安裝並設定SnapCenter伺服器

SnapCenter software

NetApp
November 06, 2025

目錄

安裝並設定SnapCenter伺服器

準備安裝SnapCenter伺服器

安裝SnapCenter伺服器的要求

在 Windows 或 Linux 主機上安裝SnapCenter Server 之前，您應該檢查並確保滿足您的環境的所有要求。

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。

具有管理員權限的使用者可以安裝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 主機上本機管理員群組的成員。
- 工作群組：您必須使用具有本機管理員權限的本機帳戶。

雖然支援域信任、多域林和跨域信任，但不支援跨林域。有關 Active Directory 網域和信任的 Microsoft 文件包含更多資訊。

> 安裝SnapCenter伺服器後，您不應變更SnapCenter主機所在的網域。如果從安裝SnapCenter Server 時所在的網域中移除SnapCenter Server 主機，然後嘗試解除安裝SnapCenter Server，則解除安裝作業將會失敗。

空間和尺寸要求

您應該熟悉空間和尺寸要求。

物品	**Windows** 主機需求	**Linux** 主機需求
作業系統	微軟 Windows 僅支援英文、德文、日文和簡體中文版本的作業系統。 有關受支援版本的最新信息，請參閱https://imt.netapp.com/matrix/imt.jsp?components=121033;&solution=1258&isHWU&src=IMT["NetApp 互通性表工具"^]。	• Red Hat Enterprise Linux (RHEL) 8 與 9 • SUSE Linux 企業伺服器 (SLES) 15 有關受支援版本的最新信息，請參閱https://imt.netapp.com/matrix/imt.jsp?components=121032;&solution=1258&isHWU&src=IMT["NetApp 互通性表工具"^]。
最小 CPU 數量	4 核	4 核

物品	**Windows** 主機需求	**Linux** 主機需求
最低記憶體	8GB MySQL 伺服器緩衝池使用了總 RAM 的 20%。	8GB
SnapCenter伺服器軟體和日誌的最小硬碟空間	7GB 如果SnapCenter儲存庫與安裝SnapCenter Server 的磁碟機位於相同磁碟機中，則建議使用 15 GB。	15GB
SnapCenter儲存庫的最小硬碟空間	8GB 注意：如果SnapCenter伺服器與安裝SnapCenter儲存庫的磁碟機相同，建議使用 15 GB。	不適用
所需軟體包	• ASP.NET Core Runtime 8.0.12（以及所有後續 8.0.x 修補程式）託管包 • PowerShell 7.4.2 或更高版本 有關 .NET 特定的故障排除信息，請參閱 "對於沒有 Internet 連線的傳統系統， SnapCenter升級或安裝失敗"。	• .NET Framework 8.0.12（以及所有後續的 8.0.x 修補程式） • PowerShell 7.4.2 或更高版本 • Nginx 是一個可以用作反向代理的 Web 伺服器 • Pam-devel PAM（可插入式身份驗證模組）是一種系統安全工具，它允許系統管理員設定身份驗證策略，而無需重新編譯執行身份驗證的程式。

ASP.NET 核心需要 IIS_IUSRS 才能存取 Windows 上SnapCenter Server 中的暫存檔案系統。

SAN 主機需求

SnapCenter不包括主機實用程式或 DSM。如果SnapCenter主機是 SAN（FC/iSCSI）環境的一部分，則可能需要在SnapCenter Server 主機上安裝和設定其他軟體。

- 主機實用程式：主機實用程式支援 FC 和 iSCSI，它使您能夠在 Windows 伺服器上使用 MPIO。 "了解更多"

。

- Microsoft DSM for Windows MPIO：軟體與 Windows MPIO 驅動程式搭配使用，以管理NetApp和 Windows 主機之間的多條路徑。高可用性配置需要 DSM。

> 如果您使用的是ONTAP DSM，則應該遷移到 Microsoft DSM。有關更多信息，請參閱 "如何從ONTAP DSM 遷移到 Microsoft DSM" 。

瀏覽器要求

SnapCenter software支援 Chrome 125 及更高版本以及 Microsoft Edge 110.0.1587.17 及更高版本。

端口要求

SnapCenter software需要不同的連接埠來實現不同元件之間的通訊。

- 應用程式不能共享連接埠。
- 對於可自訂的端口，如果您不想使用預設端口，您可以在安裝期間選擇自訂端口。
- 對於固定端口，您應該接受預設端口號。
- 防火牆
  - 防火牆、代理或其他網路設備不應幹擾連線。
  - 如果在安裝SnapCenter時指定自訂端口，則應在插件主機上為SnapCenter插件Loader的該連接埠新增防火牆規則。

下表列出了不同的連接埠及其預設值。

連接埠名稱	連接埠號	協定	方向	描述
SnapCenter Web 連接埠	8146	HTTPS	雙向	此連接埠用於SnapCenter用戶端（ SnapCenter用戶）與SnapCenter伺服器之間的通信，也用於從插件主機到SnapCenter伺服器的通訊。 您可以自訂連接埠號。
SnapCenter SMCore 通訊端口	8145	HTTPS	雙向	此連接埠用於SnapCenter伺服器與安裝了SnapCenter插件的主機之間的通訊。 您可以自訂連接埠號。

連接埠名稱	連接埠號	協定	方向	描述
調度程序服務端口	8154	HTTPS		此連接埠用於以集中方式協調SnapCenter伺服器主機內所有託管插件的SnapCenter調度程序工作流程。 您可以自訂連接埠號。
RabbitMQ 端口	5672	TCP		這是 RabbitMQ 監聽的預設端口，用於 Scheduler 服務和SnapCenter之間的發布者-訂閱者模型通訊。
MySQL 連接埠	3306	HTTPS		此連接埠用於與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。"了解更多"
Windows 插件主機	135，445	TCP		此連接埠用於SnapCenter伺服器與安裝插件的主機之間的通訊。Microsoft 指定的其他動態連接埠範圍也應開放。
Linux 或 AIX 插件主機	22	SSH	單向	此連接埠用於SnapCenter伺服器和主機之間的通信，從伺服器發起到客戶端主機。
適用於 Windows、Linux 或 AIX 的SnapCenter插件包	8145	HTTPS	雙向	此連接埠用於SMCore與安裝插件包的主機進行通訊。可客製化。 您可以自訂連接埠號。

連接埠名稱	連接埠號	協定	方向	描述
適用於 Oracle 資料庫的SnapCenter插件	27216			Oracle 插件使用預設 JDBC 連接埠來連接 Oracle 資料庫。
適用於 Exchange 資料庫的SnapCenter插件	909			Windows 插件使用預設的 NET.TCP 連接埠來連接 Exchange VSS 回呼。
NetApp支援的SnapCenter插件	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。
ONTAP叢集或 SVM 通訊埠	• 443（HTTPS） • 80（HTTP）	• HTTPS • HTTP	雙向	此連接埠由 SAL（儲存抽象層）用於執行SnapCenter Server 的主機和 SVM 之間的通訊。SnapCenter for Windows 插件主機上的 SAL 目前也使用該連接埠來實作SnapCenter插件主機和 SVM 之間的通訊。
適用於 SAP HANA 資料庫的SnapCenter插件	• 3instance_number13 • 3instance_number15	• HTTPS • HTTP	雙向	對於多租戶資料庫容器（MDC）單一租戶，連接埠號碼以13結尾；對於非MDC，連接埠號碼以15結尾。 您可以自訂連接埠號。

連接埠名稱	連接埠號	協定	方向	描述
適用於 PostgreSQL 的SnapCenter插件	5432			此連接埠是 PostgreSQL 外掛程式與 PostgreSQL 叢集通訊所使用的預設 PostgreSQL 連接埠。 您可以自訂連接埠號。

註冊以存取**SnapCenter software**

如果您是Amazon FSx for NetApp ONTAP或Azure NetApp Files 的新使用者且沒有現有的NetApp帳戶，則應該註冊以存取SnapCenter software。

開始之前

- 您應該可以存取公司電子郵件 ID。
- 如果您使用Azure NetApp Files，則應該擁有 Azure 訂閱 ID。
- 如果您使用的是Amazon FSx for NetApp ONTAP，則應該擁有 FSx for ONTAP檔案系統的檔案系統 ID。

關於此任務

您的註冊需要經過資訊驗證，可能需要一天時間才能確認並將新的NetApp支援網站 (NSS) 帳戶從 訪客 存取權限升級為 完全 存取權限。

步驟

1. 點選 https://mysupport.netapp.com/site/user/registration進行註冊。
2. 輸入您的公司電子郵件 ID，完成驗證碼，接受 NetApp 的隱私權政策，然後按一下「提交」。
3. 透過輸入發送到您的電子郵件 ID 的 OTP 來驗證註冊，然後按一下「繼續」*。
4. 在註冊完成頁面，輸入以下詳細資訊以完成註冊。
   a. 選擇* NetApp客戶/最終使用者*。
   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。

您可以提交以下票證： https://mysupport.netapp.com/site/help如果您在註冊過程中遇到任何問題或想了解狀態。

多重身份驗證 **(MFA)**

管理多重身分驗證 **(MFA)**

您可以管理 Active Directory 聯合驗證服務 (AD FS) 伺服器和SnapCenter伺服器中的多重驗證 (MFA) 功能。

啟用多重身份驗證 (MFA)

您可以使用 PowerShell 指令為SnapCenter Server 啟用 MFA 功能。

關於此任務

- 當在相同 AD FS 中設定其他應用程式時， SnapCenter支援基於 SSO 的登入。在某些 AD FS 配置中，SnapCenter可能會出於安全性原因要求使用者進行身份驗證，具體取決於 AD FS 會話持久性。
- 可以透過執行以下命令來取得有關可與 cmdlet 一起使用的參數及其描述的信息 `Get-Help command_name`。或者，您也可以查看 "SnapCenter軟體 Cmdlet 參考指南"。

開始之前

- Windows Active Directory 聯合驗證服務 (AD FS) 應該會在對應的網域中啟動並執行。
- 您應該擁有 AD FS 支援的多重驗證服務，例如 Azure MFA、 Cisco Duo 等。
- 無論時區為何， SnapCenter和 AD FS 伺服器時間戳記都應該相同。
- 為SnapCenter Server 採購並配置授權 CA 憑證。

  由於以下原因，CA 證書是強制性的：

  - 確保 ADFS-F5 通訊不會中斷，因為自簽名憑證在節點層級是唯一的。
  - 確保在獨立或高可用性配置中的升級、修復或災難復原 (DR) 期間，不會重新建立自簽名證書，從而避免重新配置 MFA。
  - 確保 IP-FQDN 解析。

    有關 CA 憑證的信息，請參閱"產生CA憑證CSR文件"。

步驟

1. 連線至 Active Directory 聯合驗證服務 (AD FS) 主機。
2. 從下列位置下載 AD FS 聯合元資料文件"https://<hostFQDN>/FederationMetadata/2007-06/FederationMetadata.xml」。
3. 將下載的檔案複製到SnapCenter Server 以啟用 MFA 功能。
4. 透過 PowerShell 以SnapCenter管理員使用者身分登入SnapCenter伺服器。
5. 使用 PowerShell 會話，使用 *New-SmMultifactorAuthenticationMetadata -path* cmdlet 產生SnapCenter MFA 元資料檔。

   path 參數指定在SnapCenter Server 主機中儲存 MFA 元資料檔案的路徑。
6. 將產生的檔案複製到 AD FS 主機以將SnapCenter配置為客戶端實體。
7. SnapCenter `Set-SmMultiFactorAuthentication`命令。
8. （可選）使用以下方式檢查 MFA 配置狀態和設置 `Get-SmMultiFactorAuthentication`命令。
9. 前往 Microsoft 管理控制台 (MMC) 並執行下列步驟：
   a. 按一下“檔案”>“新增/刪除管理單元”。
   b. 在“新增或刪除管理單元”視窗中，選擇“證書”，然後按一下“新增”。
   c. 在憑證管理單元視窗中，選擇「電腦帳戶」選項，然後按一下「完成」。

d. 按一下 控制台根 > 憑證 - 本機 > 個人 > 憑證。

e. 右鍵點選綁定到SnapCenter 的CA 證書，然後選擇 所有任務 > 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. 點擊*位置*並選擇相關主機（層次結構的頂部）。

iii. 在「位置」彈出視窗中按一下「確定」。

iv. 在物件名稱欄位中，輸入“IIS_IUSRS”，然後按一下“檢查名稱”，然後按一下“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 管理精靈並執行下列步驟：

a. 右鍵點選*依賴方信任*>*新增依賴方信任*>*開始*。

b. 選擇第二個選項並瀏覽SnapCenter MFA 元資料文件，然後按一下「下一步」。

c. 指定顯示名稱並按一下“下一步”。

d. 根據需要選擇存取控制策略，然後按一下「下一步」。

e. 在下一個選項卡中選擇預設設定。

f. 按一下“完成”。

SnapCenter現在反映為具有所提供顯示名稱的依賴方。

11. 選擇名稱並執行以下步驟：

a. 按一下「編輯索賠簽發政策」。

b. 按一下“新增規則”，然後按一下“下一步”。

c. 指定聲明規則的名稱。

d. 選擇*Active Directory*作為屬性儲存。

e. 選擇屬性為 **User-Principal-Name**，傳出宣告類型為 **Name-ID**。

f. 按一下“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. 執行下列步驟以確認元資料已成功匯入。

a. 右鍵點選信賴方信任並選擇“屬性”。

b. 確保端點、標識符和簽名欄位已填入。

14. 關閉所有瀏覽器標籤並重新開啟瀏覽器以清除現有或活動的會話 cookie，然後再次登入。

SnapCenter MFA 功能也可以使用 REST API 啟用。

有關故障排除信息，請參閱 "在多個選項卡中同時嘗試登入時顯示 MFA 錯誤"。

更新 **AD FS MFA** 元數據

每當 AD FS 伺服器發生任何修改（例如昇級、CA 憑證續約、DR 等）時，您都應該更新SnapCenter中的 AD FS MFA 元資料。

步驟

1. 從下列位置下載 AD FS 聯合元資料文件"https://<hostFQDN>/FederationMetadata/2007-06/FederationMetadata.xml”
2. 將下載的檔案複製到SnapCenter Server 以更新 MFA 設定。
3. 透過執行以下 cmdlet 更新SnapCenter中的 AD FS 元資料：

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

4. 關閉所有瀏覽器標籤並重新開啟瀏覽器以清除現有或活動的會話 cookie，然後再次登入。

更新**SnapCenter MFA** 元數據

每當 ADFS 伺服器發生任何修改（例如修復、CA 憑證續約、DR 等）時，您都應該更新 AD FS 中的SnapCenter MFA 元資料。

步驟

1. 在 AD FS 主機中，開啟 AD FS 管理精靈並執行下列步驟：
   a. 選擇*依賴方信任*。
   b. 右鍵點選為SnapCenter建立的信賴方信任並選擇「刪除」。

      將顯示依賴方信任的使用者定義名稱。

   c. 啟用多重身份驗證 (MFA)。

      看"啟用多重身份驗證" 。
2. 關閉所有瀏覽器標籤並重新開啟瀏覽器以清除現有或活動的會話 cookie，然後再次登入。

停用多重身份驗證 **(MFA)**

步驟

1. 停用 MFA 並清理啟用 MFA 時建立的設定文件，方法是使用 `Set-SmMultiFactorAuthentication`命令。
2. 關閉所有瀏覽器標籤並重新開啟瀏覽器以清除現有或活動的會話 cookie，然後再次登入。

使用 **Rest API**、**PowerShell** 和 **SCCLI** 管理多重驗證 **(MFA)**

支援透過瀏覽器、REST API、PowerShell 和 SCCLI 進行 MFA 登入。 MFA 透過 AD FS 身份管理器支援。您可以從 GUI、REST API、PowerShell 和 SCCLI 啟用 MFA、停用 MFA 和設定 MFA。

將 **AD FS** 設定為 **OAuth/OIDC**

使用 **Windows GUI** 精靈設定 **AD FS**

1. 導覽至 伺服器管理員儀表板 > 工具 > **ADFS** 管理。
2. 導覽至 **ADFS** > 應用程式群組。
   a. 右鍵點選“應用程式群組”。
   b. 選擇*新增應用程式群組*並輸入*應用程式名稱*。
   c. 選擇*伺服器應用程式*。
   d. 按一下“下一步”。
3. 複製*客戶端識別碼*。

   這是客戶端 ID。 ..在重新導向 URL 中新增回呼 URL（SnapCenter伺服器 URL）。 ..按一下“下一步”。
4. 選擇*產生共享金鑰*。

   複製秘密值。這是客戶的秘密。 ..按一下“下一步”。
5. 在「摘要」頁面上，按一下「下一步」。
   a. 在*完成*頁面上，按一下*關閉*。
6. 右鍵點選新新增的*應用程式群組*並選擇*屬性*。
7. 從應用程式屬性中選擇*新增應用程式*。
8. 點擊“新增應用程式”。

   選擇 Web API 並按一下「下一步」。
9. 在設定 Web API 頁面上，將上一個步驟建立的SnapCenter伺服器 URL 和用戶端識別碼輸入到識別碼部分。
   a. 按一下“新增”。
   b. 按一下“下一步”。
10. 在*選擇存取控制策略*頁面上，根據您的要求選擇控制策略（例如，允許所有人並要求 MFA），然後按一下*下一步*。
11. 在*配置應用程式權限*頁面，預設選擇openid作為範圍，點擊*下一步*。
12. 在「摘要」頁面上，按一下「下一步」。

