



安裝並設定 **SnapCenter** 伺服器

SnapCenter software

NetApp
February 20, 2026

目錄

安裝並設定 SnapCenter 伺服器	1
準備安裝SnapCenter 完此伺服器	1
安裝 SnapCenter 伺服器的需求	1
註冊以存取 SnapCenter 軟體	6
多因素驗證 (MFA)	7
安裝SnapCenter 此伺服器	16
在 Windows 主機上安裝 SnapCenter 伺服器	16
在 Linux 主機上安裝 SnapCenter 伺服器	20
註冊 SnapCenter	24
使用RBAC授權登入SnapCenter 到功能表	24
配置 SnapCenter 伺服器	27
新增並配置儲存系統	27
新增SnapCenter 以控制器為基礎的功能	47
設定高可用度	52
設定角色型存取控制 (RBAC)	56
設定稽核日誌設定	82
使用SnapCenter 伺服器設定安全的MySQL連線	83
設定憑證型驗證	89
啟用憑證型驗證	89
從 SnapCenter 伺服器匯出憑證授權單位 (CA) 憑證	89
將 CA 憑證匯入 Windows 外掛主機	90
將 CA 憑證匯入 UNIX 外掛主機	91
匯出SnapCenter 功能證書	92
設定 Windows 主機的 CA 憑證	93
產生CA認證CSR檔案	93
匯入CA憑證	93
取得CA憑證指紋	94
使用Windows主機外掛程式服務設定CA憑證	94
使用SnapCenter 站台設定CA憑證	95
啟用CA認證SnapCenter 以供使用	96
設定 Linux 主機的 CA 憑證	96
設定 Nginx 憑證	96
設定稽核記錄憑證	97
配置SnapCenter證書	97
在 Windows 主機上設定並啟用雙向 SSL 通訊	97
在 Windows 主機上設定雙向 SSL 通訊	98
在 Windows 主機上啟用雙向 SSL 通訊	100
在 Linux 主機上設定並啟用雙向 SSL 通訊	101
在 Linux 主機上設定雙向 SSL 通訊	101

在 Linux 主機上啟用 SSL 通訊	103
設定Active Directory、LDAP和LDAPS	103
登錄不受信任的Active Directory網域	103
設定「IIS應用程式集區」以啟用Active Directory讀取權限	105
設定LDAPS的CA用戶端憑證	105

安裝並設定 SnapCenter 伺服器

準備安裝SnapCenter 完此伺服器

安裝 SnapCenter 伺服器的需求

在 Windows 或 Linux 主機上安裝 SnapCenter 伺服器之前，您應該先檢閱並確定符合您環境的所有需求。

Windows 主機的網域和工作群組需求

SnapCenter 伺服器可以安裝在網域或工作群組中的 Windows 主機上。

擁有管理 Privileges 的使用者可以安裝 SnapCenter 伺服器。

- Active Directory 網域：您必須使用具有本機系統管理員權限的網域使用者。網域使用者必須是Windows主機上本機系統管理員群組的成員。
- 工作群組：您必須使用具有本機系統管理員權限的本機帳戶。

雖然支援網域信任、多網域樹系和跨網域信任、但不支援跨樹系網域。Microsoft的Active Directory網域及信任相關文件包含更多資訊。



安裝SnapCenter 完支援服務器後、您不應變更SnapCenter 支援該主機的網域。如果您從SnapCenter 安裝了支援服務器的網域中移除此伺服器主機SnapCenter、然後嘗試解除安裝SnapCenter 支援服務器、則解除安裝作業會失敗。

空間與規模需求

您應該熟悉空間和規模需求。

項目	Windows 主機需求	Linux 主機需求
作業系統	Microsoft Windows 僅支援英文、德文、日文及簡體中文版的作業系統。 有關受支援版本的最新信息，請參閱 " NetApp 互通性對照表工具 "。	<ul style="list-style-type: none">• Red Hat Enterprise Linux (RHEL) 8 和 9• SUSE Linux Enterprise Server (SLES) 15. 有關受支援版本的最新信息，請參閱 " NetApp 互通性對照表工具 "。
最小CPU數	4核心	4核心

項目	Windows 主機需求	Linux 主機需求
最低RAM	8 GB  MySQL伺服器緩衝資源池使用總RAM的20%。	8 GB
不需佔用SnapCenter 太多硬碟空間、即可容納整個伺服器軟體和記錄	7 GB  如果SnapCenter 您在SnapCenter 安裝了S什麼 伺服器的同一個磁碟機上有這個版本的資訊庫、建議您使用15 GB的容量。	15 GB
不需SnapCenter 佔用太多硬碟空間	8 GB  附註：如果SnapCenter 您在SnapCenter 安裝了該系統資訊庫的同一個磁碟機中安裝了該伺服器、則建議您使用15 GB的容量。	不適用
必要的軟體套件	<ul style="list-style-type: none"> • ASP.NET Core Runtime 8.0.12 (以及所有後續 8.0.x 修補程式) 代管產品組合 • PowerShell 7.4.2 或更新版本 <p>如需 .NET 特定疑難排解資訊、請參閱 "對於沒有網際網路連線的舊版系統、SnapCenter 升級或安裝失敗"。</p>	<ul style="list-style-type: none"> • NET Framework 8.0.12 (以及所有後續的 8.0.x 修補程式) • PowerShell 7.4.2 或更新版本 • Nginx 是可做為反向 Proxy 的 Web 伺服器 • Pam-devel <p>PAM (可插拔驗證模組) 是一種系統安全工具、可讓系統管理員設定驗證原則、而無需重新編譯執行驗證的程式。</p>



ASP.NET 核心需要 IIS_IUSRS 來存取 Windows 上 SnapCenter Server 中的暫存檔系統。

SAN主機需求

SnapCenter 不包含主機公用程式或 DSM。如果 SnapCenter 主機是 SAN (FC/iSCSI) 環境的一部分，您可能需要在 SnapCenter 伺服器主機上安裝及設定其他軟體。

- 主機公用程式：主機公用程式支援 FC 和 iSCSI，可讓您在 Windows 伺服器上使用 MPIO。"深入瞭解"。
- Microsoft DSM for Windows MPIO：此軟體可搭配 Windows MPIO 驅動程式使用，以管理 NetApp 和 Windows 主機電腦之間的多個路徑。高可用度組態需要 DSM。



如果您使用 ONTAP 的是功能不實的 DSM、則應移轉至 Microsoft DSM。如需詳細資訊、請參閱 "如何從 ONTAP 功能需求 DSM 移轉至 Microsoft DSM"。

瀏覽器需求

SnapCenter 軟體支援 Chrome 125 及更新版本，以及 Microsoft Edge 110.0.1587.17 及更新版本。

連接埠需求

SnapCenter 軟體需要不同的連接埠，才能在不同元件之間進行通訊。

- 應用程式無法共用連接埠。
- 對於可自訂的連接埠、如果您不想使用預設連接埠、可以在安裝期間選取自訂連接埠。
- 對於固定連接埠、您應該接受預設的連接埠號碼。
- 防火牆
 - 防火牆、Proxy 或其他網路裝置不應干擾連線。
 - 如果您在安裝 SnapCenter 時指定自訂連接埠、則應在外掛主機上新增防火牆規則、以供 SnapCenter 該連接埠用於「支援程式載入器」。

下表列出不同的連接埠及其預設值。

連接埠名稱	連接埠編號	傳輸協定	方向	說明
SnapCenter Web 連接埠	8146	HTTPS	雙向	此連接埠用於 SnapCenter 用戶端（SnapCenter 使用者）與 SnapCenter 伺服器之間的通訊，也用於從外掛主機與 SnapCenter 伺服器之間的通訊。 您可以自訂連接埠號碼。

連接埠名稱	連接埠編號	傳輸協定	方向	說明
WSSMCore通訊連接埠SnapCenter	8145	HTTPS	雙向	此連接埠可用於SnapCenter在Sfor the Sfor Server和SnapCenter安裝了該插件的主機之間進行通訊。 您可以自訂連接埠號碼。
排程器服務連接埠	8154	HTTPS		此連接埠用於SnapCenter集中化伺服器主機內所有受管理外掛程式的SnapCenter排程器工作流程。 您可以自訂連接埠號碼。
RabbitMQ 連接埠	5672	TCP		這是 RabbitMQ 接聽的預設連接埠、用於排程器服務與SnapCenter之間的發行者訂購者模式通訊。
MySQL連接埠	3306	HTTPS		連接埠用於與SnapCenter儲存庫資料庫通訊。您可以建立從SnapCenter伺服器到MySQL伺服器的安全連線。" 深入瞭解 "
Windows外掛程式主機	135 、 445	TCP		此連接埠用於SnapCenter伺服器與正在安裝外掛程式的主機之間的通訊。Microsoft指定的其他動態連接埠範圍也應該是開放的。
Linux或AIX外掛程式主機	22	SSH	單向	此連接埠用於SnapCenter伺服器與主機之間的通訊，從伺服器啟動至用戶端主機。

連接埠名稱	連接埠編號	傳輸協定	方向	說明
適用於 Windows , Linux 或 AIX 的 SnapCenter 外掛程式套件	8145	HTTPS	雙向	此連接埠用於 SMCORE 與安裝外掛程式套件的主機之間的通訊。可自訂。 您可以自訂連接埠號碼。
Oracle 資料庫的支援外掛程式 SnapCenter	27216			Oracle 的外掛程式會使用預設的 JDBC 連接埠來連線至 Oracle 資料庫。
SnapCenter Plug-in for Exchange 資料庫	909			預設的 NET 。 Windows 外掛程式使用 TCP 連接埠來連線至 Exchange VSS 回撥。
NetApp 支援的 SnapCenter 外掛程式	9090	HTTPS		這是僅在插件主機上使用的內部連接埠；不需要防火牆例外。 SnapCenter 伺服器和插件之間的通訊透過連接埠 8145 進行。
叢集或 SVM 通訊連接埠 ONTAP	<ul style="list-style-type: none"> • 443 (HTTPS) • 80 (HTTP) 	<ul style="list-style-type: none"> • HTTPS • HTTP 	雙向	此連接埠由 SAL (Storage Abstraction Layer 、 Storage Abstraction Layer) 使用、用於執行 SnapCenter 支援服務器和 SVM 的主機之間的通訊。此連接埠目前也用於 SnapCenter Windows 外掛程式主機上的 SAL、用於 SnapCenter 在支援該外掛程式的主機和 SVM 之間進行通訊。

連接埠名稱	連接埠編號	傳輸協定	方向	說明
SAP HANA資料庫適用的插件SnapCenter	<ul style="list-style-type: none"> 3instance_number13 3instance_number15 	<ul style="list-style-type: none"> HTTPS HTTP 	雙向	<p>對於多租戶資料庫容器（MDC）單一租戶、連接埠編號以13結尾；對於非MDC、連接埠編號以15結尾。</p> <p>您可以自訂連接埠號碼。</p>
適用於 PostgreSQL 的 SnapCenter 外掛程式	5432			<p>此連接埠是預設的 PostgreSQL 連接埠，可讓 PostgreSQL 外掛程式與 PostgreSQL 叢集進行通訊。</p> <p>您可以自訂連接埠號碼。</p>

註冊以存取 SnapCenter 軟體

如果您是 Amazon FSX for NetApp ONTAP 或 Azure NetApp Files 的新手，而且沒有現有的 NetApp 帳戶，則應註冊以存取 SnapCenter 軟體。

開始之前

- 您應該可以存取公司電子郵件 ID 。
- 如果您使用的是 Azure NetApp Files 、則應擁有 Azure 訂閱 ID 。
- 如果您使用的是 Amazon FSX for NetApp ONTAP 、則您應該擁有適用於 ONTAP 檔案系統的 FSX 檔案系統 ID 。

關於這項工作

您的註冊必須經過資訊驗證，並可能需要一天的時間，才能確認新的 NetApp 支援網站（NSS）帳戶，並將其升級為 * 來賓 * 存取權限的 * 完整 * 存取權限。

步驟

1. 按一下 <https://mysupport.netapp.com/site/user/registration> 以進行註冊。
2. 輸入您的公司電子郵件 ID，完成 captcha，接受 NetApp 的隱私權政策，然後按一下 * 提交 *。
3. 輸入傳送至您電子郵件 ID 的 OTP、以驗證登錄、然後按一下 * 繼續 *。
4. 在登錄完成頁面上、輸入下列詳細資料以完成登錄。
 - a. 選擇 * NetApp 客戶 / 終端使用者 *。
 - b. 在序號欄位中，如果您使用的是 Azure NetApp Files，請輸入 Azure 訂閱 ID；如果您使用的是 Amazon FSX for NetApp ONTAP，請輸入檔案系統 ID。



如果您在登錄期間遇到任何問題、或是為了瞭解狀態、您可以在提出問題單 <https://mysupport.netapp.com/site/help>。

多因素驗證 (MFA)

管理多因素驗證 (MFA)

您可以在 Active Directory Federation Service (AD FS) 伺服器 and SnapCenter 伺服器中管理多因素驗證 (MFA) 功能。

啟用多因素驗證 (MFA)

您可以使用 PowerShell 命令為 SnapCenter 伺服器啟用 MFA 功能。

關於這項工作

- 在相同的AD FS中設定其他應用程式時、支援SSO型登入。SnapCenter在某些AD FS組態中、SnapCenter由於安全原因、可能需要使用者驗證、視AD FS工作階段持續性而定。
- 有關可與 Cmdlet 搭配使用的參數及其描述的資訊，可透過執行取得 `Get-Help command_name`。或者、您也可以參閱 "[《軟件指令程式參考指南》SnapCenter](#)"。

開始之前

- Windows Active Directory Federation Service (AD FS) 應在各自的網域中啟動並執行。
- 您應該擁有 AD FS 支援的多因素驗證服務、例如 Azure MFA、Cisco Duo 等。
- 無論時區為何、均應使用相同的資訊區和AD FS伺服器時間戳記。SnapCenter
- 取得SnapCenter 並設定驗證伺服器的授權CA憑證。

CA憑證為必填、原因如下：

- 確保 ADFS-F5 通訊不會中斷、因為自我簽署的憑證在節點層級是唯一的。
- 確保在獨立式或高可用度組態的升級、修復或災難恢復 (DR) 期間、不會重新建立自我簽署的憑證、因此可避免重新設定MFA。
- 確保IP FQDN解析度。

如需CA憑證的相關資訊、請參閱 "[產生CA認證CSR檔案](#)"。

步驟

1. 連線至Active Directory Federation Services (AD FS) 主機。
2. 從下載AD FS聯盟中繼資料檔案 "<https://<host>fqfq/> 聯邦中繼資料 /2007/06/Federation中繼資料 .xml"。
3. 將下載的檔案複製到SnapCenter 支援MFA功能的伺服器。
4. 透過PowerShell以「管理員」使用者身分登入SnapCenter 到「伺服器」SnapCenter。
5. 使用PowerShell工作階段SnapCenter、使用 `_New-SmMultifactorAuthenticationMetadata -path_ Cmdlet`來產生FismFA中繼資料檔案。

path參數指定將MFA中繼資料檔案儲存到SnapCenter Sof the Server主機的路徑。

6. 將產生的檔案複製到AD FS主機、以設定SnapCenter 將SURE做為用戶端實體。
7. 使用為 SnapCenter 伺服器啟用 MFA Set-SmMultiFactorAuthentication Cmdlet。
8. (選用) 使用檢查 MFA 組態狀態和設定 Get-SmMultiFactorAuthentication Cmdlet。
9. 前往Microsoft管理主控台 (MMC) 並執行下列步驟：
 - a. 按一下*檔案*>*新增/移除Snapin*。
 - b. 在「新增或移除嵌入式管理單元」視窗中、選取「憑證」、然後按一下「新增」。
 - c. 在「憑證」嵌入式管理單元視窗中、選取「電腦帳戶」選項、然後按一下「完成」。
 - d. 按一下*主控台根目錄*>*憑證-本機電腦*>*個人*>*憑證*。
 - e. 在繫結SnapCenter 至SUn供 參考的CA憑證上按一下滑鼠右鍵、然後選取*所有工作*>*管理私密金鑰*。
 - f. 在權限精靈上執行下列步驟：
 - i. 按一下「*新增*」。
 - ii. 按一下*位置*、然後選取相關主機 (階層架構頂端)。
 - iii. 在*位置*快顯視窗中按一下*確定*。
 - iv. 在物件名稱欄位中、輸入「IIS_IUSRS」、然後按一下*檢查名稱*、再按一下*確定*。

如果檢查成功、請按一下「確定」。

10. 在AD FS主機中、開啟AD FS管理精靈、然後執行下列步驟：
 - a. 右鍵點選*信賴廠商信任*>*新增信賴廠商信任*>*開始*。
 - b. 選取第二個選項、然後瀏覽SnapCenter 「Some MFA中繼資料」 檔案、然後按一下「* Next* (下一步)」。
 - c. 指定顯示名稱、然後按一下*「下一步*」。
 - d. 視需要選擇存取控制原則、然後按一下*下一步*。
 - e. 在下一個索引標籤中選取預設值。
 - f. 單擊*完成*。

目前以依賴方的形式呈現提供的顯示名稱。SnapCenter

11. 選取名稱並執行下列步驟：
 - a. 按一下*編輯請款發放政策*。
 - b. 單擊* Add Rule (添加規則) ，然後單擊 Next* (下一步) 。
 - c. 指定宣告規則的名稱。
 - d. 選擇* Active Directory *作為屬性儲存區。
 - e. 選取「使用者-主要名稱」屬性、並選取傳出的報銷類型為*名稱- ID*。
 - f. 單擊*完成*。

12. 在ADFS伺服器上執行下列PowerShell命令。

```
Set-AdfsRelyingPartyTrust -TargetName '<Display name of relying party >'  
-SigningCertificateRevocationCheck None
```

```
Set-AdfsRelyingPartyTrust -TargetName '<Display name of relying party >'
-EncryptionCertificateRevocationCheck None
```

13. 請執行下列步驟、確認中繼資料已成功匯入。
 - a. 在依賴方信任上按一下滑鼠右鍵、然後選取*內容*。
 - b. 確認已填入端點、識別項和簽名欄位。
14. 關閉所有瀏覽器索引標籤、然後重新開啟瀏覽器、以清除現有或作用中的工作階段 Cookie、然後再次登入。

也可使用REST API來啟用「支援MFA」功能。SnapCenter

如需疑難排解資訊，請參閱 ["在多個索引標籤中同時嘗試登入會顯示 MFA 錯誤"](#)。

更新AD FS MFA中繼資料

只要AD FS伺服器有任何修改、例如升級、CA憑證續約、DR等、您就應該更新SnapCenter 位於支援區的AD FS MFA中繼資料。

步驟

1. 從下載AD FS聯盟中繼資料檔案 "<https://<host Fq>>/資料中繼資料/2007/06/FederationMetadata。XML>]
2. 將下載的檔案複製SnapCenter 到「伺服器」以更新MFA組態。
3. 執行下列Cmdlet來更新SnapCenter Sf1中的AD FS中繼資料：

```
Set-SmMultiFactorAuthentication -Path <location of ADFS MFA metadata xml file>
```

4. 關閉所有瀏覽器索引標籤、然後重新開啟瀏覽器、以清除現有或作用中的工作階段 Cookie、然後再次登入。

更新SnapCenter 功能不支援MFA中繼資料

每當有任何修改ADFS伺服器（例如修復、CA憑證續約、DR等）時、您就應該更新SnapCenter AD FS中的功能完善的MFA中繼資料。

步驟

1. 在AD FS主機中、開啟AD FS管理精靈、然後執行下列步驟：
 - a. 選擇 * 信賴方信任 * 。
 - b. 在為 SnapCenter 建立的信賴方信任上按一下滑鼠右鍵，然後選取 * 刪除 * 。

隨即顯示使用者定義的信賴關係人信任名稱。

- c. 啟用多因素驗證（MFA）。

請參閱 ["啟用多因素驗證"](#)。

2. 關閉所有瀏覽器索引標籤、然後重新開啟瀏覽器、以清除現有或作用中的工作階段 Cookie、然後再次登入。

停用多因素驗證 (MFA)

步驟

1. 停用 MFA、並清除使用啟用 MFA 時所建立的組態檔案 `Set-SmMultiFactorAuthentication Cmdlet`。
2. 關閉所有瀏覽器索引標籤、然後重新開啟瀏覽器、以清除現有或作用中的工作階段 Cookie、然後再次登入。

使用 REST API、PowerShell 和 sccli 來管理多因素驗證 (MFA)

瀏覽器、REST API、PowerShell 和 sccli 支援 MFA 登入。MFA 可透過 AD FS 身分識別管理員提供支援。您可以從 GUI、REST API、PowerShell 和 sccli 啟用 MFA、停用 MFA、以及設定 MFA。

將 AD FS 設定為 OAUTH/OIDC

- 使用 Windows GUI 精靈 * 設定 AD FS

1. 瀏覽至 * 伺服器管理員儀表板 * > * 工具 * > * ADFS 管理 *。
2. 瀏覽至 **ADFS** > * 應用程式群組 *。
 - a. 在 * 應用程式群組 * 上按一下滑鼠右鍵。
 - b. 選取 * 新增應用程式群組 *、然後輸入 * 應用程式名稱 *。
 - c. 選取 * 伺服器應用程式 *。
 - d. 單擊 * 下一步 *。

3. 複本 * 用戶端識別碼 *。

這是用戶端 ID。...在重新導向 URL 中新增回撥 URL (SnapCenter 伺服器 URL)。...單擊 * 下一步 *。

4. 選取 * 產生共用密碼 *。

複製機密值。這是用戶端的秘密。...單擊 * 下一步 *。

5. 在 * 摘要 * 頁面上、按一下 * 下一步 *。

- a. 在 * 完整 * 頁面上、按一下 * 關閉 *。

6. 右鍵單擊新添加的 * 應用程序組 *，然後選擇 * 屬性 *。

7. 從應用程式內容中選取 * 新增應用程式 *。

8. 按一下 * 新增應用程式 *。

選取「網路 API」、然後按一下「 * 下一步 * 」。

9. 在「設定 Web API」頁面上、在「識別碼」區段中、輸入上一步所建立的 SnapCenter 伺服器 URL 和用戶端識別碼。

- a. 按一下「 * 新增 * 」。
- b. 單擊 * 下一步 *。

10. 在 * 選擇存取控制原則 * 頁面上、根據您的需求選擇控制原則（例如、允許所有人並要求 MFA）、然後按一下 * 下一步 *。
11. 在「 * 設定應用程式權限 * 」頁面上、依預設會選取 OpenID 作為範圍、按一下 * 下一步 *。
12. 在 * 摘要 * 頁面上、按一下 * 下一步 *。
在 * 完整 * 頁面上、按一下 * 關閉 *。
13. 在 * 範例應用程式內容 * 頁面上、按一下 * 確定 *。
14. 由授權伺服器（AD FS）發出的 JWT 權杖、並打算由資源使用。
此權杖的「aud」或「Audience」宣告必須符合資源或 Web API 的識別碼。
15. 編輯選取的 WebAPI、並檢查回撥 URL（SnapCenter 伺服器 URL）和用戶端識別碼是否正確新增。
設定 OpenID Connect 以提供宣告的使用者名稱。
16. 開啟位於伺服器管理員右上角 * 工具 * 功能表下的 * AD FS 管理 * 工具。
 - a. 從左側側欄中選擇 * 應用程式群組 * 資料夾。
 - b. 選取 Web API、然後按一下 * 編輯 *。
 - c. 前往「發行轉換規則」標籤
17. 按一下 * 新增規則 *。
 - a. 在請款規則範本下拉式清單中、選取 * 將 LDAP 屬性傳送為請款 *。
 - b. 單擊 * 下一步 *。
18. 輸入 * 請款規則 * 名稱。
 - a. 在屬性儲存區下拉式清單中選取 * Active Directory *。
 - b. 在 **LDAP Attribute** 下拉列表中選擇 **User-Princie-Name**，在 **outGo Claim Type** 下拉列表中選擇 **UPN**。
 - c. 單擊 * 完成 *。

