



使用 **ANF** 和 **JetStream** 進行災難復原

NetApp public and hybrid cloud solutions

NetApp
August 18, 2025

目錄

使用 ANF 和 JetStream 進行災難復原	1
在本地資料中心安裝 JetStream DR	2
使用運行命令在 Azure VMware 解決方案私有雲中安裝 JetStream DR for AVS	6
執行故障轉移/故障回復	9
勒索軟體恢復	12

使用 ANF 和 JetStream 進行災難復原

災難復原到雲端是一種具有彈性且經濟高效的方法，可以保護工作負載免受網站中斷和資料損壞事件（例如勒索軟體）的影響。使用 VMware VAI/O 框架，可以將本機 VMware 工作負載複製到 Azure Blob 儲存體並進行恢復，從而實現最少或幾乎沒有資料遺失以及接近零的 RTO。

JetStream DR 可用於無縫恢復從本地複製到 AVS 以及特別是 Azure NetApp Files 的工作負載。它透過使用災難復原站點的最少資源和經濟高效的雲端儲存來實現經濟高效的災難復原。JetStream DR 透過 Azure Blob Storage 自動還原到 ANF 資料儲存。JetStream DR 根據網路映射將獨立的虛擬機器或相關虛擬機器群組還原到復原站點基礎架構中，並提供時間點復原以進行勒索軟體保護。

本文檔可協助您了解 JetStream DR 的操作原理及其主要組件。

解決方案部署概述

1. 在本地資料中心安裝 JetStream DR 軟體。
 - a. 從 Azure 市場 (ZIP) 下載 JetStream DR 軟體包，並在指定叢集中部署 JetStream DR MSA (OVA)。
 - b. 使用 I/O 過濾器包配置叢集（安裝 JetStream VIB）。
 - c. 在與 DR AVS 叢集相同的區域中設定 Azure Blob（Azure 儲存帳戶）。
 - d. 部署 DRVA 設備並分配複製日誌磁碟區（來自現有資料儲存或共用 iSCSI 儲存的 VMDK）。
 - e. 建立受保護的網域（相關 VM 群組）並指派 DRVA 和 Azure Blob 儲存體/ANF。
 - f. 開始保護。
2. 在 Azure VMware 解決方案私有雲中安裝 JetStream DR 軟體。
 - a. 使用運行命令安裝和設定 JetStream DR。
 - b. 新增相同的 Azure Blob 容器並使用掃描網域選項發現網域。
 - c. 部署所需的 DRVA 設備。
 - d. 使用可用的 vSAN 或 ANF 資料儲存建立複製日誌卷。
 - e. 導入受保護的網域並配置 RocVA（恢復 VA）以使用 ANF 資料儲存進行 VM 放置。
 - f. 選擇適當的故障轉移選項並開始對接近零 RTO 域或虛擬機器進行持續補水。
3. 在災難事件發生期間，觸發故障轉移到指定 AVS DR 站點中的 Azure NetApp Files 資料儲存。
4. 在受保護站點恢復後，呼叫故障回復到受保護站點。在開始之前，請確保滿足本 ["關聯"](#) 並執行 JetStream Software 提供的頻寬測試工具 (BWT) 來評估與 JetStream DR 軟體一起使用時 Azure Blob 儲存體及其複製頻寬的潛在效能。滿足先決條件（包括連接性）後，設定並訂閱 JetStream DR for AVS ["Azure 市場"](#)。下載軟體包後，繼續執行上面所述的安裝過程。

在規劃和啟動對大量虛擬機器（例如 100 多個）的保護時，請使用 JetStream DR 自動化工具包中的容量規劃工具 (CPT)。提供要保護的虛擬機器清單及其 RTO 和復原群組首選項，然後執行 CPT。

CPT 執行以下功能：

- 根據 RTO 將虛擬機器組合到保護域。
- 定義 DRVA 及其資源的最佳數量。
- 估計所需的複製頻寬。
- 識別複製日誌卷特徵（容量、頻寬等）。
- 估算所需的物件儲存容量等等。



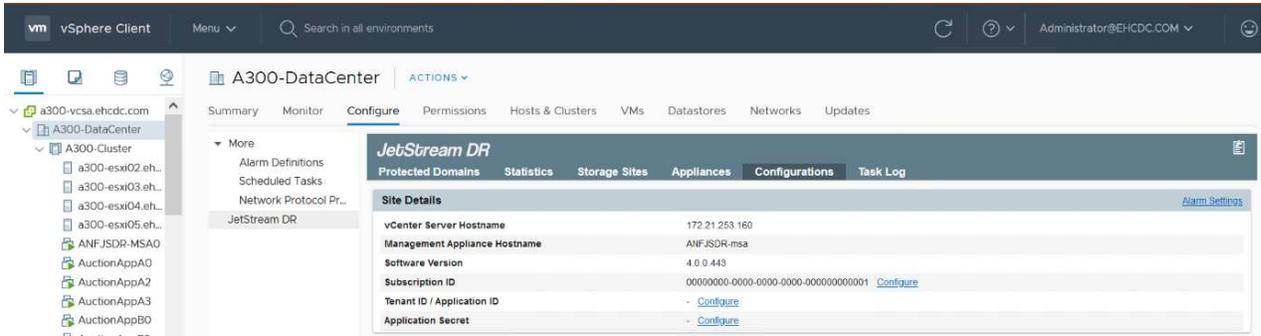
規定的域的數量和內容取決於各種 VM 特性，例如平均 IOPS、總容量、優先順序（定義故障轉移順序）、RTO 等。

