



Configurare la Virtual Storage Console per l'ambiente VMware vSphere

VSC, VASA Provider, and SRA 9.7

NetApp
March 21, 2024

This PDF was generated from <https://docs.netapp.com/it-it/vsc-vasa-provider-sra-97/deploy/reference-esx-host-values-set-by-vsc-for-vmware-vsphere.html> on March 21, 2024. Always check docs.netapp.com for the latest.

Sommario

- Configurare la Virtual Storage Console per l'ambiente VMware vSphere 1
 - Configurare le impostazioni di multipathing e timeout del server ESXi 1
 - Rigenerare un certificato SSL per Virtual Storage Console 7
 - Requisiti per la registrazione di VSC in un ambiente con più vCenter Server 7
 - Configurare i file delle preferenze VSC 8
 - Attiva il montaggio del datastore su diverse subnet 9
 - Accedere alle opzioni della console di manutenzione dell'appliance virtuale per VSC, VASA Provider e SRA 10
 - Modificare la password dell'amministratore 12
 - Configurare l'alta disponibilità per l'appliance virtuale per VSC, VASA Provider e SRA 13
 - Configurazioni MetroCluster supportate dall'appliance virtuale per VSC, provider VASA e SRA 14

Configurare la Virtual Storage Console per l'ambiente VMware vSphere

(VSC) supporta numerosi ambienti. Alcune delle funzionalità di questi ambienti potrebbero richiedere una configurazione aggiuntiva.

Potrebbe essere necessario eseguire alcune delle seguenti attività per configurare gli host ESXi, i sistemi operativi guest e VSC:

- Verifica delle impostazioni dell'host ESXi, incluse le impostazioni UNMAP
- Aggiunta di valori di timeout per i sistemi operativi guest
- Rigenerazione del certificato SSL VSC
- Creazione di profili di funzionalità storage e allarmi di soglia
- Modifica del file delle preferenze per consentire il montaggio di datastore su diverse subnet

Configurare le impostazioni di multipathing e timeout del server ESXi

Virtual Storage Console per VMware vSphere controlla e imposta le impostazioni di multipathing host ESXi e le impostazioni di timeout HBA che funzionano meglio con i sistemi storage.

