



將**NetApp Disaster Recovery**與**Amazon EVS** 結合使用

NetApp Disaster Recovery

NetApp
February 17, 2026

This PDF was generated from <https://docs.netapp.com/zh-tw/data-services-disaster-recovery/reference/evs-deploy-guide-introduction.html> on February 17, 2026. Always check docs.netapp.com for the latest.

目錄

將NetApp Disaster Recovery與 Amazon EVS 結合使用	1
使用 Amazon Elastic VMware Service 和Amazon FSx for NetApp ONTAP實作NetApp Disaster Recovery. .	1
使用 Amazon EVS 和 Amazon FS for NetApp ONTAP 的NetApp Disaster Recovery解決方案概述	1
安裝用於NetApp Disaster Recovery的NetApp Console代理	2
安裝	2
為 Amazon EVS 配置NetApp Disaster Recovery	3
為 Amazon EVS 配置NetApp Disaster Recovery概述	3
Amazon EVS 與NetApp Disaster Recovery的先決條件	3
使用NetApp Disaster Recovery功能將本機陣列新增至適用於 Amazon EVS 的NetApp Console系統	4
將NetApp Disaster Recovery服務新增至您的 Amazon EVS NetApp Console帳戶	5
在NetApp Disaster Recovery中為 Amazon EVS 新增站點	6
在NetApp Disaster Recovery中新增本機和 Amazon EVS vCenter 叢集	7
為 Amazon EVS 建立複製計畫	8
在NetApp Disaster Recovery概述中建立複製計畫	8
建立複製計畫：步驟 1 - 在NetApp Disaster Recovery中選擇 vCenter	8
建立複製計畫：步驟 2 - 在NetApp Disaster Recovery中選擇虛擬機器資源	9
建立複製計畫：步驟 3 - 在NetApp Disaster Recovery中對應資源	9
建立複製計畫：步驟 4 - 驗證NetApp Disaster Recovery中的設置	13
驗證NetApp Disaster Recovery中一切正常	13
使用NetApp Disaster Recovery執行複製計畫操作	14
故障轉移	14
測試故障轉移	14
運行合規性檢查	15
刷新資源	15
遷移	15
立即拍攝快照	16
停用或啟用複製計畫	16
清理舊快照	16
協調快照	16
刪除複製計畫	17
編輯時間表	17

將NetApp Disaster Recovery與 Amazon EVS 結合使用

使用 Amazon Elastic VMware Service 和Amazon FSx for NetApp ONTAP實作NetApp Disaster Recovery

客戶越來越依賴虛擬化基礎架構來處理生產運算工作負載，例如基於 VMware vSphere 的工作負載。由於這些虛擬機器 (VM) 對業務變得越來越重要，客戶需要保護這些 VM 免受與實體運算資源相同類型的災難的影響。目前提供的災難復原 (DR) 解決方案複雜、昂貴且資源密集。NetApp是用於虛擬化基礎架構的最大儲存供應商，它有既得利益確保其客戶的虛擬機器受到保護，就像我們保護任何類型的ONTAP儲存託管資料一樣。為了實現這一目標，NetApp創建了NetApp Disaster Recovery服務。

任何 DR 解決方案面臨的主要挑戰之一是管理購買、配置和維護額外運算、網路和儲存資源的增量成本，以提供 DR 複製和復原基礎架構。保護關鍵內部虛擬資源的一個熱門選擇是使用雲端託管虛擬資源作為 DR 複製和復原基礎架構。亞馬遜就是此類解決方案的一個例子，它可以提供與NetApp ONTAP託管 VM 基礎架構相容的經濟高效的資源。

亞馬遜推出了 Amazon Elastic VMware Service (Amazon EVS)，可在您的虛擬私有雲 (VPC) 中支援 VMware Cloud Foundation。Amazon EVS 提供 AWS 的彈性和效能以及熟悉的 VMware 軟體和工具，使 Amazon EVS vCenters 能夠作為本地虛擬化基礎架構的擴展進行整合。

雖然 Amazon EVS 附帶了儲存資源，但對於儲存工作負載繁重的組織來說，使用本機儲存可能會降低其效率。在這些情況下，將 Amazon EVS 與Amazon FSx for NetApp ONTAP儲存 (Amazon FSxN) 結合使用可以提供更靈活的儲存解決方案。此外，當您在本機上使用NetApp ONTAP儲存解決方案來託管您的 VMware 基礎架構時，使用具有 FSx for ONTAP 的Amazon EVS 意味著您可以在本機和雲端託管基礎架構之間獲得一流的資料互通性和保護功能。

有關Amazon FSx for NetApp ONTAP 的信息，請參閱 ["Amazon FSx for NetApp ONTAP入門"](#)。

使用 Amazon EVS 和 Amazon FS for NetApp ONTAP 的NetApp Disaster Recovery解決方案概述

NetApp Disaster Recovery是託管在NetApp Console軟體即服務環境中的增值服務，它依賴核心NetApp Console架構。控制台內用於 VMware 保護的 DR 服務由幾個主要元件組成。

有關NetApp Disaster Recovery解決方案的完整概述，請參閱["了解NetApp Disaster Recovery"](#)。

如果您想要將本機 VMware 託管的虛擬機器保護到 Amazon AWS，請使用該服務透過Amazon FSx for NetApp ONTAP儲存託管資料儲存備份至 Amazon EVS。

下圖顯示了該服務如何使用 Amazon EVS 保護您的虛擬機器。

使用 Amazon EVS 和 FSx for ONTAP進行NetApp Disaster Recovery概述[使用 Amazon EVS 和 FSx for ONTAP進行NetApp Disaster Recovery概述]