使用 PowerShell 命令建立應用程式群組

您可以使用 PowerShell 命令建立應用程式群組、Web API、並新增範圍和宣告。這些命令以自動指令碼格式提供。如需詳細資訊、請參閱 [<link to KB article>](#)。

1. 使用下列組合在 AD FS 中建立新的應用程式群組。

```
New-AdfsApplicationGroup -Name $ClientRoleIdentifier
-ApplicationGroupIdentifier $ClientRoleIdentifier
```

ClientRoleIdentifier 應用程式群組的名稱

redirectURL 授權後重新導向的有效 URL

2. 建立 AD FS 伺服器應用程式並產生用戶端機密。

```
Add-AdfsServerApplication -Name "$ClientRoleIdentifier - Server app"
```

```
-ApplicationGroupIdentifier $ClientRoleIdentifier -RedirectUri $redirectURL  
-Identifier $identifier -GenerateClientSecret
```

3. 建立 ADFS Web API 應用程式、並設定其應使用的原則名稱。

```
$identifier = (New-Guid).Guid
```

```
Add-AdfsWebApiApplication -ApplicationGroupIdentifier $ClientRoleIdentifier  
-Name "App Web API"
```

```
-Identifier $identifier -AccessControlPolicyName "Permit everyone"
```

4. 從下列命令的輸出中取得用戶端 ID 和用戶端機密、因為只會顯示一次。

```
"client_id = $identifier"
```

```
"client_secret: "$($ADFSApp.ClientSecret)
```

5. 將 allats 補助 和 OpenID 權限授予 AD FS 應用程式。

```
Grant-AdfsApplicationPermission -ClientRoleIdentifier $identifier  
-ServerRoleIdentifier $identifier -ScopeNames @('openid')
```

```
$transformrule = @"
```

```
@RuleTemplate = "LdapClaims"
```

```
@RuleName = "AD User properties and Groups"
```

```
c:[Type ==
```

```
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",  
Issuer ==
```

```
"AD AUTHORITY"]
```

```
⇒ issue(store = "Active Directory", types =  
("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"), query =  
";userPrincipalName;{0}", param = c.Value);
```

```
"@"
```

6. 寫出轉換規則檔案。

```
$transformrule | Out-File -FilePath .\issueancetransformrules.tmp -force  
-Encoding ascii $relativePath = Get-Item .\issueancetransformrules.tmp
```

7. 命名 Web API 應用程式、並使用外部檔案定義其「發行轉換規則」。

```
Set-AdfsWebApiApplication -Name "$ClientRoleIdentifier - Web API"  
-TargetIdentifier
```

```
$identifier -Identifier $identifier,$redirectURL -IssuanceTransformRulesFile
```

\$relativePath

更新存取權杖到期時間

您可以使用 PowerShell 命令更新存取權杖到期時間。

關於此工作

- 存取權杖只能用於使用者、用戶端和資源的特定組合。存取權杖無法撤銷、且在過期前有效。
- 依預設、存取權杖的到期時間為 60 分鐘。這段最短的到期時間已足夠且已調整。您必須提供足夠的價值、以避免任何持續進行的業務關鍵工作。

步驟

若要更新應用程式群組 WebApi 的存取權杖到期時間、請在 AD FS 伺服器中使用下列命令。

```
+ Set-AdfsWebApiApplication -TokenLifetime 3600 -TargetName "<Web API>"
```

從 AD FS 取得承載權杖

您應該在任何 REST 用戶端（例如 Postman）中填入下列參數、並提示您填寫使用者認證。此外、您應該輸入第二因素驗證（您擁有的東西和您的東西）來取得承載權杖。

+ 承載權杖的有效性可從 AD FS 伺服器根據應用程式進行設定、預設的有效期為 60 分鐘。

欄位	價值
授與類型	授權代碼
回撥 URL	如果您沒有回撥 URL、請輸入應用程式的基礎 URL。
驗證 URL	[ADFS- 網域名稱]/ADFS/OAuth2/Authorize
存取權杖 URL	[ADFS- 網域名稱]/ADFS/OAuth2/token
用戶端ID	輸入 AD FS 用戶端 ID
用戶端機密	輸入 AD FS 用戶端機密
範圍	OpenID
用戶端驗證	以基本驗證標頭傳送
資源	在 Advance Options 標籤中、新增與 Callback URL 值相同的資源欄位、此值在 JWT Token 中會顯示為「aud」值。

使用 PowerShell、sccli 和 REST API 在 SnapCenter 伺服器中設定 MFA

您可以使用 PowerShell、sccli 和 REST API 在 SnapCenter 伺服器中設定 MFA。

SnapCenter MFA CLI 驗證

在 PowerShell 和 sccli 中、現有的 Cmdlet（Open-SmConnection）會以另一個稱為「AccessToken」的欄位來延伸、以使用承載權杖來驗證使用者。

```
Open-SmConnection -Credential <PSCredential> [-SMSbaseUrl <String>] [-Port <String>] [-RoleName <String>] [-AccessToken <string>]
```

執行上述 Cmdlet 之後，會建立工作階段，讓個別使用者進一步執行 SnapCenter Cmdlet。

SnapCenter MFA REST API 驗證

在 REST API 用戶端（例如 Postman 或 swagger）中使用 `_Authorization=B承載 <access token>` 格式的承載權杖、並在標頭中提及使用者 RoleName、以取得 SnapCenter 的成功回應。

MFA REST API 工作流程

當 MFA 設定為 AD FS 時、您應該使用存取（承載）權杖進行驗證、以便透過任何 REST API 存取 SnapCenter 應用程式。

關於此工作

- 您可以使用任何 REST 用戶端、例如 Postman、Swagger UI 或 Fireplane。
- 取得存取權杖、並使用它來驗證後續要求（SnapCenter REST API）以執行任何作業。

步驟

- 透過 AD FS MFA * 驗證

1. 設定 REST 用戶端呼叫 AD FS 端點以取得存取權杖。

當您按下按鈕以取得應用程式的存取權杖時、系統會將您重新導向至 AD FS SSO 頁面、您必須在其中提供 AD 認證並驗證 MFA。

1. 在 AD FS SSO 頁面的「使用者名稱」文字方塊中、輸入您的使用者名稱或電子郵件。

使用者名稱必須格式化為 `user@domain` 或 `domain\user`。

2. 在密碼文字方塊中、輸入您的密碼。
3. 按一下*登入*。
4. 在 * 登入選項 * 區段中、選取驗證選項並進行驗證（視您的組態而定）。
 - 推播：核准傳送至手機的推播通知。
 - QR 代碼：使用驗證點行動應用程式掃描 QR 代碼、然後輸入應用程式中顯示的驗證代碼
 - 一次性密碼：輸入 Token 的一次性密碼。
5. 驗證成功後、會開啟一個快顯視窗、其中包含存取權、ID 和重新整理 Token。

複製存取權杖、並在 SnapCenter REST API 中使用它來執行作業。

6. 在 REST API 中、您應該在標頭區段中傳遞存取權杖和角色名稱。
7. SnapCenter 會從 AD FS 驗證此存取權杖。

如果它是有效的權杖、SnapCenter 會將其解碼、並取得使用者名稱。

8. SnapCenter 會使用使用者名稱和角色名稱來驗證使用者執行 API。

如果驗證成功、SnapCenter 會傳回結果、否則會顯示錯誤訊息。

啟用或停用 REST API、CLI 和 GUI 的 SnapCenter MFA 功能

- 圖形使用者介面 *

步驟

1. 以 SnapCenter 管理員身分登入 SnapCenter Server。
2. 按一下 * 設定 * > * 全域設定 * > * 多重資料驗證 (MFA) 設定 *
3. 選取介面 (GUI/REST API/CLI) 以啟用或停用 MFA 登入。
 - PowerShell 介面 *

步驟

1. 執行 PowerShell 或 CLI 命令、以啟用 MFA for GUI、REST API、PowerShell 和 sccli。

```
Set-SmMultiFactorAuthentication -IsGuiMFAEnabled -IsRestApiMFAEnabled  
-IsCliMFAEnabled -Path
```

path 參數會指定 AD FS MFA 中繼資料 XML 檔案的位置。

啟用 MFA 以使用指定的 AD FS 中繼資料檔案路徑來設定 SnapCenter GUI、REST API、PowerShell 和 sccli。

2. 使用檢查 MFA 組態狀態和設定 `Get-SmMultiFactorAuthentication Cmdlet`。

*sccli 介面 *

步驟

1. # `sccli Set-SmMultiFactorAuthentication -IsGuiMFAEnabled true -IsRESTAPIMFAEnabled true -IsCliMFAEnabled true -Path "C:\ADFS_metadata\abc.xml"`
2. # `sccli Get-SmMultiFactorAuthentication`
 - REST API*
3. 執行下列 POST API 以啟用 MFA for GUI、REST API、PowerShell 和 sccli。

參數	價值
----	----

要求的 URL	/API/4.9/settings/multifactorauthentication
HTTP方法	貼文
要求主體	{ "IsGuiMFAEnabled" : 錯誤、 "IsRestApiMFAEnabled" : 對、 "IsClicMFAEnabled" : 錯、 "ADFSConfigFilePath" : "C:\ADFS_中繼 資料 \abc.xml " }
回應本文	{ "MFAConfiguration" : { "IsGuiMFAEnabled" : 錯誤、 "ADFSConfigFilePath" : "C:\ADFS_中繼 資料 \abc.xml 、 "SCConfigFilePath" : null 、 "IsRestApiMFAEnabled" : 對、 "IsClicMFAEnabled" : 錯、 "ADFSHostName" : "win-ads-sc49.winscedom2.com } }

4. 使用下列 API 檢查 MFA 組態狀態和設定。

參數	價值
要求的 URL	/API/4.9/settings/multifactorauthentication
HTTP方法	取得
回應本文	{ "MFAConfiguration" : { "IsGuiMFAEnabled" : 錯誤、 "ADFSConfigFilePath" : "C:\ADFS_中繼 資料 \abc.xml 、 "SCConfigFilePath" : null 、 "IsRestApiMFAEnabled" : 對、 "IsClicMFAEnabled" : 錯、 "ADFSHostName" : "win-ads-sc49.winscedom2.com } }

安裝SnapCenter 此伺服器

在 Windows 主機上安裝 SnapCenter 伺服器

您可以執行SnapCenter 《伺服器安裝程式執行檔》來安裝SnapCenter 《伺服器版》。

您可以選擇使用PowerShell Cmdlet來執行多個安裝和組態程序。您應該使用 PowerShell 7.4.2 或更新版本。



不支援從SnapCenter 命令列無聲安裝支援。

開始之前

- 支援Windows更新的更新必須是最新版的伺服器SnapCenter 主機、而且不會有擱置中的系統重新啟動。
- 您應該已確定MySQL Server未安裝在您計畫安裝SnapCenter 此伺服器的主機上。
- 您應該已啟用Windows安裝程式偵錯功能。

如需啟用的相關資訊、請參閱Microsoft網站 "[Windows安裝程式記錄](#)"。



您不應在SnapCenter 擁有Microsoft Exchange Server、Active Directory或網域名稱伺服器的主機上安裝此伺服器。

步驟

1. 請SnapCenter 從下載《停止更新》安裝套件 "[NetApp 支援網站](#)"。
2. 連按兩下下載的.exe檔案、即可啟動SnapCenter 安裝程式。

在您啟動安裝之後、會執行所有預先檢查、如果未達到最低要求、則會顯示適當的錯誤或警告訊息。

您可以忽略警告訊息並繼續安裝、但錯誤應予以修正。

3. 檢閱SnapCenter 安裝此功能所需的預先填入值、並視需要進行修改。

您不需要指定MySQL Server儲存庫資料庫的密碼。在安裝過程中、會自動產生密碼。SnapCenter



儲存庫資料庫的自訂路徑不支援特殊字元「%」。如果您在路徑中加入「%」、安裝將會失敗。

4. 按一下*立即安裝*。

如果您已指定任何無效的值、將會顯示適當的錯誤訊息。您應該重新輸入值、然後開始安裝。



如果您按一下「取消」按鈕、將會完成正在執行的步驟、然後開始復原作業。將從主機中完全移除該伺服器。SnapCenter

不過、如果SnapCenter 您在執行「停止伺SnapCenter 伺服器站重新啟動」或「等待伺服器啟動」作業時按*「取消」、安裝作業將會繼續進行、而不會取消作業。

記錄檔一律會列在管理使用者的%temp%資料夾中（最舊的優先）。如果您想重新導向記錄位置、SnapCenter 請執行：`C:\installer_location\installer_name.exe /log"C:\\"`、從命令提示字元啟動安裝

安裝期間在 **Windows** 主機上啟用的功能

安裝過程中、支援Windows主機上的Windows功能和角色。SnapCenter這些可能對故障排除和維護主機系統有用。

類別	功能
Web伺服器	<ul style="list-style-type: none"> • 網際網路資訊服務 • 全球網路服務 • 一般HTTP功能 <ul style="list-style-type: none"> ◦ 預設文件 ◦ 目錄瀏覽 ◦ HTTP錯誤 ◦ HTTP重新導向 ◦ 靜態內容 ◦ WebDAWeb.發佈 • 健全狀況與診斷 <ul style="list-style-type: none"> ◦ 自訂記錄 ◦ HTTP記錄 ◦ 記錄工具 ◦ 要求監控 ◦ 追蹤 • 效能特色 <ul style="list-style-type: none"> ◦ 靜態內容壓縮 • 安全性 <ul style="list-style-type: none"> ◦ IP安全性 ◦ 基本驗證 ◦ 集中式SSL憑證支援 ◦ 用戶端憑證對應驗證 ◦ 「IIS用戶端憑證對應驗證」 ◦ IP和網域限制 ◦ 要求篩選 ◦ URL授權 ◦ Windows驗證 • 應用程式開發功能 <ul style="list-style-type: none"> ◦ .NET擴充性4.5 ◦ 應用程式初始化 ◦ ASP.NET Core Runtime 8.0.12 (以及所有後續 8.0.x 修補程式) 代管產品組合 ◦ 伺服器端隨附 ◦ WebSocket傳輸協定 <p>管理工具</p>

類別	功能
「IIS管理指令碼與工具」	<ul style="list-style-type: none"> • IIS管理服務 • 網路管理工具
.NET Framework 8.0.12 Features	<ul style="list-style-type: none"> • ASP.NET Core Runtime 8.0.12 (以及所有後續 8.0.x 修補程式) 代管產品組合 • Windows Communication Foundation (WCF) HTTP Activation45 <ul style="list-style-type: none"> ◦ TCP啟動 ◦ HTTP啟動 <p>如需 .NET 特定疑難排解資訊、請參閱 "對於沒有網際網路連線的舊版系統、SnapCenter 升級或安裝失敗"。</p>
Windows處理程序啟動服務	程序模式
組態API	全部

在 Linux 主機上安裝 SnapCenter 伺服器

您可以執行SnapCenter 《伺服器安裝程式執行檔》來安裝SnapCenter 《伺服器版》。

開始之前

- 如果您想要使用非 root 使用者安裝 SnapCenter 伺服器、但該使用者沒有足夠的權限來安裝 SnapCenter、請從 NetApp 支援網站取得 sudoers checksum 檔案。您應該根據 Linux 版本使用適當的 Checksum 檔案。
- 如果 Sudo 套件在 SUSE Linux 中無法使用、請安裝 Sudo 套件以避免驗證失敗。
- 對於 SUSE Linux、請設定主機名稱以避免安裝失敗。
- 運行命令檢查安全的 Linux 狀態 `sestatus`。如果 `SELinux` 狀態 `_` 為「已啟用」、且 `_current-mode` 為「強制」、請執行下列步驟：
 - 執行命令：`sudo semanage port -a -t http_port_t -p tcp <WEBAPP_EXTERNAL_PORT_>`
`webapp_extal_port` 的預設值為 8146
 - 如果防火牆封鎖連接埠、請執行 `sudo firewall-cmd --add-port <WEBAPP_EXTERNAL_PORT_>/tcp`
`webapp_extal_port` 的預設值為 8146
 - 從具有讀寫權限的目錄執行下列命令：
 - `sudo ausearch -c 'nginx' --raw | audit2allow -M my-nginx`

如果命令傳回「無待辦事項」、請在安裝 SnapCenter Server 之後重新執行命令。

- 如果命令會建立 *my-Nginx.pp*、請執行命令以啟用原則套件：`sudo semodule -i my-nginx.pp`
- 用於 MySQL PID 目錄的路徑是 `/var/opt/mysqld_`。執行下列命令以設定 MySQL 安裝的權限。
 - `mkdir /var/opt/mysqld`
 - `sudo semanage fcontext -a -t mysqld_var_run_t "/var/opt/mysqld(/.*)?"`
 - `sudo restorecon -Rv /var/opt/mysqld`
- 用於 MySQL Data 目錄的路徑為：`//INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL/_`。執行下列命令以設定 MySQL 資料目錄的權限。
 - `mkdir -p /INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL`
 - `sudo semanage fcontext -a -t mysqld_db_t "/INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL(/.*)?"`
 - `sudo restorecon -Rv /INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL`

關於這項工作

- 當 SnapCenter 伺服器安裝在 Linux 主機上時、會安裝第三方服務、例如 MySQL、RabbitMQ、Erlang
 - 您不應將其解除安裝。
- 安裝在 Linux 主機上的 SnapCenter 伺服器不支援：
 - 高可用度
 - Windows 外掛程式
 - Active Directory（僅支援本機使用者、包括具有 creds 的 root 和非 root 使用者）
 - 登入 SnapCenter 的金鑰型驗證
- 安裝期間。NET 執行階段時、如果安裝無法解決 *libicu* 程式庫的相依性、請執行下列命令來安裝 *libicu*：
`yum install -y libicu`
- 如果由於 *Perl* 不可用而導致 SnapCenter 伺服器安裝失敗、請執行下列命令來安裝 *Perl*：`yum install -y perl`

步驟

1. 從下載下列項目 "[NetApp 支援網站](#)" 至 / 主目錄 `_`。
 - SnapCenter 伺服器安裝套件 - `*snapcenter-linux-server- (el8/el9/sles15) .bin*`
 - 公開金鑰檔案 - `*snapcenter_public_key.pub`
 - 各自的簽名檔 - `*snapcenter-linux-server- (el8/el9/sles15) .bin.SIG*`
2. 驗證簽名檔案。`$openssl dgst -sha256 -verify snapcenter_public_key.pub -signature <path to signature file> <path to bin file>`
3. 若為非 root 使用者安裝、請新增在 `snapcenter_server_checksum _ (el8/el9/sles15)` 中指定的 **visudo** 內容。**txt** 與 **.bin** 安裝程式一起提供。
4. 指派 **.bin** 安裝程式的執行權限。`chmod +x snapcenter-linux-server-(el8/el9/sles15).bin`
5. 執行其中一個動作來安裝 SnapCenter Server。

如果您想要執行 ...	執行此動作...
互動式安裝	<pre>./snapcenter-linux-server- (el8/el9/sles15).bin</pre> <p>系統會提示您輸入下列詳細資料：</p> <ul style="list-style-type: none">• 用於存取 Linux 主機外部 SnapCenter 伺服器的 Web 應用程式外部連接埠。預設值為 8146。• 將安裝 SnapCenter 伺服器的 SnapCenter 伺服器使用者。• 安裝套件的安裝目錄。

如果您想要執行 ...	執行此動作...
非互動式安裝	<pre> sudo ./snapcenter-linux-server- (e18/e19/sles15).bin -i silent -DWEBAPP_EXTERNAL_PORT=<port> -DWEBAPP_INTERNAL_PORT=<port> -DSMCORE_PORT=<port> -DSCHEULER_PORT=<port> -DSNAPCENTER_SERVER_USER=<user> -DUSER_INSTALL_DIR=<dir> -DINSTALL_LOG_NAME=<filename> </pre> <p>範例： Sudo ./snapcenter_linux_server.bin -l silent -DWEBAPP_external_port=8146 -DSNAPCENTER_SERVER_USER=root -DUSER_INSTALL_DIR=/opt -DINSTALL_LOT_NAME=InstallerLog.log</p> <p>記錄將儲存在 /var/opt/snapcenter/logs_ 。</p> <p>安裝 SnapCenter 伺服器所需傳遞的參數：</p> <ul style="list-style-type: none"> • DWEBAPP_extal_port：Webapp 外部連接埠、用於存取 Linux 主機外部的 SnapCenter 伺服器。預設值為 8146 。 • DWEBAPP_INTERNAL_port：Webapp 內部連接埠、用於存取 Linux 主機內的 SnapCenter 伺服器。預設值為 8147 。 • DSMCORE 服務執行所在的 SMCore 連接埠。預設值為 8145 。 • DSCHEULER_port：排程器服務執行所在的排程器連接埠。預設值為 8154 。 • DSNAPCENTER_SERVER_USER：將安裝 SnapCenter 伺服器的 SnapCenter 伺服器使用者。對於 <i>DSNAPCENTER_SERVER_USER</i>、預設值為執行安裝程式的使用者。 • duser_install_DIR：安裝套件的安裝目錄。對於 <i>Duser_install_DIR</i>、預設安裝目錄為 /opt 。 • DINSTAL_log_name：儲存安裝記錄檔的記錄檔名稱。這是選用參數、如果指定、則不會在主控台上顯示任何記錄。如果您未指定此參數、記錄將會顯示在主控台上、也會儲存在預設記錄檔中。 • DSELINUX：如果 <i>_SELinux 狀態_</i> 為「已啟用」、則 <i>_目前模式_</i> 為「強制」、且您已執行「開始之前」一節中所述的命令、則應指定此參數並將值指派為 1。預設值為 0 。 • DUPGRADE：預設值為 0。將此參數及其值指定為 0 以外的任何整數、以升級 SnapCenter 伺服器。

接下來呢？

- 如果 `SELinux` 狀態 `_` 為「已啟用」、且 `_current-mode` 為「強制」、則 **NginX** 服務無法啟動。您應該執行下列命令：
 - a. 移至主目錄。
 - b. 執行命令：`journalctl -x|grep nginx`。
 - c. 如果不允許 Webapp 內部連接埠（8147）接聽、請執行下列命令：
 - `ausearch -c 'nginx' --raw | audit2allow -M my-nginx`
 - `semodule -i my-nginx.pp`
 - d. 執行 `setsebool -P httpd_can_network_connect on`

安裝期間在 **Linux** 主機上啟用的功能

SnapCenter 伺服器安裝以下軟體包，可協助排除故障和維護主機系統。

- RabbitMQ
- Erlang

註冊 SnapCenter

如果您是 NetApp 產品的新手，而且沒有現有的 NetApp 帳戶，則應註冊 SnapCenter 以啟用支援。

步驟

1. 安裝 SnapCenter 之後、請瀏覽 * 說明 > 關於 * 。
2. 在 _ 關於 SnapCenter _ 對話方塊中、記下以 971 開頭的 20 位數 SnapCenter 執行個體。
3. 單擊。 <https://register.netapp.com>
4. 按一下「* 我不是註冊的 NetApp 客戶 *」。
5. 請指定您的詳細資料以自行註冊。
6. 將 NetApp 參考 SN 欄位保留空白。
7. 從產品線下拉式清單中選取 * SnapCenter * 。
8. 選擇帳單供應商。
9. 輸入 20 位數的 SnapCenter 執行個體 ID 。
10. 按一下*提交*。

