



Monitoring und Reporting

SnapCenter Plug-in for VMware vSphere 6.2

NetApp
October 27, 2025

This PDF was generated from https://docs.netapp.com/de-de/sc-plugin-vmware-vsphere/scpivs44_view_status_information.html on October 27, 2025. Always check docs.netapp.com for the latest.

Inhalt

- Monitoring und Reporting 1
 - Zeigt Statusinformationen an 1
 - Überwachen von Jobs 3
 - Job-Protokolle herunterladen 3
 - Aufrufen von Berichten 4
 - Berichtstypen vom VMware vSphere Client 5
 - Generieren Sie ein Support-Paket aus der SnapCenter Plug-in for VMware vSphere Benutzeroberfläche . . 6
 - Generieren Sie ein Support-Bundle über die Wartungskonsole 7
- Prüfprotokolle 8
 - Ereignisse Auf Der Datensicherung 9
 - Ereignisse Der Wartungskonsole 10
 - Ereignisse Der Admin-Konsole 10
 - Konfigurieren Sie Syslog-Server 11
 - Ändern Sie die Einstellungen des Überwachungsprotokolls 11

Monitoring und Reporting

Zeigt Statusinformationen an

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

Schritte

1. Wählen Sie auf der Verknüpfungsseite des vCenter-Clients die Option SnapCenter-Plug-in für VMware vSphere (SCV) aus.
2. Wählen Sie im linken Navigationsbereich des SCV **Dashboard > Status**.
3. Zeigen Sie Statusinformationen für die Übersicht an, oder wählen Sie einen Link für weitere Details aus, 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">• Wählen Sie auf einer Job-ID aus, um weitere Details zu diesem Job anzuzeigen.• Wählen Sie Alle anzeigen, um auf die Registerkarte Job Monitor zu gelangen, um weitere Details zu allen Jobs zu erhalten.
Jobs	<p>Eine Anzahl von Jobs (Backup, Restore und Mount), die innerhalb des ausgewählten Zeitfensters ausgeführt werden. 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"> • Wählen Sie das Dropdown-Menü aus, um VMs oder Datastores auszuwählen. • Wählen Sie als Sekundärspeicher SnapVault oder SnapMirror aus. • 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. • Sie können das Zeitfenster ändern, indem Sie die Konfigurationsdatei bearbeiten. Der Standardwert ist 7 Tage. Weitere Informationen finden Sie unter "Passen Sie Ihre Konfiguration an". • 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 Sicherungszusammenfassung im SnapVault-Übersichtsdiagramm und nicht im SnapMirror Diagramm angezeigt.
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 Snapshots, SnapVault- und SnapMirror-Snapshots sowie die Menge des für primäre und sekundäre Snapshots verwendeten Speichers. Das Liniendiagramm stellt den primären und sekundären Speicherverbrauch über einen laufenden Zeitraum von 90 Tagen täglich separat dar. Storage-Informationen werden alle 24 Stunden um 1:08 UHR aktualisiert. Storage Savings ist 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. Wählen Sie auf der Verknüpfungsseite des vCenter-Clients die Option SnapCenter-Plug-in für VMware vSphere (SCV) aus.
2. Wählen Sie im linken Navigationsbereich des SCV **Dashboard**.
3. Wenn zwei oder mehr vCenter im verknüpften Modus konfiguriert sind, wählen Sie die SCV-Plug-in-Instanz aus und wählen Sie die Registerkarte **Job Monitor** aus. 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 im Dashboard keine Jobinformationen angezeigt werden, lesen Sie ["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. Wählen Sie auf der Verknüpfungsseite des vCenter-Clients die Option SnapCenter-Plug-in für VMware vSphere (SCV) aus.
2. Wählen Sie im linken Navigationsbereich des SCV **Dashboard > Job Monitor**.
3. 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 das Fenster Job-Details aufzurufen, und dann **Job-Protokolle herunterladen** auswählen.

Ergebnis

Job-Protokolle befinden sich auf dem Linux VM-Host, auf dem das SnapCenter Plug-in für VMware vSphere bereitgestellt wird. Der Standardspeicherort für das Jobprotokoll 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. Wählen Sie auf der Verknüpfungsseite des vCenter-Clients die Option SnapCenter-Plug-in für VMware vSphere (SCV) aus.
2. Wählen Sie im linken Navigationsbereich des SCV **Dashboard > Reports**.
3. 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.