1. Amazon EVS 部署在您的帳戶中的單一可用區 (AZ) 配置中以及您的虛擬私有雲 (VPC) 內。
2. FSx for ONTAP檔案系統與 Amazon EVS 部署在相同 AZ 中。檔案系統透過彈性網路介面 (ENI)、VPC 對等連接或 Amazon Transit 閘道直接連接到 Amazon EVS。
3. NetApp Console代理程式已安裝在您的 VPC 中。NetApp Console代理程式託管多個資料管理服務（稱為代理），包括管理本機實體資料中心和 Amazon AWS 託管資源上的 VMware 基礎架構的 DR 的NetApp Disaster Recovery代理程式。
4. NetApp Disaster Recovery代理程式與NetApp Console雲端託管服務安全性通訊以接收任務並將這些任務分發到適當的內部部署和 AWS 託管的 vCenter 和ONTAP儲存實例。
5. 您可以使用NetApp Console雲端託管 UI 控制台建立複製計劃，指示應保護的虛擬機器、應保護這些虛擬機器的頻率，以及在從內部網站發生故障轉移時重新啟動這些虛擬機器所需執行的程序。
6. 複製計畫決定哪些 vCenter 資料儲存庫託管受保護的虛擬機器以及託管這些資料儲存庫的ONTAP磁碟區。如果 FSx for ONTAP叢集上尚不存在磁碟區，NetApp Disaster Recovery會自動建立它們。
7. 為每個已識別的來源ONTAP磁碟區與每個目標 FSx for ONTAP託管ONTAP磁碟區建立SnapMirror關係，並根據複製計畫中使用者提供的 RPO 建立複製計畫。
8. 如果主站點發生故障，管理員會在NetApp Console內啟動手動故障轉移程序，並選擇備份作為還原點。
9. NetApp Disaster Recovery代理程式啟動 FSx for ONTAP所託管的資料保護磁碟區。
10. 該代理程式向 Amazon EVS vCenter 註冊每個已啟動的 FSx for ONTAP卷，向 Amazon EVS vCenter 註冊每個受保護的虛擬機，並根據複製計畫中包含的預定義規則啟動每個虛擬機。

安裝用於NetApp Disaster Recovery的NetApp Console代理

NetApp Console 代理程式可讓您將 NetApp Console 部署連接到基礎架構，從而安全地協調跨 AWS、Azure、Google Cloud 或內部部署環境的解決方案。Console 代理程式會執行 NetApp Console 管理資料基礎架構所需的操作。Console 代理程式會持續輪詢 NetApp Disaster Recovery 軟體即服務層，以取得所需的任何操作。

對於 NetApp Disaster Recovery，執行的操作會利用各自服務的原生 API 來協調 VMware vCenter 叢集和 ONTAP 儲存實例，從而為在內部部署位置執行的正式作業 VM 提供保護。雖然 Console 代理程式可以安裝在任何網路位置，但建議您將 Console 代理程式安裝在 NetApp Disaster Recovery 的災難復原站台。安裝在 DR 站台可確保在主站台發生故障時，NetApp Console UI 仍能保持與 Console 代理程式的連線，並能協調該 DR 站台內的復原程序。

安裝

- 若要使用 Disaster Recovery，請以標準模式安裝 Console 代理程式。若要深入瞭解 Console 代理程式安裝類型，請造訪 ["瞭解 NetApp Console 部署模式"](#)。

Console 代理程式的特定安裝步驟取決於您的部署類型。如需詳細資訊、請參閱 ["了解控制台代理"](#)。



使用 Amazon AWS 安裝 Console 代理程式最簡單的方法是使用 AWS Marketplace。有關使用 AWS Marketplace 安裝 Console 代理程式的詳細資訊，請參閱 ["從 AWS Marketplace 建立 Console 代理程式"](#)。

為 Amazon EVS 配置 NetApp Disaster Recovery

為 Amazon EVS 配置 NetApp Disaster Recovery 概述

安裝 NetApp Console 代理程式後，您需要將參與災難復原過程的所有 ONTAP 儲存和 VMware vCenter 資源與 NetApp Disaster Recovery。

- ["Amazon EVS 與 NetApp Disaster Recovery 的先決條件"](#)
- ["將 ONTAP 儲存陣列新增至 NetApp Disaster Recovery"](#)
- ["為 Amazon EVS 啟用 NetApp Disaster Recovery"](#)
- ["將 vCenter 站點新增至 NetApp Disaster Recovery"](#)
- ["將 vCenter 叢集新增至 NetApp Disaster Recovery"](#)

Amazon EVS 與 NetApp Disaster Recovery 的先決條件

請確保您已審查並滿足配置 Amazon EVS 與 NetApp Disaster Recovery 所需的要求。

先決條件

- 檢閱 ["Disaster Recovery 的一般前提條件"](#)。
- 建立 vCenter 使用者帳戶，該帳戶具有 NetApp Disaster Recovery 所需的特定 VMware 權限，以執行必要的操作。



建議您不要使用預設的「administrator@vsphere.com」管理員帳戶。相反地，您應該在所有將參與災難復原程序的 vCenter 叢集上建立一個 NetApp Disaster Recovery 專用的使用者帳戶。如需所需特定權限清單，請參閱["NetApp Disaster Recovery 所需的 vCenter 權限"](#)。

