



設定VMware vSphere環境的虛擬儲存主控台 VSC, VASA Provider, and SRA 9.7

NetApp
March 21, 2024

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

目錄

設定VMware vSphere環境的虛擬儲存主控台	1
設定ESXi伺服器多重路徑和逾時設定	1
為虛擬儲存主控台重新產生SSL憑證	7
在多個vCenter Server環境中登錄VSC的需求	7
設定VSC喜好設定檔案	8
在不同的子網路上啟用資料存放區裝載	9
存取VSC、VASA Provider和SRA虛擬應用裝置的維護主控台選項	10
變更系統管理員密碼	12
為VSC、VASA Provider及SRA設定虛擬應用裝置的高可用度	12
VSC、VASA Provider和SRA虛擬應用裝置支援的支援範本組態MetroCluster	13

設定VMware vSphere環境的虛擬儲存主控台

(VSC) 支援多種環境。這些環境中的某些功能可能需要額外的組態。

您可能必須執行下列部分工作、才能設定ESXi主機、客體作業系統和VSC：

- 驗證ESXi主機設定、包括取消對應設定
- 新增來賓作業系統的逾時值
- 重新產生VSC SSL憑證
- 建立儲存功能設定檔和臨界值警示
- 修改喜好設定檔、以便在不同的子網路上裝載資料存放區

