Monitorare e generare report

SnapCenter Plug-in for VMware vSphere

NetApp
September 29, 2025

This PDF was generated from https://docs.netapp.com/it-it/sc-plugin-vmware-vsphere-49/scpivs44_view_status_information.html on September 29, 2025. Always check docs.netapp.com for the latest.

Sommario

Monitorare e generare report . . . 1
- Visualizzare le informazioni di stato . . . 1
- Monitorare i lavori . . . 3
- Scaricare i log dei lavori . . . 3
- Accesso ai report . . . 4
  - Tipi di report dal client VMware vSphere . . . 4
- Generare un bundle di supporto dal plug-in SnapCenter per l'interfaccia grafica di VMware vSphere . . . 6
- Generare un bundle di supporto dalla console di manutenzione . . . 7
- Registri di audit . . . 8
  - Eventi di protezione dei dati . . . 9
  - Eventi della console di manutenzione . . . 10
  - Eventi della console di amministrazione . . . 10
  - Configurare i server syslog . . . 11
  - Modificare le impostazioni del registro di controllo . . . 11

Monitorare e generare report

Visualizzare le informazioni di stato

È possibile visualizzare le informazioni sullo stato nella dashboard del client vSphere. Le informazioni sullo stato vengono aggiornate una volta all'ora.

Fasi

1. Nel riquadro sinistro di Navigator del client vSphere, fare clic su **Dashboard**, selezionare un server vCenter, quindi fare clic sulla scheda **Status** nel pannello della dashboard.
2. Visualizzare le informazioni sullo stato della panoramica o fare clic su un collegamento per ulteriori dettagli, come indicato nella tabella seguente.

Questo riquadro del dashboard…	Visualizza le seguenti informazioni…
Attività lavorative recenti	I processi di backup, ripristino e montaggio più recenti sono da tre a cinque. • Fare clic su un ID lavoro per visualizzare ulteriori dettagli sul lavoro. • Fare clic su **Vedi tutto** per accedere alla scheda Job Monitor per ulteriori dettagli su tutti i lavori.
Lavori	Numero di ciascun tipo di lavoro (backup, ripristino e montaggio) eseguito nell'intervallo di tempo selezionato. Posizionare il cursore su una sezione del grafico per visualizzare ulteriori dettagli relativi a tale categoria.

Questo riquadro del dashboard…	Visualizza le seguenti informazioni…
Riepilogo della protezione più recente	Riepiloghi dello stato di protezione dei dati delle macchine virtuali o degli archivi dati primari e secondari all'interno della finestra temporale selezionata. • Fare clic sul menu a discesa per selezionare **VM** o **Datastore**. • Per lo storage secondario, selezionare **SnapVault** o **SnapMirror**. • Spostare il cursore su una sezione di un grafico per visualizzare il numero di VM o datastore in tale categoria. Nella categoria Successful (riuscito), viene elencato il backup più recente per ciascuna risorsa. • È possibile modificare la finestra dell'ora modificando il file di configurazione. L'impostazione predefinita è 7 giorni. Per ulteriori informazioni, vedere "Personalizzare la configurazione". • I contatori interni vengono aggiornati dopo ogni backup primario o secondario. Il riquadro del dashboard viene aggiornato ogni sei ore. Il tempo di refresh non può essere modificato. Nota: Se si utilizza un criterio di protezione del vault mirror, i contatori per il riepilogo della protezione vengono visualizzati nel grafico di riepilogo di SnapVault, non nel grafico di SnapMirror.
Configurazione	Il numero totale di ciascun tipo di oggetto gestito dal plug-in SnapCenter per VMware vSphere.
Storage	Il numero totale di copie Snapshot, SnapVault e Snapshot SnapMirror, generate e la quantità di storage utilizzata per le copie Snapshot primarie e secondarie. Il grafico a linee traccia separatamente il consumo di storage primario e secondario su base giornaliera in un periodo di 90 giorni. Le informazioni sullo storage vengono aggiornate ogni 24 ore alle 1:08 Il risparmio dello storage è il rapporto tra la capacità logica (risparmio di copie Snapshot e storage consumato) e la capacità fisica dello storage primario. Il grafico a barre illustra i risparmi in termini di storage. Posizionare il cursore su una riga del grafico per visualizzare i risultati dettagliati giornalieri.