使用RBAC授權登入SnapCenter 到功能表

支援角色型存取控制（RBAC） SnapCenter 。透過支援資源的RBAC、將角色和資源指派給工作群組或作用中目錄的使用者、或指派給作用中目錄中的群組。SnapCenter RBAC使用者現在可以SnapCenter 使用指派的角色登入至功能表。

開始之前

- 您應該在Windows Server Manager中啟用Windows處理程序啟動服務（WOS）。
- 如果您想要使用Internet Explorer作為瀏覽器登入SnapCenter 到該伺服器、您應該確定Internet Explorer中的「保護模式」已停用。
- 如果 SnapCenter 伺服器安裝在 Linux 主機上、您應該使用用來安裝 SnapCenter 伺服器的使用者帳戶登入。

關於此工作

安裝期間SnapCenter、「VMware Server安裝精靈」會建立捷徑、並將其放在桌面和SnapCenter 安裝了VMware的主機的「開始」功能表中。此外、在安裝結束時、安裝精靈會根據SnapCenter 您在安裝期間提供的資訊來顯示該URL、如果您想從遠端系統登入、可以複製該URL。



如果您在網頁瀏覽器中開啟多個索引標籤、只要關閉SnapCenter「瀏覽器」索引標籤、就不會將您登出SnapCenter「支援」。若要結束SnapCenter與Sendor的連線、您必須SnapCenter按一下*登出*按鈕、或關閉整個網路瀏覽器來登出Sing。

*最佳實務做法：*基於安全考量、建議您不要讓瀏覽器儲存SnapCenter 您的密碼。

預設的GUI URL是安全連線至SnapCenter 安裝了該伺服器的預設連接埠8146 (<https://server:8146>)。如果您在SnapCenter 安裝過程中提供不同的伺服器連接埠、則會改用該連接埠。

若要部署高可用度（HA）、您必須SnapCenter 使用虛擬叢集IP \ https://Virtual_Cluster_IP_or_FQDN:8146 來存取功能。如果您在Internet Explorer（IE）中瀏覽至 https://Virtual_Cluster_IP_or_FQDN:8146 時沒有看到SnapCenter 此功能、則必須在每個外掛主機的IE中、將虛擬叢集IP位址或FQDN新增為信任的網站、或是在每個外掛主機上停用IE增強安全功能。如需詳細資訊、請參閱 "[無法從外部網路存取叢集IP位址](#)"。

除了使用SnapCenter 還原GUI、您還可以使用PowerShell Cmdlet建立指令碼來執行組態、備份及還原作業。每SnapCenter 個版本的各個版本可能都有一些Cmdlet變更。"《[軟件指令程式參考指南](#)》SnapCenter"有詳細資料。



如果SnapCenter 您是第一次登入到此資訊中心、則必須使用安裝程序中提供的認證登入。

步驟

1. 從SnapCenter 本機主機桌面上的捷徑、安裝結束時提供的URL、或SnapCenter 從您的管理員提供的URL啟動支援。
2. 輸入使用者認證資料。

若要指定下列項目...	使用下列其中一種格式...
網域管理員	<ul style="list-style-type: none"> • NetBios \使用者名稱 • 使用者名稱@ UPN尾碼 <p>例如：username@netapp.com</p> <ul style="list-style-type: none"> • 網域FQDN \使用者名稱
本機系統管理員	使用者名稱

3. 如果您被指派一個以上的角色、請從「角色」方塊中選取您要用於此登入工作階段的角色。

登入後、您目前的使用者和相關角色會顯示在SnapCenter 畫面右上角。

◦ 結果 *

隨即顯示儀表板頁面。

如果記錄失敗並顯示無法連線至站台的錯誤、您應該將SSL憑證對應SnapCenter 至 ["深入瞭解"](#)

完成後

初次以SnapCenter RBAC使用者身分登入到支援服務器之後、請重新整理資源清單。

如果您有不受信任的Active Directory網域想SnapCenter 要支援此功能、則必須先以SnapCenter 支援的方式登錄這些網域、然後再為不受信任網域上的使用者設定角色。["深入瞭解"](#)。

如果您想要在 Linux 主機上執行的 SnapCenter 中新增外掛主機、您應該從位置取得 Checksum 檔案：
`//opt/NetApp/snapcenter/SnapManagerWeb/Repository`。

從 6.0 版本開始、桌面上會建立 SnapCenter PowerShell 的捷徑。您可以使用捷徑直接存取 SnapCenter PowerShell Cmdlet。

使用多因素驗證 (MFA) 登入SnapCenter

支援MFA的網域帳戶是作用中目錄的一部分。SnapCenter

開始之前

您應該已經啟用MFA。如需如何啟用 MFA 的資訊、請參閱 ["啟用多因素驗證"](#)

關於此工作

- 僅支援FQDN
- 工作群組和跨網域使用者無法使用MFA登入

步驟

1. 從SnapCenter 本機主機桌面上的捷徑、安裝結束時提供的URL、或SnapCenter 從您的管理員提供的URL啟動支援。
2. 在AD FS登入頁面中、輸入使用者名稱和密碼。

當AD FS頁面上顯示使用者名稱或密碼無效錯誤訊息時、您應該檢查下列項目：

◦ 使用者名稱或密碼是否有效

使用者帳戶應存在於Active Directory (AD) 中

- 是否超過AD中設定的允許嘗試次數上限
- AD和AD FS是否已啟動並正在執行

修改SnapCenter 功能不全的GUI工作階段逾時時間

您可以修改SnapCenter 不必要的GUI工作階段逾時期間、使其低於或大於預設的逾時期間20分鐘。

作為一項安全功能、SnapCenter 當預設的閒置時間為15分鐘後、下列警告將在5分鐘內登出GUI工作階段。根據預設SnapCenter、若無活動20分鐘、將會從GUI工作階段登出、您必須重新登入。

步驟

1. 在左導覽窗格中、按一下*設定*>*全域設定*。
2. 在「全域設定」頁面中、按一下*「組態設定」*。
3. 在工作階段逾時欄位中、輸入以分鐘為單位的新工作階段逾時時間、然後按一下*儲存*。

停用SSL 3.0來保護SnapCenter Web伺服器的安全

基於安全考量、如果在SnapCenter 您的支援網頁伺服器上啟用安全通訊端層 (SSL) 3.0傳輸協定、您應該在Microsoft IIS中停用該傳輸協定。

SSL 3.0傳輸協定有漏洞、攻擊者可以用來造成連線失敗、或是執行攔截式攻擊、以及觀察網站與訪客之間的加密流量。

步驟

1. 若要在SnapCenter SWeb伺服器主機上啟動登錄編輯程式、請按一下*開始*>*執行*、然後輸入regedit.
2. 在「登錄編輯程式」中、瀏覽至「本地機器\系統\控制項\安全性供應商\ SChannel\傳輸協定\ SSL 3.0\」。
 - 如果伺服器金鑰已經存在：
 - i. 選取「已啟用」的雙字節、然後按一下「編輯>*修改*」。
 - ii. 將值變更為0、然後按一下「確定」。
 - 如果伺服器金鑰不存在：
 - i. 按一下*編輯*>*新增*>*金鑰*、然後命名金鑰伺服器。
 - ii. 選取新的伺服器機碼後、按一下*編輯*>*新增*>*雙字節*。
 - iii. 將新的「啟用的雙字節」命名為「已啟用」、然後輸入0作為值。
3. 關閉「登錄編輯程式」。

配置 SnapCenter 伺服器

新增並配置儲存系統

新增儲存系統

您應該設定儲存系統，讓 SnapCenter 能夠存取 ONTAP 儲存設備，ASA R2 系統或 Amazon FSX for NetApp ONTAP，以執行資料保護和資源配置作業。

您可以新增獨立SVM或由多個SVM組成的叢集。如果您使用Amazon FSx for NetApp ONTAP 支援NetApp、則可以使用fsxadmin帳戶新增由多個SVM組成的FSx管理LIF、或在Sfsx SnapCenter 中新增FSVM。

開始之前

- 您應該在「基礎架構管理員」角色中擁有必要的權限、才能建立儲存連線。
- 您應確保外掛程式安裝不進行中。

在新增儲存系統連線時、主機外掛程式安裝不得進行、因為主機快取可能不會更新、而且SnapCenter 資料庫狀態可能會顯示在「無法備份」或「不在NetApp儲存設備上」。

- 儲存系統名稱應該是唯一的。

不支援在不同叢集上使用相同名稱的多個儲存系統。SnapCenter每個SnapCenter 受支援的儲存系統都應有唯一的名稱和唯一的資料LIF IP位址。

關於此工作

- 當您設定儲存系統時、也可以啟用事件管理系統 (EMS) 和AutoSupport 功能。此功能可收集系統健全狀況的相關資料、並自動將資料傳送給NetApp技術支援部門、讓他們能夠疑難排解您的系統。AutoSupport

如果啟用這些功能、SnapCenter 當AutoSupport 資源受到保護、還原或複製作業成功完成或作業失敗時、將會將支援資訊傳送至儲存系統、並將EMS訊息傳送至儲存系統的系統記錄。

- 如果您打算將 Snapshot 複寫到 SnapMirror 目的地或 SnapVault 目的地、則必須為目的地 SVM 或叢集、以及來源 SVM 或叢集設定儲存系統連線。



如果您變更儲存系統密碼、排程工作、隨需備份和還原作業可能會失敗。變更儲存系統密碼之後、您可以按一下「Storage (儲存設備)」索引標籤中的* Modify* (修改*) 來更新密碼。

步驟

1. 在左導覽窗格中、按一下*儲存系統*。
2. 在「Storage Systems (儲存系統)」頁面中、按一下「* New* (*新
3. 在「Add Storage System (新增儲存系統)」頁面中、提供下列資訊：

針對此欄位...	執行此動作...
儲存系統	<p>輸入儲存系統名稱或IP位址。</p> <p> 儲存系統名稱（不包括網域名稱）必須有 15 個或更少的字元、而且名稱必須可解析。若要建立名稱超過15個字元的儲存系統連線、您可以使用Add-SmStorageConnectionPowerShell Cmdlet。</p> <p> 對於MetroCluster 採用非破壞性組態（MCC）的儲存系統、建議同時登錄本機和對等叢集、以進行不中斷營運。</p> <p>不支援在不同叢集上使用相同名稱的多個SVM ◦ SnapCenter支援的每個SVM SnapCenter 都必須有唯一的名稱。</p> <p> 將儲存連線新增SnapCenter 至Sfing 之後、您不應使用ONTAP SVM或叢集重新命名。</p> <p> 如果SVM是以簡短名稱或FQDN新增、則必須同時從SnapCenter 支援程式和外掛程式主機解析。</p>
使用者名稱/密碼	輸入擁有存取儲存系統所需權限的儲存使用者認證。
事件管理系統（EMS）與AutoSupport Esority設定	<p>如果您想要傳送EMS訊息到儲存系統的系統記錄、或是想AutoSupport 要將還原訊息傳送到儲存系統以進行套用保護、完成還原作業或失敗作業、請選取適當的核取方塊。</p> <p>當您選取「將AutoSupport 失敗作業的資訊傳送到儲存系統」核取方塊時、也SnapCenter 會選取「將資料記錄到SysLog*」核取方塊、因為必須使用EMS 訊息才能啟用AutoSupport 資訊功能通知。</p>

4. 如果要修改指派給平台、傳輸協定、連接埠和逾時的預設值、請按一下*「更多選項」*。

a. 在平台中、從下拉式清單中選取其中一個選項。

如果SVM是備份關係中的次要儲存系統、請選取「次要」核取方塊。如果選擇*二線*選項、SnapCenter 則無法立即執行授權檢查。

如果您在 SnapCenter 中新增了 SVM 、則使用者需要從下拉式清單中手動選取平台類型。

a. 在「傳輸協定」中、選取在SVM或叢集設定期間設定的傳輸協定、通常是HTTPS。

b. 輸入儲存系統接受的連接埠。

預設連接埠443通常正常運作。

c. 輸入在通訊嘗試停止之前應經過的時間（以秒為單位）。

預設值為60秒。

d. 如果SVM有多個管理介面、請選取「慣用IP」核取方塊、然後輸入SVM連線的慣用IP位址。

e. 按一下「* 儲存 *」。

5. 按一下*提交*。

◦ 結果 *

在「儲存系統」頁面的「類型」下拉式清單中、執行下列其中一項動作：

• 如果ONTAP 您要檢視所有新增的SVM、請選取*《SVMS*》。

如果您已新增FSX SVM、此處會列出FSX SVM。

• 如果ONTAP 您要檢視所有新增的叢集、請選取*《叢集*》。

如果您已使用fsxadmin新增FSX叢集、則此處會列出FSx叢集。

當您按一下叢集名稱時、屬於叢集一部分的所有SVM都會顯示在「儲存虛擬機器」區段中。

如果ONTAP 使用ONTAP RefesGUI將新的SVM新增至Refes叢集、請按一下*重新探索*以檢視新增的SVM。

完成後

叢集管理員必須在AutoSupport 每個儲存系統節點上啟用「支援功能」、SnapCenter 才能從所有可存取的儲存系統傳送電子郵件通知、方法是從儲存系統命令列執行下列命令：

```
autosupport trigger modify -node nodename -autosupport-message client.app.info  
-to enable -noteto enable
```



儲存虛擬機器（SVM）管理員無法存取AutoSupport VMware。

儲存連線與認證

在執行資料保護作業之前、您應該先設定儲存連線、並新增SnapCenter 功能、以供使用。SnapCenter

儲存連接

儲存連線可讓SnapCenter Sfor Sfor Server和SnapCenter Sfor插座存取ONTAP 功能豐富的功能。設定這些連線時、也需要設定AutoSupport 功能性的功能性和事件管理系統（EMS）。

認證資料

- 網域管理員或系統管理員群組的任何成員

在您要安裝SnapCenter 此插件的系統上、指定網域管理員或任何系統管理員群組成員。「使用者名稱」欄位的有效格式為：

- *netbios*\使用者名稱
 - 網域FQDN \使用者名稱_
 - *username@UPN*
- 本機管理員（僅適用於工作群組）

對於屬於工作群組的系統、請在安裝SnapCenter 此插件的系統上指定內建的本機管理員。如果使用者帳戶擁有較高的權限、或主機系統上的使用者存取控制功能已停用、您可以指定屬於本機系統管理員群組的本機使用者帳戶。

「使用者名稱」欄位的有效格式為：*username*

- 個別資源群組的認證資料

如果您為個別資源群組設定認證、但使用者名稱沒有完整的管理權限、則必須至少將資源群組和備份權限指派給使用者名稱。

在Windows主機上配置儲存設備

建立及管理igroup

您可以建立啟動器群組（igroup）、以指定哪些主機可以存取儲存系統上的特定LUN。您可以使用SnapCenter 支援功能來建立、重新命名、修改或刪除Windows主機上的igroup。

建立igroup

您可以使用SnapCenter 支援功能在Windows主機上建立igroup。當您將igroup對應至LUN時、即可在Create Disk（建立磁碟）或Connect Disk（連線磁碟）精靈中使用igroup。

步驟

1. 在左側導覽窗格中、按一下*主機*。
2. 在「主機」頁面中、按一下* igroup*。
3. 在「啟動器群組」頁面中、按一下「新增」。
4. 在「建立igroup」對話方塊中、定義igroup：

在此欄位中...	執行此動作...
儲存系統	選取要對應至igroup的LUN SVM。
主機	選取您要在其中建立igroup的主機。

在此欄位中...	執行此動作...
igroup名稱	輸入igroup的名稱。
啟動器	選取啟動器。
類型	選取啟動器類型、iSCSI、FCP或混合（FCP和iSCSI）。

- 當您對輸入項目感到滿意時、請按一下*確定*。

在儲存系統上建立igroup。SnapCenter

重新命名igroup

您可以使用SnapCenter 效益管理功能來重新命名現有的igroup。

步驟

- 在左側導覽窗格中、按一下*主機*。
- 在「主機」頁面中、按一下* igroup*。
- 在「啟動器群組」頁面中、按一下「儲存虛擬機器」欄位以顯示可用的SVM清單、然後針對您要重新命名的igroup選取SVM。
- 在SVM的igroup清單中、選取您要重新命名的igroup、然後按一下* Rename *。
- 在「重新命名igroup」對話方塊中、輸入igroup的新名稱、然後按一下「重新命名」。

修改igroup

您可以使用SnapCenter 效益管理功能將igroup啟動器新增至現有的igroup。建立igroup時、您只能新增一部主機。如果您要為叢集建立igroup、可以修改igroup以新增其他節點至該igroup。

步驟

- 在左側導覽窗格中、按一下*主機*。
- 在「主機」頁面中、按一下* igroup*。
- 在「啟動器群組」頁面中、按一下「儲存虛擬機器」欄位以顯示可用的SVM下拉式清單、然後針對您要修改的igroup選取SVM。
- 在igroup清單中、選取一個igroup、然後按一下* 「Add Initiator to igroup*（將啟動器新增至igroup*）」。
- 選取主機。
- 選取啟動器、然後按一下*確定*。

刪除igroup

當您不再需要igroup時、可以使用SnapCenter 功能表來刪除它。

步驟

1. 在左側導覽窗格中、按一下*主機*。
2. 在「主機」頁面中、按一下*igroup*。
3. 在「啟動器群組」頁面中、按一下「儲存虛擬機器」欄位以顯示可用的SVM下拉式清單、然後針對您要刪除的igroup選取SVM。
4. 在SVM的igroup清單中、選取您要刪除的igroup、然後按一下*刪除*。
5. 在刪除igroup對話方塊中、按一下*確定*。

不刪除igroup。SnapCenter

建立及管理磁碟

Windows主機將儲存系統上的LUN視為虛擬磁碟。您可以使用SnapCenter 支援功能來建立及設定FC連接或iSCSI連接的LUN。

- 支援僅基本磁碟。SnapCenter不支援動態磁碟。
- 若為GPT、則僅允許一個資料分割區和一個主分割區使用NTFS或CSVFS格式化一個磁碟區、並有一個掛載路徑。
- 支援的分割區樣式：GPT、MBR;在VMware UEFI VM中、僅支援iSCSI磁碟



不支援重新命名磁碟。SnapCenter如果SnapCenter 以這個名稱重新命名由該系統管理的磁碟、SnapCenter 則無法成功執行此功能。

檢視主機上的磁碟

您可以在每個使用SnapCenter 支援的Windows主機上檢視磁碟。

步驟

1. 在左側導覽窗格中、按一下*主機*。
2. 在「主機」頁面中、按一下「磁碟」。
3. 從*主機*下拉式清單中選取主機。

隨即列出磁碟。

檢視叢集式磁碟

您可以檢視SnapCenter 叢集上的叢集式磁碟、並使用NetApp進行管理。叢集式磁碟只有在您從「主機」下拉式清單中選取叢集時才會顯示。

步驟

1. 在左側導覽窗格中、按一下*主機*。
2. 在「主機」頁面中、按一下「磁碟」。

3. 從*主機*下拉式清單中選取叢集。

隨即列出磁碟。

建立iSCSI工作階段

如果您使用iSCSI連線至LUN、則必須先建立iSCSI工作階段、再建立LUN以啟用通訊。

開始之前

- 您必須將儲存系統節點定義為iSCSI目標。
- 您必須已在儲存系統上啟動iSCSI服務。["深入瞭解"](#)

關於此工作

您只能在相同的IP版本之間建立iSCSI工作階段、無論是從IPv6到IPv6、或是從IPv4到IPv6。

您可以使用連結本機IPv6位址進行iSCSI工作階段管理、以及僅當主機和目標位於相同子網路時、才進行通訊。

如果變更iSCSI啟動器的名稱、則存取iSCSI目標的權限會受到影響。變更名稱之後、您可能需要重新設定啟動器存取的目標、以便辨識新名稱。變更iSCSI啟動器名稱後、您必須確保重新啟動主機。

如果您的主機有多個iSCSI介面、當您在SnapCenter 第一個介面上使用IP位址建立iSCSI工作階段以供支援時、就無法從另一個介面建立具有不同IP位址的iSCSI工作階段。

步驟

1. 在左側導覽窗格中、按一下*主機*。
2. 在「主機」頁面中、按一下「* iSCSI工作階段*」。
3. 從*儲存虛擬機器*下拉式清單中、選取iSCSI目標的儲存虛擬機器 (SVM) 。
4. 從*主機*下拉式清單中、選取工作階段的主機。
5. 按一下*建立工作階段*。

隨即顯示「建立工作階段精靈」。

6. 在建立工作階段精靈中、找出目標：

在此欄位中...	輸入...
目標節點名稱	iSCSI目標的節點名稱 如果有現有的目標節點名稱、則名稱會以唯讀格式顯示。
目標入口網站位址	目標網路入口網站的IP位址
目標入口網站連接埠	目標網路入口網站的TCP連接埠

在此欄位中...	輸入...
啟動器入口網站位址	啟動器網路入口網站的IP位址

7. 當您對輸入項目感到滿意時、請按一下*「Connect（連線）」*。

建立iSCSI工作階段。SnapCenter

8. 重複此程序、為每個目標建立工作階段。

建立FC連接或iSCSI連接的LUN或磁碟

Windows主機將儲存系統上的LUN視為虛擬磁碟。您可以使用SnapCenter 支援功能來建立及設定FC連接或iSCSI連接的LUN。

如果您想要建立及格式化SnapCenter 非支援的磁碟、則僅支援NTFS和CSVFS檔案系統。

開始之前

- 您必須為儲存系統上的LUN建立磁碟區。

磁碟區只能容納LUN、而只能容納使用SnapCenter NetApp建立的LUN。



除非已分割實體複本、否則您無法在SnapCenter建立的實體複本磁碟區上建立LUN。

- 您必須已在儲存系統上啟動FC或iSCSI服務。
- 如果您使用iSCSI、則必須已與儲存系統建立iSCSI工作階段。
- 適用於Windows的支援功能外掛程式套件只能安裝在您要建立磁碟的主機上。SnapCenter

關於此工作

- 除非Windows Server容錯移轉叢集中的主機共用LUN、否則您無法將LUN連線至多個主機。
- 如果LUN由使用CSV（叢集共用磁碟區）的Windows Server容錯移轉叢集主機共用、則必須在擁有叢集群組的主機上建立磁碟。

步驟

1. 在左側導覽窗格中、按一下*主機*。
2. 在「主機」頁面中、按一下「磁碟」。
3. 從*主機*下拉式清單中選取主機。
4. 按一下「新增」。

「Create Disk（建立磁碟）」精靈隨即開啟。

5. 在LUN Name（LUN名稱）頁面中、識別LUN：

在此欄位中...	執行此動作...
儲存系統	選取LUN的SVM。
LUN路徑	單擊*瀏覽*以選擇包含LUN的文件夾的完整路徑。
LUN名稱	輸入LUN的名稱。
叢集大小	選取叢集的LUN區塊配置大小。 叢集大小取決於作業系統和應用程式。
LUN標籤	(可選) 輸入LUN的描述性文字。

6. 在「磁碟類型」頁面中、選取磁碟類型：

選取...	如果...
專用磁碟	LUN只能由一部主機存取。 忽略*資源群組*欄位。
共享磁碟	LUN由Windows Server容錯移轉叢集中的主機共用。 在「資源群組」欄位中輸入叢集資源群組的名稱。您只需要在容錯移轉叢集中的一部主機上建立磁碟。
叢集共用Volume (CSV)	LUN由使用CSV的Windows Server容錯移轉叢集中的主機共用。 在「資源群組」欄位中輸入叢集資源群組的名稱。請確定您要在其中建立磁碟的主機是叢集群組的擁有者。

