



Konfigurieren Sie Ihre Virtual Storage Console für VMware vSphere Umgebung

VSC, VASA Provider, and SRA 9.7

NetApp
March 21, 2024

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

Inhalt

Konfigurieren Sie Ihre Virtual Storage Console für VMware vSphere Umgebung	1
Konfigurieren Sie Multipathing- und Zeitüberschreitungseinstellungen für ESXi-Server	1
Erstellen Sie ein SSL-Zertifikat für die virtuelle Speicherkonsole erneut	7
Voraussetzungen für die Registrierung von VSC in einer Umgebung mit mehreren vCenter Servern	7
Konfigurieren Sie die VSC Preferences-Dateien	8
Aktivieren Sie das Mounten von Datenspeichern in unterschiedlichen Subnetzen	10
Greifen Sie auf die Optionen der Wartungskonsole der virtuellen Appliance für VSC, VASA Provider und SRA zu	11
Ändern Sie das Administratorpasswort	13
Konfigurieren Sie Hochverfügbarkeit für die virtuelle Appliance für VSC, VASA Provider und SRA	13
Von der virtuellen Appliance unterstützte MetroCluster Konfigurationen für VSC, VASA Provider und SRA	15

Konfigurieren Sie Ihre Virtual Storage Console für VMware vSphere Umgebung

(VSC) unterstützt zahlreiche Umgebungen. Einige Funktionen in diesen Umgebungen erfordern möglicherweise zusätzliche Konfigurationen.

Möglicherweise müssen Sie einige der folgenden Aufgaben durchführen, um Ihre ESXi Hosts, Gastbetriebssysteme und VSC zu konfigurieren:

- Überprüfen der ESXi-Hosteinstellungen, einschließlich der UNMAP-Einstellungen
- Hinzufügen von Timeout-Werten für Gastbetriebssysteme
- Erneutes Generieren des VSC SSL-Zertifikats
- Erstellung von Storage-Funktionsprofilen und Schwellenwertwarnungen
- Ändern der Preferences-Datei, um das Mounten von Datastores über verschiedene Subnetze zu ermöglichen

Konfigurieren Sie Multipathing- und Zeitüberschreitungseinstellungen für ESXi-Server

Die Virtual Storage Console für VMware vSphere überprüft und legt die Einstellungen für Multipathing des ESXi Hosts und HBA-Zeitüberschreitungseinstellungen fest, die für Storage-Systeme am besten geeignet sind.

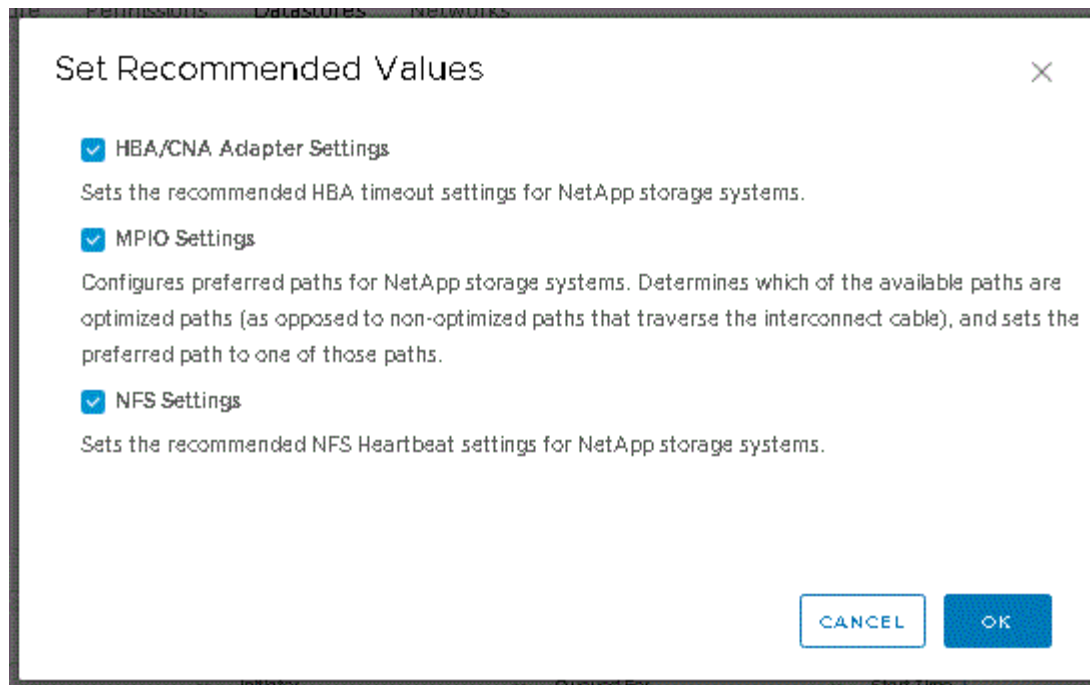
Über diese Aufgabe

Dieser Prozess kann je nach Konfiguration und Systemlast sehr viel Zeit in Anspruch nehmen. Der Aufgabenfortschritt wird im Fenster **Letzte Aufgaben** angezeigt. Wenn die Aufgaben abgeschlossen sind, wird das Symbol für die Warnung des Host-Status durch das Symbol Normal oder das Symbol Ausstehender Neustart ersetzt.

