



Implementazione e aggiornamento

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/concept-virtual-storage-console-overview.html> on March 21, 2024. Always check docs.netapp.com for the latest.

Sommario

- Implementazione e aggiornamento 1
 - Panoramica dell’appliance virtuale per VSC, VASA Provider e SRA 1
 - Workflow di implementazione per nuovi utenti di VSC, provider VASA e appliance virtuali SRA 2
 - Requisiti per l’implementazione dell’appliance virtuale per VSC, VASA Provider e SRA 5
 - Implementare o aggiornare VSC, VASA Provider e SRA. 9
 - Configurare la Virtual Storage Console per l’ambiente VMware vSphere 20
 - Configurare la Virtual Storage Console per l’ambiente del sistema di storage VMware vSphere 34
 - Funzionalità di controllo degli accessi basate sui ruoli di vCenter Server in VSC per VMware vSphere ... 38
 - Configurare Storage Replication Adapter per il disaster recovery 48
 - Risolvere i problemi relativi all’appliance virtuale per VSC, VASA Provider e SRA 50

Implementazione e aggiornamento

Panoramica dell'appliance virtuale per VSC, VASA Provider e SRA

L'appliance virtuale per Virtual Storage Console (VSC), VASA Provider e Storage Replication Adapter (SRA) offre una gestione end-to-end del ciclo di vita delle macchine virtuali negli ambienti VMware che utilizzano i sistemi storage NetApp. Semplifica lo storage e la gestione dei dati per gli ambienti VMware consentendo agli amministratori di gestire lo storage direttamente all'interno di vCenter Server.

Con vSphere 6.5, VMware ha introdotto un nuovo client basato su HTML5 chiamato vSphere Client. La versione 9.6 dell'appliance virtuale per VSC, VASA Provider e SRA supporta solo vSphere Client. L'appliance virtuale per VSC, VASA Provider e SRA si integra con vSphere Client e consente di utilizzare i servizi SSO (Single Sign-on). In un ambiente con più istanze di vCenter Server, ogni istanza di vCenter Server che si desidera gestire deve avere la propria istanza registrata di VSC.

Ogni componente dell'appliance virtuale per VSC, VASA Provider e SRA offre funzionalità che consentono di gestire lo storage in modo più efficiente.

Virtual Storage Console (VSC)

VSC consente di eseguire le seguenti attività:

- Aggiunta di controller di storage, assegnazione di credenziali e impostazione di autorizzazioni per controller di storage a VSC che possono essere sfruttate sia da SRA che dal provider VASA
- Eseguire il provisioning degli archivi dati
- Monitorare le performance dei datastore e delle macchine virtuali nell'ambiente vCenter Server
- Controllare l'accesso degli amministratori agli oggetti vCenter Server utilizzando RBAC (role-based access control) a due livelli:
 - Oggetti vSphere, come macchine virtuali e datastore

Questi oggetti vengono gestiti utilizzando vCenter Server RBAC.

- Storage ONTAP

I sistemi storage vengono gestiti utilizzando ONTAP RBAC.

- Visualizzare e aggiornare le impostazioni host degli host ESXi connessi allo storage

Le operazioni di provisioning VSC traggono vantaggio dall'utilizzo del plug-in NFS per VMware VMware vStorage API per l'integrazione array (VAAI). Il plug-in NFS per VAAI è una libreria software che integra le librerie di dischi virtuali VMware installate sull'host ESXi. Il pacchetto VMware VAAI consente l'offload di determinate attività dagli host fisici all'array di storage. È possibile eseguire attività come il thin provisioning e l'accelerazione hardware a livello di array per ridurre il carico di lavoro sugli host ESXi. La funzione di offload delle copie e di riserva dello spazio migliorano le prestazioni delle operazioni VSC.

Il plug-in NetApp NFS per VAAI non viene fornito con VSC. Tuttavia, è possibile scaricare il pacchetto di installazione del plug-in e ottenere le istruzioni per l'installazione del plug-in da .

Provider VASA

IL provider VASA per ONTAP utilizza le API VMware vSphere per la consapevolezza dello storage (VASA) per inviare informazioni sullo storage utilizzato da VMware vSphere al server vCenter. L'appliance virtuale per VSC, VASA Provider e SRA, VASA Provider è integrata con VSC e VASA Provider consente di eseguire le seguenti attività:

- Provisioning di datastore vVol (VMware Virtual Volumes)
- Creare e utilizzare profili di funzionalità storage che definiscono diversi obiettivi di livello di servizio dello storage (SLO) per il proprio ambiente
- Verificare la conformità tra i datastore e i profili di funzionalità dello storage
- Impostare gli allarmi per avvisare l'utente quando volumi e aggregati stanno raggiungendo i limiti di soglia
- Monitorare le performance dei dischi delle macchine virtuali (VMDK) e delle macchine virtuali create negli archivi dati vVols

Se si utilizza ONTAP 9.6 o versioni precedenti, il provider VASA comunica con il server vCenter utilizzando le API VASA e comunica con ONTAP utilizzando le API chiamate ZAPI. Per visualizzare la dashboard vVol per ONTAP 9.6 e versioni precedenti, è necessario aver installato e registrato il server vCenter. Se si utilizza ONTAP 9.7, non è necessario essere registrati con il provider VASA per visualizzare la dashboard di vVol.



Per ONTAP 9.6 e versioni precedenti, il provider VASA richiede un'istanza dedicata dei servizi API di OnCommand. Un'istanza dei servizi API di OnCommand non può essere condivisa con più istanze del provider VASA.

Storage Replication Adapter (SRA)

Quando SRA viene attivato e utilizzato insieme a VMware Site Recovery Manager (SRM), è possibile ripristinare i datastore e le macchine virtuali di vCenter Server in caso di guasto. SRA consente di configurare siti protetti e siti di ripristino nell'ambiente per il disaster recovery in caso di guasto.

Informazioni correlate

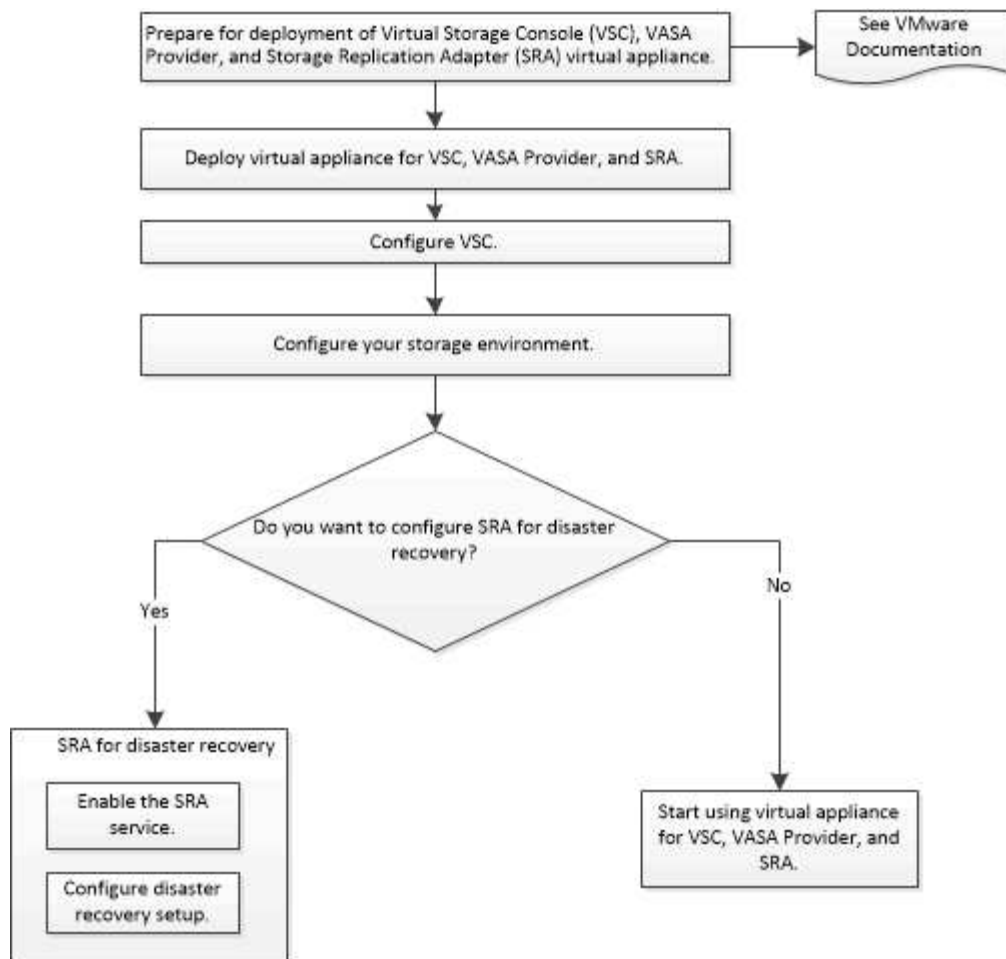
["Documentazione NetApp: Servizi API OnCommand"](#)

["Documentazione NetApp: Plug-in NetApp NFS per VMware VAAI"](#)

["Supporto NetApp"](#)

Workflow di implementazione per nuovi utenti di VSC, provider VASA e appliance virtuali SRA

Se non hai mai utilizzato un prodotto NetApp VSC per la prima volta in VMware, devi configurare vCenter Server e un host ESXi prima di implementare e configurare l'appliance virtuale per VSC, VASA Provider e SRA.



Workflow di implementazione per gli utenti esistenti di VSC, provider VASA e SRA

Le versioni 9.7 dell'appliance virtuale per VSC, VASA Provider e SRA supportano l'aggiornamento diretto alla versione più recente.

Le versioni precedenti di singole applicazioni come VSC, VASA Provider e SRA utilizzano un processo di aggiornamento diverso. Se nel programma di installazione è installato VSC, VASA Provider o SRA, eseguire le seguenti operazioni:

1. Implementa l'ultima release dell'appliance virtuale per VSC, VASA Provider e SRA.
2. Eseguire la migrazione dei dati di configurazione esistenti.

I dati di configurazione includono le credenziali del sistema di storage e le preferenze presenti in `kaminoprefs.xml` e `vscPreferences.xml` file.

"Configurare i file delle preferenze VSC"

In molti casi, potrebbe non essere necessario migrare i dati di configurazione. Tuttavia, se i file delle preferenze sono stati personalizzati in precedenza, potrebbe essere necessario esaminarli e apportare modifiche simili all'appliance virtuale appena implementata. È possibile eseguire una delle seguenti operazioni:

- Utilizzare ["Utility di importazione per SnapCenter e console di storage virtuale"](#) Per migrare le credenziali del sistema storage da VSC 6.X e SRA 4.X alla nuova implementazione.

- Aggiungere i sistemi storage all'appliance virtuale appena implementata e specificare le credenziali man mano che vengono aggiunte.

Se si esegue l'aggiornamento dal provider VASA 6.X, è necessario annullare la registrazione del provider VASA prima di eseguire l'aggiornamento. Per ulteriori informazioni, consultare la documentazione relativa alla versione corrente.

Se si esegue anche l'aggiornamento da SRA 4.0 o versioni precedenti:

- Se si utilizza SRA 4.0P1, è necessario prima eseguire l'aggiornamento a SRA 9.6 e solo in questo caso è possibile eseguire un aggiornamento in-place di SRA 9.6 alla versione più recente.

["Effettua l'upgrade all'appliance virtuale 9.7.1 per VSC, VASA Provider e SRA"](#)

- Se si utilizza SRA 2.1 o 3.0, è necessario prima annotare i dettagli della configurazione del sito esistente.

Guida all'installazione e alla configurazione di Storage Replication Adapter 4.0 per ONTAP contiene le istruzioni dettagliate nella sezione "Panoramica sull'aggiornamento". Queste release SRA utilizzano anche il provider VASA, pertanto è necessario annullare la registrazione del provider VASA e implementare la versione più recente dell'appliance virtuale per VSC, VASA Provider e SRA. La versione precedente del server (.ova) può essere rimosso al termine dell'aggiornamento.

Per qualsiasi aggiornamento SRA, il software SRA (l'adattatore sul server Site Recovery Manager, installato da .msi File) deve essere rimosso dal server Site Recovery Manager. È possibile utilizzare il pannello di controllo del sistema Windows per disinstallare il software e installare il software SRA più recente sul server SRA utilizzando .msi file.

Se si dispone dell'implementazione del provider VASA, dopo l'aggiornamento dalla configurazione esistente, è necessario configurare le dimensioni della memoria per l'appliance virtuale in modo che siano 12 GB utilizzando Edit Settings opzione. È inoltre necessario modificare la prenotazione della memoria virtuale. La macchina virtuale deve essere spenta per modificare le dimensioni della memoria.

Un aggiornamento diretto da qualsiasi release precedente alla 9.7 a 9.7P2 o successiva non è supportato dall'appliance virtuale per VSC, VASA Provider e SRA. Prima di eseguire l'aggiornamento a qualsiasi versione successiva, è necessario aggiornare la configurazione esistente alla versione 9.7 dell'appliance virtuale per VSC, VASA Provider e SRA.

Se si intende implementare l'ultima versione dell'appliance virtuale, è necessario consultare l'argomento "requisiti per l'implementazione dell'appliance virtuale per VSC, VASA Provider e SRA". L'argomento "aggiornamento alla versione 9.6 dell'appliance virtuale per VSC, VASA Provider e SRA" contiene informazioni sull'esecuzione di un aggiornamento in-place.