7. 在「磁碟機內容」頁面中、指定磁碟機內容：

屬性	說明
自動指派掛載點	根據系統磁碟機自動指派磁碟區掛載點。SnapCenter 例如、如果您的系統磁碟機為C：、則自動指派會在C：磁碟機 (C：\scmnpt\) 下建立磁碟區掛載點。共享磁碟不支援自動指派。
指派磁碟機代號	將磁碟掛載到您在鄰近下拉式清單中選取的磁碟機。

屬性	說明
使用Volume掛載點	將磁碟掛載到您在鄰近欄位中指定的磁碟機路徑。 磁碟區掛載點的根目錄必須由您建立磁碟的主機擁有。
請勿指派磁碟機代號或磁碟區掛載點	如果您偏好在Windows中手動掛載磁碟、請選擇此選項。
LUN大小	指定LUN大小；至少150 MB。 在鄰近的下拉式清單中選取MB、GB或TB。
針對裝載此LUN的磁碟區使用精簡配置	精簡配置LUN。 資源隨需配置一次只會配置所需的儲存空間、讓LUN能夠有效率地擴充至最大可用容量。 請確定磁碟區上有足夠的可用空間、以容納您認為需要的所有LUN儲存設備。
選擇分割區類型	選取「Guid分割表」的GPT分割區、或「主開機記錄」的「MBR-分割區」。 在Windows Server容錯移轉叢集中、MBR分區可能會導致錯誤對齊問題。  不支援統一化可延伸韌體介面 (UEFI) 分割磁碟。

8. 在「Map LUN (對應LUN)」頁面中、選取主機上的iSCSI或FC啟動器：

在此欄位中...	執行此動作...
主機	按兩下叢集群組名稱以顯示下拉式清單、其中會顯示屬於叢集的主機、然後選取啟動器的主機。 此欄位只有在Windows Server容錯移轉叢集中的主機共用LUN時才會顯示。
選擇主機啟動器	選取* Fibre Channel*或* iscsi *、然後選取主機上的啟動器。 如果您使用FC搭配多重路徑I/O (MPIO)、則可以選取多個FC啟動器。

9. 在「群組類型」頁面中、指定要將現有的igroup對應至LUN、或是建立新的igroup：

選取...	如果...
為選取的啟動器建立新的igroup	您想要為選取的啟動器建立新的igroup。
選擇現有的igroup或為選取的啟動器指定新的igroup	<p>您想要為選取的啟動器指定現有的igroup、或使用您指定的名稱建立新的igroup。</p> <p>在* igroup name*欄位中輸入igroup名稱。輸入現有igroup名稱的前幾個字母、以自動填寫欄位。</p>

10. 在「摘要」頁面中、檢閱您的選擇、然後按一下「完成」。

實體建立LUN、並將其連接至主機上的指定磁碟機或磁碟機路徑。SnapCenter

調整磁碟大小

您可以隨著儲存系統的需求變更而增加或減少磁碟的大小。

關於此工作

- 對於精簡配置的LUN、ONTAP 將以最大大小顯示LUN幾何大小。
- 對於完整配置的LUN、可擴充的大小（磁碟區中可用的大小）會顯示為最大大小。
- 具有MBR-型分割區的LUN大小上限為2 TB。
- 具有GPT型分割區的LUN儲存系統大小上限為16 TB。
- 建議您在調整 LUN 大小之前先建立 Snapshot。
- 如果您需要從重新調整 LUN 大小之前建立的 Snapshot 還原 LUN、SnapCenter 會自動將 LUN 調整為 Snapshot 的大小。

還原作業完成後、重新調整 LUN 大小後新增至 LUN 的資料必須從重新調整大小後所建立的 Snapshot 還原。

步驟

1. 在左側導覽窗格中、按一下*主機*。
2. 在「主機」頁面中、按一下「磁碟」。
3. 從主機下拉式清單中選取主機。

隨即列出磁碟。

4. 選取您要調整大小的磁碟、然後按一下「調整大小」。
5. 在「調整磁碟大小」對話方塊中、使用滑桿工具來指定磁碟的新大小、或是在「大小」欄位中輸入新的大小。



如果您手動輸入大小、則必須在適當啟用「縮小或擴充」按鈕之前、先在「大小」欄位外按一下。此外、您必須按一下MB、GB或TB以指定測量單位。

6. 如果您對輸入項目滿意、請視需要按一下*縮小*或*展開*。

可重新調整磁碟大小。SnapCenter

連接磁碟

您可以使用「連線磁碟」精靈、將現有的LUN連線至主機、或重新連線已中斷連線的LUN。

開始之前

- 您必須已在儲存系統上啟動FC或iSCSI服務。
- 如果您使用iSCSI、則必須已與儲存系統建立iSCSI工作階段。
- 除非Windows Server容錯移轉叢集中的主機共用LUN、否則您無法將LUN連線至多個主機。
- 如果LUN由使用CSV（叢集共用磁碟區）的Windows Server容錯移轉叢集主機共用、則您必須連接擁有叢集群組的主機上的磁碟。
- Windows外掛程式只需安裝在要連接磁碟的主機上。

步驟

1. 在左側導覽窗格中、按一下*主機*。
2. 在「主機」頁面中、按一下「磁碟」。
3. 從*主機*下拉式清單中選取主機。
4. 按一下「連線」。

「連線磁碟」精靈隨即開啟。

5. 在LUN Name（LUN名稱）頁面中、識別要連線的LUN：

在此欄位中...	執行此動作...
儲存系統	選取LUN的SVM。
LUN路徑	按一下*瀏覽*以選取包含LUN的磁碟區完整路徑。
LUN名稱	輸入LUN的名稱。
叢集大小	選取叢集的LUN區塊配置大小。 叢集大小取決於作業系統和應用程式。
LUN標籤	（可選）輸入LUN的描述性文字。

6. 在「磁碟類型」頁面中、選取磁碟類型：

選取...	如果...
專用磁碟	LUN只能由一部主機存取。
共享磁碟	LUN由Windows Server容錯移轉叢集中的主機共用。 您只需要將磁碟連接至容錯移轉叢集中的一部主機。
叢集共用Volume (CSV)	LUN由使用CSV的Windows Server容錯移轉叢集中的主機共用。 請確定您要連線至磁碟的主機是叢集群組的擁有者。

7. 在「磁碟機內容」頁面中、指定磁碟機內容：

屬性	說明
自動指派	讓SnapCenter 我們根據系統磁碟機自動指派磁碟區掛載點。 例如、如果您的系統磁碟機為C：、則自動指派內容會在C：磁碟機 (C：\scmnpt) 下建立磁碟區掛載點。共享磁碟不支援自動指派內容。
指派磁碟機代號	將磁碟掛載到您在鄰近下拉式清單中選取的磁碟機。
使用Volume掛載點	將磁碟掛載到您在鄰近欄位中指定的磁碟機路徑。 磁碟區掛載點的根目錄必須由您建立磁碟的主機擁有。
請勿指派磁碟機代號或磁碟區掛載點	如果您偏好在Windows中手動掛載磁碟、請選擇此選項。

8. 在「Map LUN (對應LUN)」頁面中、選取主機上的iSCSI或FC啟動器：

在此欄位中...	執行此動作...
主機	按兩下叢集群組名稱以顯示下拉式清單、其中會顯示屬於叢集的主機、然後選取啟動器的主機。 此欄位只有在Windows Server容錯移轉叢集中的主機共用LUN時才會顯示。

在此欄位中...	執行此動作...
選擇主機啟動器	<p>選取* Fibre Channel*或* iscsi *、然後選取主機上的啟動器。</p> <p>如果您使用FC搭配MPIO、則可以選取多個FC啟動器。</p>

9. 在「群組類型」頁面中、指定要將現有的igroup對應至LUN、還是要建立新的igroup：

選取...	如果...
為選取的啟動器建立新的igroup	您想要為選取的啟動器建立新的igroup。
選擇現有的igroup或為選取的啟動器指定新的igroup	<p>您想要為選取的啟動器指定現有的igroup、或使用您指定的名稱建立新的igroup。</p> <p>在* igroup name*欄位中輸入igroup名稱。輸入現有igroup名稱的前幾個字母、以自動填寫欄位。</p>

10. 在「摘要」頁面中、檢閱您的選擇、然後按一下「完成」。

將LUN連接到主機上指定的磁碟機或磁碟機路徑。SnapCenter

中斷磁碟連線

您可以中斷LUN與主機的連線、而不影響LUN的內容、但有一項例外：如果您在將實體複本分割之前中斷連線、則會遺失該實體複本的內容。

開始之前

- 請確定任何應用程式都未使用LUN。
- 請確定未使用監控軟體監控LUN。
- 如果LUN是共享的、請務必從LUN移除叢集資源相依性、並確認叢集中的所有節點都已開啟電源、正常運作且可供SnapCenter使用。

關於此工作

如果您中斷SnapCenter 連接已建立的FlexClone Volume中的LUN、且該磁碟區上沒有連接其他LUN、SnapCenter 則會刪除該磁碟區。在中斷LUN連線之前SnapCenter、將會顯示一則訊息、警告您FlexClone Volume可能會被刪除。

為了避免自動刪除FlexClone Volume、您應該在中斷連接最後一個LUN之前、重新命名該磁碟區。當您重新命名Volume時、請務必變更多個字元、而非僅變更名稱中的最後一個字元。

步驟

1. 在左側導覽窗格中、按一下*主機*。
2. 在「主機」頁面中、按一下「磁碟」。

3. 從*主機*下拉式清單中選取主機。

隨即列出磁碟。

4. 選取您要中斷連線的磁碟、然後按一下「中斷連線」。
5. 在「中斷磁碟連線」對話方塊中、按一下「確定」。

中斷磁碟連線。SnapCenter

刪除磁碟

您可以在不再需要時刪除磁碟。刪除磁碟之後、您無法取消刪除該磁碟。

步驟

1. 在左側導覽窗格中、按一下*主機*。
2. 在「主機」頁面中、按一下「磁碟」。
3. 從*主機*下拉式清單中選取主機。

隨即列出磁碟。

4. 選取您要刪除的磁碟、然後按一下*刪除*。
5. 在刪除磁碟對話方塊中、按一下*確定*。

系統會刪除磁碟。SnapCenter

建立及管理SMB共用區

若要在儲存虛擬機器（SVM）上設定SMB3共用區、您可以使用SnapCenter 物件使用者介面或PowerShell Cmdlet。

*最佳實務做法：*建議使用Cmdlet、因為它可讓您利用SnapCenter 隨附的範本來自動化共用組態。

這些範本會封裝磁碟區和共用組態的最佳實務做法。您可以在安裝資料夾的「範本」資料夾中找到適用於SnapCenter Windows的「版本資訊」套件的範本。



如果您覺得這樣做很舒服、可以依照所提供的模型來建立自己的範本。建立自訂範本之前、您應該先檢閱Cmdlet文件中的參數。

建立SMB共用區

您可以使用SnapCenter 「不共用」頁面、在儲存虛擬機器（SVM）上建立SMB3共用區。

您無法使用SnapCenter 支援功能來備份SMB共用區上的資料庫。SMB支援僅限於資源配置。

步驟

1. 在左側導覽窗格中、按一下*主機*。

2. 在「主機」頁面中、按一下「共用」。
3. 從*儲存虛擬機器*下拉式清單中選取SVM。
4. 按一下「新增」。

「新增共用」對話方塊隨即開啟。

5. 在「新共用」對話方塊中、定義共用：

在此欄位中...	執行此動作...
說明	輸入共用的說明文字。
共用名稱	輸入共用名稱、例如test_Share。 您為共用區輸入的名稱也會用作磁碟區名稱。 共用名稱： <ul style="list-style-type: none"> • 必須是utf-8字串。 • 不得包含下列字元：控制字元：從0x00到0x1F（含）、0x22（雙引號）、以及特殊字元「\ ：（垂直列）<>+=；、？」
共用路徑	<ul style="list-style-type: none"> • 按一下欄位以輸入新的檔案系統路徑、例如/。 • 按兩下欄位、從現有檔案系統路徑清單中選取。

6. 當您對輸入項目感到滿意時、請按一下*確定*。

此功能可在SVM上建立SMB共用區。SnapCenter

刪除SMB共用區

您可以在不再需要SMB共用時刪除它。

步驟

1. 在左側導覽窗格中、按一下*主機*。
2. 在「主機」頁面中、按一下「共用」。
3. 在「共用」頁面中、按一下*儲存虛擬機器*欄位、顯示下拉式清單、其中包含可用的儲存虛擬機器（SVM）、然後選取您要刪除之共用的SVM。
4. 從SVM上的共用清單中、選取您要刪除的共用、然後按一下*刪除*。
5. 在刪除共用對話方塊中、按一下*確定*。

支援從SVM刪除SMB共用區。SnapCenter

雖然NTFS會在刪除或修改檔案時追蹤LUN上的可用空間、但不會向儲存系統報告新資訊。您可以在Windows主機的外掛程式上執行空間回收PowerShell Cmdlet、以確保新釋出的區塊已標示為可用於儲存設備。

如果您是在遠端外掛程式主機上執行Cmdlet、則必須執行SnapCenterOpen-SMConnection Cmdlet、才能開啟SnapCenter 連線至該伺服器。

開始之前

- 在執行還原作業之前、您必須確保空間回收程序已完成。
- 如果LUN由Windows Server容錯移轉叢集中的主機共用、則必須在擁有叢集群組的主機上執行空間回收。
- 為了獲得最佳儲存效能、您應該儘可能頻繁地執行空間回收。

您應確保已掃描整個NTFS檔案系統。

關於此工作

- 空間回收既耗時又佔用大量CPU資源、因此通常最好是在儲存系統和Windows主機使用率較低時執行作業。
- 空間回收幾乎可回收所有可用空間、但不能100%回收。
- 您不應在執行空間回收的同時執行磁碟重組。

這樣做可能會拖慢回收程序。

步驟

在應用程式伺服器PowerShell命令提示字元中、輸入下列命令：

```
「Invoke (叫用) SdHostVolume空間Reclaim -Path drive_path (叫用)」
```

drive_path是對應至LUN的磁碟機路徑。

使用PowerShell Cmdlet來配置儲存設備

如果您不想使用 SnapCenter GUI 執行主機設定和空間回收作業，則可以使用 PowerShell cmdlet。您可以直接使用Cmdlet或將Cmdlet新增至指令碼。

如果您是在遠端外掛程式主機上執行Cmdlet、則必須執行SnapCenter 《The支援不中斷連線指令程式》、才能開啟與SnapCenter 該伺服器的連線。

您可以執行_Get-Help命令name_來取得可搭配Cmdlet使用之參數及其說明的相關資訊。或者、您也可以參閱"[《軟件指令程式參考指南》 SnapCenter](#)"。

如果SnapCenter 由於從SnapDrive 伺服器移除適用於Windows的功能、導致無法使用任何版本的功能、請參閱"[解除安裝適用於Windows的功能時、無法使用的Cmdlet SnapCenter SnapDrive](#)"。

在VMware環境中配置儲存設備

您可以在 VMware 環境中使用適用於 Microsoft Windows 的 SnapCenter 外掛程式來建立和管理 LUN、以及管理快照。

支援的VMware來賓作業系統平台

- 支援的Windows Server版本
- Microsoft叢集組態

使用Microsoft iSCSI軟體啟動器時、VMware最多支援16個節點、或使用FC最多支援兩個節點

- RDM LUN

對於一般RDM、最多可支援56個RDM LUN、四個LSI Logic SCSI控制器、或是在VMware VM的Windows組態中、使用三個LSI Logic SCSI控制器的42個RDM LUN

支援VMware半虛擬SCSI控制器。RDM磁碟可支援256個磁碟。

VMware ESXi伺服器相關限制

- 不支援在使用ESXi認證的虛擬機器上、於Microsoft叢集上安裝Windows外掛程式。
在叢集式虛擬機器上安裝Windows外掛程式時、您應該使用vCenter認證。
- 所有叢集式節點都必須使用相同的目標ID（位於虛擬SCSI介面卡上）來處理同一個叢集式磁碟。
- 當您在外掛程式for Windows之外建立RDM LUN時、必須重新啟動外掛程式服務、使其能夠辨識新建立的磁碟。
- 您無法在VMware來賓作業系統上同時使用iSCSI和FC啟動器。

執行不必要的vCenter權限SnapCenter

您應該在主機上擁有下列vCenter權限、以便在客體作業系統中執行RDM作業：

- 資料存放區：移除檔案
- 主機：組態>儲存分割區組態
- 虛擬機器：組態

您必須將這些權限指派給Virtual Center Server層級的角色。您指派這些權限的角色無法指派給沒有root權限的任何使用者。

指派這些權限之後、您就可以在客體作業系統上安裝Windows外掛程式。

管理Microsoft叢集中的FC RDM LUN

您可以使用Windows外掛程式來管理使用FC RDM LUN的Microsoft叢集、但必須先在外掛程式之外建立共用的RDM仲裁和共用儲存設備、然後將磁碟新增至叢集的虛擬機器。

從ESXi 5.5開始、您也可以使用ESX iSCSI和FCoE硬體來管理Microsoft叢集。適用於Windows的外掛程式包

含Microsoft叢集的隨裝即用支援。

需求

當您符合特定組態需求時、適用於Windows的外掛程式會在兩部不同的虛擬機器上使用FC RDM LUN來支援Microsoft叢集、這些虛擬機器屬於兩部不同的ESX或ESXi伺服器、也稱為跨機箱叢集。

- 虛擬機器 (VM) 必須執行相同的Windows Server版本。
- 每個VMware父主機的ESX或ESXi伺服器版本必須相同。
- 每個父主機必須至少有兩個網路介面卡。
- 兩部ESX或ESXi伺服器之間必須至少共用一個VMware虛擬機器檔案系統 (VMFS) 資料存放區。
- VMware建議在FC SAN上建立共用資料存放區。

如有必要、也可透過iSCSI建立共用資料存放區。

- 共享的RDM LUN必須處於實體相容模式。
- 共享的RDM LUN必須在Windows的外掛程式之外手動建立。

您無法將虛擬磁碟用於共享儲存設備。

- 叢集中的每個虛擬機器上、必須以實體相容模式設定SCSI控制器：

Windows Server 2008 R2要求您在每個虛擬機器上設定LSI Logic SAS SCSI控制器。如果現有的LSI Logic SAS控制器只有其中一種類型存在、且已連接至C：磁碟機、則共享LUN無法使用。

VMware Microsoft叢集不支援半虛擬化類型的SCSI控制器。



在實體相容模式下、將SCSI控制器新增至虛擬機器上的共享LUN時、您必須在VMware Infrastructure Client中選取*原始裝置對應* (RDM) 選項、而非*建立新磁碟*選項。

- Microsoft虛擬機器叢集不能是VMware叢集的一部分。
- 在屬於Microsoft叢集的虛擬機器上安裝Windows外掛程式時、您必須使用vCenter認證、而非ESX或ESXi認證。
- Windows外掛程式無法使用多個主機的啟動器建立單一igroup。

必須先在儲存控制器上建立包含所有ESXi主機啟動器的igroup、然後再建立將用作共用叢集磁碟的RDM LUN。

- 請確定您使用FC啟動器在ESXi 5.0上建立RDM LUN。

建立RDM LUN時、會使用ALUA建立啟動器群組。

限制

適用於Windows的外掛程式可在屬於不同ESX或ESXi伺服器的不同虛擬機器上、使用FC/iSCSI RDM LUN來支援Microsoft叢集。



ESX 5.5i之前的版本不支援此功能。

- Windows外掛程式不支援ESX iSCSI和NFS資料存放區上的叢集。
- Windows外掛程式不支援叢集環境中的混合啟動器。

啟動器必須是FC或Microsoft iSCSI、但不能同時是兩者。

- Microsoft叢集中的共享磁碟不支援ESX iSCSI啟動器和HBA。
- 如果虛擬機器是Microsoft叢集的一部分、則適用於Windows的外掛程式不支援使用VMotion進行虛擬機器移轉。
- Windows外掛程式不支援Microsoft叢集中虛擬機器上的MPIO。

建立共享的FC RDM LUN

在使用FC RDM LUN在Microsoft叢集中的節點之間共用儲存設備之前、您必須先建立共用仲裁磁碟和共用儲存磁碟、然後將它們新增至叢集中的兩個虛擬機器。

共享磁碟並非使用 Plug-in for Windows 建立。您需要建立共用 LUN，然後將其新增至叢集中的每個虛擬機器。

相關資訊

請參閱 "[Broadcom 技術文件](#)" 並搜尋有關跨實體主機對虛擬機器進行叢集以及為 Microsoft 叢集建立共用 FC RDM LUN 的文件。

新增SnapCenter 以控制器為基礎的功能

如果您使用的是 FAS、AFF 或 ASA 儲存控制器、則需要 SnapCenter 標準控制器型授權。

控制器型授權具有下列特性：

- 隨附於購買Premium或Flash產品組合的標準授權（不含基礎套件）SnapCenter
- 無限使用儲存設備
- 使用ONTAP系統管理器或ONTAP CLI 直接加入到FAS、AFF或ASA儲存控制器。



您無需在SnapCenter使用者介面中輸入基於SnapCenter控制器的授權的任何授權資訊。

- 鎖定至控制器的序號

如需所需授權的相關資訊，請參閱 "[不需要授權SnapCenter](#)"。

步驟 1：確認是否已安裝 SnapManager 套件授權

您可以使用SnapCenter使用者介面檢查FAS、AFF或ASA主儲存系統上是否安裝了SnapManager Suite 許可證，並確定哪些系統需要許可證。SnapManager Suite 授權僅適用於主儲存系統上的FAS、AFF和ASA SVM 或叢集。



如果您的控制器上已有SnapManager Suite 許可證， SnapCenter會自動提供基於標準控制器的授權授權。 SnapManagerSuite 授權和基於SnapCenter Standard 控制器的授權這兩個名稱可以互換使用，但它們指的是同一個授權。

步驟

1. 在左導覽窗格中、選取 * 儲存系統 * 。
2. 在「儲存系統」頁面的「類型」下拉式清單中、選取是否要檢視所有新增的SVM或叢集：
 - 若要檢視所有新增的SVM、請選取* ONTAP 《SVMS*》。
 - 若要檢視所有已新增的叢集、請選取* ONTAP 《叢集》*。

當您選取叢集名稱時、屬於叢集一部分的所有 SVM 都會顯示在儲存虛擬機器區段中。

3. 在Storage Connections (儲存連線) 清單中、找到Controller License (控制器授權) 欄。

「Controller License」 (控制器授權) 欄會顯示下列狀態：

-  表示 SnapManager 套件授權已安裝在 FAS 、 AFF 或 ASA 主儲存系統上。
-  表示 SnapManager 套件授權未安裝在 FAS 、 AFF 或 ASA 主儲存系統上。
- 不適用表示 SnapManager 套件授權不適用、因為儲存控制器位於 Amazon FSX for NetApp ONTAP 、 Cloud Volumes ONTAP 、 ONTAP Select 或次要儲存平台上。

步驟 2：識別安裝在控制器上的授權

您可以使用ONTAP 效益指令列來檢視控制器上安裝的所有授權。您應該是 FAS 、 AFF 或 ASA 系統上的叢集管理員。



控制器將基於SnapCenter Standard 控制器的授權顯示為 SnapManagerSuite 授權。

步驟

1. 使用ONTAP flexline命令列登入NetApp控制器。
2. 輸入 license show 命令，然後查看輸出以查看是否已安裝 SnapManagerSuite 授權。

輸出範例

```
cluster1::> license show
(system license show)

Serial Number: 1-80-0000xx
Owner: cluster1
Package          Type          Description          Expiration
-----
Base             site         Cluster Base License -

Serial Number: 1-81-00000000000000000000000000xx
Owner: cluster1-01
Package          Type          Description          Expiration
-----
NFS              license      NFS License         -
CIFS             license      CIFS License        -
iSCSI           license      iSCSI License       -
FCP              license      FCP License         -
SnapRestore     license      SnapRestore License -
SnapMirror      license      SnapMirror License  -
FlexClone       license      FlexClone License   -
SnapVault       license      SnapVault License   -
SnapManagerSuite license      SnapManagerSuite License -
```

在此範例中、SnapManagerSuite授權已安裝、因此不SnapCenter 需要執行其他的功能驗證動作。

步驟 3：擷取控制器序號

使用ONTAP命令列取得控制器序號。您必須是FAS、AFF或ASA系統上的叢集管理員才能取得基於控制器的許可證序號。

步驟

1. 使用ONTAP flexline命令列登入控制器。
2. 輸入system show -instance命令、然後檢閱輸出以找出控制器序號。

輸出範例

```
cluster1::> system show -instance

Node: fasxxxx-xx-xx-xx
Owner:
Location: RTP 1.5
Model: FAS8080
Serial Number: 123451234511
Asset Tag: -
Uptime: 143 days 23:46
NVRAM System ID: xxxxxxxxxx
System ID: xxxxxxxxxx
Vendor: NetApp
Health: true
Eligibility: true
Differentiated Services: false
All-Flash Optimized: false

Node: fas8080-41-42-02
Owner:
Location: RTP 1.5
Model: FAS8080
Serial Number: 123451234512
Asset Tag: -
Uptime: 144 days 00:08
NVRAM System ID: xxxxxxxxxx
System ID: xxxxxxxxxx
Vendor: NetApp
Health: true
Eligibility: true
Differentiated Services: false
All-Flash Optimized: false
2 entries were displayed.
```

3. 記錄序號。

步驟 4：擷取控制器型授權的序號

如果您使用的是FAS、ASA或AFF存儲，則可以先從NetApp支援站點擷取基於SnapCenter控制器的許可證，然後再使用ONTAP命令列進行安裝。

開始之前

- 您應該擁有有效的NetApp支援網站登入認證資料。

如果您沒有輸入有效的憑證，系統將不會傳回任何有關您搜尋的資訊。

- 您應該有控制器序號。

步驟

1. 登入 "NetApp 支援網站"。
2. 瀏覽至* Systems > Software Licenses*。
3. 在「選擇條件」區域中、確認已選取序號（位於裝置背面）、輸入控制器序號、然後選取「Go!」。

Software Licenses

Selection Criteria

Choose a method by which to search

- ▶ Serial Number (located on back of unit) ▾ Enter Value: Go!