在本地資料中心安裝 JetStream DR

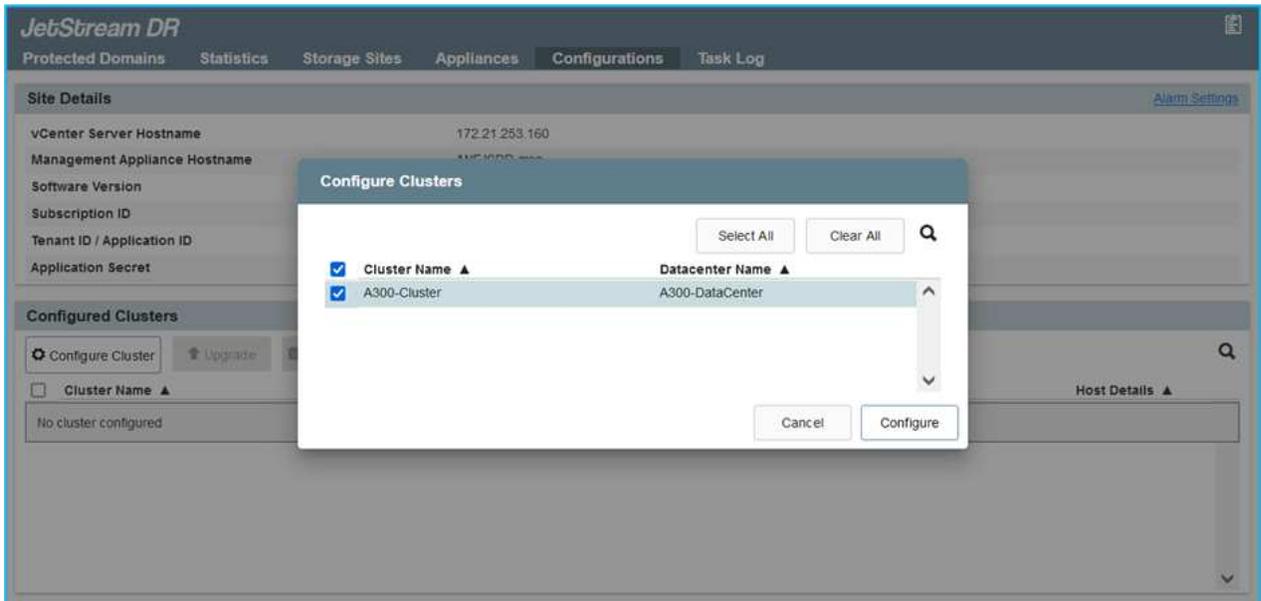
JetStream DR 軟體由三個主要元件組成：JetStream DR 管理伺服器虛擬裝置 (MSA)、DR 虛擬裝置 (DRVA) 和主機元件 (I/O 篩選器套件)。MSA 用於在運算叢集上安裝和設定主機元件，然後管理 JetStream DR 軟體。以下列表提供了安裝過程的高級描述：

如何為本地安裝 JetStream DR

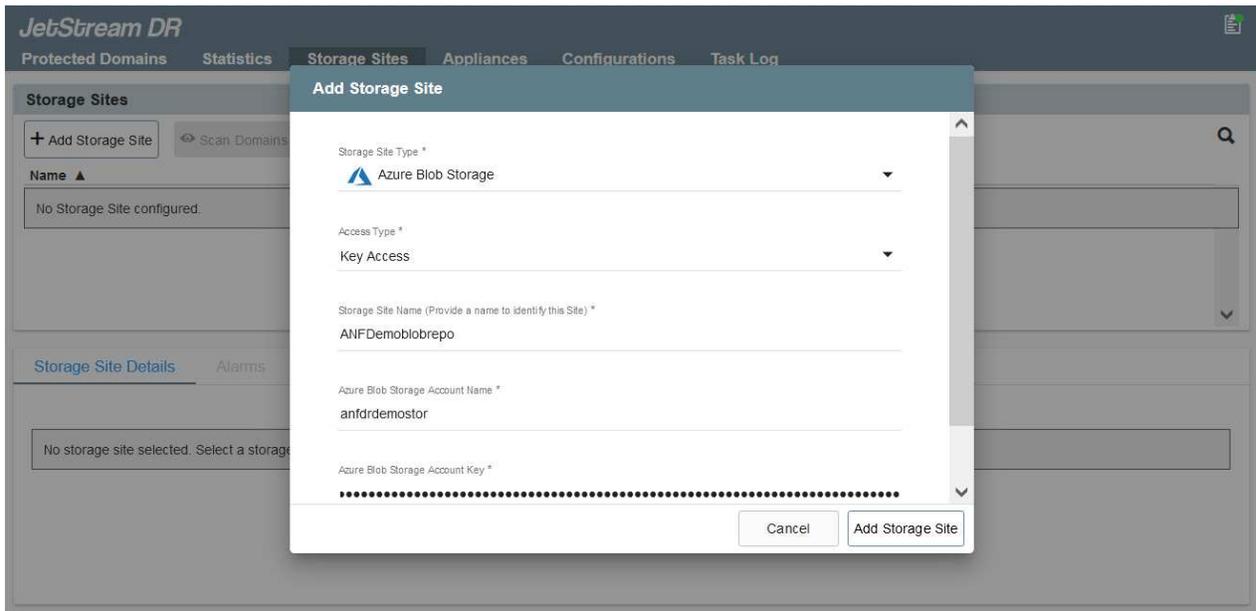
1. 檢查先決條件。
2. 運行容量規劃工具可取得資源和配置建議（可選，但建議用於概念驗證試驗）。
3. 將 JetStream DR MSA 部署到指定叢集中的 vSphere 主機。
4. 在瀏覽器中使用其 DNS 名稱啟動 MSA。
5. 向 MSA 註冊 vCenter 伺服器。若要執行安裝，請完成以下詳細步驟：
6. 部署 JetStream DR MSA 並註冊 vCenter Server 後，使用 vSphere Web Client 存取 JetStream DR 外掛程式。這可以透過導覽至資料中心 > 配置 > JetStream DR 來完成。



