



Überwachen und berichten

SnapCenter Plug-in for VMware vSphere

NetApp

December 09, 2025

Inhalt

Überwachen und berichten	1
Statusinformationen anzeigen	1
Überwachen von Jobs	3
Jobprotokolle herunterladen	3
Zugriffsberichte	4
Berichtstypen vom VMware vSphere-Client	4
Generieren Sie ein Support-Paket aus dem SnapCenter Plug-in for VMware vSphere GUI	6
Generieren Sie ein Support-Paket aus der Wartungskonsole	7
Überwachungsprotokolle	8
Datenschutzereignisse	9
Ereignisse der Wartungskonsole	10
Ereignisse in der Admin-Konsole	10
Konfigurieren von Syslog-Servern	11
Ändern der Überwachungsprotokolleinstellungen	11

Überwachen und berichten

Statusinformationen anzeigen

Sie können Statusinformationen auf dem Dashboard des vSphere-Clients anzeigen. Die Statusinformationen werden stündlich aktualisiert.

Schritte

1. Wählen Sie auf der Verknüpfungsseite des vCenter-Clients das SnapCenter Plug-in for VMware vSphere (SCV) aus.
2. Wählen Sie im linken Navigationsbereich von SCV **Dashboard > Status**.
3. Zeigen Sie eine Übersicht der Statusinformationen an oder wählen Sie einen Link aus, um weitere Details anzuzeigen, wie in der folgenden Tabelle aufgeführt.

Diese Dashboard-Kachel ...	Zeigt die folgenden Informationen an ...
Aktuelle berufliche Tätigkeiten	Die drei bis fünf aktuellsten Sicherungs-, Wiederherstellungs- und Bereitstellungsaufträge. • Wählen Sie eine Job-ID aus, um weitere Details zu diesem Job anzuzeigen. • Wählen Sie Alle anzeigen, um zur Registerkarte „Job-Monitor“ zu gelangen und weitere Details zu allen Jobs anzuzeigen.
Jobs	Eine Zählung aller Auftragsstypen (Sicherung, Wiederherstellung und Bereitstellung), die innerhalb des ausgewählten Zeitfensters ausgeführt wurden. Bewegen Sie den Cursor über einen Abschnitt des Diagramms, um weitere Details zu dieser Kategorie anzuzeigen.

Diese Dashboard-Kachel ...	Zeigt die folgenden Informationen an ...
Neueste Schutzzusammenfassung	Zusammenfassungen des Datenschutzzustatus primärer und sekundärer VMs oder Datenspeicher innerhalb des ausgewählten Zeitfensters. • Wählen Sie im Dropdown-Menü VMs oder Datastores aus. • Wählen Sie als sekundären Speicher * SnapVault* oder * SnapMirror*. • Bewegen Sie den Cursor über einen Abschnitt eines Diagramms, um die Anzahl der VMs oder Datenspeicher in dieser Kategorie anzuzeigen. In der Kategorie „Erfolgreich“ wird für jede Ressource das aktuellste Backup aufgelistet. • Sie können das Zeitfenster ändern, indem Sie die Konfigurationsdatei bearbeiten. Der Standardwert beträgt 7 Tage. Weitere Informationen finden Sie unter "Passen Sie Ihre Konfiguration an". • Interne Zähler werden nach jeder primären oder sekundären Sicherung 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 Schutzzusammenfassung im SnapVault Zusammenfassungsdiagramm und nicht im SnapMirror Diagramm angezeigt.
Konfiguration	Die Gesamtzahl aller Objekttypen, die vom SnapCenter Plug-in for VMware vSphere verwaltet werden.
Storage	Die Gesamtzahl der generierten Snapshots, SnapVault und SnapMirror -Snapshots und die für primäre und sekundäre Snapshots verwendete Speichermenge. Das Liniendiagramm stellt den Primär- und Sekundärspeicherverbrauch über einen rollierenden 90-Tage-Zeitraum hinweg getrennt auf Tagesbasis dar. Die Speicherinformationen werden alle 24 Stunden um 1:08 Uhr aktualisiert. Die Speichereinsparungen sind das Verhältnis der logischen Kapazität (Snapshot-Einsparungen plus verbrauchter Speicher) zur physischen Kapazität des Primärspeichers. Das Balkendiagramm veranschaulicht die Speichereinsparungen. Bewegen Sie den Cursor über eine Linie im Diagramm, um detaillierte Tagesergebnisse anzuzeigen.

