Proteggere i file system Unix

SnapCenter software

NetApp
November 06, 2025

Sommario

Proteggere i file system Unix . . . 1
Cosa puoi fare con il plug-in SnapCenter per i file system Unix . . . 1
Configurazioni supportate . . . 1
Limitazioni . . . 2
Caratteristiche . . . 2
Installa il plug-in SnapCenter per i file system Unix . . . 2
Prerequisiti per l'aggiunta di host e l'installazione del pacchetto Plug-in per Linux . . . 2
Aggiungi host e installa il pacchetto Plug-in per Linux utilizzando l'interfaccia grafica . . . 4
Configurare il servizio SnapCenter Plug-in Loader . . . 6
Configurare il certificato CA con il servizio SnapCenter Plug-in Loader (SPL) sull'host Linux . . . 9
Abilita i certificati CA per i plug-in . . . 12
Installa il SnapCenter Plug-in for VMware vSphere . . . 13
Distribuisci il certificato CA . . . 13
Configurare il file CRL . . . 13
Prepararsi alla protezione dei file system Unix . . . 13
Eseguire il backup dei file system Unix . . . 14
Scopri i file system UNIX disponibili per il backup . . . 14
Creare policy di backup per i file system Unix . . . 14
Crea gruppi di risorse e allega policy per i file system Unix . . . 17
Crea gruppi di risorse e abilita la protezione secondaria per i file system Unix sui sistemi ASA r2 . . . 19
Eseguire il backup dei file system Unix . . . 21
Eseguire il backup dei gruppi di risorse dei file system Unix . . . 23
Monitorare il backup dei file system Unix . . . 23
Visualizza i file system Unix protetti nella pagina Topologia . . . 25
Ripristinare e recuperare i file system Unix . . . 27
Ripristinare i file system Unix . . . 27
Monitorare le operazioni di ripristino dei file system Unix . . . 28
Clonare i file system Unix . . . 29
Clona il backup del file system Unix . . . 29
Dividi un clone . . . 31
Monitorare le operazioni di clonazione dei file system Unix . . . 32

Proteggere i file system Unix

Cosa puoi fare con il plug-in SnapCenter per i file system Unix

Una volta installato il plug-in per i file system Unix nel tuo ambiente, puoi utilizzare SnapCenter per eseguire il backup, il ripristino e la clonazione dei file system Unix. È anche possibile eseguire attività di supporto a tali operazioni.

- Scopri le risorse
- Eseguire il backup dei file system Unix
- Pianificare le operazioni di backup
- Ripristinare i backup del file system
- Clonazione dei backup del file system
- Monitorare le operazioni di backup, ripristino e clonazione

Configurazioni supportate

Articolo	Configurazione supportata
Ambienti	• Server fisico • Server virtuale Datastore vVol sia su NFS che su SAN. Il provisioning del datastore vVol può essere effettuato solo con ONTAP Tools per VMware vSphere.
Sistemi operativi	• Red Hat Enterprise Linux • Oracle Linux • SUSE Linux Enterprise Server (SLES)
Sistemi di file	• SAN: ◦ Sia i file system basati su LVM che quelli non basati su LVM ◦ LVM su VMDK ext3, ext4 e xfs • NFS: NFS v3, NFS v4.x
Protocolli	• FC • FCoE • iSCSI • NFS

Articolo	Configurazione supportata
Multipercorso	SÌ

Limitazioni

- Non è supportata la combinazione di RDM e dischi virtuali in un gruppo di volumi.
- Il ripristino a livello di file non è supportato.

  Tuttavia, è possibile eseguire manualmente il ripristino a livello di file clonando il backup e quindi copiando manualmente i file.

- Non è supportato il mix di file system distribuiti su VMDK provenienti sia da datastore NFS che VMFS.
- NVMe non è supportato.
- Il provisioning non è supportato.

Caratteristiche

- Consente al plug-in per Oracle Database di eseguire operazioni di protezione dei dati sui database Oracle gestendo lo stack di archiviazione host sottostante sui sistemi Linux o AIX
- Supporta i protocolli Network File System (NFS) e Storage Area Network (SAN) su un sistema di archiviazione che esegue ONTAP.
- Per i sistemi Linux, i database Oracle su VMDK e RDM LUN sono supportati quando si distribuisce il SnapCenter Plug-in for VMware vSphere e si registra il plug-in con SnapCenter.
- Supporta Mount Guard per AIX su file system SAN e layout LVM.
- Supporta Enhanced Journaled File System (JFS2) con registrazione in linea sui file system SAN e layout LVM solo per sistemi AIX.

  Sono supportati dispositivi SAN nativi, file system e layout LVM creati su dispositivi SAN.

- Automatizza le operazioni di backup, ripristino e clonazione basate sulle applicazioni per i file system UNIX nel tuo ambiente SnapCenter

Installa il plug-in SnapCenter per i file system Unix

Prerequisiti per l'aggiunta di host e l'installazione del pacchetto Plug-in per Linux

Prima di aggiungere un host e installare il pacchetto plug-in per Linux, è necessario soddisfare tutti i requisiti.

- Se si utilizza iSCSI, il servizio iSCSI deve essere in esecuzione.
- È possibile utilizzare l'autenticazione basata su password per l'utente root o non root oppure l'autenticazione basata su chiave SSH.

  Il plug-in SnapCenter per i file system Unix può essere installato da un utente non root. Tuttavia, è necessario configurare i privilegi sudo per l'utente non root per installare e avviare il processo del plug-in. Dopo aver installato il plug-in, i processi verranno eseguiti come utente non root.

- Creare credenziali con modalità di autenticazione Linux per l'utente installatore.
- Devi aver installato Java 11 sul tuo host Linux.

  Assicurarsi di aver installato solo l'edizione certificata di JAVA 11 sull'host Linux.

  Per informazioni su come scaricare JAVA, vedere: "Download Java per tutti i sistemi operativi"

- Dovresti avere **bash** come shell predefinita per l'installazione del plug-in.

Requisiti dell'host Linux

Prima di installare il pacchetto plug-in SnapCenter per Linux, è necessario assicurarsi che l'host soddisfi i requisiti.

Articolo	Requisiti
Sistemi operativi	• Red Hat Enterprise Linux • Oracle Linux • SUSE Linux Enterprise Server (SLES)
RAM minima per il plug-in SnapCenter sull'host	2 GB
Spazio minimo di installazione e registro per il plug-in SnapCenter sull'host	2 GB È necessario allocare spazio su disco sufficiente e monitorare il consumo di spazio di archiviazione da parte della cartella dei registri. Lo spazio di registro richiesto varia a seconda del numero di entità da proteggere e della frequenza delle operazioni di protezione dei dati. Se non c'è spazio sufficiente sul disco, i registri per le operazioni eseguite di recente non verranno creati.
Pacchetti software richiesti	Java 11 Oracle Java e OpenJDK Assicurarsi di aver installato solo l'edizione certificata di JAVA 11 sull'host Linux. Se hai aggiornato JAVA alla versione più recente, devi assicurarti che l'opzione JAVA_HOME situata in /var/opt/snapcenter/spl/etc/spl.properties sia impostata sulla versione JAVA corretta e sul percorso corretto.

Per le informazioni più recenti sulle versioni supportate, vedere "Strumento matrice di interoperabilità NetApp" .

Aggiungi host e installa il pacchetto Plug-in per Linux utilizzando l'interfaccia grafica

È possibile utilizzare la pagina Aggiungi host per aggiungere host e quindi installare il pacchetto plug-in SnapCenter per Linux. I plug-in vengono installati automaticamente sugli host remoti.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Verificare che la scheda **Host gestiti** sia selezionata in alto.
3. Fare clic su **Aggiungi**.
4. Nella pagina Host, eseguire le seguenti azioni:

Per questo campo…	Fai questo…
Tipo di host	Selezionare **Linux** come tipo di host.
Nome host	Immettere il nome di dominio completo (FQDN) o l'indirizzo IP dell'host. SnapCenter dipende dalla corretta configurazione del DNS. Pertanto, la prassi migliore è quella di immettere il nome di dominio completo (FQDN). Se si aggiunge un host tramite SnapCenter e l'host fa parte di un sottodominio, è necessario fornire l'FQDN.
Credenziali	Seleziona il nome delle credenziali che hai creato oppure creane di nuove. La credenziale deve disporre di diritti amministrativi sull'host remoto. Per maggiori dettagli, consultare le informazioni sulla creazione delle credenziali. È possibile visualizzare i dettagli sulle credenziali posizionando il cursore sul nome della credenziale specificato. La modalità di autenticazione delle credenziali è determinata dal tipo di host specificato nella procedura guidata Aggiungi host.