    在*完成*頁面上，按一下*關閉*。
13. 在「範例應用程式屬性」頁面上，按一下「確定」。
14. JWT 令牌由授權伺服器（AD FS）頒發，供資源使用。

    此令牌的「aud」或受眾聲明必須與資源或 Web API 的識別碼相符。
15. 編輯選定的 WebAPI 並檢查回呼 URL（SnapCenter伺服器 URL）和用戶端識別碼是否正確新增。

    配置 OpenID Connect 以提供使用者名稱作為聲明。

16. 開啟位於伺服器管理員右上角*工具*選單下的*AD FS 管理*工具。
    a. 從左側邊欄中選擇“應用程式群組”資料夾。
    b. 選擇 Web API 並點選 **EDIT**。
    c. 前往發行轉換規則標籤
17. 按一下“新增規則”。
    a. 在聲明規則範本下拉選單中選擇*將 LDAP 屬性作為聲明傳送*。
    b. 按一下“下一步”。
18. 輸入*聲明規則*名稱。
    a. 在屬性儲存下拉選單中選擇*Active Directory*。
    b. 在 **LDAP Attribute** 下拉選單中選擇 **User-Principal-Name**，在 O*utgoing Claim Type* 下拉選單中選擇 **UPN**。
    c. 按一下“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 並新增範圍和聲明。這些命令以自動腳本格式提供。欲了解更多信息，請參閱<連結至知識庫文章>。

1. 使用以下命令在 AD FS 中建立新的應用程式組。

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

   `ClientRoleIdentifier`您的應用程式群組的名稱

   `redirectURL`授權後重定向的有效 URL

2. 建立 AD FS 伺服器應用程式並產生客戶端機密。

   ```
   Add-AdfsServerApplication -Name "$ClientRoleIdentifier - Server app"
   -ApplicationGroupIdentifier $ClientRoleIdentifier -RedirectUri $redirectURL
   -Identifier $identifier -GenerateClientSecret
   ```

3. 建立 ADFS Web API 應用程式並配置其應使用的策略名稱。

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

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

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

4. 從以下命令的輸出中取得客戶端 ID 和客戶端金鑰，因為它只顯示一次。

   ```
   "client_id = $identifier"

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

5. 授予 AD FS 應用程式 allatclaims 和 openid 權限。

```
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。

```
$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文件定義其頒發轉換規則。

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

$identifier -Identifier $identifier,$redirectURL -IssuanceTransformRulesFile

$relativePath
```

更新訪問令牌到期時間

您可以使用 PowerShell 指令更新存取權杖的到期時間。

關於此任務

- 存取令牌只能用於使用者、用戶端和資源的特定組合。存取令牌不能被撤銷，並且在到期前有效。
- 預設情況下，存取令牌的有效期為 60 分鐘。此最短到期時間足夠且可擴充。您必須提供足夠的價值以避免任何正在進行的關鍵業務工作。

步

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** 取得持有者令牌

您應該在任何 REST 用戶端（如 Postman）中填寫下面提到的參數，它會提示您填寫使用者憑證。此外，您應該輸入第二因素身份驗證（您擁有的東西和您是的東西）來獲取承載令牌。

+ 持有者令牌的有效性可根據應用程式從 AD FS 伺服器進行配置，預設有效期為 60 分鐘。

場地	價值
資助類型	授權碼
回調URL	如果您沒有回調 URL，請輸入應用程式的基本 URL。
授權網址	[adfs 網域]/adfs/oauth2/授權
訪問令牌 URL	[adfs 網域]/adfs/oauth2/token
客戶端 ID	輸入 AD FS 用戶端 ID
客戶端機密	輸入 AD FS 用戶端機密
範圍	OpenID
客戶端身份驗證	作為基本 AUTH 標頭發送
資源	在「進階選項」標籤中，新增與回呼 URL 具有相同值的資源字段，該字段會作為 JWT 令牌中的「aud」值出現。

使用 **PowerShell**、**SCCLI** 和 **REST API** 在**SnapCenter Server** 中設定 **MFA**

您可以使用 PowerShell、SCCLI 和 REST API 在SnapCenter Server 中設定 MFA。

SnapCenter MFA CLI 身份驗證

在 PowerShell 和 SCCLI 中，現有的 cmdlet（Open-SmConnection）擴展了一個名為「AccessToken」的字段，以使用承載令牌對使用者進行身份驗證。

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

執行上述 cmdlet 後，將為對應使用者建立一個會話以執行進一步的SnapCenter cmdlet。

SnapCenter MFA Rest API 驗證

在 REST API 用戶端（如 Postman 或 swagger）中使用格式為 *Authorization=Bearer <access token>* 的承載令

牌，並在標頭中提及使用者 RoleName 以從SnapCenter獲得成功回應。

MFA Rest API 工作流程

當使用 AD FS 設定 MFA 時，您應該使用存取（承載）令牌進行身份驗證，以透過任何 Rest API 存取SnapCenter應用程式。

關於此任務

- 您可以使用任何 REST 用戶端，例如 Postman、Swagger UI 或 FireCamp。
- 取得存取權杖並使用它來驗證後續請求（SnapCenter Rest API）以執行任何操作。

步驟

透過 **AD FS MFA** 進行身份驗證

1. 配置 REST 用戶端以呼叫 AD FS 端點來取得存取權杖。

   當您點擊按鈕以取得應用程式的存取權杖時，您將被重新導向至 AD FS SSO 頁面，您必須在該頁面提供您的 AD 憑證並使用 MFA 進行驗證。1.在 AD FS SSO 頁面中，在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. 點選“登入”。
4. 從*登入選項*部分，選擇一個身份驗證選項並進行身份驗證（取決於您的配置）。
   - 推播：批准發送到您手機的推播通知。
   - 二維碼：使用 AUTH Point 手機應用程式掃描二維碼，然後輸入應用程式中顯示的驗證碼
   - 一次性密碼：輸入您的令牌的一次性密碼。
5. 身份驗證成功後，將開啟一個彈出窗口，其中包含存取、ID 和刷新令牌。

   複製存取權杖並在SnapCenter Rest API 中使用它來執行操作。

6. 在 Rest API 中，您應該在標題部分傳遞存取權杖和角色名稱。
7. SnapCenter從 AD FS 驗證此存取權杖。

   如果它是有效令牌， SnapCenter會對其進行解碼並取得使用者名稱。

8. SnapCenter使用使用者名稱和角色名稱對使用者進行身份驗證以執行 API。

   如果驗證成功， SnapCenter將傳回結果，否則將顯示錯誤訊息。

為 **Rest API**、**CLI** 和 **GUI** 啟用或停用**SnapCenter MFA** 功能

圖形使用者介面

步驟

1. 以SnapCenter管理員身分登入SnapCenter伺服器。
2. 點擊“設定”>“全域設定”>“多重身份驗證 (MFA) 設定”
3. 選擇介面（GUI/RST 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 GUI、Rest API、PowerShell 和 SCCLI 的 MFA。

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

   路徑參數指定 AD FS MFA 元資料 xml 檔案的位置。

   使用指定的 AD FS 元資料檔案路徑配置的SnapCenter GUI、Rest API、PowerShell 和 SCCLI 啟用 MFA。

2. 使用 `Get-SmMultiFactorAuthentication`命令。

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

1. 執行以下文章 API 以啟用 GUI、Rest API、PowerShell 和 SCCLI 的 MFA。

範圍	價值
請求的 URL	/api/4.9/settings/multifactorauthentication
HTTP 方法	郵政
請求正文	{ “IsGuiMFAEnabled”：false ，「IsRestApiMFAEnabled」：true ，「IsCliMFAEnabled」：false ，「ADFSConfigFilePath」 ：「C:\\ADFS_metadata\\abc.xml」}

回應主體	{ “MFAConfiguration”：{ “IsGuiMFAEnabled”：false ，“ADFSConfigFilePath”：“C：\\ADFS_metadata \\abc.xml”， 「SCConfigFilePath」：null ，「IsRestApiMFAEnabled」：true ，「IsCliMFAEnabled」：false ，「ADFSHostName」：「win-adfs-sc49.winscedom2.com」 } }

2. 使用以下 API 檢查 MFA 配置狀態和設定。

範圍	價值
請求的 URL	/api/4.9/settings/multifactorauthentication
HTTP 方法	得到
回應主體	{ “MFAConfiguration”：{ “IsGuiMFAEnabled”：false ，“ADFSConfigFilePath”：“C：\\ADFS_metadata \\abc.xml”， 「SCConfigFilePath」：null ，「IsRestApiMFAEnabled」：true ，「IsCliMFAEnabled」：false ，「ADFSHostName」：「win-adfs-sc49.winscedom2.com」 } }

安裝SnapCenter伺服器

在 Windows 主機上安裝SnapCenter伺服器

您可以執行SnapCenter Server 安裝程式執行檔來安裝SnapCenter Server。

您可以選擇使用 PowerShell cmdlet 執行多個安裝和設定程序。您應該使用 PowerShell 7.4.2 或更高版本。

不支援從命令列靜默安裝SnapCenter伺服器。

開始之前

- SnapCenter伺服器主機必須保持最新的 Windows 更新，且無需重新啟動系統。
- 您應該確保計劃安裝SnapCenter伺服器的主機上未安裝 MySQL 伺服器。
- 您應該啟用 Windows 安裝程式偵錯。

  有關啟用 "Windows 安裝程式日誌記錄"。

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

步驟

1. 從下列位置下載SnapCenter Server 安裝包 "NetApp支援站點"。
2. 雙擊下載的 .exe 檔案啟動SnapCenter Server 安裝。

   啟動安裝後，將執行所有預檢查，如果不符合最低要求，則會顯示相應的錯誤或警告訊息。

   您可以忽略警告訊息並繼續安裝；但是，錯誤應該得到修復。

3. 查看SnapCenter伺服器安裝所需的預先填入值並根據需要進行修改。

   您不必指定 MySQL 伺服器儲存庫資料庫的密碼。在SnapCenter Server 安裝期間，密碼會自動產生。

   特殊字元“`%`" is not supported in the custom path for the repository database. If you include " %`”，則安裝失敗。

4. 按一下“立即安裝”。

   如果您指定的任何值無效，則會顯示相應的錯誤訊息。您應該重新輸入這些值，然後啟動安裝。

   如果點選*取消*按鈕，正在執行的步驟將會完成，然後開始回溯操作。 SnapCenter伺服器將從主機中完全刪除。

   但是，如果在執行“SnapCenter Server 網站重新啟動”或“等待SnapCenter Server 啟動”操作時按一下“取消”，則安裝將繼續進行而不會取消操作。

   日誌檔案始終列在管理員使用者的 %temp% 資料夾中（最早的在前）。如果要重新導向日誌位置，請透過執行下列命令從命令提示字元啟動SnapCenter Server 安裝
   ：`C:\installer_location\installer_name.exe /log"C:\"`

安裝期間在 **Windows** 主機上啟用的功能

SnapCenter Server 安裝程式在安裝期間在 Windows 主機上啟用 Windows 功能和角色。這些可能對故障排除和維護主機系統有用。

類別	特徵
Web 伺服器	• 網路資訊服務 • 萬維網服務 • 常見 HTTP 功能 ◦ 預設文檔 ◦ 目錄瀏覽 ◦ HTTP 錯誤 ◦ HTTP 重新導向 ◦ 靜態內容 ◦ WebDAV 發布 • 健康與診斷 ◦ 自訂日誌 ◦ HTTP 日誌記錄 ◦ 測井工具 ◦ 請求監控 ◦ 追蹤 • 性能特點 ◦ 靜態內容壓縮 • 安全 ◦ IP 安全 ◦ 基本驗證 ◦ 集中式 SSL 憑證支持 ◦ 用戶端憑證對應認證 ◦ IIS 用戶端憑證對應驗證 ◦ IP 和網域限制 ◦ 請求過濾 ◦ URL 授權 ◦ Windows 驗證 • 應用程式開發功能 ◦ .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）託管包 ◦ 伺服器端包含 ◦ WebSocket 協議 管理工具
	◦ IIS 管理控制台

類別	特徵
IIS 管理腳本和工具	• IIS 管理服務 • Web管理工具
.NET Framework 8.0.12 功能	• ASP.NET Core Runtime 8.0.12（以及所有後續 8.0.x 修補程式）託管包 • Windows Communication Foundation (WCF) HTTP 啟動45 ◦ TCP 啟用設定 ◦ HTTP 啟用設定 有關 .NET 特定的故障排除信息，請參閱 "對於沒有 Internet 連線的傳統系統， SnapCenter升級或安裝失敗"。
Windows 進程啟動服務	流程模型
配置 API	全部

在 **Linux** 主機上安裝**SnapCenter**伺服器

您可以執行SnapCenter Server 安裝程式執行檔來安裝SnapCenter Server。

開始之前

- 如果您想要使用沒有足夠權限安裝SnapCenter的非 root 使用者安裝SnapCenter伺服器，請從NetApp支援網站取得 sudoers 校驗和檔案。您應該根據 Linux 版本使用適當的校驗和檔案。
- 如果 SUSE Linux 中沒有 sudo 套件，請安裝 sudo 套件以避免身份驗證失敗。
- 對於SUSE Linux，請配置主機名稱以避免安裝失敗。
- 透過執行以下命令檢查 Linux 的安全狀態 `sestatus`。如果 _SELinux 狀態_為“已啟用”且 _當前模式_為“強制”，請執行下列操作：
  - 運行以下命令： `sudo semanage port -a -t http_port_t -p tcp <WEBAPP_EXTERNAL_PORT_>`

    WEBAPP_EXTERNAL_PORT 的預設值為 8146
  - 如果防火牆阻止了端口，請運行 `sudo firewall-cmd --add-port <WEBAPP_EXTERNAL_PORT_>/tcp`

    WEBAPP_EXTERNAL_PORT 的預設值為 8146
  - 從您具有讀寫權限的目錄執行以下命令：
    - `sudo ausearch -c 'nginx' --raw | audit2allow -M my-nginx`

      如果命令返回“無事可做”，請在安裝SnapCenter Server 後重新執行該命令。

- 如果命令建立了_my-nginx.pp_，則執行命令使策略包處於活動狀態： `sudo semodule -i my-nginx.pp`

◦ MySQL PID 目錄所使用的路徑是 */var/opt/mysqld*。執行以下命令設定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`

◦ MySQL 資料目錄所使用的路徑是 */INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL/*。執行以下命令設定 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`

關於此任務

- 當SnapCenter Server 安裝在 Linux 主機上時，就會安裝 MySQL、RabbitMq、Errlang 等第三方服務。您不應該卸載它們。
- Linux 主機上安裝的SnapCenter伺服器不支援：
  - 高可用性
  - Windows 外掛
  - Active Directory（僅支援本機用戶，包括具有憑證的 root 用戶和非 root 用戶）
  - 基於金鑰的身份驗證以登入SnapCenter
- 在安裝 .NET 執行時期期間，如果安裝無法解析 *libicu* 庫的依賴關係，則透過執行以下命令安裝 *libicu*： `yum install -y libicu`
- 如果由於_Perl_不可用而導致SnapCenter Server 安裝失敗，則透過執行下列命令安裝_Perl_： `yum install -y perl`

步驟

1. 從以下位置下載 "NetApp支援站點"到 */home* 目錄。
   - SnapCenter伺服器安裝套件 - * SnapCenter -linux-server-(el8/el9/sles15).bin*
   - 公鑰檔案 - **snapcenter_public_key.pub**
   - 對應的簽章檔案 - **snapcenter-linux-server-(el8/el9/sles15).bin.sig**
2. 驗證簽名文件。 `$openssl dgst -sha256 -verify snapcenter_public_key.pub -signature <path to signature file> <path to bin file>`
3. 對於非 root 使用者安裝，請新增 .bin 安裝程式隨附的 **snapcenter_server_checksum_(el8/el9/sles15).txt** 中指定的 visudo 內容。
4. 為.bin安裝程式分配執行權限。 `chmod +x snapcenter-linux-server-(el8/el9/sles15).bin`
5. 執行其中一項操作來安裝SnapCenter Server。

如果你想表演...	這樣做...
互動式安裝	`./snapcenter-linux-server-(el8/el9/sles15).bin` 系統將提示您輸入以下詳細資訊： • 用於存取 Linux 主機外部的SnapCenter伺服器的 webapp 外部連接埠。預設值為 8146。 • 將安裝SnapCenter Server 的SnapCenter Server 使用者。 • 將安裝軟體包的安裝目錄。