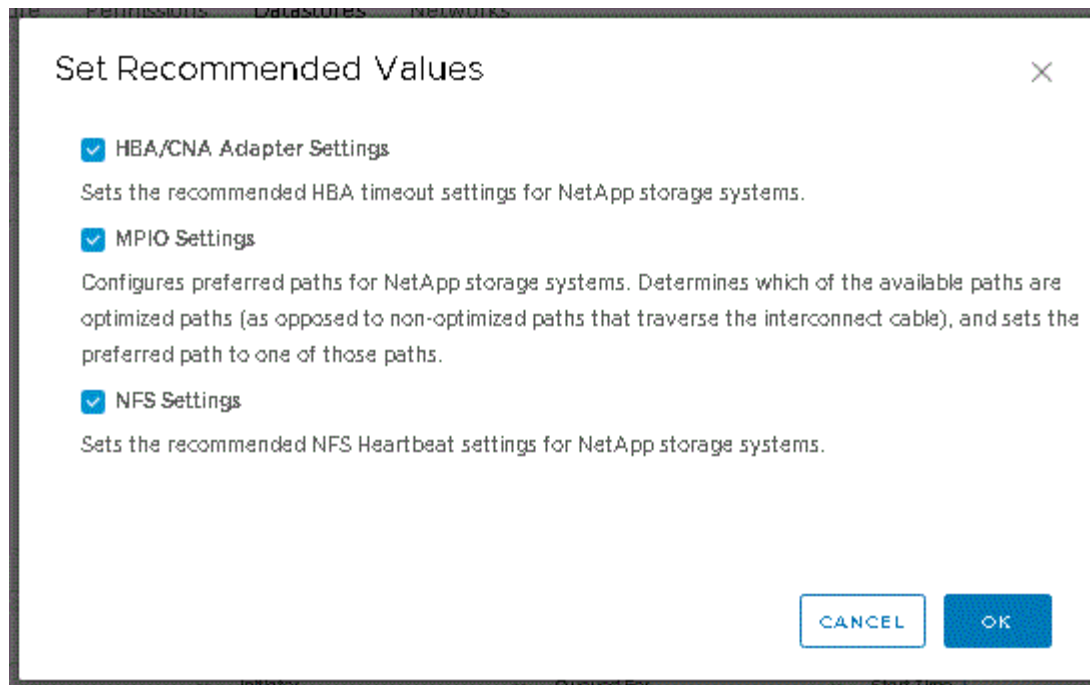
A proposito di questa attività

Questo processo potrebbe richiedere molto tempo, a seconda della configurazione e del carico di sistema. L'avanzamento dell'attività viene visualizzato nel pannello **attività recenti**. Una volta completate le attività, l'icona Avviso di stato dell'host viene sostituita dall'icona normale o dall'icona di riavvio in sospeso.

Fasi

1. Dalla pagina iniziale di VMware vSphere Web Client, fare clic su **vCenter > hosts**.
2. Fare clic con il pulsante destro del mouse su un host, quindi selezionare **Actions > NetApp VSC > Set Recommended Values** (azioni[NetApp VSC > Imposta valori consigliati]).
3. Nella finestra di dialogo **NetApp Recommended Settings** (Impostazioni consigliate NetApp), selezionare i valori più adatti al sistema.

I valori standard e consigliati sono impostati per impostazione predefinita.



4. Fare clic su **OK**.

Valori host ESXi impostati utilizzando Virtual Storage Console per VMware vSphere

È possibile impostare timeout e altri valori sugli host ESXi utilizzando Virtual Storage Console per VMware vSphere per garantire le migliori performance e il failover corretto. I valori impostati da Virtual Storage Console (VSC) si basano su test interni.

È possibile impostare i seguenti valori su un host ESXi:

Configurazione avanzata di ESXi

- **VMFS3.HardwareAcceleratedLocking**

Impostare questo valore su 1.

- **VMFS3.EnableBlockDelete**

Impostare questo valore su 0.

Impostazioni NFS

- **Net.TcpipHeapSize**

Se si utilizza vSphere 6.0 o versione successiva, impostare questo valore su 32.

- **Net.TcpipHeapMax**

Se si utilizza vSphere 6.0 o versione successiva, impostare questo valore su 1536.

- **NFS.MaxVolumes**

Se si utilizza vSphere 6.0 o versione successiva, impostare questo valore su 256.

- **NFS41.MaxVolumes**

Se si utilizza vSphere 6.0 o versione successiva, impostare questo valore su 256.

- **NFS.MaxQueueDepth**

Se si utilizza vSphere 6.0 o una versione successiva dell'host ESXi, impostare questo valore su 128 o superiore per evitare colli di bottiglia in coda.

Per le versioni di vSphere precedenti alla 6.0, impostare questo valore su 64.

- **NFS.HeartbeatMaxFailures**

Impostare questo valore su 10 per tutte le configurazioni NFS.

- **NFS.HeartbeatFrequency**

Impostare questo valore su 12 per tutte le configurazioni NFS.

- **NFS.HeartbeatTimeout**

Impostare questo valore su 5 per tutte le configurazioni NFS.

Impostazioni FC/FCoE

- **Criterio di selezione del percorso**

Impostare questo valore su “RR” (round robin) quando si utilizzano percorsi FC con ALUA.

Impostare questo valore su “FIXED” per tutte le altre configurazioni.

L'impostazione di questo valore su “RR” aiuta a fornire il bilanciamento del carico in tutti i percorsi attivi/ottimizzati. Il valore “FIXED” viene utilizzato per le configurazioni precedenti, non ALUA e aiuta a prevenire l'i/o del proxy

- **Disk.QFullSampleSize**

Impostare questo valore su 32 per tutte le configurazioni. L'impostazione di questo valore aiuta a prevenire gli errori di i/O.

- **Disk.QFullThreshold**

Impostare questo valore su 8 per tutte le configurazioni. L'impostazione di questo valore aiuta a prevenire gli errori di i/O.

- **Timeout HBA FC Emulex**

Utilizzare il valore predefinito.

- **Timeout HBA FC QLogic**

Utilizzare il valore predefinito.

Impostazioni iSCSI

- **Criterio di selezione del percorso**

Impostare questo valore su “RR” per tutti i percorsi iSCSI.

L'impostazione di questo valore su “RR” aiuta a fornire il bilanciamento del carico in tutti i percorsi attivi/ottimizzati.