5. Nella sezione Seleziona plug-in da installare, seleziona **File System Unix**.
6. (Facoltativo) Fare clic su **Altre opzioni**.

Per questo campo…	Fai questo…
Porta	Mantenere il numero di porta predefinito oppure specificare il numero di porta. Il numero di porta predefinito è 8145. Se SnapCenter Server è stato installato su una porta personalizzata, tale numero di porta verrà visualizzato come porta predefinita. Se hai installato manualmente i plug-in e hai specificato una porta personalizzata, devi specificare la stessa porta. In caso contrario, l'operazione fallisce.
Percorso di installazione	Il percorso predefinito è */opt/ NetApp/snapcenter*. Facoltativamente, è possibile personalizzare il percorso. Se si utilizza il percorso personalizzato, assicurarsi che il contenuto predefinito dei sudoer venga aggiornato con il percorso personalizzato.
Salta i controlli di preinstallazione facoltativi	Selezionare questa casella di controllo se i plug-in sono già stati installati manualmente e non si desidera verificare se l'host soddisfa i requisiti per l'installazione del plug-in.

7. Fare clic su **Invia**.

   Se non hai selezionato la casella di controllo Salta controlli preliminari, l'host viene convalidato per verificare se soddisfa i requisiti per l'installazione del plug-in.

   Lo script di pre-controllo non convalida lo stato del firewall della porta del plug-in se è specificato nelle regole di rifiuto del firewall.

   Se i requisiti minimi non vengono soddisfatti, vengono visualizzati messaggi di errore o di avviso appropriati. Se l'errore è correlato allo spazio su disco o alla RAM, è possibile aggiornare il file web.config situato in *C:\Programmi\ NetApp\ SnapCenter WebApp* per modificare i valori predefiniti. Se l'errore è correlato ad altri parametri, dovresti risolvere il problema.

   In una configurazione HA, se si aggiorna il file web.config, è necessario aggiornare il file su entrambi i nodi.

8. Verificare l'impronta digitale, quindi fare clic su **Conferma e invia**.

   SnapCenter non supporta l'algoritmo ECDSA.

   La verifica dell'impronta digitale è obbligatoria anche se lo stesso host è stato aggiunto in precedenza a SnapCenter e l'impronta digitale è stata confermata.

9. Monitorare l'avanzamento dell'installazione.

   I file di registro specifici dell'installazione si trovano in */custom_location/snapcenter/logs*.

Risultato

Tutti i file system montati sull'host vengono automaticamente rilevati e visualizzati nella pagina Risorse. Se non viene visualizzato nulla, fare clic su **Aggiorna risorse**.

Monitorare lo stato dell'installazione

È possibile monitorare l'avanzamento dell'installazione del pacchetto plug-in SnapCenter tramite la pagina Lavori. Potrebbe essere opportuno controllare l'avanzamento dell'installazione per stabilire quando è completa o se si è verificato un problema.

Informazioni su questo compito

Le seguenti icone compaiono nella pagina Lavori e indicano lo stato dell'operazione:

- In corso
- Completato con successo
- Fallito
- Completato con avvisi o non è stato possibile avviarlo a causa di avvisi
- In coda

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Lavori**.
3. Nella pagina **Lavori**, per filtrare l'elenco in modo che vengano elencate solo le operazioni di installazione dei plug-in, procedere come segue:
   a. Fare clic su **Filtro**.
   b. Facoltativo: specificare la data di inizio e di fine.
   c. Dal menu a discesa Tipo, seleziona **Installazione plug-in**.
   d. Dal menu a discesa Stato, selezionare lo stato dell'installazione.
   e. Fare clic su **Applica**.
4. Selezionare il lavoro di installazione e fare clic su **Dettagli** per visualizzare i dettagli del lavoro.
5. Nella pagina **Dettagli lavoro**, fare clic su **Visualizza registri**.

Configurare il servizio SnapCenter Plug-in Loader

Il servizio SnapCenter Plug-in Loader carica il pacchetto plug-in per consentire a Linux di interagire con SnapCenter Server. Il servizio SnapCenter Plug-in Loader viene installato quando si installa il pacchetto SnapCenter Plug-ins per Linux.

Informazioni su questo compito

Dopo aver installato il pacchetto di plug-in SnapCenter per Linux, il servizio SnapCenter Plug-in Loader si avvia automaticamente. Se il servizio SnapCenter Plug-in Loader non si avvia automaticamente, è necessario:

- Assicurarsi che la directory in cui è in esecuzione il plug-in non venga eliminata
- Aumentare lo spazio di memoria assegnato alla Java Virtual Machine

Il file spl.properties, che si trova in */custom_location/ NetApp/snapcenter/spl/etc/*, contiene i seguenti parametri. A questi parametri vengono assegnati valori predefiniti.

Nome del parametro	Descrizione
LOG_LEVEL	Visualizza i livelli di registro supportati. I valori possibili sono TRACE, DEBUG, INFO, WARN, ERROR e FATAL.
SPL_PROTOCOL	Visualizza il protocollo supportato da SnapCenter Plug-in Loader. È supportato solo il protocollo HTTPS. È possibile aggiungere il valore se manca il valore predefinito.
PROTOCOLLO_SERVER_SNAPCENTER	Visualizza il protocollo supportato da SnapCenter Server. È supportato solo il protocollo HTTPS. È possibile aggiungere il valore se manca il valore predefinito.
SKIP_JAVAHOME_UPDATE	Per impostazione predefinita, il servizio SPL rileva il percorso Java e aggiorna il parametro JAVA_HOME. Pertanto il valore predefinito è impostato su FALSE. È possibile impostare su TRUE se si desidera disabilitare il comportamento predefinito e correggere manualmente il percorso Java.
SPL_KEYSTORE_PASS	Visualizza la password del file keystore. È possibile modificare questo valore solo se si modifica la password o si crea un nuovo file keystore.
SPL_PORT	Visualizza il numero di porta su cui è in esecuzione il servizio SnapCenter Plug-in Loader . È possibile aggiungere il valore se manca il valore predefinito. Non modificare il valore dopo aver installato i plug-in.

Nome del parametro	Descrizione
SNAPCENTER_SERVER_HOST	Visualizza l'indirizzo IP o il nome host del server SnapCenter .
SPL_KEYSTORE_PATH	Visualizza il percorso assoluto del file keystore.
SNAPCENTER_SERVER_PORT	Visualizza il numero di porta su cui è in esecuzione SnapCenter Server.
LOGS_MAX_COUNT	Visualizza il numero di file di registro di SnapCenter Plug-in Loader conservati nella cartella */custom_location/snapcenter/spl/logs*. Il valore predefinito è impostato su 5000. Se il conteggio è superiore al valore specificato, vengono conservati gli ultimi 5000 file modificati. Il controllo del numero di file viene eseguito automaticamente ogni 24 ore dall'avvio del servizio SnapCenter Plug-in Loader . Se si elimina manualmente il file spl.properties, il numero di file da conservare viene impostato su 9999.
JAVA_HOME	Visualizza il percorso assoluto della directory JAVA_HOME utilizzata per avviare il servizio SPL. Questo percorso viene determinato durante l'installazione e come parte dell'avvio di SPL.
LOG_MAX_SIZE	Visualizza la dimensione massima del file di registro dei lavori. Una volta raggiunta la dimensione massima, il file di registro viene compresso e i registri vengono scritti nel nuovo file di quel processo.
CONSERVA_I_LOG_DEGLI_ULTIMI_GIORNI	Visualizza il numero di giorni per i quali vengono conservati i registri.
ABILITA_VALIDAZIONE_CERTIFICATO	Visualizza true quando la convalida del certificato CA è abilitata per l'host. È possibile abilitare o disabilitare questo parametro modificando spl.properties oppure utilizzando l'interfaccia utente grafica o il cmdlet SnapCenter .

Se uno qualsiasi di questi parametri non è assegnato al valore predefinito o se si desidera assegnare o modificare il valore, è possibile modificare il file spl.properties. È inoltre possibile verificare il file spl.properties

e modificarlo per risolvere eventuali problemi relativi ai valori assegnati ai parametri. Dopo aver modificato il file spl.properties, è necessario riavviare il servizio SnapCenter Plug-in Loader .

