationen an, oder klicken Sie auf einen Link, um weitere Informationen zu erhalten, wie in der folgenden Tabelle aufgeführt.

Dieses Dashboard-Feld...	Zeigt die folgenden Informationen an...
Zuletzt verwendete Job-Aktivitäten	<p>Die drei bis fünf letzten Backup-, Restore- und Mount-Aufgaben.</p> <ul style="list-style-type: none"><li>• Klicken Sie auf eine Job-ID, um weitere Details zu diesem Job anzuzeigen.</li><li>• Klicken Sie auf <b>Alle anzeigen</b>, um zur Registerkarte Job Monitor zu gelangen, um weitere Details zu allen Jobs anzuzeigen.</li></ul>
Jobs	<p>Eine Anzahl von Jobs (Backup, Restore und Mount), die innerhalb des ausgewählten Zeitfensters ausgeführt werden.</p> <p>Bewegen Sie den Cursor über einen Abschnitt des Diagramms, um weitere Details zu dieser Kategorie anzuzeigen.</p>

Dieses Dashboard-Feld...	Zeigt die folgenden Informationen an...
Aktuelle Zusammenfassung Des Schutzes	<p>Zusammenfassungen des Datensicherungsstatus von primären und sekundären VMs oder Datastores im ausgewählten Zeitfenster.</p> <ul style="list-style-type: none"> <li>• Klicken Sie auf das Dropdown-Menü, um <b>VMs</b> oder <b>Datastores</b> auszuwählen.</li> <li>• Wählen Sie als Sekundärspeicher <b>SnapVault</b> oder <b>SnapMirror</b> aus.</li> <li>• Bewegen Sie den Mauszeiger über einen Abschnitt eines Diagramms, um die Anzahl der VMs oder Datastores in dieser Kategorie anzuzeigen. In der Kategorie erfolgreich wird für jede Ressource das aktuellste Backup aufgeführt.</li> <li>• Sie können das Zeitfenster ändern, indem Sie die Konfigurationsdatei bearbeiten. Der Standardwert ist 7 Tage. Weitere Informationen finden Sie unter "<a href="#">Passen Sie Ihre Konfiguration an</a>".</li> <li>• Interne Zähler werden nach jedem primären oder sekundären Backup aktualisiert. Die Dashboard-Kachel wird alle sechs Stunden aktualisiert. Die Aktualisierungszeit kann nicht geändert werden. Hinweis: Wenn Sie eine Mirror-Vault-Schutzrichtlinie verwenden, werden die Zähler für die Sicherheitszusammenfassung im SnapVault-Übersichtsdiagramm und nicht im SnapMirror Diagramm angezeigt.</li> </ul>
Konfiguration	Gesamtzahl der jeden Objekttyp, die vom SnapCenter Plug-in für VMware vSphere gemanagt wird

Dieses Dashboard-Feld...	Zeigt die folgenden Informationen an...
Storage	<p>Die Gesamtzahl der erstellten Snapshot Kopien, SnapVault und SnapMirror Snapshot Kopien und die Menge des für primäre und sekundäre Snapshot Kopien verwendeten Storage. Das Liniendiagramm stellt den primären und sekundären Speicherverbrauch über einen laufenden Zeitraum von 90 Tagen täglich separat dar. Die Speicherinformationen werden alle 24 Stunden um 1:08 UHR aktualisiert</p> <p>Storage-Einsparungen sind das Verhältnis der logischen Kapazität (Snapshot-Einsparungen plus verbrauchter Storage) zur physischen Kapazität des primären Storage. Das Balkendiagramm zeigt die Storage-Einsparungen.</p> <p>Bewegen Sie den Cursor über eine Linie auf der Karte, um detaillierte Ergebnisse für Tag anzuzeigen.</p>

## Überwachen von Jobs

Nachdem Sie mit dem VMware vSphere-Client einen Datensicherungsvorgang durchgeführt haben, können Sie den Job-Status über die Registerkarte Job Monitor im Dashboard überwachen und Jobdetails anzeigen.