設定ESXi伺服器多重路徑和逾時設定

適用於VMware vSphere的虛擬儲存主控台會檢查並設定ESXi主機多重路徑設定、以及最適合儲存系統的HBA逾時設定。

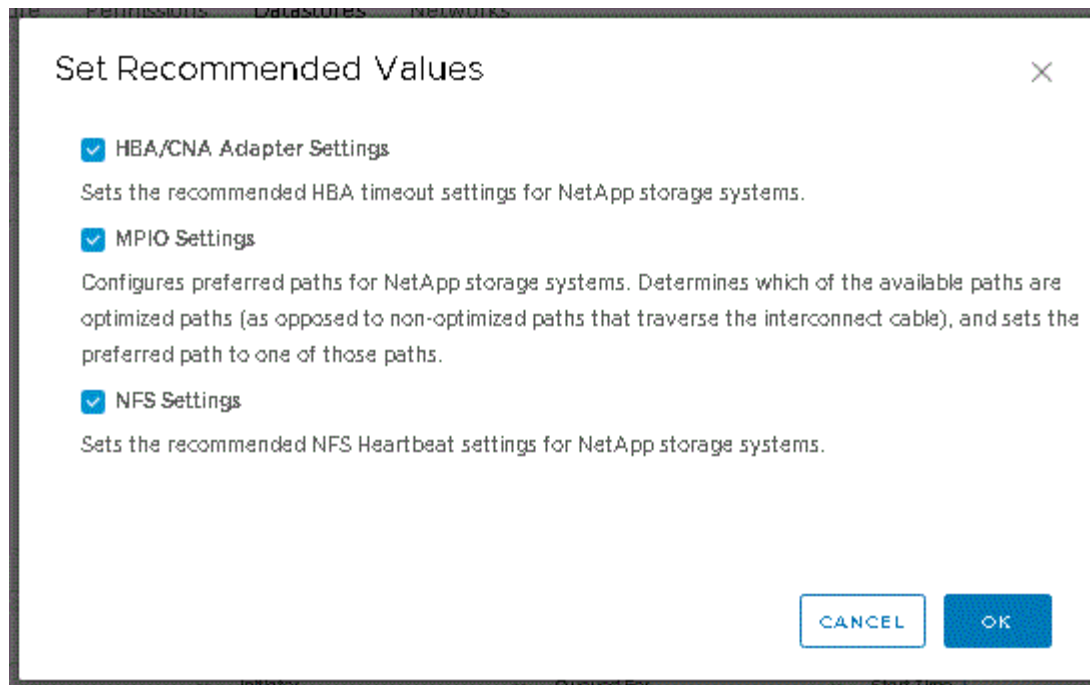
關於這項工作

視組態和系統負載而定、此程序可能需要很長時間。工作進度會顯示在「近期工作」面板中。工作完成時、主機狀態警示圖示會以正常圖示或「等待重新開機」圖示取代。

步驟

1. 在VMware vSphere Web Client *主頁*頁面中、按一下功能表：vCenter[hosts]。
2. 以滑鼠右鍵按一下主機、然後選取功能表：「Actions（動作）」[NetApp VSC > 「Set Recommended Values（設定建議值）」。
3. 在「* NetApp Recommended Settings*（* NetApp建議設定*）」對話方塊中、選取最適合您系統的值。

預設會設定建議的標準值。



4. 按一下「確定」。

使用VMware vSphere虛擬儲存主控台設定的ESXi主機值

您可以使用VMware vSphere的虛擬儲存主控台、在ESXi主機上設定逾時和其他值、以確保最佳效能和成功容錯移轉。虛擬儲存主控台（VSC）設定的值是以內部測試為基礎。

您可以在ESXi主機上設定下列值：

ESXi進階組態

- 《硬體加速器鎖定》
您應該將此值設為1。
- 《支援的BlockDelete》
您應該將此值設為0。

NFS設定

- * Net.TcpipHeapSiz*
如果您使用的是vSphere 6.0或更新版本、則應將此值設為32。
- * Net.TcpipHeapMax*
如果您使用的是vSphere 6.0或更新版本、則應將此值設為1536。
- * NFS.MaxVolumes.*

如果您使用的是vSphere 6.0或更新版本、則應將此值設為256。

- * NFS41.MaxVolumes.*

如果您使用的是vSphere 6.0或更新版本、則應將此值設為256。

- * NFS.MaxQuesteDepet深度*

如果您使用的是vSphere 6.0或更新版本的ESXi主機、則應將此值設為128或更新版本、以避免出現佇列瓶頸。

對於6.0之前的vSphere版本、您應該將此值設為64。

- * NFS.HeartbeatMaxFailures *

您應該將所有NFS組態的此值設為10。

- * NFS.HeartbeatFrequency*

您應該將所有NFS組態的此值設為12。

- * NFS.Heartbeattimeout*

您應該將所有NFS組態的此值設為5。

FC/FCoE設定

- 路徑選擇原則

當使用具有ALUA的FC路徑時、您應該將此值設為「RR」（循環配置資源）。

對於所有其他組態、您應該將此值設為「固定」。

將此值設為「RR」有助於在所有主動/最佳化路徑之間提供負載平衡。「固定」值用於舊版非ALUA組態、有助於防止Proxy I/O

- 磁碟.QFullSampleSize

您應該將所有組態的此值設為32。設定此值有助於避免I/O錯誤。

- 磁碟.QFullTresh

您應該將所有組態的此值設為8。設定此值有助於避免I/O錯誤。

- * Emulex FC HBA超時*

使用預設值。

- * QLogic FC HBA逾時*

使用預設值。

iSCSI設定

- 路徑選擇原則

您應該將所有iSCSI路徑的此值設為「RR」。

將此值設為「RR」有助於在所有主動/最佳化路徑之間提供負載平衡。

- 磁碟.QFullSampleSize

您應該將所有組態的此值設為32。設定此值有助於避免I/O錯誤。

- 磁碟QFullTrresh

您應該將所有組態的此值設為8。設定此值有助於避免I/O錯誤。

設定客體作業系統指令碼

客體作業系統（OS）指令碼的ISO映像會掛載到VMware vSphere伺服器的虛擬儲存主控台。若要使用客體作業系統指令碼來設定虛擬機器的儲存逾時、您必須從vSphere Client掛載指令碼。