7. 從 JetStream DR 介面中，選擇適當的叢集。



8. 使用 I/O 篩選器包配置叢集。

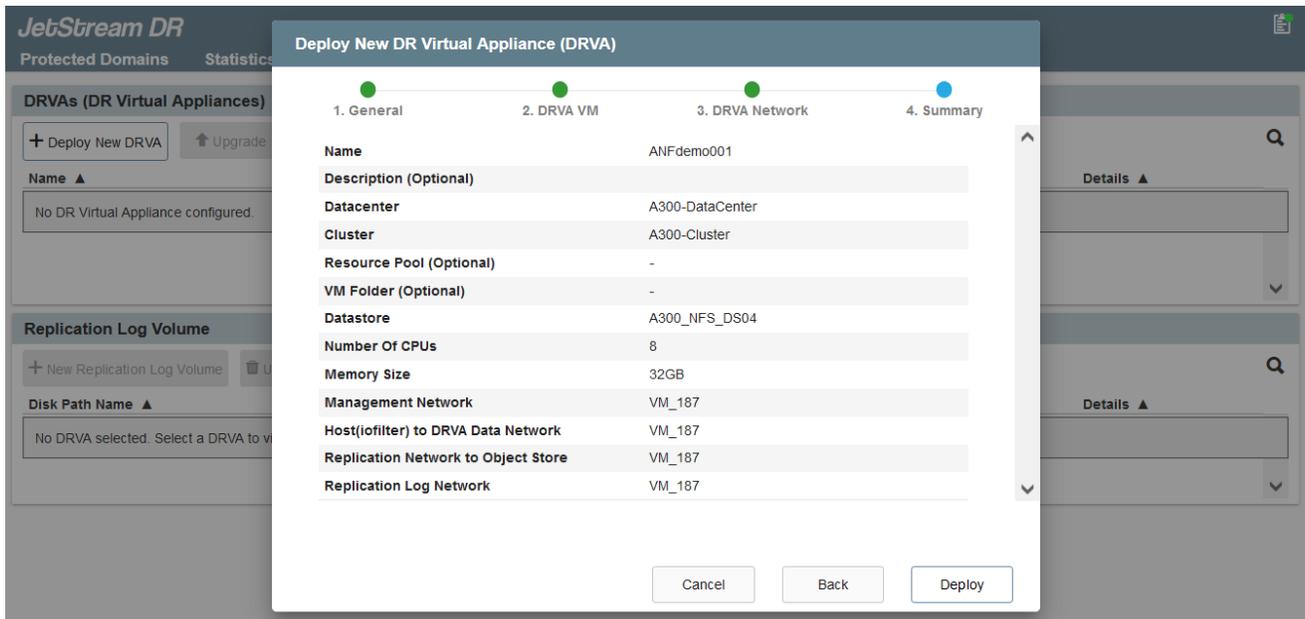


9. 新增位於復原站台的 Azure Blob 儲存體。
10. 從設備選項卡部署 DR 虛擬設備 (DRVA)。



DRVA 可以由 CPT 自動創建，但對於 POC 試驗，我們建議手動配置和運行 DR 週期（啟動保護 > 故障轉移 > 故障恢復）。

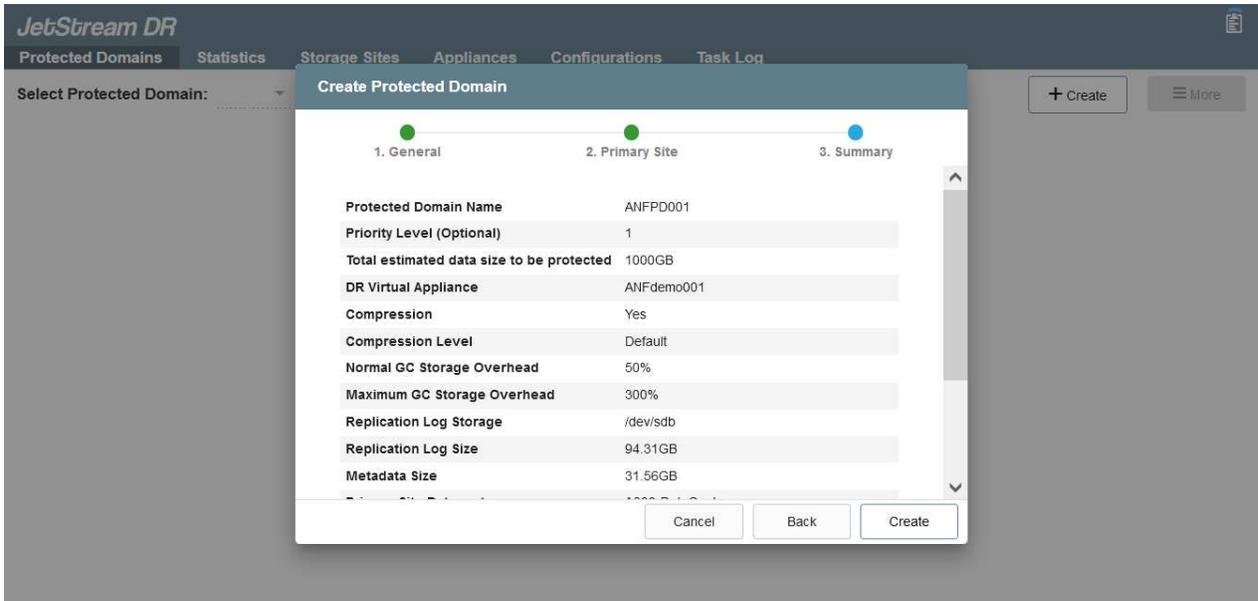
JetStream DRVA 是一種虛擬設備，可促進資料複製過程中的關鍵功能。受保護的叢集必須至少包含一個 DRVA，並且通常每個主機配置一個 DRVA。每個 DRVA 可以管理多個受保護域。