Schritte

1. Klicken Sie auf der Seite VMware vSphere Web Client **Home** auf Menü:vCenter[Hosts].
2. Klicken Sie mit der rechten Maustaste auf einen Host und wählen Sie dann Menü:Actions[NetApp VSC > Set Recommended Values] aus.
3. Wählen Sie im Dialogfeld **NetApp Recommended Settings** die Werte aus, die für Ihr System am besten geeignet sind.

Standardmäßig werden die empfohlenen Standardwerte festgelegt.



4. Klicken Sie auf **OK**.

ESXi-Hostwerte werden mit Virtual Storage Console für VMware vSphere festgelegt

Sie können mithilfe der virtuellen Speicherkonsole für VMware vSphere Timeouts und andere Werte auf den ESXi-Hosts festlegen, um beste Leistung und erfolgreiches Failover zu gewährleisten. Die Werte, die Virtual Storage Console (VSC) setzt, basieren auf internen Tests.

Auf einem ESXi-Host können Sie die folgenden Werte festlegen:

Erweiterte ESXi Konfiguration

- **VMFS3.HardwareAcceleratLocking**

Sie sollten diesen Wert auf 1 setzen.

- **VMFS3.EnableBlockDelete**

Sie sollten diesen Wert auf 0 setzen.

NFS-Einstellungen

- **Net.TcpipHeapSize**

Wenn Sie vSphere 6.0 oder höher verwenden, sollten Sie diesen Wert auf 32 setzen.

- **Net.TcpipHeapMax**

Wenn Sie vSphere 6.0 oder höher verwenden, sollten Sie diesen Wert auf 1536 setzen.

- **NFS.MaxVolumes**

Wenn Sie vSphere 6.0 oder höher verwenden, sollten Sie diesen Wert auf 256 setzen.

- **NFS41.MaxVolumes**

Wenn Sie vSphere 6.0 oder höher verwenden, sollten Sie diesen Wert auf 256 setzen.

- **NFS.MaxQueueDepth**

Wenn Sie vSphere 6.0 oder höhere ESXi Host-Version verwenden, sollten Sie diesen Wert auf 128 oder höher einstellen, um Engpässe zu vermeiden, in denen es zu Warteschlangen kommt.

Bei vSphere-Versionen vor 6.0 sollten Sie diesen Wert auf 64 einstellen.

- **NFS.HeartbeatMaxFailures**

Sie sollten diesen Wert für alle NFS-Konfigurationen auf 10 setzen.

- **NFS.HeartbeatFrequency**

Sie sollten diesen Wert für alle NFS-Konfigurationen auf 12 setzen.

- **NFS.HeartbeatTimeout**

Sie sollten diesen Wert für alle NFS-Konfigurationen auf 5 setzen.

FC-/FCoE-Einstellungen

- **Pfadauswahl-Richtlinie**

Wenn FC-Pfade mit ALUA verwendet werden, sollten Sie diesen Wert auf „RR“ (Round Robin) setzen.

Sie sollten diesen Wert für alle anderen Konfigurationen auf „FIXED“ setzen.

Wenn Sie diesen Wert auf „RR“ setzen, ist für den Lastausgleich über alle aktiven/optimierten Pfade hinweg hilfreich. Der Wert „FIXED“ wird für ältere Konfigurationen ohne ALUA verwendet und verhindert Proxy-I/O

- **Disk.QFullSampleSize**

Sie sollten diesen Wert für alle Konfigurationen auf 32 setzen. Durch die Festlegung dieses Wertes werden I/O-Fehler verhindert.

- **Disk.QFullThreshold**

Sie sollten diesen Wert für alle Konfigurationen auf 8 setzen. Durch die Festlegung dieses Wertes werden I/O-Fehler verhindert.

- *** Emulex FC HBA-Timeouts***

Standardwert verwenden.

- **QLogic FC HBA Timeouts**

Standardwert verwenden.

ISCSI-Einstellungen

- **Pfadauswahl-Richtlinie**

Sie sollten diesen Wert für alle iSCSI-Pfade auf „RR“ setzen.

Wenn Sie diesen Wert auf „RR“ setzen, ist für den Lastausgleich über alle aktiven/optimierten Pfade hinweg hilfreich.

- **Disk.QFullSampleSize**

Sie sollten diesen Wert für alle Konfigurationen auf 32 setzen. Durch die Festlegung dieses Wertes werden I/O-Fehler verhindert.