### Schritte

1. Klicken Sie im linken Navigator-Bereich des vSphere-Clients auf **Dashboard**. Wenn zwei oder mehr vCenters im verknüpften Modus konfiguriert sind, wählen Sie einen vCenter-Server aus und klicken Sie dann im Dashboard-Bereich auf die Registerkarte **Job Monitor**.  
Auf der Registerkarte Job Monitor werden die einzelnen Jobs sowie deren Status, die Startzeit und die Endzeit aufgelistet. Wenn die Jobnamen lang sind, müssen Sie möglicherweise nach rechts blättern, um die Start- und Endzeiten anzuzeigen. Das Display wird alle 30 Sekunden aktualisiert.
  - Wählen Sie das Symbol Aktualisieren in der Symbolleiste aus, um die Anzeige bei Bedarf zu aktualisieren.
  - Wählen Sie das Filtersymbol aus, um den Zeitraum, den Typ, das Tag und den Status der Jobs auszuwählen, die angezeigt werden sollen. Der Filter ist Groß-/Kleinschreibung beachten.
  - Wählen Sie das Symbol Aktualisieren im Fenster Job-Details aus, um die Anzeige während der Ausführung des Jobs zu aktualisieren.

Wenn auf dem Dashboard keine Jobinformationen angezeigt werden, finden Sie im ["KB-Artikel: SnapCenter vSphere-Client-Dashboard zeigt keine Jobs an"](#).

## Job-Protokolle herunterladen

Sie können die Jobprotokolle von der Registerkarte Job Monitor auf dem Dashboard des SnapCenter VMware vSphere Clients herunterladen.

Wenn bei der Verwendung des VMware vSphere-Clients ein unerwartetes Verhalten auftritt, können Sie mithilfe der Protokolldateien die Ursache identifizieren und das Problem lösen.



Der Standardwert für die Aufbewahrung von Jobprotokollen beträgt 30 Tage; der Standardwert für die Beibehaltung von Jobs beträgt 90 Tage. Job-Protokolle und Jobs, die älter als die konfigurierte Aufbewahrung sind, werden alle sechs Stunden gelöscht. Sie können die Konfiguration verwenden `jobs/cleanup` REST-APIs ändern, wie lange Jobs und Job-Logs aufbewahrt werden. Der Spülzeitplan kann nicht geändert werden.

### Schritte

1. Klicken Sie im linken Navigator-Bereich des vSphere-Clients auf **Dashboard**, wählen Sie einen vCenter-Server aus und klicken Sie dann im Dashboard-Bereich auf die Registerkarte **Job Monitor**.
2. Wählen Sie in der Titelleiste des Job Monitors das Download-Symbol aus.

Möglicherweise müssen Sie nach rechts blättern, um das Symbol zu sehen.

Sie können auch auf einen Job doppelklicken, um auf das Fenster Job Details zuzugreifen und dann auf **Job Logs herunterladen** klicken.

### Ergebnis

Job-Protokolle befinden sich auf dem Linux VM-Host, auf dem das SnapCenter VMware Plug-in bereitgestellt wird. Der Standard-Job-Log-Speicherort ist `/var/log/netapp`.

Wenn Sie versucht haben, Jobprotokolle herunterzuladen, aber die Protokolldatei mit dem Namen in der Fehlermeldung gelöscht wurde, kann es zu folgendem Fehler kommen: `HTTP ERROR 500 Problem accessing /export-scv-logs`. Um diesen Fehler zu beheben, überprüfen Sie den Zugriffsstatus und die Berechtigungen für die Datei mit dem Namen in der Fehlermeldung und beheben Sie das Zugriffsproblem.

## Aufrufen von Berichten

Sie können über das Dashboard Berichte für einen oder mehrere Jobs anfordern.

Die Registerkarte Berichte enthält Informationen zu den Jobs, die auf der Seite Jobs im Dashboard ausgewählt wurden. Wenn keine Jobs ausgewählt sind, ist die Registerkarte Berichte leer.