- 確保所有將託管受 Disaster Recovery 保護的 VM 的 vCenter 資料存放區都位於 NetApp ONTAP 儲存資源上。

Disaster Recovery 在使用 Amazon FSx for NetApp ONTAP 時支援 iSCSI 上的 NFS 和 VMFS（而非 FC）。儘管 Disaster Recovery 支援 FC，但 Amazon FSx for NetApp ONTAP 並不支援。

- 請確保您的 Amazon EVS vCenter 已連線至 Amazon FSx for NetApp ONTAP 儲存叢集。
- 確保所有受保護的 VM 都已安裝 VMware Tools。
- 請確保您的本地網路使用 Amazon 認可的連線方式連接到您的 AWS VPC 網路。建議您使用 AWS Direct Connect、AWS Private Link 或 AWS Site-to-Site VPN。
- 審查並確保符合 EVS 與 Disaster Recovery 的連線和連接埠要求：

來源	目的地	連接埠	詳細資料
Amazon FSxN	內部部署 ONTAP	TCP 11104、11105 、ICMP	SnapMirror
內部部署 ONTAP	Amazon FSxN	TCP 11104、11105 、ICMP	SnapMirror
NetApp Console 代理	內部部署 ONTAP	僅限 TCP 443、ICMP	API 呼叫

來源	目的地	連接埠	詳細資料
NetApp Console 代理	Amazon FSxN	TCP 441、僅限 ICMP	API 呼叫
NetApp Console 代理	vCenter（本地部署、EVS）、ESXi 主機（本地部署、EVS）	443	API 呼叫、指令碼執行

使用**NetApp Disaster Recovery**功能將本機陣列新增至適用於 **Amazon EVS** 的**NetApp Console**系統

在使用NetApp Disaster Recovery之前，您必須將內部部署和雲端託管儲存實例新增至NetApp Console系統。

您需要執行以下操作：

- 將內部部署陣列新增至您的NetApp Console系統。
- 將Amazon FSx for NetApp ONTAP（FSx for ONTAP）實例新增至您的NetApp Console系統。

將本機儲存陣列新增至**NetApp Console**系統

將本機ONTAP儲存資源新增至您的NetApp Console系統。

1. 在NetApp Console系統頁面中，選擇「新增系統」。

[新增系統]

2. 在新增系統頁面中，選擇*On-Premises*卡。

[新增系統映像]

3. 在 On-Premises ONTAP卡上選擇 發現。

[新增系統映像]

4. 在發現集群頁面上，輸入以下資訊：

- a. ONTAP陣列叢集管理埠的 IP 位址
- b. 管理員使用者名稱
- c. 管理者密碼

5. 選擇頁面底部的“發現”。

[新增系統映像]

6. 對將託管 vCenter 資料儲存區的每個ONTAP陣列重複步驟 1-5。

將**Amazon FSx for NetApp ONTAP**儲存實例新增至**NetApp Console**系統

接下來，將Amazon FSx for NetApp ONTAP儲存資源新增至您的NetApp Console系統。

1. 在NetApp Console系統頁面中，選擇「新增系統」。

[新增系統映像]

2. 從新增系統頁面中，選擇*Amazon Web Services*卡。

[新增系統映像]

3. 選擇Amazon FSx for ONTAP卡上的 **Discover Existing** 連結。

[新增系統映像]

4. 選擇託管 FSx for ONTAP實例的憑證和 AWS 區域。

5. 選擇一個或多個要新增的 FSx for ONTAP檔案系統。

6. 選擇頁面底部的“發現”。

[新增系統映像]

7. 對於將託管 vCenter 資料儲存區的每個 FSx for ONTAP執行個體重複步驟 1-6。

將NetApp Disaster Recovery服務新增至您的 Amazon EVS NetApp Console帳戶

NetApp Disaster Recovery是一種授權產品，必須先購買才能使用。有多種類型的許可證，您可以透過多種方式購買許可證。許可證授權您在特定時間內保護特定數量的資料。

有關NetApp Disaster Recovery許可證的更多信息，請參閱["設定NetApp Disaster Recovery許可"](#)。

許可證類型

許可證主要有兩種類型：

- NetApp提供["30天試用許可證"](#)您可以使用它來評估使用ONTAP和 VMware 資源的NetApp Disaster Recovery。此許可證提供 30 天的使用期限，不受限制地使用受保護的容量。
- 如果您希望在 30 天試用期之後獲得 DR 保護，請購買生產許可證。您可以透過任何 NetApp 雲端合作夥伴的市場購買此許可證，但對於本指南，我們建議您使用 Amazon AWS Marketplace 購買NetApp Disaster Recovery的市場授權。要了解有關透過 Amazon Marketplace 購買許可證的更多信息，請參閱["透過 AWS Marketplace 訂閱"](#)。

確定災難復原容量需求

在購買許可證之前，您應該了解需要保護多少ONTAP儲存容量。使用NetApp ONTAP儲存的優點之一是NetApp儲存資料的效率很高。ONTAP磁碟區中儲存的所有資料（例如託管虛擬機器的 VMware 資料儲存區）都是以高效率的方式儲存的資料。ONTAP在將資料寫入實體儲存時預設採用三種儲存效率：壓縮、重複資料刪除和壓縮。最終結果是儲存效率在 1.5:1 到 4:1 之間，具體取決於所儲存的資料類型。事實上，NetApp提供了["儲存效率保證"](#)對於某些工作負載。

這對您有利，因為在應用所有ONTAP儲存效率之後，NetApp Disaster Recovery會計算授權容量。例如，假設您在 vCenter 中設定了一個 100 TB (TiB) NFS 資料儲存區來託管您想要使用該服務保護的 100 台虛擬機器。此外，假設當資料寫入ONTAP磁碟區時，自動應用的儲存效率技術會導致這些虛擬機器僅消耗 33TiB（3：1 的儲存效率）。NetApp Disaster Recovery只需要 33TiB 的許可，而不是 100TiB。與其他 DR 解決方案相比，這對