在此範例中，為 80 台虛擬機器建立了 4 個 DRVA。

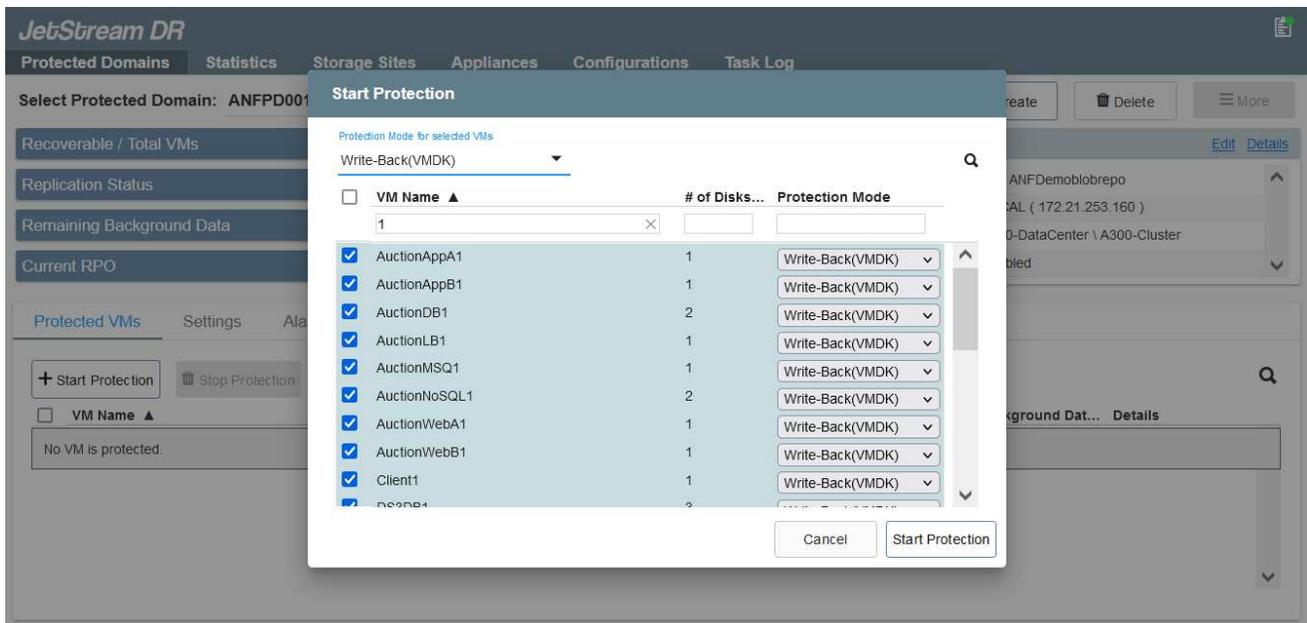
1. 使用來自可用資料儲存或獨立共用 iSCSI 儲存池的 VMDK 為每個 DRVA 建立複製日誌磁碟區。
2. 在「受保護的網域」標籤中，使用有關 Azure Blob 儲存站台、DRVA 執行個體和複製日誌的資訊建立所需數量的受保護網域。受保護域定義了叢集內的特定虛擬機或一組虛擬機，這些虛擬機受到共同保護

，並分配了故障轉移/故障回復操作的優先順序。



3. 選擇需要保護的虛擬機，啟動受保護域的虛擬機保護。這將開始將資料複製到指定的 Blob 儲存。

-  驗證受保護域中的所有虛擬機器是否使用相同的保護模式。
-  寫回 (VMDK) 模式可以提供更高的效能。



驗證複製日誌卷是否放置在高效能儲存上。

-  可以設定故障轉移運作手冊來對虛擬機器進行分組（稱為復原群組）、設定啟動順序以及修改 CPU/記憶體設定以及 IP 配置。

使用運行命令在 Azure VMware 解決方案私有雲中安裝 JetStream DR for AVS

恢復站點 (AVS) 的最佳實踐是提前創建一個三節點的試點燈叢集。這允許預先配置恢復站點基礎設施，包括以下項目：

- 目標網路段、防火牆、DHCP 和 DNS 等服務等等。
- 為 AVS 安裝 JetStream DR
- 將 ANF 卷配置為資料存儲，並且更多 JetStream DR 支援關鍵任務域的近零 RTO 模式。對於這些網域，應該預先安裝目標儲存。在這種情況下，ANF 是建議的儲存類型。



應在 AVS 叢集上配置包括段創建在內的網路配置以滿足本機要求。

根據 SLA 和 RTO 要求，可以使用連續故障轉移或常規（標準）故障轉移模式。對於接近零的 RTO，應在恢復站點開始持續補液。

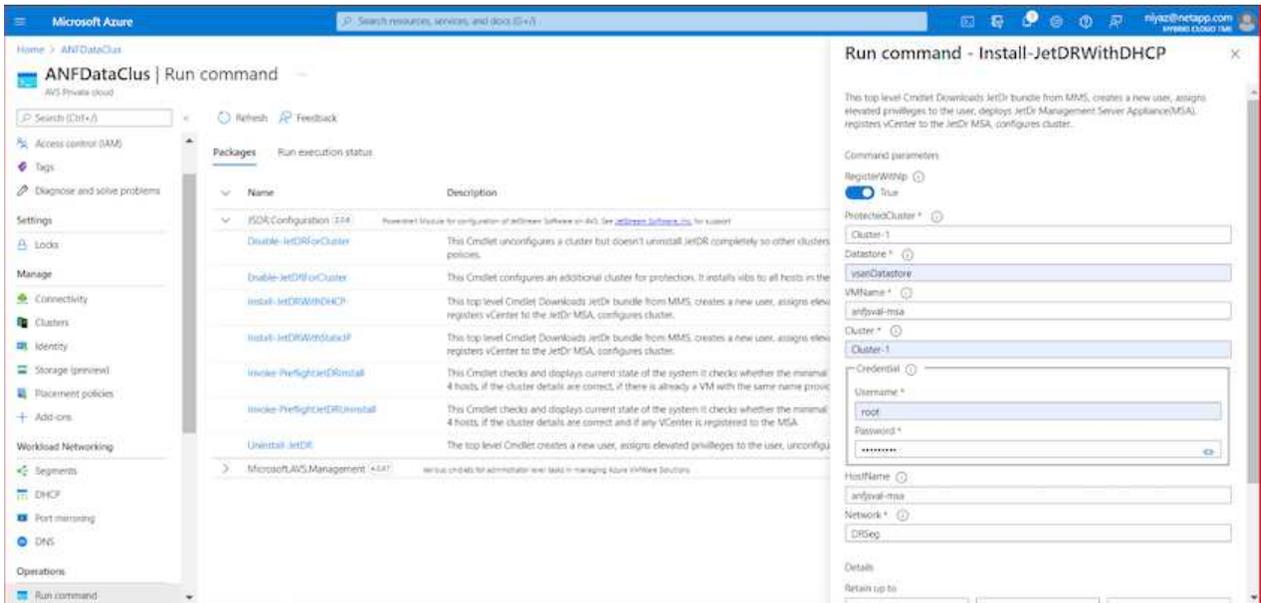
若要在 Azure VMware 解決方案私有雲上安裝 JetStream DR for AVS，請完成下列步驟：