### Schritte

1. Klicken Sie im linken Navigator-Bereich des vSphere-Clients auf **Dashboard**, wählen Sie einen vCenter-Server aus und klicken Sie dann auf die Registerkarte **Berichte**.
2. Für Backup-Berichte können Sie Folgendes tun:

- a. Ändern Sie den Bericht

Wählen Sie das Filtersymbol aus, um den Zeitbereich, den Jobstatustyp, die Ressourcengruppen und die Richtlinien zu ändern, die in den Bericht aufgenommen werden sollen.

- b. Erstellen eines detaillierten Berichts

Doppelklicken Sie auf einen Job, um einen detaillierten Bericht für diesen Job zu erstellen.

3. Optional: Klicken Sie auf der Registerkarte Berichte auf **Download** und wählen Sie das Format (HTML oder CSV) aus.

Sie können auch auf das Download-Symbol klicken, um Plug-in-Protokolle herunterzuladen.

## Berichtstypen vom VMware vSphere Client

Der VMware vSphere Client für SnapCenter bietet anpassbare Berichtsoptionen, die Ihnen Details zu Ihren Datensicherungsaufgaben und zum Plug-in-Ressourcenstatus liefern. Sie können Berichte nur für den Primärschutz erstellen.



Backup-Zeitpläne werden in der Zeitzone ausgeführt, in der das SnapCenter VMware Plug-in implementiert wird. vCenter meldet Daten in der Zeitzone, in der sich die vCenter befindet. Wenn sich das SnapCenter VMware Plug-in und vCenter in verschiedenen Zeitzonen befinden, sind die Daten im VMware vSphere Client Dashboard möglicherweise nicht mit den Daten in den Berichten identisch.

Das Dashboard zeigt Informationen zu migrierten Backups nur an, nachdem Backups nach der Migration durchgeführt wurden.

Berichtstyp	Beschreibung
Backup-Bericht	<p>Zeigt Übersichtsdaten zu Sicherungsaufträgen an. Klicken Sie auf einen Abschnitt/Status im Diagramm, um eine Liste der Jobs mit diesem Status auf der Registerkarte <b>Berichte</b> anzuzeigen.</p> <p>Für jeden Job listet der Bericht die Job-ID, die entsprechende Ressourcengruppe, die Backup-Richtlinie, Startzeit und Dauer, den Status und die Jobdetails auf, die den Jobnamen (Name der Snapshot-Kopie) enthalten, falls der Job abgeschlossen ist, sowie alle Warn- oder Fehlermeldungen.</p> <p>Sie können die Berichtstabelle im HTML- oder CSV-Format herunterladen. Sie können auch die Job Monitor-Job-Protokolle für alle Jobs herunterladen (nicht nur die Jobs im Bericht). Gelöschte Backups sind nicht im Bericht enthalten.</p>

Berichtstyp	Beschreibung
Mount-Bericht	<p>Zeigt Übersichtsdaten zu Mount-Jobs an. Klicken Sie auf einen Abschnitt/Status im Diagramm, um eine Liste der Jobs mit diesem Status auf der Registerkarte Berichte anzuzeigen.</p> <p>Für jeden Job werden die Job-ID, der Job-Status, der Job-Name sowie die Start- und Endzeiten des Jobs im Bericht aufgelistet. Der Job-Name enthält den Namen der Snapshot-Kopie.</p> <p>Beispiel: Mount Backup &lt;snapshot-copy-name&gt;</p> <p>Sie können die Berichtstabelle im HTML- oder CSV-Format herunterladen.</p> <p>Sie können auch die Job Monitor-Job-Protokolle für alle Jobs herunterladen (nicht nur die Jobs im Bericht).</p>
Bericht Wiederherstellen	<p>Zeigt Überblicksinformationen zu wiederherstellenden Jobs an. Klicken Sie auf einen Abschnitt/Status im Diagramm, um eine Liste der Jobs mit diesem Status auf der Registerkarte Berichte anzuzeigen.</p> <p>Für jeden Job werden die Job-ID, der Job-Status, der Job-Name sowie die Start- und Endzeiten des Jobs im Bericht aufgelistet. Der Job-Name enthält den Namen der Snapshot-Kopie. Beispiel: Restore Backup &lt;snapshot-copy-name&gt;</p> <p>Sie können die Berichtstabelle im HTML- oder CSV-Format herunterladen. Sie können auch die Job Monitor-Job-Protokolle für alle Jobs herunterladen (nicht nur die Jobs im Bericht).</p>