Informazioni correlate

["ToolChest NetApp: Utility di importazione NetApp per SnapCenter e console di storage virtuale"](#)

["Requisiti per l'implementazione dell'appliance virtuale per VSC, VASA Provider e SRA"](#)

["Effettua l'upgrade all'appliance virtuale 9.7.1 per VSC, VASA Provider e SRA"](#)

Requisiti per l'implementazione dell'appliance virtuale per VSC, VASA Provider e SRA

Prima di implementare l'appliance virtuale per Virtual Storage Console (VSC), VASA Provider e Storage Replication Adapter (SRA), è necessario conoscere i requisiti di implementazione e decidere le attività da eseguire. In base alle tue attività, puoi scegliere il modello di implementazione per l'implementazione dell'appliance virtuale per VSC, VASA Provider e SRA.

Requisiti delle porte per VSC

Per impostazione predefinita, (VSC) utilizza le porte designate per abilitare la comunicazione tra i suoi componenti, che includono i sistemi storage e VMware vCenter Server. Se si dispone di firewall abilitati, assicurarsi che i firewall siano impostati in modo da consentire eccezioni.

Per firewall diversi da Windows, è necessario concedere manualmente l'accesso a porte specifiche utilizzate da VSC. Se non si concede l'accesso a queste porte, viene visualizzato un messaggio di errore simile al seguente.

Impossibile comunicare con il server

VSC utilizza le seguenti porte TCP bidirezionali predefinite:

Numero di porta predefinito	Descrizione
9083	Quando questa opzione è attivata, il provider VASA e l'adattatore di replica dello storage (SRA) utilizzano questa porta per comunicare con il server vCenter. Questa porta è necessaria anche per ottenere le impostazioni TCP/IP.
443	A seconda di come sono state configurate le credenziali, VMware vCenter Server e i sistemi storage sono in attesa di comunicazioni sicure su questa porta.
8143	VSC è in attesa di comunicazioni sicure su questa porta.
7	VSC invia una richiesta echo a ONTAP per verificare la raggiungibilità ed è necessaria solo quando si aggiunge un sistema storage e può essere disattivata in un secondo momento.



Prima di implementare l'appliance virtuale per VSC, VASA Provider e SRA, è necessario aver attivato il protocollo ICMP (Internet Control message Protocol).

Se ICMP è disattivato, la configurazione iniziale dell'appliance virtuale per VSC, VASA Provider e SRA non riesce e VSC non può avviare i servizi VSC e VASA Provider dopo l'implementazione. Dopo l'implementazione, è necessario attivare manualmente i servizi VSC e VASA Provider.

Requisiti di spazio e dimensioni per l'appliance virtuale per VSC, VASA Provider e SRA

Prima di implementare l'appliance virtuale per Virtual Storage Console (VSC), VASA Provider e Storage Replication Adapter (SRA), è necessario conoscere i requisiti di spazio per il pacchetto di implementazione e alcuni requisiti di base del sistema host.

- **Requisiti di spazio per il pacchetto di installazione**

- 2.1 GB per installazioni con thin provisioning
- 54.0 GB per installazioni con thick provisioning

- **Requisiti di dimensionamento del sistema host**

- ESXi 6.5U2 o versione successiva
- Memoria consigliata: 12 GB di RAM
- CPU consigliate: 2

Sistemi storage, licenze e applicazioni supportati per appliance virtuali per VSC, VASA Provider e SRA

Prima di iniziare l'implementazione dell'appliance virtuale per Virtual Storage Console (VSC), VASA Provider e Storage Replication Adapter (SRA), è necessario conoscere i requisiti di base del sistema di storage, i requisiti delle applicazioni e i requisiti di licenza.

(IMT) contiene le informazioni più recenti sulle versioni supportate di ONTAP, vCenter Server, host ESXi, applicazioni plug-in e Gestione ripristino sito (SRM).

- ["Matrice di interoperabilità Tool: VSC 9.7.1"](#)
- ["Matrice di interoperabilità Tool: VASA Provider 9.7.1"](#)
- ["Matrice di interoperabilità Tool: SRA 9.7.1"](#)

È necessario attivare la licenza FlexClone per eseguire operazioni di snapshot delle macchine virtuali e operazioni di clonazione per gli archivi dati VMware Virtual Volumes (vVols).

Storage Replication Adapter (SRA) richiede le seguenti licenze:

- Licenza SnapMirror

Per eseguire operazioni di failover per SRA, è necessario attivare la licenza SnapMirror.

- Licenza FlexClone

È necessario attivare la licenza FlexClone per eseguire operazioni di failover di test per SRA.

Per visualizzare gli IOPS di un datastore, è necessario attivare il controllo Storage i/o o o deselezionare la casella di controllo Disable Storage i/o statistics collection (Disattiva raccolta statistiche i/o storage) nella configurazione Storage i/o control (controllo i/o storage). È possibile attivare il controllo i/o dello storage solo se si dispone della licenza Enterprise Plus di VMware.

- ["Articolo della Knowledge base di VMware 1022091: Risoluzione dei problemi relativi al controllo i/o dello storage"](#)
- ["Documentazione VMware vSphere: Requisiti per il controllo i/o dello storage"](#)

Considerazioni e requisiti per l'implementazione dell'appliance virtuale per VSC, VASA Provider e SRA

Prima di implementare l'appliance virtuale per Virtual Storage Console (VSC), VASA Provider e Storage Replication Adapter (SRA), è consigliabile pianificare l'implementazione e decidere come configurare VSC, VASA Provider e SRA nel proprio ambiente.

La seguente tabella presenta una panoramica di ciò che occorre prendere in considerazione prima di implementare l'appliance virtuale per VSC, VASA Provider e SRA.

Considerazioni	Descrizione
Prima implementazione dell'appliance virtuale per VSC, VASA Provider e SRA	L'implementazione dell'appliance virtuale per VSC, VASA Provider e SRA installa automaticamente le funzionalità VSC. "Implementazione o aggiornamento di VSC, VASA Provider e SRA" "Workflow di implementazione per nuovi utenti di VSC, provider VASA e appliance virtuali SRA"

Considerazioni	Descrizione
Aggiornamento da un'implementazione esistente di VSC	<p>La procedura di aggiornamento da un'implementazione esistente di VSC all'appliance virtuale per VSC, VASA Provider e SRA dipende dalla versione di VSC e dalla distribuzione di VSC, VASA Provider e SRA. La sezione relativa ai flussi di lavoro di implementazione e all'aggiornamento contiene ulteriori informazioni. "Workflow di implementazione per gli utenti esistenti di VSC, provider VASA e SRA"</p> <p>Best practice prima di un aggiornamento:</p> <ul style="list-style-type: none"> • È necessario registrare le informazioni relative ai sistemi storage utilizzati e alle relative credenziali. <p>Dopo l'aggiornamento, verificare che tutti i sistemi storage siano stati rilevati automaticamente e che dispongano delle credenziali corrette.</p> <ul style="list-style-type: none"> • Se sono stati modificati i ruoli VSC standard, è necessario copiarli per salvare le modifiche. <p>VSC sovrascrive i ruoli standard con le impostazioni predefinite correnti ogni volta che si riavvia il servizio VSC.</p>
Rigenerazione di un certificato SSL per VSC	<p>Il certificato SSL viene generato automaticamente quando si implementa l'appliance virtuale per VSC, VASA Provider e SRA. Potrebbe essere necessario rigenerare il certificato SSL per creare un certificato specifico del sito. "Rigenerare un certificato SSL per"</p>
Impostazione dei valori del server ESXi	<p>Sebbene la maggior parte dei valori del server ESXi sia impostata per impostazione predefinita, è consigliabile controllarli. Questi valori si basano su test interni. A seconda dell'ambiente in uso, potrebbe essere necessario modificare alcuni valori per migliorare le performance.</p> <ul style="list-style-type: none"> • "Configurare le impostazioni di multipathing e timeout del server ESXi" • "Valori host ESXi impostati utilizzando Virtual Storage Console per VMware vSphere"
Valori di timeout del sistema operativo guest	<p>Gli script di timeout del sistema operativo guest (sistema operativo guest) impostano i valori di timeout i/o SCSI per i sistemi operativi guest Linux, Solaris e Windows supportati per garantire il corretto funzionamento del failover.</p>

La seguente tabella presenta una panoramica delle operazioni necessarie per configurare l'appliance virtuale

per VSC, VASA Provider e SRA.

Considerazioni	Descrizione
Requisiti di RBAC (role-based access control)	<p>VSC supporta sia vCenter Server RBAC che ONTAP RBAC. L'account utilizzato per registrare VSC su vCenter Server (utilizzando <code>https://<appliance_ip>:8143/Register.html</code>) Deve essere un amministratore di vCenter Server (assegnato al ruolo di amministratore o amministratore di vCenter Server). Se si intende eseguire VSC come amministratore, è necessario disporre di tutte le autorizzazioni e i privilegi necessari per tutte le attività.</p> <p>Se l'azienda richiede di limitare l'accesso agli oggetti vSphere, è possibile creare e assegnare ruoli VSC standard agli utenti per soddisfare i requisiti di vCenter Server.</p> <p>È possibile creare i ruoli ONTAP consigliati utilizzando Gestione di sistema ONTAP utilizzando il file JSON fornito con l'appliance virtuale per VSC, provider VASA e SRA.</p> <p>Se un utente tenta di eseguire un'attività senza i privilegi e le autorizzazioni corretti, le opzioni dell'attività non sono disponibili.</p> <ul style="list-style-type: none">• "Ruoli standard in bundle con l'appliance virtuale per VSC, VASA Provider e SRA"• "Ruoli ONTAP consigliati quando si utilizza VSC per VMware vSphere"
Versione di ONTAP	I sistemi storage devono eseguire ONTAP 9.1, 9.3, 9.5, 9.6 o 9.7.
Profili di capacità dello storage	<p>Per utilizzare i profili delle funzionalità di storage o per impostare gli allarmi, è necessario attivare il provider VASA per ONTAP. Dopo aver attivato il provider VASA, è possibile configurare gli archivi dati di VMware Virtual Volumes (vVol) e creare e gestire gli allarmi e i profili delle funzionalità di storage.</p> <p>Gli allarmi avvisano l'utente quando un volume o un aggregato è quasi alla capacità massima o quando un datastore non è più conforme al profilo di capacità dello storage associato.</p>

Implementare o aggiornare VSC, VASA Provider e SRA

È necessario scaricare e implementare l'appliance virtuale per VSC, VASA Provider e

SRA nell'ambiente VMware vSphere, quindi configurare le applicazioni richieste in base alle attività che si desidera eseguire utilizzando VSC, VASA Provider e SRAVSC, VASA Provider e SRA.

Informazioni correlate

[Abilitare il provider VASA per la configurazione di datastore virtuali](#)

Come scaricare l'appliance virtuale per VSC, VASA Provider e SRA

È possibile scaricare .ova File per l'appliance virtuale per Virtual Storage Console, VASA Provider e Storage Replication Adapter da .

Il .ova Il file include VSC, VASA Provider e SRA. Una volta completata l'implementazione, tutti e tre i prodotti vengono installati nell'ambiente in uso. Per impostazione predefinita, VSC inizia a funzionare non appena si decide il modello di implementazione successivo e si sceglie se attivare il provider VASA e SRA in base ai propri requisiti.

È possibile scaricare l'appliance virtuale per VSC, VASA Provider e SRA da ["Sito di supporto NetApp"](#) utilizzando la pagina di download del software.

Se si desidera abilitare SRA nell'implementazione dell'appliance virtuale per VSC, VASA Provider e SRA, è necessario aver installato il plug-in SRA sul server SRM (Site Recovery Manager). È possibile scaricare il file di installazione per il plug-in SRA dal menu **Storage Replication Adapter for ONTAP** nella sezione **Download software**.

Implementa l'appliance virtuale per VSC, VASA Provider e SRA

È necessario implementare l'appliance virtuale per Virtual Storage Console (VSC), VASA Provider e Storage Replication Adapter (SRA) nel proprio ambiente e specificare i parametri richiesti per poter utilizzare l'appliance.

Prima di iniziare

- È necessario eseguire una release supportata di vCenter Server.



L'appliance virtuale per VSC, VASA Provider e SRA può essere registrata con un'implementazione Windows di vCenter Server o con un'implementazione VMware vCenter Server Virtual Appliance (vCSA).

["Matrice di interoperabilità Tool: VSC 9.7"](#)

- È necessario aver configurato e configurato l'ambiente vCenter Server.
- È necessario aver configurato un host ESXi per la macchina virtuale.
- È necessario aver scaricato .ova file.
- È necessario disporre delle credenziali di accesso dell'amministratore per l'istanza di vCenter Server.
- È necessario disconnettersi e chiudere tutte le sessioni del browser di vSphere Client ed eliminare la cache del browser per evitare qualsiasi problema di cache del browser durante l'implementazione dell'appliance virtuale per VSC, VASA Provider e SRA.

[Pulire i pacchetti di plug-in scaricati dalla cache di vSphere](#)

- È necessario aver attivato il protocollo ICMP (Internet Control message Protocol).

Se ICMP è disattivato, la configurazione iniziale dell'appliance virtuale per VSC, VASA Provider e SRA non riesce e VSC non può avviare i servizi VSC e VASA Provider dopo l'implementazione. Dopo l'implementazione, è necessario attivare manualmente i servizi VSC e VASA Provider.