1. 從 Azure 入口網站前往 Azure VMware 解決方案，選擇私有雲，然後選擇執行命令 > 套件 > JSDR.Configuration。



Azure VMware 解決方案中的預設 CloudAdmin 使用者沒有足夠的權限來為 AVS 安裝 JetStream DR。Azure VMware 解決方案透過呼叫 JetStream DR 的 Azure VMware 解決方案來執行指令，實現了 JetStream DR 的簡化和自動化安裝。

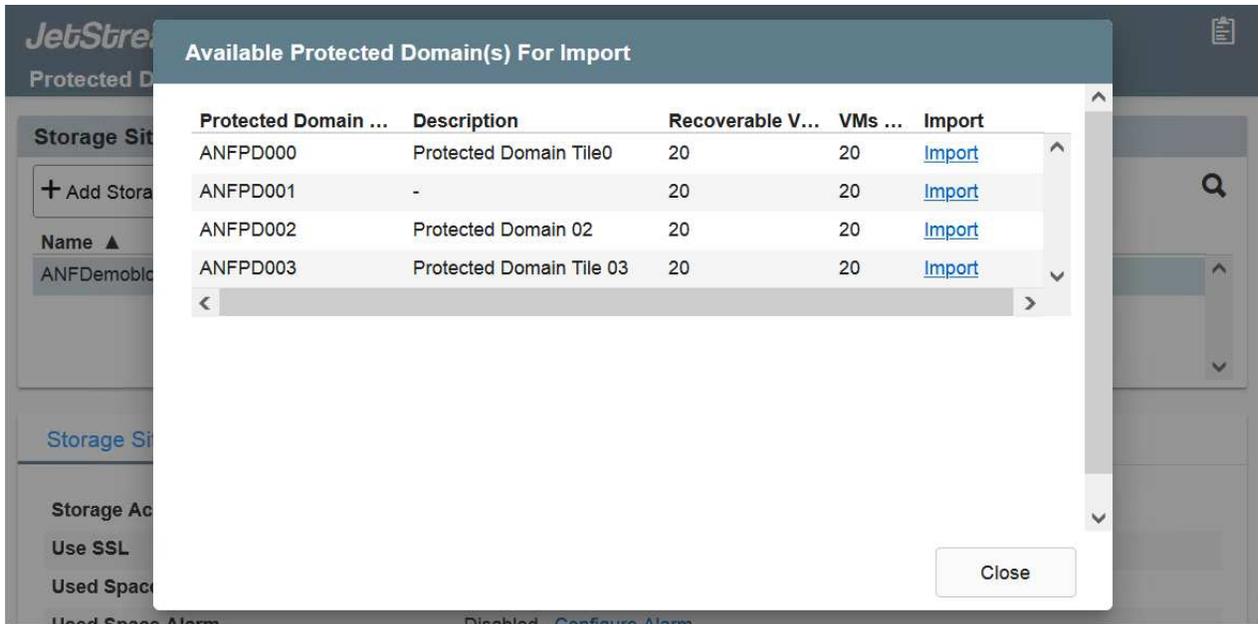
以下螢幕截圖顯示了使用基於 DHCP 的 IP 位址的安裝。



2. JetStream DR for AVS 安裝完成後，刷新瀏覽器。若要存取 JetStream DR UI，請前往 SDDC 資料中心 > 設定 > JetStream DR。



3. 從 JetStream DR 介面，新增用於保護本機叢集的 Azure Blob 儲存帳戶作為儲存站點，然後執行掃描網域選項。

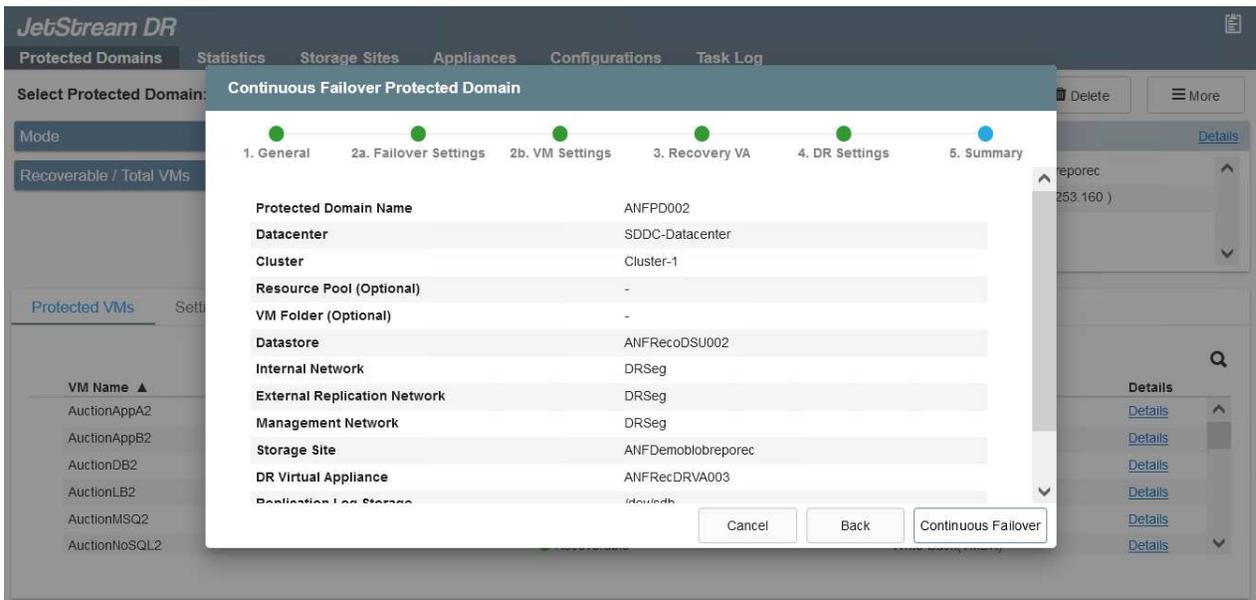


4. 導入受保護域後，部署 DRVA 設備。在此範例中，使用 JetStream DR UI 從復原站台手動啟動連續補水。



這些步驟也可以使用 CPT 建立的計劃自動執行。

5. 使用可用的 vSAN 或 ANF 資料儲存建立複製日誌卷。
6. 導入受保護的網域並配置恢復 VA 以使用 ANF 資料儲存進行 VM 放置。



確保所選網段上啟用了 DHCP 並且有足夠的可用 IP。在網域名稱恢復期間，暫時使用動態 IP。每個復原的虛擬機器（包括持續補水）都需要一個單獨的動態 IP。恢復完成後，IP 被釋放並可重複使用。

7. 選擇適當的故障轉移選項（連續故障轉移或故障轉移）。在這個例子中，選擇了持續補水（持續故障轉移）。