- **Disk.QFullThreshold**

Sie sollten diesen Wert für alle Konfigurationen auf 8 setzen. Durch die Festlegung dieses Wertes werden I/O-Fehler verhindert.

Konfigurieren von Gast-Betriebssystem-Skripten

Die ISO-Images des Gastbetriebssystems (OS)-Skripte werden auf der Virtual Storage Console für VMware vSphere Server eingebunden. Damit Sie die Speicherzeituts für virtuelle Maschinen mithilfe der Gast-BS-Skripts festlegen können, müssen Sie die Skripte vom vSphere-Client mounten.

Betriebssystemtyp	Einstellungen für das Zeitlimit von 60 Sekunden	Einstellungen für das Zeitlimit von 190 Sekunden
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>

Sie sollten das Skript aus der Kopie der VSC-Instanz installieren, die beim vCenter Server registriert ist, der die Virtual Machine managt. Wenn in Ihrer Umgebung mehrere vCenter-Server enthalten sind, sollten Sie den Server auswählen, der die virtuelle Maschine enthält, für die Sie die Werte für das Speicherzeitlimit festlegen möchten.

Sie sollten sich bei der virtuellen Maschine anmelden und dann das Skript ausführen, um die Werte für die Speicherzeitüberschreitung festzulegen.

Legen Sie die Zeitüberschreitungswerte für Windows Gastbetriebssysteme fest

Die Timeout-Skripte des Gastbetriebssystems (OS) legen die SCSI I/O Timeout-Einstellungen für Windows Gastbetriebssysteme fest. Sie können entweder eine Zeitüberschreitung von 60 Sekunden oder eine Zeitüberschreitung von 190 Sekunden angeben. Sie müssen das Windows Gast-Betriebssystem neu booten, damit die Einstellungen wirksam werden.

Bevor Sie beginnen

Sie müssen das ISO-Image mit dem Windows-Skript angehängt haben.

Schritte

1. Greifen Sie auf die Konsole der virtuellen Windows-Maschine zu und melden Sie sich bei einem Konto mit Administratorrechten an.
2. Wenn das Skript nicht automatisch startet, öffnen Sie das CD-Laufwerk, und führen Sie dann den aus `windows_gos_timeout.reg` Skript:

Das Dialogfeld Registry-Editor wird angezeigt.

3. Klicken Sie auf **Ja**, um fortzufahren.

Die folgende Meldung wird angezeigt: The keys and values contained in `D:\windows_gos_timeout.reg` have been successfully added to the registry.

4. Starten Sie das Windows Gastbetriebssystem neu.
5. Heben Sie die Bereitstellung des ISO-Images auf.

Legen Sie Timeout-Werte für Solaris Gastbetriebssysteme fest

Die Timeout-Skripte des Gastbetriebssystems (OS) legen die SCSI I/O Timeout-Einstellungen für Solaris 10 fest. Sie können entweder eine Zeitüberschreitung von 60 Sekunden oder eine Zeitüberschreitung von 190 Sekunden angeben.

Bevor Sie beginnen

Sie müssen das ISO-Image mit dem Solaris-Skript angehängt haben.

Schritte

1. Greifen Sie auf die Konsole der virtuellen Solaris-Maschine zu und melden Sie sich bei einem Konto mit Root-Berechtigungen an.
2. Führen Sie die aus `solaris_gos_timeout-install.sh` Skript:

Bei Solaris 10 wird eine Meldung wie die folgende angezeigt:

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

3. Heben Sie die Bereitstellung des ISO-Images auf.

Legen Sie Timeout-Werte für Linux Gast-Betriebssysteme fest

Die Timeout-Skripte des Gastbetriebssystems (OS) stellen die SCSI-I/O-Zeitüberschreitungseinstellungen für die Versionen 4, 5, 6 und 7 von Red hat Enterprise Linux sowie 9, 10 und 11 von SUSE Linux Enterprise Server ein. Sie können entweder eine Zeitüberschreitung von 60 Sekunden oder eine Zeitüberschreitung von 190 Sekunden angeben. Sie müssen das Skript jedes Mal ausführen, wenn Sie auf eine neue Linux-Version aktualisieren.

Bevor Sie beginnen

Sie müssen das ISO-Image mit dem Linux-Skript angehängt haben.

