配置SnapCenter伺服器

SnapCenter software

NetApp
November 06, 2025

目錄

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
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。

在這個領域...	這樣做...
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。
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。

財產	描述
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。

選擇...	如果...
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。