The screenshot shows the JetStream DR web interface. At the top, there are navigation tabs: Protected Domains, Statistics, Storage Sites, Appliances, Configurations, and Task Log. Below the tabs, there is a dropdown menu for 'Select Protected Domain' set to 'ANFPD000' and a 'View all' link. To the right are buttons for '+ Create', 'Delete', and 'More'. A 'Configurations' dropdown menu is open, showing options: 'Restore', 'Failover', 'Continuous Failover', and 'Test Failover'. Below this, there are summary statistics: 'Mode Imported' and 'Recoverable / Total VMs 20 / 20'. At the bottom, there is a table of 'Protected VMs' with columns for VM Name, Protection Status, Protection Mode, and Details.

VM Name ▲	Protection Status ▲	Protection Mode ▲	Details
AuctionAppA0	✔ Recoverable	Write-Back(VMDK)	Details ^
AuctionAppB0	✔ Recoverable	Write-Back(VMDK)	Details

執行故障轉移/故障回復

如何執行故障轉移/故障復原

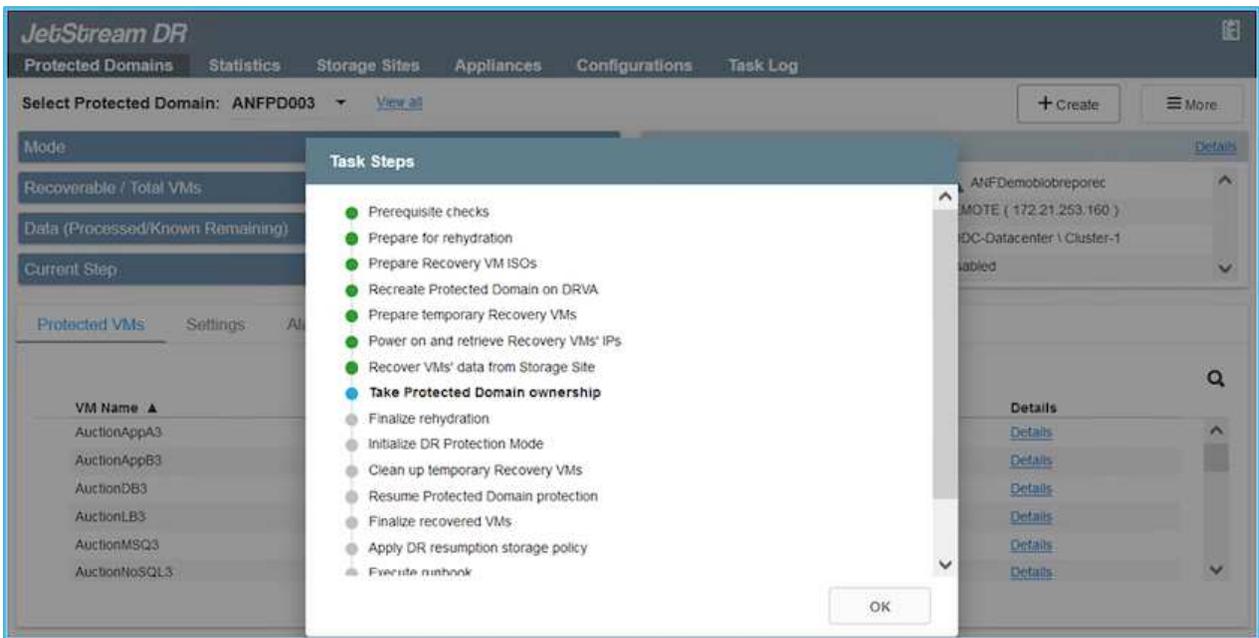
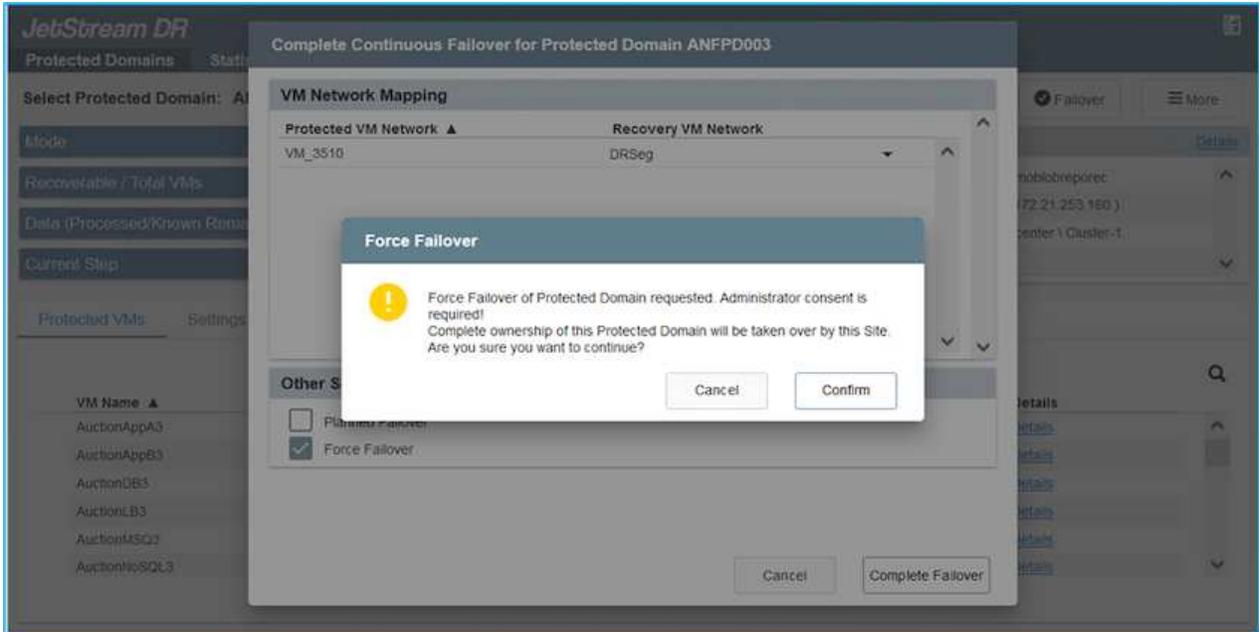
1. 當本地環境受保護叢集發生災難（部分或全部故障）後，觸發故障轉移。