A proposito di questa attività

Se si sta implementando una nuova installazione dell'appliance virtuale per VSC, VASA Provider e SRA, il provider VASA viene attivato per impostazione predefinita. Tuttavia, in caso di aggiornamento da una versione precedente dell'appliance virtuale, lo stato del provider VASA viene mantenuto e potrebbe essere necessario attivare il provider VASA manualmente.

"Abilitare il provider VASA per la configurazione di datastore virtuali"

Fasi

1. Accedere al client vSphere.
2. Selezionare **Home > host e cluster**.
3. Fare clic con il pulsante destro del mouse sul data center richiesto, quindi fare clic su **Deploy OVA template** (implementa modello OVA).
4. Selezionare il metodo appropriato per fornire il file di implementazione per VSC, VASA Provider e SRA, quindi fare clic su **Avanti**.

Posizione	Azione
URL	Fornire l'URL per .ova File per l'appliance virtuale per VSC, VASA Provider e SRA.
Cartella	Selezionare .ova File per l'appliance virtuale per VSC, VASA Provider e SRA dalla posizione salvata.

5. Immettere i dettagli per personalizzare la procedura guidata di implementazione.

Vedere "[Considerazioni sulla personalizzazione dell'implementazione](#)" per dettagli completi.

6. Esaminare i dati di configurazione, quindi fare clic su **Avanti** per terminare l'implementazione.

Mentre si attende il completamento della distribuzione, è possibile visualizzare l'avanzamento della distribuzione dalla scheda **Tasks**.

7. Accendere la macchina virtuale dell'appliance, quindi aprire una console della macchina virtuale che esegue l'appliance virtuale.
8. Verificare che i servizi VSC, VASA Provider e SRA siano in esecuzione al termine dell'implementazione.
9. Se l'appliance virtuale per VSC, VASA Provider e SRA non è registrata con alcun vCenter Server, utilizzare `https://appliance_ip:8143/Register.html` Per registrare l'istanza di VSC.
10. Disconnettersi e accedere nuovamente a vSphere Client per visualizzare l'appliance virtuale implementata per VSC, VASA Provider e SRA.

L'aggiornamento del plug-in nel client vSphere potrebbe richiedere alcuni minuti.



Se non è possibile visualizzare il plug-in anche dopo l'accesso, è necessario pulire la cache del client vSphere. [Pulire i pacchetti di plug-in scaricati dalla cache di vSphere](#)

Al termine



Se si utilizza ONTAP 9.6 o versioni precedenti, per visualizzare la dashboard di vVol, è necessario scaricare e installare . Tuttavia, per ONTAP 9.7 non è necessario essere registrati presso il provider VASA.

[Registrati con l'appliance virtuale per VSC, VASA Provider e SRA](#)

Considerazioni sulla personalizzazione dell'implementazione

È necessario considerare alcune limitazioni durante la personalizzazione dell'implementazione di appliance virtuali per VSC, VASA Provider e SRA.

Password utente amministratore dell'appliance

Non utilizzare spazi nella password dell'amministratore.

Credenziali della console di manutenzione dell'appliance

È necessario accedere alla console di manutenzione utilizzando il nome utente "maint". È possibile impostare la password per l'utente "maint" durante l'implementazione. È possibile utilizzare il menu **Application Configuration** della console di manutenzione dell'appliance virtuale per VSC, VASA Provider e SRA per modificare la password.

Credenziali dell'amministratore di vCenter Server

È possibile impostare le credenziali di amministratore per vCenter Server durante l'implementazione dell'appliance virtuale per VSC, VASA Provider e SRA.

Se la password per vCenter Server cambia, è possibile aggiornare la password per l'amministratore utilizzando il seguente URL: <https://<IP>:8143/Register.html> Dove l'indirizzo IP è dell'appliance virtuale per VSC, VASA Provider e SRA forniti durante l'implementazione.

Indirizzo IP del server vCenter

- Specificare l'indirizzo IP (IPv4 o IPv6) dell'istanza di vCenter Server a cui si desidera registrare l'appliance virtuale per VSC, VASA Provider e SRA.

Il tipo di certificati VSC e VASA generati dipende dall'indirizzo IP (IPv4 o IPv6) fornito durante l'implementazione. Durante l'implementazione dell'appliance virtuale per VSC, VASA Provider e SRA, se non sono stati immessi dettagli IP statici e DHCP, la rete fornisce indirizzi IPv4 e IPv6.

- L'appliance virtuale per VSC, il provider VASA e l'indirizzo IP SRA utilizzati per la registrazione con vCenter Server dipende dal tipo di indirizzo IP di vCenter Server (IPv4 o IPv6) immesso nella procedura guidata di implementazione.

I certificati VSC e VASA verranno generati utilizzando lo stesso tipo di indirizzo IP utilizzato durante la registrazione di vCenter Server.



IPv6 è supportato solo con vCenter Server 6.7 e versioni successive.

Proprietà di rete dell'appliance

Se non si utilizza DHCP, specificare un nome host DNS valido (non qualificato), l'indirizzo IP statico per l'appliance virtuale per VSC, VASA Provider e SRA e gli altri parametri di rete. Tutti questi parametri sono necessari per un'installazione e un funzionamento corretti.

Abilitare il provider VASA per la configurazione di datastore virtuali

Per impostazione predefinita, l'appliance virtuale per Virtual Storage Console (VSC), VASA Provider e Storage Replication Adapter (SRA) dispone della funzione VASA Provider (Provider VASA) attivata. È possibile configurare gli archivi dati di VMware Virtual Volumes (vVols) con i profili di funzionalità storage richiesti per ciascun datastore vVols.

Prima di iniziare

- È necessario aver configurato l'istanza di vCenter Server e ESXi.
- È necessario aver implementato l'appliance virtuale per VSC, VASA Provider e SRA.

A proposito di questa attività

Se la funzionalità del provider VASA viene disattivata prima dell'aggiornamento alla versione 9.7.1 dell'appliance virtuale per Virtual Storage Console (VSC), VASA Provider e Storage Replication Adapter (SRA), la funzionalità del provider VASA rimane disattivata dopo l'aggiornamento. Questa release consente di attivare la funzione di replica vVols per gli archivi dati vVols.

Fasi

1. Accedere all'interfaccia utente Web di VMware vSphere.
2. Dal client vSphere, fare clic su **Menu** > **Virtual Storage Console**.
3. Fare clic su **Impostazioni**.
4. Fare clic su **Manage Capabilities** (Gestisci funzionalità) nella scheda **Administrative Settings** (Impostazioni amministrative).
5. Nella finestra di dialogo **Manage Capabilities** (Gestisci funzionalità), selezionare l'interno del provider VASA da attivare.
6. Se si desidera utilizzare la funzionalità di replica per gli archivi dati vVols, utilizzare il pulsante di commutazione **Enable vVols Replication** (attiva replica vVols).
7. Inserire l'indirizzo IP dell'appliance virtuale per VSC, VASA Provider e SRA e la password dell'amministratore, quindi fare clic su **Apply** (Applica).

Al termine

Se si utilizzano cluster ONTAP 9.6 o precedenti, è necessario registrarsi con il provider VASA per ottenere informazioni dettagliate sui datastore vVol e sulle macchine virtuali utilizzati nei report datastore SAN vVols VM e SAN vVols. Tuttavia, se si utilizza ONTAP 9.7 o versione successiva, non è necessario registrarsi con il provider VASA.

Registrati con l'appliance virtuale per VSC, VASA Provider e SRA

Se si utilizza ONTAP 9.6 o versioni precedenti, la dashboard di vVol consente di

visualizzare i dettagli dei datastore e delle macchine virtuali di VMware Virtual Volumes (vVol) solo se si è registrati al provider VASA per ottenere i dati per i report di vVol VM e datastore.

Prima di iniziare

È necessario aver scaricato la versione 2.1 o successiva da .



La dashboard di vVol visualizza le metriche delle performance solo quando i datastore E le macchine virtuali DI SAN vVol sono configurati utilizzando ONTAP 9.3 o versione successiva.

Fasi

1. Dalla pagina iniziale della console di storage virtuale (VSC), fare clic su **Impostazioni**.
2. Fare clic su **Manage Extension** (Gestisci estensione) nella scheda **Administrative Settings** (Impostazioni amministrative).
3. Utilizzare il dispositivo di scorrimento **Registra servizi API OnCommand** per attivare .
4. Immettere l'indirizzo IP, la porta di servizio e le credenziali per .

È inoltre possibile utilizzare la finestra di dialogo **Manage VASA Provider Extensions** (Gestisci estensioni provider VASA) per le seguenti modifiche:

- Per aggiornare la registrazione in caso di modifiche alle credenziali.
- Per annullare la registrazione quando non è più necessaria la dashboard di vVol.

Deselezionare la casella di controllo **Registra servizi API OnCommand** per rimuovere la registrazione per il provider VASA.

5. Fare clic su **Apply** (Applica).

La dashboard di vVol visualizza le metriche per gli archivi dati DI ONTAP 9.6 o di SAN vVol precedenti solo dopo il completamento della registrazione di.

Informazioni correlate

["Supporto NetApp"](#)

Installare il plug-in NFS VAAI

È possibile installare il plug-in NFS per VMware vStorage API for Array Integration (VAAI) utilizzando la GUI dell'appliance virtuale per Virtual Storage Console (VSC), VASA Provider e Storage Replication Adapter (SRA).

Prima di iniziare

- È necessario aver scaricato il pacchetto di installazione per il plug-in NFS per VAAI (.vib) da .

["Supporto NetApp"](#)

- È necessario aver installato l'host ESXi 6.5 o versione successiva e ONTAP 9.1 o versione successiva.
- È necessario aver acceso l'host ESXi e montato un datastore NFS.
- È necessario impostare i valori di `DataMover.HardwareAcceleratedMove`,

DataMover.HardwareAcceleratedInit, e. VMFS3.HardwareAcceleratedLocking impostazioni host su "1".

Questi valori vengono impostati automaticamente sull'host ESXi quando viene aggiornata la finestra di dialogo **Recommended Settings** (Impostazioni consigliate).

- È necessario aver attivato l'opzione vstorage su utilizzando `vserver nfs modify -vserver vserver_name -vstorage enabled` comando.

Fasi

1. Rinominare il .vib file scaricato da a. NetAppNasPlugin.vib Per corrispondere al nome predefinito utilizzato da VSC.
2. Fare clic su **Settings** (Impostazioni) nella home page di VSC.
3. Fare clic sulla scheda **NFS VAAI Tools** (Strumenti VAAI NFS).
4. Fare clic su **Cambia** nella sezione **versione esistente**.
5. Cercare e selezionare il rinominato .vib Quindi fare clic su **Upload** per caricare il file sull'appliance virtuale.
6. Nella sezione **Installa su host ESXi**, selezionare l'host ESXi su cui si desidera installare il plug-in NFS VAAI, quindi fare clic su **Installa**.

Per completare l'installazione, seguire le istruzioni visualizzate sullo schermo. È possibile monitorare l'avanzamento dell'installazione nella sezione Tasks (attività) di vSphere Web Client.

7. Riavviare l'host ESXi al termine dell'installazione.

Quando si riavvia l'host ESXi, VSC rileva automaticamente il plug-in NFS VAAI. Non è necessario eseguire ulteriori operazioni per attivare il plug-in.

Abilitare Storage Replication Adapter

L'appliance virtuale per Virtual Storage Console (VSC), VASA Provider e Storage Replication Adapter (SRA) offre l'opzione per abilitare la funzionalità SRA da utilizzare con VSC per configurare il disaster recovery.

Prima di iniziare

- È necessario aver configurato l'istanza di vCenter Server e ESXi.
- È necessario aver implementato l'appliance virtuale per VSC, VASA Provider e SRA.
- È necessario aver scaricato .msi File per il plug-in SRA o il .tar.gz File per l'appliance SRM solo se si desidera configurare la soluzione di disaster recovery di Site Recovery Manager (SRM).

["Site Recovery Manager Installazione e configurazione Site Recovery Manager 8.2"](#) contiene ulteriori informazioni.

A proposito di questa attività

La flessibilità necessaria per abilitare le funzionalità di provider VASA e SRA consente di eseguire solo i flussi di lavoro necessari per la tua azienda.

Fasi

1. Accedere all'interfaccia utente Web di VMware vSphere.
2. Dal client vSphere, fare clic su **Menu > Virtual Storage Console**.
3. Fare clic su **Impostazioni**.
4. Fare clic su **Manage Capabilities** (Gestisci funzionalità) nella scheda **Administrative Settings** (Impostazioni amministrative).
5. Nella finestra di dialogo **Manage Capabilities** (Gestisci funzionalità), selezionare l'estensione SRA che si desidera attivare.
6. Inserire l'indirizzo IP dell'appliance virtuale per VSC, VASA Provider e SRA e la password dell'amministratore, quindi fare clic su **Apply** (Applica).
7. Per implementare SRA, è possibile utilizzare uno dei seguenti metodi:

Opzione	Descrizione
Per Windows SRM	<ol style="list-style-type: none"> a. Fare doppio clic sul scaricato .msi Programma di installazione del plug-in SRA. b. Seguire le istruzioni a schermo. c. Inserire l'indirizzo IP e la password dell'appliance virtuale implementata.
Per appliance SRM	<ol style="list-style-type: none"> a. Accedere alla pagina dell'appliance SRM, quindi alla pagina Storage Replication Adapter dell'appliance SRM. b. Fare clic su New Adapter (nuovo adattatore). c. Caricare il programma di installazione di .tar.gz per il plug-in SRM. d. Eseguire nuovamente la scansione degli adattatori per verificare che i dettagli siano aggiornati nella pagina SRM Storage Replication Adapter.

