



適用於**AWS / VMC**的**NetApp** NetApp Solutions

NetApp
September 26, 2024

目錄

適用於AWS / VMC的NetApp	1
適用於AWS VMC的NetApp功能	1
保護 AWS / VMC 上的工作負載	2
在 AWS / VMC 上移轉工作負載	131
區域可用度–VMC的補充NFS資料存放區	149

適用於AWS / VMC的NetApp

適用於AWS VMC的NetApp功能

深入瞭解NetApp為AWS VMware Cloud (VMC) 帶來的功能：從NetApp做為來賓連線儲存設備或補充NFS資料存放區、移轉工作流程、延伸/突增至雲端、備份/還原及災難恢復。

從下列選項中選取、跳至所需內容的區段：

- ["在AWS中設定VMC"](#)
- ["適用於VMC的NetApp儲存選項"](#)
- ["NetApp / VMware雲端解決方案"](#)

在AWS中設定VMC

如同內部部署、規劃雲端型虛擬化環境對於成功建立虛擬機器和移轉的正式作業就緒環境來說、是非常重要的。

本節說明如何在AWS SDDC上設定及管理VMware Cloud、並搭配可用的選項來連接NetApp儲存設備。



客體內儲存設備是唯一支援的將Cloud Volumes ONTAP 功能連接到AWS VMC的方法。

設定程序可分為下列步驟：

- 部署及設定適用於AWS的VMware Cloud
- 將VMware Cloud連接至FSX ONTAP VMware

檢視詳細資訊 ["VMC的組態步驟"](#)。

適用於VMC的NetApp儲存選項

NetApp儲存設備可在AWS VMC中以多種方式使用、例如猜測連接的或補充的NFS資料存放區。

請造訪 ["支援的NetApp儲存選項"](#) 以取得更多資訊。

AWS支援下列組態的NetApp儲存設備：

- FSX ONTAP 支援以客為本的連線儲存設備
- 以客體連線儲存設備形式提供的資訊 (CVO) Cloud Volumes ONTAP
- FSX ONTAP 不只是NFS的補充資料存放區

檢視詳細資訊 ["VMC的來賓連線儲存選項"](#)。檢視詳細資訊 ["VMC的補充NFS資料存放區選項"](#)。

解決方案使用案例

有了NetApp和VMware雲端解決方案、許多使用案例都很容易部署在AWS VMC中。每個VMware定義的雲端領域都定義了使用案例：

- 保護（包括災難恢復和備份/還原）
- 延伸
- 移轉

["瀏覽NetApp的AWS VMC解決方案"](#)

保護 AWS / VMC 上的工作負載

TR-4931：在Amazon Web Services和Guest Connect上使用VMware Cloud進行災難恢復

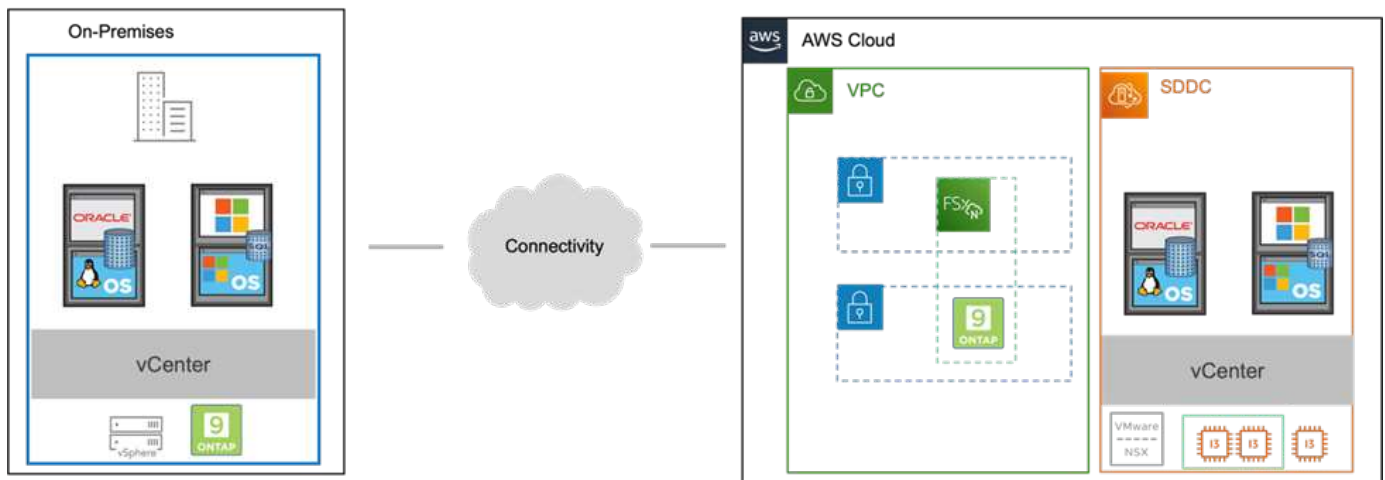
備受肯定的災難恢復（DR）環境與計畫、對於組織而言至關重要、因為如此一來、組織就能確保在重大停機事件中迅速還原業務關鍵應用程式。本解決方案著重於示範DR使用案例、重點在於內部部署的VMware與NetApp技術、以及使用AWS上的VMware Cloud。

作者：Chris Reno、Josh Powell和Suresh Thopp付款- NetApp解決方案工程

總覽

NetApp與VMware的整合歷史悠久、已有數萬家客戶選擇NetApp做為其虛擬化環境的儲存合作夥伴、證明這一點。這項整合會繼續與雲端的來賓連線選項整合、以及最近與NFS資料存放區的整合。本解決方案著重於通常稱為來賓連線儲存設備的使用案例。

在客體連線儲存設備中、客體VMDK會部署在VMware資源配置的資料存放區上、而應用程式資料則儲存在iSCSI或NFS上、並直接對應至VM。Oracle和MS SQL應用程式用於示範DR案例、如下圖所示。



假設、先決條件和元件總覽

在部署此解決方案之前、請先檢閱元件的總覽、部署解決方案所需的先決條件、以及記錄此解決方案時所做的假設。

["災難恢復解決方案要求、預先要求和規劃"](#)

使用SnapCenter NetApp執行災難恢復

在本解決方案中SnapCenter、支援針對SQL Server和Oracle應用程式資料提供應用程式一致的快照。此組態搭配SnapMirror技術、可在內部部署AFF的Sf6 ONTAP和FSX支援叢集之間提供高速資料複寫功能。此外、Veeam備份與複寫也為我們的虛擬機器提供備份與還原功能。

在本節中、我們將說明SnapCenter如何設定用於備份與還原的SnapMirror、SnapMirror和Veeam。

下列各節涵蓋在次要站台完成容錯移轉所需的組態和步驟：

設定SnapMirror關係和保留排程

為了長期歸檔和保留、可在主要儲存系統（主儲存系統>鏡射）和次要儲存系統（主儲存系統>保存庫）內更新SnapMirror關係。SnapCenter若要這麼做、您必須使用SnapMirror建立並初始化目的地Volume與來源Volume之間的資料複寫關係。

來源ONTAP和目的地的不全系統必須位於使用Amazon VPC對等網路、傳輸閘道、AWS Direct Connect或AWS VPN進行對等處理的網路中。

在內部部署ONTAP的SnapMirror系統與FSX Sing之間建立SnapMirror關係時、必須執行下列步驟ONTAP：



請參閱 ["FSX- ONTAP for Sfor Sfor Sfor - ONTAP 《用戶指南》"](#) 如需建立SnapMirror與FSX關係的詳細資訊、

對於ONTAP 內部部署的來源版的來源版系統、您可以從System Manager或CLI擷取叢集間的LIF資訊。

1. 在「支援系統管理程式」中ONTAP、瀏覽至「網路總覽」頁面、並擷取「類型：叢集間」的IP位址、這些位址已設定為與安裝FSx的AWS VPC通訊。

Name	Status	Storage VM	IPspace	Address	Current Node	Current Port	Portset	Protocols	Type	Thru
veeam_repo	✓	Backup	Default	10.61.181.179	E13A300_1	a0a-181		SMB/CIFS, NFS, S3	Data	0
CM01	✓		Default	10.61.181.180	E13A300_1	a0a-181			Cluster/Node Mgmt	0
HC_N1	✓		Default	10.61.181.183	E13A300_1	a0a-181			Intercluster,Cluster/Node Mgmt	0
HC_N2	✓		Default	10.61.181.184	E13A300_2	a0a-181			Intercluster,Cluster/Node Mgmt	0
lif_ora_vsm_614	✓	ora_vsm	Default	10.61.181.185	E13A300_1	a0a-181		SMB/CIFS, NFS, FL...	Data	0

2. 若要擷取FSX的叢集間IP位址、請登入CLI並執行下列命令：

```
FSx-Dest::> network interface show -role intercluster
```

```
FsxId0ae40e08acc0dea67::> network interface show -role intercluster
      Logical   Status   Network   Current   Current   Is
Vserver  Interface  Admin/Oper  Address/Mask   Node       Port     Home
-----
FsxId0ae40e08acc0dea67
      inter_1   up/up     172.30.15.42/25  FsxId0ae40e08acc0dea67-01
                                                e0e       true
      inter_2   up/up     172.30.14.28/26  FsxId0ae40e08acc0dea67-02
                                                e0e       true
2 entries were displayed.
```

在ONTAP Sfx6和FSX之間建立叢集對等關係

若要在ONTAP 各個叢集之間建立叢集對等關係、必須ONTAP 在其他對等叢集中確認在起始的叢集上輸入的獨特通關密碼。

1. 使用「叢集對等點create」命令、在目的地FSX叢集上設定對等。出現提示時、請輸入稍後在來源叢集上使用的唯一密碼、以完成建立程序。

```
FSx-Dest::> cluster peer create -address-family ipv4 -peer-addr  
source_intercluster_1, source_intercluster_2  
Enter the passphrase:  
Confirm the passphrase:
```

2. 在來源叢集上、您可以使用ONTAP SysSystem Manager或CLI建立叢集對等關係。從「系統管理程式」中、瀏覽至「保護」>「總覽」、然後選取「對等叢集」ONTAP。



DASHBOARD

STORAGE

Overview

Volumes

LUNs

Consistency Groups

NVMe Namespaces

Shares

Buckets

Qtrees

Quotas

Storage VMs

Tiers

NETWORK

Overview

Ethernet Ports

FC Ports

EVENTS & JOBS

PROTECTION

Overview

Relationships

HOSTS

Overview

< Intercluster Settings

Network Interfaces

IP ADDRESS

- ✓ 10.61.181.184
- ✓ 172.21.146.217
- ✓ 10.61.181.183
- ✓ 172.21.146.216

Cluster Peers

PEERED CLUSTER NAME

- ✓ FsxId0ae40e08acc0dea67
- ✓ OTS02

Mediator ?

Not configured.

Configure

Storage VM Peers

PEERED STORAGE VMS

- ✓ 3

3. 在對等叢集對話方塊中、填寫必要資訊：
 - a. 輸入用於在目的地FSX叢集上建立對等叢集關係的通關密碼。
 - b. 選取「是」以建立加密關係。

c. 輸入目的地FSX叢集的叢集間LIF IP位址。

d. 按一下「初始化叢集對等」以完成程序。

Peer Cluster

Local

Remote

STORAGE VM PERMISSIONS

All storage VMs (incl... X)

Storage VMs created in the future also will be given permissions.

PASSPHRASE ?

.....

It cannot be determined from the passphrase whether this relationship was encrypted. Is the relationship encrypted?

Yes No

To generate passphrase, Launch Remote Cluster

Intercluster Network Interfaces IP Addresses

172.30.15.42

172.30.14.28

Cancel

+ Add

Initiate Cluster Peering Cancel

4. 使用下列命令驗證來自FSX叢集的叢集對等關係狀態：

```
FSx-Dest::> cluster peer show
```

```
FsxId0ae40e08acc0dea67::> cluster peer show
Peer Cluster Name      Cluster Serial Number Availability  Authentication
-----
E13A300                1-80-000011 Available    ok
```

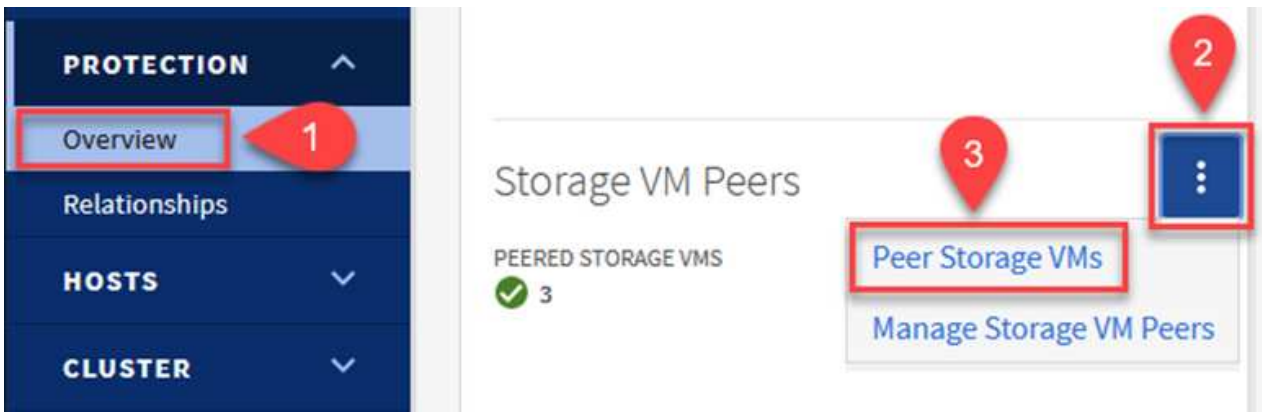
建立SVM對等關係

下一步是在包含SnapMirror關係的磁碟區的目的地與來源儲存虛擬機器之間建立SVM關係。

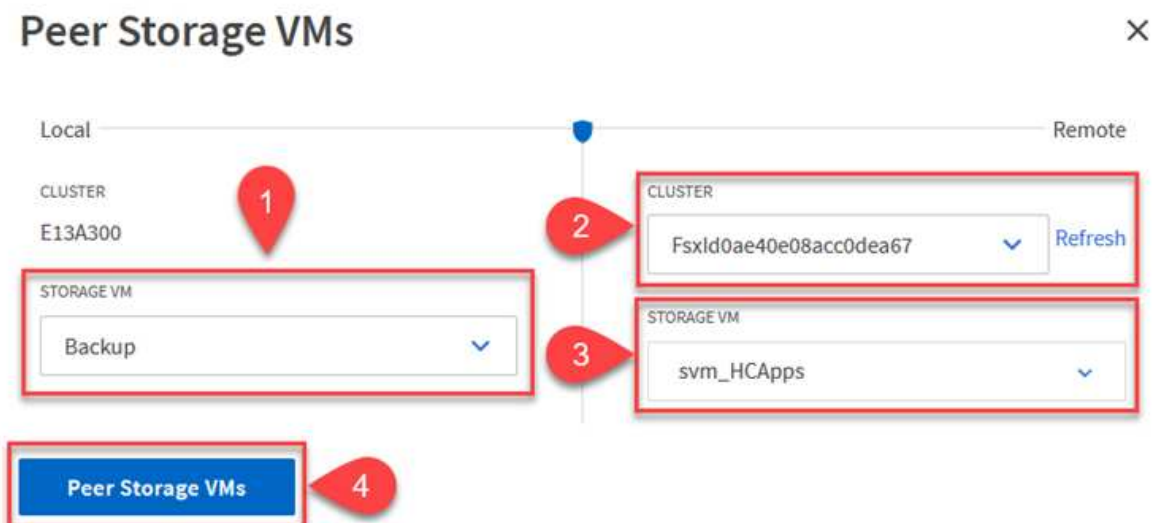
1. 從來源FSX叢集、從CLI使用下列命令建立SVM對等關係：

```
FSx-Dest::> vserver peer create -vserver DestSVM -peer-vserver Backup -peer-cluster OnPremSourceSVM -applications snapmirror
```

2. 從來源ONTAP 的物件叢集、接受與ONTAP SysSystem Manager或CLI的對等關係。
3. 從「支援系統管理程式」移至「保護」>「總覽」、然後在「儲存VM對等端點」下選取「對等儲存VM」ONTAP。



4. 在對等儲存VM對話方塊中、填寫必填欄位：
 - 來源儲存VM
 - 目的地叢集
 - 目的地儲存VM



5. 按一下對等儲存VM以完成SVM對等處理程序。

可管理主要儲存系統上以快照複本形式存在的備份保留排程。SnapCenter這是SnapCenter 在建立一套以功能為基礎的原則時所建立的。不管理保留在二線儲存系統上的備份保留原則。SnapCenter這些原則是透過在次要FSX叢集上建立的SnapMirror原則來個別管理、並與與來源Volume處於SnapMirror關係中的目的地磁碟區相關聯。

建立SnapCenter Eshot原則時、您可以選擇指定次要原則標籤、並將其新增至SnapCenter 擷取此備份時所產生之每個Snapshot的SnapMirror標籤。



在二線儲存設備上、這些標籤會符合與目的地Volume相關的原則規則、以強制保留快照。

以下範例顯示SnapMirror標籤、其存在於所有快照上、這些快照是作為每日備份SQL Server資料庫和記錄磁碟區的原則之一。

Select secondary replication options ⓘ

Update SnapMirror after creating a local Snapshot copy.

Update SnapVault after creating a local Snapshot copy.

Secondary policy label

Custom Label ⓘ

sql-daily

Error retry count

3 ⓘ

如需建立SnapCenter SQL Server資料庫的各項功能性原則的詳細資訊、請參閱 ["本文檔SnapCenter"](#)。

您必須先建立SnapMirror原則、其中規定要保留的快照複本數量。

1. 在FSX叢集上建立SnapMirror原則。

```
FSx-Dest::> snapmirror policy create -vserver DestSVM -policy  
PolicyName -type mirror-vault -restart always
```

2. 使用SnapMirror標籤將規則新增至原則、這些標籤符合SnapCenter 在《保護原則》中指定的次要原則標籤。

```
FSx-Dest::> snapmirror policy add-rule -vserver DestSVM -policy  
PolicyName -snapmirror-label SnapMirrorLabelName -keep  
#ofSnapshotsToRetain
```

下列指令碼提供可新增至原則的規則範例：

```
FSx-Dest::> snapmirror policy add-rule -vserver sql_svm_dest -policy Async_SnapCenter_SQL -snapmirror-label sql-ondemand -keep 15
```



針對每個SnapMirror標籤和要保留的快照數量（保留期間）建立其他規則。

建立目的地Volume

若要在FSXTM上建立目的地Volume、使其成為來源Volume中快照複本的接收者、請在FSxTM上執行下列命令ONTAP：

```
FSx-Dest::> volume create -vserver DestSVM -volume DestVolName  
-aggregate DestAggrName -size VolSize -type DP
```

在來源與目的地磁碟區之間建立SnapMirror關係

若要在來源與目的地Volume之間建立SnapMirror關係、請在FSX ONTAP Sf2上執行下列命令：

```
FSx-Dest::> snapmirror create -source-path  
OnPremSourceSVM:OnPremSourceVol -destination-path DestSVM:DestVol -type  
XDP -policy PolicyName
```

初始化SnapMirror關係

初始化SnapMirror關係。此程序會啟動從來源磁碟區產生的新快照、並將其複製到目的地磁碟區。

```
FSx-Dest::> snapmirror initialize -destination-path DestSVM:DestVol
```

在SnapCenter 內部部署及設定Windows靜態伺服器。

在SnapCenter 內部部署Windows功能伺服器

此解決方案使用NetApp SnapCenter 解決方案來執行SQL Server和Oracle資料庫的應用程式一致備份。搭配使用Veeam備份與複寫來備份虛擬機器VMDK、可為內部部署與雲端型資料中心提供全方位的災難恢復解決方案。

NetApp支援網站提供支援軟體、可安裝在位於網域或工作群組的Microsoft Windows系統上。SnapCenter如需詳細的規劃指南和安裝指示、請參閱 "[NetApp文件中心](#)"。

您可SnapCenter 從取得此軟體 "[此連結](#)"。

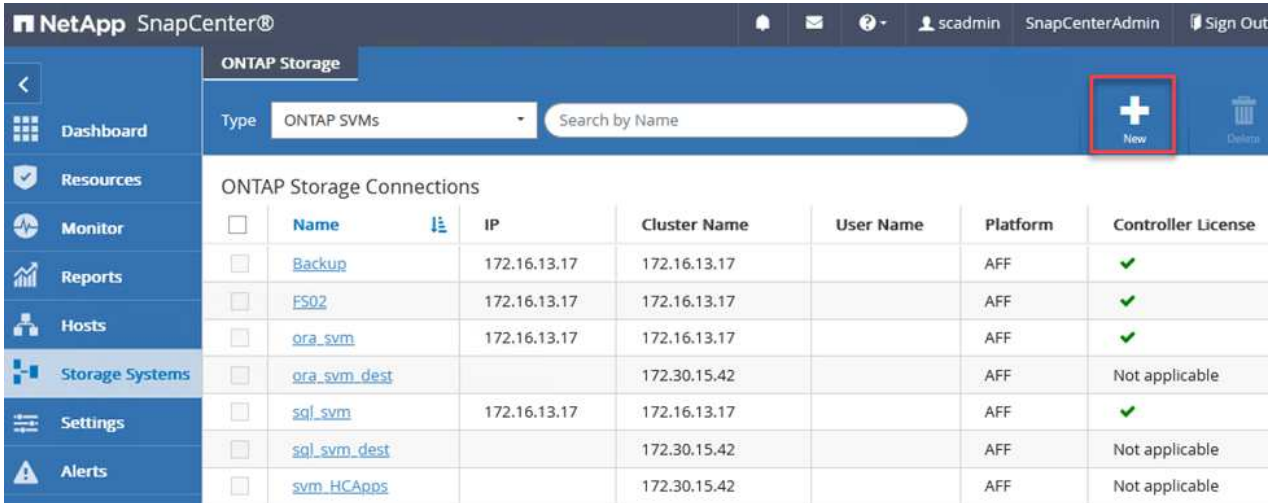
安裝完畢後、您可以SnapCenter 使用 `_https://Virtual_Cluster_IP_or_FQDN:8146_` 從網頁瀏覽器存取此功能。

登入主控台之後、您必須設定SnapCenter 支援備份SQL Server和Oracle資料庫的功能。

將儲存控制器新增SnapCenter 至

若要將儲存控制器新增SnapCenter 至效益區、請完成下列步驟：

1. 從左功能表中選取「Storage Systems (儲存系統)」、然後按一下「New (新增)」開始將儲存控制器新增SnapCenter 至VMware。



The screenshot shows the NetApp SnapCenter interface. The left sidebar contains navigation options: Dashboard, Resources, Monitor, Reports, Hosts, Storage Systems (highlighted), Settings, and Alerts. The main content area is titled 'ONTAP Storage' and shows a search bar for 'ONTAP SVMs'. A red box highlights the 'New' button in the top right corner. Below this is a table of 'ONTAP Storage Connections'.