如果你想表演...	這樣做...
非互動式安裝	`sudo ./snapcenter-linux-server-(el8/el9/sles15).bin -i silent -DWEBAPP_EXTERNAL_PORT=<port> -DWEBAPP_INTERNAL_PORT=<port> -DSMCORE_PORT=<port> -DSCHEDULER_PORT=<port> -DSNAPCENTER_SERVER_USER=<user> -DUSER_INSTALL_DIR=<dir> -DINSTALL_LOG_NAME=<filename>` 範例：sudo ./snapcenter_linux_server.bin -i silent -DWEBAPP_EXTERNAL_PORT=8146 -DSNAPCENTER_SERVER_USER=root -DUSER_INSTALL_DIR=/opt -DINSTALL_LOG_NAME=InstallerLoglog 日誌將儲存在 */var/opt/snapcenter/logs*。 安裝SnapCenter Server 時要傳遞的參數： • DWEBAPP_EXTERNAL_PORT：用於存取 Linux 主機外部的SnapCenter伺服器的 Webapp 外部連接埠。預設值為 8146。 • DWEBAPP_INTERNAL_PORT：用於存取 Linux 主機內的SnapCenter伺服器的 Webapp 內部連接埠。預設值為 8147。 • DSMCORE_PORT：smcore 服務正在執行的 SMCore 連接埠。預設值為 8145。 • DSCHEDULER_PORT：執行調度程序服務的調度程序連接埠。預設值為 8154。 • DSNAPCENTER_SERVER_USER：將安裝SnapCenter Server 的SnapCenter Server 使用者。對於 *DSNAPCENTER_SERVER_USER*，預設值是執行安裝程式的使用者。 • DUSER_INSTALL_DIR：將安裝套件的安裝目錄。對於_DUSER_INSTALL_DIR_，預設安裝目錄是_/opt_。 • DINSTALL_LOG_NAME：儲存安裝日誌的日誌檔案名稱。這是一個可選參數，如果指定，則控制台上不會顯示任何日誌。如果不指定此參數，則日誌將顯示在控制台上，並儲存在預設日誌檔案中。 • DSELINUX：如果_SELinux 狀態_為“啟用”，_當前模式_為“強制”，並且您已執行“開始之前”部分中提到的命令，則應指定此參數並將其值指定為 1。預設值為 0。 • DUPGRADE：預設值為 0。指定此參數及其值為 0 以外的任何整數來升級SnapCenter伺服器。

下一步是什麼？

- 如果 _SELinux 狀態_為“啟用”且 _當前模式_為“強制”，則 **nginx** 服務無法啟動。您應該執行以下命令：
  a. 前往主目錄。
  b. 運行以下命令： `journalctl -x|grep nginx` 。
  c. 如果不允許Webapp內部連接埠（8147）監聽，則執行下列命令：
     - `ausearch -c 'nginx' --raw | audit2allow -M my-nginx`
     - `semodule -i my-nginx.pp`
  d. 跑步 `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產品的新用戶且沒有現有的NetApp帳戶，則應該註冊SnapCenter以獲得支援。

步驟

1. 安裝SnapCenter後，導覽至 幫助 **>** 關於。
2. 在「關於 SnapCenter」對話方塊中，記下SnapCenter實例，這是一個以 971 開頭的 20 位數。
3. 點選 https://register.netapp.com。
4. 點擊“我不是註冊的**NetApp**客戶”。
5. 指定您的詳細資料以進行註冊。
6. 將NetApp參考 SN 欄位留空。
7. 從產品線下拉式選單中選擇* SnapCenter*。
8. 選擇計費提供者。
9. 輸入 20 位元SnapCenter執行個體 ID。
10. 點選“提交”。

使用 **RBAC** 授權登入**SnapCenter**

SnapCenter支援基於角色的存取控制 (RBAC)。 SnapCenter管理員透過SnapCenter RBAC 將角色和資源分配給工作群組或活動目錄中的用戶，或活動目錄中的群組。 RBAC 使用者現在可以使用指派的角色登入SnapCenter 。

開始之前

- 您應該在 Windows 伺服器管理員中啟用 Windows 進程啟動服務 (WAS)。

- 如果您想要使用 Internet Explorer 作為瀏覽器登入SnapCenter伺服器，則應確保 Internet Explorer 中的保護模式已停用。
- 如果SnapCenter Server 安裝在 Linux 主機上，則應使用用於安裝SnapCenter Server 的使用者帳號登入。

關於此任務

在安裝過程中， SnapCenter伺服器安裝精靈會建立一個捷徑並將其放在桌面上和安裝SnapCenter的主機的「開始」功能表中。此外，在安裝結束時，安裝精靈會根據您在安裝期間提供的資訊顯示SnapCenter URL，如果您想從遠端系統登錄，可以複製該 URL。

如果您在 Web 瀏覽器中開啟了多個選項卡，則僅關閉SnapCenter瀏覽器標籤並不會將您登出SnapCenter。若要結束與SnapCenter的連接，您必須透過點擊「退出」按鈕或關閉整個 Web 瀏覽器來退出SnapCenter 。

*最佳實務：*出於安全原因，建議您不要啟用瀏覽器來儲存您的SnapCenter密碼。

預設 GUI URL 是與安裝SnapCenter Server 的伺服器上的預設連接埠 8146 的安全連線（*https://server:8146*）。如果您在SnapCenter安裝期間提供了不同的伺服器端口，則將使用該端口。

對於高可用性 (HA) 部署，您必須使用虛擬叢集 IP *https://Virtual_Cluster_IP_or_FQDN:8146* 存取SnapCenter。如果在 Internet Explorer (IE) 中導覽至 *https://Virtual_Cluster_IP_or_FQDN:8146* 時沒有看到SnapCenter UI，則必須在每個外掛程式主機上的 IE 中將虛擬叢集 IP 位址或 FQDN 新增為受信任的網站，或者必須在每個外掛程式主機上停用 IE 增強性。有關更多信息，請參閱 "無法從外部網路存取群集 IP 位址" 。

除了使用SnapCenter GUI 之外，您還可以使用 PowerShell cmdlet 建立腳本來執行設定、備份和復原作業。每次發布SnapCenter時，某些 cmdlet 可能會發生變化。這 "SnapCenter軟體 Cmdlet 參考指南"有詳細資料。

如果您是第一次登入SnapCenter ，則必須使用安裝過程中提供的憑證登入。

步驟

1. 從本機主機桌面上的捷徑、安裝結束時提供的 URL 或SnapCenter管理員提供的 URL 啟動SnapCenter 。
2. 輸入使用者憑證。

若要指定以下內容...	使用以下格式之一...
網域管理員	• NetBIOS\使用者名 • 使用者名稱@UPN後綴 例如，username@netapp.com • 網域 FQDN\用戶名
本機管理員	使用者名稱

3. 如果您被指派了多個角色，請從角色方塊中選擇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將顯示在SnapCenter的右上角。

結果

將顯示“儀表板”頁面。

如果日誌記錄失敗並出現無法存取網站的錯誤，則應將 SSL 憑證對應到SnapCenter。 "了解更多"

完成後

首次以 RBAC 使用者登入SnapCenter Server 後，重新整理資源清單。

如果您有不受信任的 Active Directory 網域並且希望SnapCenter支援這些網域，則必須先向SnapCenter註冊這些網域，然後再為不受信任網域上的使用者設定角色。"了解更多" 。

如果要在 Linux 主機上執行的SnapCenter中新增插件主機，則應從下列位置取得校驗和檔案：*/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。

使用多重身份驗證 **(MFA)** 登入**SnapCenter**

SnapCenter Server 支援網域帳戶的 MFA，它是活動目錄的一部分。

開始之前

您應該啟用 MFA。有關如何啟用 MFA 的信息，請參閱"啟用多重身份驗證"

關於此任務

- 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. 從本機主機桌面上的捷徑、安裝結束時提供的 URL 或SnapCenter管理員提供的 URL 啟動SnapCenter 。
2. 在 AD FS 登入頁面，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，您應該檢查以下內容：

   - 使用者名稱或密碼是否有效

     使用者帳戶應該存在於 Active Directory (AD) 中

   - 您是否超出了 AD 中設定的最大允許嘗試次數
   - AD 和 AD FS 是否已啟動並執行

修改**SnapCenter**預設 **GUI** 會話逾時

您可以修改SnapCenter GUI 會話逾時期限，使其小於或大於預設逾時期限 20 分鐘。

作為一項安全功能，在預設 15 分鐘不活動時間後， SnapCenter會警告您將在 5 分鐘內退出 GUI 工作階段。預設情況下， SnapCenter會在 20 分鐘不活動後將您從 GUI 工作階段中登出，您必須重新登入。

步驟

1. 在左側導覽窗格中，按一下「設定」>「全域設定」。
2. 在全域設定頁面中，按一下*配置設定*。
3. 在會話逾時欄位中，輸入新的會話逾時時間（分鐘），然後按一下「儲存」。

透過停用 **SSL 3.0** 來保護**SnapCenter Web** 伺服器

出於安全目的，如果您的SnapCenter Web 伺服器上啟用了安全通訊端層 (SSL) 3.0 協議，則應在 Microsoft IIS 中停用該協定。

SSL 3.0 協定有缺陷，攻擊者可以利用這些缺陷導致連線失敗，或進行中間人攻擊並觀察您的網站與其訪客之間的加密流量。

步驟

1. 若要在SnapCenter Web 伺服器主機上啟動登錄編輯器，請按一下“開始”>“執行”，然後輸入 regedit。
2. 在登錄編輯器中，導覽至 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\。
   - 如果伺服器金鑰已經存在：
     i. 選擇已啟用的 DWORD，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”>“新建”>“金鑰”，然後將金鑰命名為“伺服器”。
     ii. 選擇新的伺服器金鑰後，按一下*編輯* > 新建 > **DWORD**。
     iii. 將新的 DWORD 命名為 Enabled，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，使SnapCenter能夠存取ONTAP儲存、 ASA r2 系統或Amazon FSx for NetApp ONTAP來執行資料保護和設定作業。

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

開始之前

- 您應該擁有基礎設施管理員角色所需的權限來建立儲存連線。
- 您應該確保插件安裝沒有正在進行中。

新增儲存系統連線時，不得進行主機外掛程式安裝，因為主機快取可能不會更新，且資料庫狀態可能會在SnapCenter GUI 中顯示為「不可用於備份」或「不在NetApp儲存上」。

- 儲存系統名稱應該是唯一的。

  SnapCenter不支援不同叢集上具有相同名稱的多個儲存系統。 SnapCenter支援的每個儲存系統都應具有唯一的名稱和唯一的資料 LIF IP 位址。

關於此任務

- 配置儲存系統時，您還可以啟用事件管理系統 (EMS) 和AutoSupport功能。 AutoSupport工具收集有關係統健康狀況的數據，並自動將數據發送給NetApp技術支持，使他們能夠排除系統故障。

  如果啟用這些功能，當資源受到保護、還原或複製作業成功完成或操作失敗時， SnapCenter會將AutoSupport資訊傳送至儲存系統，並將 EMS 訊息傳送至儲存系統系統日誌。

- 如果您打算將快照複製到SnapMirror目標或SnapVault目標，則必須為目標 SVM 或叢集以及來源 SVM 或叢集設定儲存系統連線。

如果變更儲存系統密碼，排程作業、按需備份和復原作業可能會失敗。更改儲存系統密碼後，您可以透過點擊「儲存」標籤中的「修改」來更新密碼。

步驟

1. 在左側導覽窗格中，按一下「儲存系統」。
2. 在儲存系統頁面中，按一下*新建*。
3. 在新增儲存系統頁面中，提供以下資訊：

對於這個領域...	這樣做...
儲存系統	輸入儲存系統名稱或IP位址。 儲存系統名稱（不包括網域名稱）必須包含 15 個或更少的字符，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接，可以使用 Add-SmStorageConnectionPowerShell cmdlet。 對於具有MetroCluster配置 (MCC) 的儲存系統，建議同時註冊本地集群和對等集群，以實現無中斷操作。 SnapCenter不支援不同叢集上具有相同名稱的多個 SVM。 SnapCenter支援的每個 SVM 都必須具有唯一的名稱。 將儲存連線新增至SnapCenter後，不應使用ONTAP重命名 SVM 或叢集。 如果使用短名稱或 FQDN 新增了 SVM，則它必須能夠從SnapCenter和外掛程式主機解析。
使用者名稱/密碼	輸入具有存取儲存系統所需權限的儲存使用者的憑證。
事件管理系統 (EMS) 和AutoSupport設置	如果您想要將 EMS 訊息傳送到儲存系統 syslog，或想要將AutoSupport訊息傳送到儲存系統以套用保護、完成還原作業或失敗操作，請選取對應的核取方塊。 當您勾選 向儲存系統發送失敗操作的**AutoSupport** 通知 複選框時，也會選取 將**SnapCenter**伺服器事件記錄到 **syslog** 複選框，因為啟用AutoSupport通知需要 EMS 訊息傳遞。

4. 如果要修改指派給平台、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，從下拉清單中選擇一個選項。

      如果 SVM 是備份關係中的輔助儲存系統，請選取 輔助 複選框。當選擇“**Secondary**”選項時，SnapCenter不會立即執行許可證檢查。

如果您已在SnapCenter中新增了 SVM，則使用者需要從下拉清單中手動選擇平台類型。

a. 在協定中，選擇在 SVM 或叢集設定期間配置的協議，通常是 HTTPS。
b. 輸入儲存系統接受的連接埠。

   預設連接埠 443 通常有效。

c. 輸入停止通訊嘗試前應經過的時間（以秒為單位）。

   預設值為 60 秒。

d. 如果 SVM 有多個管理接口，請勾選「首選 **IP**」複選框，然後輸入 SVM 連接的首選 IP 位址。
e. 點選“儲存”。

5. 點選“提交”。

結果

在儲存系統頁面中，從*類型*下拉式選單中執行下列其中一項：

- 如果要查看已新增的所有 SVM，請選擇 * ONTAP SVM *。

  如果您已新增 FSx SVM，則 FSx SVM 將在此處列出。

- 如果要查看所有已新增的集群，請選擇* ONTAP集群*。

  如果您已使用 fsxadmin 新增了 FSx 集群，則 FSx 集群將在此處列出。

  當您按一下叢集名稱時，叢集中的所有 SVM 都會顯示在儲存虛擬機器部分。

  如果使用ONTAP GUI 將新的 SVM 新增至ONTAP集群，請按一下 重新發現 查看新新增的 SVM。

完成後

叢集管理員必須在每個儲存系統節點上啟用AutoSupport ，以便從SnapCenter有權存取的所有儲存系統發送電子郵件通知，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。

儲存連接和憑證

在執行資料保護操作之前，您應該設定儲存連線並新增SnapCenter伺服器和SnapCenter插件將使用的憑證。

儲存連接

儲存連接使SnapCenter伺服器和SnapCenter插件能夠存取ONTAP儲存。設定這些連線也涉及設定AutoSupport和事件管理系統 (EMS) 功能。

證書

- 網域管理員或管理員群組的任何成員

  指定要安裝SnapCenter插件的系統上的網域管理員或管理員群組的任何成員。用戶名字段的有效格式為：

  - *NetBIOS*\使用者名稱
  - 域 *FQDN*\用戶名
  - 用戶名@*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，請在要安裝SnapCenter插件的系統上指定內建的本機管理員。如果使用者帳戶具有提升的權限或主機系統上停用了使用者存取控制功能，則可以指定屬於本機管理員群組的本機使用者帳戶。

  使用者名字段的有效格式為：*UserName*

- 各資源組的憑證

  如果您為單一資源群組設定憑證，且使用者名稱沒有完全管理權限，則必須至少為該使用者名稱指派資源群組和備份權限。

在 **Windows** 主機上設定儲存

建立和管理 **igroup**

您可以建立啟動器群組 (igroup) 來指定哪些主機可以存取儲存系統上的給定 LUN。您可以使用SnapCenter在 Windows 主機上建立、重新命名、修改或刪除 igroup。

建立 **igroup**

您可以使用SnapCenter在 Windows 主機上建立 igroup。當您將 igroup 對應到 LUN 時，igroup 將在建立磁碟或連線磁碟精靈中可用。

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「新建」。
4. 在建立 Igroup 對話方塊中，定義 igroup：

在這個領域...	這樣做...
儲存系統	選擇要對應到 igroup 的 LUN 的 SVM。
主持人	選擇要在其上建立 igroup 的主機。

在這個領域...	這樣做...
群組名稱	輸入 igroup 的名稱。
發起者	選擇發起者。
類型	選擇啟動器類型：iSCSI、FCP 或混合（FCP 和 iSCSI）。

5. 如果您對輸入的內容滿意，請按一下「確定」。

   SnapCenter在儲存系統上建立 igroup。

重命名 **igroup**

您可以使用SnapCenter重新命名現有的 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 **Storage Virtual Machine** 欄位以顯示可用 SVM 的列表，然後選擇要重新命名的 igroup 的 SVM。
4. 在 SVM 的 igroup 清單中，選擇要重新命名的 igroup，然後按一下「重新命名」。
5. 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將 igroup 啟動器新增至現有 igroup。建立 igroup 時，您只能新增一個主機。如果要為叢集建立 igroup，則可以修改 igroup 以將其他節點新增至該 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「**Storage Virtual Machine**」欄位以顯示可用 SVM 的下拉列表，然後選擇要修改的 igroup 的 SVM。
4. 在 igroup 清單中，選擇一個 igroup 並按一下「將啟動器新增至 igroup」。
5. 選擇主機。
6. 選擇啟動器並按一下“確定”。

刪除 **igroup**

當您不再需要某個 igroup 時，可以使用SnapCenter將其刪除。

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「**Storage Virtual Machine**」欄位以顯示可用 SVM 的下拉列表，然後選取要刪除的 igroup 的 SVM。
4. 在 SVM 的 igroup 清單中，選擇要刪除的 igroup，然後按一下「刪除」。
5. 在「刪除 igroup」對話方塊中，按一下「確定」。