È necessario disconnettersi da vSphere Client, quindi effettuare nuovamente l'accesso per verificare che l'estensione selezionata sia disponibile per la configurazione.

Informazioni correlate

[Configurare Storage Replication Adapter per il disaster recovery](#)

Configurare SRA sull'appliance SRM

Dopo aver implementato l'appliance SRM, è necessario configurare SRA sull'appliance SRM. La corretta configurazione di SRA consente a SRM Appliance di comunicare con SRA per la gestione del disaster recovery. È necessario memorizzare l'appliance virtuale per le credenziali VSC, VASA Provider e SRA (indirizzo IP e password amministratore) nell'appliance SRM per consentire la comunicazione tra l'appliance SRM e SRA.

Prima di iniziare

È necessario caricare `tar.gz` File sull'appliance SRM.

A proposito di questa attività

La configurazione di SRA sull'appliance SRM memorizza le credenziali SRA nell'appliance SRM.

Fasi

1. Effettuare l'accesso utilizzando l'account amministratore all'appliance SRM utilizzando PuTTY.
2. Passare all'utente root utilizzando il comando: `su root`
3. Nella posizione del log, immettere il comando per ottenere l'ID del docker utilizzato da SRA `docker ps -l`
4. Per accedere all'ID contenitore, immettere il comando `docker exec -it -u srm <container id> sh`
5. Configurare SRM con l'appliance virtuale per VSC, VASA Provider e indirizzo IP e password SRA utilizzando il comando: `perl command.pl -I <va-IP> administrator <va-password>`

Viene visualizzato un messaggio di conferma dell'avvenuta memorizzazione delle credenziali di storage. SRA può comunicare con il server SRA utilizzando l'indirizzo IP, la porta e le credenziali forniti.

Aggiornare le credenziali di Storage Replication Adapter (SRA)

Affinché SRM comunichi con SRA, è necessario aggiornare le credenziali SRA sul server SRM se sono state modificate.

Prima di iniziare

Dovresti aver eseguito i passaggi descritti nell'argomento "Configurazione di SRA su appliance SRM".

Configurare SRA sull'appliance SRM

Fasi

1. Eliminare il contenuto di `/srm/sra/confdirectory` che utilizza:
 - a. `cd /srm/sra/conf`
 - b. `rm -rf *`
2. Eseguire il comando `perl` per configurare SRA con le nuove credenziali:
 - a. `cd /srm/sra/`
 - b. `perl command.pl -i <va-IP> Administrator <va-password>`

Migrazione di Windows SRM all'appliance SRM

Se si utilizza Site Recovery Manager (SRM) basato su Windows per il disaster recovery e si desidera utilizzare SRM Appliance per la stessa configurazione, eseguire la migrazione della configurazione di disaster recovery di Windows all'SRM basato sull'appliance.

Le fasi della migrazione del disaster recovery sono:

1. Aggiornamento dell'appliance virtuale esistente per VSC, VASA Provider e SRA alla versione 9.7.1.

["Effettua l'upgrade all'appliance virtuale 9.7.1 per VSC, VASA Provider e SRA"](#)

2. Migrazione di Storage Replication Adapter basato su Windows a un SRA basato su appliance.
3. Migrazione dei dati di Windows SRM all'appliance SRM.

["Fare clic qui"](#) per i passaggi dettagliati.

Effettua l'upgrade all'appliance virtuale 9.7.1 per VSC, VASA Provider e SRA

È possibile eseguire un aggiornamento diretto alla versione 9.7.1 dell'appliance virtuale per VSC, VASA Provider e SRA dalla configurazione 9.7 esistente seguendo le istruzioni fornite qui.

Prima di iniziare

- È necessario aver scaricato `.iso` File per la versione 9.7.1 dell'appliance virtuale per VSC, VASA Provider e SRA.
- È necessario riservare almeno 12 GB di RAM per l'appliance virtuale affinché VSC, VASA Provider e SRA funzionino in modo ottimale dopo l'aggiornamento.
- È necessario pulire la cache del browser del client vSphere.

[Pulire i pacchetti di plug-in scaricati dalla cache di vSphere](#)


A proposito di questa attività

Lo stato del provider VASA dall'implementazione esistente viene mantenuto dopo l'aggiornamento. Dopo l'aggiornamento, attivare o disattivare manualmente il provider VASA in base alle proprie esigenze. Tuttavia, è meglio abilitare il provider VASA anche se i volumi virtuali VMware (vVol) non sono in uso, in quanto abilita i profili di funzionalità dello storage per il provisioning tradizionale del datastore e gli allarmi dello storage.



Un aggiornamento diretto da qualsiasi release precedente alla 9.7 a 9.7P2 o successiva non è supportato dall'appliance virtuale per VSC, VASA Provider e SRA. Prima di eseguire l'aggiornamento a qualsiasi versione successiva, è necessario aggiornare la configurazione esistente alla versione 9.7 dell'appliance virtuale per VSC, VASA Provider e SRA. Quando si esegue l'aggiornamento alla versione 9.7.1 dell'appliance virtuale per VSC, VASA Provider e SRA e si desidera utilizzare la replica vVol, sarà necessario configurare un altro vCenter Server con l'appliance virtuale con Site Recovery Manager (SRM) installato.

Fasi

1. Montare il scaricato `.iso` file sull'appliance virtuale:
 - a. Fare clic su menu:Edit Settings [DVD/CD-ROM Drive] (Modifica impostazioni [unità DVD/CD-ROM]).
 - b. Selezionare **Datastore ISO** file dall'elenco a discesa.
 - c. Individuare e selezionare il file scaricato `.iso` Quindi selezionare la casella di controllo **Connetti all'accensione**.
2. Accedere alla scheda **Riepilogo** dell'appliance virtuale implementata.
3. Fare clic su  per avviare la console di manutenzione.
4. Al prompt "Main Menu", immettere l'opzione 2 Per **Configurazione di sistema**, quindi immettere l'opzione 8 Per **Upgrade**.

Al termine dell'aggiornamento, l'appliance virtuale viene riavviata. L'appliance virtuale per VSC, VASA

Provider e SRA viene registrata su vCenter Server con lo stesso indirizzo IP di prima dell'aggiornamento.

5. Se si desidera che l'appliance virtuale per VSC, VASA Provider e SRA sia registrata con vCenter Server con l'indirizzo IPv6, eseguire le seguenti operazioni:

- a. Annullare la registrazione dell'appliance virtuale per VSC, VASA Provider e SRA.
- b. Registrare l'indirizzo IPv6 dell'appliance virtuale per VSC, VASA Provider e SRA su vCenter Server utilizzando la pagina **Register**.
- c. Rigenerare i certificati VSC e VASA Provider dopo la registrazione.



IPv6 è supportato solo con vCenter Server 6.7 e versioni successive.

6. Disconnettersi e accedere nuovamente a vSphere Client per visualizzare l'appliance virtuale implementata per VSC, VASA Provider e SRA.

- a. Disconnettersi dal client Web vSphere o dal client vSphere esistente e chiudere la finestra.
- b. Accedere al client vSphere.

L'aggiornamento del plug-in nel client vSphere potrebbe richiedere alcuni minuti.

Informazioni correlate

[Abilitare il provider VASA per la configurazione di datastore virtuali](#)

Aggiornare Storage Replication Adapter

Dopo aver aggiornato l'appliance virtuale per VSC, VASA Provider e SRA o aver implementato la versione più recente dell'appliance virtuale, è necessario aggiornare Storage Replication Adapter (SRA).

Fasi

1. È necessario eseguire l'aggiornamento alla scheda più recente utilizzando una delle seguenti procedure in base all'adattatore:

Per...	Eseguire le seguenti operazioni...
Windows	<ol style="list-style-type: none">a. Accedere a SRM Windows Server.b. Disinstallare il programma di installazione esistente di SRA <i>.msi</i> da SRM Server.c. Modificare il percorso di sistema in C:\Program Files\VMware\VMware vCenter Site Recovery Manager\external\perl\c\bind. Fare doppio clic sul programma di installazione <i>.msi</i> scaricato dal sito di supporto NetApp e seguire le istruzioni a schermo.e. Inserire l'indirizzo IP e la password dell'appliance virtuale implementata per VSC, VASA Provider e SRA.

Per...	Eseguire le seguenti operazioni...
Scheda di rete basata su appliance	<p>a. Accedere alla pagina SRM Appliance Managementpage.</p> <p>b. Fare clic su Storage Replication Adapter, quindi su Delete (Elimina) per rimuovere l'SRA esistente.</p> <p>c. Fare clic sul New Adapter > Browse (nuovo adattatore[Sfoglia])</p> <p>d. Fare clic per selezionare il file di tarball SRA più recente scaricato dal sito di supporto NetApp, quindi fare clic su Installa.</p> <p>e. Configurare SRA sull'appliance SRM.</p> <p>Configurare SRA sull'appliance SRM</p>

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.

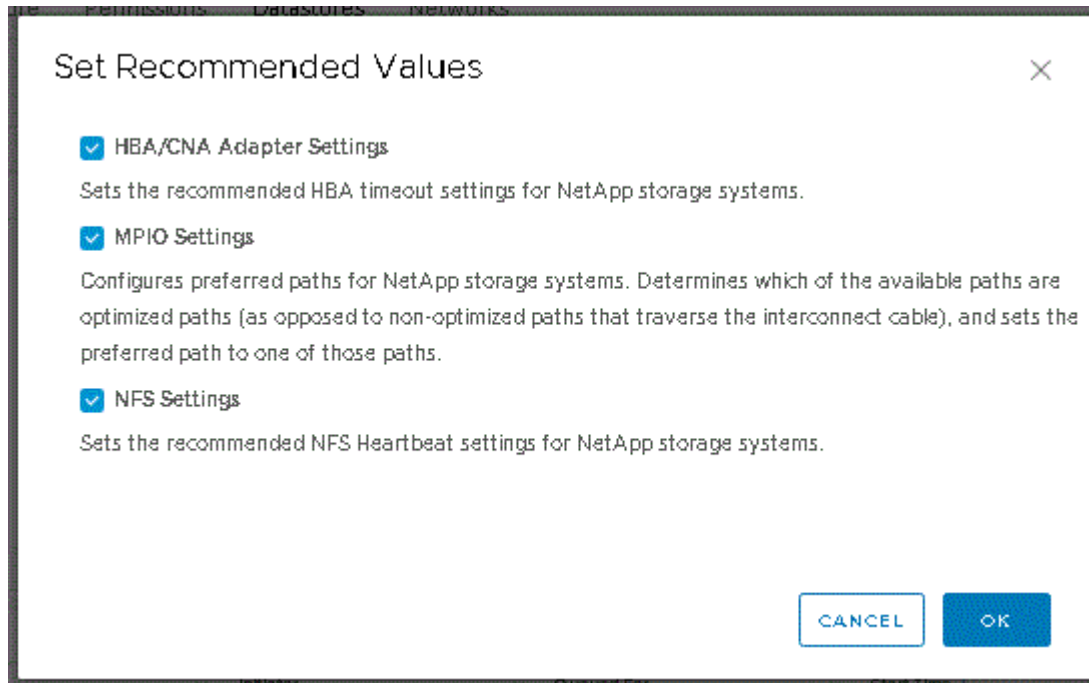
Fasi

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.

Configurare la Virtual Storage Console per l'ambiente del sistema di storage VMware vSphere

Virtual Storage Console per VMware vSphere offre un unico meccanismo per rilevare i sistemi storage e impostare le credenziali dello storage. Le credenziali forniscono le autorizzazioni ONTAP necessarie per consentire agli utenti della console di storage virtuale (VSC) di eseguire le attività utilizzando i sistemi di storage.

Prima che VSC possa visualizzare e gestire le risorse di storage, VSC deve rilevare i sistemi di storage. Nell'ambito del processo di rilevamento, è necessario fornire le credenziali ONTAP per i sistemi storage. Si tratta dei privilegi (o ruoli) associati alla coppia di nome utente e password assegnata a ciascun sistema di storage. Queste coppie di nome utente e password utilizzano il RBAC (Role-Based Access Control) di ONTAP e devono essere configurate da ONTAP. Non è possibile modificare queste credenziali da VSC. È possibile definire i ruoli RBAC di ONTAP utilizzando .



Se si effettua l'accesso come amministratore, si dispone automaticamente di tutti i privilegi per il sistema di storage in questione.

Quando si aggiunge un sistema di storage a VSC, è necessario fornire un indirizzo IP per il sistema di storage e la coppia di nome utente e password associata al sistema. È possibile impostare le credenziali predefinite che VSC utilizzerà durante il processo di rilevamento del sistema di storage oppure immettere manualmente le credenziali una volta rilevato il sistema di storage. I dettagli del sistema di storage aggiunto a VSC vengono inviati automaticamente alle estensioni attivate nella distribuzione. Non è necessario aggiungere manualmente lo storage al provider VASA e a Storage Replication Adapter (SRA). Sia VSC che SRA supportano l'aggiunta di credenziali a livello di cluster. IL provider VASA supporta solo le credenziali a livello di cluster per l'aggiunta di sistemi storage.