<input type="checkbox"/>	Name	IP	Cluster Name	User Name	Platform	Controller License
<input type="checkbox"/>	Backup	172.16.13.17	172.16.13.17		AFF	✓
<input type="checkbox"/>	FS02	172.16.13.17	172.16.13.17		AFF	✓
<input type="checkbox"/>	ora_svm	172.16.13.17	172.16.13.17		AFF	✓
<input type="checkbox"/>	ora_svm_dest		172.30.15.42		AFF	Not applicable
<input type="checkbox"/>	sql_svm	172.16.13.17	172.16.13.17		AFF	✓
<input type="checkbox"/>	sql_svm_dest		172.30.15.42		AFF	Not applicable
<input type="checkbox"/>	svm_HCApps		172.30.15.42		AFF	Not applicable


2. 在「Add Storage System (新增儲存系統)」對話方塊中、新增本機內部部署ONTAP 的元件叢集的管理IP位址、以及使用者名稱和密碼。然後按一下「提交」開始探索儲存系統。

Add Storage System

Add Storage System

Storage System	<input type="text" value="10.61.181.180"/>
Username	<input type="text" value="admin"/>
Password	<input type="password" value="••••••••"/>

Event Management System (EMS) & AutoSupport Settings

- Send AutoSupport notification to storage system
- Log SnapCenter Server events to syslog
-  **More Options** : Platform, Protocol, Preferred IP etc..

- 重複此程序、將FSX ONTAP 更新SnapCenter 為支援。在這種情況下、請選取「Add Storage System」（新增儲存系統）視窗底部的「More Options」（更多選項）、然後按一下「Secondary」（次要）核取方塊、將FSX系統指定為使用SnapMirror複本或我們的主要備份快照更新的次要儲存系統。

More Options




Platform FAS

Secondary 

Protocol HTTPS

Port 443

Timeout 60 seconds 

Preferred IP 

Save

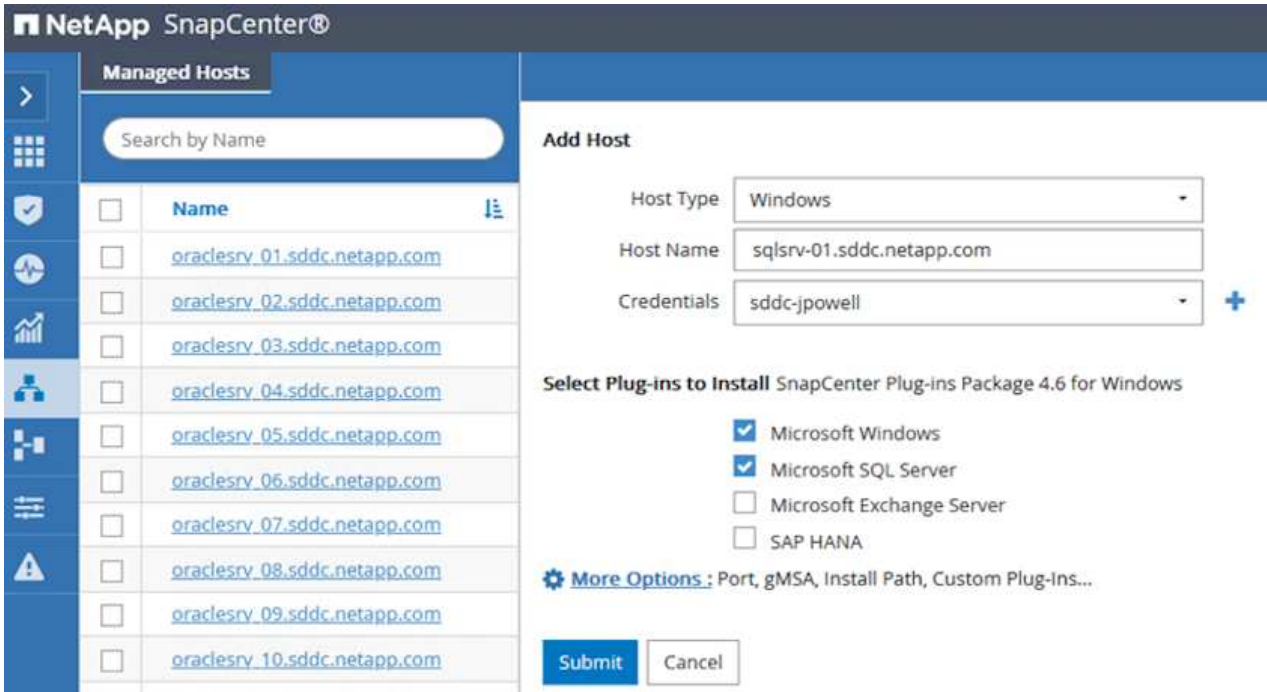
Cancel

如需將儲存系統新增SnapCenter 至效益管理系統的相關資訊、請參閱文件、網址為 "[此連結](#)"。

將主機新增SnapCenter 至

下一步是將主機應用程式伺服器新增SnapCenter 至SQL Server和Oracle的程序類似。

1. 從左功能表中選取「hosts」、然後按一下「Add (新增)」、開始將儲存控制器新增SnapCenter 至VMware。
2. 在Add hosts (新增主機) 視窗中、新增Host Type (主機類型)、Hostname (主機名稱) 和主機系統認證。選取外掛程式類型。若為SQL Server、請選取Microsoft Windows和Microsoft SQL Server外掛程式。



3. 對於Oracle、請在「新增主機」對話方塊中填寫必填欄位、然後選取Oracle資料庫外掛程式的核取方塊。然後按一下「提交」開始探索程序、並將主機新增SnapCenter 至VMware。

Add Host

Host Type

Host Name

Credentials



Select Plug-ins to Install SnapCenter Plug-ins Package 4.6 for Linux

Oracle Database

SAP HANA

[More Options](#) : Port, Install Path, Custom Plug-Ins...

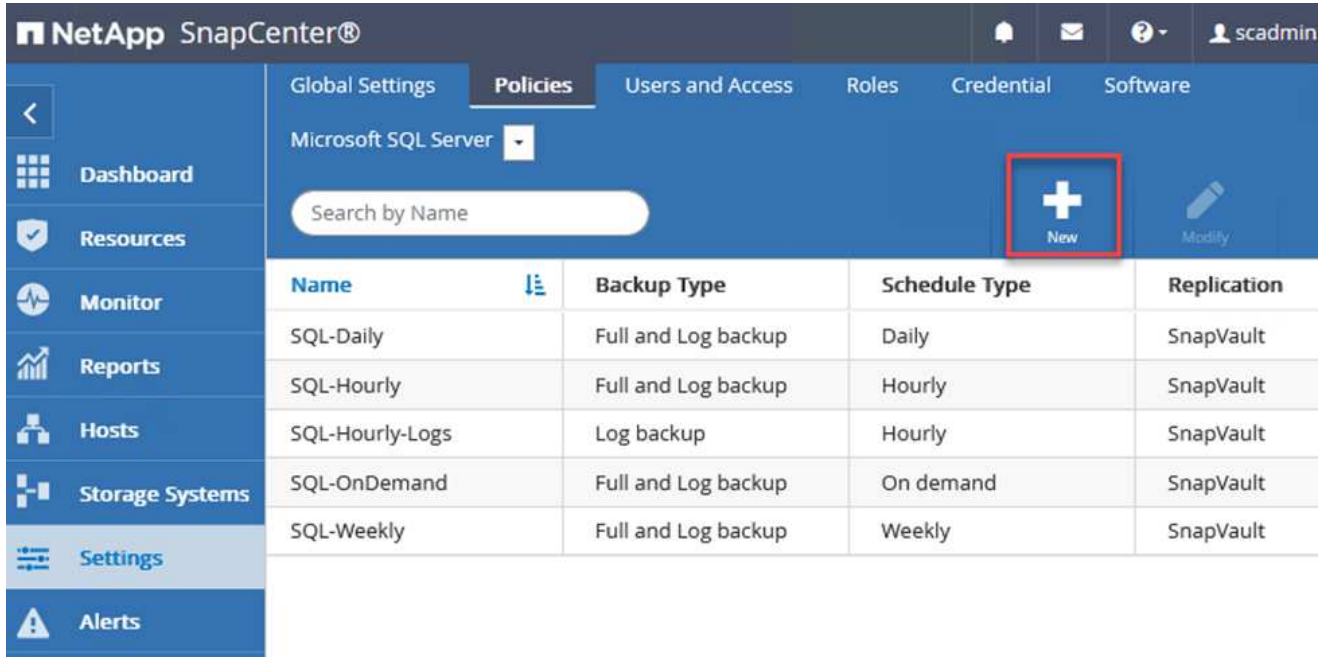
Submit

Cancel

建立SnapCenter 不規則

原則會針對備份工作建立要遵循的特定規則。其中包括但不限於備份排程、複寫類型、SnapCenter 以及如何處理備份和刪節交易記錄。

您可以在SnapCenter 「功能性」 (英語) 的「設定」 (Settings) 區段中存取原則。



The screenshot shows the NetApp SnapCenter interface. The top navigation bar includes 'Global Settings', 'Policies', 'Users and Access', 'Roles', 'Credential', and 'Software'. The 'Policies' tab is selected, and the system is identified as 'Microsoft SQL Server'. A search bar labeled 'Search by Name' is present. A red box highlights a '+ New' button. Below the navigation is a table of backup policies:

Name	Backup Type	Schedule Type	Replication
SQL-Daily	Full and Log backup	Daily	SnapVault
SQL-Hourly	Full and Log backup	Hourly	SnapVault
SQL-Hourly-Logs	Log backup	Hourly	SnapVault
SQL-OnDemand	Full and Log backup	On demand	SnapVault
SQL-Weekly	Full and Log backup	Weekly	SnapVault

如需建立SQL Server備份原則的完整資訊、請參閱 "[本文檔SnapCenter](#)"。

如需建立Oracle備份原則的完整資訊、請參閱 "[本文檔SnapCenter](#)"。

- 附註：*
- 當您逐步完成原則建立精靈時、請特別注意「複寫」區段。在本節中、您將說明您要在備份程序中取得的次要SnapMirror複本類型。
- 「建立本機Snapshot複本後再更新SnapMirror」設定是指當位於同一個叢集上的兩個儲存虛擬機器之間存在SnapMirror關係時、更新SnapMirror關係。
- 「建立SnapVault 本機快照複本後更新功能」設定可用來更新兩個獨立叢集之間、內部部署ONTAP的SnapMirror系統與Cloud Volumes ONTAP BIOS或FSxN之間存在的SnapMirror關係。

下圖顯示上述選項、以及它們在備份原則精靈中的外觀。

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

Select secondary replication options ⓘ

Update SnapMirror after creating a local Snapshot copy.

Update SnapVault after creating a local Snapshot copy.

Secondary policy label

Choose

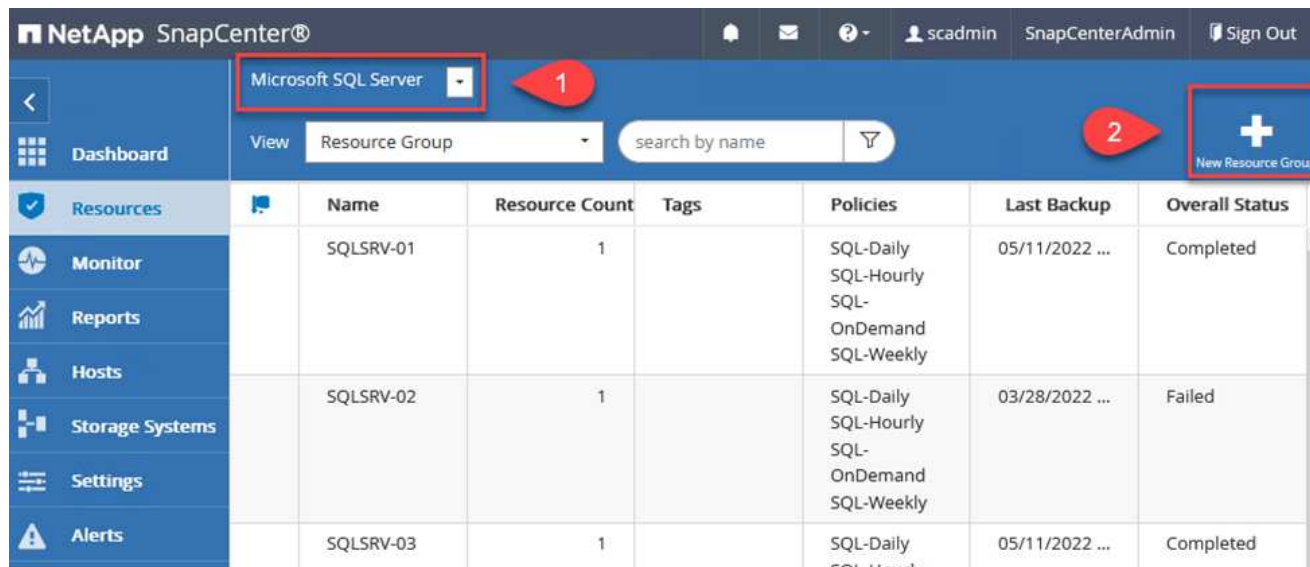
Error retry count

3

建立SnapCenter 資源群組

資源群組可讓您選取要納入備份的資料庫資源、以及這些資源所遵循的原則。

1. 前往左側功能表的「資源」區段。
2. 在視窗頂端、選取要使用的資源類型（在此情況下是Microsoft SQL Server）、然後按一下「New Resource Group（新資源群組）」。



Name	Resource Count	Tags	Policies	Last Backup	Overall Status
SQLSRV-01	1		SQL-Daily SQL-Hourly SQL-OnDemand SQL-Weekly	05/11/2022 ...	Completed
SQLSRV-02	1		SQL-Daily SQL-Hourly SQL-OnDemand SQL-Weekly	03/28/2022 ...	Failed
SQLSRV-03	1		SQL-Daily SQL-Hourly	05/11/2022 ...	Completed

本《支援》文件涵蓋SnapCenter 建立SQL Server和Oracle資料庫資源群組的逐步詳細資料。

如需備份SQL資源、請遵循 ["此連結"](#)。

如需備份Oracle資源、請遵循 ["此連結"](#)。

部署及設定Veeam備份伺服器

解決方案中使用Veeam備份與複寫軟體來備份應用程式虛擬機器、並使用Veeam橫向擴充備份儲存庫 (SOBR) 將備份複本歸檔至Amazon S3儲存庫。在本解決方案中、Veeam部署於Windows伺服器上。如需部署Veeam的具體指引、請參閱 "[Veeam說明中心技術文件](#)"。

設定Veeam橫向擴充備份儲存庫

在您部署並授權軟體之後、您可以建立橫向擴充備份儲存庫 (SOBR) 作為備份工作的目標儲存設備。您也應該將S3儲存區納入異地備份VM資料、以便進行災難恢復。

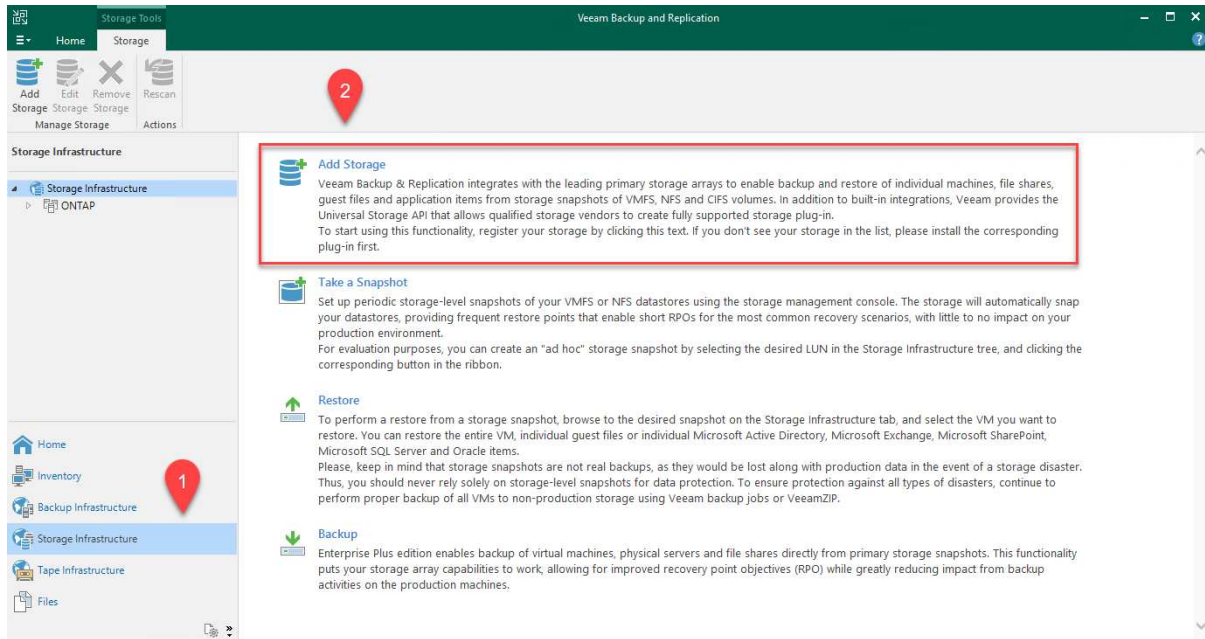
請先參閱下列必要條件、再開始使用。

1. 在內部部署ONTAP 的支援系統上建立SMB檔案共用區、做為備份的目標儲存設備。
2. 建立Amazon S3儲存庫以納入SOBR。這是用於異地備份的儲存庫。

新增ONTAP 功能至Veeam

首先、在ONTAP Veeam中新增功能不支援的儲存叢集和相關的SMB/NFS檔案系統作為儲存基礎架構。

1. 開啟Veeam主控台並登入。瀏覽至Storage Infrastructure、然後選取Add Storage。



2. 在「Add Storage（新增儲存設備）」精靈中、選取NetApp作為儲存設備廠商、然後選取Data ONTAP「NetApp」。
3. 輸入管理IP位址、然後勾選NAS Filer方塊。按一下「下一步」

New NetApp Data ONTAP Storage



Name

Register NetApp Data ONTAP storage by specifying DNS name or IP address.

Name	Management server DNS name or IP address: <input type="text" value="10.61.181.180"/>
Credentials	Description: <input type="text" value="Created by SDDC\jpowell at 5/17/2022 10:34 AM."/>
NAS Filer	Role: <input type="checkbox"/> Block or file storage for VMware vSphere <input type="checkbox"/> Block storage for Microsoft Windows servers <input checked="" type="checkbox"/> NAS filer
Apply	
Summary	

< Previous **Next >** Finish Cancel

4. 新增您的認證資料以存取ONTAP 整個叢集。

New NetApp Data ONTAP Storage



Credentials

Specify account with storage administrator privileges.

Name	Credentials: <input type="text" value="HCIEUC\Admin (HCIEUC\Admin, last edited: 98 days ago)"/>	<input type="button" value="Add..."/>
Credentials	Manage accounts	
NAS Filer	Protocol: <input type="text" value="HTTPS"/>	
Apply	Port: <input type="text" value="443"/>	
Summary		

< Previous **Next >** Finish Cancel

5. 在NAS Filer™頁面上、選擇所需的掃描傳輸協定、然後選取Next（下一步）。

New NetApp Data ONTAP Storage ✕

NAS Filer
Specify how this storage can be accessed by file backup jobs.

Name	Protocol to use:
Credentials	<input checked="" type="checkbox"/> SMB
NAS Filer	<input type="checkbox"/> NFS
Apply	<input checked="" type="checkbox"/> Create required export rules automatically
Summary	Volumes to scan:
	All volumes Choose...
	Backup proxies to use:
	Automatic selection Choose...