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

Sie können das Download-Symbol auswählen, 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 Plug-in für VMware vSphere bereitgestellt wird. VCenter meldet Daten in der Zeitzone, in der sich vCenter befindet. Wenn sich das SnapCenter-Plug-in für VMware vSphere und vCenter daher in unterschiedlichen 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	Zeigt Übersichtsdaten zu Sicherungsaufträgen an. Wählen Sie einen Abschnitt/Status im Diagramm aus, um eine Liste der Jobs mit diesem Status auf der Registerkarte Reports anzuzeigen. Für jeden Job werden im Bericht die Job-ID, die entsprechende Ressourcengruppe, die Backup-Richtlinie, die Startzeit und -Dauer, der Status und die Jobdetails aufgeführt, die den Jobnamen (Snapshot-Name), wenn der Job abgeschlossen ist, sowie alle Warn- oder Fehlermeldungen enthalten. 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.
Mount-Bericht	Zeigt Übersichtsdaten zu Mount-Jobs an. Wählen Sie einen Abschnitt/Status im Diagramm aus, um eine Liste der Jobs mit diesem Status auf der Registerkarte Berichte anzuzeigen. Für jeden Job werden die Job-ID, der Job-Status, der Job-Name sowie die Start- und Endzeiten des Jobs im Bericht aufgelistet. Der Jobname enthält den Snapshot-Namen. Zum Beispiel: Mount Backup <snapshot-copy-name> 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).

Berichtstyp	Beschreibung
Bericht Wiederherstellen	Zeigt Überblicksinformationen zu wiederherstellenden Jobs an. Wählen Sie einen Abschnitt/Status im Diagramm aus, um eine Liste der Jobs mit diesem Status auf der Registerkarte Berichte anzuzeigen. Für jeden Job werden die Job-ID, der Job-Status, der Job-Name sowie die Start- und Endzeiten des Jobs im Bericht aufgelistet. Der Jobname enthält den Snapshot-Namen. Zum Beispiel: Restore Backup <snapshot-copy-name> 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).
Letzter Sicherungsstatus von VMs oder Datastores	Zeigt eine Übersicht über den Schutzstatus während der konfigurierten Anzahl von Tagen für VMs und Datastores an, die vom SnapCenter-Plug-in für VMware vSphere verwaltet werden. Der Standardwert ist 7 Tage. Informationen zum Ändern des Werts in der Eigenschaftendatei finden Sie unter "Ändern Sie die Standardwerte der Konfiguration" . Wählen Sie im primären Schutzdiagramm einen Abschnitt/Status aus, um eine Liste der VMs oder Datastores mit diesem Status auf der Registerkarte Reports anzuzeigen. Der Bericht zum Schutz der VMs oder Datastores für geschützte VMs und Datastores zeigt die Namen der VMs oder Datenspeicher an, die während der konfigurierten Anzahl von Tagen gesichert wurden, den Namen des letzten Snapshots sowie die Start- und Endzeiten der letzten Backup-Ausführung. 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. 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.

Generieren Sie ein Support-Paket aus der SnapCenter Plug-in for VMware vSphere Benutzeroberfläche

Bevor Sie beginnen

Um sich bei der Verwaltungsbenutzeroberfläche des SnapCenter Plug-in for VMware vSphere anzumelden, müssen Sie die IP-Adresse und die Anmeldeinformationen

kennen. Sie müssen sich auch das von der Wartungskonsole generierte MFA-Token notieren.