Monitorare i lavori

Dopo aver eseguito un'operazione di protezione dei dati utilizzando il client VMware vSphere, è possibile monitorare lo stato del lavoro dalla scheda Job Monitor nel dashboard e visualizzare i dettagli del lavoro.

Fasi

1. Nel riquadro sinistro di Navigator del client vSphere, fare clic su **Dashboard**. Quando due o più vCenter sono configurati in modalità Linked, selezionare un vCenter Server, quindi fare clic sulla scheda **Job Monitor** nel pannello Dashboard.
   La scheda Job Monitor elenca ogni lavoro, il relativo stato, l'ora di inizio e l'ora di fine. Se i nomi dei lavori sono lunghi, potrebbe essere necessario scorrere verso destra per visualizzare l'ora di inizio e di fine. Il display viene aggiornato ogni 30 secondi.
   - Selezionare l'icona di refresh nella barra degli strumenti per aggiornare la visualizzazione su richiesta.
   - Selezionare l'icona del filtro per scegliere l'intervallo di tempo, il tipo, il tag e lo stato dei processi che si desidera visualizzare. Il filtro fa distinzione tra maiuscole e minuscole.
   - Selezionare l'icona di aggiornamento nella finestra Dettagli processo per aggiornare la visualizzazione mentre il processo è in esecuzione.

Se la dashboard non visualizza le informazioni sul lavoro, consultare "Articolo della Knowledge base: Il dashboard del client SnapCenter vSphere non visualizza i processi".

Scaricare i log dei lavori

È possibile scaricare i registri dei processi dalla scheda monitoraggio processi del dashboard del client VMware vSphere di SnapCenter.

Se si verificano comportamenti imprevisti durante l'utilizzo del client VMware vSphere, è possibile utilizzare i file di log per identificare la causa e risolvere il problema.

> Il valore predefinito per la conservazione dei registri dei lavori è 30 giorni; il valore predefinito per la conservazione dei lavori è 90 giorni. I log dei lavori e i lavori più vecchi della conservazione configurata vengono eliminati ogni sei ore. È possibile utilizzare la configurazione `jobs/cleanup` API REST per modificare la durata di conservazione dei job e dei log dei job. Non è possibile modificare il programma di eliminazione.

Fasi

1. Nel riquadro sinistro di Navigator del client vSphere, fare clic su **Dashboard**, selezionare un server vCenter, quindi fare clic sulla scheda **Job Monitor** nel pannello Dashboard.
2. Selezionare l'icona di download nella barra del titolo di Job Monitor.

   Potrebbe essere necessario scorrere verso destra per visualizzare l'icona.

   È inoltre possibile fare doppio clic su un lavoro per accedere alla finestra Dettagli lavoro, quindi fare clic su **Download Job Logs**.

Risultato

I log dei processi si trovano sull'host VM Linux in cui viene implementato il plug-in VMware di SnapCenter. La posizione predefinita del registro lavori è `/var/log/netapp`.

Se si è tentato di scaricare i log dei lavori ma il file di log indicato nel messaggio di errore è stato eliminato, potrebbe verificarsi il seguente errore: `HTTP ERROR 500 Problem accessing /export-scv-logs`. Per correggere questo errore, controllare lo stato di accesso al file e le autorizzazioni per il file indicato nel messaggio di errore e correggere il problema di accesso.

Accesso ai report

È possibile richiedere report per uno o più lavori dalla dashboard.

La scheda rapporti contiene informazioni sui lavori selezionati nella pagina lavori della dashboard. Se non viene selezionato alcun processo, la scheda Report è vuota.