< Previous
Apply
Finish
Cancel

- 完成精靈的「Apply (套用)」和「Summary (摘要)」頁面、然後按一下「Finish (完成)」開始儲存探索程序。掃描完成後、ONTAP 即可將支援此功能的叢集與NAS檔案管理器一起新增為可用資源。

Add Storage

Edit Storage

Remove Storage

Rescan

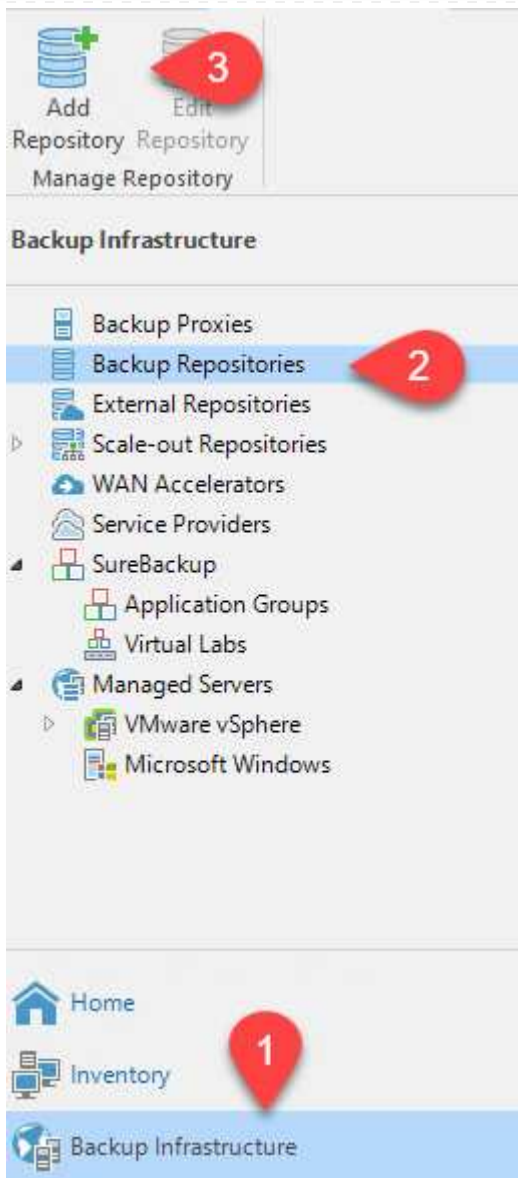
Manage Storage

Actions

Storage Infrastructure

- Storage Infrastructure
 - ONTAP
 - E13A300
 - OTS-HC-Cluster
 - svm_nfs-A
 - svm0
 - iSCSI_Datastore
 - sqldb_vol2
 - sqldb_vol1
 - svm0_root

- 使用新發現的NAS共用區建立備份儲存庫。從備份基礎架構選取備份儲存庫、然後按一下新增儲存庫功能表項目。



8. 請依照「新備份儲存庫精靈」中的所有步驟來建立儲存庫。如需建立Veeam備份儲存庫的詳細資訊、請參閱 "[Veeam文件](#)"。

New Backup Repository



Share

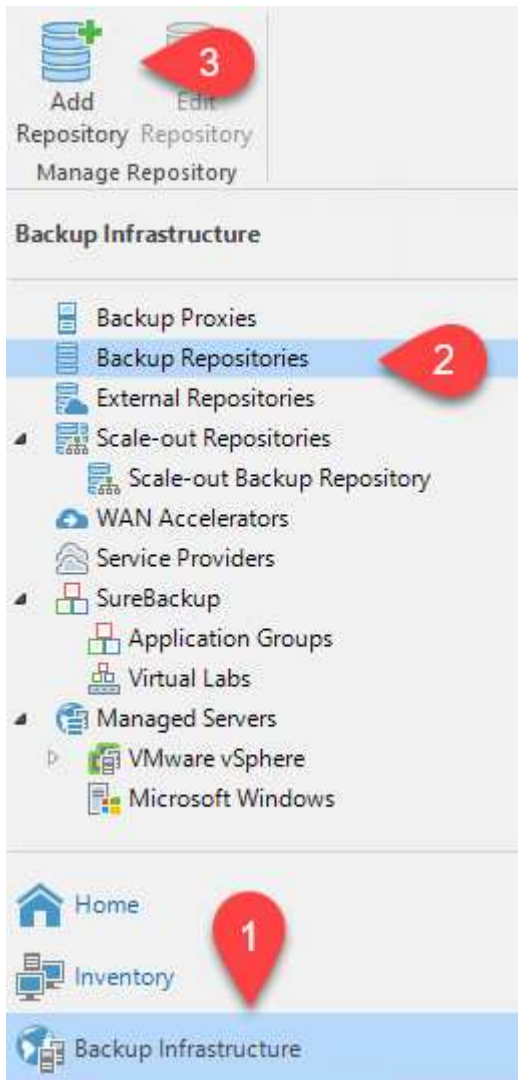
Type in UNC path to share (mapped drives are not supported), specify share access credentials and how backup jobs should write data to this share.

Name	Shared folder:
Share	<input type="text" value="\\172.21.162.181\VBRRepo"/> <input type="button" value="Browse..."/>
Repository	Use <code>\\server\folder format</code>
Mount Server	<input checked="" type="checkbox"/> This share requires access credentials:
Review	<input type="button" value="Key icon"/> <input type="text" value="sddc\administrator (sddc\administrator, last edited: 85 days ago)"/> <input type="button" value="Add..."/>
Apply	Manage accounts
Summary	Gateway server:
	<input checked="" type="radio"/> Automatic selection
	<input type="radio"/> The following server:
	<input type="text" value="veeam.sddc.netapp.com (Backup server)"/>
	Use this option to improve performance and reliability of backup to a NAS located in a remote site.

將Amazon S3儲存庫新增為備份儲存庫

下一步是將Amazon S3儲存設備新增為備份儲存庫。

1. 瀏覽至「備份基礎架構」>「備份儲存庫」。按一下新增儲存庫。



2. 在「新增備份儲存庫」精靈中、選取「物件儲存設備」、然後選取「Amazon S3」。這會啟動「新增物件儲存庫」精靈。

Add Backup Repository

Select the type of backup repository you want to add.



Direct attached storage

Microsoft Windows or Linux server with internal or direct attached storage. This configuration enables data movers to run directly on the server, allowing for fastest performance.



Network attached storage

Network share on a file server or a NAS device. When backing up to a remote share, we recommend that you select a gateway server located in the same site with the share.



Deduplicating storage appliance

Dell EMC Data Domain, ExaGrid, HPE StoreOnce or Quantum DXi. If you are unable to meet the requirements of advanced integration via native appliance API, use the network attached storage option instead.



Object storage

On-prem object storage system or a cloud object storage provider. Object storage can only be used as a Capacity Tier of scale-out backup repositories, backing up directly to object storage is not currently supported.

3. 提供物件儲存庫的名稱、然後按「Next（下一步）」。
4. 在下一節中、提供您的認證資料。您需要AWS存取金鑰和秘密金鑰。

New Object Storage Repository



Account

Specify AWS account to use for connecting to Amazon S3 storage bucket.

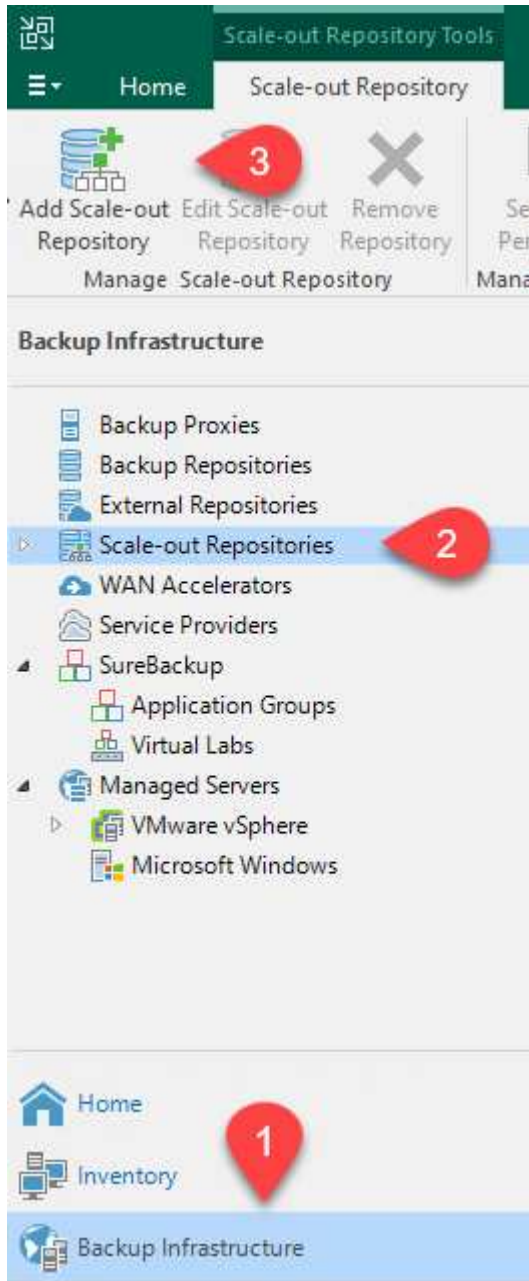
Name	Credentials:
Account	<input type="text" value="AKIAX4H43ZT557HXQT2W (last edited: 107 days ago)"/> Add...
Bucket	Manage cloud accounts
Summary	AWS region:
	<input type="text" value="Global"/>
	<input type="checkbox"/> Use the following gateway server:
	<input type="text" value="veeam.sddc.netapp.com (Backup server)"/>
	Select a gateway server to proxy access to Amazon S3. If no gateway server is specified, all scale-out backup repository extents must have direct Internet access.
	<input type="button" value=" < Previous"/> <input type="button" value=" Next >"/> <input type="button" value=" Finish"/> <input type="button" value=" Cancel"/>

5. Amazon組態載入後、請選擇您的資料中心、儲存庫和資料夾、然後按一下「Apply（套用）」。
- 最後、按一下「完成」以關閉精靈。

建立橫向擴充備份儲存庫

現在我們已將儲存儲存庫新增至Veeam、我們可以建立SOBR、將備份複本自動分層至異地Amazon S3物件儲存設備、以進行災難恢復。

1. 從備份基礎架構選取橫向擴充儲存庫、然後按一下新增橫向擴充儲存庫功能表項目。



2. 在「新增橫向擴充備份儲存庫」中、提供SOBR名稱、然後按「下一步」。
3. 對於效能層、請選擇包含SMB共用的備份儲存庫、該SMB共用位於本機ONTAP 的資訊區叢集上。

New Scale-out Backup Repository



Performance Tier

Select backup repositories to use as the landing zone and for the short-term retention.

Name	Extents:	
Performance Tier	Name	Add...
Placement Policy	VBRRepo2	Remove

4. 針對「放置原則」、請根據您的需求選擇「資料位置」或「效能」。選取「下一步」。
5. 在容量層方面、我們將SOBR延伸至Amazon S3物件儲存設備。為了進行災難恢復、請在建立備份後立即選取「複製備份到物件儲存設備」、以確保我們的次要備份能夠及時交付。

New Scale-out Backup Repository



Capacity Tier

Specify object storage to copy backups to for redundancy and DR purposes. Older backups can be moved to object storage completely to reduce long-term retention costs while preserving the ability to restore directly from offloaded backups.

Name	<input checked="" type="checkbox"/> Extend scale-out backup repository capacity with object storage:
Performance Tier	Amazon S3 Repo Add...
Placement Policy	Define time windows when uploading to capacity tier is allowed Window...
Capacity Tier	<input checked="" type="checkbox"/> Copy backups to object storage as soon as they are created Create additional copy of your backups for added redundancy by having all backups copied to the capacity tier as soon as they are created on the performance tier.
Archive Tier	<input checked="" type="checkbox"/> Move backups to object storage as they age out of the operational restore window Reduce your long-term retention costs by moving older backups to object storage completely while preserving the ability to restore directly from offloaded backups.
Summary	Move backup files older than 14 days (your operational restore window) Override...
	<input type="checkbox"/> Encrypt data uploaded to object storage Password: Add... Manage passwords
	< Previous Next > Finish Cancel

6. 最後、選取「Apply (套用)」和「Finish (完成)」以完成建立SOBR。

建立橫向擴充備份儲存庫工作

設定Veeam的最後步驟、是使用新建立的SOBR作為備份目的地來建立備份工作。建立備工作是何儲存系統管理員的常用程序、我們不在此詳述詳細步驟。如需在Veeam中建立備份工作的完整資訊、請參閱 "[Veeam說明中心技術文件](#)"。

若要將應用程式VM和資料庫Volume容錯移轉至執行於AWS的VMware Cloud Volume服務、您必須同時安裝SnapCenter 並設定執行中的VMware Server和Veeam備份與複寫伺服器執行個體。容錯移轉完成後、您也必須設定這些工具、以便恢復正常的備份作業、直到規劃並執行內部部署資料中心的容錯回復為止。

部署次要Windows SnapCenter 功能伺服器

支援VMware Cloud SDDC部署的VMware伺服器、或安裝在VPC中的EC2執行個體上、並可透過網路連線至VMware Cloud環境。SnapCenter

NetApp支援網站提供支援軟體、可安裝在位於網域或工作群組的Microsoft Windows系統上。SnapCenter如需詳細的規劃指南和安裝指示、請參閱 "[NetApp文件中心](#)"。

您可以在找到SnapCenter 該軟件 "[此連結](#)"。

設定次要Windows SnapCenter 靜態伺服器

若要還原鏡射至FSXS庫ONTAP 的應用程式資料、您必須先執行內部部署SnapCenter 的整套還原資料庫。完成此程序後、將重新建立與VM的通訊、並使用FSX還原ONTAP 做為主要儲存設備來恢復應用程式備份。

若要達成此目標、您必須在SnapCenter 的努力伺服器上完成下列項目：

1. 將電腦名稱設定為與原始內部部署SnapCenter 的內部部署伺服器相同。
2. 設定網路功能、以便與VMware Cloud和FSX ONTAP 支援例項進行通訊。
3. 完成還原SnapCenter 整套程序以還原整個資料庫。
4. 確認SnapCenter 支援功能為災難恢復模式、以確保FSX現在是備份的主要儲存設備。
5. 確認已與還原的虛擬機器重新建立通訊。

部署次要Veeam備份與擴大機；複寫伺服器

您可以將Veeam備份與複寫伺服器安裝在AWS或EC2執行個體上VMware Cloud的Windows伺服器上。如需詳細的實作指南、請參閱 "[Veeam說明中心技術文件](#)"。

設定次要Veeam備份與擴大機；複寫伺服器

若要還原已備份至Amazon S3儲存設備的虛擬機器、您必須在Windows伺服器上安裝Veeam伺服器、並將其設定為與VMware Cloud、FNSX ONTAP 及包含原始備份儲存庫的S3儲存庫進行通訊。此外、還必須在FSX ONTAP 更新上設定新的備份儲存庫、以便在VM還原後進行新的備份。

若要執行此程序、必須完成下列項目：

1. 設定網路功能、以便與VMware Cloud、FSX ONTAP 功能區及內含原始備份儲存庫的S3儲存區進行通訊。
2. 將FSXSf2 ONTAP 上的SMB共用區設定為新的備份儲存庫。
3. 將原本作為橫向擴充備份儲存庫一部分的S3儲存庫掛載到內部部署。
4. 還原VM之後、請建立新的備份工作來保護SQL和Oracle VM。

如需使用Veeam還原VM的詳細資訊、請參閱一節 "[使用Veeam完整還原還原應用程式VM](#)"。

適用於災難恢復的資料庫備份SnapCenter

支援基礎MySQL資料庫及組態資料的備份與還原、以便在發生災難時恢復該伺服器。SnapCenter SnapCenter就我們的解決方案而言、我們在SnapCenter VPC內的AWS EC2執行個體上恢復了該資料庫和組態。如需此步驟的詳細資訊、請參閱 "[此連結](#)"。

支援需求SnapCenter

下列先決條件是SnapCenter 進行資訊備份所需的條件：

- 在內部部署ONTAP 的支援系統上建立一個Volume和SMB共用區、以找出備份的資料庫和組態檔案。
- 內部部署ONTAP 的SnapMirror系統與AWS帳戶中的FSX或CVO之間的SnapMirror關係。此關係用於傳輸包含備份SnapCenter 的還原資料庫和組態檔案的快照。
- 安裝在雲端帳戶的Windows Server、可安裝在EC2執行個體或VMware Cloud SDDC的VM上。
- 安裝在Windows EC2執行個體或VMware Cloud VM上的SnapCenter

支援備份與還原程序摘要SnapCenter

- 在內部部署ONTAP 的內部系統上建立一個磁碟區、以裝載備份資料庫和組態檔案。
- 在內部部署與FSx/CVO之間建立SnapMirror關係。
- 掛載SMB共用區。
- 擷取Swagger授權權杖以執行API工作。
- 啟動資料庫還原程序。
- 使用xcopy公用程式將資料庫和組態檔案本機目錄複製到SMB共用區。
- 在FSX上、建立ONTAP 一個Clone of the Sf2 Volume（透過內部部署的SnapMirror複製）。
- 將SMB共用區從FSX掛載至EC2/VMware Cloud。
- 將還原目錄從SMB共用複製到本機目錄。
- 從Swagger執行SQL Server還原程序。

支援執行REST API命令的Web用戶端介面。SnapCenter如需透過Swagger存取REST API的相關資訊、請參閱SnapCenter 上的《》文件 ["此連結"](#)。

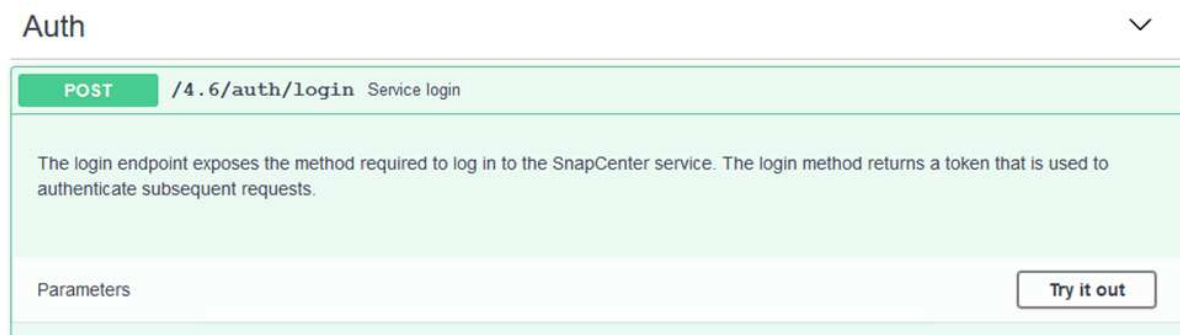
登入Swagger並取得授權權杖

瀏覽至Swagger頁面後、您必須擷取授權權杖、才能啟動資料庫還原程序。

1. 請至SnapCenter https://<SnapCenter伺服器IP:8146/swagger/_存取《Seswagger API》網頁。



2. 展開「驗證」區段、然後按一下「試用」。



3. 在UserOperationContext區域中、填入SnapCenter「資訊」認證和角色、然後按一下「執行」。

Name	Description
TokenNeverExpires	Token never expires
boolean (query)	<input type="text" value="false"/>
UserOperationContext * required	User credentials
object (body)	<div style="border: 1px solid #ccc; padding: 5px;"> Edit Value Model <pre> { "UserOperationContext": { "User": { "Name": "localhost\\scadmin", "Passphrase": "NetApp321", "Rolename": "SnapCenterAdmin" } } } </pre> </div>
	<input type="button" value="Cancel"/>
	Parameter content type <input type="text" value="application/json"/>
<input type="button" value="Execute"/>	

4. 在下方的「回應」本文中、您可以看到權杖。執行備份程序時、請複製權杖文字以進行驗證。

200 Response body

```

{
  "PluginName": null,
  "HostId": 0,
  "RoleId": null,
  "JobIds": null
},
"User": {
  "Token": "KlYxOg==tsV6EOdttdAmAYpe8q5SG6wcoGaSjwHE6jrNy5CsY63HRQ5LkoZLIESRNAhpGJJ0UUQynEMdgtVGDZnvx+I/ZJZIn5MINZrj6CLfGTApplGmcagT08bqb5kMTx07EcdRAidzAXUDb3GyLQKtW0GdwKzSeUwKj3uVupnk1E31skK6PRBv9RS8j0qHQvo4v4RL0hhThwFhV9/23nFeJVP/p1Ev4vrV/zeZVTUHFPHUM069XRe5cuW9nwyj4b0I5Y5FN3XDkjq=",
  "Name": "SCAdmin",
  "TokenHashed": null,
  "Type": "",
  "TokenTime": "2022-03-22T14:21:57.3665661-07:00",
  "Id": "1",
  "FullName": "SCAdmin",
  "Host": null,
  "Author": null,
  "UserName": "",
  "Domain": "",
  "Passphrase": ""
}

```

執行SnapCenter 資料庫的還原備份

接下來前往Swagger頁面上的Disaster Recovery區域、開始SnapCenter 執行VMware還原程序。

1. 按一下「Disaster Recovery（災難恢復）」區域即可展開。

The screenshot shows the 'Disaster Recovery' section of the Swagger API interface. It lists five endpoints:

- GET** `/4.6/disasterrecovery/server/backup` Fetch all the existing SnapCenter Server DR Backups.
- POST** `/4.6/disasterrecovery/server/backup` Starts the SnapCenter Server DR backup.
- DELETE** `/4.6/disasterrecovery/server/backup` Deletes the existing Snapcenter DR backup.
- POST** `/4.6/disasterrecovery/server/restore` Starts SnapCenter Server Restore.
- POST** `/4.6/disasterrecovery/storage` Enable or disable the storage disaster recovery.

2. 展開「/4.6/dissterrecovery /server/Backup」區段、然後按一下「Try it out（試用）」。

The screenshot shows the 'Try it out' button for the `/4.6/disasterrecovery/server/backup` endpoint. The button is labeled 'Try it out' and is located in the bottom right corner of the endpoint's details panel. The panel also contains the text: 'Starts and creates a new SnapCenter Server DR backup.' and a 'Parameters' section.