於您的 DR 解決方案的整體擁有成本來說是一個非常大的好處。

步驟

1. 若要確定託管要保護的 VMware 資料儲存庫的每個磁碟區上消耗的資料量，請透過對每個磁碟區執行 ONTAP CLI 命令來確定磁碟容量消耗：`volume show-space -volume < volume name > -vserver < SVM name >`。

例如：

```
cluster1::> volume show-space
Vserver : vm-nfs-ds1
Volume  : vol0
Feature                                Used      Used%
-----
User Data                             163.4MB    3%
Filesystem Metadata                    172KB     0%
Inodes                                2.93MB    0%
Snapshot Reserve                       292.9MB    5%
Total Metadata                         185KB     0%
Total Used                             459.4MB    8%
Total Physical Used                    166.4MB    3%
```

2. 注意每個磁碟區的“總物理使用量”值。這是 NetApp Disaster Recovery 需要保護的資料量，也是您將用來決定需要許可多少容量的值。

在 NetApp Disaster Recovery 中為 Amazon EVS 新增站點

在保護虛擬機器基礎架構之前，請先確定哪些 VMware vCenter 叢集託管著要保護的虛擬機器以及這些 vCenter 位於何處。第一步是建立一個網站來代表來源資料中心和目標資料中心。站點是故障域或恢復域。

您需要建立以下內容：

- 代表生產 vCenter 叢集所在的每個生產資料中心的站點
- Amazon FSx for NetApp ONTAP 站點

建立本地站點

建立生產 vCenter 網站。

步驟

1. 從 NetApp Console 左側導覽列中，選擇 保護 > 災難復原。
2. 從 NetApp Disaster Recovery 中的任何頁面中，選擇「網站」選項。

[網站選項]

3. 從網站選項中，選擇*新增*。

[在網站選項中新增選項]

4. 在新增網站對話方塊中，提供網站名稱。
5. 選擇“On-prem”作為位置。
6. 選擇“新增”。

[建立網站對話框]

如果您有其他生產 vCenter 站點，則可以使用相同的步驟新增它們。

創建亞馬遜雲端站點

使用Amazon FSx for NetApp ONTAP儲存為 Amazon EVS 建立 DR 站點。

1. 從NetApp Disaster Recovery中的任何頁面中，選擇「網站」選項。

[網站選項]

2. 從網站選項中，選擇*新增*。

[在網站頁面上新增選項]

3. 在新增網站對話方塊中，提供網站名稱。
4. 選擇“AWS-EVS”作為位置。
5. 選擇“新增”。

[新增對話框]

結果

現在您已經建立了一個生產（來源）網站和一個 DR（目標）網站。

在NetApp Disaster Recovery中新增本機和 Amazon EVS vCenter 叢集

建立網站後，現在可以將 vCenter 叢集新增至NetApp Disaster Recovery中的每個網站。當我們建立每個網站時，我們都會指出每種網站的類型。這會告訴NetApp Disaster Recovery每種網站類型中託管的 vCenter 需要什麼類型的存取。Amazon EVS 的優勢之一是 Amazon EVS vCenter 和本機 vCenter 之間沒有真正的區別。兩者都需要相同的連線和身份驗證資訊。

在每個站點新增 vCenter 的步驟

1. 從「網站」選項中，選擇所需網站的「新增 vCenter」。

[新增 vCenter 選項]

2. 在新增 vCenter 伺服器對話方塊中，選擇或提供以下資訊：

- a. 託管在您的 AWS VPC 內的NetApp Console代理程式。
 - b. 要新增的 vCenter 的 IP 位址或 FQDN。
 - c. 如果不同，請將連接埠值變更為 vCenter 叢集管理器使用的 TCP 連接埠。
 - d. 先前建立的帳戶的 vCenter 使用者名， NetApp Disaster Recovery將使用該使用者名稱來管理 vCenter。
 - e. 所提供使用者名稱的 vCenter 密碼。
 - f. 如果您的公司使用外部憑證授權單位 (CA) 或 vCenter Endpoint 憑證儲存空間來存取您的 vCenter，請取消選取 使用自簽名憑證 複選框。否則，請保留此方塊的選取狀態。
3. 選擇“新增”。

[新增 vCenter 對話框]

為 Amazon EVS 建立複製計劃

在NetApp Disaster Recovery概述中建立複製計劃

在本機網站上有要保護的 vCenter 並且您有一個配置為使用Amazon FSx for NetApp ONTAP 的Amazon EVS 站點（可將其用作 DR 目標）後，您可以建立複製計劃 (RP) 來保護本地站點內 vCenter 叢集上託管的任何虛擬機器集。

若要開始複製計劃創建過程：

1. 從任何NetApp Disaster Recovery畫面中，選擇「複製計畫」選項。

[複製計劃選項]

2. 在複製計劃頁面中，選擇*新增*。

[複製計劃畫面]

這將開啟建立複製計劃精靈。

繼續["建立複製計劃精靈步驟 1"](#)。

建立複製計畫：步驟 1 - 在NetApp Disaster Recovery中選擇 vCenter

首先，使用NetApp Disaster Recovery，提供複製計劃名稱並選擇複製的來源和目標 vCenter。

1. 為複製計劃輸入一個唯一的名稱。

複製計劃名稱僅允許使用字母數字字元和底線 (_)。

2. 選擇來源 vCenter 叢集。
3. 選擇目標 vCenter 叢集。

4. 選擇“下一步”。

[建立複製計劃，選擇 vCenter]