Fasi

1. Nel riquadro sinistro di Navigator del client vSphere, fare clic su **Dashboard**, selezionare un server vCenter, quindi fare clic sulla scheda **Report**.
2. Per i report di backup, è possibile effettuare le seguenti operazioni:
   a. Modificare il report

      Selezionare l'icona del filtro per modificare l'intervallo di tempo, il tipo di stato del processo, i gruppi di risorse e i criteri da includere nel report.

   b. Generare un report dettagliato

      Fare doppio clic su un lavoro per generare un report dettagliato per tale lavoro.
3. Facoltativo: Nella scheda Report, fare clic su **Download** e selezionare il formato (HTML o CSV).

   È inoltre possibile fare clic sull'icona di download per scaricare i log dei plug-in.

Tipi di report dal client VMware vSphere

Il client VMware vSphere per SnapCenter offre opzioni di report personalizzabili che forniscono dettagli sui processi di protezione dei dati e sullo stato delle risorse dei plug-in. È possibile generare report solo per la protezione primaria.

> Le pianificazioni di backup vengono eseguite nel fuso orario in cui viene implementato il plug-in VMware di SnapCenter. VCenter riporta i dati nel fuso orario in cui si trova vCenter. Pertanto, se il plug-in VMware e vCenter si trovano in fusi orari diversi, i dati nel dashboard del client SnapCenter vSphere potrebbero non coincidere con quelli dei report.

La dashboard visualizza le informazioni sui backup migrati solo dopo l'esecuzione dei backup post-migrazione.

Tipo di report	Descrizione
Report di backup	Visualizza una panoramica dei dati relativi ai processi di backup. Fare clic su una sezione/stato del grafico per visualizzare un elenco di lavori con tale stato nella scheda **Report**. Per ogni lavoro, il report elenca l'ID del lavoro, il gruppo di risorse corrispondente, la politica di backup, l'ora e la durata di inizio, lo stato e i dettagli del lavoro, che includono il nome del lavoro (nome della copia Snapshot) se il lavoro è stato completato, nonché eventuali messaggi di avviso o di errore. È possibile scaricare la tabella dei report in formato HTML o CSV. È inoltre possibile scaricare i log dei lavori di Job Monitor per tutti i lavori (non solo per quelli contenuti nel report). I backup cancellati non sono inclusi nel report.
Report di montaggio	Visualizza una panoramica dei lavori di montaggio. Fare clic su una sezione/stato del grafico per visualizzare un elenco di processi con tale stato nella scheda Report. Per ogni lavoro, il report elenca l'ID del lavoro, lo stato del lavoro, il nome del lavoro e gli orari di inizio e di fine del lavoro. Il nome del lavoro include il nome della copia Snapshot. Ad esempio: `Mount Backup <snapshot-copy-name>` È possibile scaricare la tabella dei report in formato HTML o CSV. È inoltre possibile scaricare i log dei lavori di Job Monitor per tutti i lavori (non solo per quelli contenuti nel report).
Ripristina report	Visualizza informazioni generali sullo stato dei processi di ripristino. Fare clic su una sezione/stato del grafico per visualizzare un elenco di processi con tale stato nella scheda Report. Per ogni lavoro, il report elenca l'ID del lavoro, lo stato del lavoro, il nome del lavoro e gli orari di inizio e di fine del lavoro. Il nome del lavoro include il nome della copia Snapshot. Ad esempio: `Restore Backup <snapshot-copy-name>` È possibile scaricare la tabella dei report in formato HTML o CSV. È inoltre possibile scaricare i log dei lavori di Job Monitor per tutti i lavori (non solo per quelli contenuti nel report).