Überwachen von Jobs

Nachdem Sie mit dem VMware vSphere-Client einen Datenschutzvorgang durchgeführt haben, können Sie den Jobstatus auf der Registerkarte „Job Monitor“ im Dashboard überwachen und Jobdetails anzeigen.

Schritte

1. Wählen Sie auf der Verknüpfungsseite des vCenter-Clients das SnapCenter Plug-in for VMware vSphere (SCV) aus.
2. Wählen Sie im linken Navigationsbereich von SCV **Dashboard** aus.
3. Wenn zwei oder mehr vCenter im verknüpften Modus konfiguriert sind, wählen Sie die SCV-Plug-In-Instanz und wählen Sie die Registerkarte **Job Monitor**. Auf der Registerkarte „Job Monitor“ werden alle Jobs und ihr Status sowie ihre Start- und Endzeit aufgelistet. Wenn die Jobnamen lang sind, müssen Sie möglicherweise nach rechts scrollen, um die Start- und Endzeiten anzuzeigen. Die Anzeige wird alle 30 Sekunden aktualisiert.
 - Wählen Sie das Aktualisierungssymbol in der Symbolleiste, 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 berücksichtigt die Groß- und Kleinschreibung.
 - Wählen Sie das Aktualisierungssymbol im Fenster „Auftragsdetails“ aus, um die Anzeige während der Ausführung des Auftrags zu aktualisieren.

Wenn das Dashboard keine Jobinformationen anzeigt, lesen Sie ["KB-Artikel: SnapCenter vSphere-Client-Dashboard zeigt keine Jobs an"](#).

Jobprotokolle herunterladen

Sie können die Jobprotokolle von der Registerkarte „Job Monitor“ im Dashboard des SnapCenter VMware vSphere-Clients herunterladen.

Wenn bei der Verwendung des VMware vSphere-Clients unerwartetes Verhalten auftritt, können Sie die Protokolldateien verwenden, um die Ursache zu ermitteln und das Problem zu beheben.



Der Standardwert für die Aufbewahrung von Jobprotokollen beträgt 30 Tage; der Standardwert für die Aufbewahrung von Jobs beträgt 90 Tage. Jobprotokolle und Jobs, die älter als die konfigurierte Aufbewahrungsdauer sind, werden alle sechs Stunden gelöscht. Sie können die Konfiguration verwenden `jobs/cleanup` REST-APIs zum Ändern der Aufbewahrungsdauer von Jobs und Jobprotokollen. Sie können den Bereinigungszeitplan nicht ändern.

Schritte

1. Wählen Sie auf der Verknüpfungsseite des vCenter-Clients das SnapCenter Plug-in for VMware vSphere (SCV) aus.
2. Wählen Sie im linken Navigationsbereich von SCV **Dashboard > Job Monitor**.
3. Wählen Sie das Download-Symbol in der Titelleiste des Job Monitors.

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

Sie können auch auf einen Job doppelklicken, um auf das Fenster „Jobdetails“ zuzugreifen, und dann

„Jobprotokolle herunterladen“ auswählen.

Ergebnis

Jobprotokolle befinden sich auf dem Linux-VM-Host, auf dem das SnapCenter Plug-in for VMware vSphere bereitgestellt wird. Der Standardspeicherort des Jobprotokolls ist `/var/log/netapp`.

Wenn Sie versucht haben, Jobprotokolle herunterzuladen, die in der Fehlermeldung genannte Protokolldatei jedoch gelöscht wurde, tritt möglicherweise der folgende Fehler auf: `HTTP ERROR 500 Problem accessing /export-scv-logs`. Um diesen Fehler zu beheben, überprüfen Sie den Dateizugriffsstatus und die Berechtigungen für die in der Fehlermeldung genannte Datei und beheben Sie das Zugriffsproblem.