作業系統類型	60秒逾時設定	190秒逾時設定
Linux	「https」 ：//<applet_ip>:8143/Vsc/public/可 寫入/linux_gos_timeout-install.iso'	「https」 ：//<applet_ip>:8143/Vsc/public/可 寫入/linux_gos_timeout_190- install.iso'
Windows	「https」 ：//<apply_ip>:8143/Vsc/public/可 寫入/windows_go_timeout.iso'	「https」 ：//<applet_ip>:8143/Vsc/public/可 寫入/windows_go_timeout_190.iso'
Solaris	「https」 ：//<applet_ip>:8143/Vsc/public/可 寫入/solaris Gos_timeout-install.iso'	「https」 ：//<applet_ip>:8143/Vsc/public/可 寫入/solaris Gos_timeout_190- install.iso'

您應該從登錄到管理虛擬機器的vCenter Server的VSC執行個體複本安裝指令碼。如果您的環境包含多個vCenter Server、則應選取包含您要設定其儲存逾時值之虛擬機器的伺服器。

您應該登入虛擬機器、然後執行指令碼來設定儲存逾時值。

設定**Windows**客體作業系統的逾時值

客體作業系統（OS）逾時指令碼可設定Windows客體作業系統的SCSI I/O逾時設定。您可以指定60秒逾時或190秒逾時。您必須重新開機Windows來賓作業系統、設定才會生效。

開始之前

您必須已掛載包含Windows指令碼的ISO映像。

步驟

1. 存取Windows虛擬機器的主控台、並以系統管理員權限登入帳戶。
2. 如果指令碼沒有自動啟動、請開啟CD磁碟機、然後執行「windows_go_timeout.reg」指令碼。

此時會顯示「登錄編輯程式」對話方塊。

3. 按一下「是」繼續。

此時會顯示以下訊息：「D:\windows_Gos_timeout.reg中包含的機碼和值已成功新增至登錄。」

4. 重新啟動Windows來賓作業系統。
5. 卸載ISO映像。

設定Solaris客體作業系統的逾時值

客體作業系統（OS）逾時指令碼可設定Solaris 10的SCSI I/O逾時設定。您可以指定60秒逾時或190秒逾時。

開始之前

您必須已掛載包含Solaris指令碼的ISO映像。

步驟

1. 存取Solaris虛擬機器的主控台、然後以root權限登入帳戶。
2. 執行「Poolaris_GOL_timeout-install.sh」指令碼。

對於Solaris 10、會顯示類似下列內容的訊息：

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

3. 卸載ISO映像。

設定Linux客體作業系統的逾時值

客體作業系統（OS）逾時指令碼可設定Red Hat Enterprise Linux版本4、5、6和7以及SUSE Linux Enterprise Server版本9、10和11的SCSI I/O逾時設定。您可以指定60秒逾時或190秒逾時。每次升級至新版Linux時、您都必須執行指令碼。

開始之前

您必須已掛載包含Linux指令碼的ISO映像。

步驟

1. 存取Linux虛擬機器的主控台、然後以root權限登入帳戶。
2. 執行「Linux_Gos_timeout-install.sh」指令碼。

若為Red Hat Enterprise Linux 4或SUSE Linux Enterprise Server 9、會顯示類似下列訊息：

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

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

對於Red Hat Enterprise Linux 5、Red Hat Enterprise Linux 6和Red Hat Enterprise Linux 7、會顯示類似以下內容的訊息：

```
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!
```