   SnapCenter刪除 igroup。

建立和管理磁碟

Windows 主機將儲存系統上的 LUN 視為虛擬磁碟。您可以使用SnapCenter建立和設定 FC 連線或 iSCSI 連線的 LUN。

- SnapCenter僅支援基本磁碟。不支援動態磁碟。
- 對於 GPT，只允許一個資料分割區，對於 MBR，只允許一個主分割區，該主分割區具有一個使用 NTFS 或 CSVFS 格式化的磁碟區和一個掛載路徑。
- 支援的分割區樣式：GPT、MBR；在 VMware UEFI VM 中，僅支援 iSCSI 磁碟

SnapCenter不支援重新命名磁碟。如果重新命名由SnapCenter管理的磁碟， SnapCenter作業將不會成功。

查看主機上的磁碟

您可以使用SnapCenter檢視管理的每個 Windows 主機上的磁碟。

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*下拉清單中選擇主機。

   磁碟已列出。

查看叢集磁碟

您可以查看使用SnapCenter管理的叢集上的叢集磁碟。僅當您從主機下拉式選單中選擇叢集時才會顯示叢集磁碟。

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*下拉清單中選擇叢集。

   磁碟已列出。

建立 iSCSI 會話

如果您使用 iSCSI 連線至 LUN，則必須在建立 LUN 之前建立 iSCSI 會話以啟用通訊。

開始之前

- 您必須已將儲存系統節點定義為 iSCSI 目標。
- 您必須已經在儲存系統上啟動了 iSCSI 服務。 "了解更多"

關於此任務

您只能在相同的 IP 版本之間建立 iSCSI 會話，無論是從 IPv6 到 IPv6，還是從 IPv4 到 IPv4。

只有當主機和目標位於相同子網路中時，才可以使用連結本機 IPv6 位址進行 iSCSI 會話管理以及主機和目標之間的通訊。

如果變更 iSCSI 啟動器的名稱，則對 iSCSI 目標的存取會受到影響。更改名稱後，您可能需要重新配置啟動器存取的目標，以便它們能夠識別新名稱。變更 iSCSI 啟動器的名稱後，必須確保重新啟動主機。

如果您的主機有多個 iSCSI 接口，一旦您使用第一個介面上的 IP 位址建立了與SnapCenter 的iSCSI 會話，您就無法從具有不同 IP 位址的另一個介面建立 iSCSI 會話。

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** 會話」。
3. 從「儲存虛擬機器」下拉清單中，選擇 iSCSI 目標的儲存虛擬機器 (SVM)。
4. 從「主機」下拉清單中，選擇會話的主機。
5. 點選*建立會話*。

   將顯示「建立會話」精靈。

6. 在建立會話精靈中，確定目標：

在這個領域...	進入...
目標節點名稱	iSCSI 目標的節點名稱 如果存在現有的目標節點名稱，則以唯讀格式顯示該名稱。
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端口

在這個領域...	進入...
發起者入口網站位址	發起者網路入口網站的 IP 位址

7. 當您對輸入的內容滿意時，請按一下「連線」。

   SnapCenter建立 iSCSI 會話。

8. 重複此程序為每個目標建立會話。

建立 **FC** 連線或 **iSCSI** 連線的 **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建立和設定 FC 連線或 iSCSI 連線的 LUN。

如果您想在SnapCenter之外建立和格式化磁碟，則僅支援 NTFS 和 CSVFS 檔案系統。

開始之前

- 您必須已經在儲存系統上為 LUN 建立了一個磁碟區。

  該磁碟區應該僅保存 LUN，並且僅保存使用SnapCenter建立的 LUN。

  除非克隆已拆分，否則您無法在SnapCenter建立的複製磁碟區上建立 LUN。

- 您必須已在儲存系統上啟動 FC 或 iSCSI 服務。
- 如果您正在使用 iSCSI，則必須與儲存系統建立 iSCSI 會話。
- 適用於 Windows 的SnapCenter插件包必須僅安裝在要建立磁碟的主機上。

關於此任務

- 除非 Windows Server 故障轉移叢集中的主機共用 LUN，否則您無法將 LUN 連線至多個主機。
- 如果使用 CSV（叢集共用磁碟區）的 Windows Server 故障轉移叢集中的主機共用 LUN，則必須在擁有該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*下拉清單中選擇主機。
4. 點選“新建”。

   將開啟建立磁碟精靈。

5. 在 LUN 名稱頁面中，識別 LUN：

在這個領域...	這樣做...
儲存系統	選擇 LUN 的 SVM。
LUN 路徑	按一下「瀏覽」以選擇包含 LUN 的資料夾的完整路徑。
LUN 名稱	輸入 LUN 的名稱。
簇大小	選擇叢集的 LUN 區塊分配大小。 叢集大小取決於作業系統和應用程式。
LUN 標籤	或者，輸入 LUN 的描述性文字。

6. 在磁碟類型頁面中，選擇磁碟類型：

選擇...	如果...
專用磁碟	該 LUN 只能被一個主機存取。 忽略*資源組*欄位。
共享磁碟	LUN 由 Windows Server 故障轉移叢集中的主機共用。 在「資源組」欄位中輸入群集資源組的名稱。您只需在故障轉移群集中的一個主機上建立磁碟。
叢集共用磁碟區 (CSV)	此 LUN 由使用 CSV 的 Windows Server 故障轉移群集中的主機共用。 在「資源組」欄位中輸入群集資源組的名稱。確保在其上建立磁碟的主機是叢集群組的擁有者。

7. 在磁碟機屬性頁面中，指定磁碟機屬性：

財產	描述
自動分配掛載點	SnapCenter根據系統磁碟機自動分配磁碟區掛載點。 例如，如果您的系統磁碟機是 C:，則自動指派會在您的 C: 磁碟機下方建立磁碟區裝入點 (C:\scmnpt\)。共享磁碟不支援自動分配。
分配磁碟機號	將磁碟安裝到您在相鄰下拉清單中選擇的磁碟機。

財產	描述
使用卷掛載點	將磁碟安裝到您在相鄰欄位中指定的磁碟機路徑。 磁碟區安裝點的根目錄必須由您正在建立磁碟的主機擁有。
不要分配磁碟機號或磁碟區安裝點	如果您希望在 Windows 中手動安裝磁碟，請選擇此選項。
LUN大小	指定 LUN 大小；最小 150 MB。 在相鄰的下拉清單中選擇 MB、GB 或 TB。
託管此 LUN 的磁碟區使用精簡配置	精簡配置 LUN。 精簡配置一次僅分配所需的儲存空間，使 LUN 能夠有效率地成長到最大可用容量。 確保磁碟區上有足夠的可用空間來容納您認為需要的所有 LUN 儲存。
選擇分割區類型	為 GUID 分割區表選擇 GPT 分割區，或為主開機記錄選擇 MBR 分割區。 MBR 分割區可能會導致 Windows Server 故障轉移叢集中發生錯位問題。 不支援統一可擴充韌體介面 (UEFI) 分割區磁碟。

8. 在映射 LUN 頁面中，選擇主機上的 iSCSI 或 FC 啟動器：

在這個領域...	這樣做...
主持人	雙擊群集組名稱，顯示屬於該群集的主機的下拉列表，然後選擇啟動器的主機。 只有當 LUN 由 Windows Server 故障轉移叢集中的主機共用時，才會顯示此欄位。
選擇主機發起者	選擇“光纖通道”或“**iSCSI**”，然後選擇主機上的啟動器。 如果您使用具有多路徑 I/O (MPIO) 的 FC，則可以選擇多個 FC 啟動器。

9. 在「群組類型」頁面中，指定是否要將現有 igroup 對應到 LUN，還是建立新的 igroup：

選擇...	如果...
為選定的啟動器建立新的 igroup	您想要為選定的啟動器建立一個新的 igroup。
為選定的啟動器選擇現有的 igroup 或指定新的 igroup	您想要為選定的啟動器指定現有的 igroup，或使用您指定的名稱建立新的 igroup。 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完成該欄位。

10. 在「摘要」頁面中，檢查您的選擇，然後按一下「完成」。

    SnapCenter建立 LUN 並將其連接到主機上的指定磁碟機或磁碟機路徑。

調整磁碟大小

您可以根據儲存系統需求的變化增加或減少磁碟的大小。

關於此任務

- 對於精簡配置的 LUN， ONTAP LUN 幾何大小顯示為最大大小。
- 對於厚置備 LUN，可擴充大小（磁碟區中的可用大小）顯示為最大大小。
- 具有 MBR 樣式分割的 LUN 的大小限制為 2 TB。
- 具有 GPT 樣式分割區的 LUN 的儲存系統大小限制為 16 TB。
- 在調整 LUN 大小之前製作快照是一個好主意。
- 如果您需要從調整 LUN 大小之前建立的快照中還原 LUN， SnapCenter會自動將 LUN 調整為快照的大小。

  復原操作後，必須從調整大小後建立的快照中復原調整大小後新增至 LUN 的資料。

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. 從主機下拉清單中選擇主機。

   磁碟已列出。

4. 選擇要調整大小的磁碟，然後按一下“調整大小”。
5. 在「調整磁碟大小」對話方塊中，使用滑桿工具指定磁碟的新大小，或在「大小」欄位中輸入新大小。

   如果您手動輸入尺寸，則需要按一下「尺寸」欄位外部，然後才能正確啟用「收縮」或「擴充」按鈕。此外，您必須按一下 MB、GB 或 TB 來指定測量單位。

6. 當您對輸入的內容滿意時，請根據需要按一下「收縮」或「擴充」。

   SnapCenter調整磁碟大小。

連接磁碟

您可以使用連線磁碟精靈將現有 LUN 連線到主機，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。
- 如果您正在使用 iSCSI，則必須與儲存系統建立 iSCSI 會話。
- 除非 Windows Server 故障轉移叢集中的主機共用 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 故障轉移叢集中的主機共用，則必須連接擁有叢集群組的主機上的磁碟。
- 只需在連接磁碟的主機上安裝適用於 Windows 的插件。

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*下拉清單中選擇主機。
4. 按一下“連接”。

   將開啟連接磁碟精靈。

5. 在 LUN 名稱頁面中，確定要連接的 LUN：

在這個領域...	這樣做...
儲存系統	選擇 LUN 的 SVM。
LUN 路徑	按一下「瀏覽」以選擇包含 LUN 的磁碟區的完整路徑。
LUN 名稱	輸入 LUN 的名稱。
簇大小	選擇叢集的 LUN 區塊分配大小。 叢集大小取決於作業系統和應用程式。
LUN 標籤	或者，輸入 LUN 的描述性文字。

6. 在磁碟類型頁面中，選擇磁碟類型：

選擇...	如果...
專用磁碟	該 LUN 只能被一個主機存取。

選擇...	如果...
共享磁碟	LUN 由 Windows Server 故障轉移叢集中的主機共用。 您只需將磁碟連接到故障轉移群集中的一台主機。
叢集共用磁碟區 (CSV)	此 LUN 由使用 CSV 的 Windows Server 故障轉移群集中的主機共用。 確保連接到磁碟的主機是叢集群組的擁有者。

7. 在磁碟機屬性頁面中，指定磁碟機屬性：

財產	描述
自動分配	讓SnapCenter根據系統磁碟機自動分配磁碟區掛載點。 例如，如果您的系統磁碟機是 C:，則自動指派屬性會在您的 C: 磁碟機下方建立磁碟區裝入點 (C:\scmnpt\)。共享磁碟不支援自動分配屬性。
分配磁碟機號	將磁碟安裝到您在相鄰下拉清單中選擇的磁碟機。
使用卷掛載點	將磁碟安裝到您在相鄰欄位中指定的磁碟機路徑。 磁碟區安裝點的根目錄必須由您正在建立磁碟的主機擁有。
不要分配磁碟機號或磁碟區安裝點	如果您希望在 Windows 中手動安裝磁碟，請選擇此選項。

8. 在映射 LUN 頁面中，選擇主機上的 iSCSI 或 FC 啟動器：

在這個領域...	這樣做...
主持人	雙擊叢集群組名稱，顯示屬於該叢集的主機的下拉列表，然後選擇啟動器的主機。 只有當 LUN 由 Windows Server 故障轉移叢集中的主機共用時，才會顯示此欄位。
選擇主機發起者	選擇“光纖通道”或“**iSCSI**”，然後選擇主機上的啟動器。 如果您使用具有 MPIO 的 FC，則可以選擇多個 FC 啟動器。

9. 在「群組類型」頁面中，指定是否要將現有 igroup 對應到 LUN 或建立新的 igroup：

選擇...	如果...
為選定的啟動器建立新的 igroup	您想要為選定的啟動器建立一個新的 igroup。
為選定的啟動器選擇現有的 igroup 或指定新的 igroup	您想要為選定的啟動器指定現有的 igroup，或使用您指定的名稱建立新的 igroup。 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完成該欄位。

10. 在「摘要」頁面中，檢查您的選擇並按一下「完成」。

    SnapCenter將 LUN 連接到主機上的指定磁碟機或磁碟機路徑。

斷開磁碟

您可以將 LUN 與主機斷開連接，而不會影響 LUN 的內容，但有一個例外：如果在克隆分離之前斷開連接，則會丟失克隆的內容。

開始之前

- 確保 LUN 未被任何應用程式使用。
- 確保 LUN 未被監控軟體監控。
- 如果 LUN 是共享的，請確保從 LUN 中刪除叢集資源相依性，並驗證叢集中的所有節點是否都已開啟電源、正常運作且可供SnapCenter使用。

關於此任務

如果中斷SnapCenter建立的FlexClone磁碟區中的某個 LUN 且該磁碟區上沒有連接任何其他 LUN，SnapCenter會刪除該磁碟區。在斷開 LUN 之前， SnapCenter會顯示一則訊息，警告您FlexClone磁碟區可能會被刪除。

為避免自動刪除FlexClone磁碟區，您應該在斷開最後一個 LUN 之前重新命名該磁碟區。重命名卷時，請確保更改多個字符，而不僅僅是名稱中的最後一個字符。

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*下拉清單中選擇主機。

    磁碟已列出。

4. 選擇要斷開的磁碟，然後按一下“斷開連接”。
5. 在「斷開磁碟」對話方塊中，按一下「確定」。

    SnapCenter斷開磁碟連線。

刪除磁碟

當您不再需要磁碟時，可以將其刪除。刪除磁碟後，將無法復原。

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*下拉清單中選擇主機。

   磁碟已列出。
4. 選擇要刪除的磁碟，然後按一下“刪除”。
5. 在「刪除磁碟」對話方塊中，按一下「確定」。

   SnapCenter刪除磁碟。

建立和管理 **SMB** 共享

若要在儲存虛擬機器 (SVM) 上設定 SMB3 共用，您可以使用SnapCenter使用者介面或 PowerShell cmdlet。

*最佳實踐：*建議使用 cmdlet，因為它使您能夠利用SnapCenter提供的範本來自動化共享配置。

模板概括了磁碟區和共享配置的最佳實踐。您可以在 Windows 版SnapCenter插件包的安裝資料夾中的 Templates 資料夾中找到這些範本。

如果您願意，您可以按照提供的模型建立自己的模板。在建立自訂範本之前，您應該查看 cmdlet 文件中的參數。

建立 **SMB** 共享

您可以使用SnapCenter共用頁面在儲存虛擬機器 (SVM) 上建立 SMB3 共用。

您不能使用SnapCenter備份 SMB 共用上的資料庫。 SMB 支援僅限於設定。

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「共享」。
3. 從「儲存虛擬機器」下拉清單中選擇 SVM。
4. 點選“新建”。

   “新共享”對話方塊開啟。
5. 在新共享對話方塊中，定義共享：

在這個領域...	這樣做...
描述	輸入共享的描述性文字。
共享名稱	輸入共享名稱，例如 test_share。 您輸入的共享名稱也將用作磁碟區名稱。 共享名稱： • 必須是 UTF-8 字串。 • 不得包含以下字符：從 0x00 到 0x1F（含）的控製字符、0x22（雙引號）以及特殊字符 `\ / [ ] : (vertical bar) < > + = ; , ?`
分享路徑	• 按一下該欄位以輸入新的檔案系統路徑，例如 /。 • 雙擊該欄位以從現有檔案系統路徑清單中進行選擇。

6. 如果您對輸入的內容滿意，請按一下「確定」。

   SnapCenter在 SVM 上建立 SMB 共用。

刪除 **SMB** 共享

當您不再需要 SMB 共用時，可以將其刪除。

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「共享」。
3. 在共用頁面中，按一下「儲存虛擬機器」欄位以顯示下拉式選單，其中包含可用儲存虛擬機器 (SVM) 的列表，然後選擇要刪除的共用的 SVM。
4. 從 SVM 上的共享清單中，選擇要刪除的共享，然後按一下「刪除」。
5. 在「刪除共享」對話方塊中，按一下「確定」。

   SnapCenter從 SVM 中刪除 SMB 共用。

回收儲存系統上的空間

儘管 NTFS 在檔案被刪除或修改時會追蹤 LUN 上的可用空間，但它不會將新資訊報告給儲存系統。您可以在適用於 Windows 主機的插件上執行空間回收 PowerShell cmdlet，以確保新釋放的區塊在儲存中標記為可用。