Zugriffsberichte

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 sind. Wenn keine Jobs ausgewählt sind, ist die Registerkarte „Berichte“ leer.

Schritte

1. Wählen Sie auf der Verknüpfungsseite des vCenter-Clients das SnapCenter Plug-in for VMware vSphere (SCV) aus.
2. Wählen Sie im linken Navigationsbereich von SCV die Registerkarte **Dashboard > Berichte** aus.
3. Für Sicherheitsberichte können Sie Folgendes tun:

- a. Ändern des Berichts

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

- b. Erstellen Sie einen detaillierten Bericht

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

4. Optional: Wählen Sie auf der Registerkarte „Berichte“ die Option „Herunterladen“ und wählen Sie das Format (HTML oder CSV).

Sie können auch 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 Datenschutzaufträgen und dem Status der Plug-In-Ressourcen liefern. Sie können nur Berichte zum primären Schutz erstellen.



Sicherungspläne werden in der Zeitzone ausgeführt, in der das SnapCenter Plug-in for VMware vSphere bereitgestellt wird. vCenter meldet Daten in der Zeitzone, in der sich das vCenter befindet. Wenn sich das SnapCenter Plug-in for VMware vSphere und das vCenter in unterschiedlichen Zeitzonen befinden, stimmen die Daten im Dashboard des VMware vSphere-Clients möglicherweise nicht mit den Daten in den Berichten überein.

Das Dashboard zeigt Informationen zu migrierten Sicherungen erst an, nachdem Sicherungen nach der Migration durchgeführt wurden.

Berichtstyp	Beschreibung
Sicherungsbericht	Zeigt Übersichtsdaten zu Sicherungsaufträgen an. Wählen Sie einen Abschnitt/Status im Diagramm aus, um auf der Registerkarte Berichte eine Liste der Jobs mit diesem Status anzuzeigen. Für jeden Job listet der Bericht die Job-ID, die entsprechende Ressourcengruppe, die Sicherungsrichtlinie, Startzeit und Dauer, den Status und die Jobdetails auf, einschließlich des Jobnamens (Snapshot-Namens), wenn der Job abgeschlossen ist, sowie etwaige Warn- oder Fehlermeldungen. Sie können die Berichtstabelle im HTML- oder CSV-Format herunterladen. Sie können auch die Job Monitor-Jobprotokolle für alle Jobs herunterladen (nicht nur für 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 auf der Registerkarte „Berichte“ eine Liste der Jobs mit diesem Status anzuzeigen. Für jeden Auftrag listet der Bericht die Auftrags-ID, den Auftragsstatus, den Auftragsnamen sowie die Start- und Endzeiten des Auftrags auf. 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-Jobprotokolle für alle Jobs herunterladen (nicht nur für die Jobs im Bericht).
Wiederherstellungsbericht	Zeigt eine Übersicht über Statusinformationen zu Wiederherstellungsaufträgen an. Wählen Sie einen Abschnitt/Status im Diagramm aus, um auf der Registerkarte „Berichte“ eine Liste der Jobs mit diesem Status anzuzeigen. Für jeden Auftrag listet der Bericht die Auftrags-ID, den Auftragsstatus, den Auftragsnamen sowie die Start- und Endzeiten des Auftrags auf. 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-Jobprotokolle für alle Jobs herunterladen (nicht nur für die Jobs im Bericht).