3. 在「SmDRBackup Request」區段中、新增正確的本機目標路徑、然後選取「執行」以開始SnapCenter 備份整個過程中的資料庫和組態。

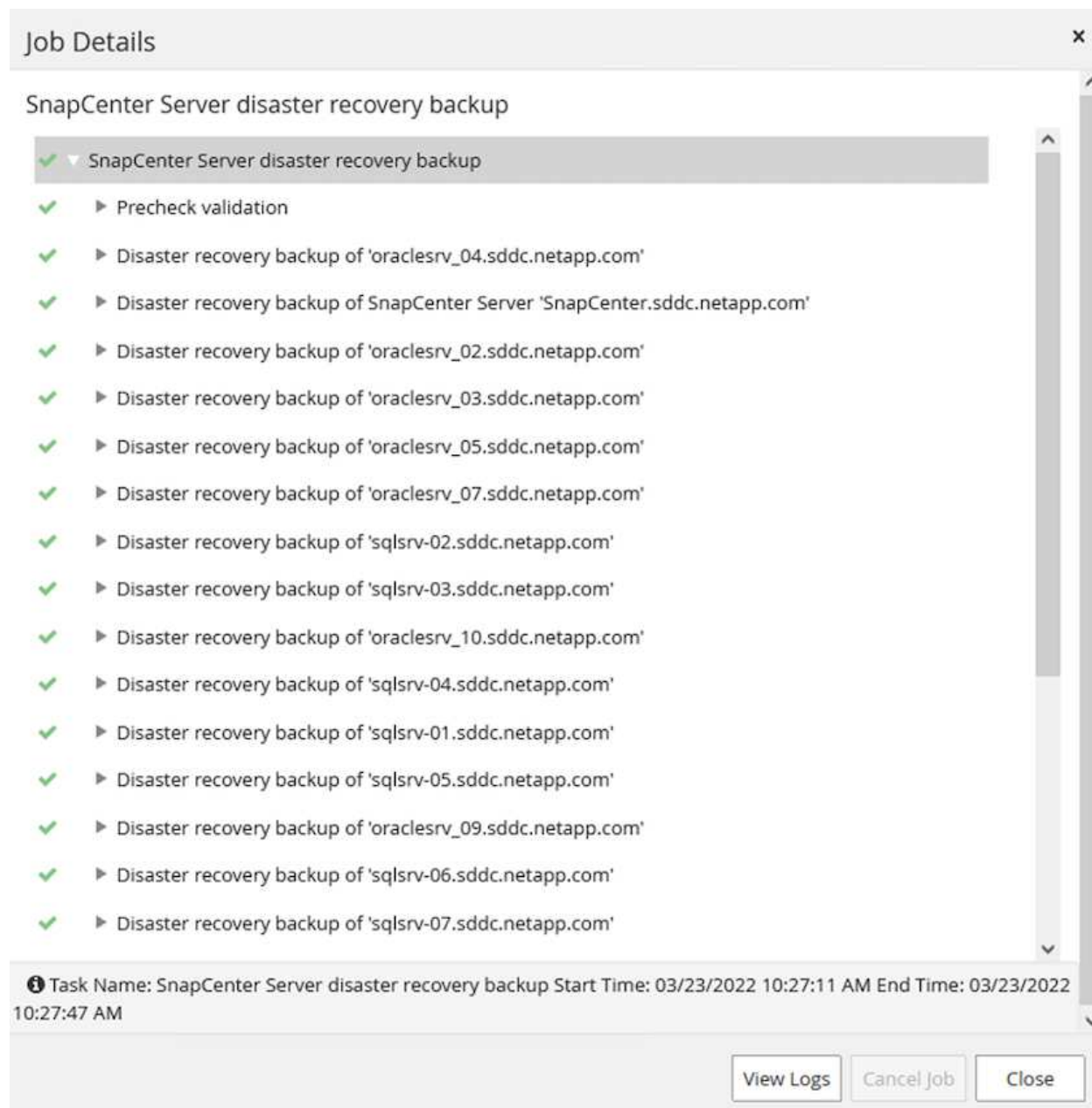


備份程序不允許直接備份到NFS或CIFS檔案共用區。

Name	Description
Token * required string (header)	User authorization token <input data-bbox="584 231 1023 283" type="text" value="TUHFHUM069XRe5cuW9nwyj4b0I5Y5FN3XDkjQ=="/>
SmDRBackupRequest * required object (body)	Parameters to take Backup <div data-bbox="576 378 1404 787"><p>Edit Value Model</p><pre>{ "TargetPath": "C:\\\\SnapCenter_Backups\\" }</pre></div> <div data-bbox="576 798 885 934"><input type="button" value="Cancel"/> Parameter content type <input type="text" value="application/json"/></div>

從SnapCenter 無法監控備份工作

登入SnapCenter 功能以在開始資料庫還原程序時檢閱記錄檔。在「Monitor (監控)」區段下、您可以檢視SnapCenter 有關支援伺服器災難恢復備份的詳細資料。



The screenshot shows a 'Job Details' window for a SnapCenter Server disaster recovery backup. The job is completed successfully, as indicated by green checkmarks next to each step. The steps include a precheck validation and 15 individual disaster recovery backups for various servers. At the bottom, there is a task summary bar with the task name, start and end times, and three buttons: 'View Logs', 'Cancel Job', and 'Close'.

Job Details

SnapCenter Server disaster recovery backup

- ✓ SnapCenter Server disaster recovery backup
 - ✓ ▶ Precheck validation
 - ✓ ▶ Disaster recovery backup of 'oraclesrv_04.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of SnapCenter Server 'SnapCenter.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'oraclesrv_02.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'oraclesrv_03.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'oraclesrv_05.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'oraclesrv_07.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'sqlsrv-02.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'sqlsrv-03.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'oraclesrv_10.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'sqlsrv-04.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'sqlsrv-01.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'sqlsrv-05.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'oraclesrv_09.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'sqlsrv-06.sddc.netapp.com'
 - ✓ ▶ Disaster recovery backup of 'sqlsrv-07.sddc.netapp.com'

i Task Name: SnapCenter Server disaster recovery backup Start Time: 03/23/2022 10:27:11 AM End Time: 03/23/2022 10:27:47 AM

[View Logs](#) [Cancel Job](#) [Close](#)

使用XCOPY公用程式將資料庫備份檔案複製到SMB共用區

接下來、您必須將備份從SnapCenter 位於支援服務器上的本機磁碟機移至CIFS共用區、以便SnapMirror將資料複製到位於AWS FSX執行個體上的次要位置。使用xcopy搭配保留檔案權限的特定選項。

以系統管理員身分開啟命令提示字元。在命令提示字元中輸入下列命令：

```
xcopy <Source_Path> \\<Destination_Server_IP>\<Folder_Path> /O /X  
/E /H /K  
xcopy c:\SC_Backups\SnapCenter_DR \\10.61.181.185\snapcenter_dr /O  
/X /E /H /K
```

容錯移轉

災難發生在主站台

如果發生在一線內部部署資料中心的災難、我們的案例包括使用AWS上的VMware Cloud、將容錯移轉到位於Amazon Web Services基礎架構上的二線站台。我們假設虛擬機器和內部部署ONTAP 的VMware叢集已無法再存取。此外SnapCenter、無法再存取VMware和Veeam虛擬機器、而且必須在我們的次要站台上重建。

本節說明將基礎架構容錯移轉至雲端、並涵蓋下列主題：

- 還原資料庫。SnapCenter建立新SnapCenter 的支援伺服器之後、請還原MySQL資料庫和組態檔案、並將資料庫切換為災難恢復模式、以便次要FSX儲存設備成為主要儲存設備。
- 使用Veeam備份與複寫還原應用程式虛擬機器。連接內含VM備份的S3儲存設備、匯入備份、然後將其還原至AWS上的VMware Cloud。
- 使用SnapCenter 支援功能還原SQL Server應用程式資料。
- 使用SnapCenter 支援功能還原Oracle應用程式資料。

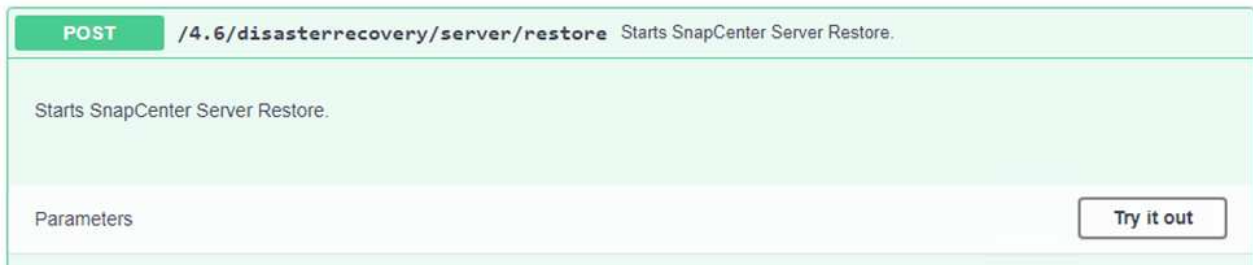
支援災難恢復案例、可備份及還原MySQL資料庫和組態檔案。SnapCenter這可讓管理員在SnapCenter 內部部署資料中心維持對該資料庫的定期備份、並於稍後將該資料庫還原至次要SnapCenter 的還原資料庫。

若要存取SnapCenter 遠端SnapCenter 還原伺服器上的還原備份檔案、請完成下列步驟：

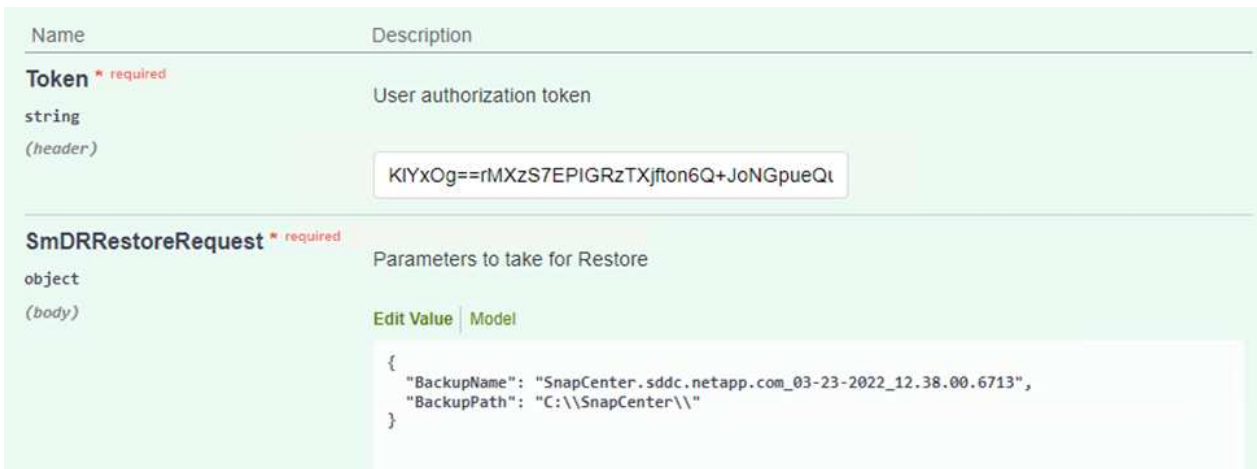
1. 中斷來自FSX叢集的SnapMirror關係、這會使磁碟區變成讀取/寫入。
2. 建立CIFS伺服器（如有必要）、並建立CIFS共用區、指向複製Volume的交會路徑。
3. 使用xcopy將備份檔案複製到二線SnapCenter 版的本機目錄。
4. 安裝SnapCenter vsv4.6。
5. 請確保SnapCenter 該伺服器的FQDN與原始伺服器相同。若要成功還原資料庫、就必須執行此動作。

若要開始還原程序、請完成下列步驟：

1. 瀏覽至次要SnapCenter 版伺服器的Swagger API網頁、並依照先前的指示取得授權權杖。
2. 瀏覽至Swagger頁面的Disaster Recovery（災難恢復）區段、選取「/4.6/disasterrecovery / server/recovery」（/4.6/disasterrecovery /伺服器/還原）、然後按一下「Try it out（試用）」。



3. 貼上您的授權權杖、然後在「SmDRResterRequest」區段中、貼上備份名稱和次要SnapCenter 伺服器上的本機目錄。



4. 選取「執行」按鈕以開始還原程序。
5. 從功能區塊瀏覽至「監控」區段、以檢視還原工作的進度。SnapCenter

NetApp SnapCenter®

Jobs Schedules Events Logs

search by name

Jobs - Filter

ID	Status	Name
20482	✓	SnapCenter Server Disaster Recovery
20481	✓	SnapCenter Server disaster recovery backup
20480	✗	SnapCenter Server disaster recovery backup
20475	✓	Backup of Resource Group 'SQLSRV-09' with policy 'SQL-Hourly'
20474	✓	Backup of Resource Group 'SQLSRV-05' with policy 'SQL-Hourly'
20473	🔄	Backup of Resource Group 'OracleSrv_06' with policy 'Oracle-Hourly'
20472	✗	SnapCenter Server disaster recovery backup

Job Details

SnapCenter Server Disaster Recovery

- ✓ ▼ SnapCenter Server Disaster Recovery
- ✓ ▼ Prepare for restore job
- ✓ ▼ Precheck validation
- ✓ ▼ Saving original server state
- ✓ ▼ Schedule restore
- ✓ ▼ Repository restore
- ✓ ▼ Config restore
- ✓ ▼ Reset MySQL password

6. 若要從二線儲存設備啟用SQL Server還原、您必須將SnapCenter 此還原資料庫切換為「災難恢復」模式。這是以個別作業的形式執行、並在Swagger API網頁上啟動。
 - a. 瀏覽至「Disaster Recovery (災難恢復)」區段、然後按一下「/4.6/dissterrecovery / storage (/4.6/disstersterrecovery
 - b. 貼入使用者授權權杖。
 - c. 在SmSetDissterRecoverySettingsRequest區段中、將「EnablDisasterRecover」變更為「true」。
 - d. 按一下「執行」以啟用SQL Server的災難恢復模式。

Name	Description				
Token * required string (header)	User authorization token <div style="border: 1px solid #ccc; padding: 2px;">KIYxOg==rMXzS7EPIGRzTXjfton6Q+JoNGpueQt</div>				
SmSetDisasterRecoverySettingsRequest * required object (body)	Parameters to enable or disable the DR mode <div style="border: 1px solid #ccc; padding: 2px;"> <table border="0"> <tr> <td style="border-right: 1px solid #ccc; padding-right: 5px;">Edit Value</td> <td>Model</td> </tr> <tr> <td colspan="2" style="padding: 5px;"> <pre>{ "EnableDisasterRecovery": true }</pre> </td> </tr> </table> </div>	Edit Value	Model	<pre>{ "EnableDisasterRecovery": true }</pre>	
Edit Value	Model				
<pre>{ "EnableDisasterRecovery": true }</pre>					



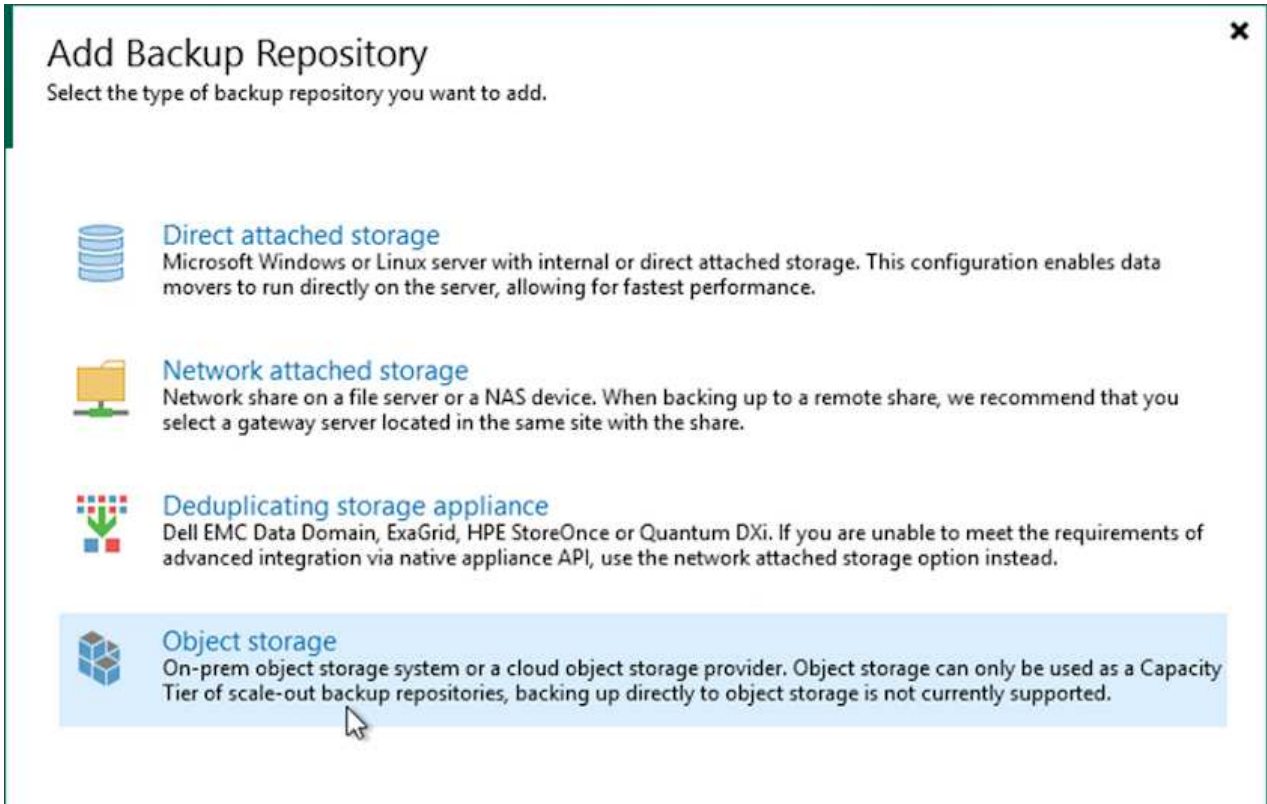
請參閱其他程序的相關意見。

使用Veeam完整還原還原應用程式VM


從次要Veeam伺服器、從S3儲存設備匯入備份、並將SQL Server和Oracle VM還原至VMware Cloud叢集。

若要從內部部署橫向擴充備份儲存庫中的S3物件匯入備份、請完成下列步驟：

1. 移至「備份儲存庫」、然後按一下上方功能表中的「新增儲存庫」、以啟動「新增備份儲存庫」精靈。在精靈的第一頁、選取「物件儲存」作為備份儲存庫類型。








2. 選取「Amazon S3」作為「物件儲存類型」。




Object Storage

Select the type of object storage you want to use as a backup repository.




- **S3 Compatible**
Adds an on-premises object storage system or a cloud object storage provider.
- **Amazon S3**
Adds Amazon cloud object storage. Amazon S3, Amazon S3 Glacier (including Deep Archive) and Amazon Snowball Edge are supported.
- **Google Cloud Storage**
Adds Google Cloud storage. Both Standard and Nearline storage classes are supported.
- **IBM Cloud Object Storage**
Adds IBM Cloud object storage. S3 compatible versions of both on-premises and IBM Cloud storage offerings are supported.
- **Microsoft Azure Storage**
Adds Microsoft Azure cloud object storage. Microsoft Azure Blob Storage, Microsoft Azure Archive Storage and Microsoft Azure Data Box are supported.

3. 從Amazon Cloud Storage Services清單中、選取Amazon S3。




Amazon Cloud Storage Services

Select the type of Amazon storage you want to use as a backup repository.

- **Amazon S3**
Adds Amazon S3 storage. Both Standard and Infrequent Access (IA) storage classes are supported.
- **Amazon S3 Glacier**
Adds Amazon S3 Glacier storage. Both Amazon S3 Glacier and Glacier Deep Archive are supported.
- **AWS Snowball Edge**
Adds AWS Snowball Edge appliance to enable seeding of backups into Amazon S3 object storage.

4. 從下拉式清單中選取預先輸入的認證資料、或新增認證資料以存取雲端儲存資源。按一下「下一步」繼續。

New Object Storage Repository ×

 **Account**
Specify AWS account to use for connecting to Amazon S3 storage bucket.

Name	Credentials:
Account	<input type="text" value="AKIA4H43ZT53YJXPY2Y (last edited: 33 days ago)"/> Add...
Bucket	Manage cloud accounts
Summary	AWS region: <input type="text" value="Global"/>


Use the following gateway server:

Select a gateway server to proxy access to Amazon S3. If no gateway server is specified, all scale-out backup repository extents must have direct Internet access.