- **Disk.QFullSampleSize**

Impostare questo valore su 32 per tutte le configurazioni. L'impostazione di questo valore aiuta a prevenire gli errori di i/O.

- **Disk.QFullThreshold**

Impostare questo valore su 8 per tutte le configurazioni. L'impostazione di questo valore aiuta a prevenire gli errori di i/O.

Configurare gli script del sistema operativo guest

Le immagini ISO degli script del sistema operativo guest sono montate sulla Virtual Storage Console per il server VMware vSphere. Per utilizzare gli script del sistema operativo guest per impostare i timeout dello storage per le macchine virtuali, è necessario montare gli script dal client vSphere.

Tipo di sistema operativo	impostazioni di timeout di 60 secondi	impostazioni di timeout di 190 secondi
Linux	<code>https://<appliance_ip>:8143/vsc/public/writable/linux_gos_timeout-install.iso</code>	<code>https://<appliance_ip>:8143/vsc/public/writable/linux_gos_timeout_190-install.iso</code>
Windows	<code>https://<appliance_ip>:8143/vsc/public/writable/windows_gos_timeout.iso</code>	<code>https://<appliance_ip>:8143/vsc/public/writable/windows_gos_timeout_190.iso</code>
Solaris	<code>https://<appliance_ip>:8143/vsc/public/writable/solaris_gos_timeout-install.iso</code>	<code>https://<appliance_ip>:8143/vsc/public/writable/solaris_gos_timeout_190-install.iso</code>

È necessario installare lo script dalla copia dell'istanza di VSC registrata nel vCenter Server che gestisce la macchina virtuale. Se l'ambiente include più vCenter Server, selezionare il server che contiene la macchina virtuale per cui si desidera impostare i valori di timeout dello storage.

È necessario accedere alla macchina virtuale ed eseguire lo script per impostare i valori di timeout dello storage.

Impostare i valori di timeout per i sistemi operativi guest di Windows

Gli script di timeout del sistema operativo guest impostano le impostazioni di timeout i/o SCSI per i sistemi operativi guest di Windows. È possibile specificare un timeout di 60 secondi o di 190 secondi. Per rendere effettive le impostazioni, è necessario riavviare il sistema operativo guest di Windows.

Prima di iniziare

È necessario aver montato l'immagine ISO contenente lo script di Windows.

Fasi

1. Accedere alla console della macchina virtuale Windows e a un account con privilegi di amministratore.
2. Se lo script non si avvia automaticamente, aprire l'unità CD ed eseguire `windows_gos_timeout.reg` script.

Viene visualizzata la finestra di dialogo Editor del Registro di sistema.

3. Fare clic su **Sì** per continuare.

Viene visualizzato il seguente messaggio: The keys and values contained in `D:\windows_gos_timeout.reg` have been successfully added to the registry.

4. Riavviare il sistema operativo guest di Windows.
5. Smontare l'immagine ISO.

Impostare i valori di timeout per i sistemi operativi guest Solaris

Gli script di timeout del sistema operativo guest impostano le impostazioni di timeout i/o SCSI per Solaris 10. È possibile specificare un timeout di 60 secondi o di 190 secondi.

Prima di iniziare

È necessario aver montato l'immagine ISO contenente lo script Solaris.

Fasi

1. Accedere alla console della macchina virtuale Solaris e a un account con privilegi root.
2. Eseguire `solaris_gos_timeout-install.sh` script.

Per Solaris 10, viene visualizzato un messaggio simile al seguente:

```
Setting I/O Timeout for /dev/s-a - SUCCESS!
```

3. Smontare l'immagine ISO.

Impostare i valori di timeout per i sistemi operativi guest Linux

Gli script di timeout del sistema operativo guest impostano le impostazioni di timeout i/o SCSI per le versioni 4, 5, 6 e 7 di Red Hat Enterprise Linux e le versioni 9, 10 e 11 di SUSE Linux Enterprise Server. È possibile specificare un timeout di 60 secondi o di 190

secondi. È necessario eseguire lo script ogni volta che si esegue l'aggiornamento a una nuova versione di Linux.

Prima di iniziare

È necessario aver montato l'immagine ISO contenente lo script Linux.

Fasi

1. Accedere alla console della macchina virtuale Linux e a un account con privilegi root.
2. Eseguire `linux_gos_timeout-install.sh` script.