Tipo di report	Descrizione
Ultimo stato di protezione di Report sulle macchine virtuali o sui datastore	Visualizza informazioni generali sullo stato della protezione, durante il numero di giorni configurato, per macchine virtuali e datastore gestiti dal plug-in VMware di SnapCenter. L'impostazione predefinita è 7 giorni. Per modificare il valore nel file di proprietà, vedere "Modificare i valori predefiniti della configurazione". Fare clic su una sezione/stato del grafico di protezione principale per visualizzare un elenco di VM o datastore con tale stato nella scheda **Report**. Il report sullo stato di protezione di VM o datastore per VM e datastore protetti visualizza i nomi delle macchine virtuali o datastore di cui è stato eseguito il backup durante il numero di giorni configurato, il nome della copia Snapshot più recente e gli orari di inizio e fine dell'ultima esecuzione del backup. Il report sullo stato di protezione di VM o datastore per VM o datastore non protetti visualizza i nomi delle macchine virtuali o datastore che non dispongono di backup riusciti durante il numero di giorni configurato. È possibile scaricare la tabella dei report in formato HTML o CSV. È inoltre possibile scaricare i log dei lavori di Job Monitor per tutti i lavori (non solo per quelli contenuti nel report). Questo report viene aggiornato ogni ora quando la cache del plug-in viene aggiornata. Pertanto, il report potrebbe non visualizzare le macchine virtuali o gli archivi dati di cui è stato eseguito il backup di recente.

Generare un bundle di supporto dal plug-in SnapCenter per l'interfaccia grafica di VMware vSphere

Prima di iniziare

Per accedere all'interfaccia grafica di gestione del plug-in SnapCenter per VMware vSphere, è necessario conoscere l'indirizzo IP e le credenziali di accesso. È inoltre necessario annotare il token MFA generato dalla console di manutenzione.

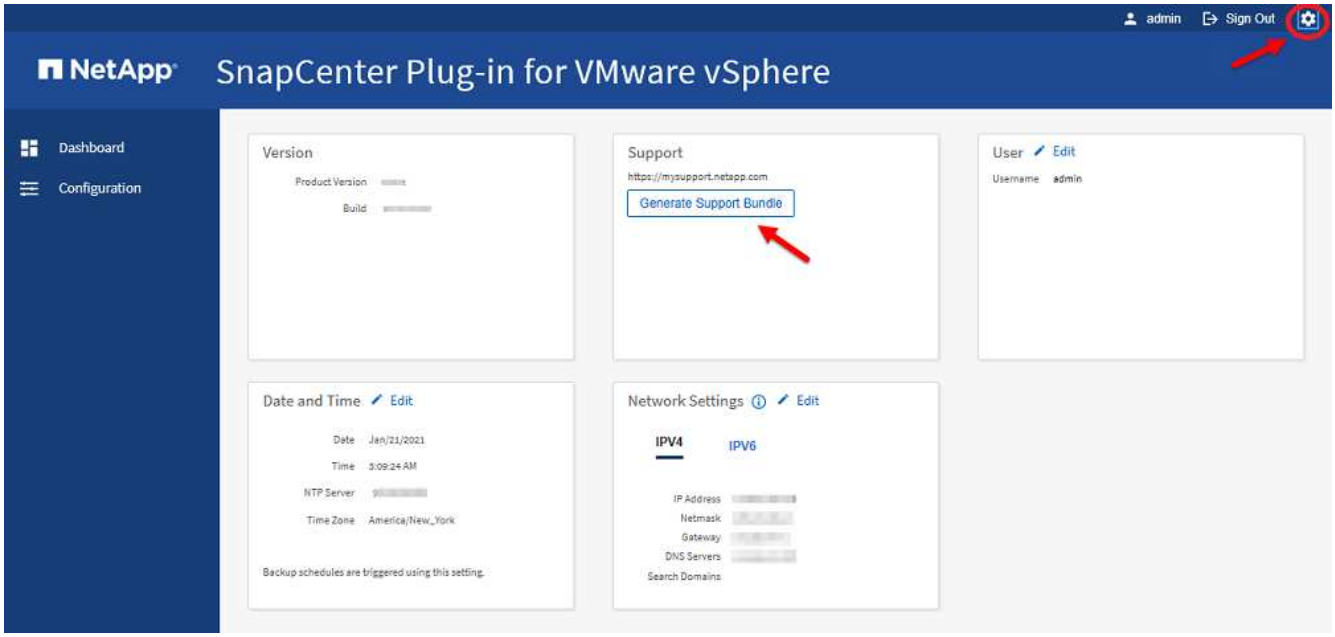
- L'indirizzo IP è stato visualizzato al momento dell'implementazione del plug-in VMware di SnapCenter.
- Utilizzare le credenziali di accesso fornite durante l'implementazione del plug-in VMware di SnapCenter o come successivamente modificato.
- Generare un token MFA a 6 cifre utilizzando le opzioni di configurazione del sistema della console di manutenzione.