Berichtstyp	Beschreibung
<p>Letzter Schutzstatus von Bericht zu VMs oder Datastores</p>	<p>Zeigt Überblicksinformationen zum Sicherungsstatus während der konfigurierten Anzahl von Tagen für VMs und Datenspeicher an, die vom VMware-Plug-in von SnapCenter gemanagt werden. Der Standardwert ist 7 Tage. Informationen zum Ändern des Werts in der Eigenschaftendatei finden Sie unter <a href="#">"Ändern Sie die Standardwerte der Konfiguration"</a>.</p> <p>Klicken Sie auf einen Abschnitt/Status auf dem primären Schutzdiagramm, um eine Liste von VMs oder Datastores mit diesem Status auf der Registerkarte <b>Berichte</b> anzuzeigen.</p> <p>Der Protection Status Report für VM- oder Datastores für geschützte VMs und Datastores zeigt die Namen von VMs oder Datastores an, die während der konfigurierten Anzahl von Tagen gesichert wurden, den Namen der neuesten Snapshot-Kopie sowie die Start- und Endzeiten für die letzte Backup-Ausführung.</p> <p>In der VM- oder Datastores-Sicherungsstatusbericht für ungesicherte VMs oder Datastores werden die Namen von VMs oder Datastores angezeigt, die während der konfigurierten Anzahl von Tagen keine erfolgreichen Backups aufweisen.</p> <p>Sie können die Berichtstabelle im HTML- oder CSV-Format herunterladen. Sie können auch die Job Monitor-Job-Protokolle für alle Jobs herunterladen (nicht nur die Jobs im Bericht). Dieser Bericht wird jede Stunde aktualisiert, wenn der Plug-in-Cache aktualisiert wird. Daher zeigt der Bericht möglicherweise keine VMs oder Datenspeicher an, die kürzlich gesichert wurden.</p>

## Generieren Sie ein Support Bundle aus dem SnapCenter Plug-in für VMware vSphere

### Bevor Sie beginnen

Um sich beim SnapCenter Plug-in für die Management-GUI von VMware vSphere anzumelden, müssen Sie die IP-Adresse und die Anmeldedaten kennen. Sie müssen auch das MFA-Token notieren, das von der Wartungskonsole generiert wurde.