對於SUSE Linux Enterprise Server 10或SUSE Linux Enterprise Server 11、會顯示類似下列訊息：

```
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. 卸載ISO映像。

為虛擬儲存主控台重新產生SSL憑證

SSL憑證會在您安裝（VSC）時產生。為SSL憑證產生的辨別名稱（DN）可能不是用戶端機器識別的一般名稱（CN）。藉由變更Keystore和私密金鑰密碼、您可以重新產生憑證並建立站台專屬的憑證。

關於這項工作

您可以使用維護主控台啟用遠端診斷、並產生站台專屬的憑證。

["NetApp知識庫答案1075654：虛擬儲存主控台7.x：實作CA簽署的憑證"](#)

步驟

1. 登入維護主控台。
2. 輸入「1」存取「應用程式組態」功能表。
3. 在「應用程式組態」功能表中、輸入「3」以停止VSC服務。
4. 輸入「7」重新產生SSL憑證。

在多個vCenter Server環境中登錄VSC的需求

如果您是在單一VMware vSphere HTML5用戶端環境中、使用適用於VMware vSphere的Virtual Storage Console。在管理多個vCenter Server執行個體時、您必須在每個vCenter Server上登錄一個VSC執行個體、以便VSC與vCenter Server之間進行一對一配對。如此一來、您就能從單一vSphere HTML5用戶端、以連結模式和非連結模式、同時管理執行vCenter 6.0或更新版本的所有伺服器。



如果您想要將VSC搭配vCenter Server使用、則必須為每個想要管理的vCenter Server執行個體設定或登錄一個VSC執行個體。每個登錄的VSC執行個體必須為相同版本。

連結模式會在vCenter Server部署期間自動安裝。連結模式使用Microsoft Active Directory應用程式模式（ADAM）、在多個vCenter Server系統之間儲存及同步資料。

若要使用vSphere HTML5用戶端在多個vCenter Server上執行VSC工作、必須具備下列條件：

- 您要管理的VMware庫存中的每個vCenter Server、都必須以獨特的一對一配對方式、在其中註冊單一VSC伺服器。

例如、您可以將VSC伺服器A登錄至vCenter Server A、將VSC伺服器B登錄至vCenter Server B、將VSC伺服器C登錄至vCenter Server C等。

您*無法*將VSC伺服器A登錄至vCenter Server A和vCenter Server B

如果VMware庫存包含未註冊VSC伺服器的vCenter Server、但有一或多個vCenter Server已註冊VSC、然後您可以檢視VSC的執行個體、並針對已登錄VSC的vCenter Server執行VSC作業。

- 您必須擁有登錄至單一登入（SSO）之每個vCenter Server的VSC專屬檢視權限。

您也必須擁有正確的RBAC權限。

當您執行需要指定vCenter Server的工作時、* vCenter Server*下拉式方塊會以英數字元順序顯示可用的vCenter Server。預設vCenter Server永遠是下拉式清單中的第一個伺服器。

如果已知儲存位置（例如、當您使用*資源配置*精靈、且資料存放區位於由特定vCenter Server管理的主機上時）、vCenter Server清單會顯示為唯讀選項。只有在您使用滑鼠右鍵選項選取vSphere Web Client中的項目時、才會發生此情況。

VSC會在您嘗試選取未管理的物件時發出警告。

您可以從VSC摘要頁面、根據特定vCenter Server篩選儲存系統。每個登錄到vCenter Server的VSC執行個體都會顯示摘要頁面。您可以管理與特定VSC執行個體和vCenter Server相關聯的儲存系統、但如果您執行多個VSC執行個體、則應將每個儲存系統的登錄資訊分開。

設定VSC喜好設定檔案

喜好設定檔案包含可控制VMware vSphere作業虛擬儲存主控台的設定。在大多數情況下、您不需要修改這些檔案中的設定。瞭解哪些偏好設定檔（VSC）會很有幫助。