Per Red Hat Enterprise Linux 4 o SUSE Linux Enterprise Server 9, viene visualizzato un messaggio simile al seguente:

```
Restarting udev... this may take a few seconds.
```

```
Setting I/O Timeout (60s) for /dev/sda - SUCCESS!
```

Per Red Hat Enterprise Linux 5, Red Hat Enterprise Linux 6 e Red Hat Enterprise Linux 7 viene visualizzato un messaggio simile al seguente:

```
patching file /etc/udev/rules.d/50-udev.rules
```

```
Hunk #1 succeeded at 333 (offset 13 lines).
```

```
Restarting udev... this may take a few seconds.
```

```
Starting udev: [ OK ]
```

```
Setting I/O Timeout (60s) for /dev/sda - SUCCESS!
```

Per SUSE Linux Enterprise Server 10 o SUSE Linux Enterprise Server 11, viene visualizzato un messaggio simile al seguente:

```
patching file /etc/udev/rules.d/50-udev-default.rules
```

```
Hunk #1 succeeded at 114 (offset 1 line).
```



```
Restarting udev ...this may take a few seconds.
```

```
Updating all available device nodes in /dev: done
```

3. Smontare l'immagine ISO.

Rigenerare un certificato SSL per Virtual Storage Console

Il certificato SSL viene generato quando si installa (VSC). Il nome distinto (DN) generato per il certificato SSL potrebbe non essere un nome comune (CN) riconosciuto dai computer client. Modificando le password del keystore e della chiave privata, è possibile rigenerare il certificato e creare un certificato specifico del sito.

A proposito di questa attività

È possibile attivare la diagnostica remota utilizzando la console di manutenzione e generare un certificato specifico del sito.

["Risposta della Knowledge base di NetApp 1075654: Virtual Storage Console 7.x: Implementazione dei certificati firmati dalla CA"](#)

Fasi

1. Accedere alla console di manutenzione.
2. Invio 1 per accedere a Application Configuration menu.
3. In Application Configuration, invio 3 Per arrestare il servizio VSC.
4. Invio 7 Per rigenerare il certificato SSL.

Requisiti per la registrazione di VSC in un ambiente con più vCenter Server

Se si utilizza Virtual Storage Console per VMware vSphere in un ambiente in cui è presente un singolo client VMware vSphere HTML5. Se si gestiscono più istanze di vCenter Server, è necessario registrare un'istanza di VSC con ciascun vCenter Server in modo che vi sia un'associazione 1:1 tra VSC e vCenter Server. Questa operazione consente di gestire tutti i server che eseguono vCenter 6.0 o versioni successive in modalità Linked e non Linked da un singolo client vSphere HTML5.



Se si desidera utilizzare VSC con un vCenter Server, è necessario aver impostato o registrato un'istanza VSC per ogni istanza di vCenter Server che si desidera gestire. Ogni istanza VSC registrata deve essere della stessa versione.

Linked mode viene installato automaticamente durante l'implementazione di vCenter Server. Linked mode utilizza Microsoft Active Directory Application Mode (ADAM) per memorizzare e sincronizzare i dati su più sistemi vCenter Server.

L'utilizzo del client vSphere HTML5 per eseguire attività VSC su più vCenter Server richiede quanto segue:

- Ogni vCenter Server nell'inventario VMware che si desidera gestire deve disporre di un singolo server VSC registrato con esso in un'unica associazione 1:1.

Ad esempio, è possibile avere il server VSC A registrato su vCenter Server A, il server VSC B registrato su vCenter Server B, il server VSC C registrato su vCenter Server C e così via.

Non è possibile* avere il server VSC A registrato su vCenter Server A e vCenter Server B.

Se un inventario VMware include un vCenter Server che non dispone di un server VSC registrato, ma sono presenti uno o più vCenter Server registrati con VSC, Quindi, è possibile visualizzare le istanze di VSC ed eseguire operazioni VSC per i server vCenter che hanno registrato VSC.

- È necessario disporre del privilegio View specifico di VSC per ogni vCenter Server registrato nel Single Sign-on (SSO).

È inoltre necessario disporre delle autorizzazioni RBAC corrette.

Quando si esegue un'attività che richiede di specificare un vCenter Server, la casella a discesa **vCenter Server** visualizza i vCenter Server disponibili in ordine alfanumerico. Il server vCenter predefinito è sempre il primo server nell'elenco a discesa.