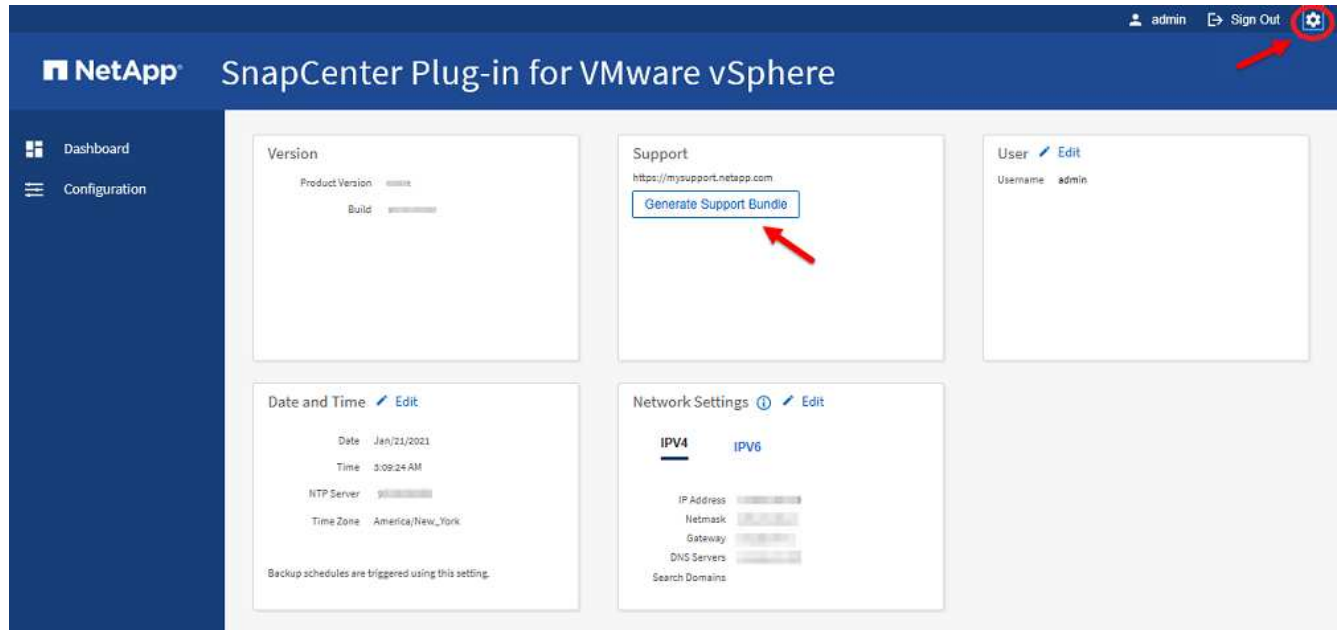
- Die IP-Adresse wurde bei der Bereitstellung des SnapCenter-VMware-Plug-ins angezeigt.
- Verwenden Sie die Login-Anmeldedaten, die bei der Bereitstellung des SnapCenter VMware Plug-ins oder einer späteren Änderung zur Verfügung gestellt werden.
- Generieren Sie ein 6-stelliges MFA-Token mithilfe der Systemkonfigurationsoptionen der Wartungskonsole.

## Schritte

1. Melden Sie sich im SnapCenter Plug-in für VMware vSphere an.

Verwenden Sie das Format <https://<OVA-IP-address>:8080>.

2. Klicken Sie in der oberen Symbolleiste auf das Symbol Einstellungen.



3. Klicken Sie auf der Seite **Einstellungen** im Abschnitt **Support** auf **Support** Paket generieren.
4. Nachdem das Support Bundle generiert wurde, klicken Sie auf den Link, der zur Verfügung steht, um das Bundle auf NetApp herunterzuladen.

## Generieren Sie ein Support-Bundle über die Wartungskonsole

### Schritte

1. Wählen Sie auf dem VMware vSphere-Client die VM aus, auf der sich das SnapCenter VMware Plug-in befindet.
2. Klicken Sie mit der rechten Maustaste auf die VM und anschließend auf der Registerkarte **Zusammenfassung** der virtuellen Appliance auf **Remote-Konsole starten** oder **Webkonsole starten**, um ein Fenster der Wartungskonsole zu öffnen und sich dann anzumelden.

Informationen zum Zugriff auf und zur Anmeldung bei der Wartungskonsole finden Sie unter "[Öffnen Sie die Wartungskonsole](#)".

```
VMware Remote Console
VMRC | [Pause] [Fullscreen]
Maintenance Console : "SnapCenter Plug-in for VMware vSphere"
Discovered interfaces: eth0 (ENABLED)
Main Menu:
-----
 1 ) Application Configuration
 2 ) System Configuration
 3 ) Network Configuration
 4 ) Support and Diagnostics

 x ) Exit

Enter your choice: _
```

3. Geben Sie im Hauptmenü die Option **4) Support und Diagnose** ein.
4. Geben Sie im Menü Support und Diagnose die Option **1) Supportpaket generieren** ein.