Enter the Cluster Serial Number value without dashes.

- OR -

- ▶ Show Me All: Serial Numbers with Licenses ▾ For Company: Go!

隨即顯示指定控制器的授權清單。

4. 找出SnapCenter 並記錄《不實的標準版》或SnapManagerSuite授權。

步驟 5：新增控制器型授權

當您使用 FAS、AFF 或 ASA 系統、並且擁有 SnapCenter Standard 或 SnapManagerSuite 授權時、您可以使用 ONTAP 命令列來新增 SnapCenter 控制器型授權。

開始之前

- 您應該是 FAS、AFF 或 ASA 系統上的叢集管理員。
- 您應該擁有 SnapCenter 「不含任何功能的標準版」或「SnapManagerSuite」授權。

關於這項工作

如果您想要試用 FAS、AFF 或 ASA 儲存設備來安裝 SnapCenter、您可以取得優質產品組合評估授權、以便在控制器上安裝。

如果您想 SnapCenter 要試用版安裝、請聯絡您的銷售代表、以取得 Premium 產品組合評估授權、以便安裝在您的控制器上。

步驟

1. 使用 ONTAP flexline 命令列登入 NetApp 叢集。
2. 新增 SnapManagerSuite 授權金鑰：

「系統授權新增-授權碼 license_key」

此命令可在管理權限層級使用。

3. 確認SnapManagerSuite授權已安裝：

《許可證展示》

步驟 6：移除試用授權

如果您正在使用基於控制器的SnapCenter標準許可證，並且需要刪除基於容量的試用許可證（序號以「50」結尾），則應使用 MySQL 命令手動刪除試用許可證。無法使用SnapCenter使用者介面刪除試用許可證。



只有在使用SnapCenter 以VMware控制器為基礎的授權時、才需要手動移除試用授權。

步驟

1. 在伺服器SnapCenter 器上、開啟PowerShell視窗以重設MySQL密碼。
 - a. 執行 Open-SmConnection cmdlet 為 SnapCenterAdmin 帳戶與SnapCenter伺服器建立連線。
 - b. 執行Set-SmRegistryPassword以重設MySQL密碼。

有關 cmdlet 的信息，請參閱 "[《軟件指令程式參考指南》 SnapCenter](#)"。

2. 開啟命令提示字元並執行mysql -u root -p以登入MySQL。

MySQL會提示您輸入密碼。輸入您在重設密碼時提供的認證資料。

3. 從資料庫移除試用授權：

```
use nsm;DELETE FROM nsm_License WHERE nsm_License_Serial_Number='510000050';
```

設定高可用度

設定 SnapCenter 伺服器的高可用度

若要在 Windows 或 Linux 上執行的 SnapCenter 中支援高可用度（HA），您可以安裝 F5 負載平衡器。在同SnapCenter 一位置的最多兩部主機中、使用F5可支援主動-被動組態。若要在SnapCenter 整個過程中使用F5負載平衡器、您應該設定SnapCenter 「伺服器」並設定「F5負載平衡器」。

您也可以設定網路負載平衡（NLB）來設定 SnapCenter 高可用度。您應該在 SnapCenter 安裝之外手動設定 NLB，以獲得高可用度。

對於雲端環境，您可以使用 Amazon Web Services（AWS）Elastic Load Balancing（Elb）和 Azure 負載平衡器來設定高可用度。

使用F5設定高可用度

有關使用 F5 負載平衡器設定SnapCenter伺服器以實現高可用性的說明，請參閱 ["如何使用SnapCenter F5 負載平衡器設定高可用度的功能"](#)。

您必須是SnapCenter 本機「管理員」群組的成員（除了指派給SnapCenterAdmin角色之外）、才能使用下列Cmdlet來新增和移除F5叢集：

- add-SmServerCluster
- add-SmServer
- 移除SmServerCluster

如需詳細資訊、請 "[《軟件指令程式參考指南》 SnapCenter](#)"參閱。

其他資訊

- 安裝並設定SnapCenter 好高可用度的功能後、請編輯SnapCenter 「不間斷」桌面捷徑、以指向F5叢集IP。
- 如果SnapCenter 在伺服器之間發生容錯移轉、而且還有現有SnapCenter 的故障恢復工作階段、您必須關閉瀏覽器並SnapCenter 重新登入。
- 在負載平衡器設定（NLB 或 F5）中，如果您新增的主機有部分由 NLB 或 F5 主機解析，而且 SnapCenter 主機無法連線至此主機，則 SnapCenter 主機頁面會經常在主機停機和執行中狀態之間切換。若要解決此問題，您應該確定兩台 SnapCenter 主機都能解決 NLB 或 F5 主機中的主機問題。
- MFA 設定的 SnapCenter 命令應在所有主機上執行。依賴方組態應在Active Directory Federation Services (AD FS) 伺服器中使用F5叢集詳細資料進行。啟用 MFA 之後，主機層級的 SnapCenter UI 存取將會遭到封鎖。
- 在容錯移轉期間，稽核記錄設定不會反映在第二部主機上。因此，您應該在 F5 被動式主機變成主動式時，手動重複稽核記錄設定。

使用網路負載平衡（NLB）設定高可用度

您可以設定網路負載平衡（NLB）來設定 SnapCenter 高可用度。您應該在 SnapCenter 安裝之外手動設定 NLB，以獲得高可用度。

如需如何使用 SnapCenter 設定網路負載平衡（NLB）的相關資訊，請參閱 ["如何使用SnapCenter 功能進行NLB設定"](#)。

使用 AWS 彈性負載平衡（Elastic Load Balancing）設定高可用度

您可以在 Amazon Web Services（AWS）中設定高可用度 SnapCenter 環境，方法是在不同的可用性區域（AZs）中設定兩部 SnapCenter 伺服器，並將它們設定為自動容錯移轉。此架構包括虛擬私有 IP 位址，路由表，以及作用中和待命 MySQL 資料庫之間的同步處理。

步驟

1. 在 AWS 中設定虛擬私有重疊 IP。如需相關資訊、請 "[設定虛擬私有覆蓋 IP](#)"參閱。
2. 準備 Windows 主機
 - a. 強制將 IPv4 排定優先順序高於 IPv6：
 - 位置：HKLM\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters

- 金鑰： DisabledComponents
 - 鍵入： reg_dWord
 - 值： 0x20
- b. 請確定完整網域名稱可透過 DNS 或本機主機組態解析至 IPv4 位址。
 - c. 請確定您尚未設定系統 Proxy 。
 - d. 如果在沒有 Active Directory 的情況下使用安裝程式，且伺服器不在同一個網域中，請確定 Windows Server 上的管理員密碼相同。
 - e. 在兩部 Windows Server 上新增虛擬 IP 。
3. 建立 SnapCenter 叢集。
 - a. 啟動 PowerShell 並連線至 SnapCenter 。 `Open-SmConnection`
 - b. 建立叢集。 `Add-SmServerCluster -ClusterName <cluster_name> -ClusterIP <cluster_ip> -PrimarySCServerIP <primary_ip> -Verbose -Credential administrator`
 - c. 新增次要伺服器。 `Add-SmServer -ServerName <server_name> -ServerIP <server_ip> -CleanUpSecondaryServer -Verbose -Credential administrator`
 - d. 取得高可用度詳細資料。 `Get-SmServerConfig`
 4. 建立 Leda 功能，以在虛擬私有 IP 端點無法使用時調整路由表，並由 AWS CloudWatch 監控。如需相關資訊、請 ["建立 Lambda 函數"](#)參閱。
 5. 在 CloudWatch 中建立監控器，以監控 SnapCenter 端點的可用度。如果端點無法連線，則會設定警示來觸發 Lambda 功能。Lambda 功能可調整路由表，將流量重新導向至作用中的 SnapCenter 伺服器。如需相關資訊、請 ["建立合成炮"](#)參閱。
 6. 使用步驟功能來實作工作流程，作為 CloudWatch 監控的替代方案，可縮短容錯移轉時間。此工作流程包含 Lambda 探查功能，可測試 SnapCenter URL ，用於儲存故障計數的 DynamoDB 表格，以及 Step 功能本身。
 - a. 使用 lambda 函數來探查 SnapCenter URL 。如需相關資訊、請 ["建立 Lambda 函數"](#)參閱。
 - b. 建立一個 DynamoDB 表格，用於在兩個 Step 函數迭代之間儲存失敗計數。如需相關資訊、請 ["從 DynamoDB 表開始"](#)參閱。
 - c. 建立 Step 功能。如需相關資訊、請 ["步驟功能文件"](#)參閱。
 - d. 測試單一步驟。
 - e. 測試完整功能。
 - f. 建立 IAM 角色，並調整允許執行 Lambda 功能的權限。
 - g. 建立觸發步驟功能的排程。如需相關資訊、請 ["使用 Amazon EventBridge 排程器啟動「步驟」功能"](#)參閱。

使用 Azure 負載平衡器設定高可用度

您可以使用 Azure 負載平衡器來設定高可用度 SnapCenter 環境。

步驟

1. 使用 Azure 入口網站，在規模集中建立虛擬機器。Azure 虛擬機器磅秤集可讓您建立及管理一組負載平衡的虛擬機器。虛擬機器執行個體的數量可以自動增加或減少，以因應需求或定義的排程。如需相關資訊、請 ["使用 Azure 入口網站，在規模集中建立虛擬機器"](#)參閱。

2. 設定虛擬機器之後，請登入 VM Set 中的每個虛擬機器，然後在兩個節點中安裝 SnapCenter Server。
3. 在主機 1 中建立叢集。Add-SmServerCluster -ClusterName <cluster_name> -ClusterIP <specify the load balancer front end virtual ip> -PrimarySCServerIP <ip address> -Verbose -Credential <credentials>
4. 新增次要伺服器。Add-SmServer -ServerName <name of node2> -ServerIP <ip address of node2> -Verbose -Credential <credentials>
5. 取得高可用度詳細資料。Get-SmServerConfig
6. 如有需要，請重新建置次要主機。Set-SmRepositoryConfig -RebuildSlave -Verbose
7. 容錯移轉至第二個主機。Set-SmRepositoryConfig ActiveMaster <name of node2> -Verbose

= 從 NLB 切換至 F5 以獲得高可用度

您可以將SnapCenter 您的「叢集HA」組態從「網路負載平衡」（NLB）變更為使用「5負載平衡器」。

步驟

1. 使用SnapCenter F5設定高可用度的功能。"深入瞭解"。
2. 在支援服務器的支援主機上、啟動PowerShell。SnapCenter
3. 使用Open-SmConnection Cmdlet啟動工作階段、然後輸入認證資料。
4. 使用SnapCenter update-SmServerCluster Cmdlet更新支援服務器、使其指向F5叢集IP位址。

您可以執行_Get-Help命令name_來取得可搭配Cmdlet使用之參數及其說明的相關資訊。或者、您也可以參閱 "[《軟件指令程式參考指南》 SnapCenter](#)"。

高可用度：**SnapCenter** 適用於**MySQL**的功能

MySQL複寫是MySQL Server的一項功能、可讓您將資料從一個MySQL資料庫伺服器（主要）複寫到另一個MySQL資料庫伺服器（從屬）。支援MySQL複寫、只能在兩個啟用網路負載平衡（啟用NLB）的節點上提供高可用度。SnapCenter

當主要儲存庫發生故障時、系統會在主要儲存庫上執行讀取或寫入作業、並將其連線傳送至從屬儲存庫。SnapCenter從屬儲存庫隨即成為主要儲存庫。支援反轉複寫、僅在容錯移轉期間啟用。SnapCenter

若要使用MySQL高可用度（HA）功能、您必須在第一個節點上設定網路負載平衡器（NLB）。MySQL儲存庫會安裝在此節點上、做為安裝的一部分。在SnapCenter 第二個節點上安裝時、您必須加入第一個節點的F5、並在第二個節點上建立MySQL儲存庫的複本。

提供_Get-SmrepositoryConfig_和_Set-SmrepositoryConfig_ PowerShell Cmdlet來管理MySQL複寫。SnapCenter

您可以執行_Get-Help命令name_來取得可搭配Cmdlet使用之參數及其說明的相關資訊。或者、您也可以參閱 "[《軟件指令程式參考指南》 SnapCenter](#)"。

您必須瞭解MySQL HA功能的相關限制：

- NLB和MySQL HA不支援超過兩個節點。
- 不支援從SnapCenter 不支援使用支援功能的獨立安裝切換至NLB安裝、或從MySQL獨立安裝切換至MySQL HA。
- 如果從屬儲存庫資料未與主要儲存庫資料同步、則不支援自動容錯移轉。

您可以使用 `_Set-SmRegistryConfig_ Cmdlet` 來啟動強制容錯移轉。

- 啟動容錯移轉時、執行中的工作可能會失敗。

如果發生容錯移轉是因為MySQL Server或SnapCenter 現象伺服器停機、則執行中的任何工作都可能失敗。容錯移轉至第二個節點之後、所有後續工作都會成功執行。

如需設定高可用度的相關資訊、請參閱 ["如何設定NLB與ARR SnapCenter 搭配使用功能"](#)。

設定角色型存取控制 (RBAC)

建立角色

除了使用現有SnapCenter 的功能、您還可以建立自己的角色、並自訂權限。

若要建立自己的角色、必須以「SnapCenterAdmin」角色登入。

步驟

1. 在左側導覽窗格中、按一下*設定*。
2. 在「設定」頁面中、按一下「角色」。
3. 按一下 。
4. 為新角色指定名稱和描述。



使用者名稱和群組名稱中只能使用以下特殊字元：空格 ()、連字號 (-)、底線 (_) 和冒號 (:)。

5. 選取*此角色的所有成員都可以看到其他成員的物件*、以便其他角色成員在重新整理資源清單之後、能夠查看資源、例如磁碟區和主機。

如果不希望此角色的成員看到指派給其他成員的物件、則應取消選取此選項。



啟用此選項時、如果使用者與建立物件或資源的使用者具有相同角色、則不需要指派使用者存取物件或資源的權限。

6. 在「權限」頁面中、選取您要指派給該角色的權限、或按一下*全選*、將所有權限授予該角色。
7. 按一下*提交*。

使用安全登入命令新增 NetApp ONTAP RBAC 角色

當儲存系統執行叢集式 ONTAP 時、您可以使用安全登入命令來新增 NetApp ONTAP RBAC 角色。

開始之前

- 確定您要執行的任務以及執行這些任務所需的權限。
- 授予命令和（或）命令目錄的權限。

每個命令/命令目錄都有兩種存取層級：All存取和唯讀。

您必須一律先指派所有存取權限。

- 指派角色給使用者。
- 根據您的 SnapCenter 外掛程式是連接到整個叢集的叢集管理員 IP 還是直接連接到叢集內的 SVM 來確定您的配置。

關於這項工作

為了簡化儲存系統上這些角色的配置，您可以使用 NetApp ONTAP 的 RBAC 使用者建立器工具，該工具發佈在 NetApp 社群論壇上。

此工具會自動ONTAP 正確處理設定功能不正確的功能。例如， NetApp ONTAP 的 RBAC 使用者建立工具會以正確順序自動新增 Privileges ，讓 All Access Privileges 最先出現。如果您先新增唯讀權限、然後新增全存取權限、ONTAP 則將全存取權限標示為重複、並予以忽略。



如果您稍後升級 SnapCenter 或 ONTAP ，則應重新執行 RBAC User Creator for NetApp ONTAP 工具，以更新您先前建立的使用者角色。為SnapCenter 舊版的版本的使用者角色無法ONTAP 在升級版本中正常運作。當您重新執行此工具時、它會自動處理升級作業。您不需要重新建立角色。

如需設定ONTAP RBAC角色的詳細資訊、請參閱 "[《Administrator驗證與RBAC電源指南》（英文） ONTAP](#)"。

步驟

1. 在儲存系統上、輸入下列命令以建立新角色：

```
「安全登入角色create <role名稱>>-cmd目錄名稱"command"-access all-vserver <Svm_name\>」
```

- SVM_name是SVM的名稱。如果您將此欄位保留空白、則預設為叢集管理員。
- role名稱是您為角色指定的名稱。
- Command ONTAP 是功能不一的功能。



您必須針對每個權限重複此命令。請記住、All Access命令必須在唯讀命令之前列出。

如需權限清單的相關資訊，請參閱 "[用於建立角色和指派權限的CLI命令ONTAP](#)"。

2. 輸入下列命令來建立使用者名稱：

```
「安全性登入建立-使用者名稱>-applicationontapi -authmethod <password\>-role <name_of_rouse_in_step_1\>-vserver <Svm_name\>-comment "user_description"」
```

- user_name是您要建立的使用者名稱。
- 是您的密碼。如果您未指定密碼、系統會提示您輸入密碼。
- SVM_name是SVM的名稱。

3. 輸入下列命令、將角色指派給使用者：

```
「安全性登入修改使用者名稱」：-vserver <Svm_name>-role <rose_name>-application-ontapi應用程式主控台-authmethod <password>`
```

- 是您在步驟2中建立的使用者名稱。此命令可讓您修改使用者、使其與角色建立關聯。
- SVM_name>是SVM的名稱。
- <role名稱>是您在步驟1中建立的角色名稱。
- 是您的密碼。如果您未指定密碼、系統會提示您輸入密碼。

4. 輸入下列命令、確認使用者已正確建立：

```
「安全登入show-vserver <Svm_name>-user-or group name <user_name>」
```

user_name是您在步驟3中建立的使用者名稱。

以最低權限建立SVM角色

在這個功能中為新的SVM使用者建立角色時、您必須執行幾ONTAP 個SfCLI命令ONTAP。如果您將SVM設定ONTAP 為搭配SnapCenter 使用、但不想使用vsadmin角色、則需要此角色。

步驟

1. 在儲存系統上、建立角色並將所有權限指派給該角色。

```
「安全登入角色create-vserver <Svm_name>- role <Svm_rouse_Name>-cmd目錄名稱<permission>」
```



您應該針對每個權限重複此命令。

2. 建立使用者並將角色指派給該使用者。

```
「安全性登入建立-使用者<user_name>>-vserver <Svm_name>-應用程式ontapi -auth方法 密碼-role <Svm_rouse_Name>」
```

3. 解除鎖定使用者。

```
「安全登入解除鎖定-使用者<user_name>-vserver <Svm_name>」
```

用於建立SVM角色和指派權限的CLI命令ONTAP

您應該執行幾ONTAP 個SVM命令來建立SVM角色並指派權限。

- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror list-destinations" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "event generate-autosupport-log" -access all
- 「安全登入角色create -vserver Svm_Name -role Svm_rouse_Name -cmd目錄名稱 「jobhistory show」

-access all」

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "job show" -access all
- 「安全登入角色create -vserver Svm_Name -role Svm_rouse_Name -cmd目錄名稱「jobstop」 -access all」
- 「安全登入角色create -vserver Svm_Name -role Svm_rouse_Name -cmd目錄名稱"LUN"-access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱"LUN cree"-access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱"lun刪除"-access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rou_name -cmd目錄名稱"LUN igroup add"-access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rou_name -cmd目錄名稱"LUN igroup cree"-access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rou_name -cmd目錄名稱"LUN igroup delete"-access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rou_name -cmd目錄名稱"LUN igroup rame"-access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rou_name -cmd目錄名稱"LUN igroup show"-access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「LUN mapping add-report-nodes」 -access all」
- 「安全登入角色create -vserver Svm_Name -role Svm_rouse_Name -cmd目錄名稱「LUN mapping create」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「LUN mapping delete」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「LUN mapping remove-reporting節點」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「LUN mapping show」 -access all」
- 「安全性登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「LUN modify」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「LUN move-in Volume」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「lun offline」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「LUN online」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「LUN resize」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱"LUN serial」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱"LUN show"-access all」
- 「安全登入角色create -vserver Svm_Name -role Svm_road_Name -cmd目錄名稱「network interface」 -access readonly」

- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「SnapMirror原則附加規則」-access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「SnapMirror原則modify-rRule」-access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「SnapMirror原則移除規則」-access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「SnapMirror原則show」-access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「SnapMirror還原」-access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱"SnapMirror show"-access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「SnapMirror show-history」-access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「SnapMirror update」-access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「SnapMirror update-ls-set」-access all」
- 「安全性登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「version」-access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「volume clone create」-access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「volume clone show」-access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「volume clone s折分start」-access all」
- 「安全性登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「Volume clone split stop」-access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「volume create」-access all」
- 「安全性登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「volume destrole」-access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「volume file clone create」-access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「volume file show-disk-usage」-access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「volume modify」-access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「volume offline」-access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「volume online」-access all」

- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「volume qtree create」-access all」
- 「安全性登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱"volume qtree delete"-access all"
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「volume qtree modify」-access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rous_Name -cmd目錄名稱"volume qtree show"-access all"
- 「安全登入角色create -vserver Svm_name -role Svm_rous_Name -cmd目錄名稱「volume restrict」-access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rous_Name -cmd目錄名稱「volume show」-access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rous_Name -cmd目錄名稱「volume snapshot create」-access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rous_Name -cmd目錄名稱「volume snapshot delete」-access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「volume snapshot modify」-access all」
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume snapshot modify-snaplock-expiry-time" -access all
- 「安全登入角色create -vserver Svm_name -role Svm_rous_Name -cmd目錄名稱「volume snapshot rame」-access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rous_Name -cmd目錄名稱「Volume snapshot還原」-access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rous_Name -cmd目錄名稱「Volume snapshot還原檔案」-access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rous_Name -cmd目錄名稱「volume snapshot show」-access all」
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show-delta" -access all
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「volume unmount」-access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rous_Name -cmd目錄名稱「vserver CIFS共用create」-access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rous_Name -cmd目錄名稱「vserver CIFS共用刪除」-access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rous_Name -cmd目錄名稱「vserver CIFS共用show」-access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rous_Name -cmd目錄名稱「vserver CIFS show」-access all」
- 「安全性登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「vserver EXECION-policy create」-access all」

- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「vserver EXECUTE-Fpolicy DELETE」 -access all」
- 「安全性登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「vserver匯出原則規則create」 -access all」
- 「安全性登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「vserver匯出原則規則show」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「vserver EXECUTE-Fpolicy show」 -access all」
- 「安全登入角色create -vserver Svm_Name -role Svm_rous_Name -cmd目錄名稱「vserver iSCSI connection show」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_road_Name -cmd目錄名稱"vserver"-access readonly」
- 「安全性登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「vserver EXECUTE-policy」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rous_Name -cmd目錄名稱「vserver iSCSI」 -access all」
- 「安全性登入角色create -vserver Svm_Name -role Svm_rous_Name -cmd目錄名稱「Volume Clone分割狀態」 -access all」
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume managed-feature" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem map" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem create" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem delete" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem host" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem controller" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace create" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace delete" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace show" -access all

為 ASA R2 系統建立 SVM 角色

您必須執行多個ONTAP CLI 命令才能在ASA r2 系統中為新的 SVM 使用者建立角色。如果您在ASA r2 系統中設定 SVM 以與SnapCenter一起使用且不想使用 vsadmin 角色，則需要此角色。

步驟

1. 在儲存系統上、建立角色並將所有權限指派給該角色。

```
「安全登入角色create-vserver <Svm_name>- role <Svm_rouse_Name>-cmd目錄名稱<permission>」
```



您應該針對每個權限重複此命令。

2. 建立使用者並將角色指派給該使用者。

```
security login create -user <user_name> -vserver <svm_name> -application  
http -authmethod password -role <SVM_Role_Name>
```

3. 解除鎖定使用者。

```
「安全登入解除鎖定-使用者<user_name>-vserver <Svm_name>」
```

用於建立SVM角色和指派權限的CLI命令ONTAP

您應該執行幾ONTAP 個SVM命令來建立SVM角色並指派權限。

- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror list-destinations" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "event generate-autosupport-log" -access all
- 「安全登入角色create -vserver Svm_Name -role Svm_rouse_Name -cmd目錄名稱「jobhistory show」 -access all」
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "job show" -access all
- 「安全登入角色create -vserver Svm_Name -role Svm_rouse_Name -cmd目錄名稱「jobstop」 -access all」
- 「安全登入角色create -vserver Svm_Name -role Svm_rouse_Name -cmd目錄名稱"LUN"-access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱"LUN cree"-access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱"lun刪除"-access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rou_name -cmd目錄名稱"LUN igroup add"-access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rou_name -cmd目錄名稱"LUN igroup cree"-access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rou_name -cmd目錄名稱"LUN igroup delete"-access all」

- 「安全登入角色create -vserver Svm_name -role Svm_rou_name -cmd目錄名稱"LUN igroup rame"-access all"
- 「安全登入角色create -vserver Svm_name -role Svm_rou_name -cmd目錄名稱"LUN igroup show"-access all"
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「LUN mapping add-report-nodes」 -access all」
- 「安全登入角色create -vserver Svm_Name -role Svm_rous_Name -cmd目錄名稱「LUN mapping create」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rous_Name -cmd目錄名稱「LUN mapping delete」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rous_Name -cmd目錄名稱「LUN mapping remove-reporting節點」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「LUN mapping show」 -access all」
- 「安全性登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「LUN modify」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rous_Name -cmd目錄名稱「LUN move-in Volume」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rous_Name -cmd目錄名稱「lun offline」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rous_Name -cmd目錄名稱「LUN online」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「LUN resize」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rous_Name -cmd目錄名稱"LUN serial」 -access all"
- 「安全登入角色create -vserver Svm_name -role Svm_rous_Name -cmd目錄名稱"LUN show"-access all"
- 「安全登入角色create -vserver Svm_Name -role Svm_road_Name -cmd目錄名稱「network interface」 -access readonly」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「SnapMirror原則附加規則」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「SnapMirror原則modify-rRule」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「SnapMirror原則移除規則」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rous_Name -cmd目錄名稱「SnapMirror原則show」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「SnapMirror還原」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rous_Name -cmd目錄名稱"SnapMirror show"-access all"
- 「安全登入角色create -vserver Svm_Name -role Svm_rous_Name -cmd目錄名稱「SnapMirror show-history」 -access all」

- 「安全登入角色create -vserver Svm_name -role Svm_rous_Name -cmd目錄名稱「SnapMirror update」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rous_Name -cmd目錄名稱「SnapMirror update-ls-set」 -access all」
- 「安全性登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「version」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rous_Name -cmd目錄名稱「volume clone create」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rous_Name -cmd目錄名稱「volume clone show」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rous_Name -cmd目錄名稱「volume clone s拆分start」 -access all」
- 「安全性登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「Volume clone split stop」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rous_Name -cmd目錄名稱「volume create」 -access all」
- 「安全性登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「volume destrole」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rous_Name -cmd目錄名稱「volume file clone create」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「volume file show-disk-usage」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「volume modify」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rous_Name -cmd目錄名稱「volume offline」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rous_Name -cmd目錄名稱「volume online」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「volume qtree create」 -access all」
- 「安全性登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱"volume qtree delete"-access all"
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「volume qtree modify」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rous_Name -cmd目錄名稱"volume qtree show"-access all"
- 「安全登入角色create -vserver Svm_name -role Svm_rous_Name -cmd目錄名稱「volume restrict」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rous_Name -cmd目錄名稱「volume show」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rous_Name -cmd目錄名稱「volume snapshot create」 -access all」

- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「volume snapshot delete」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「volume snapshot modify」 -access all」
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume snapshot modify-snaplock-expiry-time" -access all
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「volume snapshot rame」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「Volume snapshot還原」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「Volume snapshot還原檔案」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「volume snapshot show」 -access all」
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show-delta" -access all
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「volume unmount」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「vserver CIFS共用create」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「vserver CIFS共用刪除」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「vserver CIFS共用show」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「vserver CIFS show」 -access all」
- 「安全性登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「vserver EXEC-ON-policy create」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「vserver EXEC-Fpolicy DELETE」 -access all」
- 「安全性登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「vserver匯出原則規則create」 -access all」
- 「安全性登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「vserver匯出原則規則show」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「vserver EXEC-Fpolicy show」 -access all」
- 「安全登入角色create -vserver Svm_Name -role Svm_rouse_Name -cmd目錄名稱「vserver iSCSI connection show」 -access all」
- 「安全登入角色create -vserver Svm_name -role Svm_road_Name -cmd目錄名稱"vserver"-access readonly」
- 「安全性登入角色create -vserver Svm_name -role Svm_rouse_Name -cmd目錄名稱「vserver EXEC-policy」 -access all」

- 「安全登入角色create -vserver Svm_name -role Svm_rous_Name -cmd目錄名稱「vserver iSCSI」 -access all」
- 「安全性登入角色create -vserver Svm_Name -role Svm_rous_Name -cmd目錄名稱「Volume Clone分割狀態」 -access all」
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume managed-feature" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem map" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem create" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem delete" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem host" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem controller" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace create" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace delete" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "storage-unit show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "consistency-group" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror protect" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume delete" -access all
- security login create -user-or-group-name user_name -application http -authentication-method password -role SVM_Role_Name -vserver SVM_Name
- security login create -user-or-group-name user_name -application ssh -authentication-method password -role SVM_Role_Name -vserver SVM_Name

以ONTAP 最低權限建立叢集角色

您應該建立ONTAP 具有最低權限的支援功能、以便不必使用ONTAP 這個功能來SnapCenter 執行動作。您可以執行數ONTAP 個CLI命令來建立ONTAP 一個不含指令集的叢集角色、並指派最低權限。

步驟

1. 在儲存系統上、建立角色並將所有權限指派給該角色。

「安全登入角色create-vserver <cluster名稱>- role <role名稱>-cmd目錄名稱<permission>」



您應該針對每個權限重複此命令。

2. 建立使用者並將角色指派給該使用者。

```
security login create -user <user_name\> -vserver <cluster_name\> -application  
ontapi http -authmethod password -role <role_name\>
```

3. 解除鎖定使用者。

「安全登入解除鎖定-使用者<使用者名稱>-vserver <叢集名稱>」

用於建立叢集角色和指派權限的CLI命令ONTAP

您應該執行幾ONTAP 個CLI命令來建立叢集角色並指派權限。

- security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "metrocluster show" -access readonly
- security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "cluster identity modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster identity show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster peer show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "event generate-autosupport-log" -access all
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱「jobhistory show」 -access all」
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job show" -access all
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "jobstop" -access all」

- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱"LUN"-access all"
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱"LUN cree"-access all"
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱"lun刪除"-access all"
- 「安全登入角色create -vserver Cluster_name -role rou_name -cmd dirname "LUN igroup add"-access all"
- 「安全登入角色create -vserver Cluster_name -role rou_name -cmd dirname "LUN igroup cree"-access all"
- 「安全登入角色create -vserver Cluster_name -role rou_name -cmd dirname "LUN igroup delete"-access all"
- 「安全登入角色create -vserver Cluster_name -role rou_name -cmd dirname "LUN igroup modify"-access all"
- 「安全登入角色create -vserver Cluster_name -role rou_name -cmd dirname "LUN igroup rame"-access all"
- 「安全登入角色create -vserver Cluster_name -role rou_name -cmd dirname "LUN igroup show"-access all"
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd dirname 「LUN mapping add-report-nodes」 -access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱 「LUN mapping create」 -access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱 「LUN mapping delete」 -access all」
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd dirname 「LUN mapping remove-report-nodes」 -access all」
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱 「LUN mapping show」 -access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱"lun modify"-access all"
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "LUN move-in-volume」 -access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱"lun offline"-access all"
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱 「LUN online」 -access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "LUN永久性保留區Clear"-access all"
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱 「LUN resize」 -access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "LUN serial」 -access all」
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱"LUN show"-access all"
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname 「network interface create」 -access readonly」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname 「network interface delete」 -access readonly」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname 「network interface modify」 -access readonly」
- 「安全登入角色create -vserver Cluster_name -role road_Name -cmd dirname 「network interface show」 -access readonly」

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem map" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem host" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem controller" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace show" -access all
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname 「安全性登入」 -access readonly」
- 「安全登入角色create -role rose_Name -cmd目錄名稱"SnapMirror cree"-vserver Cluster_name -access all」
- 「安全登入角色create -role rose_Name -cmd目錄名稱"SnapMirror list-destinations"-vserver Cluster_name -access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname 「SnapMirror原則附加規則」 -access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱 「SnapMirror原則create」 -access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱 「SnapMirror原則刪除」 -access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱 「SnapMirror原則修改」 -access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱 「SnapMirror原則modify-rRule」 -access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱 「SnapMirror原則移除規則」 -access all」
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱 「SnapMirror原則show」 -access all」

- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱"SnapMirror還原"-access all"
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱"SnapMirror show"-access all"
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱「SnapMirror show-history」-access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱「SnapMirror update」-access all」
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd dirname「SnapMirror update-ls-set」-access all」
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱「system license add」-access all」
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd dirname「system license clear-up」-access all」
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱「system license delete」-access all」
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱「system license show」-access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱「system license Status show」-access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱「system nodemodify」-access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱「system Node show」-access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱「system Status show」-access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱「version」-access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname「volume clone create」-access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱「volume clone show」-access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname「volume clone s拆分 start」-access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname「volume clone split stop」-access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "volume cree"-access all"
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "volume destrode"-access all"
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname「volume file clone create」-access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname「volume file show-disk-usage」-access all」

- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "volume modify"-access all"
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify-snaplock-expiry-time" -access all
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "volume offline"-access all"
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "volume online - access all"
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "volume qtree cree"-access all"
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "volume qtree delete"-access all"
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "volume qtree modify"-access all"
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "volume qtree show"-access all"
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "volume restrent"-access all"
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "volume show"-access all"
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname 「volume snapshot create」 -access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "volume snapshot delete"-access all"
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname 「volume snapshot modify」 -access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname 「volume snapshot Promote」 -access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname 「volume snapshot rame」 -access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱 「Volume snapshot還原」 -access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname 「volume snapshot還原檔案」 -access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname 「volume snapshot show」 -access all」
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show-delta" -access all
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "volume unmount」 -access all」
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "vserver"-access all"
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱 「vserver CIFS create」 -access all」

- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱「vserver CIFS刪除」-access all」
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱「vserver CIFS modify」-access all」
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱「vserver CIFS共用修改」-access all」
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱「vserver CIFS共用create」-access all」
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱「vserver CIFS共用刪除」-access all」
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱「vserver CIFS共用修改」-access all」
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱「vserver CIFS共用show」-access all」
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱「vserver CIFS show」-access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱「vserver create」-access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "vserver EXECLON-policy cree"-access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "vserver EXECLON-policy DELETE」-access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname 「vserver EXECLON-policy rule create」-access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "vserver EXECLON-policy rule DELETE」-access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "vserver EXECLON-policy rule modify"-access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "vserver EXECLON-policy rule show"-access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱「vserver EXECLON-policy show」-access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱「vserver iSCSI connection show」-access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "vserver modify"-access all」
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "vserver show"-access all」

為 **ASA R2** 系統建立 **ONTAP** 叢集角色

您應該建立ONTAP 具有最低權限的支援功能、以便不必使用ONTAP 這個功能來SnapCenter 執行動作。您可以執行數ONTAP 個CLI命令來建立ONTAP 一個不含指令集的叢集角色、並指派最低權限。

步驟

1. 在儲存系統上、建立角色並將所有權限指派給該角色。

「安全登入角色create-vserver <cluster名稱>- role <role名稱>-cmd目錄名稱<permission>」



您應該針對每個權限重複此命令。

2. 建立使用者並將角色指派給該使用者。

```
security login create -user <user_name\> -vserver <cluster_name\> -application  
http -authmethod password -role <role_name\>
```

3. 解除鎖定使用者。

「安全登入解除鎖定-使用者<使用者名稱>-vserver <叢集名稱>」

用於建立叢集角色和指派權限的**CLI命令ONTAP**

您應該執行幾ONTAP 個CLI命令來建立叢集角色並指派權限。

- security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "metrocluster show" -access readonly
- security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "cluster identity modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster identity show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster peer show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "event generate-autosupport-log" -access all
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱「jobhistory show」 -access all」
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job show" -access all
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "jobstop" -access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱"LUN"-access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱"LUN cree"-access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱"lun刪除"-access all」
- 「安全登入角色create -vserver Cluster_name -role rou_name -cmd dirname "LUN igroup add"-access all」

- 「安全登入角色create -vserver Cluster_name -role rou_name -cmd dirname "LUN igroup cree"-access all"
- 「安全登入角色create -vserver Cluster_name -role rou_name -cmd dirname "LUN igroup delete"-access all"
- 「安全登入角色create -vserver Cluster_name -role rou_name -cmd dirname "LUN igroup modify"-access all"
- 「安全登入角色create -vserver Cluster_name -role rou_name -cmd dirname "LUN igroup rame"-access all"
- 「安全登入角色create -vserver Cluster_name -role rou_name -cmd dirname "LUN igroup show"-access all"
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd dirname 「LUN mapping add-report-nodes」 -access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱 「LUN mapping create」 -access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱 「LUN mapping delete」 -access all」
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd dirname 「LUN mapping remove-report-nodes」 -access all」
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱 「LUN mapping show」 -access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱"lun modify"-access all"
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "LUN move-in-volume」 -access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱"lun offline"-access all"
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱 「LUN online」 -access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "LUN永久性保留區Clear"-access all"
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱 「LUN resize」 -access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "LUN serial」 -access all」
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱"LUN show"-access all"
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname 「network interface create」 -access readonly」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname 「network interface delete」 -access readonly」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname 「network interface modify」 -access readonly」
- 「安全登入角色create -vserver Cluster_name -role road_Name -cmd dirname 「network interface show」 -access readonly」
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem map" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem create" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem host" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem controller" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace show" -access all
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname 「安全性登入」 -access readonly」
- 「安全登入角色create -role rose_Name -cmd目錄名稱"SnapMirror cree"-vserver Cluster_name -access all」
- 「安全登入角色create -role rose_Name -cmd目錄名稱"SnapMirror list-destinations"-vserver Cluster_name -access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname 「SnapMirror原則附加規則」 -access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱 「SnapMirror原則create」 -access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱 「SnapMirror原則刪除」 -access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱 「SnapMirror原則修改」 -access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱 「SnapMirror原則modify-rRule」 -access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱 「SnapMirror原則移除規則」 -access all」
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱 「SnapMirror原則show」 -access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱"SnapMirror還原"-access all」
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱"SnapMirror show"-access all」

- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱「SnapMirror show-history」
-access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱「SnapMirror update」
-access all」
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd dirname「SnapMirror update-ls-set」
-access all」
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱「system license add」
-access all」
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd dirname「system license clear-up」
-access all」
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱「system license delete」
-access all」
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱「system license show」
-access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱「system license Status
show」 -access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱「system nodemodify」
-access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱「system Node show」
-access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱「system Status show」
-access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱「version」 -access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname「volume clone create」
-access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱「volume clone show」
-access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname「volume clone s拆分
start」 -access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname「volume clone split
stop」 -access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "volume cree"-access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "volume destrode"-access
all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname「volume file clone
create」 -access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname「volume file show-disk-
usage」 -access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "volume modify"-access
all」
- security login role create -vserver Cluster_name -role Role_Name -cmddirname
"volume snapshot modify-snaplock-expiry-time" -access all

- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "volume offline"-access all"
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "volume online - access all"
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "volume qtree cree"-access all"
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "volume qtree delete"-access all"
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "volume qtree modify"-access all"
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "volume qtree show"-access all"
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "volume restrent"-access all"
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "volume show"-access all"
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname 「volume snapshot create」 -access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "volume snapshot delete"-access all"
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname 「volume snapshot modify」 -access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname 「volume snapshot Promote」 -access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname 「volume snapshot rame」 -access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱 「Volume snapshot還原」 -access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname 「volume snapshot還原檔案」 -access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname 「volume snapshot show」 -access all」
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show-delta" -access all
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "volume unmount」 -access all」
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "vserver"-access all"
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱 「vserver CIFS create」 -access all」
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱 「vserver CIFS刪除」 -access all」
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱 「vserver CIFS modify」 -access all」

- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱「vserver CIFS共用修改」-access all」
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱「vserver CIFS共用create」-access all」
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱「vserver CIFS共用刪除」-access all」
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱「vserver CIFS共用修改」-access all」
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱「vserver CIFS共用show」-access all」
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱「vserver CIFS show」-access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱「vserver create」-access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "vserver EXECLON-policy cree"-access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "vserver EXECLON-policy DELETE」-access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname 「vserver EXECLON-policy rule create」-access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "vserver EXECLON-policy rule DELETE」-access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "vserver EXECLON-policy rule modify"-access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "vserver EXECLON-policy rule show"-access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱「vserver EXECLON-policy show」-access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd目錄名稱「vserver iSCSI connection show」-access all」
- 「安全性登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "vserver modify"-access all」
- 「安全登入角色create -vserver Cluster_name -role rose_Name -cmd dirname "vserver show"-access all」
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "storage-unit show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "consistency-group" show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror protect" show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume delete" show" -access all

新增使用者或群組、並指派角色和資產

若要設定SnapCenter 適用於哪些使用者的角色型存取控制、您可以新增使用者或群組並指派角色。角色決定SnapCenter 了使用者可以存取的選項。

開始之前

- 您必須以「SnapCenterAdmin」角色登入。
- 您必須在作業系統或資料庫的Active Directory中建立使用者或群組帳戶。您無法使用SnapCenter 禁用功能來建立這些帳戶。



您只能在使用者名稱和群組名稱中包含下列特殊字元：空格 ()，連字號 (-)，底線 (_) 和冒號 (:)。

- 包含數個預先定義的角色。SnapCenter

您可以將這些角色指派給使用者、或是建立新角色。

- 新增至SnapCenter RBAC的AD使用者和AD群組必須擁有Active Directory中「使用者容器」和「電腦容器」的讀取權限。
- 將角色指派給包含適當權限的使用者或群組之後、您必須指派使用者存取SnapCenter 諸如主機和儲存連線等各種資源。

如此一來、使用者就能對指派給他們的資產執行其擁有權限的動作。

- 您應該在某個時間點指派角色給使用者或群組、以充分利用RBAC權限和效率。
- 您可以指派主機、資源群組、原則、儲存連線、外掛程式、並在建立使用者或群組時向使用者提供認證。
- 您應指派使用者執行特定作業的最低資產如下：

營運	資產指派
保護資源	主機、原則
備份	主機、資源群組、原則
還原	主機、資源群組
複製	主機、資源群組、原則
複製生命週期	主機
建立資源群組	主機

- 當新節點新增至Windows叢集或DAG (Exchange Server資料庫可用度群組) 資產、且此新節點已指派給使用者時、您必須將資產重新指派給使用者或群組、以便將新節點納入使用者或群組。

您應該將RBAC使用者或群組重新指派給叢集或DAG、以便將新節點納入RBAC使用者或群組。例如、您有一個雙節點叢集、而且已將RBAC使用者或群組指派給叢集。當您將另一個節點新增至叢集時、應將RBAC

使用者或群組重新指派至叢集、以納入RBAC使用者或群組的新節點。

- 如果您打算複寫 Snapshot、則必須將來源和目的地 Volume 的儲存連線指派給執行作業的使用者。

您應該先新增資產、再將存取權指派給使用者。



如果您使用SnapCenter VMware vSphere的VMware vSphere功能的VMware vCenter外掛程式來保護VM、VMDK或資料存放區、則應使用VMware vSphere GUI將vCenter使用者新增至SnapCenter VMware vSphere的「VMware vSphere的VMware vSphere插件」角色。如需VMware vSphere角色的相關資訊、請參閱 "[VMware SnapCenter vSphere隨附於VMware vSphere的VMware vCenter外掛程式的預先定義角色](#)"。

步驟

1. 在左側導覽窗格中、按一下*設定*。
2. 在「設定」頁面中、按一下「使用者與存取>」 *。
3. 在「從Active Directory或工作群組新增使用者/群組」頁面中：

針對此欄位...	執行此動作...
存取類型	選取網域或工作群組 對於網域驗證類型、您應該指定要將使用者新增至角色的使用者或群組網域名稱。 依預設、系統會預先填入登入的網域名稱。  您必須在「設定>*全域設定*>*網域設定*」頁面中註冊不受信任的網域。
類型	選取使用者或群組  支援僅安全群組、不支援通訊群組。SnapCenter