Passi

1. Eseguire una delle seguenti azioni, a seconda delle necessità:
   - Avviare il servizio SnapCenter Plug-in Loader :
     - Come utente root, esegui: `/custom_location/NetApp/snapcenter/spl/bin/spl start`
     - Come utente non root, esegui: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl start`
   - Arrestare il servizio SnapCenter Plug-in Loader :
     - Come utente root, esegui: `/custom_location/NetApp/snapcenter/spl/bin/spl stop`
     - Come utente non root, esegui: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl stop`

     È possibile utilizzare l'opzione -force con il comando stop per arrestare forzatamente il servizio SnapCenter Plug-in Loader . Tuttavia, è necessario procedere con cautela prima di procedere, poiché ciò interrompe anche le operazioni in corso.

   - Riavviare il servizio SnapCenter Plug-in Loader :
     - Come utente root, esegui: `/custom_location/NetApp/snapcenter/spl/bin/spl restart`
     - Come utente non root, esegui: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl restart`
   - Trova lo stato del servizio SnapCenter Plug-in Loader :
     - Come utente root, esegui: `/custom_location/NetApp/snapcenter/spl/bin/spl status`
     - Come utente non root, esegui: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl status`
   - Trova la modifica nel servizio SnapCenter Plug-in Loader :
     - Come utente root, esegui: `/custom_location/NetApp/snapcenter/spl/bin/spl change`
     - Come utente non root, esegui: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl change`

Configurare il certificato CA con il servizio SnapCenter Plug-in Loader (SPL) sull'host Linux

È necessario gestire la password del keystore SPL e il relativo certificato, configurare il certificato CA, configurare i certificati radice o intermedi per l'archivio attendibile SPL e configurare la coppia di chiavi firmata dalla CA per l'archivio attendibile SPL con il servizio SnapCenter Plug-in Loader per attivare il certificato digitale installato.

SPL utilizza il file 'keystore.jks', che si trova in '/var/opt/snapcenter/spl/etc' sia come archivio attendibile che come archivio chiavi.

Gestisci la password per il keystore SPL e l'alias della coppia di chiavi firmata dalla CA in uso

Passi

1. È possibile recuperare la password predefinita del keystore SPL dal file delle proprietà SPL.

   È il valore corrispondente alla chiave 'SPL_KEYSTORE_PASS'.

2. Cambia la password del keystore:

```
 keytool -storepasswd -keystore keystore.jks
. Modificare la password per tutti gli alias delle voci di chiave
privata nel keystore con la stessa password utilizzata per il keystore:
```

```
keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks
```

   Aggiornare lo stesso per la chiave SPL_KEYSTORE_PASS nel file spl.properties.

3. Riavviare il servizio dopo aver modificato la password.

> La password per il keystore SPL e per tutte le password alias associate della chiave privata devono essere le stesse.

Configurare i certificati radice o intermedi per l'archivio attendibile SPL

È necessario configurare i certificati radice o intermedi senza la chiave privata nell'archivio attendibile SPL.

Passi

1. Passare alla cartella contenente il keystore SPL: */var/opt/snapcenter/spl/etc*.
2. Individuare il file 'keystore.jks'.
3. Elenca i certificati aggiunti nel keystore:

```
 keytool -list -v -keystore keystore.jks
. Aggiungi un certificato radice o intermedio:
```

```
 keytool -import -trustcacerts -alias
<AliasNameForCerticateToBeImported> -file /<CertificatePath> -keystore
keystore.jks
. Riavviare il servizio dopo aver configurato i certificati radice o
intermedi su SPL trust-store.
```

> Dovresti aggiungere il certificato CA radice e poi i certificati CA intermedi.

Configurare la coppia di chiavi firmate dalla CA nell'archivio attendibile SPL

È necessario configurare la coppia di chiavi firmata dalla CA nell'archivio attendibile SPL.

Passi

1. Passare alla cartella contenente il keystore dell'SPL /var/opt/snapcenter/spl/etc.
2. Individuare il file 'keystore.jks'.
3. Elenca i certificati aggiunti nel keystore:

```
 keytool -list -v -keystore keystore.jks
. Aggiungere il certificato CA con chiave sia privata che pubblica.
```

```
 keytool -importkeystore -srckeystore <CertificatePathToImport>
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
. Elenca i certificati aggiunti nel keystore.
```

```
 keytool -list -v -keystore keystore.jks
. Verificare che il keystore contenga l'alias corrispondente al nuovo
certificato CA aggiunto al keystore.
. Modificare la password della chiave privata aggiunta per il
certificato CA con la password del keystore.
```

La password predefinita del keystore SPL è il valore della chiave SPL_KEYSTORE_PASS nel file spl.properties.

```
 keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore
keystore.jks
. Se il nome alias nel certificato CA è lungo e contiene spazi o
caratteri speciali ("*",","), modificare il nome alias in un nome
semplice:
```

```
 keytool -changealias -alias "<OrignalAliasName>" -destalias
"<NewAliasName>" -keystore keystore.jks
. Configurare il nome alias dal keystore situato nel file
spl.properties.
```

Aggiornare questo valore in base alla chiave SPL_CERTIFICATE_ALIAS.

4. Riavviare il servizio dopo aver configurato la coppia di chiavi firmate dalla CA nell'archivio attendibile SPL.

Configurare l'elenco di revoche dei certificati (CRL) per SPL

Dovresti configurare il CRL per SPL

Informazioni su questo compito

- SPL cercherà i file CRL in una directory preconfigurata.
- La directory predefinita per i file CRL per SPL è */var/opt/snapcenter/spl/etc/crl*.

Passi

1. È possibile modificare e aggiornare la directory predefinita nel file spl.properties in base alla chiave SPL_CRL_PATH.
2. È possibile inserire più di un file CRL in questa directory.

   I certificati in arrivo saranno verificati rispetto a ciascun CRL.

Abilita i certificati CA per i plug-in

È necessario configurare i certificati CA e distribuirli nel server SnapCenter e negli host dei plug-in corrispondenti. Dovresti abilitare la convalida del certificato CA per i plug-in.

Prima di iniziare

- È possibile abilitare o disabilitare i certificati CA utilizzando il cmdlet run *Set-SmCertificateSettings*.
- È possibile visualizzare lo stato del certificato per i plug-in utilizzando *Get-SmCertificateSettings*.

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Nella pagina Host, fare clic su **Host gestiti**.
3. Selezionare uno o più host di plug-in.
4. Fare clic su **Altre opzioni**.
5. Selezionare **Abilita convalida certificato**.

Dopo aver finito

Nella scheda Host gestiti viene visualizzato un lucchetto e il colore del lucchetto indica lo stato della connessione tra SnapCenter Server e l'host del plug-in.

- * * indica che il certificato CA non è abilitato né assegnato all'host del plug-in.
- * * indica che il certificato CA è stato convalidato correttamente.
- * * indica che il certificato CA non è stato convalidato.
- * * indica che non è stato possibile recuperare le informazioni di connessione.

> Quando lo stato è giallo o verde, le operazioni di protezione dei dati sono state completate correttamente.

Installa il SnapCenter Plug-in for VMware vSphere

Se il database o il file system è archiviato su macchine virtuali (VM) o se si desidera proteggere VM e datastore, è necessario distribuire il SnapCenter Plug-in for VMware vSphere .

Per informazioni da distribuire, vedere "Panoramica della distribuzione" .

Distribuisci il certificato CA

Per configurare il certificato CA con il SnapCenter Plug-in for VMware vSphere, vedere "Crea o importa un certificato SSL" .

Configurare il file CRL

Il SnapCenter Plug-in for VMware vSphere cerca i file CRL in una directory preconfigurata. La directory predefinita dei file CRL per il SnapCenter Plug-in for VMware vSphere è */opt/netapp/config/crl*.

È possibile inserire più di un file CRL in questa directory. I certificati in arrivo saranno verificati rispetto a ciascun CRL.

Prepararsi alla protezione dei file system Unix

Prima di eseguire qualsiasi operazione di protezione dei dati, come backup, clonazione o ripristino, è necessario configurare l'ambiente. È anche possibile configurare SnapCenter Server per utilizzare la tecnologia SnapMirror e SnapVault .