Se la posizione dello storage è nota (ad esempio, quando si utilizza la procedura guidata **Provisioning** e il datastore si trova su un host gestito da uno specifico vCenter Server), l'elenco vCenter Server viene visualizzato come opzione di sola lettura. Ciò si verifica solo se si utilizza l'opzione del pulsante destro del mouse per selezionare un elemento nel client Web vSphere.

VSC avvisa l'utente quando tenta di selezionare un oggetto non gestito.

È possibile filtrare i sistemi storage in base a uno specifico vCenter Server dalla pagina di riepilogo di VSC. Viene visualizzata una pagina di riepilogo per ogni istanza di VSC registrata con un vCenter Server. È possibile gestire i sistemi di storage associati a un'istanza VSC specifica e a vCenter Server, ma è necessario mantenere separate le informazioni di registrazione per ciascun sistema di storage se si eseguono più istanze di VSC.

Configurare i file delle preferenze VSC

I file delle preferenze contengono impostazioni che controllano Virtual Storage Console per le operazioni di VMware vSphere. Nella maggior parte dei casi, non è necessario modificare le impostazioni di questi file. È utile sapere quali file delle preferenze (VSC) utilizzano.

VSC dispone di diversi file di preferenze. Questi file includono chiavi di immissione e valori che determinano il modo in cui VSC esegue varie operazioni. Di seguito sono riportati alcuni dei file delle preferenze utilizzati da VSC:

```
/opt/netapp/vscserver/etc/kamino/kaminoprefs.xml
```

```
/opt/netapp/vscserver/etc/vsc/vscPreferences.xml
```

In alcune situazioni potrebbe essere necessario modificare i file delle preferenze. Ad esempio, se si utilizza iSCSI o NFS e la subnet è diversa tra gli host ESXi e il sistema di storage, è necessario modificare i file delle

preferenze. Se non si modificano le impostazioni nel file delle preferenze, il provisioning del datastore non riesce perché VSC non può montare il datastore.

Impostare IPv4 o IPv6

Al file delle preferenze è stata aggiunta una nuova opzione `kaminoprefs.xml` Che è possibile impostare per abilitare il supporto per IPv4 o IPv6 per tutti i sistemi storage aggiunti a VSC.

- Il `default.override.option.provision.mount.datastore.address.family` il parametro è stato aggiunto a `kaminoprefs.xml` File delle preferenze per impostare un protocollo LIF dati preferito per il provisioning del datastore.

Questa preferenza è applicabile a tutti i sistemi storage aggiunti a VSC.

- I valori per la nuova opzione sono IPv4, IPv6, e. NONE.
- Per impostazione predefinita, il valore è impostato su NONE.

Valore	Descrizione
NESSUNO	<ul style="list-style-type: none">• Il provisioning avviene utilizzando lo stesso tipo di indirizzo IPv6 o IPv4 di dati LIF del tipo di cluster o LIF di gestione utilizzato per l'aggiunta dello storage.• Se lo stesso tipo di indirizzo IPv6 o IPv4 di dati LIF non è presente in , il provisioning avviene attraverso l'altro tipo di dati LIF, se disponibile.
IPv4	<ul style="list-style-type: none">• Il provisioning avviene utilizzando la LIF dei dati IPv4 nel selezionato.• Se non dispone di una LIF di dati IPv4, il provisioning avviene tramite LIF di dati IPv6, se disponibile in .
IPv6	<ul style="list-style-type: none">• Il provisioning avviene utilizzando la LIF dei dati IPv6 nel selezionato.• Se non dispone di una LIF dati IPv6, il provisioning avviene tramite LIF dati IPv4, se disponibile in .

Attiva il montaggio del datastore su diverse subnet

Se si utilizza iSCSI o NFS e la subnet è diversa tra gli host ESXi e il sistema di storage, è necessario modificare i file delle preferenze di Virtual Storage Console per VMware vSphere. Se non si modifica il file delle preferenze, il provisioning del datastore non riesce perché (VSC) non può montare il datastore.

A proposito di questa attività

Quando il provisioning del datastore non riesce, VSC registra i seguenti messaggi di errore:

```
Unable to continue. No ip addresses found when cross-referencing kernel ip addresses and addresses on the controller.
```

```
Unable to find a matching network to NFS mount volume to these hosts."
```

Fasi

1. Accedere all'istanza di vCenter Server.
2. Avviare la console di manutenzione utilizzando la macchina virtuale dell'appliance unificata.