Schritte

1. Greifen Sie auf die Konsole der virtuellen Linux-Maschine zu und melden Sie sich bei einem Konto mit Root-Berechtigungen an.
2. Führen Sie die aus `linux_gos_timeout-install.sh` Skript:

Für Red hat Enterprise Linux 4 oder SUSE Linux Enterprise Server 9 wird eine Meldung wie die folgende angezeigt:

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

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

Für Red hat Enterprise Linux 5, Red hat Enterprise Linux 6 und Red hat Enterprise Linux 7 wird eine Meldung wie die folgende angezeigt:

```
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!
```

Für SUSE Linux Enterprise Server 10 oder SUSE Linux Enterprise Server 11 wird eine Meldung wie die folgende angezeigt:


```
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. Heben Sie die Bereitstellung des ISO-Images auf.

Erstellen Sie ein SSL-Zertifikat für die virtuelle Speicherkonsole erneut

Das SSL-Zertifikat wird bei der Installation (VSC) generiert. Der Distinguished Name (DN), der für das SSL-Zertifikat generiert wird, ist möglicherweise kein allgemeiner Name (CN), den die Clientcomputer erkennen. Durch Ändern der Passwörter für den Schlüsselspeicher und den privaten Schlüssel können Sie das Zertifikat erneut generieren und ein standortspezifisches Zertifikat erstellen.

Über diese Aufgabe

Sie können die Remote-Diagnose mit der Wartungskonsole aktivieren und standortspezifisches Zertifikat generieren.

["Antwort der NetApp Knowledgebase 1075654: Virtual Storage Console 7.x: Implementierung von CA-signierten Zertifikaten"](#)

Schritte

1. Melden Sie sich bei der Wartungskonsole an.
2. Eingabe 1 Für den Zugriff auf Application Configuration Menü.
3. Im Application Configuration Menü, ENTER 3 Um den VSC Service zu beenden.
4. Eingabe 7 Um das SSL-Zertifikat erneut zu generieren.

Voraussetzungen für die Registrierung von VSC in einer Umgebung mit mehreren vCenter Servern

Wenn Sie Virtual Storage Console für VMware vSphere in einer Umgebung mit einem einzelnen VMware vSphere HTML5-Client verwenden. Managt mehrere vCenter Server-Instanzen, müssen Sie eine Instanz von VSC bei jedem vCenter Server registrieren, sodass ein 1:1-Paarung zwischen der VSC und dem vCenter Server besteht. Auf diese Weise können Sie alle Server mit vCenter 6.0 oder höher sowohl im verknüpften Modus

als auch im nicht verknüpften Modus von einem einzelnen vSphere HTML5 Client aus verwalten.



Falls Sie VSC mit einem vCenter Server verwenden möchten, müssen Sie eine VSC-Instanz für jede zu verwaltende vCenter Server-Instanz eingerichtet oder registriert haben. Jede registrierte VSC Instanz muss von der gleichen Version sein.

Der verknüpfte Modus wird während der Bereitstellung von vCenter Server automatisch installiert. Der Linked-Modus verwendet den Microsoft Active Directory Application Mode (ADAM), um Daten über mehrere vCenter Server-Systeme hinweg zu speichern und zu synchronisieren.

Die Verwendung des vSphere HTML5 Client zur Durchführung von VSC Aufgaben über mehrere vCenter Server hinweg erfordert Folgendes:

- Für jeden vCenter Server im VMware Inventar, den Sie managen möchten, muss ein einzelner VSC Server mit einem eindeutigen 1:1-Paarungsvorgang registriert sein.

Zum Beispiel können Sie den VSC-Server A bei vCenter Server A registrieren, VSC-Server B bei vCenter Server B registriert sein, VSC-Server C bei vCenter Server C registriert sind usw.

Sie können * nicht * VSC Server Eine registriert haben, sowohl vCenter Server A und vCenter Server B.

Wenn ein VMware Inventar einen vCenter Server beinhaltet, für den kein VSC Server registriert ist, aber es gibt einen oder mehrere vCenter Server, die bei VSC registriert sind, Anschließend können Sie die Instanzen von VSC anzeigen und VSC Vorgänge für die vCenter Server ausführen, auf denen die VSC registriert ist.

- Sie müssen über die VSC-spezifische View-Berechtigung für jeden vCenter Server verfügen, der bei Single Sign-On (SSO) registriert ist.

Außerdem müssen Sie über die richtigen RBAC-Berechtigungen verfügen.

Wenn Sie eine Aufgabe ausführen, bei der Sie einen vCenter-Server angeben müssen, werden im Dropdown-Feld **vCenter Server** die verfügbaren vCenter-Server in alphanumerischer Reihenfolge angezeigt. Der standardmäßige vCenter Server ist immer der erste Server in der Dropdown-Liste.