繼續["建立複製計劃精靈步驟 2"](#)。

建立複製計畫：步驟 2 - 在NetApp Disaster Recovery中選擇虛擬機器資源

選擇要使用NetApp Disaster Recovery保護的虛擬機器。

有多種方法可以選擇要保護的虛擬機器：

- 選擇單一虛擬機器：按一下「虛擬機器」按鈕，您可以選擇要保護的單一虛擬機器。當您選擇每個虛擬機器時，服務會將其新增至位於螢幕右側的預設資源群組。
- 選擇先前建立的資源組：您可以使用NetApp Disaster Recovery選單中的資源組選項預先建立自訂資源組。這不是必需的，因為您可以使用其他兩種方法來建立資源組作為複製計劃過程的一部分。有關詳細信息，請參閱["建立複製計劃"](#)。
- 選擇整個 vCenter 資料儲存：如果您有大量虛擬機器需要使用此複製計畫保護，則選擇單一虛擬機器可能效率不高。由於NetApp Disaster Recovery使用基於磁碟區的SnapMirror複製來保護虛擬機，因此駐留在資料儲存區上的所有虛擬機都將作為磁碟區的一部分進行複製。大多數情況下，您應該使用NetApp Disaster Recovery保護並重新啟動資料儲存區上的所有虛擬機器。使用此選項可告知服務將選定資料儲存體上託管的任何虛擬機器新增至受保護虛擬機器清單中。

對於本指導說明，我們選擇整個 vCenter 資料儲存。

造訪此頁面的步驟

1. 從「複製計畫」頁面繼續到「應用程式」部分。
2. 查看開啟的「應用程式」頁面中的資訊。

[複製計畫，應用程式頁面]

選擇資料儲存區的步驟：

1. 選擇*資料儲存*。
2. 選取您想要保護的每個資料儲存旁邊的複選框。
3. （可選）透過選擇資源組名稱旁邊的鉛筆圖標，將資源組重新命名為適當的名稱。
4. 選擇“下一步”。

繼續["建立複製計劃精靈步驟3"](#)。

建立複製計畫：步驟 3 - 在NetApp Disaster Recovery中對應資源

在您取得要使用NetApp Disaster Recovery保護的虛擬機器清單後，請提供故障轉移期間要使用的故障轉移對映和虛擬機器設定資訊。

您需要映射四種主要類型的信息：

- 計算資源
- 虛擬網路
- 虛擬機器重新配置
- 資料儲存映射

每個虛擬機器都需要前三種類型的資訊。每個託管要保護的虛擬機器的資料儲存都需要進行資料儲存對應。

- 帶有警告圖示 ([25.25]) 要求您提供地圖資訊。
- 標有複選圖示 ([25.25]) 已被映射或具有預設映射。檢查它們以確保當前配置符合您的要求。

造訪此頁面的步驟

1. 從「複製計畫」頁面繼續到「資源映射」部分。
2. 查看開啟的「資源映射」頁面上的資訊。

[建立複製計畫，資源映射頁面]

3. 若要開啟所需的每個映射類別，請選擇該部分旁邊的向下箭頭 (v) 。

計算資源映射

由於一個網站可以託管多個虛擬資料中心和多個 vCenter 集群，因此您需要確定在發生故障轉移時在哪個 vCenter 集群上復原虛擬機器。

映射計算資源的步驟

1. 從位於 DR 站點的資料中心清單中選擇虛擬資料中心。
2. 從所選虛擬資料中心內的叢集清單中選擇用於託管資料儲存區和虛擬機器的叢集。
3. (可選) 選擇目標叢集中的目標主機。

此步驟不是必要的，因為 NetApp Disaster Recovery 會選擇在 vCenter 中新增至叢集的第一個主機。此時，虛擬機器要么繼續在該 ESXi 主機上運行，要么 VMware DRS 根據配置的 DRS 規則根據需要將虛擬機器移至不同的 ESXi 主機。

4. (可選) 提供用於放置 VM 註冊的頂級 vCenter 資料夾的名稱。

這是為了滿足您的組織需求，並不是必要的。

[建立複製計畫、計算資源]

映射虛擬網路資源

每個虛擬機器可以有一個或多個虛擬網路卡連接到 vCenter 網路基礎架構內的虛擬網路。為了確保每個虛擬機器在 DR 站點重新啟動時都能正確連接到所需的網路，請確定哪些 DR 站點虛擬網路可連接這些虛擬機器。透過將本地站點中的每個虛擬網路對應到 DR 站點上的關聯網路來實現此目的。

選擇每個來源虛擬網路要對應到哪個目標虛擬網路

1. 從下拉清單中選擇目標段。
2. 對列出的每個來源虛擬網路重複上一步驟。

[建立複製計劃、網路資源]

定義故障轉移期間虛擬機器重新配置的選項

每個虛擬機器可能都需要修改才能在 DR vCenter 站點中正常運作。虛擬機器部分使您能夠提供必要的變更。

預設情況下，NetApp Disaster Recovery 對每個虛擬機器使用與來源本機站點相同的設定。這假設虛擬機器將使用相同的 IP 位址、虛擬 CPU 和虛擬 DRAM 配置。