["Accedere alle opzioni della console di manutenzione dell'appliance virtuale per VSC, VASA Provider e SRA"](#)

3. Invio 4 Per accedere all'opzione **supporto e diagnostica**.
4. Invio 2 Per accedere all'opzione **Access Diagnostic Shell**.
5. Invio `vi /opt/netapp/vscserver/etc/kamino/kaminoprefs.xml` per aggiornare `kaminoprefs.xml` file.
6. Aggiornare `kaminoprefs.xml` file.

Se si utilizza...	Eseguire questa operazione...
ISCSI	Modificare il valore della chiave di immissione <code>default.allow.iscsi.mount.networks</code> Da TUTTO al valore delle reti host ESXi.
NFS	Modificare il valore della chiave di immissione <code>default.allow.nfs.mount.networks</code> Da TUTTO al valore delle reti host ESXi.

Il file delle preferenze include valori di esempio per queste chiavi di immissione.



Il valore "ALL" non indica tutte le reti. Il valore "ALL" consente di utilizzare tutte le reti corrispondenti, tra l'host e il sistema di storage, per il montaggio degli archivi dati. Quando si specificano le reti host, è possibile attivare il montaggio solo attraverso le subnet specificate.

7. Salvare e chiudere `kaminoprefs.xml` file.

Accedere alle opzioni della console di manutenzione dell'appliance virtuale per VSC, VASA Provider e SRA

È possibile gestire le configurazioni di applicazioni, sistemi e reti utilizzando la console di manutenzione dell'appliance virtuale per Virtual Storage Console (VSC), VASA Provider e Storage Replication Adapter (SRA). È possibile modificare la password di amministratore e la password di manutenzione. È inoltre possibile generare pacchetti di supporto, impostare diversi livelli di log, visualizzare e gestire le configurazioni TLS e avviare la diagnostica remota.


Prima di iniziare

Dopo aver implementato l'appliance virtuale per VSC, VASA Provider e SRA, è necessario aver installato gli strumenti VMware.

A proposito di questa attività

- È necessario utilizzare "maint" come nome utente e password configurati durante l'implementazione per accedere alla console di manutenzione dell'appliance virtuale per VSC, VASA Provider e SRA.
- È necessario impostare una password per l'utente "diag" durante l'attivazione della diagnostica remota.

Fasi

1. Accedere alla scheda **Riepilogo** dell'appliance virtuale implementata.
2. Fare clic su  per avviare la console di manutenzione.

È possibile accedere alle seguenti opzioni della console di manutenzione:

◦ Configurazione dell'applicazione

Sono disponibili le seguenti opzioni:

- Visualizza il riepilogo dello stato del server
- Avviare il servizio Virtual Storage Console
- Arrestare il servizio Virtual Storage Console
- Avviare il provider VASA e il servizio SRA
- Arrestare il provider VASA e il servizio SRA
- Modificare la password utente 'amministratore'
- Generare nuovamente i certificati
- Keystore e certificati con reimpostazione a freddo
- Database con hard reset
- Modificare il livello DI REGISTRO per il servizio Virtual Storage Console
- Modificare il livello DI LOG per il provider VASA e il servizio SRA
- Visualizza la configurazione TLS
- Attiva il protocollo TLS
- Disattiva il protocollo TLS

◦ Configurazione del sistema

Sono disponibili le seguenti opzioni:

- Riavviare la macchina virtuale
- Arrestare la macchina virtuale
- Modificare la password utente "maint"
- Modificare il fuso orario
- Modificare il server NTP

È possibile fornire un indirizzo IPv6 per il server NTP.

- Attiva/disattiva accesso SSH
- Aumentare la dimensione del disco jail (/jail)
- Eseguire l'upgrade
- Installare VMware Tools

◦ **Configurazione di rete**

Sono disponibili le seguenti opzioni:

- Visualizzare le impostazioni dell'indirizzo IP
- Modificare le impostazioni dell'indirizzo IP

È possibile utilizzare questa opzione per modificare l'indirizzo IP post-implementazione in IPv6.