VSC有多個偏好設定檔。這些檔案包含可決定VSC執行各種作業的輸入金鑰和值。以下是VSC使用的部分偏好設定檔：

「/opt/NetApp/vscserver/etc/kamino/kaminoprefs.xml」

「/opt/NetApp/vscserver/etc/Vsc/vscpets.xml」

在某些情況下、您可能必須修改偏好設定檔。例如、如果您使用iSCSI或NFS、而且ESXi主機和儲存系統之間的子網路不同、則必須修改喜好設定檔。如果您未修改喜好設定檔中的設定、則由於VSC無法掛載資料存放區、資料存放區資源配置會失敗。

設定IPV4或IPV6

您可以將喜好設定檔「kaminoprefs.xml」新增一個選項、設定為針對所有新增至VSC的儲存系統、啟用支援IPV4或IPV6。

- 「default.override.option.provision.mount.datastore.address.family」參數已新增至「kaminoprefs.xml」偏好檔案、以設定資料存放區資源配置的偏好資料LIF傳輸協定。

此偏好選項適用於所有新增至VSC的儲存系統。

- 新選項的值包括「ipv4」、「ipv6」和「none」。
- 預設值設為「無」。

價值	說明
無	<ul style="list-style-type: none">• 資源配置會使用與新增儲存設備所用叢集類型或管理LIF相同的IPv6或IPv4位址類型資料LIF。• 如果中沒有相同的IPv6或IPv4位址類型的資料LIF、則資源配置會透過其他類型的資料LIF（如果有）進行。

價值	說明
IPV4	<ul style="list-style-type: none"> 資源配置是使用所選中的IPV4資料LIF進行。 如果沒有IPV4資料LIF、則資源配置會透過IPv6資料LIF進行（如果可在中使用）。
IPv6	<ul style="list-style-type: none"> 資源配置是使用所選中的IPv6資料LIF進行。 如果沒有IPv6資料LIF、則資源配置會透過IPv4資料LIF進行（如果可在中使用）。

在不同的子網路上啟用資料存放區裝載

如果您使用iSCSI或NFS、且ESXi主機與儲存系統之間的子網路不同、則必須修改VMware vSphere喜好設定檔案的虛擬儲存主控台。如果您未修改喜好設定檔、則資料存放區資源配置會失敗、因為（VSC）無法掛載資料存放區。

關於這項工作

當資料存放區資源配置失敗時、VSC會記錄下列錯誤訊息：

「無法繼續。當控制器上的核心IP位址與位址相互參照時、找不到IP位址

「找不到與這些主機的NFS掛載磁碟區相符的網路。」

步驟

1. 登入vCenter Server執行個體。
2. 使用統一化應用裝置虛擬機器啟動維護主控台。

"存取VSC、VASA Provider和SRA虛擬應用裝置的維護主控台選項"

3. 輸入「4」以存取*支援與診斷*選項。
4. 輸入「2」以存取*存取診斷Shell*選項。
5. 輸入「vi /opt/NetApp/vscserver/etc/kamino/kaminoprefs.xml」以更新「kaminoprefs.xml」檔案。
6. 更新「kaminoprefs.xml」檔案。

如果您使用...	執行此動作...
iSCSI	將輸入金鑰「efault.allow.iscsi.mount.networks`從all」的值變更為ESXi主機網路的值。
NFS	將輸入金鑰「efault.allow.nfs.mount.networks`從all」的值變更為ESXi主機網路的值。

喜好設定檔包含這些項目金鑰的範例值。



「all」值並不代表所有網路。「all」值可讓主機與儲存系統之間的所有相符網路用於掛載資料存放區。指定主機網路時、您只能在指定的子網路上啟用掛載。

7. 儲存並關閉「kaminoprefs.xml」檔案。

存取VSC、VASA Provider和SRA虛擬應用裝置的維護主控台選項

您可以使用虛擬儲存主控台（VSC）、VASA Provider和儲存複寫介面卡（SRA）的虛擬應用程式維護主控台、來管理應用程式、系統和網路組態。您可以變更系統管理員密碼和維護密碼。您也可以產生支援服務包、設定不同的記錄層級、檢視及管理TLS組態、以及啟動遠端診斷。