網路重新配置

支援的 IP 位址類型為靜態和 DHCP。對於靜態 IP 位址，您有下列目標 IP 設定：

- 與來源相同：顧名思義，該服務在目標虛擬機器上使用的 IP 位址與來源站點虛擬機器上使用的 IP 位址相同。這要求您為上一個步驟中映射的虛擬網路配置相同的子網路設定。
- 與來源不同：此服務為每個 VM 提供了一組 IP 位址字段，這些字段必須針對目標虛擬網路上使用的適當子網路進行配置，您在上一節中已對應該子網路。對於每個虛擬機，您必須提供 IP 位址、子網路遮罩、DNS 和預設閘道值。或者，對所有虛擬機器使用相同的子網路遮罩、DNS 和網關設置，以簡化所有虛擬機器連接到相同子網路時的流程。
- 子網路對映：此選項會根據目標虛擬網路的 CIDR 設定重新配置每個 VM 的 IP 位址。若要使用此功能，請確保每個 vCenter 的虛擬網路在服務內都有定義的 CIDR 設置，如「站點」頁面中的 vCenter 資訊中所更改的。

配置子網路後，子網路對來源和目標 VM 配置使用相同的 IP 位址單元元件，但根據提供的 CIDR 資訊取代 IP 位址的子網路元件。此功能還要求來源虛擬網路和目標虛擬網路具有相同的 IP 位址類別（/xx CIDR 的組成部分）。這可確保目標網站有足夠的 IP 位址來託管所有受保護的虛擬機器。

對於此 EVS 設置，我們假設來源和目標 IP 配置相同，不需要任何額外的重新配置。

變更網路設定重新配置

1. 選擇故障轉移虛擬機器使用的 IP 位址類型。
2. （可選）透過提供可選的前綴和後綴值為重新啟動的虛擬機器提供虛擬機器重命名方案。

[建立複製計劃、網路資源]

VM 運算資源重新配置

重新配置虛擬機器運算資源有多種選擇。NetApp Disaster Recovery 支援更改虛擬 CPU 的數量、虛擬 DRAM 的數量和 VM 名稱。

指定任何 VM 配置更改

1. （可選）修改每個虛擬機器應使用的虛擬 CPU 數量。如果您的 DR vCenter 叢集主機沒有來源 vCenter 叢集那麼多的 CPU 核心，則可能需要這樣做。
2. （可選）修改每個虛擬機器應使用的虛擬 DRAM 數量。如果您的 DR vCenter 叢集主機沒有來源 vCenter 叢集主機那麼多的實體 DRAM，則可能需要這樣做。

[建立複製計劃、虛擬機器資源]

啟動順序

NetApp Disaster Recovery支援根據啟動順序欄位有序重啟虛擬機器。啟動順序欄位指示每個資源組中的虛擬機器如何啟動。啟動順序欄位中具有相同值的虛擬機器將會並行啟動。

修改啟動順序設定

1. (可選) 修改您希望重新啟動虛擬機器的順序。此欄位可採用任意數值。NetApp Disaster Recovery嘗試並行重新啟動具有相同數值的虛擬機器。
2. (可選) 提供每次 VM 重新啟動之間的延遲。該時間是在該虛擬機重啟完成後、具有下一個更高啟動順序號的虛擬機之前註入的。這個數字以分鐘為單位。

[建立複製計畫、啟動順序]

自訂客戶作業系統操作

NetApp Disaster Recovery支援為每個虛擬機器執行一些客戶作業系統操作：

- NetApp Disaster Recovery可以為執行 Oracle 資料庫和 Microsoft SQL Server 資料庫的虛擬機器進行應用程式一致的備份。
- NetApp Disaster Recovery可以執行適合每個虛擬機器的客戶作業系統的自訂腳本。執行此類腳本需要客戶作業系統可接受的使用者憑證，且該憑證具有足夠的權限來執行腳本中列出的操作。

修改每個虛擬機器的自訂客戶作業系統操作

1. (可選) 如果虛擬機器託管 Oracle 或 SQL Server 資料庫，請選取「建立應用程式一致副本」複選框。
2. (可選) 若要在啟動過程中在客戶作業系統中採取自訂操作，請為任何虛擬機器上傳腳本。若要在所有虛擬機器中執行單一腳本，請使用反白的核取方塊並填寫欄位。
3. 某些配置變更需要具有足夠權限的使用者憑證才能執行操作。在下列情況下提供憑證：
 - 客戶作業系統將在虛擬機器內執行腳本。
 - 需要執行應用程式一致的快照。

[建立複製計畫、自訂客戶作業系統操作]

地圖資料存儲

建立複製計畫的最後一步是確定ONTAP應如何保護資料儲存庫。這些設定定義了複製計畫復原點目標 (RPO)、應維護多少個備份以及在何處複製每個 vCenter 資料儲存區的託管ONTAP磁碟區。

預設情況下，NetApp Disaster Recovery管理自己的快照複製計畫；但是，您可以選擇指定使用現有的SnapMirror複製策略計畫來保護資料儲存區。

此外，您還可以選擇自訂要使用的資料 LIF（邏輯介面）和匯出策略。如果您不提供這些設置，NetApp Disaster Recovery將使用與對應協定（NFS、iSCSI 或 FC）關聯的所有資料 LIF，並使用 NFS 磁碟區的預設匯出策略。

配置資料儲存（卷）映射

1. (可選) 決定是否要使用現有的ONTAP SnapMirror複製計畫或讓NetApp Disaster Recovery管理虛擬機器的保護（預設）。
2. 提供服務開始備份的起點。