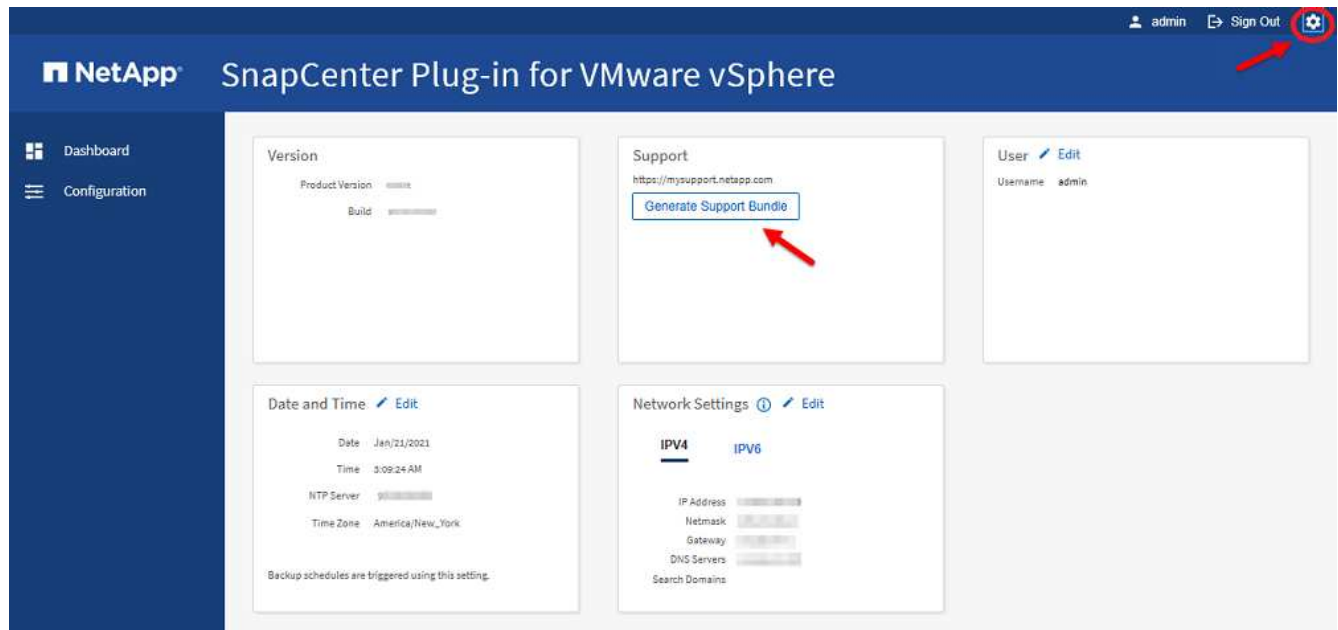
- Die IP-Adresse wurde bei der Bereitstellung des SnapCenter-Plug-ins für VMware vSphere angezeigt.
- Verwenden Sie die Anmeldeinformationen, die während der Bereitstellung des SnapCenter-Plug-ins für VMware vSphere oder später geändert wurden.
- Generieren Sie ein 6-stelliges MFA-Token mithilfe der Systemkonfigurationsoptionen der Wartungskonsole.