Se l'ambiente include più istanze di vCenter Server, quando si aggiunge un sistema di storage a VSC dalla pagina Storage Systems, la finestra di dialogo Add Storage System (Aggiungi sistema di storage) visualizza

una finestra di vCenter Server in cui è possibile specificare a quale istanza di vCenter Server aggiungere il sistema di storage. Se si aggiunge un sistema storage facendo clic con il pulsante destro del mouse sul nome di un data center, non è possibile specificare un'istanza di vCenter Server perché il server è già associato a tale data center.

Il rilevamento avviene in uno dei seguenti modi. In ogni caso, è necessario fornire le credenziali per qualsiasi sistema storage appena rilevato.

- All'avvio del servizio VSC, VSC avvia il processo automatico di rilevamento in background.
- È possibile fare clic sul pulsante **RISCOPRI tutto** nella pagina Storage Systems (sistemi storage) o su un host o un data center per selezionarlo dal menu **Actions (Actions > NetApp VSC > Update host and Storage Data** (azioni[NetApp VSC > Aggiorna dati host e storage). È inoltre possibile fare clic su **DISCOVER** nella scheda Getting Started (Guida introduttiva) della sezione Overview (Panoramica).

Tutte le funzioni VSC richiedono autorizzazioni specifiche per eseguire le attività. È possibile limitare le operazioni che gli utenti possono eseguire in base alle credenziali associate al ruolo di ONTAP. Tutti gli utenti che hanno la stessa coppia di nome utente e password del sistema di storage condividono lo stesso set di credenziali del sistema di storage e possono eseguire le stesse operazioni.

Impostare le credenziali predefinite per i sistemi storage

È possibile utilizzare Virtual Storage Console per VMware vSphere per impostare le credenziali predefinite per un sistema storage nel vCenter Server.

Prima di iniziare

È necessario selezionare il vCenter Server che si desidera utilizzare per creare le credenziali predefinite.

A proposito di questa attività

Se si impostano le credenziali predefinite per i sistemi storage, (VSC) utilizza queste credenziali per accedere a un sistema storage che VSC ha appena scoperto. Se le credenziali predefinite non funzionano, è necessario accedere manualmente al sistema di storage. VSC e SRA supportano l'aggiunta di credenziali di sistema storage a livello di cluster o di livello. Tuttavia, il provider VASA funziona solo con le credenziali a livello di cluster.

Fasi

1. Nella pagina VSC **Home**, fare clic su **Impostazioni > Impostazioni amministrative > Configura credenziali predefinite per il sistema di storage**.
2. Nella finestra di dialogo **Storage System Default Credentials** (credenziali predefinite del sistema di storage), immettere il nome utente e la password del sistema di storage.

Le credenziali dello storage controller vengono assegnate in ONTAP in base alla coppia di nome utente e password. Le credenziali dello storage controller possono essere l'account amministratore o un account personalizzato che utilizza RBAC (role-based access control).

Non è possibile utilizzare VSC per modificare i ruoli associati alla coppia di nome utente e password del controller di storage. Per modificare o creare un nuovo ruolo utente ONTAP da utilizzare con l'appliance virtuale per VSC, provider VASA e SRA, è possibile utilizzare Gestione sistema.

Consultare la sezione "Configurazione dei ruoli e dei privilegi utente" nella *Guida all'installazione e all'installazione di Virtual Storage Console, VASA Provider e Storage Replication Adapter per VMware® vSphere per la versione 9.7*.

3. Fare clic su **OK** per salvare le credenziali predefinite.

Al termine

Se le credenziali del sistema di storage sono state aggiornate perché un sistema di storage ha riportato lo stato “Authentication Failure” (errore di autenticazione), fare clic sull'opzione **REDISCOVER ALL** (RISCOPRI TUTTO) disponibile nella pagina Storage Systems (sistemi di storage). In questo modo, VSC tenta di connettersi al sistema di storage utilizzando le nuove credenziali.

Aggiungere sistemi storage a VSC

È possibile aggiungere manualmente il sistema di storage a Virtual Storage Console (VSC).

A proposito di questa attività

Ogni volta che si avvia (VSC) o si seleziona l'opzione **RISCOPRI tutto**, VSC rileva automaticamente i sistemi di storage disponibili.

Fasi

1. Aggiungere un sistema storage a VSC utilizzando la home page di VSC:
 - Fare clic sul **Storage Systems > Add** (sistemi storage[Aggiungi]).
 - Fare clic su **Panoramica > Guida introduttiva**, quindi fare clic sul pulsante **AGGIUNGI** in **Aggiungi sistema di storage**.
2. Nella finestra di dialogo **Add Storage System** (Aggiungi sistema di storage), immettere l'indirizzo IP di gestione e le credenziali del sistema di storage.

È inoltre possibile aggiungere sistemi storage utilizzando l'indirizzo IPv6 del cluster o . In questa finestra di dialogo è inoltre possibile modificare i valori predefiniti per TLS e il numero di porta.

Quando si aggiunge storage dalla pagina VSC **Storage System**, è necessario specificare anche l'istanza di vCenter Server in cui si trova lo storage. La finestra di dialogo **Add Storage System** (Aggiungi sistema di storage) fornisce un elenco a discesa delle istanze di vCenter Server disponibili. VSC non visualizza questa opzione se si aggiunge storage a un data center già associato a un'istanza di vCenter Server.

3. Fare clic su **OK** dopo aver aggiunto tutte le informazioni richieste.

Rilevamento di host e sistemi storage

Quando si esegue per la prima volta (VSC) in un client vSphere, VSC rileva gli host ESXi, le loro LUN ed esportazioni NFS e i sistemi storage NetApp che possiedono tali LUN ed esportazioni.

Prima di iniziare

- Tutti gli host ESXi devono essere accesi e connessi.
- Tutti i da rilevare devono essere in esecuzione e ciascun nodo del cluster deve avere almeno una LIF di dati configurata per il protocollo di storage in uso (NFS, iSCSI o FC).

A proposito di questa attività

È possibile scoprire nuovi sistemi storage o aggiornare le informazioni sui sistemi storage esistenti per ottenere le informazioni più aggiornate sulla capacità e sulla configurazione in qualsiasi momento. È inoltre possibile modificare le credenziali utilizzate da VSC per accedere ai sistemi di storage.

Durante il rilevamento dei sistemi storage, VSC raccoglie informazioni dagli host ESXi gestiti dall'istanza di vCenter Server.

Fasi

1. Dalla pagina iniziale del client vSphere, selezionare **host e cluster**.
2. Fare clic con il pulsante destro del mouse sul data center desiderato, quindi selezionare **NetApp VSC › Update host and Storage Data** (Aggiorna dati host e storage).

VSC visualizza una finestra di dialogo di conferma che informa che questa operazione potrebbe richiedere molto tempo.

3. Fare clic su **OK**.
4. Selezionare i controller di storage rilevati con stato "Authentication Failure" (errore di autenticazione), quindi fare clic su **AZIONI › Modify** (Modifica).
5. Inserire le informazioni richieste nella finestra di dialogo **Modify Storage System** (Modifica sistema di storage).
6. Ripetere i passaggi 4 e 5 per tutti i controller storage con stato "Authentication Failure".

Al termine

Al termine del processo di rilevamento, eseguire le seguenti operazioni:

- Utilizzare VSC per configurare le impostazioni dell'host ESXi per gli host che visualizzano l'icona Alert (Avviso) nella colonna **Adapter Settings** (Impostazioni adattatore), nella colonna **MPIO Settings** (Impostazioni MPIO) o nella colonna **NFS Settings** (Impostazioni NFS).
- Fornire le credenziali del sistema storage.

Aggiornare il display del sistema di storage

È possibile utilizzare la funzione di aggiornamento fornita da Virtual Storage Console per VMware vSphere per aggiornare le informazioni sui sistemi storage e forzare Virtual Storage Console (VSC) a rilevare i sistemi storage.

A proposito di questa attività

L'opzione "refresh" è utile se sono state modificate le credenziali predefinite per i sistemi di storage dopo aver ricevuto un errore di autenticazione. È necessario eseguire sempre un'operazione di aggiornamento se sono state modificate le credenziali del sistema di storage dopo che il sistema ha segnalato un "Authentication Failure Status" (Stato errore di autenticazione). Durante l'operazione di aggiornamento, VSC tenta di connettersi al sistema di storage utilizzando le nuove credenziali.

A seconda della configurazione del sistema, il completamento di questa attività può richiedere molto tempo.

Fasi

1. Nella pagina VMware vSphere Client **Home**, fare clic su **Storage Systems**.
2. Avviare l'aggiornamento:

Se questa posizione è...	Fare clic su...
Virtual Storage Console	Icona RISCOPRI TUTTO .

Se questa posizione è...	Fare clic su...
Data center	Fare clic con il pulsante destro del mouse sul data center, quindi scegliere NetApp VSC › Update host and Storage Data (Aggiorna dati host e storage NetApp).

3. Nella finestra di dialogo **Update host and Storage Data** (Aggiorna dati host e storage), fare clic su **OK**.

Il rilevamento potrebbe richiedere alcuni minuti a seconda del numero di host e sistemi storage nel data center. Questa operazione di rilevamento funziona in background.

4. Fare clic su **OK** nella finestra di dialogo **Success**.

Funzionalità di controllo degli accessi basate sui ruoli di vCenter Server in VSC per VMware vSphere

VCenter Server offre RBAC (role-based access control) che consente di controllare l'accesso agli oggetti vSphere. Nella console di storage virtuale per VMware vSphere, vCenter Server RBAC lavora con ONTAP RBAC per determinare le attività VSC che un utente specifico può eseguire sugli oggetti di un sistema storage specifico.

Per completare correttamente un'attività, è necessario disporre delle autorizzazioni RBAC vCenter Server appropriate. Durante un'attività, VSC controlla le autorizzazioni vCenter Server di un utente prima di controllare i privilegi ONTAP dell'utente.

È possibile impostare le autorizzazioni vCenter Server sull'oggetto root (nota anche come cartella root). È quindi possibile perfezionare la protezione limitando le entità figlio che non necessitano di tali autorizzazioni.

Componenti delle autorizzazioni vCenter Server

VCenter Server riconosce le autorizzazioni e non i privilegi. Ogni autorizzazione vCenter Server è composta da tre componenti.

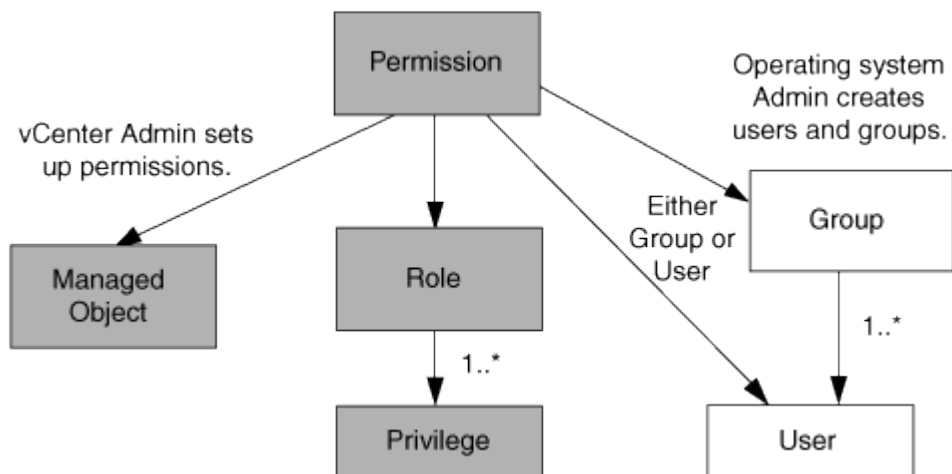
VCenter Server include i seguenti componenti:

- Uno o più privilegi (il ruolo)
I privilegi definiscono le attività che un utente può eseguire.
- Un oggetto vSphere
L'oggetto è la destinazione delle attività.
- Un utente o un gruppo
L'utente o il gruppo definisce chi può eseguire l'attività.

Come illustrato nel diagramma seguente, per poter disporre di un'autorizzazione è necessario disporre di tutti e tre gli elementi.



In questo diagramma, le caselle grigie indicano i componenti presenti in vCenter Server e le caselle bianche indicano i componenti presenti nel sistema operativo in cui è in esecuzione vCenter Server.



Privilegi

Sono associati due tipi di privilegi a Virtual Storage Console per VMware vSphere:

- Privilegi vCenter Server nativi

Questi privilegi vengono forniti con vCenter Server.

- Privilegi specifici di VSC

Questi privilegi sono definiti per attività VSC specifiche. Sono esclusivi di VSC.

Le attività VSC richiedono privilegi specifici di VSC e privilegi nativi di vCenter Server. Questi privilegi costituiscono “role” per l’utente. Un’autorizzazione può avere più privilegi. Questi privilegi sono riservati a un utente che ha effettuato l’accesso a vCenter Server.



Per semplificare l’utilizzo di vCenter Server RBAC, VSC offre diversi ruoli standard che contengono tutti i privilegi nativi e specifici di VSC necessari per eseguire le attività VSC.

Se si modificano i privilegi all’interno di un’autorizzazione, l’utente associato a tale autorizzazione deve disconnettersi e quindi accedere per attivare l’autorizzazione aggiornata.