Fasi

1. Accedere al plug-in SnapCenter per l'interfaccia grafica di VMware vSphere.

Utilizzare il formato `https://<OVA-IP-address>:8080`.

2. Fare clic sull'icona Impostazioni nella barra degli strumenti superiore.



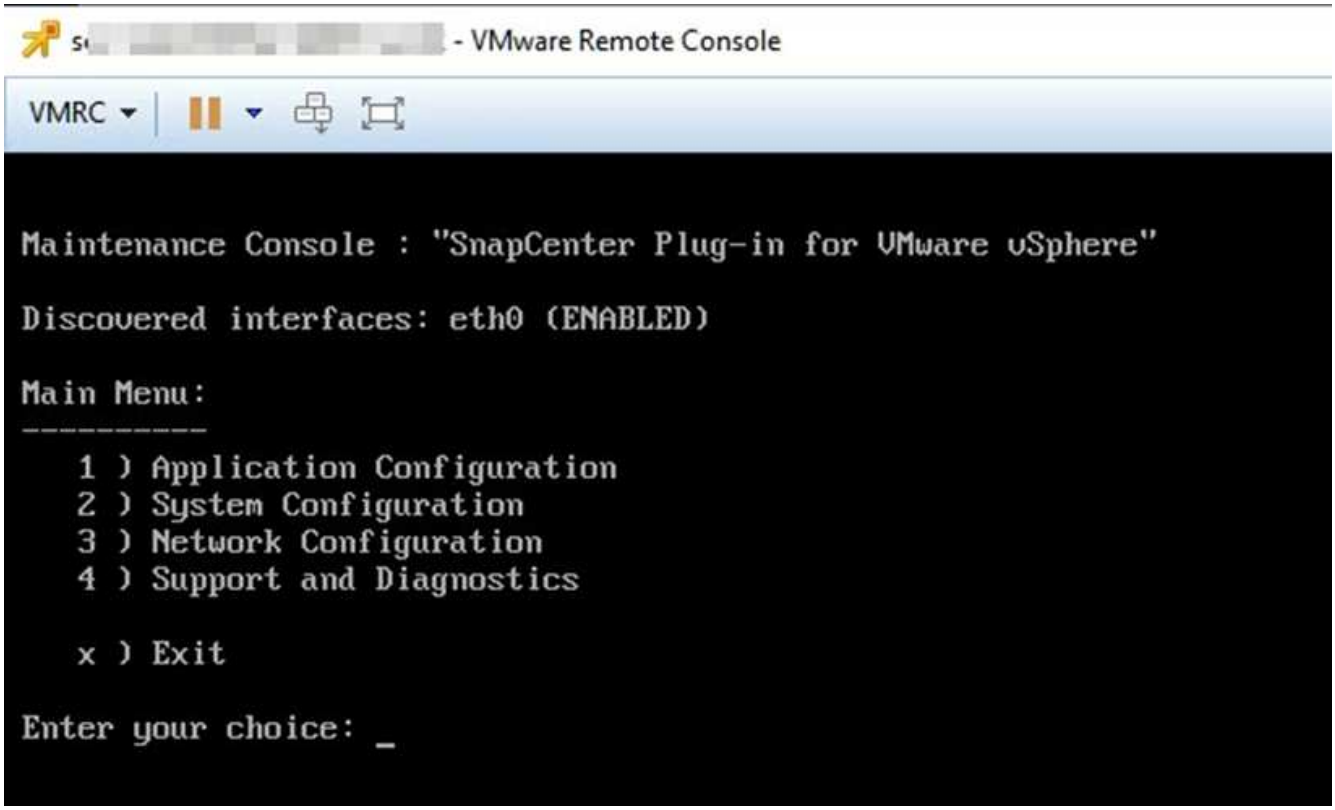
3. Nella sezione **supporto** della pagina **Impostazioni**, fare clic su **genera bundle di supporto**.
4. Una volta generato il bundle di supporto, fare clic sul link fornito per scaricare il bundle su NetApp.