如果您在遠端插件主機上執行 cmdlet，則必須執行 SnapCenterOpen-SMConnection cmdlet 才能開啟

與SnapCenter伺服器的連線。

開始之前

- 您必須確保在執行復原作業之前空間回收過程已完成。
- 如果 LUN 由 Windows Server 故障轉移叢集中的主機共用，則必須在擁有該叢集群組的主機上執行空間回收。
- 為了獲得最佳儲存效能，您應該盡可能頻繁地執行空間回收。

  您應該確保已掃描整個 NTFS 檔案系統。

關於此任務

- 空間回收非常耗時且佔用大量 CPU 資源，因此最好在儲存系統和 Windows 主機使用率較低時執行此操作。
- 空間回收幾乎可以回收所有可用空間，但並非 100%。
- 您不應在執行空間回收的同時執行磁碟碎片整理。

  這樣做會減慢回收過程。

步

在應用程式伺服器 PowerShell 命令提示字元下，輸入以下命令：

```
Invoke-SdHostVolumeSpaceReclaim -Path drive_path
```

drive_path 是對應到 LUN 的磁碟機路徑。

使用 **PowerShell cmdlet** 設定存儲

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 或將其新增至腳本。

如果您在遠端插件主機上執行 cmdlet，則必須執行SnapCenter Open-SMConnection cmdlet 來開啟與SnapCenter伺服器的連線。

可以透過執行_Get-Help command_name_來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 "SnapCenter軟體 Cmdlet 參考指南"。

如果因為從伺服器移除SnapDrive for Windows 而導致SnapCenter PowerShell cmdlet 損壞，請參閱 "卸載SnapDrive for Windows 時SnapCenter cmdlet 損壞"。

在 **VMware** 環境中設定存儲

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** 客戶作業系統平台

- 支援的 Windows Server 版本

- Microsoft 群集配置

  使用 Microsoft iSCSI Software Initiator 時，VMware 上最多支援 16 個節點，使用 FC 時最多支援兩個節點

- RDM LUN

  對於普通 RDMS，最多支援 56 個 RDM LUN，配備四個 LSI Logic SCSI 控制器；對於 Windows 配置，VMware VM MSCS 盒對盒插件最多支援 42 個 RDM LUN，配備三個 LSI Logic SCSI 控制器

  支援 VMware ParaVirtual SCSI 控制器。 RDM 磁碟上可支援 256 個磁碟。

有關受支援版本的最新信息，請參閱 "NetApp互通性表工具"。

VMware ESXi 伺服器相關限制

- 不支援使用 ESXi 憑證在虛擬機器上的 Microsoft 叢集上安裝適用於 Windows 的插件。

  在叢集虛擬機器上安裝適用於 Windows 的插件時，您應該使用 vCenter 憑證。

- 所有叢集節點必須對同一個叢集磁碟使用相同的目標 ID（在虛擬 SCSI 適配器上）。
- 當您在適用於 Windows 的插件之外建立 RDM LUN 時，必須重新啟動插件服務以使其能夠識別新建立的磁碟。
- 您無法在 VMware 客戶作業系統上同時使用 iSCSI 和 FC 啟動器。

SnapCenter RDM 操作所需的最低 **vCenter** 權限

您應該在主機上擁有下列 vCenter 權限才能在來賓作業系統中執行 RDM 操作：

- 資料儲存：刪除文件
- 主機：配置 > 儲存分區配置
- 虛擬機器：配置

您必須將這些權限指派給 Virtual Center Server 等級的角色。您指派了這些權限的角色不能指派給沒有 root 權限的任何使用者。

指派這些權限後，您可以在來賓作業系統上安裝適用於 Windows 的插件。

管理 **Microsoft** 叢集中的 **FC RDM LUN**

您可以使用適用於 Windows 的插件來管理使用 FC RDM LUN 的 Microsoft 群集，但必須先在插件外部建立共用 RDM 仲裁和共用存儲，然後將磁碟新增至叢集中的虛擬機器。

從 ESXi 5.5 開始，您也可以使用 ESX iSCSI 和 FCoE 硬體來管理 Microsoft 叢集。 Windows 外掛程式包含對 Microsoft 叢集的開箱即用支援。

要求

當您滿足特定的配置要求時，適用於 Windows 的插件可為 Microsoft 群集提供支持，這些群集使用屬於兩個不同 ESX 或 ESXi 伺服器的兩個不同虛擬機器上的 FC RDM LUN，也稱為跨箱群集。

- 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。
- 兩個 ESX 或 ESXi 伺服器之間必須共用至少一個 VMware 虛擬機器檔案系統 (VMFS) 資料儲存。
- VMware 建議在 FC SAN 上建立共用資料儲存。

  如果需要，也可以透過 iSCSI 建立共享資料儲存。

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

  您不能將虛擬磁碟用於共享儲存。

- 必須在實體相容模式下在叢集中的每個虛擬機器上設定 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。如果僅存在一個相同類型的控制器且該控制器已連接到 C: 驅動器，則共用 LUN 無法使用現有的 LSI Logic SAS 控制器。

  VMware Microsoft 叢集不支援半虛擬化類型的 SCSI 控制器。

  > 當您在實體相容模式下將 SCSI 控制器新增至虛擬機器上的共用 LUN 時，您必須在 VMware Infrastructure Client 中選擇 原始裝置對應 (RDM) 選項，而不是 建立新磁碟 選項。

- Microsoft 虛擬機器叢集不能成為 VMware 叢集的一部分。
- 在屬於 Microsoft 叢集的虛擬機器上安裝適用於 Windows 的插件時，必須使用 vCenter 憑證，而非 ESX 或 ESXi 憑證。
- Windows 外掛程式無法使用來自多個主機的啟動器建立單一 igroup。

  在建立將用作共用叢集磁碟的 RDM LUN 之前，必須在儲存控制器上建立包含所有 ESXi 主機的啟動器的 igroup。

- 確保使用 FC 啟動器在 ESXi 5.0 上建立 RDM LUN。

  建立 RDM LUN 時，將使用 ALUA 建立啟動器群組。

限制

Windows 外掛程式支援在屬於不同 ESX 或 ESXi 伺服器的不同虛擬機器上使用 FC/iSCSI RDM LUN 的 Microsoft 叢集。

> ESX 5.5i 之前的版本不支援此功能。

- Windows 插件不支援 ESX iSCSI 和 NFS 資料儲存上的叢集。
- 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 叢集中的共用磁碟不支援 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 進行虛擬機器遷移。
- Windows 外掛程式不支援 Microsoft 群集中虛擬機器上的 MPIO。

建立共享 **FC RDM LUN**

在使用 FC RDM LUN 在 Microsoft 叢集中的節點之間共用儲存體之前，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。

共享磁碟不是使用 Windows 插件建立的。您應該建立共用 LUN，然後將其新增至叢集中的每個虛擬機器。有關信息，請參閱 "跨實體主機叢集虛擬機"。

新增基於**SnapCenter Standard** 控制器的許可證

如果您使用FAS、 AFF或ASA儲存控制器，則需要基於SnapCenter Standard 控制器的授權。

基於控制器的授權具有以下特點：

- 購買 Premium 或 Flash Bundle 即可獲得SnapCenter Standard 權利（不包含在基礎包中）
- 無限儲存使用
- 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。

- 鎖定到控制器的序號

有關所需許可證的信息，請參閱"SnapCenter許可證"。

步驟 **1**：驗證是否安裝了**SnapManager Suite** 許可證

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. 在左側導覽窗格中，選擇*儲存系統*。
2. 在「儲存系統」頁面中，從「類型」下拉式選單中選擇是否要查看已新增的所有 SVM 或叢集：
   - 若要查看已新增的所有 SVM，請選擇 * ONTAP SVM*。
   - 若要查看已新增的所有集群，請選擇「ONTAP集群」。

     當您選擇叢集名稱時，叢集中的所有 SVM 都會顯示在 Storage Virtual Machines 部分。

3. 在儲存連接清單中，找到控制器許可證列。

   控制器許可證列顯示以下狀態：

   -  表示SnapManager Suite 許可證已安裝在FAS、 AFF或ASA主儲存系統上。
   -  表示FAS、 AFF或ASA主儲存系統上未安裝SnapManager Suite 授權。
   - 不適用表示SnapManager Suite 授權不適用，因為儲存控制器位於Amazon FSx for NetApp ONTAP、Cloud Volumes ONTAP、 ONTAP Select或輔助儲存平台。

第 **2** 步：識別控制器上安裝的許可證

您可以使用ONTAP命令列查看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。

範例輸出

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

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

Serial Number: 1-81-00000000000000000000000xx
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 -
```

在範例中，已安裝 SnapManagerSuite 許可證，因此不需要額外的SnapCenter許可操作。

步驟 **3**：檢索控制器序號

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命令列登入控制器。
2. 輸入 system show -instance 命令，然後查看輸出以找到控制器序號。

範例輸出

```
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: xxxxxxxxx
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: xxxxxxxxx
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**：檢索基於控制器的許可證的序號

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支援網站登入憑證。

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支援站點"。
2. 導覽至*系統* > 軟體許可證。
3. 在選擇標準區域，確保選擇了序號（位於裝置背面），輸入控制器序號，然後選擇*Go!*。

顯示指定控制器的許可證清單。

4. 找到並記錄SnapCenter Standard 或 SnapManagerSuite 許可證。

步驟 **5**：新增基於控制器的許可證

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命令列新增基於SnapCenter控制器的授權。

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 Standard 或 SnapManagerSuite 授權。

關於此任務

如果您想使用FAS、 AFF或ASA儲存試用安裝SnapCenter ，您可以取得 Premium Bundle 評估授權以安裝在控制器上。

如果您想嘗試安裝SnapCenter ，您應該聯絡您的銷售代表以取得 Premium Bundle 評估授權以安裝在您的控制器上。

步驟

1. 使用ONTAP命令列登入NetApp叢集。
2. 新增 SnapManagerSuite 許可證金鑰：

```
system license add -license-code license_key
```

此命令在管理員權限層級可用。

3. 驗證是否已安裝 SnapManagerSuite 授權：

```
license show
```

步驟 **6**：刪除試用許可證

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。

只有當您使用基於SnapCenter Standard 控制器的授權時才需要手動刪除試用授權。

步驟

1. 在SnapCenter伺服器上，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-SmRepositoryPassword 重設 MySQL 密碼。

      有關 cmdlet 的信息，請參閱 "SnapCenter軟體 Cmdlet 參考指南"。

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

   MySQL 提示您輸入密碼。輸入您在重設密碼時提供的憑證。

3. 從資料庫中刪除試用許可證：

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

配置高可用性

配置**SnapCenter**伺服器以實現高可用性

為了支援在 Windows 或 Linux 上執行的SnapCenter中的高可用性 (HA)，您可以安裝 F5 負載平衡器。 F5 使SnapCenter伺服器能夠支援位於相同位置的最多兩台主機的主動-被動配置。若要在SnapCenter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高可用性。您應該在SnapCenter安裝之外手動配置 NLB 以實現高可用性。

對於雲端環境，您可以使用 Amazon Web Services (AWS) 彈性負載平衡 (ELB) 和 Azure 負載平衡器來設定高可用性。

使用 **F5** 配置高可用性

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 F5 負載平衡器配置SnapCenter伺服器以實現高可用性"。

您必須是SnapCenter伺服器上本機管理員群組的成員（除了指派 SnapCenterAdmin 角色），才能使用下列 cmdlet 新增和刪除 F5 叢集：

- 新增SmServerCluster
- 新增SmServer
- 刪除-SmServerCluster

  有關更多信息，請參閱 "SnapCenter軟體 Cmdlet 參考指南" 。

附加資訊

- 安裝並配置SnapCenter以實現高可用性後，編輯SnapCenter桌面捷徑以指向 F5 叢集 IP。
- 如果SnapCenter伺服器之間發生故障轉移，並且還存在現有的SnapCenter會話，則必須關閉瀏覽器並再次登入SnapCenter 。
- 在負載平衡器設定（NLB 或 F5）中，如果新增由 NLB 或 F5 主機部分解析的主機，如果SnapCenter主機無法連線到該主機，則SnapCenter主機頁面會在主機關閉和運作狀態之間經常切換。要解決此問題，您應該確保兩個SnapCenter主機都能夠解析 NLB 或 F5 主機中的主機。
- 應在所有主機上執行 MFA 設定的SnapCenter指令。依賴方設定應使用 F5 叢集詳細資訊在 Active Directory 聯合驗證服務 (AD FS) 伺服器中完成。啟用 MFA 後，主機級SnapCenter UI 存取將被阻止。
- 在故障轉移期間，稽核日誌設定不會反映在第二台主機上。因此，當 F5 被動主機變成主動主機時，您應該手動重複審核日誌設定。

使用網路負載平衡 **(NLB)** 配置高可用性

您可以設定網路負載平衡 (NLB) 來設定SnapCenter高可用性。您應該在SnapCenter安裝之外手動配置 NLB 以實現高可用性。

有關如何使用SnapCenter配置網路負載平衡 (NLB) 的信息，請參閱 "如何使用SnapCenter配置 NLB"。

使用 **AWS Elastic Load Balancing (ELB)** 配置高可用性

您可以在 Amazon Web Services (AWS) 中設定高可用性SnapCenter環境，方法是在不同的可用區域 (AZ) 中設定兩個SnapCenter伺服器並對其進行設定以實現自動故障轉移。此架構包括虛擬專用IP位址、路由表以及主備MySQL資料庫之間的同步。

步驟

1. 在 AWS 中配置虛擬專用覆蓋 IP。有關信息，請參閱 "配置虛擬專用覆蓋 IP"。
2. 準備 Windows 主機
   a. 強制 IPv4 優先權高於 IPv6：
      - 位置：HKLM\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters
      - 鍵：DisabledComponents
      - 類型：REG_DWORD

- 值：0x20

b. 確保完全限定網域名稱可以透過 DNS 或本機設定解析為 IPv4 位址。

c. 確保您沒有配置系統代理程式。

d. 當使用沒有 Active Directory 的設定且伺服器不在一個網域中時，請確保兩個 Windows Server 上的管理員密碼相同。

e. 在兩個 Windows 伺服器上新增虛擬 IP。

3. 建立SnapCenter叢集。

a. 啟動 Powershell 並連線到SnapCenter。 `Open-SmConnection`

b. 建立集群。 `Add-SmServerCluster -ClusterName <cluster_name> -ClusterIP <cluster_ip> -PrimarySCServerIP <primary_ip> -Verbose -Credential administrator`

c. 新增輔助伺服器。 `Add-SmServer -ServerName <server_name> -ServerIP <server_ip> -CleanUpSecondaryServer -Verbose -Credential administrator`

d. 取得高可用性詳細資訊。 `Get-SmServerConfig`

4. 建立 Lamda 函數以在虛擬私人 IP 端點不可用時調整路由表，並由 AWS CloudWatch 監控。有關信息，請參閱 "建立 Lambda 函數"。

5. 在 CloudWatch 中建立一個監視器來監控SnapCenter端點的可用性。如果端點無法訪問，則配置警報以觸發 Lambda 函數。 Lambda 函數會調整路由表以將流量重新導向至活動的SnapCenter伺服器。有關信息，請參閱 "創建合成金絲雀"。

6. 使用步驟函數實作工作流程作為 CloudWatch 監控的替代方案，從而提供更短的故障轉移時間。此工作流程包括一個用於測試SnapCenter URL 的 Lambda 探測函數、一個用於儲存故障計數的 DynamoDB 表以及 Step Function 本身。

a. 使用 lambda 函數探測SnapCenter URL。有關信息，請參閱 "建立 Lambda 函數"。

b. 建立一個 DynamoDB 表來儲存兩次 Step Function 迭代之間的失敗計數。有關信息，請參閱 "DynamoDB 表格入門"。

c. 建立步進函數。有關信息，請參閱 "Step Function 文檔"。

d. 測試單一步驟。

e. 測試完整功能。

f. 建立 IAM 角色並調整權限以允許執行 Lambda 函數。

g. 建立計劃以觸發 Step Function。有關信息，請參閱 "使用 Amazon EventBridge Scheduler 啟動 Step Functions"。

使用 **Azure** 負載平衡器配置高可用性

您可以使用 Azure 負載平衡器設定高可用性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 虛擬機器規模集可讓您建立和管理一組負載平衡的虛擬機器。虛擬機器實例的數量可以根據需求或定義的時間表自動增加或減少。有關信息，請參閱 "使用 Azure 入口網站在規模集中建立虛擬機"。

2. 配置虛擬機器後，登入 VM 集中的每個虛擬機器並在兩個節點上安裝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. 新增輔助伺服器。 `Add-SmServer -ServerName <name of node2> -ServerIP <ip address of node2> -Verbose -Credential <credentials>`
5. 取得高可用性詳細資訊。 `Get-SmServerConfig`
6. 如果需要，重建輔助主機。 `Set-SmRepositoryConfig -RebuildSlave -Verbose`
7. 故障轉移到第二台主機。 `Set-SmRepositoryConfig ActiveMaster <name of node2> -Verbose`