Privilegio	Ruoli	Attività
Menu:NetApp Virtual Storage Console[Visualizza]	<ul style="list-style-type: none">• Amministratore di VSC• Provisioning VSC• VSC di sola lettura	Tutte le attività specifiche del provider VSC e VASA richiedono il privilegio di visualizzazione.

Privilegio	Ruoli	Attività
Menu:NetApp Virtual Storage Console[Gestione basata su policy > Gestione] o privilege.nvpfVSC.VASAGroup.com.netapp.nvpf.label > Management	Amministratore di VSC	Attività del provider VSC e VASA correlate ai profili di capacità dello storage e alle impostazioni delle soglie.

Oggetti vSphere

Le autorizzazioni sono associate agli oggetti vSphere, come vCenter Server, host ESXi, macchine virtuali, datastore, data center, e cartelle. È possibile assegnare autorizzazioni a qualsiasi oggetto vSphere. In base all'autorizzazione assegnata a un oggetto vSphere, vCenter Server determina chi può eseguire le attività su tale oggetto. Per attività specifiche di VSC, le autorizzazioni vengono assegnate e validate solo a livello di cartella principale (vCenter Server) e non su altre entità. Ad eccezione del funzionamento del plugin VAAI, in cui i permessi sono validati rispetto all'ESXi interessato.

Utenti e gruppi

È possibile utilizzare Active Directory (o la macchina vCenter Server locale) per configurare utenti e gruppi di utenti. È quindi possibile utilizzare le autorizzazioni vCenter Server per concedere l'accesso a questi utenti o gruppi per consentire loro di eseguire attività VSC specifiche.



Queste autorizzazioni vCenter Server si applicano agli utenti VSC vCenter e non agli amministratori VSC. Per impostazione predefinita, gli amministratori VSC hanno accesso completo al prodotto e non richiedono autorizzazioni assegnate.

Gli utenti e i gruppi non hanno ruoli assegnati. Ottengono l'accesso a un ruolo facendo parte di un'autorizzazione vCenter Server.

Punti chiave relativi all'assegnazione e alla modifica delle autorizzazioni per vCenter Server

Esistono diversi punti chiave da tenere a mente quando si utilizzano le autorizzazioni di vCenter Server. Il successo di un'attività di Virtual Storage Console per VMware vSphere dipende dalla posizione in cui è stata assegnata un'autorizzazione o dalle azioni intraprese da un utente dopo la modifica di un'autorizzazione.

Assegnazione delle autorizzazioni

È necessario impostare le autorizzazioni di vCenter Server solo se si desidera limitare l'accesso agli oggetti e alle attività di vSphere. In caso contrario, è possibile accedere come amministratore. Questo login consente di accedere automaticamente a tutti gli oggetti vSphere.

La posizione in cui si assegna un'autorizzazione determina le attività VSC che un utente può eseguire.

A volte, per garantire il completamento di un'attività, è necessario assegnare l'autorizzazione a un livello superiore, ad esempio l'oggetto root. Questo accade quando un'attività richiede un privilegio che non si applica a un oggetto vSphere specifico (ad esempio, il monitoraggio dell'attività) o quando un privilegio richiesto si applica a un oggetto non vSphere (ad esempio, un sistema storage).

In questi casi, è possibile impostare un'autorizzazione in modo che venga ereditata dalle entità figlio. È inoltre possibile assegnare altre autorizzazioni alle entità figlio. L'autorizzazione assegnata a un'entità figlio sovrascrive sempre l'autorizzazione ereditata dall'entità padre. Ciò significa che è possibile concedere autorizzazioni a un'entità figlio per limitare l'ambito di un'autorizzazione assegnata a un oggetto root ed ereditata dall'entità figlio.



A meno che le policy di sicurezza aziendali non richiedano autorizzazioni più restrittive, è consigliabile assegnare autorizzazioni all'oggetto root (anche noto come cartella root).

Permessi e oggetti non vSphere

L'autorizzazione creata viene applicata a un oggetto non vSphere. Ad esempio, un sistema storage non è un oggetto vSphere. Se un privilegio viene applicato a un sistema di storage, è necessario assegnare l'autorizzazione contenente tale privilegio all'oggetto root VSC perché non esiste alcun oggetto vSphere a cui è possibile assegnarlo.

Ad esempio, qualsiasi autorizzazione che includa un privilegio come il privilegio VSC "Add/Modify/Skip storage Systems" deve essere assegnata a livello di oggetto root.

Modifica delle autorizzazioni

È possibile modificare un'autorizzazione alla volta.

Se si modificano i privilegi all'interno di un'autorizzazione, l'utente associato a tale autorizzazione deve disconnettersi e quindi accedere nuovamente per attivare l'autorizzazione aggiornata.

Ruoli standard in bundle con l'appliance virtuale per VSC, VASA Provider e SRA

Per semplificare l'utilizzo dei privilegi di vCenter Server e del RBAC (role-based access control), (VSC) fornisce ruoli VSC standard che consentono di eseguire le principali attività VSC. Esiste anche un ruolo di sola lettura che consente di visualizzare le informazioni VSC, ma non di eseguire alcuna attività.

I ruoli VSC standard dispongono sia dei privilegi specifici di VSC che dei privilegi nativi di vCenter Server necessari per eseguire le attività VSC. Inoltre, i ruoli sono configurati in modo da disporre dei privilegi richiesti per tutte le versioni supportate di vCenter Server.

In qualità di amministratore, è possibile assegnare questi ruoli agli utenti, in base alle esigenze.



Quando si aggiorna VSC alla versione più recente, i ruoli standard vengono automaticamente aggiornati per funzionare con la nuova versione di VSC.

È possibile visualizzare i ruoli standard VSC facendo clic su **ruoli** nella pagina iniziale del client vSphere.

I ruoli forniti da VSC consentono di eseguire le seguenti attività:

Ruolo	Descrizione
Amministratore di VSC	Fornisce tutti i privilegi nativi di vCenter Server e i privilegi specifici di VSC necessari per eseguire tutte le attività di VSC.

Ruolo	Descrizione
VSC di sola lettura	<p>Fornisce l'accesso in sola lettura a VSC.</p> <p>Questi utenti non possono eseguire alcuna azione VSC controllata dall'accesso.</p>
Provisioning VSC	<p>Fornisce tutti i privilegi nativi di vCenter Server e i privilegi specifici di VSC necessari per il provisioning dello storage.</p> <p>È possibile eseguire le seguenti operazioni:</p> <ul style="list-style-type: none"> • Creare nuovi datastore • Distruggere i datastore • Visualizza informazioni sui profili delle funzionalità di storage

Linee guida per l'utilizzo dei ruoli standard VSC

Quando si lavora con i ruoli standard di Virtual Storage Console per VMware vSphere, è necessario seguire alcune linee guida.

Non modificare direttamente i ruoli standard. In tal caso, VSC sovrascriverà le modifiche ogni volta che si aggiorna VSC. Il programma di installazione aggiorna le definizioni dei ruoli standard ogni volta che si aggiorna VSC. In questo modo si garantisce che i ruoli siano aggiornati per la versione di VSC e per tutte le versioni supportate di vCenter Server.

Tuttavia, è possibile utilizzare i ruoli standard per creare ruoli personalizzati in base all'ambiente. A tale scopo, è necessario copiare il ruolo standard VSC e quindi modificare il ruolo copiato. Creando un nuovo ruolo, è possibile mantenere questo ruolo anche quando si riavvia o si aggiorna il servizio VSC Windows.

Di seguito sono riportati alcuni dei modi in cui è possibile utilizzare i ruoli standard di VSC:

- Utilizzare i ruoli VSC standard per tutte le attività VSC.

In questo scenario, i ruoli standard forniscono tutti i privilegi di cui un utente ha bisogno per eseguire le attività VSC.

- Combina i ruoli per espandere le attività che un utente può eseguire.

Se i ruoli VSC standard forniscono una granularità eccessiva per l'ambiente, è possibile espandere i ruoli creando gruppi di livello superiore che contengono più ruoli.

Se un utente deve eseguire altre attività non VSC che richiedono ulteriori privilegi nativi di vCenter Server, è possibile creare un ruolo che fornisca tali privilegi e aggiungerlo anche al gruppo.

- Crea ruoli più specifici.

Se l'azienda richiede l'implementazione di ruoli più restrittivi rispetto ai ruoli VSC standard, è possibile utilizzare i ruoli VSC per creare nuovi ruoli.

In questo caso, clonare i ruoli VSC necessari e modificare il ruolo clonato in modo che disponga solo dei

privilegi richiesti dall'utente.

Privilegi richiesti per le attività VSC

Le diverse attività di Virtual Storage Console per VMware vSphere richiedono diverse combinazioni di privilegi specifici per (VSC) e i privilegi nativi di vCenter Server.

Informazioni sui privilegi richiesti per le attività VSC sono disponibili nell'articolo della Knowledge base di NetApp 1032542.

["Come configurare RBAC per Virtual Storage Console"](#)

Privilegio a livello di prodotto richiesto da VSC per VMware vSphere

Per accedere alla GUI di Virtual Storage Console per VMware vSphere, è necessario disporre del privilegio View specifico per VSC a livello di prodotto assegnato al livello di oggetto vSphere corretto. Se si effettua l'accesso senza questo privilegio, VSC visualizza un messaggio di errore quando si fa clic sull'icona NetApp e impedisce l'accesso a VSC.

Le seguenti informazioni descrivono il privilegio View a livello di prodotto VSC:

Privilegio	Descrizione	Livello di assegnazione
Visualizza	È possibile accedere alla GUI di VSC. Questo privilegio non consente di eseguire attività all'interno di VSC. Per eseguire qualsiasi attività VSC, è necessario disporre dei privilegi vCenter Server nativi e specifici di VSC corretti per tali attività.	<p>Il livello di assegnazione determina le parti dell'interfaccia utente che è possibile visualizzare.</p> <p>L'assegnazione del privilegio View all'oggetto root (cartella) consente di accedere a VSC facendo clic sull'icona NetApp.</p> <p>È possibile assegnare il privilegio View a un altro livello di oggetto vSphere; tuttavia, ciò limita i menu VSC che è possibile visualizzare e utilizzare.</p> <p>L'oggetto root è la posizione consigliata per assegnare qualsiasi autorizzazione contenente il privilegio View.</p>

Controllo degli accessi basato sul ruolo di ONTAP per l'appliance virtuale per VSC, provider VASA e SRA

Il RBAC (Role-Based Access Control) di ONTAP consente di controllare l'accesso a specifici sistemi storage e le azioni che un utente può eseguire su tali sistemi storage. Nella console di storage virtuale per VMware vSphere, ONTAP RBAC lavora con vCenter Server RBAC per determinare quali attività possono essere eseguite da un utente specifico sugli oggetti di un sistema storage specifico.

VSC utilizza le credenziali (nome utente e password) impostate in VSC per autenticare ciascun sistema storage e determinare quali operazioni storage possono essere eseguite su tale sistema. VSC utilizza un set di credenziali per ciascun sistema storage. Queste credenziali determinano quali attività VSC possono essere eseguite su quel sistema di storage; in altre parole, le credenziali sono per VSC, non per un singolo utente VSC.

ONTAP RBAC si applica solo all'accesso ai sistemi storage e all'esecuzione di task VSC correlati allo storage, come il provisioning di macchine virtuali. Se non si dispone dei privilegi RBAC ONTAP appropriati per uno specifico sistema di storage, non è possibile eseguire attività su un oggetto vSphere ospitato su tale sistema di storage. È possibile utilizzare ONTAP RBAC insieme ai privilegi specifici di VSC per controllare quali attività di VSC possono essere eseguite da un utente:

- Monitoraggio e configurazione degli oggetti storage o vCenter Server che risiedono su un sistema storage
- Provisioning di oggetti vSphere residenti su un sistema storage

L'utilizzo di ONTAP RBAC con i privilegi specifici di VSC offre un livello di sicurezza orientato allo storage che l'amministratore dello storage può gestire. Di conseguenza, si dispone di un controllo degli accessi più dettagliato rispetto a quello supportato da solo da ONTAP RBAC o da solo da vCenter Server RBAC. Ad esempio, con vCenter Server RBAC, è possibile consentire a vCenterUserB di eseguire il provisioning di un datastore sullo storage, impedendo al contempo a vCenterUserA di eseguire il provisioning dei datastore. Se le credenziali del sistema di storage per un sistema di storage specifico non supportano la creazione di storage, né vCenterUserB né vCenterUserA possono eseguire il provisioning di un datastore su tale sistema di storage.

Quando si avvia un'attività VSC, VSC verifica innanzitutto se si dispone dell'autorizzazione vCenter Server corretta per tale attività. Se l'autorizzazione vCenter Server non è sufficiente per consentire l'esecuzione dell'attività, VSC non deve controllare i privilegi ONTAP per il sistema di storage in quanto non è stato superato il controllo di protezione iniziale di vCenter Server. Di conseguenza, non è possibile accedere al sistema di storage.

Se l'autorizzazione del server vCenter è sufficiente, VSC verifica i privilegi RBAC di ONTAP (il proprio ruolo ONTAP) associati alle credenziali del sistema di storage (nome utente e password). Per determinare se si dispone di privilegi sufficienti per eseguire le operazioni di storage richieste dall'attività VSC sul sistema di storage in questione. Se si dispone dei privilegi ONTAP corretti, è possibile accedere al sistema di storage ed eseguire l'attività VSC. I ruoli ONTAP determinano le attività VSC che è possibile eseguire sul sistema di storage.