Generare un bundle di supporto dalla console di manutenzione

Fasi

1. Dal client VMware vSphere, selezionare la macchina virtuale in cui si trova il plug-in SnapCenter.
2. Fare clic con il pulsante destro del mouse sulla macchina virtuale, quindi sulla scheda **Riepilogo** dell'appliance virtuale fare clic su **Avvia console remota o Avvia console Web** per aprire una finestra della console di manutenzione e accedere.

   Per informazioni sull'accesso e l'accesso alla console di manutenzione, vedere "Accedere alla console di manutenzione".



3. Dal menu principale, immettere l'opzione **4) Support and Diagnostics** (supporto e diagnostica).
4. Dal menu Support and Diagnostics (supporto e diagnostica), immettere l'opzione **1) generate support bundle** (genera bundle di supporto).

Per accedere al bundle di supporto, dal menu Support and Diagnostics (supporto e diagnostica) selezionare l'opzione **2) Access Diagnostic Shell**. Nella console, selezionare `/support/support/<bundle_name>.tar.gz`.

Registri di audit

Il registro di audit è una raccolta di eventi in ordine cronologico, che viene scritta in un file all'interno dell'appliance. I file di log di audit vengono generati in `/var/log/netapp/audit` la posizione e i nomi dei file seguono una delle seguenti convenzioni di denominazione:

- Audit.log: File di log di audit attivo in uso.
- Audit-%d{yyyy-MM-dd-HH-mm-ss}.log.gz: Eseguito il rollover del file di log di audit. La data e l'ora nel nome del file indicano quando è stato creato il file, ad esempio: Audit-2022-12-15-16-28-01.log.gz.

Nell'interfaccia utente del plug-in SCV, è possibile visualizzare ed esportare i dettagli del registro di controllo da Scheda **Dashboard** > **Settings** > **Audit Logs**
È possibile visualizzare l'audit delle operazioni nei registri di audit. I registri di controllo vengono scaricati con il pacchetto di supporto.

Se sono configurate le impostazioni e-mail, SCV invia una notifica e-mail in caso di errore nella verifica dell'integrità del registro di controllo. Un errore di verifica dell'integrità del registro di controllo può verificarsi quando uno dei file viene manomesso o cancellato.

Le configurazioni predefinite dei file di audit sono:

- Il file di log di audit in uso può aumentare fino a un massimo di 10 MB
- Vengono conservati un massimo di 10 file di log di audit

Per modificare le configurazioni predefinite, aggiungere una coppia di valori chiave in /opt/netapp/scvservice/standalone_aegis/etc/scbr/scbr.properties e riavviare scvservice.

Le configurazioni per i file di log di audit sono:

- AuditMaxROFiles=<xx>, dove xx è il numero massimo di file di log di controllo di cui è stato eseguito il rollover, ad esempio: AuditMaxROFiles=15.
- AuditLogSize=<XX>, dove xx è la dimensione del file in MB, ad esempio: AuditLogSize=15MB.

I log di controllo di cui è stato eseguito il rollover vengono periodicamente verificati per verificarne l'integrità. SCV fornisce API REST per visualizzare i registri e verificarne l'integrità. Una pianificazione integrata attiva e assegna uno dei seguenti stati di integrità.