Um auf das Support-Paket zuzugreifen, geben Sie im Menü Support und Diagnose die Option **2) Zugriff auf Diagnose Shell** ein. Navigieren Sie in der Konsole zu `/support/support/<bundle_name>.tar.gz`.

## Prüfprotokolle

Audit Log ist eine Sammlung von Ereignissen in chronologischer Reihenfolge, die in eine Datei innerhalb der Appliance geschrieben wird. Die Audit-Log-Dateien werden in `generiert /var/log/netapp/audit` Standort und Dateiname folgen einer der folgenden Namenskonventionen:

- `Audit.log`: Aktive Audit-Log-Datei, die verwendet wird.
- `Audit-%d{yyyy-MM-dd-HH-mm-ss}.log.gz`: Gerollt über Audit-Log-Datei. Das Datum und die Uhrzeit im Dateinamen geben an, wann die Datei erstellt wurde, z. B. `Audit-2022-12-15-16-28-01.log.gz`.

In der Benutzeroberfläche des SCV-Plug-ins können Sie die Details des Überwachungsprotokolls anzeigen und exportieren

### Dashboard > Einstellungen > Audit Logs Tab

Sie können die Betriebsüberprüfung in den Überwachungsprotokollen anzeigen. Die Prüfprotokolle werden mit dem Support Bundle heruntergeladen.

Wenn E-Mail-Einstellungen konfiguriert sind, sendet SCV eine E-Mail-Benachrichtigung im Falle eines Fehlers bei der Integritätsprüfung des Überwachungsprotokolls. Ein Fehler bei der Integritätsprüfung für das Prüfprotokoll kann auftreten, wenn eine der Dateien manipuliert oder gelöscht wird.

Die Standardkonfigurationen der Audit-Dateien sind:

- Die verwendete Audit-Log-Datei kann auf maximal 10 MB anwachsen
- Es werden maximal 10 Audit-Log-Dateien aufbewahrt

Um die Standardkonfigurationen zu ändern, fügen Sie ein Schlüsselwert-Paar in /opt/netapp/scvservice/Standalone\_aegis/etc/scbr/scbr.properties hinzu und starten den scvservice neu.

Die Konfigurationen für Audit-Log-Dateien sind:

- AuditMaxROFiles=<xx>, wobei xx die maximale Anzahl von gerollten über Audit-Log-Dateien ist, zum Beispiel: AuditMaxROFiles=15.
- AuditLogSize=<XX>-Funktionen, wobei xx die Größe der Datei in MB ist, z. B. auditLogSize=15MB.

Gerollte über Audit-Protokolle werden regelmäßig auf ihre Integrität überprüft. SCV stellt REST-APIs zur Verfügung, um Protokolle anzuzeigen und deren Integrität zu überprüfen. Ein integrierter Zeitplan löst und weist einen der folgenden Integritätsstatus zu.

Status	Beschreibung
MANIPULIERT	Der Inhalt der Audit-Log-Datei wird geändert
NORMAL	Audit-Log-Datei wurde nicht geändert
ROLLOVER LÖSCHEN	- Audit-Log-Datei wird auf Basis der Aufbewahrung gelöscht - Standardmäßig bleiben nur 10 Dateien erhalten
UNERWARTETES LÖSCHEN	Audit-Log-Datei wird gelöscht
AKTIV	- Audit Log Datei wird verwendet - Gilt nur für audit.log

Die Ereignisse lassen sich in drei Hauptkategorien einteilen:

- Ereignisse Auf Der Datensicherung
- Ereignisse Der Wartungskonsole
- Ereignisse Der Admin-Konsole

## Ereignisse Auf Der Datensicherung

Die Ressourcen in SCV sind:

- Storage-System
- Ressourcengruppe
- Richtlinie
- Backup

In der folgenden Tabelle sind die Vorgänge aufgeführt, die für jede Ressource durchgeführt werden können:

Ressourcen	Betrieb
Storage-System	Erstellt, Geändert, Gelöscht

Ressourcengruppe	Erstellt, Geändert, Gelöscht, Unterbrochen, Fortgesetzt
Richtlinie	Erstellt, Geändert, Gelöscht
Backup	Erstellt, Umbenannt, Gelöscht, Angehängt, Abgehängt, VMDK wiederhergestellt, VM wiederhergestellt, VMDK anhängen, VMDK trennen, Gastdatei wiederherstellen

## Ereignisse Der Wartungskonsole

Der administrative Betrieb in der Wartungskonsole wird geprüft.  
Folgende Optionen für die Wartungskonsole sind verfügbar:

1. Dienste starten/stoppen
2. Benutzername und Passwort ändern
3. MySQL-Kennwort ändern
4. Konfigurieren Sie MySQL Backup
5. MySQL Backup wiederherstellen
6. Ändern Sie das Benutzerpasswort „Wartung“
7. Zeitzone ändern
8. Ändern Sie den NTP-Server
9. Deaktivieren Sie den SSH-Zugriff
10. Erhöhen Sie die Größe der Jail-Festplatte
11. Upgrade
12. VMware-Tools installieren (wir arbeiten daran, diese durch Open-vm-Tools zu ersetzen)
13. Ändern Sie die IP-Adresseinstellungen
14. Ändern Sie die Einstellungen für die DNS-Suche
15. Ändern Sie statische Routen
16. Zugriff auf die Diagnoseschale
17. Remote-Diagnosezugriff aktivieren

## Ereignisse Der Admin-Konsole

Die folgenden Vorgänge in der Admin Console-UI werden geprüft:

- Einstellungen
  - Ändern Sie die Anmeldedaten des Administrators
  - Ändern Sie die Zeitzone
  - Ändern Sie den NTP-Server
  - Ändern der IPv4-/IPv6-Einstellungen
- Konfiguration
  - Ändern Sie die vCenter Credentials

- Plug-in-Aktivierung/Deaktivierung

## Konfigurieren Sie Syslog-Server

Prüfprotokolle werden in der Appliance gespeichert und regelmäßig auf ihre Integrität überprüft. Mit der Ereignisweiterleitung können Sie Ereignisse vom Quell- oder Weiterleitungscomputer abrufen und auf einem zentralen Computer, dem Syslog-Server, speichern. Die Daten werden während der Übertragung zwischen Quelle und Ziel verschlüsselt.

### Bevor Sie beginnen

Sie müssen über Administratorrechte verfügen.

### Über diese Aufgabe

Diese Aufgabe unterstützt Sie bei der Konfiguration des Syslog-Servers.

### Schritte

1. Melden Sie sich beim SnapCenter-Plug-in für VMware vSphere an.
2. Wählen Sie im linken Navigationsbereich **Einstellungen > Audit-Protokolle > Einstellungen**.
3. Wählen Sie im Bereich **Audit Log Settings** die Option **Send Audit Logs to Syslog Server** aus
4. Geben Sie die folgenden Details ein:
  - Syslog-Server-IP
  - Syslog-Server-Port
  - RFC-Format
  - Syslog-Serverzertifikat
5. Klicken Sie auf **SAVE**, um die Syslog-Server-Einstellungen zu speichern.

## Ändern Sie die Einstellungen des Überwachungsprotokolls

Sie können die Standardkonfigurationen der Protokolleinstellungen ändern.

### Bevor Sie beginnen

Sie müssen über Administratorrechte verfügen.

### Über diese Aufgabe

Mit dieser Aufgabe können Sie die standardmäßigen Einstellungen des Überwachungsprotokolls ändern.

### Schritte

1. Melden Sie sich beim SnapCenter-Plug-in für VMware vSphere an.
2. Wählen Sie im linken Navigationsbereich **Einstellungen > Audit-Protokolle > Einstellungen**.
3. Geben Sie im Bereich **Audit Log Settings** die Werte **Anzahl der Audit-Einträge** und **Audit Log Size Limit** entsprechend Ihren Anforderungen ein.

## Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

## Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.