開始之前

您必須在部署VSC、VASA Provider和SRA的虛擬應用裝置之後、安裝VMware工具。

關於這項工作

- 您必須使用「maint」做為部署期間設定的使用者名稱和密碼、才能登入VSC、VASA Provider和SRA虛擬應用裝置的維護主控台。
- 啟用遠端診斷時、您必須為「diag」使用者設定密碼。

步驟

1. 存取已部署虛擬應用裝置的* Summary（摘要）*索引標籤。
2. 按一下  以啟動維護主控台。

您可以存取下列維護主控台選項：

- 應用程式組態

提供下列選項：

- 顯示伺服器狀態摘要
- 啟動虛擬儲存主控台服務
- 停止虛擬儲存主控台服務
- 啟動VASA Provider和SRA服務
- 停止VASA Provider和SRA服務
- 變更「系統管理員」使用者密碼
- 重新產生憑證
- 硬重設金鑰儲存區和憑證
- 硬重設資料庫
- 變更虛擬儲存主控台服務的記錄層級
- 變更VASA Provider和SRA服務的記錄層級

- 顯示TLS組態
- 啟用TLS傳輸協定
- 停用TLS傳輸協定
- 系統組態

提供下列選項：

- 重新開機虛擬機器
- 關閉虛擬機器
- 變更「maint」使用者密碼
- 變更時區
- 變更NTP伺服器

您可以為NTP伺服器提供IPv6位址。

- 啟用/停用SSH存取
- 增加監獄磁碟大小（/監獄）
- 升級
- 安裝VMware Tools

- 網路組態

提供下列選項：

- 顯示IP位址設定
- 變更IP位址設定

您可以使用此選項、將部署後的IP位址變更為IPv6。

- 顯示網域名稱搜尋設定
- 變更網域名稱搜尋設定
- 顯示靜態路由
- 變更靜態路由

您可以使用此選項來新增IPv6路由。

- 提交變更
- Ping主機

您可以使用此選項ping IPv6主機。

- 還原預設設定

- 支援與診斷

提供下列選項：

- 產生支援服務組合
- 存取診斷Shell
- 啟用遠端診斷存取

相關資訊

[VSC和VASA Provider記錄檔](#)

變更系統管理員密碼

您可以使用維護主控台變更VSC、VASA Provider及SRA部署後的虛擬應用裝置管理員密碼。

步驟

1. 從vCenter Server開啟VSC、VASA Provider及SRA的主控台至虛擬應用裝置。
2. 以維護使用者身分登入。
3. 在維護控制檯中輸入「1」以選擇*應用程式組態*。
4. 輸入「6」以選擇*變更「系統管理員」使用者密碼*。
5. 輸入至少八個字元、最多63個字元的密碼。
6. 在確認對話方塊中輸入「y」。

為VSC、VASA Provider及SRA設定虛擬應用裝置的高可用度

適用於虛擬儲存主控台（VSC）、VASA Provider及儲存複寫介面卡（SRA）的虛擬應用裝置支援（HA）組態、可在故障期間提供VSC、VASA Provider及SRA不中斷的功能。

VSC、VASA Provider和SRA的虛擬應用裝置仰賴VMware vSphere（HA）功能和vSphere容錯（FT）功能來提供。（HA）解決方案可讓您從下列原因造成的停機中快速恢復：

- 主機故障
- 網路故障
- 虛擬機器故障（客體作業系統故障）
- 應用程式（VSC、VASA Provider和SRA）當機

虛擬應用裝置不需要額外的組態即可提供。只有vCenter Server和ESXi主機必須根據需求、設定VMware vSphere HA功能或vSphere FT功能。HA和FT都需要叢集式主機搭配共用儲存設備。FT有額外的要求和限制。

除了VMware vSphere HA解決方案和vSphere FT解決方案之外、虛擬應用裝置也有助於維持VSC、VASA Provider和SRA服務隨時運作。虛擬應用裝置監控程序會定期監控這三項服務、並在偵測到任何故障時自動重新啟動。這有助於預防應用程式故障。



VSC、VASA Provider及SRA的虛擬應用裝置不支援vCenter HA。

VMware vSphere HA

您可以設定vSphere環境、讓虛擬儲存主控台（VSC）、VASA Provider及儲存複寫介面卡（SRA）的虛擬應用裝置部署於（HA）。VMware HA功能可提供容錯移轉保護、避免虛擬環境中的硬體故障和作業系統故障。