Stato	Descrizione
MANOMESSO	Il contenuto del file di log di audit viene modificato
NORMALE	Il file di log di audit non è stato modificato
SPOSTA IL MOUSE SU ELIMINA	- Il file di registro di controllo viene cancellato in base alla conservazione Per impostazione predefinita, vengono conservati solo 10 file
ELIMINAZIONE IMPREVISTA	Il file di log di audit viene cancellato
ATTIVO	- Il file di log di audit è in uso - Applicabile solo a audit.log

Gli eventi sono suddivisi in tre categorie principali:

- Eventi di protezione dei dati
- Eventi della console di manutenzione
- Eventi della console di amministrazione

Eventi di protezione dei dati

Le risorse di SCV sono:

- Sistema storage
- Gruppo di risorse
- Policy
- Backup

La seguente tabella elenca le operazioni che possono essere eseguite su ciascuna risorsa:

Risorse	Operazioni

Sistema storage	Creato, modificato, eliminato
Gruppo di risorse	Creato, modificato, cancellato, sospeso, ripreso
Policy	Creato, modificato, eliminato
Backup	Creato, rinominato, cancellato, montato, non montato, Ripristino VMDK, ripristino VM, collegamento VMDK, scollegamento VMDK, Ripristino file guest

Eventi della console di manutenzione

Le operazioni amministrative nella console di manutenzione vengono controllate.
Le opzioni della console di manutenzione disponibili sono:

1. Avvio/interruzione dei servizi
2. Modificare nome utente e password
3. Cambiare la password MySQL
4. Configurare MySQL Backup
5. Ripristinare MySQL Backup
6. Modificare la password utente "maint"
7. Modificare il fuso orario
8. Modificare il server NTP
9. Disattiva l'accesso SSH
10. Aumentare le dimensioni del disco jail
11. Eseguire l'upgrade
12. Installare VMware Tools (stiamo lavorando per sostituire questo con strumenti Open-vm)
13. Modificare le impostazioni dell'indirizzo IP
14. Modificare le impostazioni di ricerca dei nomi di dominio
15. Modificare i percorsi statici
16. Accedere alla shell di diagnostica
17. Abilitare l'accesso remoto alla diagnostica

Eventi della console di amministrazione

Vengono controllate le seguenti operazioni nell'interfaccia utente della Admin Console:

- Impostazioni
  - Modificare le credenziali di amministratore
  - Modificare il fuso orario
  - Modificare il server NTP
  - Modificare le impostazioni IPv4 / IPv6
- Configurazione
  - Modificare le credenziali vCenter

- Plug-in Enable/Disable (attiva/Disattiva plug-in

Configurare i server syslog

I registri di audit vengono memorizzati all'interno dell'appliance e verificati periodicamente per verificarne l'integrità. L'inoltro degli eventi consente di ottenere eventi dal computer di origine o di inoltro e di memorizzarli in un computer centralizzato, ovvero Syslog Server. I dati vengono crittografati durante il trasferimento tra l'origine e la destinazione.

Prima di iniziare

È necessario disporre dei privilegi di amministratore.

A proposito di questa attività

Questa attività consente di configurare il server syslog.

Fasi

1. Accedere al plug-in SnapCenter per VMware vSphere.
2. Nel riquadro di navigazione a sinistra, selezionare **Impostazioni** > **registri di controllo** > **Impostazioni**.
3. Nel riquadro **Audit Log Settings**, selezionare **Send audit logs to Syslog server** (Invia log di controllo al server Syslog)
4. Inserire i seguenti dati:
   - IP server syslog
   - Porta server syslog
   - Formato RFC
   - Certificato server syslog
5. Fare clic su **SAVE** (SALVA) per salvare le impostazioni del server Syslog.

Modificare le impostazioni del registro di controllo

È possibile modificare le configurazioni predefinite delle impostazioni del registro.

Prima di iniziare

È necessario disporre dei privilegi di amministratore.

A proposito di questa attività

Questa attività consente di modificare le impostazioni predefinite del registro di controllo.

Fasi

1. Accedere al plug-in SnapCenter per VMware vSphere.
2. Nel riquadro di navigazione a sinistra, selezionare **Impostazioni** > **registri di controllo** > **Impostazioni**.
3. Nel riquadro **Audit Log Settings** (Impostazioni registro di controllo), immettere il **numero di voci di controllo** e il **limite di dimensione del registro di controllo** in base ai requisiti.

Informazioni sul copyright

Copyright © 2025 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina http://www.netapp.com/TM sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.