A ciascun sistema storage è associato un set di privilegi ONTAP.

L'utilizzo di ONTAP RBAC e vCenter Server RBAC offre i seguenti vantaggi:

- Sicurezza

L'amministratore può controllare quali utenti possono eseguire le attività a livello di oggetto vCenter Server e a livello di sistema di storage.

- Informazioni di audit

In molti casi, VSC fornisce un audit trail sul sistema storage che consente di tenere traccia degli eventi all'utente di vCenter Server che ha eseguito le modifiche dello storage.

- Usabilità

È possibile conservare tutte le credenziali del controller in un'unica posizione.

Ruoli ONTAP consigliati quando si utilizza VSC per VMware vSphere

È possibile impostare diversi ruoli ONTAP consigliati per lavorare con la console di storage virtuale per VMware vSphere e il RBAC (role-based access control). Questi ruoli contengono i privilegi di ONTAP necessari per eseguire le operazioni di storage richieste eseguite dalle attività (VSC).

Per creare nuovi ruoli utente, è necessario accedere come amministratore nei sistemi storage che eseguono ONTAP. È possibile creare ruoli ONTAP utilizzando una delle seguenti opzioni:

- 9.7 o versione successiva

["Configurare i ruoli e i privilegi degli utenti"](#)

- Tool RBAC User Creator per ONTAP (se si utilizza ONTAP 9.6 o versione precedente)

["Tool RBAC User Creator per VSC, VASA Provider e Storage Replication Adapter 7.0 per VMware vSphere"](#)

A ciascun ruolo di ONTAP è associata una coppia di nome utente e password, che costituiscono le credenziali del ruolo. Se non si effettua l'accesso utilizzando queste credenziali, non è possibile accedere alle operazioni di storage associate al ruolo.

Come misura di sicurezza, i ruoli ONTAP specifici del VSC sono ordinati gerarchicamente. Ciò significa che il primo ruolo è il ruolo più restrittivo e dispone solo dei privilegi associati al set più semplice di operazioni di storage VSC. Il ruolo successivo include sia i propri privilegi che tutti i privilegi associati al ruolo precedente. Ogni ruolo aggiuntivo è meno restrittivo per quanto riguarda le operazioni di storage supportate.

Di seguito sono riportati alcuni dei ruoli RBAC ONTAP consigliati quando si utilizza VSC. Dopo aver creato questi ruoli, è possibile assegnare i ruoli agli utenti che devono eseguire attività correlate allo storage, ad esempio il provisioning delle macchine virtuali.

1. Discovery (rilevamento)

Questo ruolo consente di aggiungere sistemi storage.

2. Creare storage

Questo ruolo consente di creare storage. Questo ruolo include anche tutti i privilegi associati al ruolo Discovery.

3. Modificare lo storage

Questo ruolo consente di modificare lo storage. Questo ruolo include anche tutti i privilegi associati al ruolo Discovery e al ruolo Create Storage.

4. Distruggere lo storage

Questo ruolo consente di distruggere lo storage. Questo ruolo include anche tutti i privilegi associati al ruolo Discovery, al ruolo Create Storage e al ruolo Modify Storage.

Se si utilizza il provider VASA per ONTAP, è necessario impostare anche un ruolo di gestione basato su policy (PBM). Questo ruolo consente di gestire lo storage utilizzando le policy di storage. Questo ruolo richiede anche la configurazione del ruolo "DDiscovery".

Come configurare il controllo degli accessi basato sui ruoli di ONTAP per VSC per VMware vSphere

Se si desidera utilizzare il controllo degli accessi basato sui ruoli con la console di storage virtuale per ONTAP vSphere (VSC), è necessario configurare RBAC (Role-Based Access Control) sul sistema storage. È possibile creare uno o più account utente personalizzati con privilegi di accesso limitati con la funzione RBAC di ONTAP.

VSC e SRA possono accedere ai sistemi storage a livello di cluster o di livello. Se si aggiungono sistemi storage a livello di cluster, è necessario fornire le credenziali dell'utente amministratore per fornire tutte le funzionalità richieste. Se si aggiungono i sistemi storage aggiungendo direttamente i dettagli, è necessario tenere presente che l'utente "vsadmin" non dispone di tutti i ruoli e le funzionalità necessari per eseguire determinate attività.

IL provider VASA può accedere ai sistemi storage solo a livello di cluster. Se il provider VASA è richiesto per un controller storage specifico, il sistema storage deve essere aggiunto a VSC a livello di cluster anche se si utilizza VSC o SRA.

Per creare un nuovo utente e connettere un cluster o un a VSC, VASA Provider e SRA, attenersi alla seguente procedura:

- Creare un ruolo di amministratore o amministratore del cluster

Per creare questi ruoli, è possibile utilizzare una delle seguenti opzioni:

- Gestore di sistema di ONTAP 9.7 o versione successiva



"Configurare i ruoli e i privilegi degli utenti"

- Tool RBAC User Creator per ONTAP (se si utilizza ONTAP 9.6 o versione precedente)

"Tool RBAC User Creator per VSC, VASA Provider e Storage Replication Adapter 7.0 per VMware vSphere"

- Creare utenti con il ruolo assegnato e il set di applicazioni appropriato utilizzando ONTAP

Queste credenziali del sistema storage sono necessarie per configurare i sistemi storage per VSC. È possibile configurare i sistemi storage per VSC immettendo le credenziali in VSC. Ogni volta che si accede a un sistema storage con queste credenziali, si disporranno delle autorizzazioni per le funzioni VSC configurate in ONTAP durante la creazione delle credenziali.

- Aggiungere il sistema storage a VSC e fornire le credenziali dell'utente appena creato

Ruoli VSC

VSC classifica i privilegi ONTAP nel seguente set di ruoli VSC:

- Discovery (rilevamento)

Attiva il rilevamento di tutti i controller di storage collegati

- Creare storage

Consente la creazione di volumi e LUN (Logical Unit Number)

- Modificare lo storage

Consente il ridimensionamento e la deduplica dei sistemi storage

- Distruggere lo storage

Consente la distruzione di volumi e LUN

Ruoli del provider VASA

È possibile creare solo la gestione basata su policy a livello di cluster. Questo ruolo consente la gestione dello storage basata su policy utilizzando i profili delle funzionalità di storage.

Ruoli SRA

SRA classifica i privilegi ONTAP in un ruolo SAN o NAS a livello di cluster o di livello. Ciò consente agli utenti di eseguire operazioni SRM.



Per configurare manualmente i ruoli e i privilegi utilizzando i comandi di ONTAP, consultare gli articoli della Knowledge base.

- ["Configurazione RBAC di VSC, VASA e SRA 7.0 ONTAP"](#)
- ["Eseguire il rollup di tutti i comandi per VSC e SRA per il livello di SVM"](#)

Quando si aggiunge il cluster a VSC, VSC esegue una convalida iniziale dei privilegi dei ruoli RBAC di ONTAP. Se è stato aggiunto un IP di storage diretto, VSC non esegue la convalida iniziale. VSC controlla e applica i privilegi in un secondo momento nel flusso di lavoro delle attività.

Configurare i ruoli e i privilegi degli utenti

È possibile configurare nuovi ruoli utente per la gestione dei sistemi storage utilizzando il file JSON fornito con l'appliance virtuale per VSC, provider VASA, SRA e Gestore di sistema ONTAP.

Prima di iniziare

- Il file dei privilegi ONTAP dovrebbe essere stato scaricato dall'appliance virtuale per VSC, provider VASA e SRA utilizzando
`https://{virtual_appliance_IP}:9083/vsc/config/VSC_ONTAP_User_Privileges.zip`.
- È necessario aver configurato Gestore di sistema di ONTAP 9.7.
- Si dovrebbe aver effettuato l'accesso con privilegi di amministratore per il sistema di storage.

fasi

1. Decomprimere il scaricato
`https://{virtual_appliance_IP}:9083/vsc/config/VSC_ONTAP_User_Privileges.zip`
file.
2. Accedere a Gestore di sistema di ONTAP.
3. Fare clic su **CLUSTER > Impostazioni > utenti e ruoli**.
4. Fare clic su **Add User** (Aggiungi utente).
5. Nella finestra di dialogo **Aggiungi utente**, selezionare **prodotti di virtualizzazione**.

6. Fare clic su **Browse** (Sfoglia) per selezionare e caricare il file ONTAP Privileges JSON.

Il campo DEL PRODOTTO viene compilato automaticamente.

7. Selezionare la funzionalità desiderata dal menu a discesa **PRODUCT CAPABILITY** (FUNZIONALITÀ DEL PRODOTTO).

Il campo **ROLE** viene compilato automaticamente in base alla funzionalità del prodotto selezionata.

8. Immettere il nome utente e la password richiesti.

9. Selezionare i privilegi (Discovery, Create Storage, Modify Storage, Destroy Storage) richiesti per l'utente, quindi fare clic su **Add** (Aggiungi).

Risultati

Il nuovo ruolo e l'utente vengono aggiunti e i privilegi dettagliati vengono visualizzati sotto il ruolo configurato.

Configurare Storage Replication Adapter per il disaster recovery

Se si desidera configurare vCenter Server per il disaster recovery, è necessario attivare Storage Replication Adapter (SRA) dopo aver implementato l'appliance virtuale per Virtual Storage Console (VSC), VASA Provider e Storage Replication Adapter (SRA). L'implementazione dell'appliance virtuale installa VSC per impostazione predefinita. È necessario abilitare SRA per vCenter Server dopo l'implementazione dell'appliance virtuale.

Informazioni correlate

[Abilitare Storage Replication Adapter](#)

Configurare Storage Replication Adapter per l'ambiente SAN

È necessario configurare i sistemi storage prima di eseguire Storage Replication Adapter (SRA) per Site Recovery Manager (SRM).

Prima di iniziare

È necessario aver installato i seguenti programmi sul sito protetto e sul sito di ripristino:

- SRM

La documentazione sull'installazione di SRM è disponibile sul sito VMware.

["Documentazione di VMware Site Recovery Manager"](#)

- SRA

L'adattatore viene installato su SRM.

Fasi

1. Verificare che gli host ESXi primari siano connessi alle LUN nel sistema di storage primario sul sito

protetto.

2. Verificare che i LUN si trovino in igroups che dispongono di **ostype** opzione impostata su *vmware* sul sistema di storage primario.
3. Verificare che gli host ESXi del sito di ripristino dispongano della connettività FC o iSCSI appropriata per .

È possibile eseguire questa operazione verificando che gli host ESXi dispongano di LUN locali collegati a o utilizzando `fcpl show initiators` o `iscsi show initiators` sul .

Configurare Storage Replication Adapter per l'ambiente NAS

È necessario configurare i sistemi storage prima di eseguire Storage Replication Adapter (SRA) per VMware vCenter Site Recovery Manager (SRM).

Prima di iniziare

È necessario aver installato i seguenti programmi sul sito protetto e sul sito di ripristino:

- SRM

La documentazione sull'installazione di SRM è disponibile sul sito VMware.

["Documentazione di VMware Site Recovery Manager"](#)

- SRA

L'adattatore viene installato su SRM e sul server SRA.

Fasi

1. Verificare che gli archivi dati del sito protetto contengano macchine virtuali registrate con vCenter Server.
2. Verificare che gli host ESXi nel sito protetto abbiano montato i volumi di esportazione NFS da .
3. Verificare che gli indirizzi validi come l'indirizzo IP, il nome host o l'FQDN su cui sono presenti le esportazioni NFS siano specificati nel campo **NFS Addresses** (indirizzi NFS) quando si utilizza la procedura guidata **Array Manager** per aggiungere array a SRM.
4. Utilizzare `ping` Su ciascun host ESXi nel sito di ripristino per verificare che l'host disponga di una porta VMkernel in grado di accedere agli indirizzi IP utilizzati per le esportazioni NFS da .

["Supporto NetApp"](#)

Configurazione di Storage Replication Adapter per ambienti altamente scalabili

È necessario configurare gli intervalli di timeout dello storage in base alle impostazioni consigliate per Storage Replication Adapter (SRA) in modo da ottenere prestazioni ottimali in ambienti altamente scalabili.

Impostazioni del provider di storage

- È necessario aumentare il valore di `StorageProvider.resignatureTimeout` impostazione da 900 secondi a 12000 secondi.
- È necessario attivare `StorageProvider.autoResignatureMode` opzione.

Per ulteriori informazioni sulla modifica delle impostazioni dello Storage Provider, consultare la documentazione di VMware.

["Documentazione VMware vSphere: Modifica delle impostazioni dello Storage Provider"](#)

Impostazioni di storage

È necessario impostare il valore di `storage.commandTimeout` intervallo di timeout per ambienti altamente scalati fino a 12,000 secondi.



L'intervallo di timeout specificato è il valore massimo. Non è necessario attendere il raggiungimento del timeout massimo. La maggior parte dei comandi termina entro l'intervallo di timeout massimo impostato.

["Risposta della Knowledge base di NetApp 1001111: Guida al dimensionamento di NetApp Storage Replication Adapter 4.0/7.X per ONTAP"](#)

La documentazione VMware sulla modifica delle impostazioni DEL provider SAN contiene ulteriori informazioni.