== 從 NLB 切換到 F5 以實現高可用性

您可以將SnapCenter HA 設定從網路負載平衡 (NLB) 變更為使用 F5 負載平衡器。

步驟

1. 使用 F5 設定SnapCenter伺服器以實現高可用性。 "了解更多" 。
2. 在SnapCenter伺服器主機上，啟動 PowerShell。
3. 使用 Open-SmConnection cmdlet 啟動會話，然後輸入您的憑證。
4. 使用 Update-SmServerCluster cmdlet 更新SnapCenter伺服器以指向 F5 叢集 IP 位址。

   可以透過執行_Get-Help command_name_來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 "SnapCenter軟體 Cmdlet 參考指南"。

SnapCenter MySQL 儲存庫的高可用性

MySQL 複製是 MySQL 伺服器的功能，它可讓您將資料從一個 MySQL 資料庫伺服器（主伺服器）複製到另一個 MySQL 資料庫伺服器（從伺服器）。 SnapCenter僅在兩個啟用網路負載平衡 (NLB) 的節點上支援 MySQL 複製以實現高可用性。

SnapCenter在主儲存庫上執行讀取或寫入操作，並在主儲存庫發生故障時將其連接路由至從屬儲存庫。然後從屬存儲庫將成為主存儲庫。 SnapCenter還支援反向複製，該功能僅在故障轉移期間啟用。

如果要使用 MySQL 高可用性 (HA) 功能，則必須在第一個節點上設定網路負載平衡器 (NLB)。 MySQL 儲存庫會作為安裝的一部分安裝在此節點上。在第二個節點上安裝SnapCenter時，您必須加入第一個節點的 F5 並在第二個節點上建立 MySQL 儲存庫的副本。

SnapCenter提供 *Get-SmRepositoryConfig* 和 *Set-SmRepositoryConfig* PowerShell cmdlet 來管理 MySQL 複製。

可以透過執行_Get-Help command_name_來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 "SnapCenter軟體 Cmdlet 參考指南"。

您必須了解與 MySQL HA 功能相關的限制：

- 兩個節點以上不支援 NLB 和 MySQL HA。

- 不支援從SnapCenter獨立安裝切換到 NLB 安裝或反之亦然，也不支援從 MySQL 獨立安裝切換到 MySQL HA。
- 如果從屬儲存庫資料與主儲存庫資料不同步，則不支援自動故障轉移。

  您可以使用 *Set-SmRepositoryConfig* cmdlet 啟動強制故障轉移。

- 當啟動故障轉移時，正在執行的作業可能會失敗。

  如果由於 MySQL 伺服器或SnapCenter伺服器關閉而發生故障轉移，則任何正在執行的作業都可能失敗。故障轉移到第二個節點後，所有後續作業均成功運作。

有關配置高可用性的信息，請參閱 "如何使用SnapCenter配置 NLB 和 ARR"。

配置基於角色的存取控制 (RBAC)

創建角色

除了使用現有的SnapCenter角色之外，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. 點選 ✚。
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. 選擇“此角色的所有成員都可以看到其他成員的物件”，使該角色的其他成員在刷新資源清單後可以看到磁碟區和主機等資源。

   如果您不希望該角色的成員看到指派給其他成員的對象，則應取消選取此選項。

   啟用此選項後，如果使用者與建立物件或資源的使用者屬於相同角色，則無需為使用者指派對物件或資源的存取權限。

6. 在「權限」頁面中，選擇要指派給角色的權限，或按一下「全選」將所有權限授予角色。
7. 點選“提交”。

使用安全登入指令新增**NetApp ONTAP RBAC** 角色

當您的儲存系統執行叢集ONTAP時，您可以使用安全登入指令新增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/或命令目錄權限。

  每個命令/命令目錄有兩種存取等級：全部存取和唯讀。

  您必須始終先指派所有存取權限。

- 為使用者指派角色。
- 根據您的SnapCenter插件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。

關於此任務

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

該工具會自動正確設定ONTAP權限。例如， NetApp ONTAP的 RBAC User Creator 工具會自動以正確的順序新增權限，以便所有存取權限會先出現。如果您先新增唯讀權限，然後新增所有存取權限，ONTAP會將所有存取權限標記為重複並忽略它們。

> 如果您稍後升級SnapCenter或ONTAP，則應重新執行NetApp ONTAP的 RBAC User Creator 工具來更新您先前建立的使用者角色。為早期版本的SnapCenter或ONTAP所建立的使用者角色無法與升級後的版本正常搭配使用。當您重新運行該工具時，它會自動處理升級。您不需要重新建立角色。

有關設定ONTAP RBAC 角色的更多信息，請參閱 "ONTAP 9 管理員驗證和 RBAC 電源指南"。

步驟

1. 在儲存系統上，輸入以下指令以建立新角色：

   ```
   security login role create <role_name\> -cmddirname "command" -access all
   -vserver <svm_name\>
   ```

   - svm_name 是 SVM 的名稱。如果將其留空，則預設為叢集管理員。
   - role_name 是您為角色指定的名稱。
   - 指令是ONTAP功能。

     > 您必須對每個權限重複此命令。請記住，全訪問命令必須在只讀命令之前列出。

   有關權限清單的信息，請參閱"用於建立角色和分配權限的ONTAP CLI 命令"。

2. 輸入以下命令建立使用者名稱：

   ```
   security login create -username <user_name\> -application ontapi -authmethod
   <password\> -role <name_of_role_in_step_1\> -vserver <svm_name\> -comment
   "user_description"
   ```

   - user_name 是您正在建立的使用者的名稱。
   - <password> 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. 透過輸入以下命令將角色指派給使用者：

```
security login modify username <user_name\> -vserver <svm_name\> -role
<role_name\> -application ontapi -application console -authmethod <password\>
```

- <user_name> 是您在步驟 2 中建立的使用者的名稱。此命令允許您修改使用者以將其與角色關聯。
- <svm_name> 是 SVM 的名稱。
- <role_name> 是您在步驟 1 中建立的角色的名稱。
- <password> 是您的密碼。如果您未指定密碼，系統會提示您輸入密碼。

4. 輸入以下命令驗證使用者是否已正確建立：

```
security login show -vserver <svm_name\> -user-or-group-name <user_name\>
```

user_name 是您在步驟 3 中建立的使用者的名稱。

建立具有最低權限的 **SVM** 角色

在ONTAP中為新的 SVM 使用者建立角色時，必須執行幾個ONTAP CLI 指令。如果您在ONTAP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. 在儲存系統上建立一個角色，並為該角色賦予所有權限。

```
security login role create -vserver <svm_name\>- role <SVM_Role_Name\>
-cmddirname <permission\>
```

> 您應該對每個權限重複此命令。

2. 建立一個使用者並將角色指派給該使用者。

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

3. 解除用戶鎖定。

```
security login unlock -user <user_name\> -vserver <svm_name\>
```

用於建立 **SVM** 角色和分配權限的**ONTAP CLI** 命令

您應該執行幾個ONTAP CLI 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

- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job history show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "job show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job stop" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup add" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun offline" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun online" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun resize" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun serial" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "network interface" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "version" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname

"volume file clone create" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume online" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "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
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show-delta" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume unmount" -access all

- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "vserver iscsi connection show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver" -access readonly`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver iscsi" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume clone split status" -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

您必須執行幾個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. 在儲存系統上建立一個角色，並為該角色賦予所有權限。

   ```
   security login role create –vserver <svm_name\>- role <SVM_Role_Name\>
   -cmddirname <permission\>
   ```

   您應該對每個權限重複此命令。

2. 建立一個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. 解除用戶鎖定。

   ```
   security login unlock -user <user_name\> -vserver <svm_name\>
   ```

用於建立 **SVM** 角色和分配權限的**ONTAP CLI** 命令

您應該執行幾個ONTAP CLI 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
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job history show" -access all

- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "job show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job stop" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup add" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup rename" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun mapping create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun modify" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun move-in-volume" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun offline" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun online" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun resize" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname`

"lun serial" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "network interface" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "version" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file show-disk-usage" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume online" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "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
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show-delta" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname

"vserver cifs share delete" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "vserver iscsi connection show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver iscsi" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume clone split status" -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`

建立具有最低權限的**ONTAP**叢集角色

您應該建立具有最小權限的ONTAP叢集角色，這樣您就不必使用ONTAP管理員角色在SnapCenter中執行操作。您可以執行多個ONTAP CLI 命令來建立ONTAP叢集角色並指派最低權限。

步驟

1. 在儲存系統上建立一個角色，並為該角色賦予所有權限。

   ```
   security login role create –vserver <cluster_name\>- role <role_name\>
   -cmddirname <permission\>
   ```

   您應該對每個權限重複此命令。

2. 建立一個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. 解除用戶鎖定。

   ```
   security login unlock -user <user_name\> -vserver <cluster_name\>
   ```

用於建立叢集角色和分配權限的**ONTAP CLI** 命令

您應該執行幾個ONTAP 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`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job history show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job stop" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup add" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup rename" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup show" -access all`

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun persistent-reservation clear" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun resize" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun serial" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface create" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface delete" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface modify" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "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
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "security login" -access readonly
- security login role create -role Role_Name -cmddirname "snapmirror create" -vserver Cluster_name -access all
- security login role create -role Role_Name -cmddirname "snapmirror list-destinations" -vserver Cluster_name -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show-history" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license clean-up" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "version" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

"volume snapshot modify-snaplock-expiry-time" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot promote" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show-delta" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs create" -access all

- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver iscsi connection show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver show" -access all`

為**ASA r2** 系統建立**ONTAP**叢集角色

您應該建立具有最小權限的ONTAP叢集角色，這樣您就不必使用ONTAP管理員角色

在SnapCenter中執行操作。您可以執行多個ONTAP CLI 命令來建立ONTAP叢集角色並指派最低權限。

步驟

1. 在儲存系統上建立一個角色，並為該角色賦予所有權限。

   ```
   security login role create -vserver <cluster_name\>- role <role_name\>
   -cmddirname <permission\>
   ```

   您應該對每個權限重複此命令。

2. 建立一個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. 解除用戶鎖定。

   ```
   security login unlock -user <user_name\> -vserver <cluster_name\>
   ```

用於建立叢集角色和分配權限的**ONTAP CLI** 命令

您應該執行幾個ONTAP 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`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job history show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job stop" -access all`

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun persistent-reservation clear" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun resize" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

"lun serial" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface create" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface delete" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface modify" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "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
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "security login" -access readonly
- security login role create -role Role_Name -cmddirname "snapmirror create" -vserver Cluster_name -access all
- security login role create -role Role_Name -cmddirname "snapmirror list-destinations" -vserver Cluster_name -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy add-rule" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license clean-up" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "version" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

"volume clone create" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify-snaplock-expiry-time" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot promote" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show-delta" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

```
"vserver export-policy rule create" -access all
```

- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver iscsi connection show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "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分配角色和資產

若要為SnapCenter使用者配置基於角色的存取控制，您可以新增使用者或群組並指派角色。角色決定了SnapCenter用戶可以存取的選項。

開始之前

- 您必須以「SnapCenterAdmin」角色登入。
- 您必須已經在作業系統或資料庫的 Active Directory 中建立了使用者或群組帳戶。您不能使用SnapCenter建立這些帳戶。

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

- SnapCenter包含幾個預先定義的角色。

  您可以將這些角色指派給使用者或建立新角色。

- 新增至SnapCenter RBAC 的 AD 使用者和 AD 群組必須對 Active Directory 中的使用者容器和電腦容器具有讀取權限。
- 將角色指派給包含適當權限的使用者或群組後，必須為該使用者指派對SnapCenter資產（例如主機和儲存連線）的存取權。

這使用戶能夠對分配給他們的資產執行他們有權限執行的操作。

- 您應該在某個時候為使用者或群組分配一個角色，以利用 RBAC 權限和效率。
- 您可以在建立使用者或群組時為使用者指派主機、資源群組、政策、儲存連線、外掛程式和憑證等資產。
- 您應指派給使用者執行某些操作的最低資產如下：

手術	資產轉讓
保護資源	主機、策略
備份	主機、資源群組、策略
恢復	主機、資源組
複製	主機、資源群組、策略
複製生命週期	主持人
建立資源組	主持人

- 當將新節點新增至 Windows 叢集或 DAG（Exchange Server 資料庫可用性群組）資產時，如果將此新節點指派給用戶，則必須將資產重新指派給使用者或群組，以將新節點包含至使用者或群組。

  您應該將 RBAC 使用者或群組重新指派給群集或 DAG，以將新節點包含到 RBAC 使用者或群組。例如，您有一個雙節點集群，並且已為該集群分配了 RBAC 使用者或群組。當您向集群新增另一個節點時，您應該將 RBAC 使用者或群組重新指派給集群，以便為 RBAC 使用者或群組包含新節點。

- 如果您計劃複製快照，則必須將來源磁碟區和目標磁碟區的儲存連線指派給執行操作的使用者。

  您應該在向使用者分配存取權限之前新增資產。

如果您使用適用SnapCenter Plug-in for VMware vSphere功能來保護虛擬機器、VMDK 或資料儲存區，則應使用 VMware vSphere GUI 將 vCenter 使用者新增至SnapCenter Plug-in for VMware vSphere角色。有關 VMware vSphere 角色的信息，請參閱 "SnapCenter Plug-in for VMware vSphere隨附的預先定義角色"。

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「使用者和造訪」>「* *.
3. 在「從 Active Directory 或工作群組新增使用者/群組」頁面中：

對於這個領域...	這樣做...
訪問類型	選擇網域或工作群組 對於網域身份驗證類型，您應該指定要將使用者新增至角色的使用者或群組的網域名稱。 預設情況下，它預先填入了登入的網域。 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	選擇使用者或群組 SnapCenter僅支援安全群組，不支援分發組。
使用者名稱	a. 輸入部分用戶名，然後按一下「新增」。 使用者名稱區分大小寫。 b. 從搜尋清單中選擇使用者名稱。 當您從不同的網域或不受信任的網域新增使用者時，您應該完整地輸入使用者名，因為沒有跨網域使用者的搜尋清單。 重複此步驟以將其他使用者或群組新增至所選角色。
角色	選擇您想要新增使用者的角色。

4. 按一下“分配”，然後在“分配資產”頁面中：
   a. 從*資產*下拉清單中選擇資產類型。
   b. 在資產表中，選擇資產。

      只有當使用者將資產新增至SnapCenter時，才會列出資產。

   c. 對所有所需資產重複此程序。
   d. 點選“儲存”。
5. 點選“提交”。

新增使用者或群組並指派角色後，刷新資源清單。

配置審核日誌設定

SnapCenter伺服器的每個活動都會產生審計日誌。預設情況下，稽核日誌會儲存在預設安裝位置 *C:\Program Files\ NetApp\ SnapCenter WebApp\audit*。

透過為每個稽核事件產生數位簽章摘要來保護稽核日誌，以防止未經授權的修改。產生的摘要保存在單獨的審計校驗和文件中，並進行定期的完整性檢查以確保內容的完整性。

您應該以「SnapCenterAdmin」角色登入。

關於此任務

- 在以下情況下會發送警報：
  - 審計日誌完整性檢查計劃或 Syslog 伺服器已啟用或停用
  - 稽核日誌完整性檢查、稽核日誌或 Syslog 伺服器日誌故障
  - 磁碟空間不足
- 僅當完整性檢查失敗時才發送電子郵件。
- 您應該同時修改稽核日誌目錄和稽核校驗和日誌目錄路徑。您不能只修改其中一個。
- 當稽核日誌目錄和稽核校驗和日誌目錄路徑被修改時，無法對先前位置的稽核日誌執行完整性檢查。
- 稽核日誌目錄和稽核校驗和日誌目錄路徑應位於SnapCenter Server 的本機磁碟機上。

  不支援共用或網路安裝的磁碟機。
- 如果在 Syslog 伺服器設定中使用 UDP 協議，則由於連接埠關閉或不可用而導致的錯誤無法在SnapCenter中擷取為錯誤或警報。
- 您可以使用 Set-SmAuditSettings 和 Get-SmAuditSettings 指令來設定稽核日誌。

  可以透過執行 Get-Help command_name 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 "SnapCenter軟體 Cmdlet 參考指南"。

步驟

1. 在*設定*頁面中，導覽至*設定*>*全域設定*>*稽核日誌設定*。
2. 在審計日誌部分，輸入詳細資訊。
3. 進入*審計日誌目錄*和*審計校驗和日誌目錄*
   a. 輸入最大檔案大小
   b. 輸入最大日誌檔數
   c. 輸入磁碟空間使用率百分比以發送警報
4. （可選）啟用*記錄 UTC 時間*。
5. （選用）啟用*稽核日誌完整性檢查計畫*並點選*開始完整性檢查*進行按需完整性檢查。

   您也可以執行*Start-SmAuditIntegrityCheck*指令來啟動按需完整性檢查。
6. （可選）啟用轉發審計日誌到遠端系統日誌伺服器並輸入系統日誌伺服器詳細資訊。

您應該將 Syslog 伺服器中的憑證匯入 TLS 1.2 協定的「受信任的根」。

a. 輸入 Syslog 伺服器主機
b. 輸入 Syslog 伺服器端口
c. 輸入 Syslog 伺服器協議
d. 輸入 RFC 格式

7. 點選“儲存”。
8. 您可以透過點選「監視」>「作業」查看稽核完整性檢查和磁碟空間檢查。

使用SnapCenter Server 設定安全的 MySQL 連接

如果您想在獨立配置或網路負載平衡 (NLB) 配置中保護SnapCenter伺服器和 MySQL 伺服器之間的通信，則可以產生安全通訊端層 (SSL) 憑證和金鑰檔案。