Per sfruttare i vantaggi della tecnologia SnapVault e SnapMirror , è necessario configurare e inizializzare una relazione di protezione dei dati tra i volumi di origine e di destinazione sul dispositivo di archiviazione. Per eseguire queste attività è possibile utilizzare NetAppSystem Manager oppure la riga di comando della console di archiviazione.

Prima di utilizzare il plug-in per i file system Unix, l'amministratore SnapCenter deve installare e configurare SnapCenter Server ed eseguire le attività preliminari.

- Installa e configura SnapCenter Server."Saperne di più"
- Configurare l'ambiente SnapCenter aggiungendo connessioni al sistema di archiviazione."Saperne di più"

> SnapCenter non supporta più SVM con lo stesso nome su cluster diversi. Ogni SVM registrato con SnapCenter tramite la registrazione SVM o la registrazione cluster deve essere univoco.

- Aggiungi host, installa i plug-in e scopri le risorse.
- Se si utilizza SnapCenter Server per proteggere i file system Unix che risiedono su VMware RDM LUN o VMDK, è necessario distribuire il SnapCenter Plug-in for VMware vSphere e registrare il plug-in con SnapCenter.
- Installa Java sul tuo host Linux.
- Se si desidera la replica del backup, configurare SnapMirror e SnapVault su ONTAP.

Eseguire il backup dei file system Unix

Scopri i file system UNIX disponibili per il backup

Dopo aver installato il plug-in, tutti i file system presenti su quell'host vengono automaticamente rilevati e visualizzati nella pagina Risorse. È possibile aggiungere questi file system ai gruppi di risorse per eseguire operazioni di protezione dei dati.

Prima di iniziare

- È necessario aver completato attività quali l'installazione di SnapCenter Server, l'aggiunta di host e la creazione di connessioni al sistema di archiviazione.
- Se i file system risiedono su un disco di macchina virtuale (VMDK) o su un mapping di dispositivi raw (RDM), è necessario distribuire il SnapCenter Plug-in for VMware vSphere e registrare il plug-in con SnapCenter.

  Per ulteriori informazioni, vedere "Distribuisci il SnapCenter Plug-in for VMware vSphere" .

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Percorso** dall'elenco Visualizza.
3. Fare clic su **Aggiorna risorse**.

   I file system vengono visualizzati insieme a informazioni quali tipo, nome host, gruppi di risorse e policy associati e stato.

Creare policy di backup per i file system Unix

Prima di utilizzare SnapCenter per eseguire il backup dei file system Unix, è necessario creare una policy di backup per la risorsa o il gruppo di risorse di cui si desidera eseguire il backup. Una policy di backup è un insieme di regole che regolano il modo in cui si gestiscono, si pianificano e si conservano i backup. È inoltre possibile specificare le impostazioni relative a replica, script e tipo di backup. La creazione di un criterio consente di risparmiare tempo quando si desidera riutilizzarlo su un'altra risorsa o un altro gruppo di risorse.

Prima di iniziare

- È necessario prepararsi alla protezione dei dati completando attività quali l'installazione SnapCenter, l'aggiunta di host, l'individuazione dei file system e la creazione di connessioni al sistema di archiviazione.
- Se si replicano gli snapshot su un mirror o su un archivio secondario vault, l'amministratore SnapCenter deve aver assegnato le SVM sia per il volume di origine che per quello di destinazione.
- Esaminare i prerequisiti e le limitazioni specifici SnapMirror ActiveSync. Per informazioni, fare riferimento "Limiti degli oggetti per la sincronizzazione attiva SnapMirror" .

Informazioni su questo compito

- SnapLock

◦ Se è selezionata l’opzione "Conserva le copie di backup per un numero specifico di giorni", il periodo di conservazione SnapLock deve essere inferiore o uguale ai giorni di conservazione indicati.

Specificando un periodo di blocco degli snapshot si impedisce l’eliminazione degli snapshot fino alla scadenza del periodo di conservazione. Ciò potrebbe comportare la conservazione di un numero di snapshot maggiore rispetto al conteggio specificato nella policy.

Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli SnapLock Vault Snapshot come parte del ripristino erediteranno il tempo di scadenza SnapLock Vault. L’amministratore dell’archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Criteri**.
3. Selezionare **File System Unix** dall’elenco a discesa.
4. Fare clic su **Nuovo**.
5. Nella pagina Nome, immettere il nome e i dettagli della policy.
6. Nella pagina Backup e replica, eseguire le seguenti azioni:
   a. Specificare le impostazioni di backup.
   b. Specificare la frequenza di programmazione selezionando **Su richiesta**, **Ogni ora**, **Giornaliera**, **Settimanale** o **Mensile**.
   c. Nella sezione Seleziona opzioni di replicazione secondaria, seleziona una o entrambe le seguenti opzioni di replicazione secondaria:

Per questo campo…	**Fai questo…**
Aggiorna SnapMirror dopo aver creato una copia Snapshot locale	Selezionare questo campo per creare copie mirror dei set di backup su un altro volume (replica SnapMirror). Questa opzione dovrebbe essere abilitata per la sincronizzazione attiva SnapMirror .
Aggiorna SnapVault dopo aver creato una copia Snapshot locale	Selezionare questa opzione per eseguire la replica del backup da disco a disco (backup SnapVault).
Errore nel conteggio dei tentativi	Immettere il numero massimo di tentativi di replica consentiti prima che l’operazione venga interrotta.

7. Nella pagina Conservazione, specificare le impostazioni di conservazione per il tipo di backup e il tipo di pianificazione selezionati nella pagina Backup e replica:

Se lo desidera…	Poi…

Conserva un certo numero di snapshot	Seleziona **Copie da conservare**, quindi specifica il numero di snapshot che desideri conservare. Se il numero di Snapshot supera il numero specificato, gli Snapshot vengono eliminati partendo dalle copie più vecchie. Il valore massimo di ritenzione è 1018. I backup non riusciranno se la conservazione è impostata su un valore superiore a quello supportato dalla versione ONTAP sottostante. Se si prevede di abilitare la replica SnapVault , è necessario impostare il conteggio di conservazione su 2 o su un valore superiore. Se si imposta il conteggio di conservazione su 1, l'operazione di conservazione potrebbe non riuscire perché il primo Snapshot è lo Snapshot di riferimento per la relazione SnapVault finché uno Snapshot più recente non viene replicato sulla destinazione.
Conserva gli snapshot per un certo numero di giorni	Selezionare **Conserva copie per**, quindi specificare il numero di giorni per cui si desidera conservare gli snapshot prima di eliminarli.
Periodo di blocco della copia snapshot	Selezionare **Periodo di blocco della copia snapshot** e specificare la durata in giorni, mesi o anni. Il periodo di conservazione di Snaplock dovrebbe essere inferiore a 100 anni.

8. Seleziona l'etichetta della policy.

   È possibile assegnare etichette SnapMirror agli snapshot primari per la replica remota, consentendo agli snapshot primari di trasferire l'operazione di replica degli snapshot da SnapCenter ai sistemi secondari ONTAP . Questa operazione può essere eseguita senza abilitare l'opzione SnapMirror o SnapVault nella pagina dei criteri.

9. Nella pagina Script, immettere il percorso e gli argomenti del prescript o del postscript che si desidera eseguire rispettivamente prima o dopo l'operazione di backup.

   Dovresti controllare se i comandi sono presenti nell'elenco dei comandi disponibile sull'host del plug-in dal percorso _ /opt/ NetApp/snapcenter/scc/etc/allowed_commands.config_.

È anche possibile specificare il valore di timeout dello script. Il valore predefinito è 60 secondi.

10. Rivedi il riepilogo e poi clicca su **Fine**.

Crea gruppi di risorse e allega policy per i file system Unix

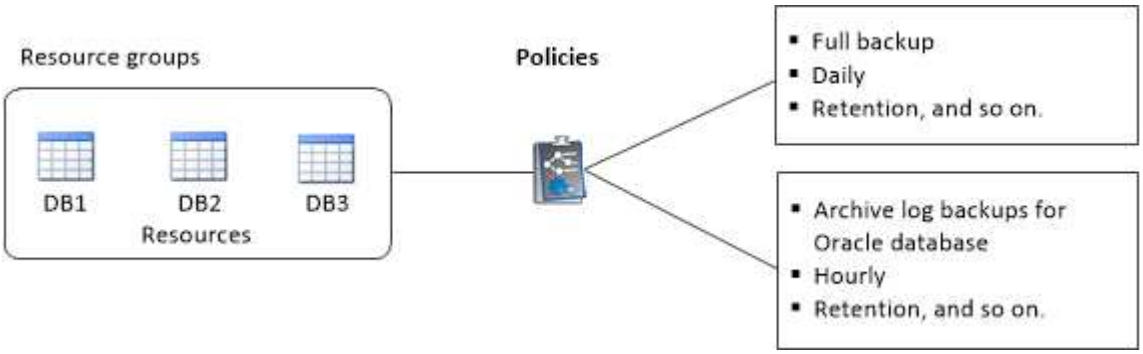
Un gruppo di risorse è un contenitore in cui aggiungere le risorse di cui si desidera eseguire il backup e la protezione. Un gruppo di risorse consente di eseguire il backup di tutti i dati associati ai file system.