Schritte

1. Melden Sie sich bei der Benutzeroberfläche des SnapCenter Plug-in for VMware vSphere an.

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

2. Wählen Sie das Symbol Einstellungen in der oberen Symbolleiste.



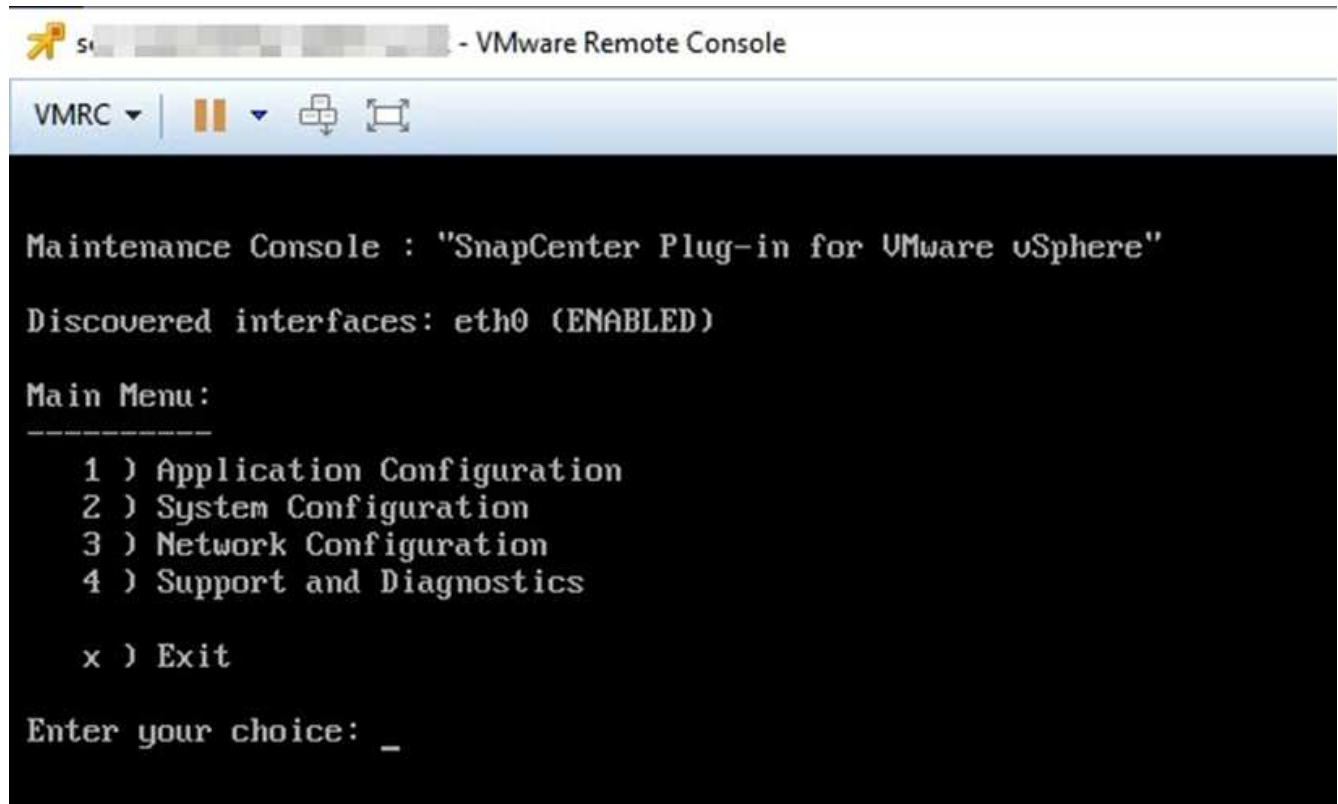
3. Wählen Sie auf der Seite **Einstellungen** im Abschnitt **Support** die Option **Support** Bundle generieren.
4. Wählen Sie nach dem Generieren des Support-Bundles den Link aus, über den das Bundle auf NetApp heruntergeladen werden kann.

Generieren Sie ein Support-Bundle über die Wartungskonsole

Schritte

1. Wählen Sie im VMware vSphere-Client die VM aus, auf der sich das SnapCenter-Plug-in für VMware vSphere befindet.
2. Wählen Sie auf der Registerkarte **Zusammenfassung** der virtuellen Appliance **Remote Console starten** oder **Web Console starten** aus, um ein Fenster der Wartungskonsole zu öffnen, und melden Sie sich dann an.

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



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

Ein Audit-Protokoll ist eine Sammlung von Ereignissen in chronologischer Reihenfolge, die in eine Datei innerhalb der Appliance geschrieben wird. Die Audit-Log-Dateien werden am Speicherort generiert `/var/log/netapp/audit`, und die Dateinamen 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 SCV-Plug-in-Benutzeroberfläche können Sie die Audit-Log-Details über **Dashboard > Einstellungen > Audit-Protokolle**-Registerkarte anzeigen und exportieren. 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 Überprüfung der Integrität des Überwachungsprotokolls 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

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
- Abonnement
- Konto

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

Ressourcen	Betrieb
Storage-System	Erstellt, Geändert, Gelöscht
Abonnement	Erstellt, Geändert, Gelöscht
Konto	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, dies 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 Sie die IPv4/IPv6-Adresseinstellungen
- 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. Wählen Sie **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 maximale Anzahl an Audit Log Files und die maximale Größe der Audit Log Files ein.
4. Wählen Sie die Option **Überwachungsprotokolle an Syslog-Server senden** aus, wenn Sie die Protokolle an Syslog-Server senden möchten. Geben Sie die Details des Servers ein.
5. Speichern Sie die Einstellungen.

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers 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, BEISPIELHAFTE 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.