針對此欄位...	執行此動作...
使用者名稱	<p>a. 輸入部分使用者名稱、然後按一下「新增」。</p> <p> 使用者名稱區分大小寫。</p> <p>b. 從搜尋清單中選取使用者名稱。</p> <p> 當您新增來自不同網域或不受信任網域的使用者時、應該完整輸入使用者名稱、因為沒有跨網域使用者的搜尋清單。</p> <p>重複此步驟、將其他使用者或群組新增至選取的角色。</p>
角色	選取您要新增使用者的角色。

4. 按一下「指派」、然後在「指派資產」頁面中：

- a. 從*資產*下拉式清單中選取資產類型。
- b. 在「資產」表格中、選取資產。

只有在使用者將資產新增SnapCenter 至下列項目時、才會列出這些資產。

- c. 針對所有必要資產重複此程序。
- d. 按一下「* 儲存 *」。

5. 按一下*提交*。

新增使用者或群組並指派角色之後、請重新整理資源清單。

設定稽核日誌設定

稽核日誌會針對SnapCenter 每項活動產生。根據預設、稽核記錄會受到預設安裝位置_C:\Program Files\NetApp\SnapCenter webapp\Audit的保護。

稽核記錄的安全機制是針對每個稽核事件產生數位簽署的摘要、以防止未經授權的修改。所產生的摘要會保留在個別的稽核Checksum檔案中、並會進行定期完整性檢查、以確保內容的完整性。

您應該以「SnapCenterAdmin」角色登入。

關於這項工作

- 警示會在下列案例中傳送：
 - 稽核記錄完整性檢查排程或Syslog伺服器已啟用或停用
 - 稽核記錄完整性檢查、稽核記錄或Syslog伺服器記錄失敗
 - 磁碟空間不足

- 只有在完整性檢查失敗時、才會傳送電子郵件。
- 您應該同時修改稽核記錄目錄和稽核Checksum記錄目錄路徑。您無法只修改其中一項。
- 修改稽核記錄目錄和稽核Checksum記錄目錄路徑時、無法對先前位置的稽核記錄執行完整性檢查。
- 稽核記錄目錄和稽核Checksum記錄目錄路徑應位於SnapCenter 支援服務器的本機磁碟機上。

不支援共用或網路掛載的磁碟機。

- 如果在Syslog伺服器設定中使用了udp傳輸協定、則連接埠關閉或無法使用所造成的錯誤將無法擷取為SnapCenter 錯誤或是在列舉時發出警示。
- 您可以使用Set-SmAuditSettings和Get-SmAuditSettings命令來設定稽核記錄。

您可以執行Get-Help命令名稱來取得可搭配Cmdlet使用之參數及其說明的相關資訊。或者，您也可以參閱"[《軟件指令程式參考指南》 SnapCenter](#)"。

步驟

1. 在「設定」頁面中、瀏覽至*設定*>*全域設定*>*稽核記錄設定*。
2. 在「稽核記錄」區段中、輸入詳細資料。
3. 輸入*稽核記錄目錄*和*稽核Checksum記錄目錄*
 - a. 輸入檔案大小上限
 - b. 輸入最大記錄檔數
 - c. 輸入要傳送警示的磁碟空間使用量百分比
4. (選用) 啟用*記錄UTC時間*。
5. (選用) 啟用*稽核記錄完整性檢查排程*、然後按一下*啟動完整性檢查*以進行隨需完整性檢查。

您也可以執行* Start-SmAuditIntegrityCheck*命令、開始隨需完整性檢查。

6. (選用) 啟用轉送稽核記錄至遠端syslog伺服器、然後輸入Syslog伺服器詳細資料。

您應該將憑證從Syslog伺服器匯入TLS 1.2傳輸協定的「信任根」。

- a. 輸入Syslog伺服器主機
 - b. 輸入Syslog伺服器連接埠
 - c. 輸入Syslog伺服器傳輸協定
 - d. 輸入RFC格式
7. 按一下「* 儲存 *」。
 8. 您可以按一下「監控>*工作*」、查看稽核完整性檢查和磁碟空間檢查。

使用SnapCenter 伺服器設定安全的MySQL連線

如果您想要在SnapCenter 獨立組態或網路負載平衡 (NLB) 組態中、確保支援彼此之間的通訊安全、可以產生安全通訊端層 (SSL) 憑證和金鑰檔。

設定安全的MySQL連線、以利獨立SnapCenter 式的伺服器組態

如果您想要保護SnapCenter 整個伺服器與MySQL伺服器之間的通訊安全、可以產生安全通訊端層（SSL）憑證和金鑰檔。您必須在MySQL伺服器和SnapCenter 還原伺服器中設定憑證和金鑰檔案。

系統會產生下列憑證：

- CA憑證
- 伺服器公開憑證和私密金鑰檔案
- 用戶端公開憑證和私密金鑰檔案

步驟

1. 使用openssl命令在Windows上設定MySQL伺服器和用戶端的SSL憑證和金鑰檔。

如需相關資訊、請參閱 ["MySQL版本5.7：使用openssl建立SSL憑證和金鑰"](#)



用於伺服器憑證、用戶端憑證和金鑰檔的一般名稱值必須各有別於用於CA憑證的一般名稱值。如果通用名稱值相同、則使用OpenSSL編譯的伺服器的憑證和金鑰檔將會失敗。

*最佳實務做法：*您應該使用伺服器完整網域名稱（FQDN）做為伺服器憑證的一般名稱。

2. 將SSL憑證和金鑰檔複製到MySQL Data資料夾。

預設的MySQL資料夾路徑為「C:\ProgramData\NetApp\SnapCenter\MySQL Data\Data\」。

3. 更新MySQL伺服器組態檔（my.ini）中的CA憑證、伺服器公開憑證、用戶端公開憑證、伺服器私密金鑰及用戶端私密金鑰路徑。

預設的MySQL伺服器組態檔（my.ini）路徑為「C:\ProgramData\NetApp\SnapCenter\MySQL Data\my.ini」。



您必須在MySQL伺服器組態檔（my.ini）的[mysqld]區段中指定CA憑證、伺服器公開憑證和伺服器私密金鑰路徑。

您必須在MySQL伺服器組態檔（my.ini）的[client]區段中指定CA憑證、用戶端公開憑證和用戶端私密金鑰路徑。

以下範例顯示複製到my.ini檔案的[mysqld]區段、預設資料夾「C:\ProgramData\NetApp\SnapCenter\MySQL Data\Data」中的憑證和金鑰檔。

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-key.pem"
```

下列範例顯示my.ini檔案的[client]區段中更新的路徑。

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-key.pem"
```

4. 停止SnapCenter Internet Information Server (IIS) 中的功能。
5. 重新啟動MySQL服務。
6. 更新 SnapManager · Web.ui.dll · config 檔案中的 MySQLProtocol 金鑰值。

下列範例顯示在 SnapManager · Web.ui.dll · config 檔案中更新的 MySQLProtocol 金鑰值。

```
<add key="MySQLProtocol" value="SSL" />
```

7. 使用 my.ini 檔案 [用戶端] 區段中提供的路徑、更新 SnapManager · Web.UI.dll.config 檔案。

下列範例顯示my.ini檔案的[client]區段中更新的路徑。

```
<add key="ssl-client-cert" value="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-cert.pem" />
```

```
<add key="ssl-client-key" value="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-key.pem" />
```

```
<add key="ssl-ca" value="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem" />
```

8. 在SnapCenter IIS中啟動「伺服器」Web應用程式。

針對HA組態設定安全的MySQL連線

如果您想要保護SnapCenter 穩定支援服務器與MySQL伺服器之間的通訊、可以為高可用性（HA）節點產生安全通訊端層（SSL）憑證和金鑰檔。您必須在MySQL伺服器和HA節點上設定憑證和金鑰檔。

系統會產生下列憑證：

- CA憑證
CA憑證會在其中一個HA節點上產生、而此CA憑證會複製到另一個HA節點。
- 兩個HA節點的伺服器公開憑證和伺服器私密金鑰檔案
- 兩個HA節點的用戶端公開憑證和用戶端私密金鑰檔案

步驟

1. 對於第一個HA節點、請使用openssl命令、在Windows上設定MySQL伺服器和用戶端的SSL憑證和金鑰檔。

如需相關資訊、請參閱 ["MySQL版本5.7：使用openssl建立SSL憑證和金鑰"](#)



用於伺服器憑證、用戶端憑證和金鑰檔的一般名稱值必須各有別於用於CA憑證的一般名稱值。如果通用名稱值相同、則使用OpenSSL編譯的伺服器的憑證和金鑰檔將會失敗。

最佳實務做法：您應該使用伺服器完整網域名稱（FQDN）做為伺服器憑證的一般名稱。

2. 將SSL憑證和金鑰檔複製到MySQL Data資料夾。

預設的MySQL資料夾路徑為C:\ProgramData\NetApp\SnapCenter\MySQL Data\。

3. 更新MySQL伺服器組態檔（my.ini）中的CA憑證、伺服器公開憑證、用戶端公開憑證、伺服器私密金鑰及用戶端私密金鑰路徑。

預設的MySQL伺服器組態檔（my.ini）路徑為C:\ProgramData\NetApp\SnapCenter\MySQL Data\my.in



您必須在MySQL伺服器組態檔（my.ini）的[mysqld]區段中指定CA憑證、伺服器公開憑證和伺服器私密金鑰路徑。

您必須在MySQL伺服器組態檔（my.ini）的[client]區段中指定CA憑證、用戶端公開憑證及用戶端私密金鑰路徑。

下列範例顯示複製到my.ini檔案的[mysqld]區段、預設資料夾C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data中的憑證和金鑰檔。

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-key.pem"
```

下列範例顯示my.ini檔案的[client]區段中更新的路徑。

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-key.pem"
```

4. 對於第二個HA節點、請複製CA憑證並產生伺服器公開憑證、伺服器私密金鑰檔、用戶端公開憑證及用戶端私密金鑰檔。請執行下列步驟：

- a. 將在第一個HA節點上產生的CA憑證複製到第二個NLB節點的MySQL Data資料夾。

預設的MySQL資料夾路徑為C:\ProgramData\NetApp\SnapCenter\MySQL Data\。



您不得再次建立CA憑證。您應該只建立伺服器公開憑證、用戶端公開憑證、伺服器私密金鑰檔和用戶端私密金鑰檔。

- b. 對於第一個HA節點、請使用openssl命令、在Windows上設定MySQL伺服器和用戶端的SSL憑證和金鑰檔。

["MySQL版本5.7：使用openssl建立SSL憑證和金鑰"](#)



用於伺服器憑證、用戶端憑證和金鑰檔的一般名稱值必須各有別於用於CA憑證的一般名稱值。如果通用名稱值相同、則使用OpenSSL編譯的伺服器的憑證和金鑰檔將會失敗。

建議使用伺服器FQDN做為伺服器憑證的一般名稱。

- c. 將SSL憑證和金鑰檔複製到MySQL Data資料夾。
- d. 更新MySQL伺服器組態檔（my.ini）中的CA憑證、伺服器公開憑證、用戶端公開憑證、伺服器私密金鑰及用戶端私密金鑰路徑。



您必須在MySQL伺服器組態檔（my.ini）的[mysqld]區段中指定CA憑證、伺服器公開憑證和伺服器私密金鑰路徑。

您必須在MySQL伺服器組態檔（my.ini）的[client]區段中指定CA憑證、用戶端公開憑證和用戶端私密金鑰路徑。

下列範例顯示複製到my.ini檔案的[mysqld]區段、預設資料夾C

: /ProgramData/NetApp/SnapCenter/MySQL Data/Data中的憑證和金鑰檔。

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-  
cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-  
key.pem"
```

下列範例顯示my.ini檔案的[client]區段中更新的路徑。

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

+

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-  
cert.pem"
```

+

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-  
key.pem"
```

5. 在SnapCenter 兩個HA節點上的Internet Information Server (IIS) 中停止使用支援功能的Web應用程式。
6. 在兩個HA節點上重新啟動MySQL服務。
7. 更新兩個 HA 節點的 SnapManager · Web.ui.dll · config 檔案中的 MySQLProtocol 金鑰值。

下列範例顯示在 SnapManager · Web.ui.dll · config 檔案中更新的 MySQLProtocol 金鑰值。

```
<add key="MySQLProtocol" value="SSL" />
```

8. 使用您在 my.ini 檔案的 [用戶端] 區段中針對兩個 HA 節點所指定的路徑、更新 SnapManager · Web.UI.dll.config 檔案。

下列範例顯示my.ini檔案的[client]區段中更新的路徑。

```
<add key="ssl-client-cert" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/client-cert.pem" />
```

```
<add key="ssl-client-key" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/client-key.pem" />
```

```
<add key="ssl-ca" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/ca.pem" />
```

9. 在 SnapCenter 兩個 HA 節點的 IIS 中啟動「支援伺服器」 Web 應用程式。
10. 使用 `Set-SmRegistryConfig -RebuildSlave -Force PowerShell Cmdlet` 搭配其中一個 HA 節點上的 `-Force` 選項、在兩個 HA 節點上建立安全的 MySQL 複寫。

即使複寫狀態正常、`-Force` 選項仍可讓您重建從屬儲存庫。

設定憑證型驗證

憑證型驗證可驗證 SnapCenter 伺服器和外掛主機的身分識別，確保安全且加密的通訊，進而提升安全性。

啟用憑證型驗證

若要為 SnapCenter Server 和 Windows 外掛程式主機啟用憑證型驗證、請執行下列 PowerShell Cmdlet。對於 Linux 外掛主機、當您啟用雙向 SSL 時、將會啟用憑證型驗證。

- 若要啟用用戶端憑證型驗證：

```
Set-SmConfigSettings -Agent -configSettings
@{"EnableClientCertificateAuthentication"="true"} -HostName[hostname]
```

- 若要停用用戶端憑證型驗證：

```
Set-SmConfigSettings -Agent -configSettings
@{"EnableClientCertificateAuthentication"="false"} -HostName [hostname]
```

從 SnapCenter 伺服器匯出憑證授權單位 (CA) 憑證

您應該使用 Microsoft 管理主控台 (MMC)、將 CA 憑證從 SnapCenter 伺服器匯出至外掛主機。

開始之前

您應該已設定雙向 SSL。

步驟

1. 移至Microsoft管理主控台（MMC）、然後按一下*檔案*>*新增/移除Snapin*。
2. 在「新增或移除嵌入式管理單元」視窗中、選取「憑證」、然後按一下「新增」。
3. 在「憑證嵌入式管理單元」視窗中，選取 * 電腦帳戶 * 選項，然後按一下 * 完成 *。
4. 按一下 * 主控台根目錄 * > * 憑證 - 本機電腦 * > * 個人 * > * 憑證 *。
5. 以滑鼠右鍵按一下用於 SnapCenter 伺服器的已取得 CA 憑證、然後選取 * 所有工作 * > * 匯出 * 以啟動匯出精靈。
6. 在精靈中執行下列動作。

針對此選項 ...	請執行下列動作...
匯出私密金鑰	選擇 * 否、不要匯出私密金鑰 *、然後按一下 * 下一步 *。
匯出檔案格式	單擊 * 下一步 *。
檔案名稱	按一下 * 瀏覽 * 並指定儲存憑證的檔案路徑、然後按一下 * 下一步 *。
完成憑證匯出精靈	檢閱摘要、然後按一下「完成」開始匯出。



SnapCenter HA 組態和 SnapCenter Plug-in for VMware vSphere 不支援憑證型驗證。

將 CA 憑證匯入 Windows 外掛主機

若要使用匯出的 SnapCenter 伺服器 CA 憑證、您應該使用 Microsoft 管理主控台（MMC）、將相關的憑證匯入 SnapCenter Windows 外掛主機。

步驟

1. 移至Microsoft管理主控台（MMC）、然後按一下*檔案*>*新增/移除Snapin*。
2. 在「新增或移除嵌入式管理單元」視窗中、選取「憑證」、然後按一下「新增」。
3. 在「憑證嵌入式管理單元」視窗中，選取 * 電腦帳戶 * 選項，然後按一下 * 完成 *。
4. 按一下 * 主控台根目錄 * > * 憑證 - 本機電腦 * > * 個人 * > * 憑證 *。
5. 在資料夾「個人」上按一下滑鼠右鍵、然後選取 * 所有工作 * > * 匯入 * 以啟動匯入精靈。
6. 在精靈中執行下列動作。

針對此選項 ...	請執行下列動作...
零售店位置	單擊 * 下一步 *。
要匯入的檔案	選取以 .cer 副檔名結尾的 SnapCenter 伺服器憑證。

針對此選項 ...	請執行下列動作...
憑證存放區	單擊 * 下一步 * 。
完成憑證匯出精靈	檢閱摘要、然後按一下「完成」開始匯入。

將 CA 憑證匯入 UNIX 外掛主機

您應該將 CA 憑證匯入 UNIX 外掛主機。

關於此工作

- 您可以管理 SPL Keystore 的密碼、以及使用中的 CA 簽署金鑰配對別名。
- SPL 密鑰庫和私鑰的所有關聯別名密碼應相同。

步驟

1. 您可以從SPL內容檔擷取SPL Keystore預設密碼。它是對應於金鑰的值 `SPL_KEYSTORE_PASS`。
2. 變更Keystore密碼：`$ keytool -storepasswd -keystore keystore.jks`
3. 將Keystore中私密金鑰項目的所有別名密碼變更為與Keystore相同的密碼：`$ keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`
4. 請針對 `SPL_Keystore` 密碼進行相同的更新 `spl.properties` 檔案：
5. 變更密碼後重新啟動服務。

將根或中繼憑證設定為SPL信任存放區

您應該將根或中繼憑證設定為 SPL 信任存放區。您應該先新增根CA憑證、然後再新增中繼CA憑證。

步驟

1. 瀏覽至包含 SPL Keystore 的資料夾：`/var/opt/snapcenter/spl/etc`。
2. 找到檔案 `keystore.jks`。
3. 在Keystore中列出新增的憑證：`$ keytool -list -v -keystore keystore.jks`
4. 新增根或中繼憑證：`$ keytool -import -trustcacerts -alias <AliasNameForCertificateToBeImported> -file /<CertificatePath> -keystore keystore.jks`
5. 將根或中繼憑證設定為SPL信任存放區之後、請重新啟動服務。

將CA簽署金鑰配對設定為SPL信任存放區

您應該將 CA 簽署金鑰配對設定為 SPL 信任存放區。

步驟

1. 瀏覽至包含 SPL Keystore 的資料夾 `/var/opt/snapcenter/spl/etc`。

2. 找到檔案 keystore.jks`。
3. 在Keystore中列出新增的憑證：\$ keytool -list -v -keystore keystore.jks
4. 新增具有私密金鑰和公開金鑰的CA憑證。\$ keytool -importkeystore -srckeystore <CertificatePathToImport> -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
5. 在Keystore中列出新增的憑證。\$ keytool -list -v -keystore keystore.jks
6. 驗證密鑰庫是否包含與新CA憑證對應的別名、該CA憑證已新增至金鑰庫。
7. 將CA憑證的新增私密金鑰密碼變更為金鑰庫密碼。

預設的 SPL 金鑰庫密碼是金鑰 SPL_Keystore 密碼的值 spl.properties 檔案：

```
$ keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore keystore.jks`
```

8. 如果CA憑證中的別名很長且包含空格或特殊字元（「*」、「」、「」）、請將別名變更為簡單名稱：\$ keytool -changealias -alias "<OriginalAliasName>" -destalias "<NewAliasName>" -keystore keystore.jks`
9. 從中的 Keystore 設定別名 spl.properties 檔案：請根據SPL_PRO證書別名更新此值。
10. 將CA簽署金鑰配對設定為SPL信任存放區後、請重新啟動服務。

匯出SnapCenter 功能證書

您應該匯出 .pfp 格式的 SnapCenter 憑證。

步驟

1. 移至Microsoft管理主控台（MMC）、然後按一下*檔案*>*新增/移除嵌入式管理單元*。
2. 在「新增或移除嵌入式管理單元」視窗中、選取「憑證」、然後按一下「新增」。
3. 在「憑證」嵌入式管理單元視窗中、選取「我的使用者帳戶」選項、然後按一下「完成」。
4. 按一下*主控台根目錄*>*憑證-目前使用者*>*信任的根憑證授權單位*>*憑證*。
5. 以滑鼠右鍵按一下含有SnapCenter「不易用名稱」的憑證、然後選取「所有工作」>「匯出」以啟動匯出精靈。
6. 完成精靈、如下所示：

在此精靈視窗中...	請執行下列動作...
匯出私密金鑰	選取選項*是、匯出私密金鑰*、然後按一下*下一步*。
匯出檔案格式	不做任何變更；按一下*下一步*。
安全性	指定匯出憑證所使用的新密碼、然後按一下*「下一步*」。

在此精靈視窗中...	請執行下列動作...
要匯出的檔案	為匯出的憑證指定檔案名稱（您必須使用.pfx） 、然後按一下*「Next*（下一步*）」。
完成憑證匯出精靈	檢閱摘要、然後按一下「完成」開始匯出。

設定 Windows 主機的 CA 憑證

產生CA認證CSR檔案

您可以產生「憑證簽署要求」（CSR）、然後匯入可以使用產生的CSR從「憑證授權單位」（CA）取得的憑證。憑證將會有與其相關的私密金鑰。

CSR是編碼文字區塊、提供給授權憑證廠商以取得簽署的CA憑證。



CA 憑證 RSA 金鑰長度必須至少為 3072 位元。

如需產生CSR的資訊、請參閱 ["如何產生CA憑證CSR檔案"](#)。



如果您擁有網域 (*.domain.company.com) 或系統 (machine1.domain.company.com) 的CA憑證、您可以跳過產生CA憑證CSR檔案的步驟。您可以使用SnapCenter 效益管理程式來部署現有的CA憑證。

對於叢集組態、叢集名稱（虛擬叢集FQDN）和各自的主機名稱應在CA憑證中提及。您可以在取得憑證之前填寫「Subject Alternative Name (SAN)（主體替代名稱 (SAN)）」欄位、以更新憑證。若為萬用字元憑證 (*.domain.company.com)、憑證將會隱含包含網域的所有主機名稱。

匯入CA憑證

您必須SnapCenter 使用Microsoft管理主控台（MMC）、將CA憑證匯入到S倚賴者支援的伺服器和Windows主機外掛程式。

步驟

1. 移至Microsoft管理主控台（MMC）、然後按一下*檔案*>*新增/移除Snapin*。
2. 在「新增或移除嵌入式管理單元」視窗中、選取「憑證」、然後按一下「新增」。
3. 在「憑證」嵌入式管理單元視窗中、選取「電腦帳戶」選項、然後按一下「完成」。
4. 按一下*主控台根目錄*>*憑證-本機電腦*>*信任的根憑證授權單位*>*憑證*。
5. 在「Trusted Root Certification Authorities」（受信任的根憑證授權單位）資料夾上按一下滑鼠右鍵、然後選取「* All Tasks」（所有工作）>「Import」（匯入）以啟動匯入精靈。
6. 完成精靈、如下所示：

在此精靈視窗中...	請執行下列動作...
匯入私密金鑰	選取選項* Yes*、匯入私密金鑰、然後按一下* Next*。
匯入檔案格式	不做任何變更；按一下*下一步*。
安全性	指定匯出憑證所使用的新密碼、然後按一下*「下一步*」。
完成「憑證匯入精靈」	檢閱摘要、然後按一下「完成」開始匯入。



匯入憑證應與私密金鑰搭售（支援的格式為：。pfx、。p12和*。p7b）。

7. 對「Personal」資料夾重複步驟5。

取得CA憑證指紋

憑證指紋是用來識別憑證的十六進位字串。指紋是使用指紋演算法、從憑證內容中計算出來。

步驟

1. 在GUI上執行下列步驟：
 - a. 按兩下憑證。
 - b. 在「憑證」對話方塊中、按一下「詳細資料」索引標籤。
 - c. 捲動欄位清單、然後按一下* Thumbprint*。
 - d. 複製方塊中的十六進位字元。
 - e. 移除十六進位數字之間的空格。

例如、如果指紋為：「A9 09 50 2D D8 2a E4 14 33 E6 F8 38 86 b0 d 42 77 A3 2a 7b」、則移除空格後、將會是：「a909502dd82ae41433e6f83886b00d4277a32a7b」。

2. 從PowerShell執行下列作業：
 - a. 執行下列命令、列出已安裝憑證的指紋、並依主體名稱識別最近安裝的憑證。