< Previous Next > Finish Cancel

5. 在「時段」頁面上、輸入資料中心、時段、資料夾及任何所需選項。按一下套用。

New Object Storage Repository ✕

 **Bucket**
Specify Amazon S3 bucket to use.

Name	Data center: US East (N. Virginia) ▼
Account	Bucket: ehcveeamrepo Browse...
Bucket	Folder: RTP Browse...
Summary	<input type="checkbox"/> Limit object storage consumption to: 10 ▼ TB ▼ This is a soft limit to help control your object storage spend. If the specified limit is exceeded, already running backup offload tasks will be allowed to complete, but no new tasks will be started.
	<input type="checkbox"/> Make recent backups immutable for: 30 ▼ days Protects backups from modification or deletion by ransomware, hackers or malicious insiders using native object storage capabilities.
	<input type="checkbox"/> Use infrequent access storage class (may result in higher costs) With lower price per GB but higher retrieval and early deletion fees, this storage class is best suited for long-term storage of GFS full backups. Avoid using it for short-term storage of recent backups.
	<input type="checkbox"/> Store backups in a single availability zone (even lower price per GB, reduced resilience)

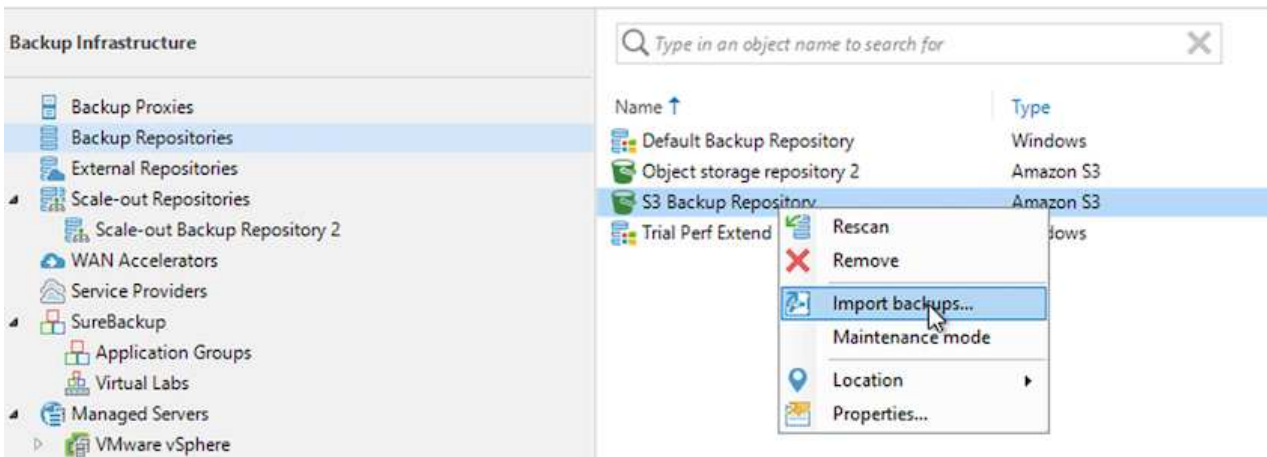
< Previous Apply Finish Cancel

6. 最後、選取「完成」以完成程序並新增儲存庫。

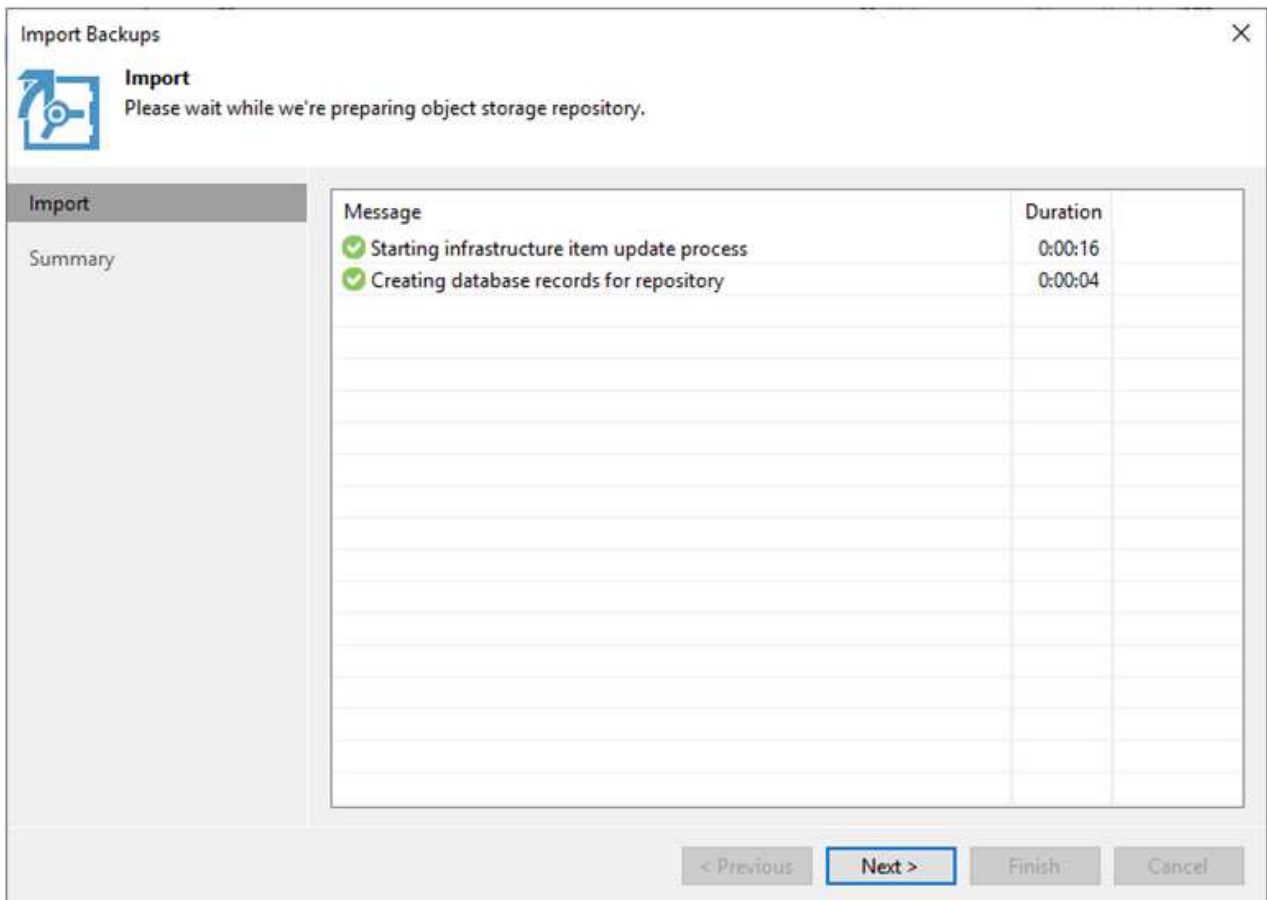
從S3物件儲存設備匯入備份

若要從上一節新增的S3儲存庫匯入備份、請完成下列步驟。

1. 從S3備份儲存庫選取匯入備份、以啟動匯入備份精靈。



2. 建立匯入的資料庫記錄之後、請在摘要畫面中選取「Next (下一步)」、然後選取「Finish (完成)」、開始匯入程序。



3. 匯入完成後、您可以將VM還原至VMware Cloud叢集。

System



Name: **Configuration Database Resynchr...** Status: **Success**
Action type: Configuration Resynchronize Start time: 4/6/2022 3:01:30 PM
Initiated by: EC2AMAZ-3POTKQV\vdadmin End time: 4/6/2022 3:04:57 PM

Log

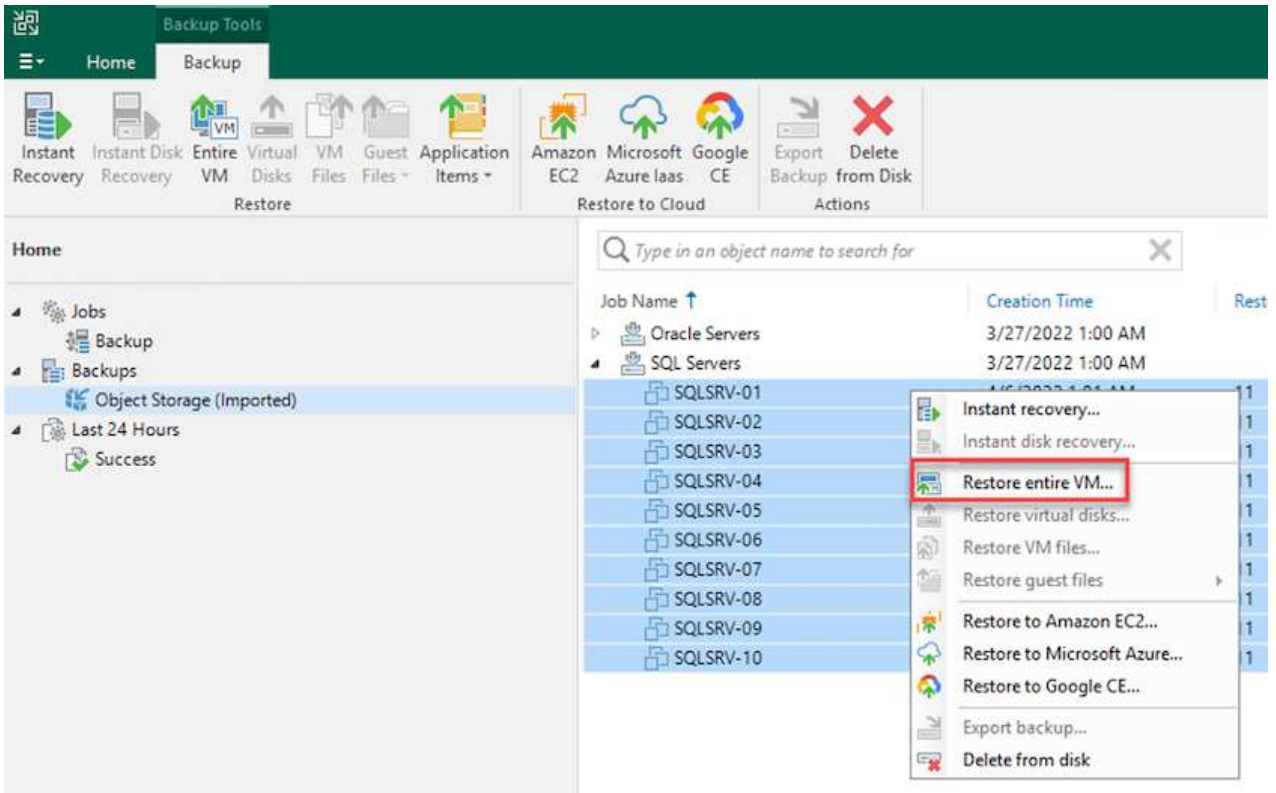
Message	Duration
✔ Starting backup repositories synchronization	
✔ Enumerating repositories	
✔ Found 1 repository	
✔ Processing capacity tier extent of S3 Backup Repository 2	0:03:23
✔ S3 Backup Repository: added 2 unencrypted	0:03:20
✔ Importing backup 2 out of 2	0:03:15
✔ Backup repositories synchronization completed successfully	

Close

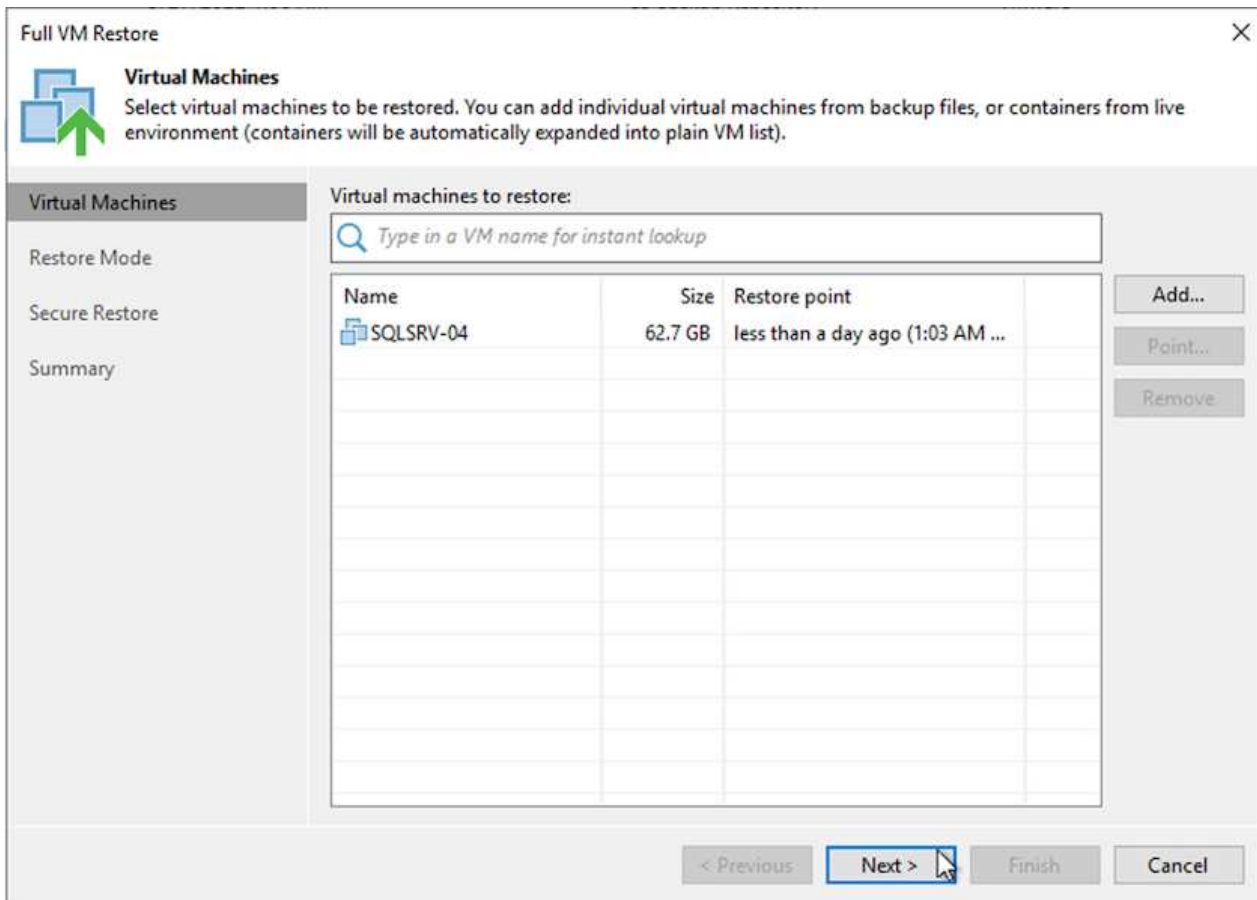
使用Veeam完整還原將應用程式VM還原至VMware Cloud

若要將SQL和Oracle虛擬機器還原至AWS工作負載網域/叢集上的VMware Cloud、請完成下列步驟。

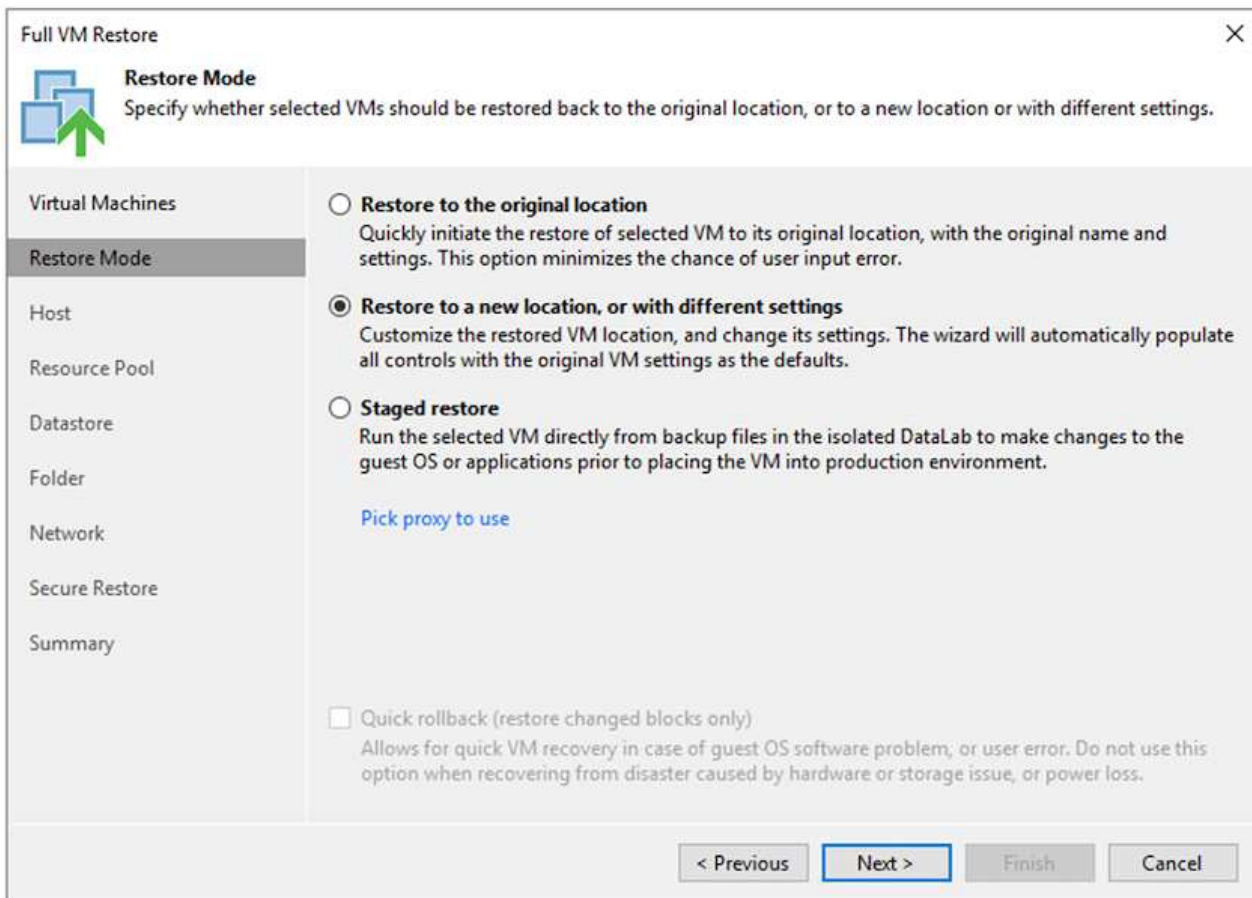
1. 在Veeam首頁中、選取包含匯入備份的物件儲存設備、選取要還原的VM、然後按一下滑鼠右鍵並選取「還原整個VM」。



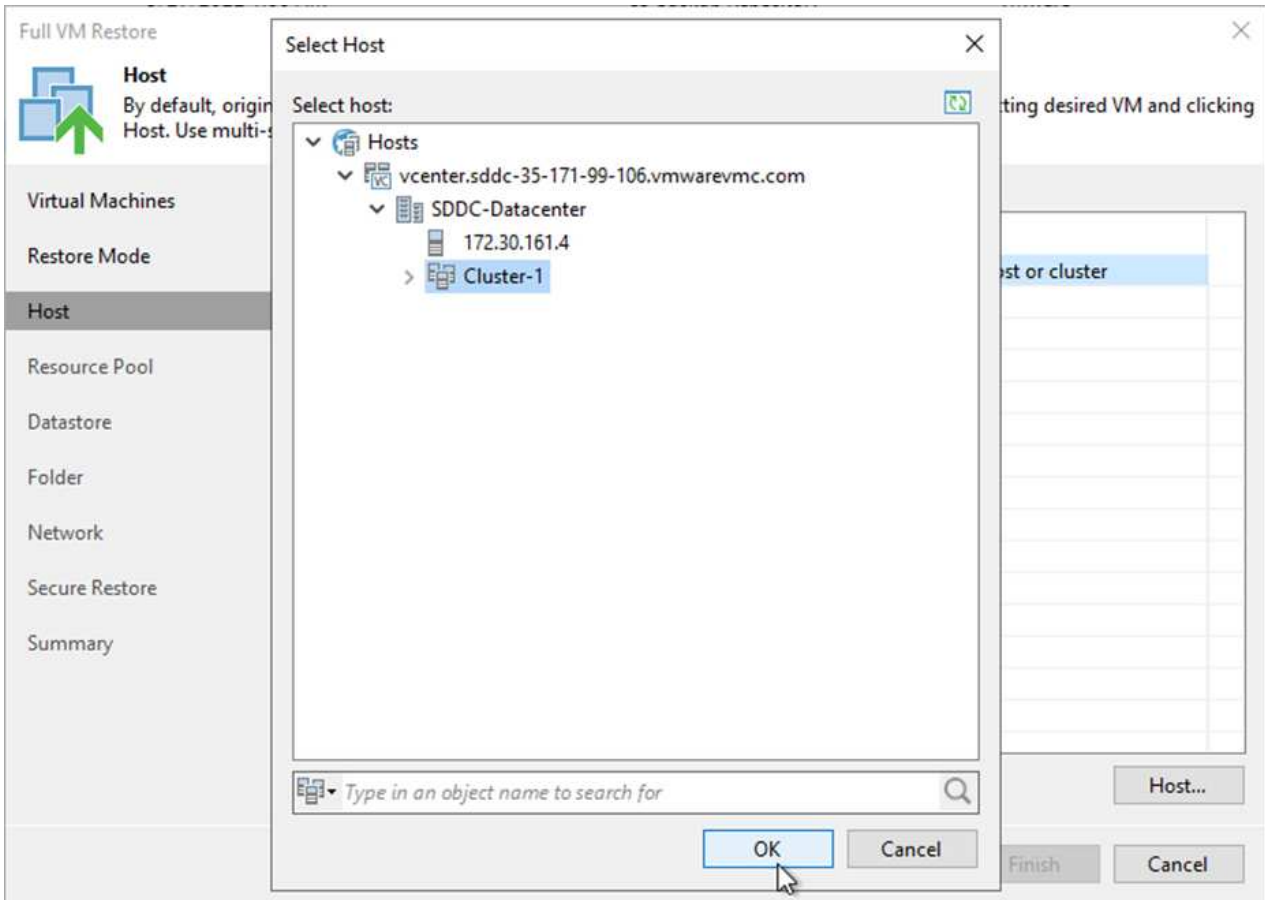
2. 在完整VM還原精靈的第一頁、視需要修改要備份的VM、然後選取「Next (下一步)」。



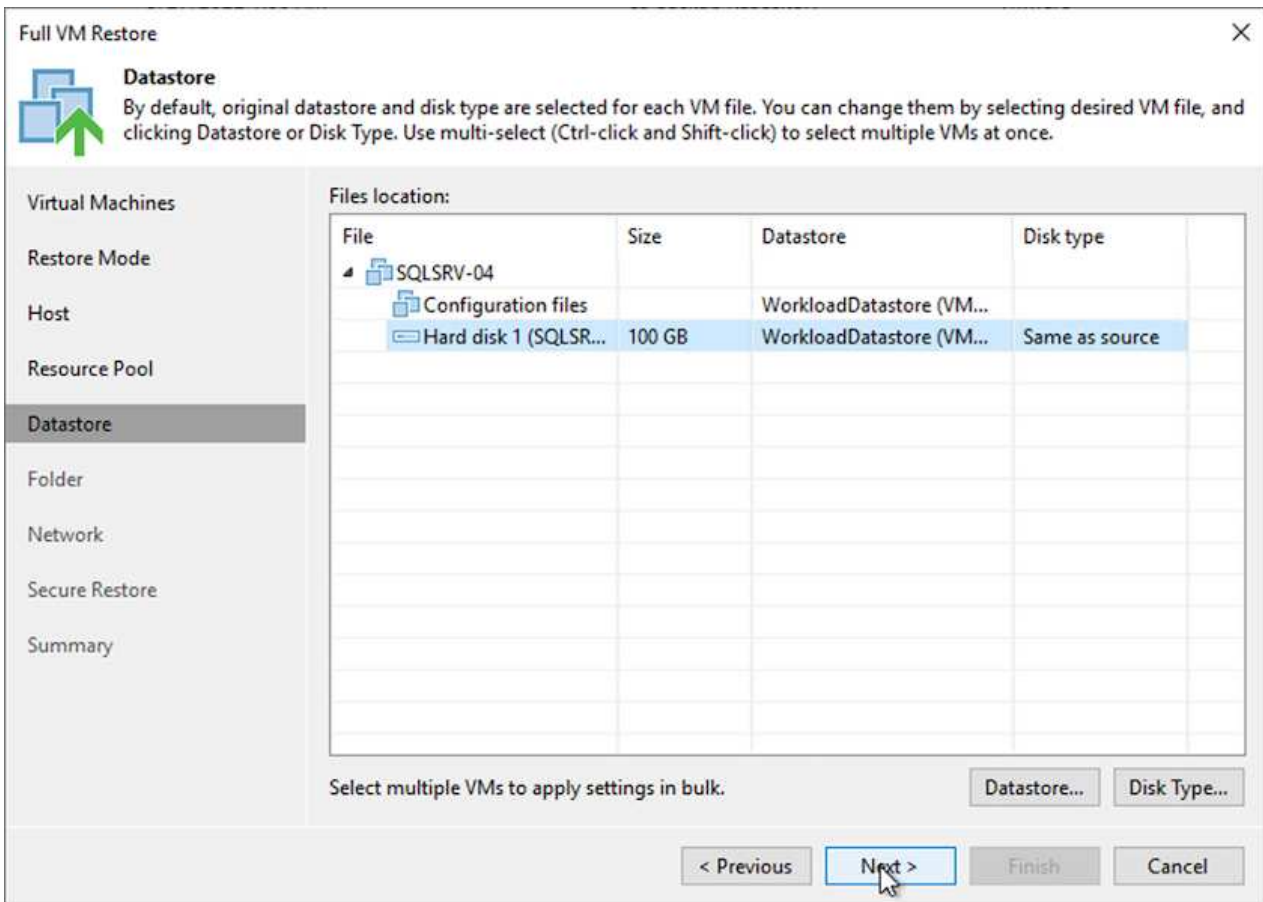
3. 在「還原模式」頁面上、選取「還原至新位置」或「使用不同的設定」。



4. 在主機頁面上、選取要還原VM的目標ESXi主機或叢集。



5. 在「資料存放區」頁面上、選取組態檔和硬碟的目標資料存放區位置。



- 在「網路」頁面上、將VM上的原始網路對應到新目標位置的網路。



Network

By default, we will connect the restored VM to the same virtual networks as the original VM. If you are restoring to a different location, specify how networks map between original and new locations.