- Visualizzare le impostazioni di ricerca dei nomi di dominio
- Modificare le impostazioni di ricerca dei nomi di dominio
- Visualizza percorsi statici
- Modificare i percorsi statici

È possibile utilizzare questa opzione per aggiungere un percorso IPv6.

- Eseguire il commit delle modifiche
- Eseguire il ping di un host

È possibile utilizzare questa opzione per eseguire il ping a un host IPv6.

- Ripristinare le impostazioni predefinite

◦ **Supporto e diagnostica**

Sono disponibili le seguenti opzioni:

- Generare bundle di supporto
- Accedere alla shell di diagnostica
- Abilitare l'accesso remoto alla diagnostica

Informazioni correlate

[File di log del provider VSC e VASA](#)

Modificare la password dell'amministratore

È possibile modificare la password di amministratore dell'appliance virtuale per VSC, VASA Provider e SRA post-implementazione utilizzando la console di manutenzione.

Fasi

1. Da vCenter Server, aprire una console per l'appliance virtuale per VSC, VASA Provider e SRA.
2. Accedere come utente di manutenzione.
3. Invio 1 Nella console di manutenzione selezionare **Application Configuration** (Configurazione

applicazione).

4. Invio **6** Per selezionare **Modifica password utente 'amministratore'**.
5. Immettere una password di almeno otto caratteri e un massimo di 63 caratteri.
6. Invio **y** nella finestra di dialogo di conferma.

Configurare l'alta disponibilità per l'appliance virtuale per VSC, VASA Provider e SRA

L'appliance virtuale per Virtual Storage Console (VSC), VASA Provider e Storage Replication Adapter (SRA) supporta una configurazione (ha) per fornire funzionalità ininterrotte di VSC, VASA Provider e SRA in caso di guasto.

L'appliance virtuale per VSC, VASA Provider e SRA si affida alle funzionalità VMware vSphere (ha) e vSphere fault tolerance (FT) per fornire . La soluzione (HA) offre un rapido ripristino in caso di interruzioni causate da:

- Errore host
- Errore di rete
- Errore della macchina virtuale (errore del sistema operativo guest)
- Arresto anomalo dell'applicazione (VSC, VASA Provider e SRA)

Non è richiesta alcuna configurazione aggiuntiva sull'appliance virtuale per fornire . Solo gli host vCenter Server e ESXi devono essere configurati con la funzionalità VMware vSphere ha o vSphere FT in base ai requisiti. Sia ha che FT richiedono host in cluster insieme allo storage condiviso. FT presenta requisiti e limitazioni aggiuntivi.

Oltre alla soluzione VMware vSphere ha e alla soluzione vSphere FT, l'appliance virtuale consente di mantenere sempre in esecuzione i servizi VSC, VASA Provider e SRA. Il processo watchdog dell'appliance virtuale monitora periodicamente tutti e tre i servizi e li riavvia automaticamente quando viene rilevato un qualsiasi tipo di errore. In questo modo si evitano gli errori delle applicazioni.



vCenter ha non è supportato dall'appliance virtuale per VSC, VASA Provider e SRA.

VMware vSphere ha

È possibile configurare l'ambiente vSphere in cui viene implementata l'appliance virtuale per la Virtual Storage Console (VSC), il provider VASA e l'adattatore di replica dello storage (SRA) per (ha). La funzionalità VMware ha offre protezione di failover da guasti hardware e guasti del sistema operativo negli ambienti virtuali.

La funzione VMware ha monitora le macchine virtuali per rilevare guasti al sistema operativo e all'hardware. Quando viene rilevato un errore, la funzione VMware ha riavvia le macchine virtuali sugli altri server fisici nel pool di risorse. L'intervento manuale non è necessario quando viene rilevato un guasto al server.

La procedura di configurazione di VMware ha dipende dalla versione di vCenter Server in uso. Ad esempio, è possibile utilizzare il seguente collegamento di riferimento e selezionare la versione di vCenter Server richiesta per visualizzare la procedura di configurazione di VMware ha.

["Documentazione VMware vSphere: Creazione e utilizzo di cluster ha vSphere"](#)

Tolleranza agli errori di VMware vSphere

La funzione Fault Tolerance (FT) di VMware vSphere offre (ha) a un livello superiore e consente di proteggere le macchine virtuali senza alcuna perdita di dati o connessioni. È necessario attivare o disattivare vSphere FT per l'appliance virtuale per VSC, VASA Provider e SRA dal server vCenter.