Informazioni su questo compito

- Un database con file in gruppi di dischi ASM deve essere nello stato "MOUNT" o "OPEN" per verificare i propri backup utilizzando l'utilità Oracle DBVERIFY.

  Allegare una o più policy al gruppo di risorse per definire il tipo di attività di protezione dei dati che si desidera eseguire.

  L'immagine seguente illustra la relazione tra risorse, gruppi di risorse e criteri per i database:



- Per i criteri abilitati per SnapLock , per ONTAP 9.12.1 e versioni precedenti, se si specifica un periodo di blocco degli snapshot, i cloni creati dagli snapshot antimanomissione come parte del ripristino erediteranno il tempo di scadenza SnapLock . L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .
- L'aggiunta di nuovi file system senza SnapMirror ActiveSync a un gruppo di risorse esistente che contiene risorse con SnapMirror ActiveSync non è supportata.
- L'aggiunta di nuovi file system a un gruppo di risorse esistente in modalità failover di SnapMirror ActiveSync non è supportata. È possibile aggiungere risorse al gruppo di risorse solo nello stato normale o di failback.

Passi

1. Nel riquadro di navigazione a sinistra, seleziona **Risorse** e il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, fare clic su **Nuovo gruppo di risorse**.
3. Nella pagina Nome, eseguire le seguenti azioni:
   a. Immettere un nome per il gruppo di risorse nel campo Nome.

      Il nome del gruppo di risorse non deve superare i 250 caratteri.

   b. Inserisci una o più etichette nel campo Tag per aiutarti a cercare il gruppo di risorse in un secondo momento.

Ad esempio, se aggiungi HR come tag a più gruppi di risorse, potrai successivamente trovare tutti i gruppi di risorse associati al tag HR.

c. Selezionare la casella di controllo e immettere un formato di nome personalizzato che si desidera utilizzare per il nome dello snapshot.

Ad esempio, customtext_resource group_policy_hostname o resource group_hostname. Per impostazione predefinita, al nome dello snapshot viene aggiunto un timestamp.

4. Nella pagina Risorse, seleziona un nome host del file system Unix dall'elenco a discesa **Host**.

Le risorse vengono elencate nella sezione Risorse disponibili solo se la risorsa viene rilevata correttamente. Se hai aggiunto risorse di recente, queste appariranno nell'elenco delle risorse disponibili solo dopo aver aggiornato l'elenco delle risorse.

5. Seleziona le risorse dalla sezione Risorse disponibili e spostale nella sezione Risorse selezionate.
6. Nella pagina Impostazioni applicazione, procedere come segue:
   - Selezionare la freccia Script e immettere i comandi pre e post per le operazioni di quiesce, snapshot e unquiesce. È anche possibile immettere i comandi pre da eseguire prima di uscire in caso di errore.
   - Selezionare una delle opzioni di coerenza del backup:
     - Selezionare **File System Consistent** se si desidera garantire che i dati memorizzati nella cache dei file system vengano svuotati prima di creare il backup e che non siano consentite operazioni di input o output sul file system durante la creazione del backup.

Per la coerenza del file system, verranno acquisiti snapshot del gruppo di coerenza per i LUN coinvolti nel gruppo di volumi.

     - Selezionare **Crash Consistent** se si desidera garantire che i dati memorizzati nella cache dei file system vengano svuotati prima di creare il backup.

Se hai aggiunto diversi file system nel gruppo di risorse, tutti i volumi provenienti da diversi file system nel gruppo di risorse verranno inseriti in un gruppo di coerenza.

7. Nella pagina Criteri, procedere come segue:

a. Selezionare una o più policy dall'elenco a discesa.

Puoi anche creare una policy cliccando + .

Nella sezione Configura pianificazioni per policy selezionate vengono elencate le policy selezionate.

b. Clic + nella colonna Configura pianificazioni per il criterio per il quale si desidera configurare una pianificazione.

c. Nella finestra Aggiungi pianificazioni per il criterio *nome_criterio*, configura la pianificazione, quindi fai clic su **OK**.

Dove *policy_name* è il nome della policy selezionata.

Le pianificazioni configurate sono elencate nella colonna Pianificazioni applicate.

Le pianificazioni di backup di terze parti non sono supportate quando si sovrappongono alle pianificazioni di backup SnapCenter .

8. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

   È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email. Se si desidera allegare il report dell'operazione eseguita sul gruppo di risorse, selezionare **Allega report lavoro**.

   Per la notifica tramite e-mail, è necessario aver specificato i dettagli del server SMTP tramite l'interfaccia grafica utente (GUI) o il comando PowerShell Set-SmSmtpServer.

9. Rivedi il riepilogo e poi clicca su **Fine**.

Crea gruppi di risorse e abilita la protezione secondaria per i file system Unix sui sistemi ASA r2

È necessario creare il gruppo di risorse per aggiungere le risorse presenti sui sistemi ASA r2. È anche possibile predisporre la protezione secondaria durante la creazione del gruppo di risorse.

Prima di iniziare

- È necessario assicurarsi di non aggiungere risorse ONTAP 9.x e risorse ASA r2 allo stesso gruppo di risorse.
- È necessario assicurarsi di non disporre di un database con risorse ONTAP 9.x e risorse ASA r2.

Informazioni su questo compito

- La protezione secondaria è disponibile solo se all'utente connesso è assegnato il ruolo per cui è abilitata la funzionalità **SecondaryProtection**.
- Se è stata abilitata la protezione secondaria, il gruppo di risorse viene messo in modalità di manutenzione durante la creazione dei gruppi di coerenza primario e secondario. Dopo aver creato i gruppi di coerenza primari e secondari, il gruppo di risorse esce dalla modalità di manutenzione.
- SnapCenter non supporta la protezione secondaria per una risorsa clone.

Passi

1. Nel riquadro di navigazione a sinistra, seleziona **Risorse** e il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, fare clic su **Nuovo gruppo di risorse**.
3. Nella pagina Nome, eseguire le seguenti azioni:
   a. Immettere un nome per il gruppo di risorse nel campo Nome.

      Il nome del gruppo di risorse non deve superare i 250 caratteri.

   b. Inserisci una o più etichette nel campo Tag per aiutarti a cercare il gruppo di risorse in un secondo momento.

      Ad esempio, se aggiungi HR come tag a più gruppi di risorse, potrai successivamente trovare tutti i gruppi di risorse associati al tag HR.

c. Selezionare questa casella di controllo e immettere un formato di nome personalizzato che si desidera utilizzare per il nome dello snapshot.

   Ad esempio, customtext_resource group_policy_hostname o resource group_hostname. Per impostazione predefinita, al nome dello snapshot viene aggiunto un timestamp.

d. Specificare le destinazioni dei file di registro dell'archivio di cui non si desidera eseguire il backup.

   Dovresti usare esattamente la stessa destinazione impostata nell'applicazione, incluso il prefisso, se necessario.

4. Nella pagina Risorse, seleziona il nome host del database dall'elenco a discesa **Host**.

   Le risorse vengono elencate nella sezione Risorse disponibili solo se la risorsa viene rilevata correttamente. Se hai aggiunto risorse di recente, queste appariranno nell'elenco delle risorse disponibili solo dopo aver aggiornato l'elenco delle risorse.

5. Selezionare le risorse ASA r2 dalla sezione Risorse disponibili e spostarle nella sezione Risorse selezionate.
6. Nella pagina Impostazioni applicazione, seleziona l'opzione di backup.
7. Nella pagina Criteri, procedere come segue:

   a. Selezionare una o più policy dall'elenco a discesa.

      Puoi anche creare una policy cliccando + .