CPT 可用於執行故障轉移計劃，將虛擬機器從 Azure Blob 儲存體還原至 AVS 叢集復原站台。

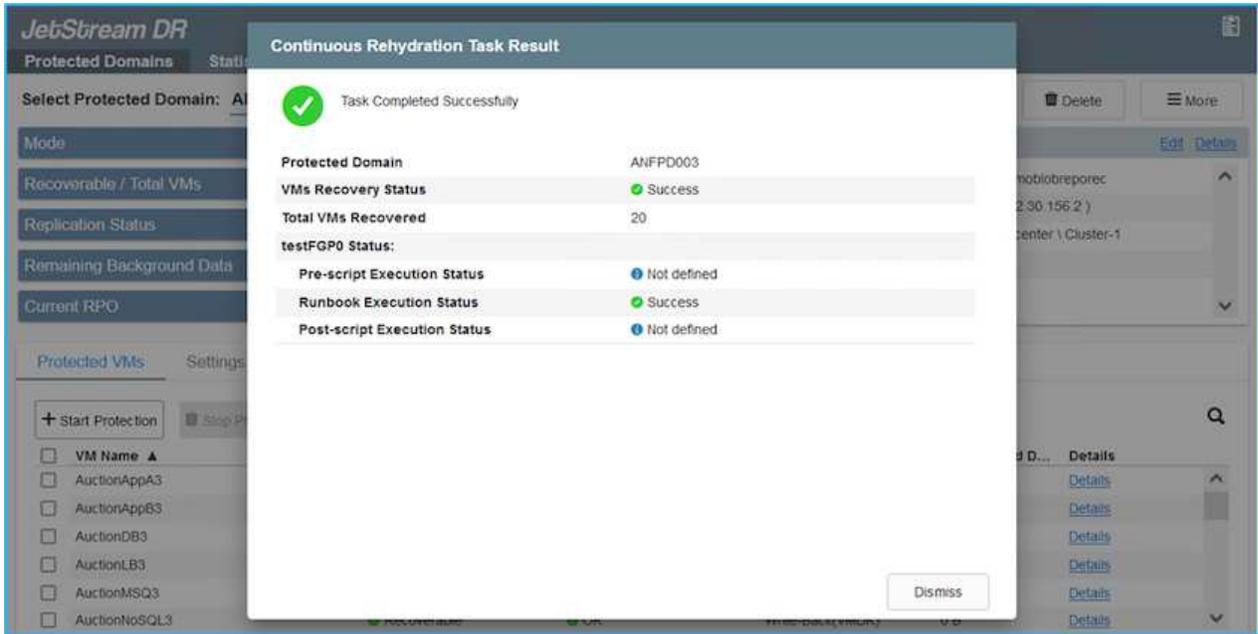


在 AVS 中啟動受保護的虛擬機器後進行故障轉移（用於連續或標準補水），保護將自動恢復，並且 JetStream DR 將繼續將其資料複製到 Azure Blob 儲存體中的相應/原始容器中。