為獨立SnapCenter伺服器設定配置安全的 MySQL 連接

如果您想要確保SnapCenter伺服器和 MySQL 伺服器之間的通訊安全，可以產生安全通訊端層 (SSL) 憑證和金鑰檔案。您必須在 MySQL 伺服器和SnapCenter伺服器中設定憑證和金鑰檔案。

產生以下證書：

- CA 憑證
- 伺服器公鑰和私鑰文件
- 客戶端公鑰和私鑰文件

步驟

1. 使用 openssl 指令為 Windows 上的 MySQL 伺服器和用戶端設定 SSL 憑證和金鑰檔案。

   有關信息，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案的通用名稱值必須與用於 CA 憑證的通用名稱值不同。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案將會失敗。

   *最佳實務：*您應該使用伺服器完全限定網域名稱 (FQDN) 作為伺服器憑證的通用名稱。

2. 將 SSL 憑證和金鑰檔案複製到 MySQL 資料夾。

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

3. 更新MySQL伺服器設定檔（my.ini）中的CA憑證、伺服器公鑰、用戶端公鑰、伺服器私鑰、用戶端私鑰路徑。

   預設的 MySQL 伺服器設定檔（my.ini）路徑是 `C:\ProgramData\NetApp\SnapCenter\MySQL Data\my.ini`。

您必須在 MySQL 伺服器設定檔（my.ini）的 [mysqld] 部分中指定 CA 憑證、伺服器公用憑證和伺服器私密金鑰路徑。

您必須在 MySQL 伺服器設定檔（my.ini）的 [client] 部分中指定 CA 憑證、用戶端公用憑證和用戶端私鑰路徑。

以下範例顯示複製到預設資料夾中 my.ini 檔案的 [mysqld] 部分的憑證和金鑰文件 `C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data`。

```
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"
```

以下範例顯示了 my.ini 檔案的 [client] 部分中更新的路徑。

```
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 Internet 資訊伺服器 (IIS) 中的SnapCenter Server Web 應用程式。
5. 重新啟動 MySQL 服務。
6. 更新SnapManager檔中 MySQLProtocol 鍵的值。

   以下範例顯示了SnapManager檔案中更新的 MySQLProtocol 鍵的值。

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

7. 使用 my.ini 檔案的 [client] 部分中提供的路徑更新SnapManager.Web.UI.dll.config 檔案。

   以下範例顯示了 my.ini 檔案的 [client] 部分中更新的路徑。

```
<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 IIS 中啟動SnapCenter Server Web 應用程式。

為 **HA** 設定配置安全的 **MySQL** 連接

如果您想要確保SnapCenter伺服器和 MySQL 伺服器之間的通訊安全，您可以為高可用性 (HA) 節點產生安全通訊端層 (SSL) 憑證和金鑰檔案。您必須在 MySQL 伺服器和 HA 節點上設定憑證和金鑰檔案。

產生以下證書：

- CA 憑證

  在其中一個 HA 節點上產生 CA 證書，並將此 CA 證書複製到另一個 HA 節點。

- 兩個 HA 節點的伺服器公共憑證和伺服器私鑰文件
- 兩個 HA 節點的客戶端公共憑證和客戶端私鑰文件

步驟

1. 對於第一個 HA 節點，使用 openssl 指令為 Windows 上的 MySQL 伺服器和用戶端設定 SSL 憑證和金鑰檔案。

   有關信息，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案的通用名稱值必須與用於 CA 憑證的通用名稱值不同。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案將會失敗。

   *最佳實務：*您應該使用伺服器完全限定網域名稱 (FQDN) 作為伺服器憑證的通用名稱。

2. 將 SSL 憑證和金鑰檔案複製到 MySQL 資料夾。

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

3. 更新MySQL伺服器設定檔（my.ini）中的CA憑證、伺服器公鑰、用戶端公鑰、伺服器私鑰、用戶端私鑰路徑。

   預設 MySQL 伺服器設定檔 (my.ini) 路徑為 C:\ProgramData\ NetApp\ SnapCenter\MySQL Data\my.ini。

您必須在 MySQL 伺服器設定檔（my.ini）的 [mysqld] 部分中指定 CA 憑證、伺服器公用憑證和伺服器私密金鑰路徑。

您必須在 MySQL 伺服器設定檔（my.ini）的 [client] 部分中指定 CA 憑證、用戶端公用憑證和用戶端私鑰路徑。

以下範例顯示複製到預設資料夾 C:/ProgramData/ NetApp/ SnapCenter/MySQL Data/Data 中 my.ini 檔案的 [mysqld] 部分的憑證和金鑰檔案。

```
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"
```

以下範例顯示了 my.ini 檔案的 [client] 部分中更新的路徑。

```
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，複製 CA 憑證並產生伺服器公鑰憑證、伺服器私鑰檔案、用戶端公鑰憑證和用戶端私鑰檔案。執行以下步驟：

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

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

      您不能再次建立 CA 憑證。您應該只建立伺服器公共憑證、客戶端公共憑證、伺服器私鑰檔案和客戶端私鑰檔案。

   b. 對於第一個 HA 節點，使用 openssl 指令為 Windows 上的 MySQL 伺服器和用戶端設定 SSL 憑證和金鑰檔案。

      "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案的通用名稱值必須與用於 CA 憑證的通用名稱值不同。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案將會失敗。

建議使用伺服器 FQDN 作為伺服器憑證的通用名稱。

c. 將 SSL 憑證和金鑰檔案複製到 MySQL 資料夾。

d. 更新MySQL伺服器設定檔（my.ini）中的CA憑證、伺服器公鑰、用戶端公鑰、伺服器私鑰、用戶端私鑰路徑。

您必須在 MySQL 伺服器設定檔（my.ini）的 [mysqld] 部分中指定 CA 憑證、伺服器公用憑證和伺服器私密金鑰路徑。

您必須在 MySQL 伺服器設定檔（my.ini）的 [client] 部分中指定 CA 憑證、用戶端公用憑證和用戶端私鑰路徑。

以下範例顯示複製到預設資料夾 C:/ProgramData/ NetApp/ SnapCenter/MySQL Data/Data 中 my.ini 檔案的 [mysqld] 部分的憑證和金鑰檔案。

```
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"
```

以下範例顯示了 my.ini 檔案的 [client] 部分中更新的路徑。

```
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. 停止兩個 HA 節點上的 Internet 資訊伺服器 (IIS) 中的SnapCenter Server 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 MySQLProtocol 鍵的值。

   以下範例顯示了SnapManager檔案中更新的 MySQLProtocol 鍵的值。

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

8. 使用您在 my.ini 檔案的 [client] 部分中為兩個 HA 節點指定的路徑更新SnapManager.Web.UI.dll.config 檔案。

   以下範例顯示了 my.ini 檔案的 [client] 部分中更新的路徑。

   ```
   <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. 在兩個 HA 節點上的 IIS 中啟動SnapCenter Server Web 應用程式。
10. 在其中一個 HA 節點上使用帶有 -Force 選項的 Set-SmRepositoryConfig -RebuildSlave -Force PowerShell cmdlet 在兩個 HA 節點上建立安全的 MySQL 複製。

    即使複製狀態良好，-Force 選項也允許您重建從屬儲存庫。

配置基於憑證的身份驗證

基於憑證的身份驗證透過驗證SnapCenter伺服器和插件主機的身份來增強安全性，確保安全和加密的通訊。

啟用基於憑證的身份驗證

若要為SnapCenter Server 和 Windows 外掛程式主機啟用基於憑證的驗證，請執行下列 PowerShell cmdlet。對於 Linux 外掛主機，啟用雙向 SSL 時將啟用基於憑證的驗證。

- 若要啟用基於用戶端憑證的身份驗證：

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

- 若要停用基於客戶端憑證的身份驗證：

```
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伺服器匯出到外掛程式主機。

開始之前

您應該已經配置了雙向 SSL。

步驟

1. 前往 Microsoft 管理主控台 (MMC)，然後按一下 檔案 > 新增/移除管理單元。
2. 在“新增或刪除管理單元”視窗中，選擇“證書”，然後按一下“新增”。
3. 在憑證管理單元視窗中，選擇「電腦帳戶」選項，然後按一下「完成」。
4. 按一下 控制台根 > 憑證 - 本機 > 個人 > 憑證。
5. 右鍵點選用於SnapCenter Server 的採購 CA 證書，然後選擇 所有任務 > 匯出 以啟動匯出精靈。
6. 在精靈中執行下列操作。

對於此選項...	執行以下操作...
匯出私鑰	選擇*否，不匯出私鑰*，然後按一下*下一步*。
匯出文件格式	按一下“下一步”。
檔案名稱	點選*瀏覽*並指定儲存憑證的檔案路徑，然後點選*下一步*。
完成憑證匯出精靈	查看摘要，然後按一下「完成」開始匯出。

SnapCenter HA 設定和SnapCenter Plug-in for VMware vSphere不支援基於憑證的驗證。

將 CA 憑證匯入 Windows 插件主機

若要使用匯出的SnapCenter Server CA 證書，您應該使用 Microsoft 管理主控台 (MMC) 將相關憑證匯入至SnapCenter Windows 外掛程式主機。

步驟

1. 前往 Microsoft 管理主控台 (MMC)，然後按一下 檔案 > 新增/移除管理單元。
2. 在“新增或刪除管理單元”視窗中，選擇“證書”，然後按一下“新增”。
3. 在憑證管理單元視窗中，選擇「電腦帳戶」選項，然後按一下「完成」。

4. 按一下 控制台根 > 憑證 - 本機 > 個人 > 憑證。
5. 右鍵單擊資料夾“個人”，然後選擇*所有任務* > *導入*以啟動導入精靈。
6. 在精靈中執行下列操作。

對於此選項...	執行以下操作...
商店位置	按一下“下一步”。
要導入的文件	選擇以 .cer 副檔名結尾的SnapCenter伺服器憑證。
證書存儲	按一下“下一步”。
完成憑證匯出精靈	查看摘要，然後按一下「完成」開始匯入。

將 CA 憑證匯入 UNIX 插件主機

您應該將 CA 憑證匯入到 UNIX 插件主機。

關於此任務

- 您可以管理 SPL 金鑰庫的密碼，以及正在使用的 CA 簽章金鑰對的別名。
- SPL 金鑰庫的密碼和私鑰的所有相關別名的密碼應該相同。

步驟

1. 您可以從 SPL 屬性檔案中檢索 SPL 金鑰庫預設密碼。它是鍵對應的值 `SPL_KEYSTORE_PASS`。
2. 更改密鑰庫密碼： `$ keytool -storepasswd -keystore keystore.jks`
3. 將金鑰庫中所有私鑰條目別名的密碼變更為與金鑰庫相同的密碼： `$ keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`
4. 對金鑰 SPL_KEYSTORE_PASS 進行相同的更新 `spl.properties``文件。
5. 修改密碼後重啟服務。

將根憑證或中繼憑證設定到 **SPL** 信任庫

您應該將根憑證或中間憑證設定到 SPL 信任庫。您應該新增根 CA 證書，然後新增中間 CA 證書。

步驟

1. 導航至包含 SPL 金鑰庫的資料夾： `/var/opt/snapcenter/spl/etc` 。
2. 找到文件 `keystore.jks`。
3. 列出密鑰庫中新增的憑證： `$ keytool -list -v -keystore keystore.jks`
4. 新增根證書或中間證書： `$ keytool -import -trustcacerts -alias <AliasNameForCerticateToBeImported> -file /<CertificatePath> -keystore keystore.jks`

5. 將根憑證或中間憑證配置到 SPL 信任庫後重新啟動服務。

將 **CA** 簽章金鑰對配置到 **SPL** 信任庫

您應該將 CA 簽署的金鑰對配置到 SPL 信任庫。

步驟

1. 導航至包含 SPL 金鑰庫的資料夾 `/var/opt/snapcenter/spl/etc`。
2. 找到文件 `keystore.jks`。
3. 列出密鑰庫中新增的憑證： `$ keytool -list -v -keystore keystore.jks`
4. 新增具有私鑰和公鑰的 CA 憑證。 `$ keytool -importkeystore -srckeystore <CertificatePathToImport> -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS`
5. 列出密鑰庫中新增的憑證。 `$ keytool -list -v -keystore keystore.jks`
6. 驗證金鑰庫是否包含與新增至金鑰庫的新 CA 憑證相對應的別名。
7. 將新增的CA憑證私鑰密碼變更為keystore密碼。

   預設 SPL 金鑰庫密碼是金鑰 SPL_KEYSTORE_PASS 的值 `spl.properties`文件。

   `$ keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore keystore.jks`
8. 如果CA憑證中的別名較長，且包含空格或特殊字元（“*”，“，”），請將別名修改為簡單名稱： `$ keytool -changealias -alias "<OrignalAliasName>" -destalias "<NewAliasName>" -keystore keystore.jks`
9. 從位於的金鑰庫配置別名 `spl.properties`文件。根據鍵 SPL_CERTIFICATE_ALIAS 更新此值。
10. 將 CA 簽署金鑰對配置到 SPL 信任庫後重新啟動服務。

匯出SnapCenter證書

您應該以 .pfx 格式匯出SnapCenter憑證。

步驟

1. 前往 Microsoft 管理主控台 (MMC)，然後按一下 檔案 > 新增/移除管理單元。
2. 在“新增或刪除管理單元”視窗中，選擇“證書”，然後按一下“新增”。
3. 在憑證管理單元視窗中，選擇「我的使用者帳戶」選項，然後按一下「完成」。
4. 按一下 控制台根 > 憑證 - 目前使用者 > 受信任的根憑證授權單位 > 憑證。
5. 右鍵點選具有SnapCenter友善名稱的證書，然後選擇 所有任務 > 匯出 以啟動匯出精靈。
6. 完成嚮導，如下圖所示：

在此精靈視窗中...	執行以下操作...
匯出私鑰	選擇選項*是，匯出私鑰*，然後按一下*下一步*。
匯出文件格式	不做任何更改；按一下“下一步”。
安全	指定匯出憑證要使用的新密碼，然後按一下「下一步」。
要匯出的文件	指定匯出憑證的檔案名稱（必須使用.pfx），然後按一下「下一步」。
完成憑證匯出精靈	查看摘要，然後按一下「完成」開始匯出。

為 Windows 主機設定 CA 憑證

產生CA憑證CSR文件

您可以產生憑證簽署要求 (CSR) 並匯入可使用產生的 CSR 從憑證授權單位 (CA) 取得的憑證。該憑證將有一個與之關聯的私鑰。

CSR 是一段編碼文本，提供給授權憑證供應商以取得簽署的 CA 憑證。

CA 憑證 RSA 金鑰長度必須至少為 3072 位元。

有關生成 CSR 的信息，請參閱 "如何產生CA憑證CSR文件"。

如果您擁有您的網域（*.domain.company.com）或您的系統（machine1.domain.company.com）的 CA 證書，您可以跳過生成 CA 證書 CSR 檔案。您可以使用SnapCenter部署現有的 CA 憑證。

對於叢集配置，CA 憑證中應提及叢集名稱（虛擬叢集 FQDN）和對應的主機名稱。在取得憑證之前，可以透過填寫主題備用名稱 (SAN) 欄位來更新憑證。對於通配符憑證（*.domain.company.com），該憑證將隱式包含網域的所有主機名稱。

匯入 CA 憑證

您必須使用 Microsoft 管理主控台 (MMC) 將 CA 憑證匯入SnapCenter伺服器和 Windows 主機外掛程式。

步驟

1. 前往 Microsoft 管理主控台 (MMC)，然後按一下 檔案 > 新增/移除管理單元。
2. 在“新增或刪除管理單元”視窗中，選擇“證書”，然後按一下“新增”。
3. 在憑證管理單元視窗中，選擇「電腦帳戶」選項，然後按一下「完成」。

4. 按一下 控制台根 > 憑證 - 本機電腦 > 受信任的根憑證授權單位 > 憑證。
5. 右鍵單擊資料夾“受信任的根憑證授權單位”，然後選擇*所有任務*>*匯入*以啟動匯入精靈。
6. 完成嚮導，如下圖所示：

在此精靈視窗中...	執行以下操作...
導入私鑰	選擇選項*是*，匯入私鑰，然後按一下*下一步*。
導入文件格式	不做任何更改；按一下“下一步”。
安全	指定匯出憑證要使用的新密碼，然後按一下「下一步」。
完成憑證匯入精靈	查看摘要，然後按一下「完成」開始匯入。

匯入憑證時需攜帶私鑰（支援格式為：**.pfx**、.p12、*.p7b）。

7. 對「個人」資料夾重複步驟 5。

取得 **CA** 憑證指紋

憑證指紋是用於識別憑證的十六進位字串。指紋是使用指紋演算法根據憑證內容計算出來的。

步驟

1. 在 GUI 上執行以下操作：
   a. 雙擊該證書。
   b. 在「證書」對話方塊中，按一下「詳細資料」標籤。
   c. 捲動瀏覽欄位清單並按一下「指紋」。
   d. 從框複製十六進位字元。
   e. 刪除十六進制數之間的空格。

      例如，如果指紋為：“a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b”，刪除空格後，將為：“a909502dd82ae41433e68383883”。