Berichtstyp	Beschreibung
Bericht zum letzten Schutzstatus von VMs oder Datenspeichern	Zeigt Übersichtsinformationen zum Schutzstatus für die konfigurierte Anzahl von Tagen für VMs und Datenspeicher an, die vom SnapCenter Plug-in for VMware vSphere verwaltet werden. Der Standardwert beträgt 7 Tage. Informationen zum Ändern des Werts in der Eigenschaftendatei finden Sie unter "Ändern der Konfigurationsstandardwerte" . Wählen Sie einen Abschnitt/Status im primären Schutzdiagramm aus, um auf der Registerkarte Berichte eine Liste der VMs oder Datenspeicher mit diesem Status anzuzeigen. Der VM- oder Datastore-Schutzstatusbericht für geschützte VMs und Datastores zeigt die Namen der VMs oder Datastores an, die während der konfigurierten Anzahl von Tagen gesichert wurden, den Namen des letzten Snapshots sowie die Start- und Endzeiten für den letzten Sicherungslauf. Der VM- oder Datenspeicher-Schutzstatusbericht für ungeschützte VMs oder Datenspeicher zeigt die Namen der VMs oder Datenspeicher an, für die während der konfigurierten Anzahl von Tagen keine erfolgreichen Sicherungen durchgeführt wurden. Sie können die Berichtstabelle im HTML- oder CSV-Format herunterladen. Sie können auch die Job Monitor-Jobprotokolle für alle Jobs herunterladen (nicht nur für die Jobs im Bericht). Dieser Bericht wird stündlich aktualisiert, wenn der Plug-In-Cache aktualisiert wird. Daher werden im Bericht möglicherweise keine VMs oder Datenspeicher angezeigt, die kürzlich gesichert wurden.

Generieren Sie ein Support-Paket aus dem SnapCenter Plug-in for VMware vSphere GUI

Bevor Sie beginnen

Um sich beim SnapCenter Plug-in for VMware vSphere Verwaltungs-GUI anzumelden, müssen Sie die IP-Adresse und die Anmeldeinformationen kennen. Sie müssen sich auch das von der Wartungskonsole generierte MFA-Token notieren.

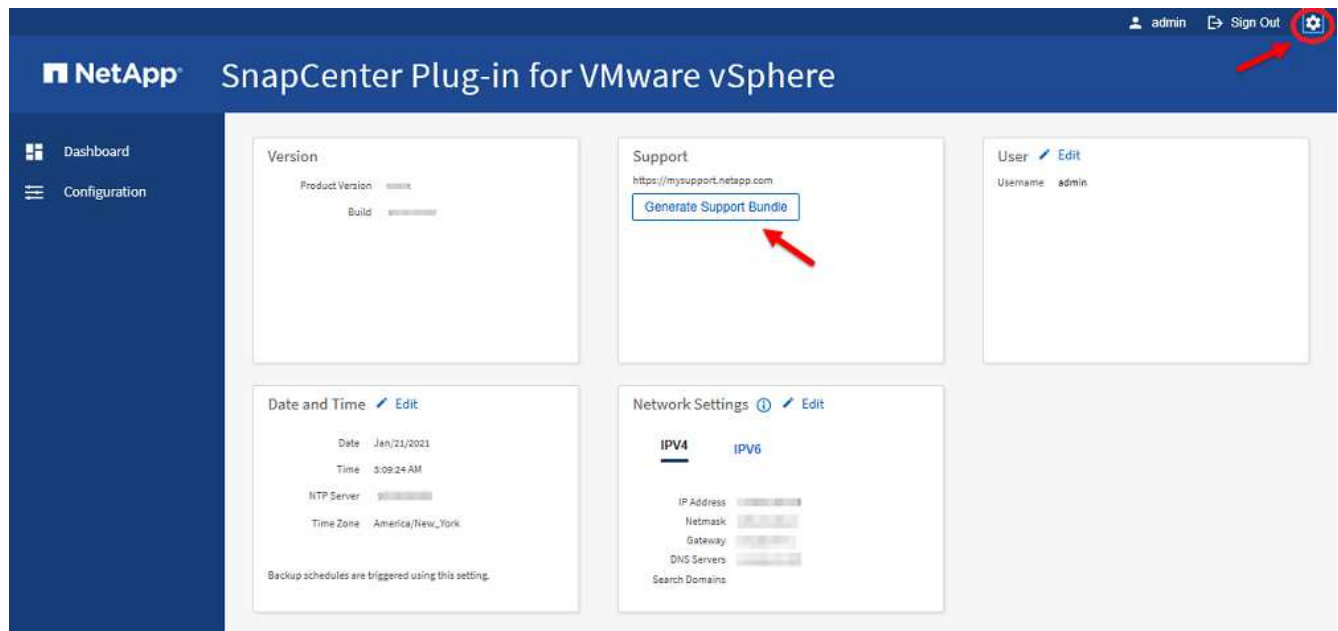
- Die IP-Adresse wurde angezeigt, als das SnapCenter Plug-in for VMware vSphere bereitgestellt wurde.
- Verwenden Sie die Anmeldeinformationen, die Sie während der Bereitstellung des SnapCenter Plug-in for VMware vSphere erhalten haben oder die später geändert wurden.
- Generieren Sie mithilfe der Systemkonfigurationsoptionen der Wartungskonsole ein 6-stelliges MFA-Token.