Virtual Machines

Restore Mode

Host

Resource Pool

Datastore

Folder

Network

Secure Restore

Summary

Network connections:

Source	Target
SQLSRV-04	
Management 181 (DSwitch)	Not connected
Data - A - 3374 (DSwitch)	Not connected
Data - B - 3375 (DSwitch)	Not connected

Select multiple VMs to apply settings change in bulk.

Network...

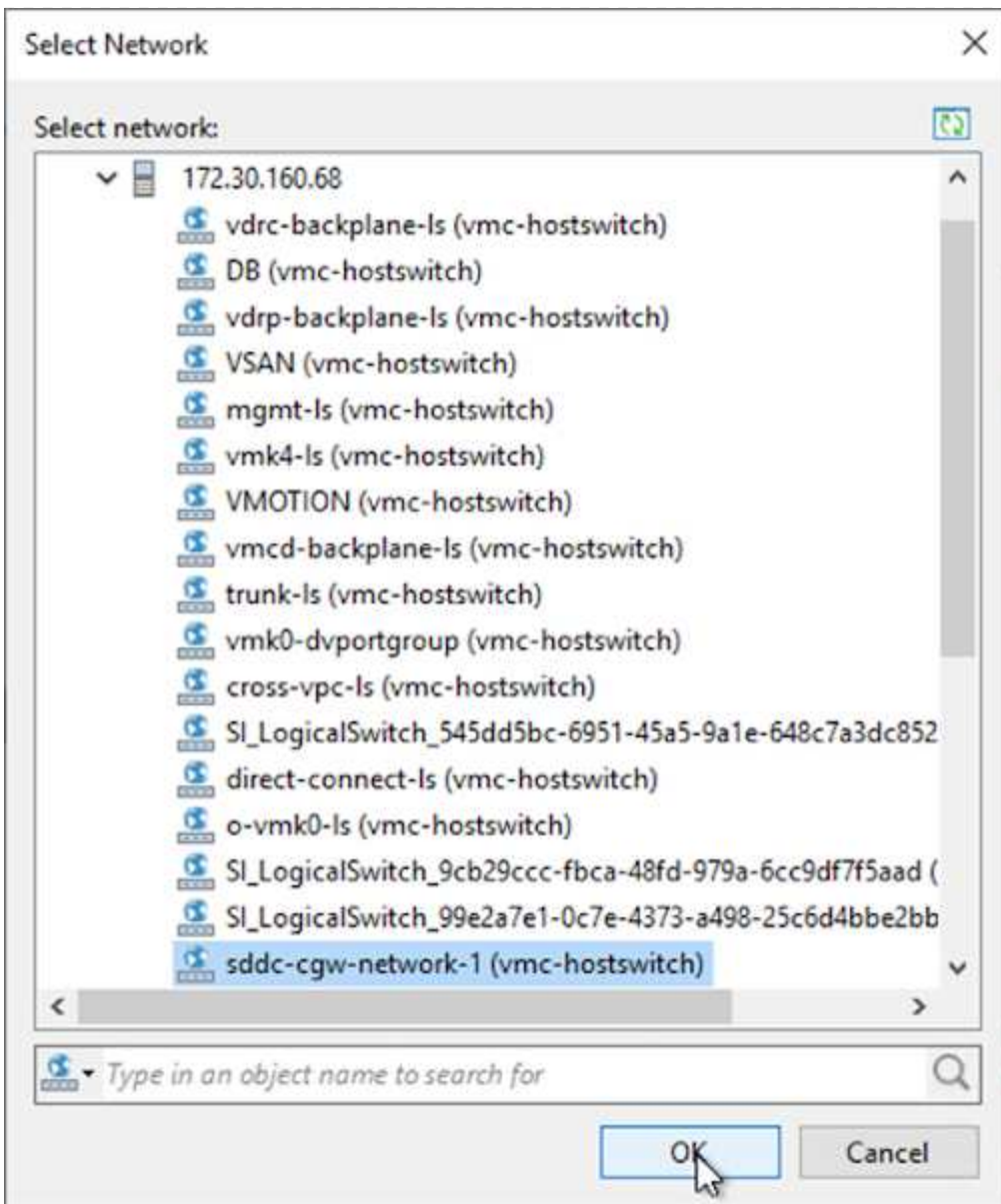
Disconnect

< Previous

Next >

Finish

Cancel



7. 選取是否掃描還原的VM以尋找惡意軟體、檢閱摘要頁面、然後按一下「Finish（完成）」以開始還原。

還原SQL Server應用程式資料

下列程序提供如何在發生導致內部部署站台無法運作的災難時、在AWS的VMware Cloud Services中還原SQL Server的指示。

為了繼續執行恢復步驟、假設您已完成下列先決條件：

1. Windows Server VM已使用Veeam完整還原還原至VMware Cloud SDDC。
2. 我們SnapCenter 已建立次要的伺服器、SnapCenter 並已使用一節中所述的步驟完成還原資料庫和組態設定"[支援備份與還原程序摘要。SnapCenter](#)"

VM：SQL Server VM的還原後組態

在VM還原完成後、您必須設定網路和其他項目、以便重新探索SnapCenter 位於支援中心內的主機VM。

1. 指派新的IP位址給管理、iSCSI或NFS。
2. 將主機加入Windows網域。
3. 將主機名稱新增至DNS或SnapCenter 到伺服器上的主機檔案。



如果SnapCenter 使用與目前網域不同的網域認證來部署這個程式、您就必須變更SQL Server VM上適用於Windows Service外掛程式的登入帳戶。變更登入帳戶後、請重新啟動SnapCenter 適用於Windows的WESTSMCore、外掛程式和適用於SQL Server服務的外掛程式。



若要自動重新探索SnapCenter 還原的虛擬機器、FQDN必須與原先新增至SnapCenter 內部部署的虛擬機器相同。

設定FSX儲存設備以進行SQL Server還原

若要完成SQL Server VM的災難恢復還原程序、您必須中斷現有的SnapMirror與FSX叢集之間的關係、並授予對該磁碟區的存取權。若要這麼做、請完成下列步驟。

1. 若要中斷SQL Server資料庫和記錄磁碟區的現有SnapMirror關係、請從FSXCLI執行下列命令：

```
FSx-Dest::> snapmirror break -destination-path DestSVM:DestVolName
```

2. 建立包含SQL Server Windows VM iSCSI IQN的啟動器群組、以授予LUN存取權：

```
FSx-Dest::> igroup create -vserver DestSVM -igroup igroupName  
-protocol iSCSI -ostype windows -initiator IQN
```

3. 最後、將LUN對應至您剛建立的啟動器群組：

```
FSx-Dest::> lun mapping create -vserver DestSVM -path LUNPath igroup  
igroupName
```

4. 若要尋找路徑名稱、請執行「LUN show」命令。

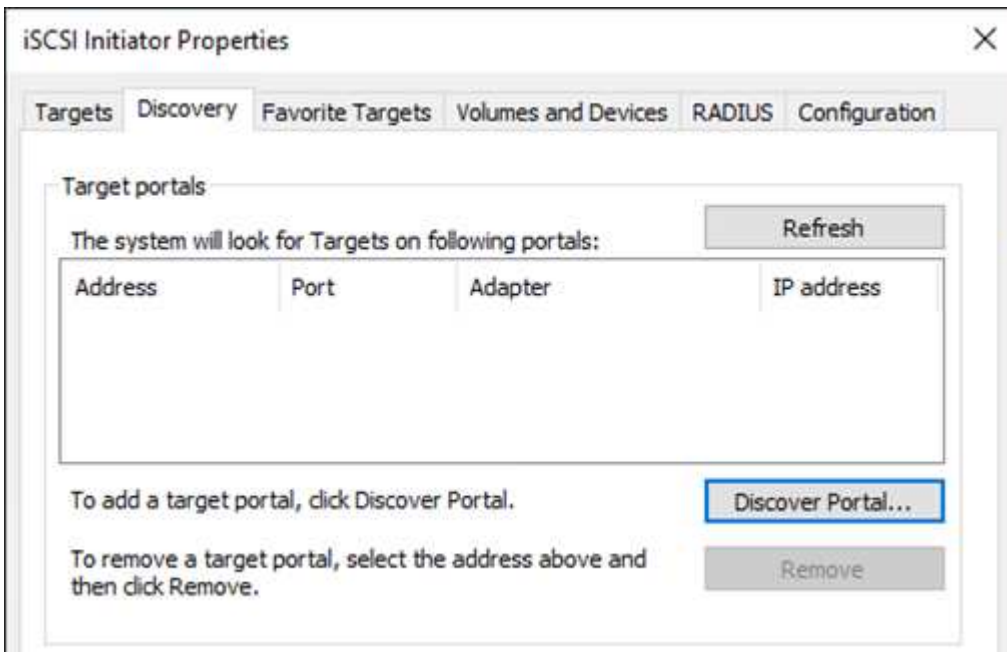
設定Windows VM以進行iSCSI存取、並探索檔案系統

1. 在SQL Server VM中、設定iSCSI網路介面卡、以便在已建立連線至FSX執行個體上iSCSI目標介面的VMware連接埠群組上進行通訊。
2. 開啟iSCSI啟動器內容公用程式、並清除「Discovery」（探索）、「Favorite Target」（最愛目標）和「Target」（目標）索引標籤上的舊連線設定。
3. 找到用於存取FSX執行個體/叢集上iSCSI邏輯介面的IP位址。這可在AWS主控台的Amazon FSX > ONTAP VMware Storage Virtual Machines下找到。

Endpoints

Management DNS name	svm-045c077375d3d9799.fs-0ae40e08acc0dea67.fsx.us-east-1.amazonaws.com	Management IP address	198.19.254.53
NFS DNS name	svm-045c077375d3d9799.fs-0ae40e08acc0dea67.fsx.us-east-1.amazonaws.com	NFS IP address	198.19.254.53
iSCSI DNS name	iscsi.svm-045c077375d3d9799.fs-0ae40e08acc0dea67.fsx.us-east-1.amazonaws.com	iSCSI IP addresses	172.30.15.101, 172.30.14.49

4. 在「Discovery（探索）」索引標籤中、按一下「Discover Portal（探索入口網站）」、然後輸入FSX iSCSI目標的IP位址。



Discover Target Portal

Enter the IP address or DNS name and port number of the portal you want to add.

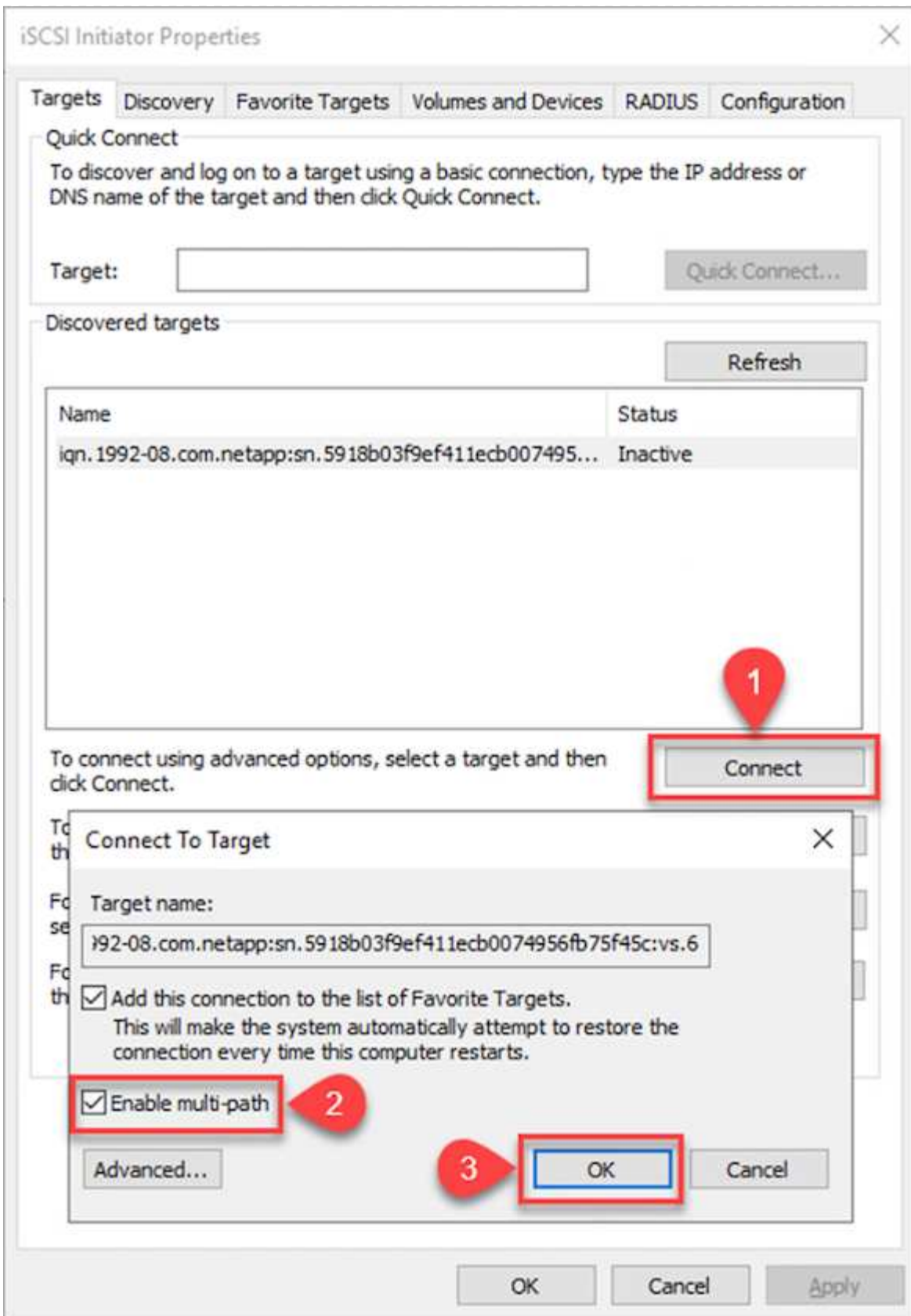
To change the default settings of the discovery of the target portal, click the Advanced button.

IP address or DNS name: 172.30.14.49

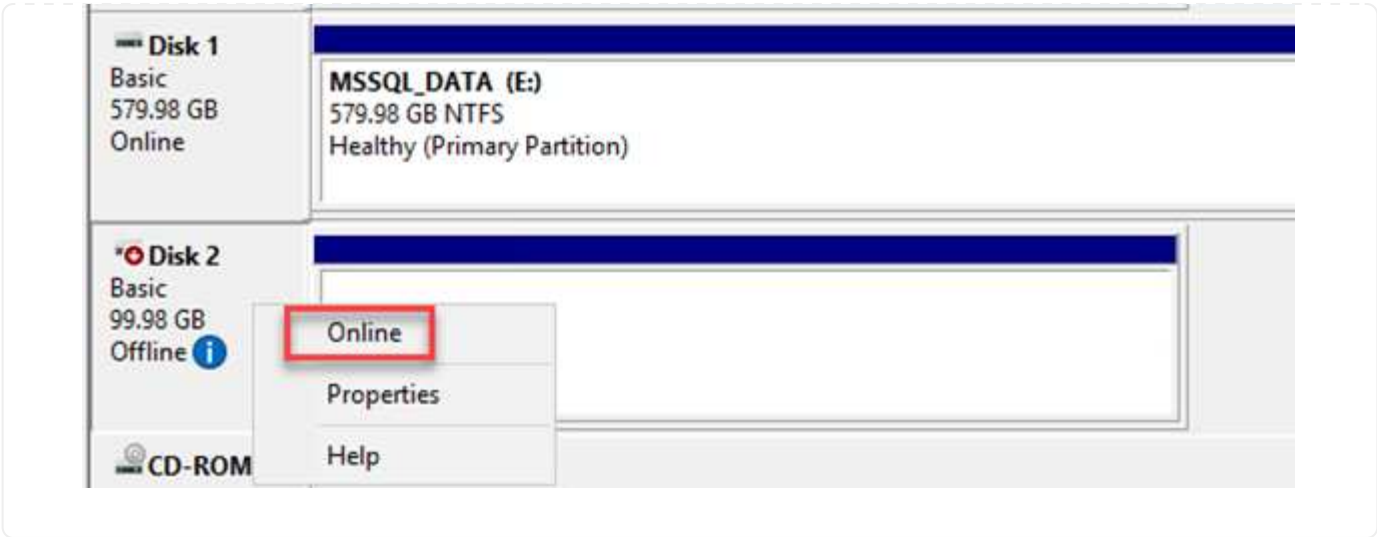
Port: (Default is 3260.) 3260

Advanced... OK Cancel

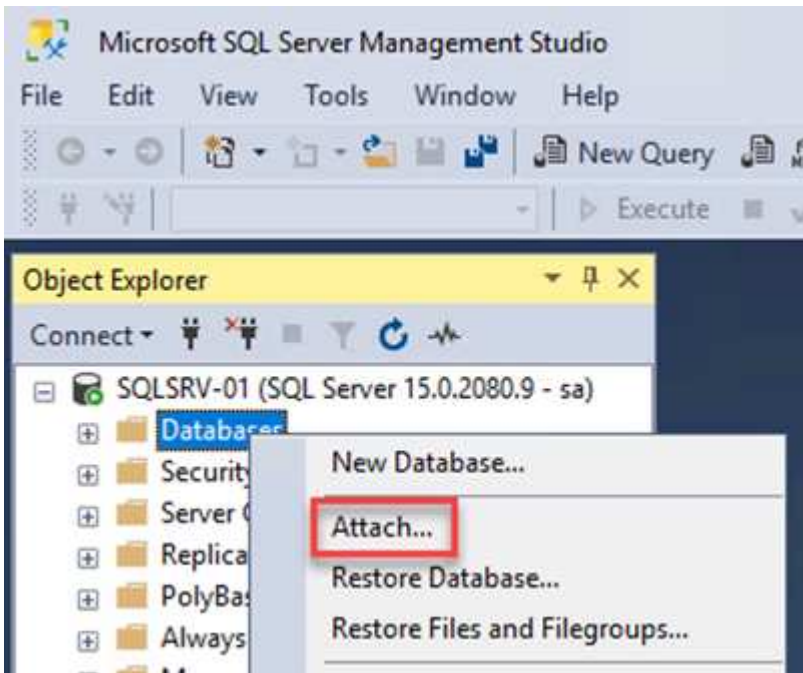
5. 在「Target」（目標）索引標籤上、按一下「Connect」（連線）、選取「Enable Multi-Path（啟用多重路徑）」（若適用於您的組態）、然後按一下「OK（確定）」連線至