VMware HA功能可監控虛擬機器、以偵測作業系統故障和硬體故障。偵測到故障時、VMware HA功能會在資源池中的其他實體伺服器上重新啟動虛擬機器。偵測到伺服器故障時、不需要手動介入。

設定VMware HA的程序取決於vCenter Server的版本。例如、您可以使用下列參考連結並選取所需的vCenter Server版本、以檢視設定VMware HA的步驟。

["VMware vSphere文件：建立及使用vSphere HA叢集"](#)

VMware vSphere容錯能力

VMware vSphere容錯（FT）功能提供更高層級的（HA）、可讓您保護虛擬機器、而不會遺失任何資料或連線。您必須從vCenter Server啟用或停用VSC、VASA Provider和SRA虛擬應用裝置的vSphere FT。

確保vSphere授權支援FT、並提供環境中虛擬應用裝置所需的vCPU數量（至少2個vCPU；大型環境需4個vCPU）。

vSphere FT可讓虛擬機器在伺服器故障期間持續運作。在虛擬機器上啟用vSphere FT時、會自動在其他由Distributed Resource Scheduler（DRS）選取的主機（次要虛擬機器）上建立主要虛擬機器的複本。如果未啟用DRS、則會從可用的主機中選取目標主機。vSphere FT會以鎖步模式操作主要虛擬機器和次要虛擬機器、每個虛擬機器都會將主要虛擬機器的執行狀態鏡射至次要虛擬機器。

當發生硬體故障導致主要虛擬機器故障時、次要虛擬機器會立即接收主要虛擬機器停止的位置。次要虛擬機器會繼續執行、不會遺失任何網路連線、交易或資料。

您的系統必須符合CPU需求、虛擬機器限制需求、以及設定vCenter Server執行個體vSphere FT的授權需求。

設定HA的程序取決於vCenter Server的版本。例如、您可以使用下列參考連結並選取所需的vCenter Server版本、以檢視設定HA的步驟。

["VMware vSphere文件：容錯要求、限制及授權"](#)

VSC、VASA Provider和SRA虛擬應用裝置支援的支援範本組態MetroCluster

適用於虛擬儲存主控台（VSC）、VASA供應商和儲存複寫介面卡（SRA）的虛擬應用裝置、可支援使用MetroCluster VMware IP和FC組態來ONTAP 進行VMware View的環境。大部分支援都是自動的。不過MetroCluster、當您搭配VSC和VASA Provider使用時、可能會注意到一些差異。

包含各種組態和VSC MetroCluster

您必須確保VSC在主要站台和次要站台上探索儲存系統控制器。通常、VSC會自動探索儲存控制器。如果您使

用叢集管理LIF、則最好驗證VSC是否已在兩個站台上探索叢集。否則、您可以手動將儲存控制器新增至VSC。您也可以修改VSC用來連線至儲存控制器的使用者名稱和密碼配對。

當發生切換時、次要站台上的會接管。這些名稱加上「-MC」字尾。如果在執行資源配置等作業時發生切換作業、則資料存放區所在的名稱會變更為包含「-MC」字尾。當發生切換時、會捨棄此字尾、而主要站台上的會恢復控制權。



如果您在MetroCluster VSC中新增了直接搭配使用的組態、則切換後、SVM名稱（加上「-MC」字尾）的變更不會反映出來。所有其他切換作業仍會正常執行。

當發生切換或切換時、VSC可能需要幾分鐘時間來自動偵測及探索叢集。如果在執行VSC作業（例如資源存放區資源配置）時發生此情況、可能會發生延遲。

提供者**MetroCluster**

VASA Provider會自動支援使用MetroCluster 不完整組態的環境。在VASA Provider環境中、切換是透明的。您無法直接新增至VASA Provider。



VASA Provider在切換後、不會在次要站台的名稱後面加上「-MC」字尾。

內部組態與**SRA MetroCluster**

SRA不支援MetroCluster 不支援的不支援的組態。

版權資訊

Copyright © 2024 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。