      Nella sezione Configura pianificazioni per policy selezionate vengono elencate le policy selezionate.

   b. Clic + nella colonna Configura pianificazioni per il criterio per il quale si desidera configurare una pianificazione.

   c. Nella finestra Aggiungi pianificazioni per il criterio *nome_criterio*, configura la pianificazione, quindi fai clic su **OK**.

      Dove *policy_name* è il nome della policy selezionata.

      Le pianificazioni configurate sono elencate nella colonna Pianificazioni applicate.

   Le pianificazioni di backup di terze parti non sono supportate quando si sovrappongono alle pianificazioni di backup SnapCenter .

8. Se la protezione secondaria è abilitata per il criterio selezionato, viene visualizzata la pagina Protezione secondaria ed è necessario eseguire i seguenti passaggi:

   a. Selezionare il tipo di criterio di replica.

      La politica di replica sincrona non è supportata.

   b. Specificare il suffisso del gruppo di coerenza che si desidera utilizzare.

   c. Dai menu a discesa Cluster di destinazione e SVM di destinazione, seleziona il cluster peer e l'SVM che desideri utilizzare.

Il cluster e il peering SVM non sono supportati da SnapCenter. Per eseguire il peering di cluster e SVM, è necessario utilizzare System Manager o ONTAP CLI.

Se le risorse sono già protette all'esterno di SnapCenter, verranno visualizzate nella sezione Risorse secondarie protette.

1. Nella pagina Verifica, procedere come segue:
   a. Fare clic su **Carica localizzatori** per caricare i volumi SnapMirror o SnapVault ed eseguire la verifica sull'archiviazione secondaria.
   b. Clic + nella colonna Configura pianificazioni per configurare la pianificazione di verifica per tutti i tipi di pianificazione del criterio.
   c. Nella finestra di dialogo Aggiungi pianificazioni di verifica policy_name, eseguire le seguenti azioni:

Se lo desidera…	Fai questo…
Esegui la verifica dopo il backup	Selezionare **Esegui verifica dopo il backup**.
Pianifica una verifica	Selezionare **Esegui verifica pianificata**, quindi selezionare il tipo di pianificazione dall'elenco a discesa.

   d. Seleziona **Verifica su posizione secondaria** per verificare i backup sul sistema di archiviazione secondario.
   e. Fare clic su **OK**.

   Le pianificazioni di verifica configurate sono elencate nella colonna Pianificazioni applicate.

2. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

   È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email. Se si desidera allegare il report dell'operazione eseguita sul gruppo di risorse, selezionare **Allega report lavoro**.

   Per la notifica tramite e-mail, è necessario aver specificato i dettagli del server SMTP tramite l'interfaccia grafica utente (GUI) o il comando PowerShell Set-SmSmtpServer.

3. Rivedi il riepilogo e poi clicca su **Fine**.

Eseguire il backup dei file system Unix

Se una risorsa non fa parte di alcun gruppo di risorse, è possibile eseguirne il backup dalla pagina Risorse.

Passi

1. Nel riquadro di navigazione a sinistra, seleziona **Risorse** e il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Percorso** dall'elenco Visualizza.

3. Clic , quindi selezionare il nome host e i file system Unix per filtrare le risorse.
4. Selezionare il file system di cui si desidera eseguire il backup.
5. Nella pagina Risorse puoi eseguire i seguenti passaggi:
   a. Selezionare la casella di controllo e immettere un formato di nome personalizzato che si desidera utilizzare per il nome dello snapshot.

      Per esempio, `customtext_policy_hostname` O `resource_hostname` . Per impostazione predefinita, al nome dello snapshot viene aggiunto un timestamp.

6. Nella pagina Impostazioni applicazione, procedere come segue:
   - Selezionare la freccia Script e immettere i comandi pre e post per le operazioni di quiesce, snapshot e unquiesce. È anche possibile immettere i comandi pre da eseguire prima di uscire in caso di errore.
   - Selezionare una delle opzioni di coerenza del backup:
     - Selezionare **File System Consistent** se si desidera garantire che i dati memorizzati nella cache del file system vengano svuotati prima di creare il backup e che non venga eseguita alcuna operazione sul file system durante la creazione del backup.
     - Selezionare **Crash Consistent** se si desidera garantire che i dati memorizzati nella cache dei file system vengano svuotati prima di creare il backup.
7. Nella pagina Criteri, procedere come segue:
   a. Selezionare una o più policy dall'elenco a discesa.

      Puoi creare una policy cliccando .

      Nella sezione Configura pianificazioni per policy selezionate vengono elencate le policy selezionate.

   b. Clic nella colonna Configura pianificazioni per configurare una pianificazione per la policy desiderata.
   c. Nella finestra Aggiungi pianificazioni per il criterio *nome_criterio*, configura la pianificazione e quindi seleziona `OK` .

      policy_name è il nome della policy selezionata.

   Le pianificazioni configurate sono elencate nella colonna Pianificazioni applicate.

8. Nella pagina Notifica, seleziona gli scenari in cui desideri inviare le email dall'elenco a discesa **Preferenza email**.

   È necessario specificare gli indirizzi e-mail del mittente e del destinatario, nonché l'oggetto dell'e-mail. Se si desidera allegare il report dell'operazione di backup eseguita sulla risorsa, selezionare **Allega report attività**.

   Per la notifica via e-mail, è necessario aver specificato i dettagli del server SMTP utilizzando l'interfaccia grafica utente o il comando PowerShell `Set-SmSmtpServer` .

9. Rivedi il riepilogo e poi clicca su **Fine**.

   Viene visualizzata la pagina della topologia.

10. Fare clic su **Esegui backup ora**.
11. Nella pagina Backup, procedere come segue:
    a. Se hai applicato più criteri alla risorsa, dall'elenco a discesa Criterio seleziona il criterio che desideri utilizzare per il backup.

       Se il criterio selezionato per il backup su richiesta è associato a una pianificazione di backup, i backup su richiesta verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.

    b. Fare clic su **Backup**.
12. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

Eseguire il backup dei gruppi di risorse dei file system Unix

È possibile eseguire il backup dei file system Unix definiti nel gruppo di risorse. È possibile eseguire il backup di un gruppo di risorse su richiesta dalla pagina Risorse. Se a un gruppo di risorse è associato un criterio e configurata una pianificazione, i backup vengono creati in base alla pianificazione.

Passi

1. Nel riquadro di navigazione a sinistra, seleziona **Risorse** e il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Gruppo di risorse** dall'elenco **Visualizza**.
3. Inserisci il nome del gruppo di risorse nella casella di ricerca oppure fai clic su e seleziona il tag.

   Clic per chiudere il riquadro del filtro.
4. Nella pagina Gruppo di risorse, seleziona il gruppo di risorse di cui eseguire il backup.
5. Nella pagina Backup, procedere come segue:
    a. Se al gruppo di risorse sono associati più criteri, selezionare il criterio di backup che si desidera utilizzare dall'elenco a discesa **Criterio**.

       Se il criterio selezionato per il backup su richiesta è associato a una pianificazione di backup, i backup su richiesta verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.

    b. Selezionare **Backup**.
6. Monitorare l'avanzamento selezionando **Monitoraggio > Lavori**.

Monitorare il backup dei file system Unix

Scopri come monitorare l'avanzamento delle operazioni di backup e di protezione dei dati.

Monitorare le operazioni di backup dei file system Unix

È possibile monitorare l'avanzamento delle diverse operazioni di backup utilizzando la pagina SnapCenterJobs. Potrebbe essere opportuno controllare lo stato di avanzamento per determinare quando il processo è completato o se si è verificato un problema.

Informazioni su questo compito

Nella pagina Lavori vengono visualizzate le seguenti icone che indicano lo stato corrispondente delle operazioni:

- In corso
- Completato con successo
- Fallito
- Completato con avvisi o non è stato possibile avviarlo a causa di avvisi
- In coda
- Annullato

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina Monitor, fare clic su **Lavori**.
3. Nella pagina Lavori, procedere come segue:
   a. Clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di backup.
   b. Specificare le date di inizio e fine.
   c. Dall'elenco a discesa **Tipo**, selezionare **Backup**.
   d. Dal menu a discesa **Stato**, seleziona lo stato del backup.
   e. Fare clic su **Applica** per visualizzare le operazioni completate correttamente.
4. Selezionare un processo di backup, quindi fare clic su **Dettagli** per visualizzare i dettagli del processo.