2. 從 PowerShell 執行以下操作：
   a. 執行以下命令列出已安裝憑證的指紋並透過主題名稱識別最近安裝的憑證。

      Get-ChildItem -Path 憑證:*\LocalMachine\My*

   b. 複製指紋。

使用 **Windows** 主機插件服務設定 **CA** 憑證

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

在SnapCenter伺服器和所有已部署 CA 憑證的插件主機上執行下列步驟。

步驟

1. 透過執行以下命令刪除與 SMCore 預設連接埠 8145 的現有憑證綁定：

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

   例如：

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

. 透過執行下列命令將新安裝的憑證與 `Windows` 主機插件服務綁定：

```
> $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**站點配置 **CA** 證書

您應該在 Windows 主機上使用SnapCenter網站設定 CA 憑證。

步驟

1. 在安裝了SnapCenter的 Windows Server 上開啟 IIS 管理員。
2. 在左側導覽窗格中，按一下「連線」。
3. 展開伺服器的名稱和*網站*。
4. 選擇要安裝 SSL 憑證的SnapCenter網站。
5. 導覽至*操作* > 編輯網站，按一下*綁定*。
6. 在綁定頁面中，選擇「https 綁定」。
7. 按一下"編輯"。

8. 從 SSL 憑證下拉清單中，選擇最近匯入的 SSL 憑證。
9. 按一下“確定”。

SnapCenter Scheduler 網站（預設連接埠：8154，HTTPS）配置了自簽名憑證。此連接埠在SnapCenter Server 主機內進行通信，且不需要使用 CA 憑證進行設定。但是，如果您的環境要求您使用 CA 證書，請使用SnapCenter Scheduler 網站重複步驟 5 到 9。

如果下拉式選單中未列出最近部署的 CA 證書，請檢查該 CA 證書是否與私鑰相關聯。

確保使用下列路徑新增憑證：控制台根 **>** 憑證 **-** 本機 **>** 受信任的根憑證授權單位 **>** 憑證。

為**SnapCenter**啟用 **CA** 憑證

您應該設定 CA 憑證並為SnapCenter伺服器啟用 CA 憑證驗證。

開始之前

- 您可以使用 Set-SmCertificateSettings cmdlet 啟用或停用 CA 憑證。
- 您可以使用 Get-SmCertificateSettings cmdlet 顯示SnapCenter伺服器的憑證狀態。

可以透過執行_Get-Help command_name_來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您可以參考 "SnapCenter軟體 Cmdlet 參考指南"。

步驟

1. 在「設定」頁面中，導覽至「設定」>「全域設定」>「**CA** 憑證設定」。
2. 選擇*啟用憑證驗證*。
3. 按一下“應用”。

完成後

託管主機選項卡主機顯示一個掛鎖，掛鎖的顏色表示SnapCenter伺服器和插件主機之間的連線狀態。

- * * 表示沒有啟用或指派給插件主機的 CA 憑證。
- * * 表示 CA 憑證驗證成功。
- * * 表示無法驗證 CA 憑證。
- * * 表示無法檢索連線資訊。

當狀態為黃色或綠色時，表示資料保護操作已成功完成。

為Linux主機設定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，則應為 nginx 反向代理、稽核日誌記錄和SnapCenter服務設定證書。

設定nginx證書

步驟

1. 導航至 */etc/nginx/conf.d*： `cd /etc/nginx/conf.d`
2. 使用 vi 或任何文字編輯器開啟 **snapcenter.conf**。
3. 導航到設定檔中的伺服器部分。
4. 修改_ssl_certificate_和_ssl_certificate_key_的路徑以指向CA憑證。
5. 儲存並關閉文件。
6. 重新載入 nginx： `$nginx -s reload`

配置審核日誌證書

步驟

1. 使用 vi 或任何文字編輯器開啟 _INSTALL_DIR/ NetApp/snapcenter/SnapManagerWeb/ SnapManager。

   INSTALL_DIR 的預設值是 */opt*。

2. 編輯 **AUDILOG_CERTIFICATE_PATH** 和 **AUDILOG_CERTIFICATE_PASSWORD** 鍵以分別包含 CA 憑證路徑和密碼。

   稽核日誌憑證僅支援 *.pfx* 格式。

3. 儲存並關閉文件。
4. 重新啟動 **snapmanagerweb** 服務： `$ systemctl restart snapmanagerweb`

配置SnapCenter服務證書

步驟

1. 使用 vi 或任何文字編輯器開啟以下設定檔。
   - *INSTALL_DIR/ NetApp/snapcenter/SnapManagerWeb/ SnapManager.Web.UI.dll.config*
   - 安裝目錄NetApp
   - 安裝目錄NetApp

     INSTALL_DIR 的預設值是 */opt*。

2. 編輯 **SERVICE_CERTIFICATE_PATH** 和 **SERVICE_CERTIFICATE_PASSWORD** 鍵以分別包含 CA 憑證路徑和密碼。

   SnapCenter服務憑證僅支援 *.pfx* 格式。

3. 儲存並關閉文件。
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 通信

在 Windows 主機上設定雙向 SSL 通信

您應該配置雙向 SSL 通訊以保護 Windows 主機上的SnapCenter伺服器與插件之間的相互通訊。

開始之前

- 您應該已經產生了具有最小支援金鑰長度 3072 的 CA 憑證 CSR 檔案。
- CA憑證應支援伺服器認證和用戶端認證。
- 您應該擁有一份包含私鑰和指紋詳細資訊的 CA 憑證。
- 您應該已經啟用單向 SSL 設定。

  有關詳細信息，請參閱 "配置CA憑證部分。"

- 您必須在所有插件主機和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. 若要綁定端口，請使用 PowerShell 命令在SnapCenter Server 主機上對SnapCenter IIS Web 伺服器連接埠 8146（預設）執行下列步驟，並再次對 SMCore 連接埠 8145（預設）執行下列步驟。

   a. 使用下列 PowerShell 指令刪除現有的SnapCenter自簽章憑證連接埠綁定。

      ```
      > 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. 將新購買的 CA 憑證與SnapCenter伺服器和 SMCore 連接埠綁定。

      ```
      > $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，請透過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**」來存取新購買的 CA 憑證。
   a. 前往 Microsoft 管理主控台 (MMC)，然後按一下 檔案 > 新增/移除管理單元。
   b. 在"新增或刪除管理單元"視窗中，選擇"證書"，然後按一下"新增"。
   c. 在憑證管理單元視窗中，選擇「電腦帳戶」選項，然後按一下「完成」。
   d. 按一下 控制台根 > 憑證 - 本機 > 個人 > 憑證。
   e. 選擇SnapCenter證書。
   f. 若要啟動新增使用者\權限精靈，請以滑鼠右鍵按一下 CA 憑證並選擇 所有任務 > 管理私密金鑰。
   g. 按一下"新增"，在"選取使用者和群組"精靈中將位置變更為本機電腦名稱（層次結構中的最頂層）
   h. 新增 IIS AppPool\ SnapCenter用戶，授予完全控制權限。
3. 對於 **CA** 憑證 **IIS** 權限，從下列路徑在SnapCenter Server 中新增新的 DWORD 登錄項目項目：

   在 Windows 登錄編輯器中，遍歷下面提到的路徑，

   ```
   HKey_Local_Machine\SYSTEM\CurrentControlSet\Control\SecurityProv ders\SCHANNEL
   ```

4. 在 SCHANNEL 註冊表配置上下文中建立新的 DWORD 註冊表項條目。

   ```
   SendTrustedIssuerList = 0

   ClientAuthTrustMode = 2
   ```

配置**SnapCenter Windows** 插件以進行雙向 **SSL** 通信

您應該使用 PowerShell 命令設定SnapCenter Windows 插件以進行雙向 SSL 通訊。

開始之前

確保 CA 憑證指紋可用。

步驟

1. 若要綁定端口，請在 Windows 插件主機上對 SMCore 連接埠 8145（預設）執行下列操作。

   a. 使用下列 PowerShell 指令刪除現有的SnapCenter自簽章憑證連接埠綁定。

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

      例如，

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

   b. 將新購買的CA憑證與SMCore連接埠綁定。

      ```
      > $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** 通信

您可以啟用雙向 SSL 通信，以使用 PowerShell 命令保護 Windows 主機上的SnapCenter伺服器與插件之間的相互通訊。

開始之前

首先執行所有插件和 SMCore 代理的命令，然後執行伺服器的命令。

步驟

1. 若要啟用雙向 SSL 通信，請在SnapCenter伺服器上執行下列命令，用於插件、伺服器以及需要雙向 SSL 通訊的每個代理程式。

   ```
   > 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應用程式集區回收作業。 `> Restart-WebAppPool -Name "SnapCenter"`
3. 對於 Windows 插件，透過執行下列 PowerShell 命令重新啟動 SMCore 服務：

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

禁用雙向 SSL 通信

您可以使用 PowerShell 指令停用雙向 SSL 通訊。

關於此任務

- 首先執行所有插件和 SMCore 代理的命令，然後執行伺服器的命令。
- 當您停用雙向 SSL 通訊時，CA 憑證及其配置不會被刪除。
- 若要為SnapCenter Server 新增主機，必須停用所有插件主機的雙向 SSL。
- 不支援 NLB 和 F5。

步驟

1. 若要停用雙向 SSL 通信，請在SnapCenter Server 上對所有插件主機和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應用程式集區回收作業。 `> Restart-WebAppPool -Name "SnapCenter"`
3. 對於 Windows 插件，透過執行下列 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 通信

在 Linux 主機上設定雙向 SSL 通信

您應該配置雙向 SSL 通訊以保護 Linux 主機上的SnapCenter伺服器與插件之間的相互通訊。

開始之前

- 您應該已經為 Linux 主機設定了 CA 憑證。
- 您必須在所有插件主機和SnapCenter伺服器上啟用雙向 SSL 通訊。

步驟

1. 將 **certificate.pem** 複製到 */etc/pki/ca-trust/source/anchors/*。
2. 將憑證新增到 Linux 主機的信任清單中。
   - `cp root-ca.pem /etc/pki/ca-trust/source/anchors/`
   - `cp certificate.pem /etc/pki/ca-trust/source/anchors/`
   - `update-ca-trust extract`
3. 驗證證書是否已新增至信任清單。`trust list | grep "<CN of your certificate>"`
4. 更新SnapCenter **nginx** 檔案中的 **ssl_certificate** 和 **ssl_certificate_key** 並重新啟動。
   - `vim /etc/nginx/conf.d/snapcenter.conf`
   - `systemctl restart nginx`
5. 刷新SnapCenter伺服器 GUI 連結。
6. 更新位於 _ /<安裝路徑>/ NetApp /snapcenter/SnapManagerWeb_ 的 * SnapManager .Web.UI.dll.config* 和位於 */<安裝路徑>/ NetApp/snapcenter/SMCore* 的 **SMCoreServiceHost.dll.config** 中的下列登錄項目的值。
   - <add key="SERVICE_CERTIFICATE_PATH" value="<證書.pfx 的路徑>" />
   - <新增鍵=“SERVICE_CERTIFICATE_PASSWORD”值=“<密碼>”/>
7. 重新啟動以下服務。
   - `systemctl restart smcore.service`
   - `systemctl restart snapmanagerweb.service`
8. 驗證憑證是否已附加至SnapManager Web 連接埠。`openssl s_client -connect localhost:8146 -brief`
9. 驗證憑證是否已附加到 smcore 連接埠。`openssl s_client -connect localhost:8145 -brief`
10. 管理 SPL 金鑰庫和別名的密碼。
    a. 檢索指派給 SPL 屬性檔案中的 **SPL_KEYSTORE_PASS** 鍵的 SPL 金鑰庫預設密碼。
    b. 更改密鑰庫密碼。`keytool -storepasswd -keystore keystore.jks`
    c. 更改所有私鑰條目別名的密碼。`keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`
    d. 為 *spl.properties* 中的金鑰 **SPL_KEYSTORE_PASS** 更新相同的密碼。
    e. 重新啟動服務。
11. 在插件 Linux 主機上，在 SPL 插件的金鑰庫中新增根憑證和中間憑證。
    - `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. 如果需要，請重新命名任何別名。 `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.pfx** 的別名更新 *spl.properties* 檔案中的 **SPL_CERTIFICATE_ALIAS** 的值，然後重新啟動 SPL 服務： `systemctl restart spl`

13. 驗證憑證是否已附加到 smcore 連接埠。 `openssl s_client -connect localhost:8145 -brief`

在 **Linux** 主機上啟用 **SSL** 通信

您可以啟用雙向 SSL 通信，以使用 PowerShell 命令保護 Linux 主機上的SnapCenter伺服器與插件之間的相互通訊。

步

1. 執行以下操作以啟用單向 SSL 通訊。
   a. 登入SnapCenter GUI。
   b. 按一下“設定”>“全域設定”，然後選擇“在**SnapCenter**伺服器上啟用憑證驗證”。
   c. 按一下“主機”>“託管主機”，然後選擇要啟用單向 SSL 的插件主機。
   d. 點選圖標，然後按一下*啟用憑證驗證*。
2. 從SnapCenter Server 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"}`

配置 **Active Directory**、**LDAP** 和 **LDAPS**

註冊不受信任的 **Active Directory** 網域

您應該向SnapCenter Server 註冊 Active Directory，以管理來自多個不受信任的 Active Directory 網域的主機、使用者和群組。

開始之前

LDAP 和 LDAPS 協議

- 您可以使用 LDAP 或 LDAPS 協定註冊不受信任的活動目錄網域。
- 您應該已經啟用插件主機和SnapCenter伺服器之間的雙向通訊。

- 應設定從SnapCenter伺服器到插件主機的 DNS 解析，反之亦然。

LDAP 協定

- 完全限定網域名稱 (FQDN) 應該可以從SnapCenter Server 解析。

  您可以使用 FQDN 註冊不受信任的網域。如果無法從SnapCenter伺服器解析 FQDN，則可以使用網域控制器 IP 位址進行註冊，並且該位址應該可以從SnapCenter伺服器解析。

LDAPS 協定

- LDAPS 需要 CA 憑證來在活動目錄通訊期間提供端對端加密。

  "為 LDAPS 設定 CA 用戶端憑證"

- 網域控制器主機名稱（DCHostName）應該可以從SnapCenter伺服器存取。

關於此任務

- 您可以使用SnapCenter使用者介面、PowerShell cmdlet 或 REST API 來註冊不受信任的網域。

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. 點選 + 註冊一個新網域。
5. 在註冊新網域頁面中，選擇 **LDAP** 或 **LDAPS**。
   a. 如果選擇 **LDAP**，請指定為 LDAP 註冊不受信任網域所需的資訊：

對於這個領域...	這樣做...
網域	指定網域的 NetBIOS 名稱。
域 FQDN	指定 FQDN 並按一下 解析。
網域控制器 IP 位址	如果無法從SnapCenter伺服器解析網域 FQDN，請指定一個或多個網域控制器 IP 位址。 有關更多信息，請參閱 "從 GUI 為不受信任的網域新增網域控制器 IP" 。

   b. 如果選擇 **LDAPS**，請指定為 LDAPS 註冊不受信任網域所需的資訊：

對於這個領域...	這樣做...
網域	指定網域的 NetBIOS 名稱。
域 FQDN	指定 FQDN。
網域控制器名稱	指定一個或多個網域控制站名稱，然後按一下「解析」。
網域控制器 IP 位址	如果網域控制站名稱無法從SnapCenter Server 解析，則應修正 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

當您需要為SnapCenter啟用 Active Directory 讀取權限時，您可以在 Windows Server 上設定 Internet 資訊服務 (IIS) 來建立自訂應用程式集區帳戶。

步驟

1. 在安裝了SnapCenter的 Windows Server 上開啟 IIS 管理員。
2. 在左側導覽窗格中，按一下「應用程式集區」。
3. 在應用程式集區清單中選擇SnapCenter ，然後按一下操作窗格中的「進階設定」。
4. 選擇“身分”，然後按一下“...”以編輯SnapCenter應用程式集區身分。
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”。

   自訂帳戶取代了SnapCenter應用程式集區的內建 ApplicationPoolIdentity 帳戶。

為 **LDAPS** 設定 **CA** 用戶端憑證

當 Windows Active Directory LDAPS 配置了 CA 憑證時，您應該在SnapCenter伺服器上為 LDAPS 設定 CA 用戶端憑證。

步驟

1. 前往 Microsoft 管理主控台 (MMC)，然後按一下 檔案 > 新增/移除管理單元。
2. 在“新增或刪除管理單元”視窗中，選擇“證書”，然後按一下“新增”。
3. 在憑證管理單元視窗中，選擇「電腦帳戶」選項，然後按一下「完成」。
4. 按一下 控制台根 > 憑證 - 本機電腦 > 受信任的根憑證授權單位 > 憑證。
5. 右鍵單擊資料夾“受信任的根憑證授權單位”，然後選擇*所有任務*>*匯入*以啟動匯入精靈。
6. 完成嚮導，如下圖所示：

在此精靈視窗中...	執行以下操作...
在嚮導的第二頁	按一下“瀏覽”，選擇“根憑證”，然後按一下“下一步”。
完成憑證匯入精靈	查看摘要，然後按一下「完成」開始匯入。

7. 對中間證書重複步驟 5 和 6。

版權資訊

商標資訊