工作列顯示故障轉移活動的進度。

2. 任務完成後，存取恢復的虛擬機，業務繼續正常進行。



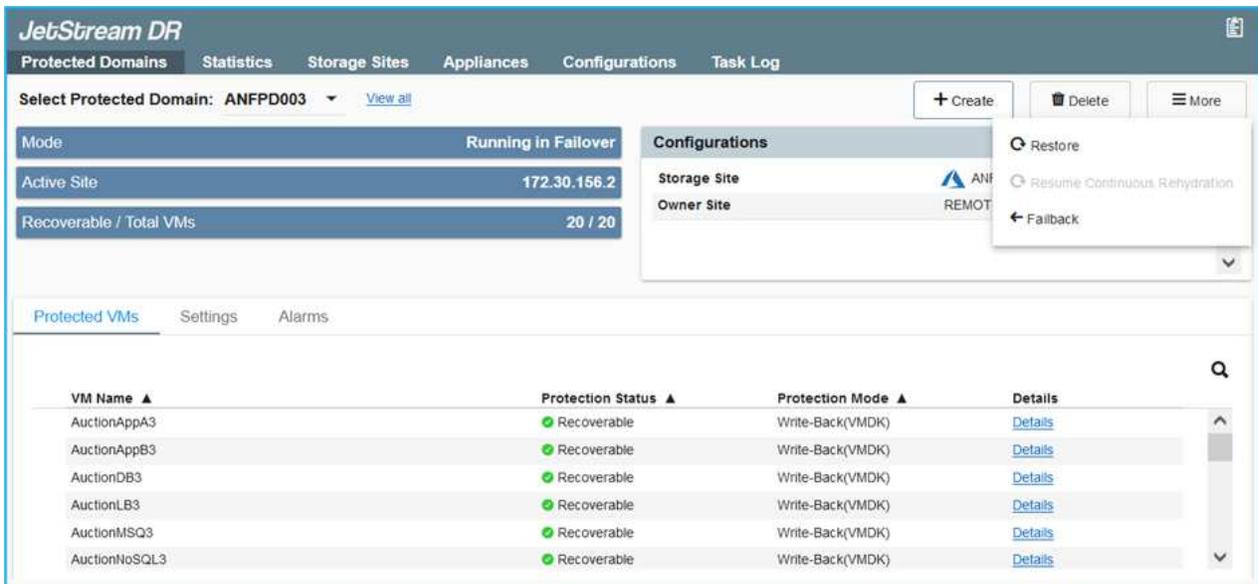
主站點重新啟動並運行後，即可執行故障復原。VM 保護已恢復，應檢查資料一致性。

3. 恢復本地環境。根據災難事件的類型，可能需要復原和/或驗證受保護叢集的配置。如有必要，可能需要重新安裝 JetStream DR 軟體。



注意：`recovery_utility_prepare_failback` 自動化工具包中提供的腳本可用於協助清理原始受保護網站中的任何過時的虛擬機器、網域資訊等。

4. 存取復原的本機環境，前往 Jetstream DR UI，然後選擇適當的受保護網域。受保護網站準備好故障復原後，在 UI 中選擇故障復原選項。



CPT 產生的故障復原計畫也可用於啟動虛擬機器及其資料從物件儲存返回原始 VMware 環境。



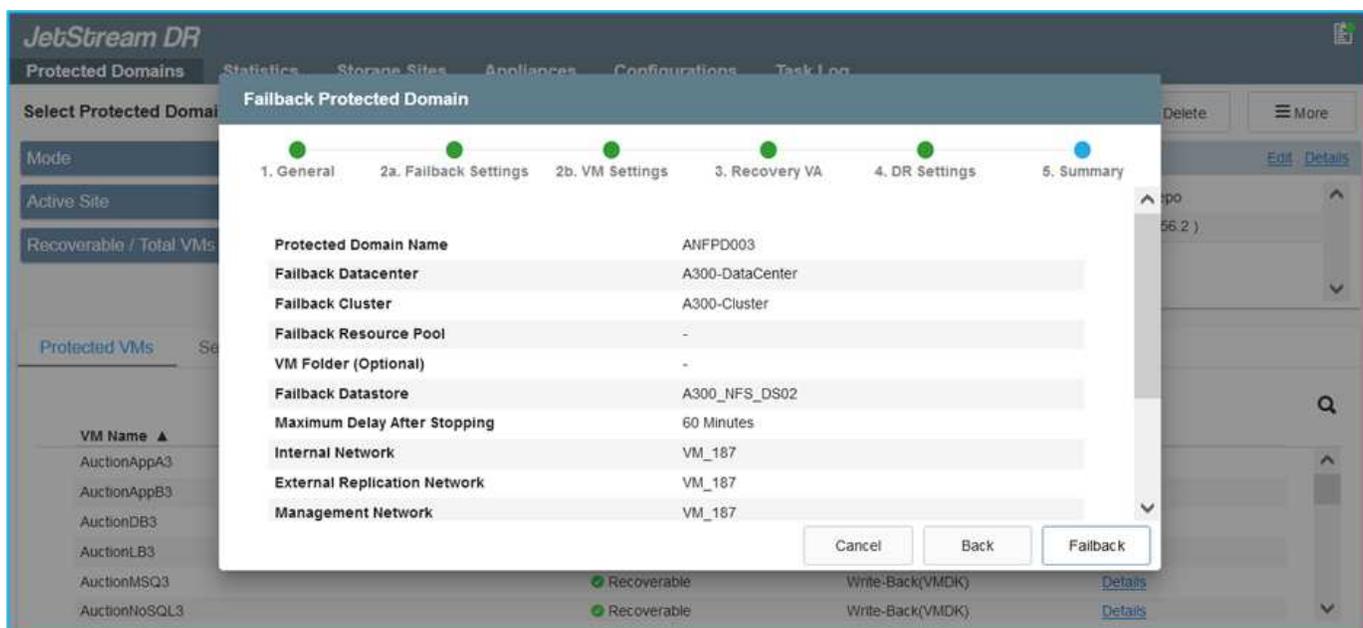
指定在復原站點中暫停虛擬機器並在受保護站點中重新啟動後的最大延遲。此時間包括停止故障轉移虛擬機器後完成複製的時間、清理復原站點的時間以及在受保護站點中重新建立虛擬機器的時間。NetApp建議值為 10 分鐘。

完成故障復原流程，然後確認復原虛擬機器保護和資料一致性。

勒索軟體恢復

從勒索軟體中恢復可能是一項艱鉅的任務。具體來說，IT 組織很難確定安全的返回點，而且一旦確定，如何確保恢復的工作負載免受再次發生的攻擊（來自休眠惡意軟體或透過易受攻擊的應用程式）。

JetStream DR for AVS 與 Azure NetApp Files 資料儲存結合，可解決這些問題，讓組織可以從可用的時間點恢復，以便在需要時將工作負載恢復到功能齊全的隔離網路。恢復允許應用程式運行並相互通信，同時不會將它們暴露在南北流量中，從而為安全團隊提供一個安全的地方來執行取證和其他必要的補救措施。



版權資訊

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

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

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

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

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

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

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

商標資訊

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