3. 指定服務進行備份並將其複製到 DR 目標Amazon FSx for NetApp ONTAP叢集的頻率。
4. 指定應保留多少個歷史備份。該服務在來源和目標儲存叢集上維護相同數量的備份。
5. （可選）為每個磁碟區選擇一個預設邏輯介面（資料 LIF）。如果未選擇任何內容，則會設定目標 SVM 中支援磁碟區存取協定的所有資料 LIF。
6. （可選）為任何 NFS 磁碟區選擇匯出策略。如果未選擇，則使用預設匯出策略

[建立複製計劃、資料儲存映射]

繼續["建立複製計劃精靈步驟4"](#)。

建立複製計畫：步驟 4 - 驗證NetApp Disaster Recovery中的設置

在NetApp Disaster Recovery中加入複製計畫資訊後，請驗證您輸入的資訊是否正確。

步驟

1. 在啟動複製計劃之前，選擇“儲存”來檢查您的設定。

您可以選擇每個選項卡來查看設置，並透過選擇鉛筆圖示在任何選項卡上進行更改。

複製計劃設定審查[複製計劃設定審查]

2. 當您確認所有設定正確無誤後，選擇螢幕底部的*新增計畫*。

繼續["驗證複製計劃"](#)。

驗證NetApp Disaster Recovery中一切正常

在NetApp Disaster Recovery中新增複製計畫後，您將返回「複製計畫」頁面，您可以在其中查看複製計畫及其狀態。您應該驗證複製計劃是否處於*健康*狀態。如果不是，您應該檢查複製計劃的狀態並在繼續之前糾正任何問題。

圖：複製計劃頁面[複製計劃頁面]

NetApp Disaster Recovery執行一系列測試，以驗證所有元件（ONTAP叢集、vCenter 叢集和虛擬機器）是否可存取且處於正確狀態，以便服務保護虛擬機器。這被稱為合規性檢查，並且會定期進行。

在複製計劃頁面中，您可以看到以下資訊：

- 上次合規性檢查的狀態
- 複製計劃的複製狀態
- 受保護（來源）網站的名稱
- 複製計劃保護的資源組列表
- 故障轉移（目標）站點的名稱

使用NetApp Disaster Recovery執行複製計畫操作

使用NetApp Disaster Recovery與 Amazon EVS 和Amazon FSx for NetApp ONTAP執行以下操作：故障轉移、測試故障轉移、刷新資源、遷移、立即拍攝快照、停用/啟用複製計畫、清理舊快照、協調快照、刪除複製計畫和編輯計畫。

故障轉移

您可能需要執行的主要操作是您希望永遠不會發生的操作：在生產本地站點發生災難性故障時故障轉移到 DR（目標）資料中心。

故障轉移是一個手動啟動的過程。

存取故障轉移操作的步驟

1. 從NetApp Console左側導覽列中，選擇 保護 > 災難復原。
2. 從NetApp Disaster Recovery選單中，選擇 複製計畫。

執行故障轉移的步驟

1. 在複製計畫頁面中，選擇複製計畫的操作選項[操作選單的水平點]。
2. 選擇*故障轉移*。

[故障轉移選單選項]

3. 如果無法存取生產（受保護）站點，請選擇先前建立的快照作為復原映像。為此，請選擇*選擇*。
4. 選擇要用於復原的備份。
5. （可選）選擇是否希望NetApp Disaster Recovery強制執行故障轉移過程，而不管複製計畫的狀態如何。這只能作為最後的手段。
6. （可選）選擇是否希望NetApp Disaster Recovery在生產站點恢復後自動建立反向保護關係。
7. 輸入單字“Failover”以確認您是否要繼續。
8. 選擇“故障轉移”。

[故障轉移對話框]

測試故障轉移

測試故障轉移與故障轉移類似，但有兩個差異。

- 生產站點仍然處於活動狀態，所有虛擬機器仍在按預期運作。
- NetApp Disaster Recovery對生產虛擬機器的保護仍在繼續。

這是透過在目標站點使用本機ONTAP FlexClone磁碟區來實現的。要了解有關測試故障轉移的更多信息，請參閱[將應用程式故障轉移到遠端站點 | NetApp文檔](#)。

執行測試故障轉移的步驟與執行實際故障轉移的步驟相同，只是您使用複製計畫的上下文功能表上的測試故障轉移操作。

步驟

1. 選擇複製計劃的操作選項[操作選單的水平點]。
2. 從選單中選擇*測試故障轉移*。

[測試故障轉移選單選項]

3. 決定是否要取得生產環境的最新狀態（立即拍攝快照）或使用先前建立的複製計畫備份（選擇）
4. 如果您選擇了先前建立的備份，則選擇要用於復原的備份。
5. 輸入“測試故障轉移”一詞來驗證您是否要繼續。
6. 選擇*測試故障轉移*。

[測試故障轉移對話框]

運行合規性檢查

預設情況下，合規性檢查每三小時運行一次。您可能隨時想要手動執行合規性檢查。

步驟

1. 選擇“操作”選項[NetApp Disaster Recovery服務中的操作選單圖標]複製計劃旁。
2. 從複製計畫的操作選單中選擇*執行合規性檢查*選項：

[運行合規性檢查選單選項]

3. 若要變更NetApp Disaster Recovery自動執行合規性檢查的頻率，請從複製計畫的操作選單中選擇「編輯計畫」選項。

刷新資源

每次對虛擬基礎架構進行變更（例如新增或刪除虛擬機器、新增或刪除資料儲存區或在資料儲存區之間移動虛擬機器）時，都需要在NetApp Disaster Recovery服務中對受影響的 vCenter 叢集執行刷新。該服務預設每 24 小時自動執行一次此操作，但手動刷新可確保最新的虛擬基礎設施資訊可用並考慮到 DR 保護。