Wenn der Speicherort des Speichers bekannt ist (z. B. wenn Sie den **Provisioning**-Assistenten verwenden und sich der Datastore auf einem Host befindet, der von einem bestimmten vCenter Server verwaltet wird), wird die vCenter Server-Liste als schreibgeschützte Option angezeigt. Dies geschieht nur, wenn Sie ein Element im vSphere Web Client mit der rechten Maustaste auswählen.

VSC warnt Sie, wenn Sie versuchen, ein Objekt auszuwählen, das nicht gemanagt wird.

Sie können Storage-Systeme auf der Grundlage eines bestimmten vCenter Servers von der VSC Übersichtsseite aus filtern. Für jede VSC Instanz, die mit einem vCenter Server registriert ist, wird eine Übersichtsseite angezeigt. Sie können die Storage-Systeme, die einer bestimmten VSC Instanz und vCenter Server zugeordnet sind, verwalten. Allerdings sollten Sie die Registrierungsinformationen für jedes Storage-System getrennt aufbewahren, wenn Sie mehrere Instanzen von VSC ausführen.

Konfigurieren Sie die VSC Preferences-Dateien

Die Einstellungsdateien enthalten Einstellungen, die die Vorgänge Virtual Storage Console für VMware vSphere steuern. In den meisten Fällen müssen Sie die

Einstellungen in diesen Dateien nicht ändern. Es ist hilfreich zu wissen, welche Vorzugsdateien (VSC) verwenden.

Die VSC enthält verschiedene Voreinstellungsdateien. Diese Dateien enthalten Eintragungsschlüssel und Werte, die bestimmen, wie VSC verschiedene Vorgänge durchführt. Im Folgenden werden einige Präferenz-Dateien beschrieben, die VSC verwendet:

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

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

Möglicherweise müssen Sie die Voreinpräferenzen-Dateien in bestimmten Situationen ändern. Wenn Sie beispielsweise iSCSI oder NFS verwenden und das Subnetz zwischen Ihren ESXi Hosts und Ihrem Speichersystem unterschiedlich ist, müssen Sie die Voreinstellungen ändern. Falls Sie die Einstellungen in der Voreinstellungsdatei nicht ändern, schlägt die Datastore-Bereitstellung fehl, da VSC den Datastore nicht mounten kann.

Legen Sie IPv4 oder IPv6 fest

Der Vorzugsdatei wurde eine neue Option hinzugefügt `kaminoprefs.xml`. Die Sie einstellen können, dass IPv4 oder IPv6 für alle Storage-Systeme, die der VSC hinzugefügt werden, aktiviert werden.

- Der `default.override.option.provision.mount.datastore.address.family` Der Parameter wurde dem hinzugefügt `kaminoprefs.xml`. Bevorzugte Datei zur Festlegung eines bevorzugten LIF-Protokolls für die Bereitstellung von Datenspeichern.

Diese Präferenz gilt für alle neu zu VSC hinzugefügten Storage-Systeme.

- Die Werte für die neue Option sind `IPv4`, `IPv6`, und `NONE`.
- Der Wert ist standardmäßig auf festgelegt `NONE`.

Wert	Beschreibung
KEINE	<ul style="list-style-type: none">• Bei der Bereitstellung wird derselbe IPv6- oder IPv4-Adresstyp von Daten-LIF wie der Typ des Clusters oder die Management-LIF verwendet, die zum Hinzufügen des Storage verwendet wird.• Wenn der gleiche IPv6- oder IPv4-Adresstyp von Daten-LIF nicht in vorhanden ist, dann erfolgt die Bereitstellung über die andere Art von Daten-LIF, falls verfügbar.
IPv4	<ul style="list-style-type: none">• Die Bereitstellung erfolgt über die IPv4 Daten-LIF in der ausgewählt .• Wenn das keine IPv4-Daten-LIF hat, dann erfolgt die Bereitstellung über die IPv6-Daten-LIF, wenn sie im verfügbar ist.

Wert	Beschreibung
IPv6	<ul style="list-style-type: none"> Die Bereitstellung erfolgt über die IPv6-Daten-LIF in der ausgewählten . Wenn das keine IPv6-Daten-LIF hat, dann erfolgt die Bereitstellung über die IPv4-Daten-LIF, sofern sie im verfügbar ist.

Aktivieren Sie das Mounten von Datenspeichern in unterschiedlichen Subnetzen

Wenn Sie iSCSI oder NFS verwenden und sich das Subnetz zwischen Ihren ESXi Hosts und Ihrem Speichersystem unterscheidet, müssen Sie die Voreinstellungen für Virtual Storage Console für VMware vSphere ändern. Wenn Sie die Voreinferenzdatei nicht ändern, schlägt die Bereitstellung von Datastore fehl, da (VSC) den Datastore nicht mounten kann.

Über diese Aufgabe

Wenn die Bereitstellung von Datenspeichern fehlschlägt, protokolliert VSC die folgenden Fehlermeldungen:

```
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."
```

Schritte

1. Melden Sie sich bei Ihrer vCenter Server-Instanz an.
2. Starten Sie die Wartungskonsole mit der virtuellen Maschine Ihrer vereinheitlichten Appliance.

"Greifen Sie auf die [Optionen der Wartungskonsole der virtuellen Appliance für VSC, VASA Provider und SRA zu](#)"

3. Eingabe 4 Um die Option **Support und Diagnose** zu öffnen.
4. Eingabe 2 Um die Option **Access Diagnostic Shell** zu öffnen.
5. Eingabe `vi /opt/netapp/vscserver/etc/kamino/kaminoprefs.xml` Um die zu aktualisieren `kaminoprefs.xml` Datei:
6. Aktualisieren Sie die `kaminoprefs.xml` Datei:

Verwenden Sie...	Tun Sie das...
iSCSI	Ändern Sie den Wert der Eintragstaste <code>default.allow.iscsi.mount.networks</code> Von ALLEN bis zum Wert Ihrer ESXi Hostnetzwerke.

Verwenden Sie...	Tun Sie das...
NFS	Ändern Sie den Wert der Eintragstaste <code>default.allow.nfs.mount.networks</code> Von ALLEN bis zum Wert Ihrer ESXi Hostnetzwerke.

Die Vorgabedatei enthält Beispielwerte für diese Eintragstasten.



Der Wert „ALL“ bedeutet nicht alle Netzwerke. „ALL“ ermöglicht die Verwendung aller übereinstimmenden Netzwerke zwischen dem Host und dem Speichersystem zur Mounten von Datastores. Wenn Sie Hostnetzwerke angeben, können Sie das Mounten nur über die angegebenen Subnetze aktivieren.

7. Speichern und schließen Sie das `kaminoprefs.xml` Datei:

Greifen Sie auf die Optionen der Wartungskonsole der virtuellen Appliance für VSC, VASA Provider und SRA zu

Ihre Applikations-, System- und Netzwerkkonfigurationen können über die Wartungskonsole der virtuellen Appliance für Virtual Storage Console (VSC), VASA Provider und Storage Replication Adapter (SRA) gemanagt werden. Sie können Ihr Administratorkennwort und Ihr Wartungskennwort ändern. Außerdem können Sie Supportpakete generieren, verschiedene Protokollebenen festlegen, TLS-Konfigurationen anzeigen und verwalten und die Remote-Diagnose starten.


Bevor Sie beginnen

Nach der Implementierung der virtuellen Appliance für VSC, VASA Provider und SRA müssen die VMware Tools installiert sein.

Über diese Aufgabe

- Sie müssen „maint“ als Benutzername und das bei der Implementierung konfigurierte Passwort verwenden, um sich bei der Wartungskonsole der virtuellen Appliance für VSC, VASA Provider und SRA anzumelden.
- Sie müssen ein Passwort für den Benutzer „diag“ festlegen, während Sie die Ferndiagnose aktivieren.

Schritte

1. Öffnen Sie die Registerkarte **Zusammenfassung** Ihrer bereitgestellten virtuellen Appliance.
2. Klicken Sie Auf  Um die Wartungskonsole zu starten.

Sie können auf die folgenden Optionen für die Wartungskonsole zugreifen:

◦ Anwendungskonfiguration

Folgende Optionen stehen zur Verfügung:

- Zeigt eine Zusammenfassung des Serverstatus an
- Starten Sie den Virtual Storage Console Service

- Beenden Sie den Virtual Storage Console Service
- Starten Sie VASA Provider und SRA Service
- Beenden Sie den VASA Provider und den SRA Service
- Ändern Sie das Benutzerpasswort „Administrator“
- Zertifikate erneut generieren
- Hard Reset KeyStore und Zertifikate
- Hard Reset-Datenbank
- ÄNDERN SIE DAS PROTOKOLL-Level für den Virtual Storage Console-Service
- Ändern Sie DIE PROTOKOLLEBENE für den VASA Provider und den SRA Service
- Anzeigen der TLS-Konfiguration
- Aktivieren des TLS-Protokolls
- Deaktivieren des TLS-Protokolls

◦ **Systemkonfiguration**

Folgende Optionen stehen zur Verfügung:

- Starten Sie die virtuelle Maschine neu
- Virtuelle Maschine herunterfahren
- Ändern Sie das Benutzerpasswort „Wartung“
- Zeitzone ändern
- NTP-Server ändern

Sie können eine IPv6-Adresse für Ihren NTP-Server angeben.

- SSH-Zugriff aktivieren/deaktivieren
- Erhöhen der Größe der Jail-Festplatte (/jail)
- Upgrade
- Installation der VMware Tools

◦ **Netzwerkkonfiguration**

Folgende Optionen stehen zur Verfügung:

- Zeigt die Einstellungen für die IP-Adresse an
- Ändern Sie die IP-Adresseinstellungen

Sie können diese Option verwenden, um die IP-Adresse nach der Implementierung in IPv6 zu ändern.

- Zeigen Sie die Einstellungen für die Suche nach Domain-Namen an
- Ändern Sie die Einstellungen für die DNS-Suche