Assicurati che la licenza vSphere supporti FT con il numero di vCPU necessarie per l'appliance virtuale nel tuo ambiente (almeno 2 vCPU; 4 vCPU per ambienti su larga scala).

VSphere FT consente alle macchine virtuali di funzionare in modo continuo anche in caso di guasti al server. Quando vSphere FT è attivato su una macchina virtuale, viene creata automaticamente una copia della macchina virtuale primaria su un altro host (la macchina virtuale secondaria) selezionato da Distributed Resource Scheduler (DRS). Se DRS non è attivato, l'host di destinazione viene selezionato tra gli host disponibili. VSphere FT gestisce la macchina virtuale primaria e la macchina virtuale secondaria in modalità lockstep, con ogni mirroring dello stato di esecuzione della macchina virtuale primaria sulla macchina virtuale secondaria.

Quando si verifica un guasto hardware che causa il guasto della macchina virtuale primaria, la macchina virtuale secondaria rileva immediatamente il punto in cui si è arrestata la macchina virtuale primaria. La macchina virtuale secondaria continua a funzionare senza alcuna perdita di connessioni di rete, transazioni o dati.

Il sistema deve soddisfare i requisiti della CPU, i requisiti dei limiti delle macchine virtuali e i requisiti di licenza per la configurazione di vSphere FT per l'istanza di vCenter Server.

La procedura per configurare ha dipende dalla versione di vCenter Server. Ad esempio, è possibile utilizzare il seguente collegamento di riferimento e selezionare la versione di vCenter Server richiesta per visualizzare la procedura di configurazione di ha.

["Documentazione di VMware vSphere: Requisiti di tolleranza agli errori, limiti e licenze"](#)

Configurazioni MetroCluster supportate dall'appliance virtuale per VSC, provider VASA e SRA

L'appliance virtuale per la console di storage virtuale (VSC), il provider VASA e l'adattatore di replica dello storage (SRA) supporta gli ambienti che utilizzano le configurazioni MetroCluster IP e FC per ONTAP. La maggior parte di questo supporto è automatica. Tuttavia, potrebbero verificarsi alcune differenze quando si utilizza un ambiente MetroCluster con VSC e provider VASA.

Configurazioni MetroCluster e VSC

È necessario assicurarsi che VSC rilevi i controller del sistema di storage nel sito primario e nel sito secondario. In genere, VSC rileva automaticamente i controller dello storage. Se si utilizza una LIF di gestione del cluster, è consigliabile verificare che VSC abbia rilevato i cluster in entrambi i siti. In caso contrario, è possibile aggiungere manualmente i controller di storage a VSC. È inoltre possibile modificare le coppie di nome utente e password utilizzate da VSC per connettersi ai controller di storage.

Quando si verifica uno switchover, il sul sito secondario prende il controllo. Questi hanno il suffisso "-mc" aggiunto ai loro nomi. Se si verifica un'operazione di switchover durante l'esecuzione di operazioni come il

provisioning di un datastore, il nome di dove risiede il datastore viene modificato in modo da includere il suffisso “-mc”. Questo suffisso viene eliminato quando si verifica lo switchback e il controllo di ripristino sul sito primario.



Se è stata aggiunta direttamente la configurazione MetroCluster a VSC, dopo lo switchover, la modifica nel nome della SVM (l'aggiunta del suffisso “-mc”) non viene riflessa. Tutte le altre operazioni di switchover continuano a essere eseguite normalmente.

Quando si verifica uno switchover o uno switchback, VSC potrebbe impiegare alcuni minuti per rilevare e rilevare automaticamente i cluster. Se ciò accade durante un'operazione VSC, ad esempio il provisioning di un datastore, potrebbe verificarsi un ritardo.

Configurazioni MetroCluster e provider VASA

Il provider VASA supporta automaticamente gli ambienti che utilizzano configurazioni MetroCluster. Lo switchover è trasparente negli ambienti provider VASA. Impossibile aggiungere direttamente al provider VASA.



IL provider VASA non aggiunge il suffisso “-mc” ai nomi del sito secondario dopo uno switchover.

Configurazioni MetroCluster e SRA

SRA non supporta le configurazioni MetroCluster.

Informazioni sul copyright

Copyright © 2024 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 COMMERCIALIZZABILITÀ 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 CONSEGUENZIALE (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.