有兩種情況需要刷新：

- vCenter 刷新：每當在 vCenter 群集中新增、刪除或移出虛擬機器時，執行 vCenter 刷新：
- 複製計劃刷新：每當虛擬機器在同一來源 vCenter 叢集中的資料儲存之間移動時，執行複製計劃刷新。

[刷新資源選單選項] | [evs-rp-menu-refresh-resources.png](#)

遷移

雖然NetApp Disaster Recovery主要用於災難復原用例，但它也可以將一組虛擬機器從來源站點一次性移至目標網站。這可能是為了協調遷移到雲端項目，也可能是為了避免災難——例如惡劣天氣、政治衝突或其他潛在的暫時災難性事件。

1. 選擇“操作”選項[NetApp Disaster Recovery服務中的操作選單圖標]複製計劃旁。
2. 若要將複製計畫中的虛擬機器移至目標 Amazon EVS 集群，請從複製計畫的操作選單中選擇「遷移」：

[遷移選單選項] | *evs-rp-menu-migrate.png*

3. 在「遷移」對話方塊中輸入資訊。

立即拍攝快照

您可以隨時立即拍攝複製計劃的快照。此快照包含在複製計劃的快照保留計數設定的NetApp Disaster Recovery考慮因素中。

1. 選擇“操作”選項[NetApp Disaster Recovery服務中的操作選單圖標]複製計劃旁。
2. 若要立即拍攝複製計畫資源的快照，請在複製計畫的操作選單上選擇*立即拍攝快照*：

[立即拍攝快照選單選項] | *evs-rp-menu-take-snapshot-now.png*

停用或啟用複製計劃

您可能需要暫時停止複製計劃來執行一些可能影響複製過程的操作或維護。該服務提供了停止和啟動複製的方法。

1. 若要暫時停止複製，請在複製計畫的操作選單上選擇*停用*。
2. 若要重新啟動複製，請在複製計畫的操作選單上選擇*啟用*。

當複製計劃處於活動狀態時，「啟用」指令將顯示為灰色。當複製計劃被停用時，「停用」指令將變灰。

[停用/啟用選單選項] | *evs-rp-menu-disable-enable.png*

清理舊快照

您可能想要清理保留在來源網站和目標網站上的舊快照。如果複製計劃的快照保留計數發生改變，就會發生這種情況。

1. 選擇“操作”選項[NetApp Disaster Recovery服務中的操作選單圖標]複製計劃旁。
2. 若要手動刪除這些舊快照，請從複製計畫的操作選單中選擇*清理舊快照*。

[清理舊快照選單選項] | *evs-rp-menu-cleanup-old-snapshots.png*

協調快照

由於本服務協調ONTAP磁碟區快照，因此ONTAP儲存管理員可以在服務不知情的情況下使用ONTAP系統管理員、ONTAP CLI 或ONTAP REST API 直接刪除快照。該服務每 24 小時自動刪除來源上不在目標叢集上的任何快照。但是，您可以根據需要執行此操作。此功能可讓您確保快照在所有網站上都是一致的。

1. 選擇“操作”選項[NetApp Disaster Recovery服務中的操作選單圖標]複製計劃旁。
2. 若要從來源叢集中刪除目標叢集上不存在的快照，請從複製計畫的操作選單中選擇*協調快照*。

[協調快照選單選項] | *evs-rp-menu-reconcile-snapshots.png*

刪除複製計劃

如果不再需要複製計劃，您可以將其刪除。

1. 選擇“操作”選項[NetApp Disaster Recovery服務中的操作選單圖標]複製計劃旁。
2. 若要刪除複製計劃，請從複製計劃的上下文功能表中選擇“刪除”。

[刪除選單選項] | *evs-rp-menu-delete.png*

編輯時間表

兩項操作會定期自動執行：測試故障轉移和合規性檢查。

1. 選擇“操作”選項[NetApp Disaster Recovery服務中的操作選單圖標]複製計劃旁。
2. 若要變更這兩個操作中的任一個的計劃，請選擇複製計劃的*編輯計劃*。

[編輯時間表選單選項] | *evs-rp-menu-edit-schedules.png*

更改合規性檢查間隔

預設情況下，每三小時執行一次合規性檢查。您可以將其變更為 30 分鐘到 24 小時之間的任意間隔。

若要變更此間隔，請變更「編輯計畫」對話方塊中的「頻率」欄位：

[合規性檢查時間表] | *evs-rp-edit-compliance-check-schedule.png*

安排自動測試故障轉移

預設情況下，測試故障轉移是手動執行的。您可以安排自動測試故障轉移，這有助於確保您的複製計劃按預期執行。要了解有關測試故障轉移過程的更多信息，請參閱["測試故障轉移過程"](#)。

安排測試故障轉移的步驟

1. 選擇“操作”選項[NetApp Disaster Recovery服務中的操作選單圖標]複製計劃旁。
2. 選擇*運行故障轉移*。
3. 選取*依計畫執行測試故障轉移*複選框。
4. （可選）檢查*使用按需快照進行計劃測試故障轉移*。
5. 在重複下拉式選單中選擇間隔類型。
6. 選擇何時執行測試故障轉移
 - a. 每週：選擇星期幾
 - b. 每月：選擇月份中的日期
7. 選擇執行測試故障轉移的時間
8. 選擇開始日期。
9. 決定是否希望服務自動清理測試環境，以及在清理過程開始之前希望測試環境運行多長時間。
10. 選擇*儲存*。

版權資訊

Copyright © 2026 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

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

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

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

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

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

商標資訊

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