- Statische Routen anzeigen
- Ändern Sie statische Routen

Sie können diese Option verwenden, um eine IPv6-Route hinzuzufügen.

- Änderungen speichern
- Ping an einen Host

Sie können diese Option verwenden, um einen Ping an einen IPv6-Host zu senden.

- Standardeinstellungen wiederherstellen

- **Support und Diagnose**

Folgende Optionen stehen zur Verfügung:

- Erzeugen Sie das Support Bundle
- Zugriff auf die Diagnoseschale
- Remote-Diagnosezugriff aktivieren

Verwandte Informationen

[Protokolldateien von VSC und VASA Provider](#)

Ändern Sie das Administratorpasswort

Sie können das Administratorpasswort der virtuellen Appliance für VSC, VASA Provider und SRA nach der Implementierung über die Wartungskonsole ändern.

Schritte

1. Öffnen Sie über den vCenter Server eine Konsole für die virtuelle Appliance für VSC, VASA Provider und SRA.
2. Melden Sie sich als Wartungbenutzer an.
3. Eingabe 1 Wählen Sie in der Wartungskonsole **Anwendungskonfiguration** aus.
4. Eingabe 6 So wählen Sie **Administratorpasswort ändern** aus.
5. Geben Sie ein Passwort mit mindestens acht Zeichen und maximal 63 Zeichen ein.
6. Eingabe y Im Bestätigungsdialogfeld.

Konfigurieren Sie Hochverfügbarkeit für die virtuelle Appliance für VSC, VASA Provider und SRA

Die virtuelle Appliance für Virtual Storage Console (VSC), VASA Provider und Storage Replication Adapter (SRA) unterstützt eine Konfiguration (HA), sodass während eines Ausfalls unterbrechungsfreie Funktionen von VSC, VASA Provider und SRA verfügbar gemacht werden.

Die virtuelle Appliance für VSC, VASA Provider und SRA basiert auf der VMware vSphere (HA)-Funktion und der vSphere Fehlertoleranz (FT)-Funktion. (HA)-Lösung bietet eine schnelle Recovery nach Ausfällen. Die folgenden Ursachen sind:

- Host-Ausfall
- Netzwerkausfall

- Fehler bei Virtual Machine (Ausfall des Gastbetriebssystems)
- Absturz der Applikation (VSC, VASA Provider und SRA)

Auf der virtuellen Appliance ist keine zusätzliche Konfiguration erforderlich. Nur vCenter-Server und ESXi-Hosts müssen mit der VMware vSphere HA-Funktion oder der vSphere FT-Funktion basierend auf ihren Anforderungen konfiguriert werden. Sowohl HA als AUCH FT erfordern Cluster-Hosts zusammen mit Shared Storage. FT hat zusätzliche Anforderungen und Einschränkungen.

Neben der VMware vSphere HA Lösung und der vSphere FT Lösung unterstützt die virtuelle Appliance auch dabei, VSC, VASA Provider und SRA Services jederzeit verfügbar zu halten. Der Watchdog-Prozess der virtuellen Appliance überwacht regelmäßig alle drei Dienste und startet sie automatisch neu, wenn Fehler erkannt werden. So wird Applikationsausfälle verhindert.



vCenter HA wird von der virtuellen Appliance für VSC, VASA Provider und SRA nicht unterstützt.

VMware vSphere HA

Sie können Ihre vSphere Umgebung dort konfigurieren, wo die virtuelle Appliance für Virtual Storage Console (VSC), VASA Provider und Storage Replication Adapter (SRA) für (HA) implementiert wird. Die VMware HA-Funktion bietet Failover-Schutz vor Hardware-Ausfällen und Ausfällen des Betriebssystems in virtuellen Umgebungen.

Die VMware HA Funktion überwacht Virtual Machines und erkennt so Betriebssystemausfälle und Hardwareausfälle. Wenn ein Fehler erkannt wird, startet die VMware HA-Funktion die virtuellen Maschinen auf den anderen physischen Servern im Ressourcenpool neu. Wenn ein Serverfehler erkannt wird, ist keine manuelle Intervention erforderlich.

Das Verfahren zur Konfiguration von VMware HA hängt von der Version des vCenter Servers ab. Sie können beispielsweise den folgenden Referenzlink verwenden und die erforderliche vCenter Server-Version auswählen, um die Schritte zum Konfigurieren von VMware HA anzuzeigen.

["VMware vSphere Dokumentation: Erstellen und Verwenden von vSphere HA-Clustern"](#)

Fehlertoleranz für VMware vSphere

Die VMware vSphere Fault Tolerance (FT) Funktion bietet (HA) auf höherer Ebene und ermöglicht es Ihnen, Virtual Machines ohne Datenverlust oder Verbindungen zu schützen. Sie müssen vSphere FT für die virtuelle Appliance für VSC, VASA Provider und SRA über Ihren vCenter Server aktivieren oder deaktivieren.