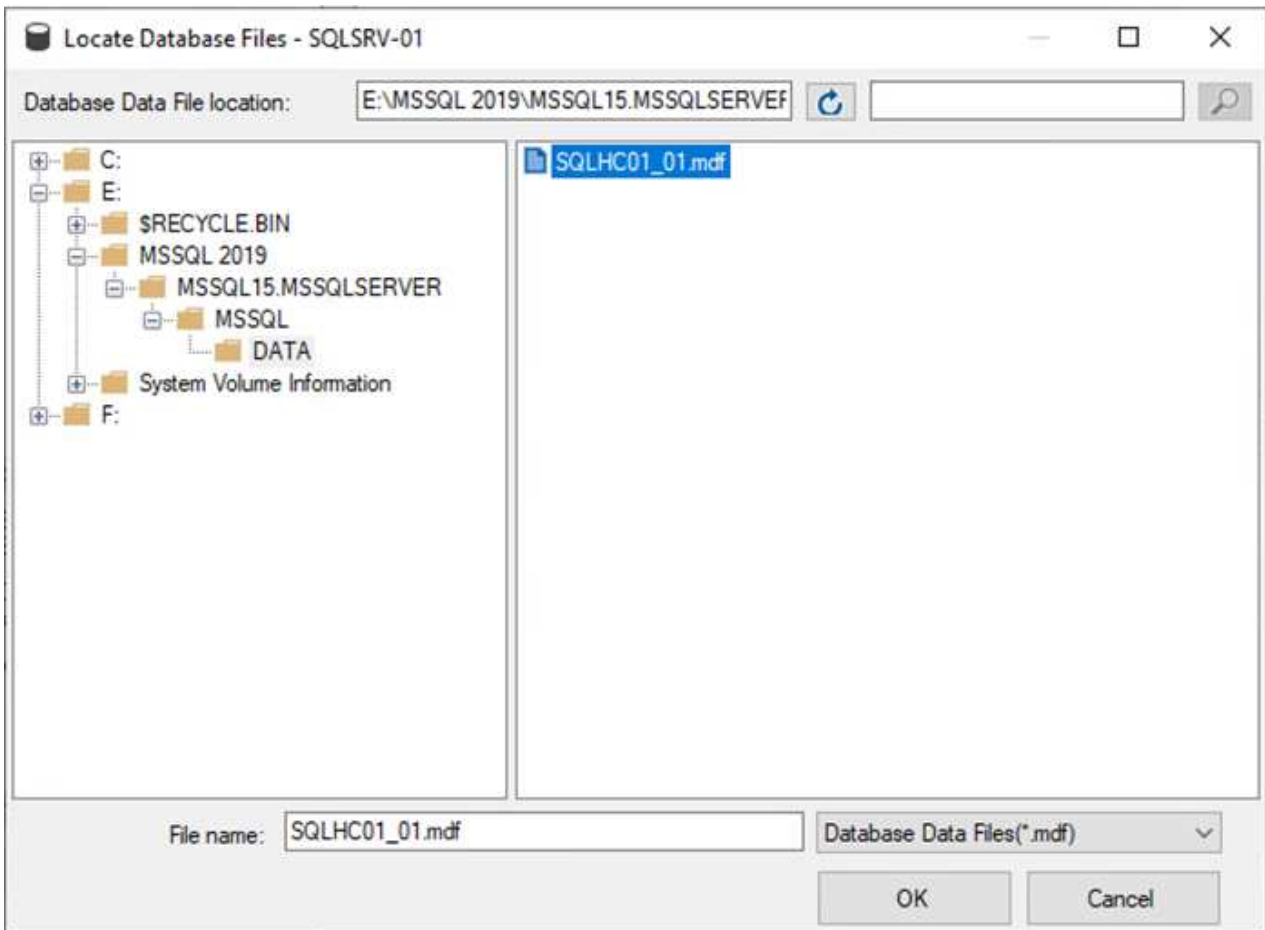
6. 開啟「電腦管理」公用程式、使磁碟上線。請確認它們保留的磁碟機代號與先前所保留的相同。



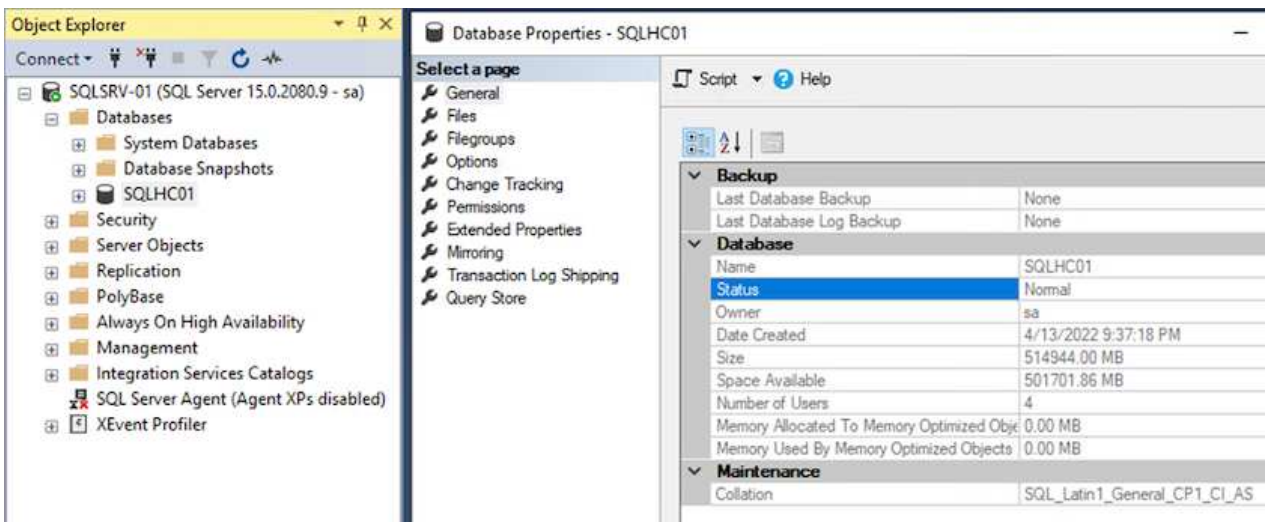
1. 從SQL Server VM開啟Microsoft SQL Server Management Studio、然後選取附加以開始連線至資料庫的程序。



2. 按一下「Add (新增)」、然後瀏覽至包含SQL Server主要資料庫檔案的資料夾、選取該檔案、然後按一下「OK (確定)」。



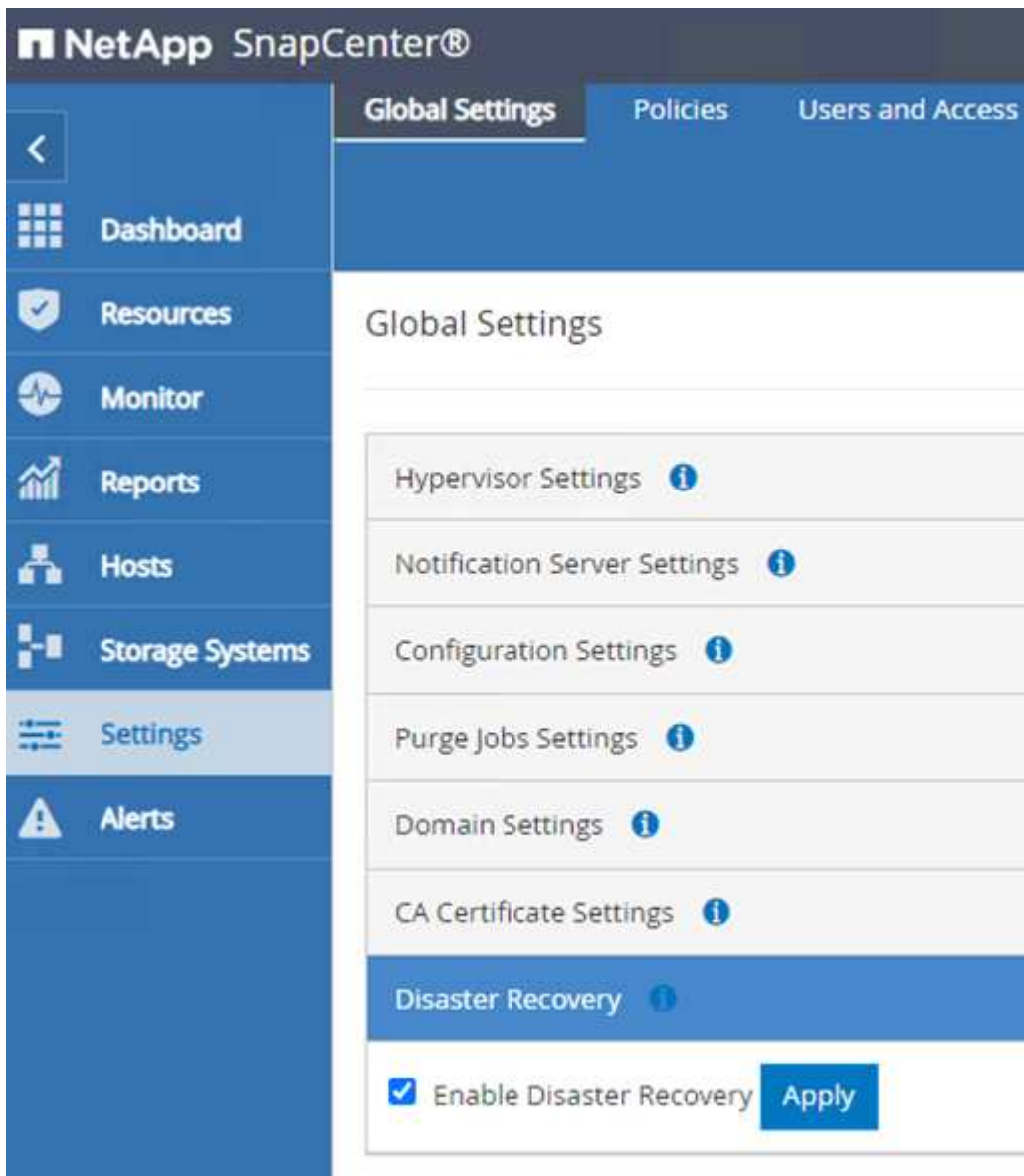
3. 如果交易記錄位於不同的磁碟機上、請選擇包含交易記錄的資料夾。
4. 完成後、按一下「確定」以附加資料庫。



利用還原為先前狀態的功能、它會自動重新探索SQL Server主機。SnapCenter若要使其正常運作、請記住下列先決條件：

- 必須將此項目置於災難恢復模式。SnapCenter這可透過Swagger API或災難恢復下的「全域設定」來完成。
- SQL Server的FQDN必須與內部部署資料中心執行的執行個體相同。
- 原始SnapMirror關係必須中斷。
- 包含資料庫的LUN必須掛載到SQL Server執行個體和附加的資料庫。

若要確認SnapCenter 此功能為災難恢復模式、請從SnapCenter Websweb用戶端瀏覽至「設定」。前往「Global Settings (全域設定)」索引標籤、然後按一下「Disaster Recovery (災難恢復) 請確定已啟用「啟用災難恢復」核取方塊。



還原Oracle應用程式資料

下列程序提供如何在發生導致內部部署站台無法運作的災難時、在AWS的VMware Cloud Services中恢復Oracle應用程式資料的指示。

完成下列先決條件、以繼續執行恢復步驟：

1. Oracle Linux伺服器VM已使用Veeam完整還原還原至VMware Cloud SDDC。
2. 已SnapCenter 建立次要的功能、SnapCenter 並已使用本節所述的步驟還原了資料庫和組態檔案 "[支援備份與還原程序摘要](#)。SnapCenter"

若要讓Oracle伺服器能夠存取位於FSxN執行個體上的次要儲存磁碟區、您必須先中斷現有的SnapMirror關係。

1. 登入FSX CLI之後、請執行下列命令、檢視依正確名稱篩選的磁碟區。

```
FSx-Dest::> volume show -volume VolumeName*
```

```
FsxId0ae40e08acc0dea67::> volume show -volume oraclesrv_03*
Vserver   Volume                Aggregate      State      Type      Size  Available Used%
-----
ora_svm_dest
           oraclesrv_03_u01_dest
           aggr1              online      DP        100GB   93.12GB  6%
ora_svm_dest
           oraclesrv_03_u02_dest
           aggr1              online      DP        200GB   34.98GB  82%
ora_svm_dest
           oraclesrv_03_u03_dest
           aggr1              online      DP        150GB   33.37GB  77%
3 entries were displayed.
FsxId0ae40e08acc0dea67::> █
```

2. 執行下列命令以中斷現有的SnapMirror關係。

```
FSx-Dest::> snapmirror break -destination-path DestSVM:DestVolName
```

```
FsxId0ae40e08acc0dea67::> snapmirror break -destination-path ora_svm_dest:oraclesrv_03_u02_dest
Operation succeeded: snapmirror break for destination "ora_svm_dest:oraclesrv_03_u02_dest".

FsxId0ae40e08acc0dea67::> snapmirror break -destination-path ora_svm_dest:oraclesrv_03_u03_dest
Operation succeeded: snapmirror break for destination "ora_svm_dest:oraclesrv_03_u03_dest".
```

3. 更新Amazon FSX Web用戶端中的交會路徑：

oraclesrv_03_u01_dest (fsvol-01167370e9b7aefa0)

Attach

Actions ▲

Update volume

Create backup


Delete volume

Summary

Volume ID

fsvol-01167370e9b7aefa0 

Volume name

oraclesrv_03_u01_dest 

UUID

3d7338ce-9f19-11ec-
b007-4956fb75f45c

File system ID

fs-0ae40e08acc0dea67 

Resource ARN

arn:aws:fsx:us-
east-1:541696183547:volume/fs-
0ae40e08acc0dea67/fsvol-
01167370e9b7aefa0 

Creation time

2022-03-08T14:52:09-05:00

Lifecycle state

 Created

Volume type

ONTAP

Size

100.00 GB 

SVM ID

svm-02b2ad25c6b2e5bc2

Junction path

- 

Tiering policy name

SNAPSHOT_ONLY

Tiering policy cooling period (days)

2

Storage efficiency enabled

Disabled

4. 新增交會路徑名稱、然後按一下「Update（更新）」。從Oracle伺服器掛載NFS Volume時、請指定此交會路徑。

Update volume



Junction path

The location within your file system where your volume will be mounted.

Volume size



Minimum 20 MiB; Maximum 104857600 MiB

Storage efficiency

Select whether you would like to enable ONTAP storage efficiencies on your volume: deduplication, compression, and compaction.

- Enabled (recommended)
- Disabled

Capacity pool tiering policy

You can optionally enable automatic tiering of your data to lower-cost capacity pool storage.



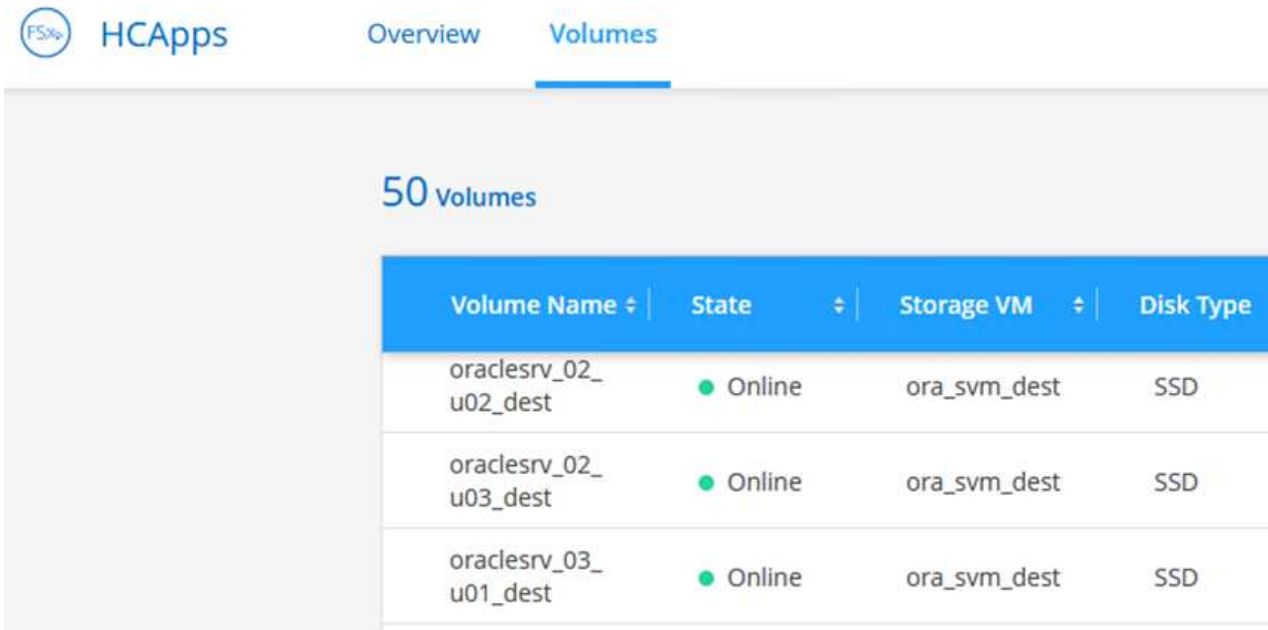
Cancel

Update

在Oracle伺服器上掛載NFS磁碟區

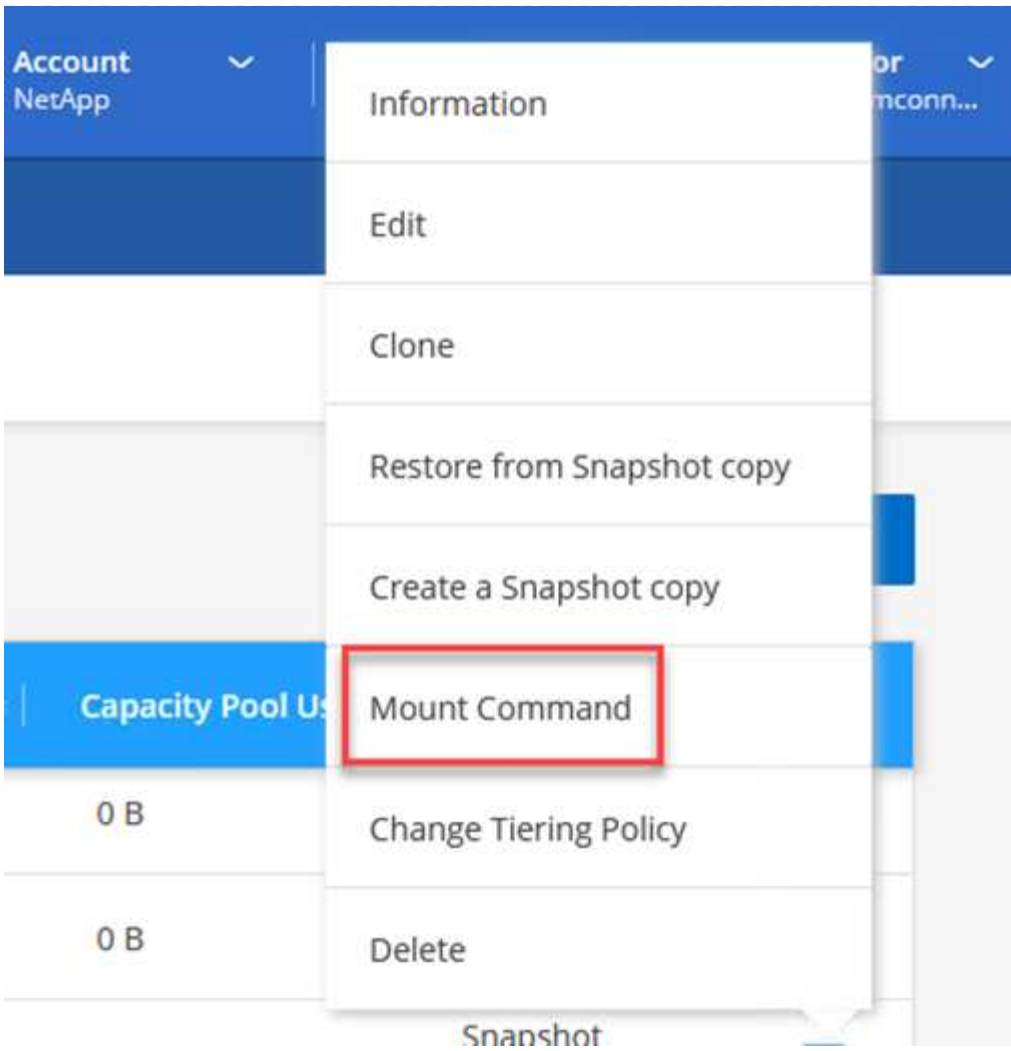
在Cloud Manager中、您可以使用正確的NFS LIF IP位址來取得掛載命令、以掛載包含Oracle資料庫檔案和記錄檔的NFS磁碟區。

1. 在Cloud Manager中、存取FSX叢集的Volume清單。



Volume Name	State	Storage VM	Disk Type
oraclesrv_02_u02_dest	Online	ora_svm_dest	SSD
oraclesrv_02_u03_dest	Online	ora_svm_dest	SSD
oraclesrv_03_u01_dest	Online	ora_svm_dest	SSD

2. 從動作功能表中、選取Mount Command（掛載命令）以檢視及複製要在Oracle Linux伺服器上使用的掛載命令。



Mount Volume NFS

oraclesrv_03_u01_dest

Go to your linux machine and enter this mount command

Mount Command

```
mount 198.19.254.180:/oraclesrv_03_u01_dest <dest_d...
```

 Copy

- 3. 將NFS檔案系統掛載至Oracle Linux Server。用於掛載NFS共用的目錄已存在於Oracle Linux主機上。
- 4. 在Oracle Linux伺服器上、使用mount命令掛載NFS磁碟區。


```
FSx-Dest::> mount -t oracle_server_ip:/junction-path
```

針對與Oracle資料庫相關的每個Volume重複此步驟。



若要讓NFS掛載在重新開機時持續執行、請編輯「/etc/stabs」檔案以包含掛載命令。

5. 重新啟動Oracle伺服器。Oracle資料庫應正常啟動、並可供使用。

容錯回復

成功完成本解決方案所述的容錯移轉程序後、SnapCenter 即可恢復在AWS中執行的備份功能、而FSXfor ONTAP 效益現已被指定為主要儲存設備、且不存在與原始內部部署資料中心的SnapMirror關係。在內部部署恢復正常功能之後、您可以使用與本文件所述相同的程序、將資料鏡射回內部部署ONTAP 的更新儲存系統。

如本文件所述、您可以設定SnapCenter 將應用程式資料Volume從FSXfor ONTAP the Sfor the Sf8鏡射至ONTAP 內部部署的靜態儲存系統。同樣地、您也可以設定Veeam使用橫向擴充備份儲存庫、將備份複本複製到Amazon S3、以便駐留在內部部署資料中心的Veeam備份伺服器能夠存取這些備份。