```
Get-ChildItem路徑認證：\LocalComputer\My
```

- b. 複製指紋。

使用Windows主機外掛程式服務設定CA憑證

您應該使用Windows主機外掛程式服務來設定CA憑證、以啟動安裝的數位憑證。

請在SnapCenter 已部署CA憑證的所有插件主機上執行下列步驟。

步驟

1. 執行下列命令、以SMCore預設連接埠8145移除現有的憑證繫結：

```
'>netsh http DELETE sslcert ipport=0.0.0.0: _<SMCore Port>'
```

例如：

```
> netsh http delete sslcert ipport=0.0.0.0:8145  
· 執行下列命令、將新安裝的憑證與Windows主機外掛程式服務連結：
```

```
> $cert = "_<certificate thumbprint>_"  
> $guid = [guid]::NewGuid().ToString("B")  
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert  
appid="$guid"
```

例如：

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"  
> $guid = [guid]::NewGuid().ToString("B")  
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert  
appid="$guid"
```

使用SnapCenter 站台設定CA憑證

您應該在SnapCenter Windows主機上使用站台來設定CA憑證。

步驟

1. 在SnapCenter 安裝了Windows*的Windows Server上開啟「IIS管理員」。
2. 在左導覽窗格中、按一下*連線*。
3. 展開伺服器 and *站台* 的名稱。
4. 選取SnapCenter 您要在其中安裝SSL憑證的站台。
5. 瀏覽至 * Actions > Edit Site> 、按一下 * Bindings * 。
6. 在「繫結」頁面中、選取「*繫結https *」。
7. 按一下 * 編輯 * 。
8. 從SSL憑證下拉式清單中、選取最近匯入的SSL憑證。
9. 按一下「確定」。



SnapCenter 排程器站台（預設連接埠：8154、HTTPS）是以自我簽署的憑證進行設定。此連接埠正在 SnapCenter 伺服器主機內通訊、因此不一定要使用 CA 憑證進行設定。不過、如果您的環境要求您使用 CA 憑證、請使用 SnapCenter 排程器網站重複步驟 5 至 9。



如果下拉式功能表中未列出最近部署的CA憑證、請檢查CA憑證是否與私密金鑰相關聯。



請確定使用下列路徑新增憑證：主控台根目錄>憑證-本機電腦>信任的根憑證授權單位>憑證。

啟用CA認證SnapCenter 以供使用

您應該設定CA憑證、並啟用SnapCenter 適用於該伺服器的CA憑證驗證。

開始之前

- 您可以使用Set-SmCertificateSettings Cmdlet來啟用或停用CA憑證。
- 您可以SnapCenter 使用Get-SmCertificateSettings Cmdlet來顯示驗證伺服器的憑證狀態。

您可以執行_Get-Help命令name_來取得可搭配Cmdlet使用之參數及其說明的相關資訊。或者、您也可以參閱"[《軟件指令程式參考指南》 SnapCenter](#)"。

步驟

1. 在「設定」頁面中、瀏覽至*設定*>*全域設定*>* CA憑證設定*。
2. 選取*啟用憑證驗證*。
3. 按一下「*套用*」。

完成後

「受管理的主機」標籤主機會顯示掛鎖、掛鎖的色彩則會指出SnapCenter 「支援服務器」與外掛主機之間的連線狀態。

- **  表示未啟用或指派 CA 憑證給外掛主機。
- **  表示 CA 憑證已成功驗證。
- **  表示 CA 憑證無法驗證。
- **  表示無法擷取連線資訊。



當狀態為黃色或綠色時、資料保護作業會成功完成。

設定 Linux 主機的 CA 憑證

在 Linux 上安裝SnapCenter伺服器後，安裝程式會建立自簽名憑證。如果要使用 CA 證書，則應設定 nginx 反向代理、稽核日誌記錄和SnapCenter 的證書。

設定 Nginx 憑證

步驟

1. 瀏覽至 /etc/Nginc/conf.d_ : `cd /etc/nginx/conf.d`
2. 使用 vi 或任何文字編輯器開啟 **snapcenter.conf** 。

3. 瀏覽至組態檔案中的伺服器區段。
4. 修改 `ssl_certificate` 及 `_ssl_certificate key` 的路徑、以指向 CA 憑證。
5. 儲存並關閉檔案。
6. 重新載入 Nginx：`$nginx -s reload`

設定稽核記錄憑證

步驟

1. 使用 vi 或任何文字編輯器開啟 `install_DIR/NetApp/snapcenter/SnapManagerWeb/SnapManager.Web.ui.dll.config`。
`install_DIR` 的預設值為：`_/opt`。
2. 編輯 `AUDILOG_CTIFOY_path` 和 `AUDILOG_CINATE_PASSI` 金鑰、分別加入 CA 憑證路徑和密碼。
稽核記錄憑證僅支援 `_.pfx` 格式。
3. 儲存並關閉檔案。
4. 重新啟動 **snapmanagerweb** 服務：`$ systemctl restart snapmanagerweb`

配置 SnapCenter 證書

步驟

1. 使用 vi 或任何文字編輯器開啟下列組態檔案。
 - `_INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/SnapManager`
 - `INSTALL_DIR/NetApp/snapcenter/SMCore/SMCoreServiceHost.dll.config`
 - `INSTALL_DIR/NetApp/snapcenter/Scheduler/Scheduler.API.dll.config``install_DIR` 的預設值為：`_/opt`。
2. 編輯 `*service_certificate 路徑 *` 和 `*service_certificate 密碼 *` 金鑰、分別包含 CA 憑證路徑和密碼。
SnapCenter 憑證僅支援 `.pfx` 格式。
3. 儲存並關閉檔案。
4. 重新啟動所有服務。
 - `$ systemctl restart snapmanagerweb`
 - `$ systemctl restart smcore`
 - `$ systemctl restart scheduler`

在 Windows 主機上設定並啟用雙向 SSL 通訊

在 Windows 主機上設定雙向 SSL 通訊

您應該設定雙向 SSL 通訊、以確保 Windows 主機上的 SnapCenter 伺服器與外掛程式之間的相互通訊安全無虞。

開始之前

- 您應該已產生 CA 憑證 CSR 檔案、其支援金鑰長度下限為 3072。
- CA 憑證應支援伺服器驗證和用戶端驗證。
- 您應該擁有內含私密金鑰和指紋詳細資料的 CA 憑證。
- 您應該已啟用單向 SSL 組態。

如需詳細資料、請參閱 ["設定 CA 憑證區段。"](#)

- 您必須在所有外掛主機和 SnapCenter 伺服器上啟用雙向 SSL 通訊。

不支援某些主機或伺服器未啟用雙向 SSL 通訊的環境。

步驟

1. 若要繫結連接埠、請在 SnapCenter 伺服器主機上針對 SnapCenter IIS 網頁伺服器連接埠 8146（預設）執行下列步驟、並使用 PowerShell 命令再次為 SMCore 連接埠 8145（預設）執行下列步驟。

- a. 使用下列 PowerShell 命令移除現有的 SnapCenter 自我簽署憑證連接埠繫結。

```
> netsh http delete sslcert ipport=0.0.0.0:<SMCore port/IIS port>
```

例如、

```
> netsh http delete sslcert ipport=0.0.0.0:8145
```

```
> netsh http delete sslcert ipport=0.0.0.0:8146
```

- b. 將新取得的 CA 憑證與 SnapCenter 伺服器和 SMCore 連接埠繫結。

```
> $cert = "<CA_certificate_thumbprint>"
```

```
> $guid = [guid]::NewGuid().ToString("B")
```

```
> netsh http add sslcert ipport=0.0.0.0: <SMCore Port/IIS port>  
certhash=$cert appid="$guid" clientcertnegotiation=enable  
verifyclientcertrevocation=disable
```

```
> netsh http show sslcert ipport=0.0.0.0:<SMCore Port/IIS port>
```

例如、

```
> $cert = "abc123abc123abc123abc123"
```

```
> $guid = [guid]::NewGuid().ToString("B")
```

```
> netsh http add sslcert ipport=0.0.0.0:8146 certhash=$cert appid="$guid"  
clientcertnegotiation=enable verifyclientcertrevocation=disable
```

```
> $guid = [guid]::NewGuid().ToString("B")
```

```
> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert appid="$guid"  
clientcertnegotiation=enable verifyclientcertrevocation=disable
```

```
> netsh http show sslcert ipport=0.0.0.0:8146
```

```
> netsh http show sslcert ipport=0.0.0.0:8145
```

2. 若要存取 CA 憑證的權限、請執行下列步驟、在憑證權限清單中新增 SnapCenter 的預設 IIS Web 伺服器使用者 "IIS AppPool、SnapCenter"、以存取新取得的 CA 憑證。
 - a. 移至 Microsoft 管理主控台 (MMC)、然後按一下 * 檔案 * > * 新增 / 移除 Snapin *。
 - b. 在「新增或移除嵌入式管理單元」視窗中、選取「憑證」、然後按一下「新增」。
 - c. 在「憑證」嵌入式管理單元視窗中、選取「電腦帳戶」選項、然後按一下「完成」。
 - d. 按一下*主控台根目錄*>*憑證-本機電腦*>*個人*>*憑證*。
 - e. 選取 SnapCenter 憑證。
 - f. 若要啟動新增使用者 \ 權限精靈、請在 CA 憑證上按一下滑鼠右鍵、然後選取 * 所有工作 * > * 管理私密金鑰 *。
 - g. 按一下 * 新增 *、在「Select Users and Groups」(選取使用者和群組) 精靈上、將位置變更為本機電腦名稱 (階層架構中最上層)。
 - h. 新增 IIS AppPool \ SnapCenter 使用者、賦予完全控制權限。
3. 對於 *CA 證書 IIS 權限*、請從以下路徑在 SnapCenter 服務器中添加新的雙字節註冊表項：

在 Windows 登錄編輯器中、遍歷下列路徑：

```
HKey_Local_Machine\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
```

4. 在 SChannel 登錄組態的內容下建立新的 DWORD 登錄機碼項目。

```
SendTrustedIssuerList = 0
```

```
ClientAuthTrustMode = 2
```

設定 SnapCenter Windows 外掛程式進行雙向 SSL 通訊

您應該使用 PowerShell 命令設定 SnapCenter Windows 外掛程式、以進行雙向 SSL 通訊。

開始之前

確保 CA 憑證指紋可用。

步驟

1. 若要連結連接埠、請在 SMCORE 連接埠 8145 的 Windows 外掛主機上執行下列動作 (預設)。

- a. 使用下列 PowerShell 命令移除現有的 SnapCenter 自我簽署憑證連接埠繫結。

```
> netsh http delete sslcert ipport=0.0.0.0:<SMCore port>
```

例如、

```
> netsh http delete sslcert ipport=0.0.0.0:8145
```

- b. 將新取得的 CA 憑證與 SMCore 連接埠繫結。

```
> $cert = "<CA_certificate thumbprint>"
```

```
> $guid = [guid]::NewGuid().ToString("B")
```

```
> netsh http add sslcert ipport=0.0.0.0: <SMCore Port> certhash=$cert  
appid="$guid" clientcertnegotiation=enable  
verifyclientcertrevocation=disable
```

```
> netsh http show sslcert ipport=0.0.0.0:<SMCore Port>
```

例如、

```
> $cert = "abc123abc123abc123abc123"
```

```
> $guid = [guid]::NewGuid().ToString("B")
```

```
> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert appid="$guid"  
clientcertnegotiation=enable verifyclientcertrevocation=disable
```

```
> netsh http show sslcert ipport=0.0.0.0:8145
```

在 Windows 主機上啟用雙向 SSL 通訊

您可以啟用雙向 SSL 通訊、以使用 PowerShell 命令保護 Windows 主機上的 SnapCenter 伺服器與外掛程式之間的相互通訊。

開始之前

先執行所有外掛程式和 SMCore 代理程式的命令、然後再執行伺服器的命令。

步驟

1. 若要啟用雙向 SSL 通訊、請在 SnapCenter 伺服器上針對外掛程式、伺服器以及需要雙向 SSL 通訊的每個代理程式執行下列命令。

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}  
-HostName <Plugin_HostName>
```

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}  
-HostName localhost
```

```
> Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="true"}
```

2. 使用下列命令執行 IIS SnapCenter 應用程式集區資源回收作業。 > Restart-WebAppPool -Name "SnapCenter"
3. 對於 Windows 外掛程式、請執行下列 PowerShell 命令、重新啟動 SMCore 服務：

```
> Restart-Service -Name SnapManagerCoreService
```

停用雙向 **SSL** 通訊

您可以使用 PowerShell 命令停用雙向 SSL 通訊。

關於此工作

- 先執行所有外掛程式和 SMCore 代理程式的命令、然後再執行伺服器的命令。
- 停用雙向 SSL 通訊時、CA 憑證及其組態不會移除。
- 若要將新主機新增至 SnapCenter 伺服器、您必須停用所有外掛主機的雙向 SSL。
- NLB 和 F5 不受支援。

步驟

1. 若要停用雙向 SSL 通訊、請在 SnapCenter 伺服器上針對所有外掛主機和 SnapCenter 主機執行下列命令。

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"}  
-HostName <Agent_HostName>
```

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"}  
-HostName localhost
```

```
> Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="false"}
```

2. 使用下列命令執行 IIS SnapCenter 應用程式集區資源回收作業。 > Restart-WebAppPool -Name "SnapCenter"
3. 對於 Windows 外掛程式、請執行下列 PowerShell 命令、重新啟動 SMCore 服務：

```
> Restart-Service -Name SnapManagerCoreService
```

在 **Linux** 主機上設定並啟用雙向 **SSL** 通訊

在 **Linux** 主機上設定雙向 **SSL** 通訊

您應該設定雙向 SSL 通訊、以保護 Linux 主機上的 SnapCenter 伺服器與外掛程式之間的相互通訊。

開始之前

- 您應該已設定 Linux 主機的 CA 憑證。

- 您必須在所有外掛主機和 SnapCenter 伺服器上啟用雙向 SSL 通訊。

步驟

1. 將 *certificate.pem* 複製到 /etc/pi/ca-trust 、 source/crons/_ 。
2. 在 Linux 主機的信任清單中新增憑證。
 - cp root-ca.pem /etc/pki/ca-trust/source/anchors/
 - cp certificate.pem /etc/pki/ca-trust/source/anchors/
 - update-ca-trust extract
3. 確認憑證是否已新增至信任清單。trust list | grep "<CN of your certificate>"
4. 在 SnapCenter *NginX* 檔案中更新 **SSL_certificate** * 和 **SSL_certificate_key** 、然後重新啟動。
 - vim /etc/nginx/conf.d/snapcenter.conf
 - systemctl restart nginx
5. 重新整理 SnapCenter 伺服器 GUI 連結。
6. 在位於 `_/NetApp/snapcenter/SnapManagerWeb_` 的 **SnapManager** 、 **Web.ui.dll.config** <installation path> 和位於 `_/NETAPP/snapcenter/SMCore` <installation path> 的 **SMCoreServiceHost.dll.config** 中更新下列機碼的值。
 - <add key="SERVICE_CERTIFICATE_PATH" value="<path of certificate.pfx>" />
 - <add key="SERVICE_CERTIFICATE_PASSWORD" value="<password>"/>
7. 重新啟動下列服務。
 - systemctl restart smcore.service
 - systemctl restart snapmanagerweb.service
8. 確認憑證已附加至 SnapManager 網路連接埠。openssl s_client -connect localhost:8146 -brief
9. 確認憑證已附加至 smcore 連接埠。openssl s_client -connect localhost:8145 -brief
10. 管理 SPL Keystore 和別名的密碼。
 - a. 擷取 SPL 內容檔案中指派給 *SPL_Keystore 密碼的 SPL 金鑰庫預設密碼。
 - b. 變更 Keystore 密碼。keytool -storepasswd -keystore keystore.jks
 - c. 變更私密金鑰項目所有別名的密碼。keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks
 - d. 在 *spl.properties* 中更新與鍵 *SPL_Keystore 密碼相同的密碼。
 - e. 重新啟動服務。
11. 在外掛式 Linux 主機上、將根憑證和中繼憑證新增至 SPL 外掛程式的 Keystore 中。
 - keytool -import -trustcacerts -alias <any preferred alias name> -file <path of root-ca.pem> -keystore <path of keystore.jks mentioned in spl.properties file>
 - keytool -importkeystore -srckeystore <path of certificate.pfx> -srcstoretype pkcs12 -destkeystore <path of keystore.jks mentioned in spl.properties file> -deststoretype JKS

- i. 檢查 keystore . jks 中的條目。 `keytool -list -v -keystore <path to keystore.jks>`
 - ii. 必要時重新命名任何別名。 `keytool -changealias -alias "old-alias" -destalias "new-alias" -keypass keypass -keystore </path/to/keystore> -storepass storepas`
12. 使用儲存在 keystore . jks 中的 * certificate . pff* 別名、更新 *spl.properties* 檔案中的 * SPL_certificate . alias* 值、然後重新啟動 SPL 服務：`systemctl restart spl`
 13. 確認憑證已附加至 smcore 連接埠。 `openssl s_client -connect localhost:8145 -brief`

在 Linux 主機上啟用 SSL 通訊

您可以啟用雙向 SSL 通訊、以使用 PowerShell 命令保護 Linux 主機上的 SnapCenter 伺服器與外掛程式之間的相互通訊。

步驟

1. 執行下列步驟以啟用單向 SSL 通訊。
 - a. 登入 SnapCenter GUI 。
 - b. 按一下 * 設定 * > * 全域設定 *、然後選取 * 在 SnapCenter 伺服器 * 上啟用憑證驗證。
 - c. 按一下 * 主機 * > * 託管主機 *、然後選取您要啟用單向 SSL 的外掛主機。
 - d. 按一下  圖示、然後按一下 * 啟用憑證驗證 * 。
2. 從 SnapCenter 伺服器 Linux 主機啟用雙向 SSL 通訊。
 - `Open-SmConnection`
 - `Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"} -HostName <Plugin Host Name>`
 - `Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"} -HostName localhost`
 - `Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="true"}`

設定Active Directory、LDAP和LDAPS

登錄不受信任的Active Directory網域

您應向SnapCenter 支援此功能的伺服器登錄Active Directory、以管理來自多個不受信任Active Directory網域的主機、使用者和群組。

開始之前

- LDAP與LDAPS傳輸協定*
- 您可以使用LDAP或LDAPS傳輸協定來登錄不受信任的Active Directory網域。
- 您應該已經啟用外掛程式主機與SnapCenter 支援伺服器之間的雙向通訊。
- DNS解析應從SnapCenter 支援支援的伺服器設定為外掛主機、反之亦然。
- LDAP傳輸協定*

- 完整網域名稱（FQDN）應可從SnapCenter esxserver解析。

您可以使用FQDN登錄不受信任的網域。如果無法從SnapCenter 無法從The Fingserver解析FQDN、您可以向網域控制器IP位址註冊、這應該可以從SnapCenter 該伺服器解析。

- LDAPS傳輸協定*
- LDAPS需要CA憑證、才能在Active Directory通訊期間提供端點對端點加密。

"設定LDAPS的CA用戶端憑證"

- 網域控制器主機名稱（DCHostName、DCHostName）應可從SnapCenter 伺服器存取。

關於此工作

- 您可以使用SnapCenter Retest使用者介面、PowerShell Cmdlet或REST API來登錄不受信任的網域。

步驟

1. 在左側導覽窗格中、按一下*設定*。
2. 在「設定」頁面中、按一下「全域設定」。
3. 在「全域設定」頁面中、按一下*網域設定*。
4. 按一下  以登錄新網域。
5. 在「Register New Domain」（註冊新網域）頁面中、選取「* LDAP*」或「* LDAPS*」。

- a. 如果選擇* LDAP*、請指定登錄LDAP不受信任網域所需的資訊：

針對此欄位...	執行此動作...
網域名稱	指定網域的NetBios名稱。
網域FQDN	指定FQDN並按一下*解析*。
網域控制器IP位址	如果網域FQDN無法從SnapCenter 無法從無法解析的伺服器、請指定一個或多個網域控制器IP位址。 如需詳細資訊、請參閱 " 從GUI新增不受信任網域的網域控制器IP "。

- b. 如果您選取* LDAPS*、請指定登錄LDAPS不受信任網域所需的資訊：

針對此欄位...	執行此動作...
網域名稱	指定網域的NetBios名稱。
網域FQDN	指定FQDN。

針對此欄位...	執行此動作...
網域控制器名稱	指定一個或多個網域控制器名稱、然後按一下*解析*。
網域控制器IP位址	如果無法從SnapCenter 無法從伺服器解析網域控制器名稱、您應該修正DNS解析。

6. 按一下「確定」。

設定「IIS應用程式集區」以啟用Active Directory讀取權限

您可以在Windows伺服器上設定Internet Information Services (IIS)、以便在需要啟用Active Directory的SnapCenter 讀取權限以供使用時建立自訂的應用程式集區帳戶。

步驟

1. 在SnapCenter 安裝了Windows*的Windows Server上開啟「IIS管理員」。
2. 在左導覽窗格中、按一下*應用程式集區*。
3. 在SnapCenter 「應用程式集區」清單中選取「功能」、然後按一下「動作」窗格中的「進階設定」。
4. 選取「Identity」、然後按一下「...」以編輯SnapCenter 該應用程式集區的身分識別。
5. 在「自訂帳戶」欄位中、輸入具有Active Directory讀取權限的網域使用者或網域管理員帳戶名稱。
6. 按一下「確定」。

自訂帳戶會取代SnapCenter 適用於整個應用程式集區的內建ApplicationPoolIdentity帳戶。

設定LDAPS的CA用戶端憑證

當Windows Active Directory LDAPS設定為使用CA憑證時、您應該在SnapCenter 列舉伺服器上設定LDAPS的CA用戶端憑證。

步驟

1. 移至Microsoft管理主控台 (MMC)、然後按一下*檔案*>*新增/移除Snapin*。
2. 在「新增或移除嵌入式管理單元」視窗中、選取「憑證」、然後按一下「新增」。
3. 在「憑證」嵌入式管理單元視窗中、選取「電腦帳戶」選項、然後按一下「完成」。
4. 按一下*主控台根目錄*>*憑證-本機電腦*>*信任的根憑證授權單位*>*憑證*。
5. 在「Trusted Root Certification Authorities」(受信任的根憑證授權單位) 資料夾上按一下滑鼠右鍵、然後選取「* All Tasks」(所有工作) > 「Import」(匯入) 以啟動匯入精靈。
6. 完成精靈、如下所示：

在此精靈視窗中...	請執行下列動作...
在精靈的第二頁	按一下*瀏覽*、選取根憑證_、然後按一下*下一步*。
完成「憑證匯入精靈」	檢閱摘要、然後按一下「完成」開始匯入。

7. 針對中繼憑證重複步驟5和6。

版權資訊

Copyright © 2026 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 保留隨時變更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。