Schritte

1. Melden Sie sich beim SnapCenter Plug-in for VMware vSphere GUI an.

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

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



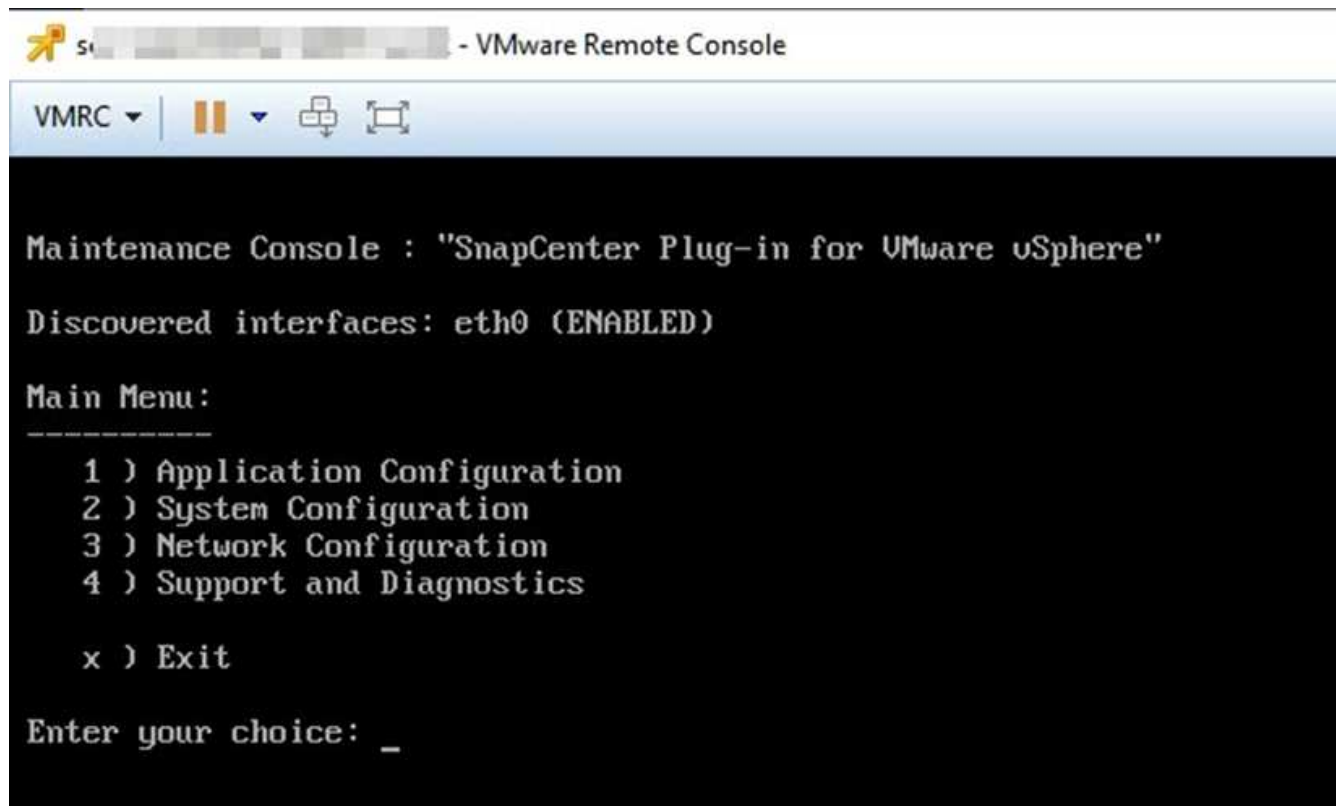
3. Wählen Sie auf der Seite **Einstellungen** im Abschnitt **Support** die Option **Support-Paket generieren** aus.
4. Nachdem das Support-Paket generiert wurde, wählen Sie den bereitgestellten Link aus, um das Paket auf NetApp herunterzuladen.