Stellen Sie sicher, dass Ihre vSphere Lizenz FT mit der Anzahl der vCPUs unterstützt, die die virtuelle Appliance in Ihrer Umgebung benötigt (mindestens 2 vCPUs; 4 vCPUs für große Umgebungen).

VSphere FT ermöglicht den Betrieb von Virtual Machines selbst bei Serverausfällen. Wenn vSphere FT auf einer virtuellen Maschine aktiviert ist, wird automatisch eine Kopie der primären virtuellen Maschine auf einem anderen Host (der sekundären virtuellen Maschine) erstellt, der vom Distributed Resource Scheduler (DRS) ausgewählt wird. Wenn DRS nicht aktiviert ist, wird der Zielhost von den verfügbaren Hosts ausgewählt. VSphere FT betreibt die primäre virtuelle Maschine und die sekundäre virtuelle Maschine im Sperrmodus, wobei jeder den Ausführungsstatus der primären Virtual Machine auf die sekundäre Virtual Machine spiegelt.

Wenn ein Hardwarefehler auftritt, der dazu führt, dass die primäre virtuelle Maschine ausfällt, nimmt die

sekundäre virtuelle Maschine sofort dort auf, wo die primäre virtuelle Maschine angehalten wurde. Die sekundäre Virtual Machine wird weiterhin ohne Verlust von Netzwerkverbindungen, Transaktionen oder Daten ausgeführt.

Ihr System muss die CPU-Anforderungen, die Grenzwerte für virtuelle Maschinen sowie die Lizenzierungsanforderungen für die Konfiguration von vSphere FT für Ihre vCenter Server-Instanz erfüllen.

Das Verfahren zur HA-Konfiguration hängt von der Version des vCenter Servers ab. Sie können beispielsweise den folgenden Referenzlink verwenden und die erforderliche vCenter Server-Version auswählen, um die Schritte zum Konfigurieren von HA anzuzeigen.

["VMware vSphere Dokumentation: Fehlertoleranz, Beschränkungen und Lizenzierung"](#)

Von der virtuellen Appliance unterstützte MetroCluster Konfigurationen für VSC, VASA Provider und SRA

Die virtuelle Appliance für Virtual Storage Console (VSC), VASA Provider und Storage Replication Adapter (SRA) unterstützt Umgebungen, die MetroCluster IP- und FC-Konfigurationen für ONTAP verwenden. Der Support erfolgt meistens automatisch. Unter Umständen können Sie bei Verwendung einer MetroCluster Umgebung mit VSC und VASA Provider jedoch einige Unterschiede feststellen.

MetroCluster Konfigurationen und VSC

Sie müssen sicherstellen, dass die VSC die Storage-System-Controller am primären und sekundären Standort erkennt. In der Regel erkennt VSC automatisch Storage Controller. Wenn Sie eine Cluster-Management-LIF verwenden, empfehlen wir, sicherzustellen, dass die VSC die Cluster an beiden Standorten erkannt hat. Andernfalls können Sie die Storage Controller manuell zur VSC hinzufügen. Sie können auch den Benutzernamen und die Passwörter, die VSC für die Verbindung zu den Storage Controllern verwendet, ändern.

Bei einem Switchover wird der am sekundären Standort übertragen. Diese haben das Suffix „-mc“ an ihre Namen angehängt. Falls während eines Umschaltvorgangs z. B. zur Bereitstellung eines Datastores ein Switchover stattfindet, wird der Name des Speicherorts geändert und schließt dann das „-mc“-Suffix ein. Dieses Suffix wird beim Zurück-Wechsel abgebrochen und das Suffix am primären Standort wird mit der Steuerung fortgesetzt.



Wenn Sie direkt mit der MetroCluster Konfiguration zur VSC hinzugefügt haben, so wird nach der Umschaltung die Änderung des SVM-Namens (hinzugefügt durch das „-mc“ Suffix) nicht wiedergegeben. Alle anderen Switchover-Vorgänge werden weiterhin normal ausgeführt.

Wenn ein Switchover oder ein Switchover stattfindet, kann die VSC einige Minuten dauern, um die Cluster automatisch zu erkennen und zu erkennen. Wenn dies während der Durchführung einer VSC-Operation wie der Bereitstellung eines Datenspeichers geschieht, kann es zu Verzögerungen kommen.

MetroCluster Konfigurationen und VASA Provider

VASA-Provider unterstützt automatisch Umgebungen, die MetroCluster-Konfigurationen verwenden. Die Umschaltung ist in VASA Provider-Umgebungen transparent. Sie können kein direktes Add-to-VASA-Provider hinzufügen.



VASA Provider fügt nach einer Umschaltung das Suffix „-mc“ nicht an die Namen des am sekundären Standort an.

MetroCluster Konfigurationen und SRA

SRA unterstützt keine MetroCluster-Konfigurationen.

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.