["Documentazione di VMware Site Recovery Manager: Modifica delle impostazioni di storage"](#)

Risolvere i problemi relativi all'appliance virtuale per VSC, VASA Provider e SRA

Se durante l'installazione o la configurazione dell'appliance virtuale per Virtual Storage Console (VSC), VASA Provider e Storage Replication Adapter (SRA) si verificano comportamenti imprevisti, è possibile seguire specifiche procedure di risoluzione dei problemi per identificare e risolvere la causa di tali problemi.

Pulire i pacchetti di plug-in scaricati dalla cache di vSphere

Se i plug-in non vengono aggiornati automaticamente dopo l'implementazione o l'aggiornamento dell'appliance virtuale per VSC, VASA Provider e SRA, è necessario pulire i pacchetti plug-in di download memorizzati nella cache nel browser e nel server vCenter per risolvere i problemi di plug-in di vCenter Server.

Fasi

1. Disconnettere dal client Web vSphere o dal client vSphere esistente.
2. Rimuovere la cache del browser.
3. Rimuovere i pacchetti di plug-in cache di vSphere Client.

Se si utilizza...	Eseguire le seguenti operazioni...
Server Windows vCenter	<p>Rimuovere le seguenti cartelle com.netapp.vasa.vvol.webclient-x.x.x.xxxx, com.netapp.nvpf.webclient-x.x.x.xxxx e com.netapp.vsch5-x.x.x.xxxx disponibili all'indirizzo:</p> <ul style="list-style-type: none"> • Percorso di vSphere Web Client: C: programdata/VMware/vCenterServer/vsphere-client/pacchetti vc/vsphere-client-Serenity • Percorso del client vSphere (HTML5): C: ProgramData/VMware/vCenterServer/vsphere-ui/pacchetti vc/vsphere-client-Serenity
VCSA	<ol style="list-style-type: none"> SSH nell'appliance VCSA. Modificare le directory nella directory delle estensioni dell'interfaccia utente del client Web vCenter utilizzando <code>cd</code> /etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity Rimuovere i pacchetti di plug-in memorizzati nella cache utilizzando i comandi: <ul style="list-style-type: none"> ° <code>rm -rf com.netapp.vasa.vvol.webclient-x.x.x.xxxx</code> ° <code>rm -rf com.netapp.nvpf.webclient-x.x.x.xxxx</code> ° <code>rm -rf com.netapp.vsch5-x.x.x.xxxx</code> Modificare le directory nella directory delle estensioni dell'interfaccia utente del client vCenter (HTML5) utilizzando <code>cd</code> /etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity Rimuovere i pacchetti di plug-in memorizzati nella cache utilizzando i comandi: <ul style="list-style-type: none"> ° <code>rm -rf com.netapp.vasa.vvol.webclient-x.x.x.xxxx</code> ° <code>rm -rf com.netapp.nvpf.webclient-x.x.x.xxxx</code> ° <code>rm -rf com.netapp.vsch5-x.x.x.xxxx</code>

4. Accedere a vSphere e riavviare il client Web vSphere e i servizi client vSphere utilizzando i seguenti comandi:

- ° `service-control --stop vsphere-client vsphere-ui`
- ° `service-control --start vsphere-client vsphere-ui`

La disinstallazione non rimuove i ruoli VSC standard

Quando si disinstalla Virtual Storage Console per VMware vSphere (VSC), i ruoli VSC standard rimangono intatti. Questo è un comportamento previsto e non influisce sulle prestazioni di VSC o sulla capacità di eseguire l'aggiornamento a una nuova versione di VSC. Se necessario, è possibile eliminare manualmente questi ruoli.

Anche se l'operazione di disinstallazione non rimuove i ruoli VSC, l'operazione di disinstallazione rimuove i nomi localizzati per i privilegi specifici di VSC e aggiunge il seguente prefisso: "XXX missing Privilege". Ad esempio, se si apre la finestra di dialogo vSphere **Edit role** (Modifica ruolo) dopo l'installazione di VSC, i privilegi specifici di VSC verranno elencati come.

Questo comportamento si verifica perché vCenter Server non fornisce un'opzione per rimuovere i privilegi.

Quando si reinstalla VSC o si esegue l'aggiornamento a una versione più recente di VSC, vengono ripristinati tutti i ruoli VSC standard e i privilegi specifici di VSC.

Virtual Storage Console e file di log del provider VASA

È possibile controllare i file di registro in `/opt/netapp/vscserver/log` e a `/opt/netapp/vpserver/log` directory in caso di errori.

I seguenti tre file di log possono essere utili per identificare i problemi:

- `cxfl.log`, Contenente informazioni sul traffico API in entrata e in uscita dal provider VASA
- `kaminoPrefs.xml`, Contenente informazioni sulle impostazioni VSC
- `vvolvvp.log`, Contenente tutte le informazioni di registro relative al provider VASA

Il menu di manutenzione dell'appliance virtuale per Virtual Storage Console (VSC), VASA Provider e Storage Replication Adapter (SRA) consente di impostare diversi livelli di log in base alle proprie esigenze. Sono disponibili i seguenti livelli di log:

- Info
- Debug
- Errore
- Traccia

Quando si impostano i livelli di log, vengono aggiornati i seguenti file:

- Server VSC: `kamino.log` e `vvolvvp.log`
- Server del provider VASA: `vvolvvp.log`, `error.log`, e `netapp.log`

Inoltre, la pagina dell'interfaccia della riga di comando web (CLI) del provider VASA contiene le chiamate API

effettuate, gli errori restituiti e diversi contatori relativi alle performance. La pagina Web CLI si trova all'indirizzo https://<IP_address_or_hostname>:9083/stats.

I servizi VSC e VASA Provider vengono riavviati in ambienti altamente scalabili

Problema

L'appliance virtuale per VSC, VASA Provider e SRA potrebbe non funzionare in modo ottimale in un ambiente altamente scalabile e potrebbero verificarsi problemi come il riavvio frequente dei servizi VSC e VASA Provider.

Azione correttiva

Modificare i requisiti di RAM e memoria heap per l'appliance virtuale per VSC, VASA Provider e SRA.

https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Software/Virtual_Storage_Console_for_VMware_vSphere/tune_memory_settings_of_VM_VSC%2C_VASA_Provider%2C_and_SRA_for_scale_and_performance

Configurare il provider VASA per l'utilizzo con SSH

È possibile configurare il provider VASA in modo che utilizzi SSH per un accesso sicuro configurando l'appliance virtuale per Virtual Storage Console (VSC), VASA Provider e Storage Replication Adapter (SRA).

A proposito di questa attività

Quando si configura SSH, è necessario accedere come utente di manutenzione. Questo perché l'accesso root al provider VASA è stato disattivato. Se si utilizzano altre credenziali di accesso, non è possibile utilizzare SSH per accedere al provider VASA.

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 3 Per selezionare **Configurazione di sistema**.
4. Invio 6 Per selezionare **Enable SSH Access** (attiva accesso SSH).
5. Invio y nella finestra di dialogo di conferma.

Configurare l'appliance virtuale per VSC, VASA Provider e SRA in modo che utilizzi SSH per l'accesso di DIAG remoto

È possibile configurare l'appliance virtuale per Virtual Storage Console (VSC), VASA Provider e Storage Replication Adapter (SRA) per abilitare l'accesso SSH per l'utente DIAG.

Prima di iniziare

L'estensione del provider VASA deve essere abilitata per l'istanza di vCenter Server.

A proposito di questa attività

L'utilizzo di SSH per accedere all'utente di DIAG presenta le seguenti limitazioni:

- È consentito un solo accesso per ogni attivazione di SSH.
- L'accesso SSH all'utente di DIAG viene disattivato quando si verifica una delle seguenti condizioni:
 - Il tempo scade.

La sessione di accesso rimane valida solo fino alla mezzanotte del giorno successivo.

- Si accede nuovamente come utente di DIAG utilizzando SSH.

Fasi

1. Dal server vCenter, aprire una console per il provider VASA.
2. Accedere come utente principale.
3. Invio 4 Per selezionare **Support and Diagnostics** (supporto e diagnostica).
4. Invio 3 Per selezionare **Enable remote Diagnostics access** (Abilita accesso remoto alla diagnostica).
5. Invio y Nella finestra di dialogo **Confirmation** (Conferma) per abilitare l'accesso remoto alla diagnostica.
6. Inserire una password per l'accesso remoto alla diagnostica.

L'installazione di SRA non riesce e viene visualizzato un errore di script

Problema

L'installazione di Storage Replication Adapter (SRA) su Windows 2008 R2 non riesce e viene visualizzato un errore di credenziali non valide.

Causa

L'errore potrebbe verificarsi a causa dell'attivazione di diverse versioni di Transport Layer Security (TLS) sull'appliance virtuale per VSC, VASA Provider, SRA e Windows 2008 R2.

Azione correttiva

Se si sta tentando di installare SRA su Windows 2008 R2, è necessario attivare TLSv1.0 per l'appliance virtuale per VSC, VASA Provider e SRA seguendo la procedura riportata nella console di manutenzione:

1. Accedere alla console di manutenzione utilizzando le credenziali utente "maint".
2. Dal menu principale, selezionare **1** per il menu **Application Configuration** (Configurazione applicazione).
3. Digitare **13** nel menu **Application Configuration** per selezionare **Enable TLS Protocol** (attiva protocollo TLS) dal menu **Application Configuration** (Configurazione applicazione).
4. Selezionare **TLSv1** nell'elenco dei protocolli TLS.

I servizi del provider VSC e VASA vengono riavviati e TLSv1.0 è attivato.

È inoltre possibile attivare TLSv1.2 su Windows 2008 R2.

SRA non funziona in modo ottimale in un ambiente altamente scalabile

Problema

SRA non riesce a funzionare in modo ottimale in un ambiente altamente scalabile (se VMware ha specificato

limiti massimi come 250 PG, 250 RPS, 5000 VM) e potrebbero verificarsi problemi come un errore di timeout o un timeout ONTAP.

Azione correttiva

È necessario modificare gli intervalli di timeout.

"Configurazione di Storage Replication Adapter per ambienti altamente scalabili"



È inoltre possibile modificare le impostazioni di memoria per la scalabilità e le prestazioni dell'appliance virtuale per VSC, VASA Provider e SRA in configurazioni altamente scalate.

https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Software/Virtual_Storage_Console_for_VMware_vSphere/tune_memory_settings_of_VM_VSC%2C_VASA_Provider%2C_and_SRA_for_scale_and_performance

Impossibile installare il plug-in SRA

Problema

Durante l'installazione del plug-in Storage Replication Adapter (SRA), il sistema si arresta nella schermata dell'indirizzo IP e della password del server e viene visualizzato il seguente messaggio di errore: "le credenziali immesse non sono valide. Immettere un nome host e una password validi."

Causa

L'errore potrebbe verificarsi a causa di uno dei seguenti motivi:

- Sono state inserite credenziali di amministratore errate.
- Le impostazioni del proxy WinHTTP non sono corrette.

Azione correttiva

- Verificare le credenziali dell'amministratore.
- L'articolo della Knowledge base contiene ulteriori informazioni sulla risoluzione dei problemi relativi alle impostazioni del proxy WinHTTP.

"Risposta della Knowledge base di NetApp 1005074: L'installazione del plug-in del client SRA 4.0P1 (netapp_sra_4.0P1_ontap_64bit.msi) si blocca nella schermata dell'IP e della password del server"

L'adattatore per la replica dello storage NetApp per ONTAP non viene visualizzato sull'appliance di gestione del ripristino del sito

Problema

Storage Replication Adapter (SRA) non viene visualizzato nell'interfaccia dell'appliance Site Recovery Manager (SRM) dopo il caricamento e la configurazione di SRA.

Causa

Non viene visualizzato alcun errore quando si utilizzano credenziali SRA errate (nome utente o password) per

configurare SRA utilizzando il seguente comando.

```
perl command.pl -I <sra-server-ip> <vp_username> <vp_passwd>
```

Azione correttiva

Aggiornare i dettagli di configurazione di SRA utilizzando il seguente comando: `perl command.pl -U <sra-server-ip> <vp_username> <vp_passwd>`

Errore durante la nuova implementazione dell'appliance virtuale per VSC, VASA Provider e SRA

Problema

Il registro degli errori “vmware tools OVF vCenter Configuration not found” viene visualizzato durante la nuova implementazione dell'appliance virtuale per VSC, VASA Provider e SRA quando viene utilizzato un indirizzo vCenter Server IPv4 non valido.

Causa

L'appliance virtuale per VSC, VASA Provider e SRA supporta gli indirizzi IPv4 e IPv6. Se l'utente fornisce un indirizzo IPv4 per vCenter Server non disponibile nella rete e non è fornito alcun indirizzo IPv6, questi messaggi del logger vengono visualizzati sulla console di manutenzione.

Azione correttiva

Per rimuovere l'errore, attenersi alla seguente procedura:

1. Accedere alla console di manutenzione.
2. Accedere alla shell di diagnostica.
3. Modificare l'utente da “diag” a “root” utilizzando `sudo su` comando.
4. Modificare il file di interfaccia utilizzando l'editor `vi` `vi /etc/network/interface`.
5. Rimuovere la voce per “inet6”.
6. Salvare il file e riavviare l'appliance virtuale per VSC, VASA Provider e SRA.

Dopo aver riavviato l'appliance virtuale, non vengono visualizzati messaggi di errore.

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.