Generieren Sie ein Support-Paket aus der Wartungskonsole

Schritte

1. Wählen Sie im VMware vSphere-Client die VM aus, auf der sich das SnapCenter Plug-in for VMware vSphere befindet.
2. Wählen Sie auf der Registerkarte **Zusammenfassung** der virtuellen Appliance **Remotekonsole starten** oder **Webkonsole starten** aus, um ein Wartungskonsolenfenster zu öffnen, und melden Sie sich dann an.

Informationen zum Zugriff auf die Wartungskonsole und zur Anmeldung finden Sie unter "[Zugriff auf 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) Support-Paket generieren**“ ein.

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

Überwachungsprotokolle

Ein Prüfprotokoll ist eine Sammlung von Ereignissen in chronologischer Reihenfolge, die in eine Datei innerhalb des Geräts geschrieben wird. Die Audit-Logdateien werden generiert unter `/var/log/netapp/audit` Speicherort und die Dateinamen folgen einer der folgenden Namenskonventionen:

- `audit.log`: Aktive Audit-Protokolldatei, die verwendet wird.
- `audit-%d{yyyy-MM-dd-HH-mm-ss}.log.gz`: Audit-Protokolldatei übertragen. Datum und Uhrzeit im Dateinamen geben an, wann die Datei erstellt wurde, zum Beispiel: `audit-2022-12-15-16-28-01.log.gz`.

In der Benutzeroberfläche des SCV-Plug-ins können Sie die Details des Prüfprotokolls unter **Dashboard > Einstellungen > Registerkarte Prüfprotokolle** anzeigen und exportieren. Sie können die Betriebsprüfung in den Prüfprotokollen anzeigen. Die Prüfprotokolle werden mit dem Support-Paket heruntergeladen.

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

Die Standardkonfigurationen der Auditdateien sind:

- Die verwendete Audit-Protokolldatei kann auf maximal 10 MB anwachsen
- Es werden maximal 10 Audit-Logdateien aufbewahrt

Übertragene Prüfprotokolle werden regelmäßig auf Integrität überprüft. SCV bietet REST-APIs zum Anzeigen von Protokollen und Überprüfen ihrer Integrität. Ein integrierter Zeitplan löst einen der folgenden Integritätsstatus aus und weist ihn zu.

Status	Beschreibung
MANIPULIERT	Der Inhalt der Überwachungsprotokolldatei wurde geändert
NORMAL	Die Audit-Protokolldatei ist unverändert
ROLLOVER-LÖSCHEN	- Die Prüfprotokolldatei wird basierend auf der Aufbewahrung gelöscht. - Standardmäßig werden nur 10 Dateien aufbewahrt
UNERWARTETES LÖSCHEN	Die Audit-Protokolldatei wird gelöscht
AKTIV	- Audit-Protokolldatei wird verwendet - Gilt nur für audit.log

Ereignisse werden in drei Hauptkategorien eingeteilt:

- Datenschutzereignisse
- Ereignisse der Wartungskonsole
- Ereignisse in der Admin-Konsole

Datenschutzereignisse

Die Ressourcen in SCV sind:

- Speichersystem
- Ressourcengruppe
- Politik
- Sicherung
- Abonnement
- Konto

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

Ressourcen	Operationen
Speichersystem	Erstellt, geändert, gelöscht
Abonnement	Erstellt, geändert, gelöscht
Konto	Erstellt, geändert, gelöscht
Ressourcengruppe	Erstellt, geändert, gelöscht, ausgesetzt, fortgesetzt
Politik	Erstellt, geändert, gelöscht

Sicherung	Erstellt, umbenannt, gelöscht, gemountet, unmountet, VMDK wiederhergestellt, VM wiederhergestellt, VMDK anhängen, VMDK trennen, Gastdatei wiederherstellen
-----------	--

Ereignisse der Wartungskonsole

Die Verwaltungsvorgänge in der Wartungskonsole werden geprüft. Verfügbare Optionen für die Wartungskonsole sind:

1. Dienste starten/stoppen
2. Benutzernamen und Passwort ändern
3. MySQL-Passwort ändern
4. Konfigurieren der MySQL-Sicherung
5. MySQL-Backup wiederherstellen
6. Ändern Sie das Benutzerkennwort „maint“.
7. Zeitzone ändern
8. NTP-Server ändern
9. SSH-Zugriff deaktivieren
10. Erhöhen Sie die Größe der Jail-Festplatte
11. Upgrade
12. Installieren Sie VMware Tools (wir arbeiten daran, diese durch Open-VM-Tools zu ersetzen)
13. IP-Adresseinstellungen ändern
14. Sucheinstellungen für Domänennamen ändern
15. Statische Routen ändern
16. Zugriff auf die Diagnose-Shell
17. Aktivieren Sie den Ferndiagnosezugriff

Ereignisse in der Admin-Konsole

Die folgenden Vorgänge in der Benutzeroberfläche der Admin-Konsole werden überwacht:

- Einstellungen
 - Administratoranmeldeinformationen ändern
 - Zeitzone ändern
 - NTP-Server ändern
 - IPv4/IPv6-Adresseinstellungen ändern
- Konfiguration
 - Ändern der vCenter-Anmeldeinformationen
 - Plug-in aktivieren/deaktivieren

Konfigurieren von Syslog-Servern

Prüfprotokolle werden innerhalb der Appliance gespeichert und regelmäßig auf Integrität überprüft. Durch die 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.

Informationen zu diesem Vorgang

Diese Aufgabe hilft Ihnen bei der Konfiguration des Syslog-Servers.

Schritte

1. Melden Sie sich beim SnapCenter Plug-in for VMware vSphere an.
2. Wählen Sie im linken Navigationsbereich **Einstellungen > Überwachungsprotokolle > Einstellungen**.
3. Wählen Sie im Bereich **Audit-Protokolleinstellungen** die Option **Audit-Protokolle an Syslog-Server senden**.
4. Geben Sie die folgenden Details ein:
 - Syslog-Server-IP
 - Syslog-Server-Port
 - RFC-Format
 - Syslog-Server-Zertifikat
5. Wählen Sie **SPEICHERN**, um die Syslog-Sereinstellungen zu speichern.

Ändern der Überwachungsprotokolleinstellungen

Sie können die Standardkonfigurationen der Protokolleinstellungen ändern.

Bevor Sie beginnen

Sie müssen über Administratorrechte verfügen.

Informationen zu diesem Vorgang

Diese Aufgabe hilft Ihnen, die Standardeinstellungen des Überwachungsprotokolls zu ändern.

Schritte

1. Melden Sie sich beim SnapCenter Plug-in for VMware vSphere an.
2. Wählen Sie im linken Navigationsbereich **Einstellungen > Überwachungsprotokolle > Einstellungen**.
3. Geben Sie im Bereich **Audit-Protokolleinstellungen** die maximale Anzahl von Audit-Protokolldateien und die Größenbeschränkung für Audit-Protokolldateien ein.
4. Wählen Sie die Option **Auditprotokolle an Syslog-Server senden**, wenn Sie die Protokolle an den 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, 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.