   Sebbene lo stato del processo di backup venga visualizzato , quando fai clic sui dettagli del processo, potresti vedere che alcune delle attività secondarie dell'operazione di backup sono ancora in corso o contrassegnate con segnali di avviso.

5. Nella pagina Dettagli lavoro, fare clic su **Visualizza registri**.

   Il pulsante **Visualizza registri** visualizza i registri dettagliati per l'operazione selezionata.

Monitorare le operazioni di protezione dei dati nel riquadro Attività

Il riquadro Attività visualizza le cinque operazioni eseguite più di recente. Nel riquadro Attività viene inoltre visualizzato quando è stata avviata l'operazione e il suo stato.

Il riquadro Attività visualizza informazioni relative alle operazioni di backup, ripristino, clonazione e backup pianificato.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Clic nel riquadro Attività per visualizzare le cinque operazioni più recenti.

   Quando si fa clic su una delle operazioni, i dettagli dell'operazione vengono elencati nella pagina **Dettagli lavoro**.

Visualizza i file system Unix protetti nella pagina Topologia

Quando ci si prepara a eseguire il backup, il ripristino o la clonazione di una risorsa, potrebbe essere utile visualizzare una rappresentazione grafica di tutti i backup, dei file system ripristinati e dei cloni nell'archiviazione primaria e secondaria.

Informazioni su questo compito

Nella pagina Topologia è possibile visualizzare tutti i backup, i file system ripristinati e i cloni disponibili per la risorsa o il gruppo di risorse selezionato. È possibile visualizzare i dettagli di tali backup, file system ripristinati e cloni, quindi selezionarli per eseguire operazioni di protezione dei dati.

È possibile esaminare le seguenti icone nella vista Gestisci copie per determinare se i backup e i cloni sono disponibili nell'archivio primario o secondario (copie mirror o copie Vault).

-  visualizza il numero di backup e cloni disponibili sullo storage primario.
-  visualizza il numero di backup e cloni di cui è stato eseguito il mirroring sullo storage secondario mediante la tecnologia SnapMirror .
-  visualizza il numero di backup e cloni replicati sullo storage secondario mediante la tecnologia SnapVault .

  Il numero di backup visualizzato include i backup eliminati dall'archivio secondario. Ad esempio, se hai creato 6 backup utilizzando un criterio per conservarne solo 4, il numero di backup visualizzato è 6.

I cloni di un backup di un mirror con versione flessibile su un volume di tipo mirror-vault vengono visualizzati nella vista topologia, ma il conteggio dei backup mirror nella vista topologia non include il backup con versione flessibile.

Se si dispone di una relazione secondaria come SnapMirror ActiveSync (inizialmente rilasciata come SnapMirror Business Continuity [SM-BC]), è possibile visualizzare le seguenti icone aggiuntive:

-  Il sito replica è attivo.
-  Il sito replica è inattivo.
-  La relazione tra specchio secondario e volta non è stata ristabilita.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona la risorsa o il gruppo di risorse dall'elenco a discesa **Visualizza**.
3. Selezionare la risorsa dalla vista dei dettagli della risorsa o dalla vista dei dettagli del gruppo di risorse.

Se la risorsa è protetta, viene visualizzata la pagina Topologia della risorsa selezionata.

4. Esaminare la scheda Riepilogo per visualizzare un riepilogo del numero di backup e cloni disponibili sullo storage primario e secondario.

   Nella sezione Scheda riepilogativa viene visualizzato il numero totale di backup e cloni.

   Facendo clic sul pulsante **Aggiorna** viene avviata una query dello spazio di archiviazione per visualizzare un conteggio accurato.

   Se viene eseguito un backup abilitato per SnapLock , facendo clic sul pulsante **Aggiorna** vengono aggiornati i tempi di scadenza SnapLock primario e secondario recuperati da ONTAP. Una pianificazione settimanale aggiorna anche il tempo di scadenza primario e secondario SnapLock recuperato da ONTAP.

   Quando il file system è distribuito su più volumi, il tempo di scadenza SnapLock per il backup sarà il tempo di scadenza SnapLock più lungo impostato per uno Snapshot in un volume. Il tempo di scadenza SnapLock più lungo viene recuperato da ONTAP.

   Per la sincronizzazione attiva SnapMirror , facendo clic sul pulsante **Aggiorna** si aggiorna l'inventario di backup SnapCenter interrogando ONTAP sia per i siti primari che per quelli di replica. Una pianificazione settimanale esegue questa attività anche per tutti i database contenenti la relazione di sincronizzazione attiva SnapMirror .

   - Per SnapMirror ActiveSync e solo per ONTAP 9.14.1, le relazioni Async Mirror o Async MirrorVault con la nuova destinazione primaria devono essere configurate manualmente dopo il failover. Da ONTAP 9.15.1 in poi, Async Mirror o Async MirrorVault vengono configurati automaticamente sulla nuova destinazione primaria.
   - Dopo il failover, è necessario creare un backup affinché SnapCenter sia a conoscenza del failover. È possibile fare clic su **Aggiorna** solo dopo aver creato un backup.

5. Nella vista Gestisci copie, fare clic su **Backup** o **Cloni** dall'archivio primario o secondario per visualizzare i dettagli di un backup o di un clone.

   I dettagli dei backup e dei cloni vengono visualizzati in formato tabella.

6. Selezionare il backup dalla tabella, quindi fare clic sulle icone di protezione dei dati per eseguire operazioni di ripristino, clonazione ed eliminazione.

   Non è possibile rinominare o eliminare i backup presenti nell'archivio secondario.

7. Se si desidera eliminare un clone, selezionare il clone dalla tabella, quindi fare clic su .

Esempio che mostra backup e cloni sullo storage primario

Ripristinare e recuperare i file system Unix

Ripristinare i file system Unix

In caso di perdita di dati, è possibile utilizzare SnapCenter per ripristinare i file system Unix.

Informazioni su questo compito

- È necessario eseguire i seguenti comandi per stabilire la connessione con SnapCenter Server, elencare i backup e recuperarne le informazioni, quindi ripristinare il backup.

  Le informazioni riguardanti i parametri che possono essere utilizzati con il comando e le relative descrizioni possono essere ottenute eseguendo Get-Help *command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai comandi del software SnapCenter" .

- Per l'operazione di ripristino di SnapMirror ActiveSync, è necessario selezionare il backup dalla posizione principale.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Percorso** o **Gruppo di risorse** dall'elenco **Visualizza**.

3. Selezionare il file system dalla vista dettagli o dalla vista dettagli del gruppo di risorse.

   Viene visualizzata la pagina della topologia.

4. Dalla vista Gestisci copie, seleziona **Backup** dai sistemi di archiviazione primario o secondario (con mirroring o replica).
5. Seleziona il backup dalla tabella, quindi fai clic su *  *.
6. Nella pagina Ambito di ripristino:
   - Per i file system NFS, per impostazione predefinita è selezionato il ripristino **Connetti e copia**. Puoi anche selezionare **Ripristino volume** o **Ripristino rapido**.
   - Per i file system non NFS, l'ambito di ripristino viene selezionato in base al layout.

     A seconda del tipo e del layout del file system, i nuovi file creati dopo il backup potrebbero non essere disponibili dopo il ripristino.
7. Nella pagina PreOps, immettere i comandi di pre-ripristino da eseguire prima di eseguire un processo di ripristino.
8. Nella pagina PostOps, immettere i comandi di post-ripristino da eseguire dopo aver eseguito un processo di ripristino.

   Dovresti controllare se i comandi sono presenti nell'elenco dei comandi disponibile sull'host del plug-in nella posizione _/opt/NetApp/snapcenter/scc/etc/allowed_commands.config_path.

9. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le notifiche e-mail.

   È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email. Se si desidera allegare il report dell'operazione di ripristino eseguita, è necessario selezionare **Allega report lavoro**.

   Per la notifica tramite e-mail, è necessario aver specificato i dettagli del server SMTP utilizzando l'interfaccia grafica utente (GUI) o il comando PowerShell Set-SmSmtpServer.

10. Rivedi il riepilogo e poi clicca su **Fine**.

    Se l'operazione di ripristino fallisce, il rollback non è supportato.

    In caso di ripristino di un file system residente su un gruppo di volumi, il vecchio contenuto del file system non viene eliminato. Solo il contenuto del file system clonato verrà copiato nel file system di origine. Questa opzione è applicabile quando sono presenti più file system nel gruppo di volumi e vengono ripristinati i file system NFS predefiniti.

11. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

Monitorare le operazioni di ripristino dei file system Unix

È possibile monitorare l'avanzamento delle diverse operazioni di ripristino SnapCenter utilizzando la pagina Lavori. Potrebbe essere opportuno controllare lo stato di

avanzamento di un'operazione per stabilire quando è stata completata o se si è verificato un problema.

Informazioni su questo compito

Gli stati post-ripristino descrivono le condizioni della risorsa dopo un'operazione di ripristino e qualsiasi ulteriore azione di ripristino che è possibile intraprendere.

Nella pagina Lavori vengono visualizzate le seguenti icone che indicano lo stato dell'operazione:

- In corso
- Completato con successo
- Fallito
- Completato con avvisi o non è stato possibile avviarlo a causa di avvisi
- In coda
- Annullato

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Lavori**.
3. Nella pagina **Lavori**, procedere come segue:
   a. Clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di ripristino.
   b. Specificare le date di inizio e fine.
   c. Dall'elenco a discesa **Tipo**, seleziona **Ripristina**.
   d. Dall'elenco a discesa **Stato**, selezionare lo stato di ripristino.
   e. Fare clic su **Applica** per visualizzare le operazioni completate correttamente.
4. Selezionare il processo di ripristino, quindi fare clic su **Dettagli** per visualizzare i dettagli del processo.
5. Nella pagina **Dettagli lavoro**, fare clic su **Visualizza registri**.

   Il pulsante **Visualizza registri** visualizza i registri dettagliati per l'operazione selezionata.

Clonare i file system Unix

Clona il backup del file system Unix

È possibile utilizzare SnapCenter per clonare il file system Unix utilizzando il backup del file system.

Prima di iniziare

- È possibile saltare l'aggiornamento del file fstab impostando il valore di *SKIP_FSTAB_UPDATE* su **true** nel file *agent.properties* che si trova in */opt/ NetApp/snapcenter/scc/etc*.
- È possibile avere un nome di volume clone statico e un percorso di giunzione impostando il valore di *USE_CUSTOM_CLONE_VOLUME_NAME_FORMAT* su **true** nel file *agent.properties* situato in */opt/ NetApp/snapcenter/scc/etc*. Dopo aver aggiornato il file, dovresti riavviare il servizio di creazione del plug-

in SnapCenter eseguendo il comando: `/opt/NetApp/snapcenter/scc/bin/scc restart`.

Esempio: senza questa proprietà il nome del volume clone e il percorso di giunzione saranno simili a <Source_volume_name>_Clone_<Timestamp> ma ora saranno <Source_volume_name>_Clone_<Clone_Name>

In questo modo il nome rimane costante, così puoi mantenere aggiornato manualmente il file fstab se non preferisci aggiornarlo tramite SnapCenter.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Percorso** o **Gruppo di risorse** dall'elenco **Visualizza**.
3. Selezionare il file system dalla vista dettagli o dalla vista dettagli del gruppo di risorse.

   Viene visualizzata la pagina della topologia.

4. Dalla vista Gestisci copie, seleziona i backup tra Copie locali (primarie), Copie mirror (secondarie) o Copie vault (secondarie).
5. Seleziona il backup dalla tabella, quindi fai clic su *  *.
6. Nella pagina Posizione, eseguire le seguenti azioni:

Per questo campo…	Fai questo…
Server clone	Per impostazione predefinita, l'host di origine è popolato.
Punto di montaggio clone	Specificare il percorso in cui verrà montato il file system.

7. Nella pagina Script, procedere come segue:
   a. Immettere i comandi per il pre-clone o il post-clone che devono essere eseguiti rispettivamente prima o dopo l'operazione di clonazione.

      Dovresti controllare se i comandi sono presenti nell'elenco dei comandi disponibile sull'host del plug-in dal percorso */opt/NetApp/snapcenter/scc/etc/allowed_commands.config*.

8. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

   È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email. Se si desidera allegare il report dell'operazione di clonazione eseguita, selezionare **Allega report lavoro**.

   Per la notifica tramite e-mail, è necessario aver specificato i dettagli del server SMTP tramite l'interfaccia grafica utente (GUI) o il comando PowerShell Set-SmSmtpServer.

9. Rivedi il riepilogo e poi clicca su **Fine**.

10. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

Dividi un clone

È possibile utilizzare SnapCenter per dividere una risorsa clonata dalla risorsa padre. Il clone diviso diventa indipendente dalla risorsa padre.

Informazioni su questo compito

- Non è possibile eseguire l'operazione di divisione del clone su un clone intermedio.

  Ad esempio, dopo aver creato clone1 da un backup del database, è possibile creare un backup di clone1 e quindi clonare questo backup (clone2). Dopo aver creato clone2, clone1 è un clone intermedio e non è possibile eseguire l'operazione di divisione del clone su clone1. Tuttavia, è possibile eseguire l'operazione di divisione del clone su clone2.

  Dopo aver diviso clone2, è possibile eseguire l'operazione di divisione del clone su clone1 perché clone1 non è più il clone intermedio.

- Quando si divide un clone, le copie di backup e i processi di clonazione del clone vengono eliminati.
- Per informazioni sulle operazioni di suddivisione del volume FlexClone , vedere, "Dividere un volume FlexClone dal suo volume padre" .
- Assicurarsi che il volume o l'aggregato sul sistema di archiviazione sia online.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina **Risorse**, seleziona l'opzione appropriata dall'elenco Visualizza:

Opzione	Descrizione
Per applicazioni di database	Selezionare **Database** dall'elenco Visualizza.
Per i file system	Selezionare **Percorso** dall'elenco Visualizza.

3. Seleziona la risorsa appropriata dall'elenco.

   Viene visualizzata la pagina della topologia delle risorse.

4. Dalla vista **Gestisci copie**, seleziona la risorsa clonata (ad esempio, il database o il LUN), quindi fai clic su *  *.
5. Verificare la dimensione stimata del clone da dividere e lo spazio disponibile richiesto sull'aggregato, quindi fare clic su **Avvia**.
6. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

   L'operazione di suddivisione del clone smette di rispondere se il servizio SMCore viene riavviato. È necessario eseguire il cmdlet Stop-SmJob per interrompere l'operazione di suddivisione del clone, quindi riprovare l'operazione.

   Se si desidera un tempo di polling più lungo o più breve per verificare se il clone è diviso o meno, è possibile modificare il valore del parametro *CloneSplitStatusCheckPollTime* nel file

SMCoreServiceHost.exe.config per impostare l'intervallo di tempo per SMCore per il polling dello stato dell'operazione di divisione del clone. Il valore è espresso in millisecondi e il valore predefinito è 5 minuti.

Per esempio:

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

L'operazione di avvio della suddivisione del clone fallisce se è in corso un backup, un ripristino o un'altra suddivisione del clone. È necessario riavviare l'operazione di suddivisione del clone solo dopo aver completato le operazioni in esecuzione.

Informazioni correlate

"La clonazione o la verifica SnapCenter non riesce perché l'aggregato non esiste"

Monitorare le operazioni di clonazione dei file system Unix

È possibile monitorare l'avanzamento delle operazioni di clonazione SnapCenter utilizzando la pagina Lavori. Potrebbe essere opportuno controllare lo stato di avanzamento di un'operazione per stabilire quando è stata completata o se si è verificato un problema.

Informazioni su questo compito

Nella pagina Lavori vengono visualizzate le seguenti icone che indicano lo stato dell'operazione:

- In corso
- Completato con successo
- Fallito
- Completato con avvisi o non è stato possibile avviarlo a causa di avvisi
- In coda
- Annullato

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Lavori**.
3. Nella pagina **Lavori**, procedere come segue:
   a. Clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di clonazione.
   b. Specificare le date di inizio e fine.
   c. Dall'elenco a discesa **Tipo**, seleziona **Clona**.
   d. Dall'elenco a discesa **Stato**, seleziona lo stato del clone.
   e. Fare clic su **Applica** per visualizzare le operazioni completate correttamente.
4. Selezionare il lavoro di clonazione, quindi fare clic su **Dettagli** per visualizzare i dettagli del lavoro.
5. Nella pagina Dettagli lavoro, fare clic su **Visualizza registri**.

Informazioni sul copyright

Informazioni sul marchio commerciale