容錯回復不在本文件的範圍之內、但容錯回復與此處概述的詳細程序幾乎沒有什麼不同。

結論

本文件所述的使用案例著重於已獲證實的災難恢復技術、強調NetApp與VMware之間的整合。NetApp ONTAP 支援的資料鏡射技術已獲證實、可讓組織設計跨越內部部署和ONTAP 與頂尖雲端供應商共同使用的不實技術的災難恢復解決方案。

FSX for ONTAP Sfor AWS是這樣的解決方案之一、可與SnapCenter 支援將SyncMirror 應用程式資料複製到雲端的功能不間斷地整合到功能上。Veeam備份與複寫是另一項廣為人知的技術、可與NetApp ONTAP 的VMware 還原儲存系統完美整合、並提供容錯移轉至vSphere原生儲存設備的功能。

本解決方案提供使用來自ONTAP 代管SQL Server和Oracle應用程式資料之VMware系統的來賓連線儲存設備的災難恢復解決方案。利用SnapMirror提供易於管理的解決方案、可在支援應用程式的各個系統上保護應用程式磁碟區、並將其複製到位於雲端的FSX或CVO。SnapCenter ONTAP支援DR的解決方案可將所有應用程式資料容錯移轉至AWS上的VMware Cloud。SnapCenter

何處可找到其他資訊

若要深入瞭解本文所述資訊、請檢閱下列文件和 / 或網站：

- 解決方案文件連結

["NetApp混合式多雲端搭配VMware解決方案"](#)

["NetApp解決方案"](#)

在 **VMware Cloud** 中使用 **Amazon FSX for ONTAP** 進行 **Veeam** 備份與還原

Veeam 備份與複寫是有效且可靠的解決方案、可在 VMware Cloud 中保護資料。此解決方

案展示了正確的設定和組態、可讓您使用 Veeam 備份和複寫來備份和還原位於 VMware Cloud 中適用於 ONTAP NFS 資料存放區的 FSX 上的應用程式 VM。

作者：Josh Powell - NetApp 解決方案工程部

總覽

VMware Cloud（在 AWS 中）支援使用 NFS 資料存放區做為補充儲存設備、而 FSX for NetApp ONTAP 則是安全的解決方案、適合需要儲存大量資料給雲端應用程式的客戶、可在 SDDC 叢集中的 ESXi 主機數量之外進行擴充。這項整合式 AWS 儲存服務提供高效率的儲存設備、具備所有傳統的 NetApp ONTAP 功能。

使用案例

本解決方案可解決下列使用案例：

- 使用適用於 NetApp ONTAP 的 FSX 作為備份儲存庫、備份及還原 VMC 中託管的 Windows 和 Linux 虛擬機器。
- 使用適用於 NetApp ONTAP 的 FSX 作為備份儲存庫、備份及還原 Microsoft SQL Server 應用程式資料。
- 使用適用於 NetApp ONTAP 的 FSX 作為備份儲存庫、備份及還原 Oracle 應用程式資料。

使用 Amazon FSX for ONTAP 的 NFS 資料存放區

此解決方案中的所有虛擬機器都位於適用於 ONTAP 補充 NFS 資料存放區的 FSX 上。將 FSX for ONTAP 作為補充 NFS 資料存放區有幾項優點。例如、它可讓您：

- 在雲端中建立可擴充且高可用度的檔案系統、無需複雜的設定與管理。
- 與現有的 VMware 環境整合、讓您使用熟悉的工具和程序來管理雲端資源。
- 從 ONTAP 提供的進階資料管理功能（例如快照和複寫）中獲益、以保護您的資料並確保其可用性。

解決方案部署總覽

此清單提供設定 Veeam 備份與複寫、使用適用於 ONTAP 的 FSX 作為備份儲存庫執行備份與還原工作、以及執行 SQL Server、Oracle VM 和資料庫還原所需的高階步驟：

1. 為 ONTAP 檔案系統建立 FSX、作為 Veeam 備份與複寫的 iSCSI 備份儲存庫。
2. 部署 Veeam Proxy 以分散備份工作負載、並裝載位於 ONTAP 適用的 FSX 上的 iSCSI 備份儲存庫。
3. 設定 Veeam 備份工作來備份 SQL Server、Oracle、Linux 和 Windows 虛擬機器。
4. 還原 SQL Server 虛擬機器和個別資料庫。
5. 還原 Oracle 虛擬機器和個別資料庫。

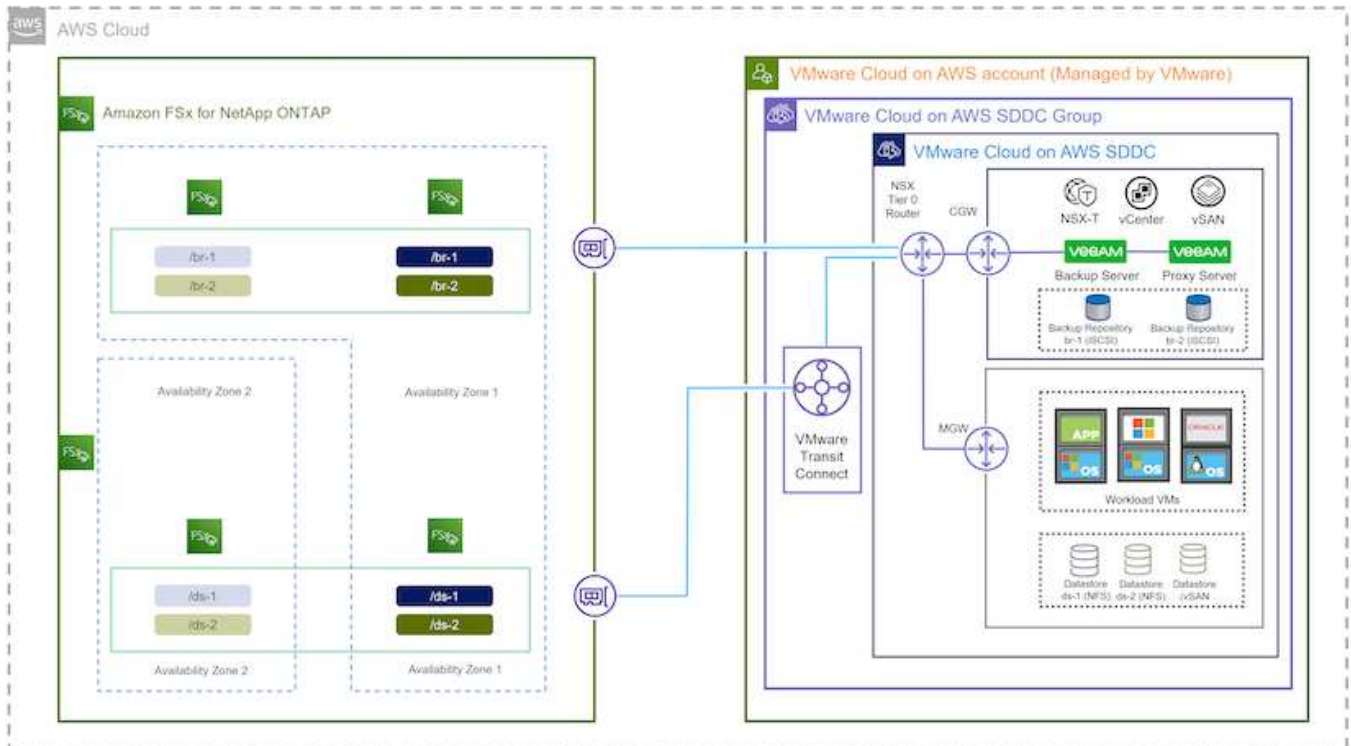
先決條件

此解決方案的目的是展示在 VMware Cloud 中執行、位於由 FSX for NetApp ONTAP 託管的 NFS 資料存放區上的虛擬機器的資料保護功能。本解決方案假設已設定下列元件、可供使用：

1. ONTAP 檔案系統的 FSX、其中有一或多個 NFS 資料存放區連線至 VMware Cloud。
2. 安裝了 Veeam 備份與複寫軟體的 Microsoft Windows Server VM。
 - Veeam 備份與複寫伺服器已使用其 IP 位址或完整網域名稱來探索 vCenter 伺服器。
3. 在解決方案部署期間與 Veeam Backup Proxy 元件一起安裝的 Microsoft Windows Server VM。
4. 內含 VMDK 的 Microsoft SQL Server VM、以及位於 ONTAP NFS 資料存放區的 FSX 上的應用程式資料。對於此解決方案、我們在兩個獨立的 VMDK 上有兩個 SQL 資料庫。
 - 附註：最佳實務做法是將資料庫和交易記錄檔放在不同的磁碟機上、如此可改善效能和可靠性。部分原因是交易記錄會依序寫入、而資料庫檔案則是隨機寫入。
5. Oracle 資料庫 VM 搭配 VMDK、以及位於 ONTAP NFS 資料存放區的 FSX 上的應用程式資料。
6. Linux 和 Windows 檔案伺服器 VM、其中 VMDK 位於 ONTAP NFS 資料存放區的 FSX 上。
7. Veeam 需要特定的 TCP 連接埠、才能在備份環境中的伺服器和元件之間進行通訊。在 Veeam 備份基礎架構元件上、系統會自動建立必要的防火牆規則。如需網路連接埠需求的完整清單、請參閱的「連接埠」一節 "[Veeam Backup and Replication User Guide for VMware vSphere](#)"。

高層架構

本解決方案的測試/驗證是在實驗室中執行、可能與最終部署環境相符或不相符。如需詳細資訊、請參閱下列各節。



此解決方案的目的是展示在 VMware Cloud 中執行、位於由 FSX for NetApp ONTAP 託管的 NFS 資料存放區上的虛擬機器的資料保護功能。本解決方案假設下列元件已設定好可供使用：

- Microsoft Windows VM 位於適用於 ONTAP NFS 資料存放區的 FSX 上
- Linux (CentOS) VM 位於適用於 ONTAP NFS 資料存放區的 FSX 上
- Microsoft SQL Server VM 位於適用於 ONTAP NFS 資料存放區的 FSX 上
 - 兩個資料庫分別託管在不同的 VMDK 上
- Oracle VM 位於適用於 ONTAP NFS 資料存放區的 FSX 上

解決方案部署

在本解決方案中、我們提供詳細說明、說明如何使用 Veeam 備份與複寫軟體來部署及驗證解決方案、以及在 AWS 上的 VMware Cloud SDDC 中執行 SQL Server、Oracle、Windows 和 Linux 檔案伺服器虛擬機器的備份與還原。此解決方案中的虛擬機器位於由 FSX for ONTAP 主控的補充 NFS 資料存放區。此外、ONTAP 檔案系統的另一個 FSX 可用來裝載 iSCSI 磁碟區、以用於 Veeam 備份儲存庫。

我們將介紹用於 ONTAP 檔案系統建立的 FSX、用於備份儲存庫的裝載 iSCSI 磁碟區、建立及執行備份工作、以及執行 VM 和資料庫還原。

如需適用於 NetApp ONTAP 的 FSX 詳細資訊、請參閱 ["適用於 ONTAP 的 FSX 使用者指南"](#)。

如需 Veeam 備份與複寫的詳細資訊、請參閱 ["Veeam 說明中心技術文件"](#) 網站。

如需在 AWS 上使用 Veeam Backup and Replication 搭配 VMware Cloud 時的考量與限制、請參閱 ["VMware Cloud on AWS 和 VMware Cloud on Dell EMC Support"](#)。 ["考量與限制"](#)。

部署 Veeam Proxy 伺服器

Veeam Proxy 伺服器是 Veeam 備份與複寫軟體的元件、在來源與備份或複寫目標之間扮演中介角色。Proxy 伺服器可在本機處理資料、協助最佳化及加速備份工作期間的資料傳輸、並可使用不同的傳輸模式、使用 VMware vStorage API 來存取資料保護、或透過直接儲存存取來存取資料。

選擇 Veeam Proxy 伺服器設計時、請務必考慮所需的並行工作數、以及傳輸模式或儲存存取類型。

如需設定 Proxy 伺服器數量及其系統需求的大小、請參閱 ["Veeam VMware vSphere 最佳實務指南"](#)。

Veeam Data Mover 是 Veeam Proxy 伺服器的元件、使用傳輸模式作為從來源取得 VM 資料並將其傳輸至目標的方法。傳輸模式是在備份工作組態期間指定的。您可以使用直接儲存存取、從 NFS 資料存放區增加效率備份。

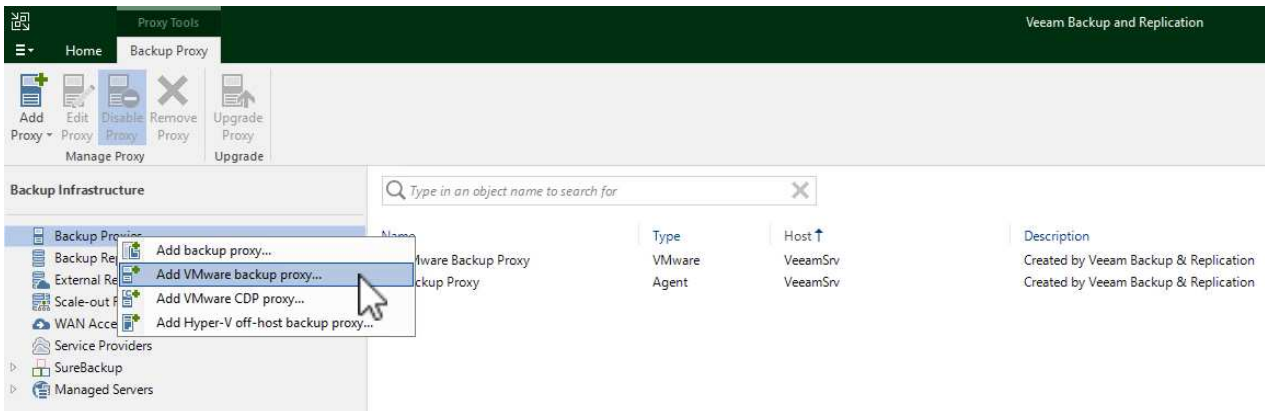
如需傳輸模式的詳細資訊、請參閱 ["Veeam Backup and Replication User Guide for VMware vSphere"](#)。

在接下來的步驟中、我們將在 VMware Cloud SDDC 中的 Windows VM 上部署 Veeam Proxy Server。

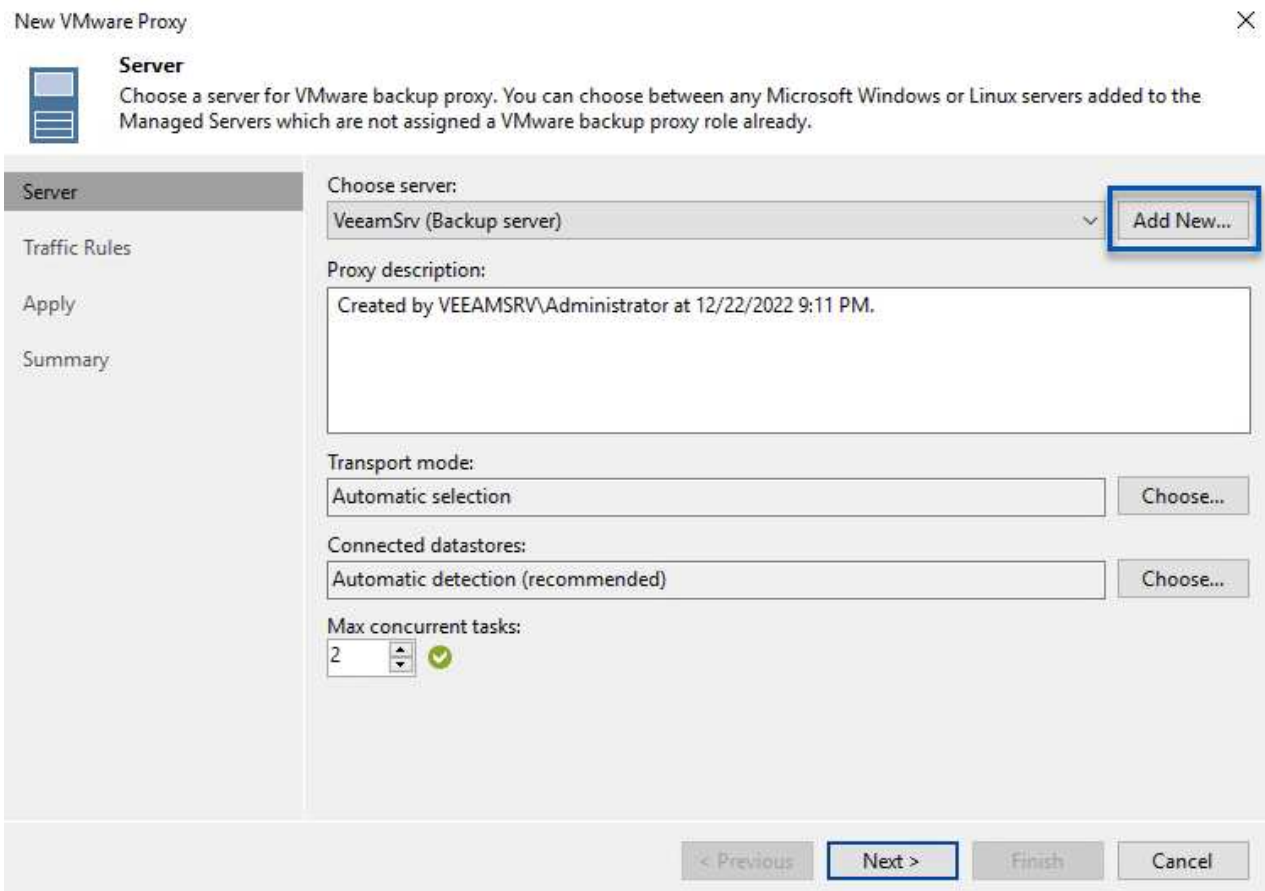
部署 Veeam Proxy 以分散備份工作負載

在此步驟中、Veeam Proxy 會部署至現有的 Windows VM。如此可在主要 Veeam Backup Server 和 Veeam Proxy 之間分配備份工作。

1. 在 Veeam Backup and Replication 伺服器上、開啟管理主控台、然後在左下角的功能表中選取 * Backup Infrastructure*。
2. 在 * 備份代理 * 上按一下滑鼠右鍵、然後按一下 * 新增 VMware 備份代理伺服器 ... * 以開啟精靈。

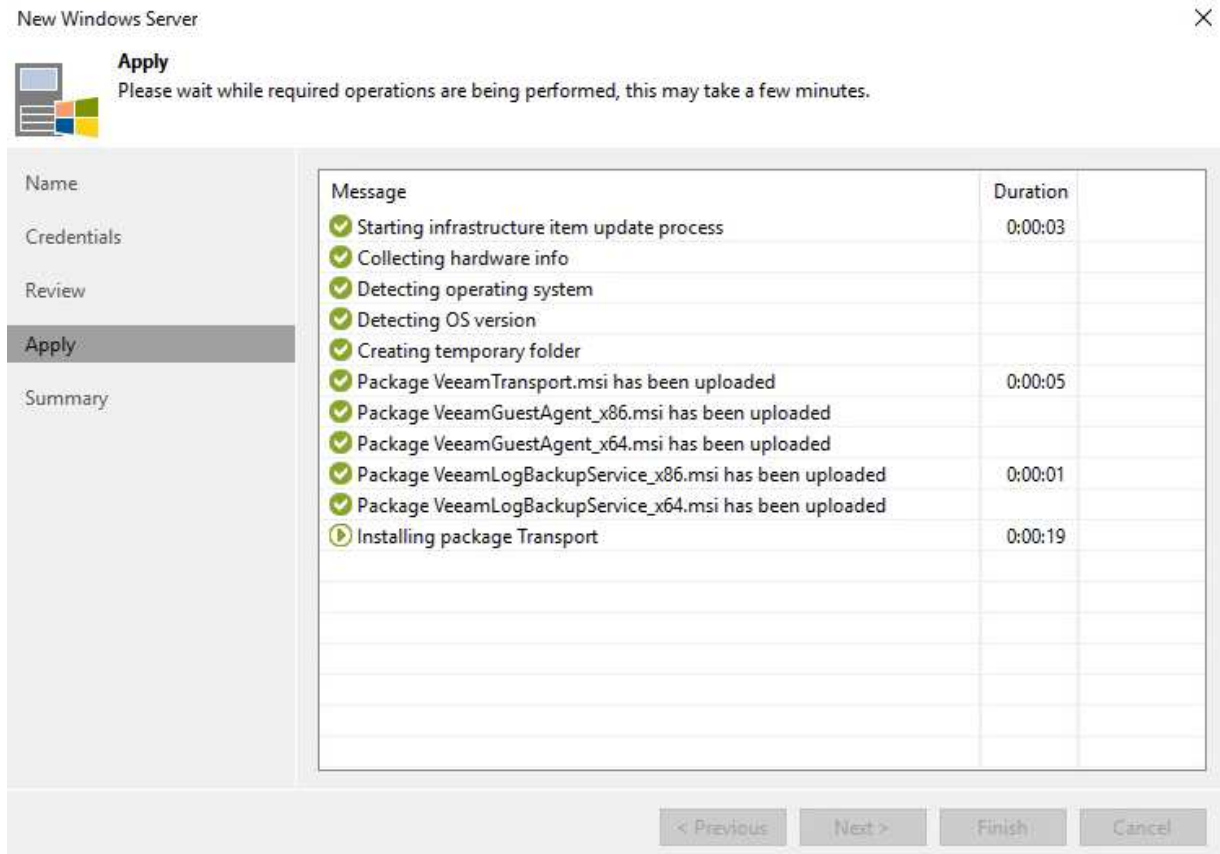


3. 在 * 新增 VMware Proxy* 精靈中、按一下 * 新增 ... * 按鈕以新增 Proxy 伺服器。

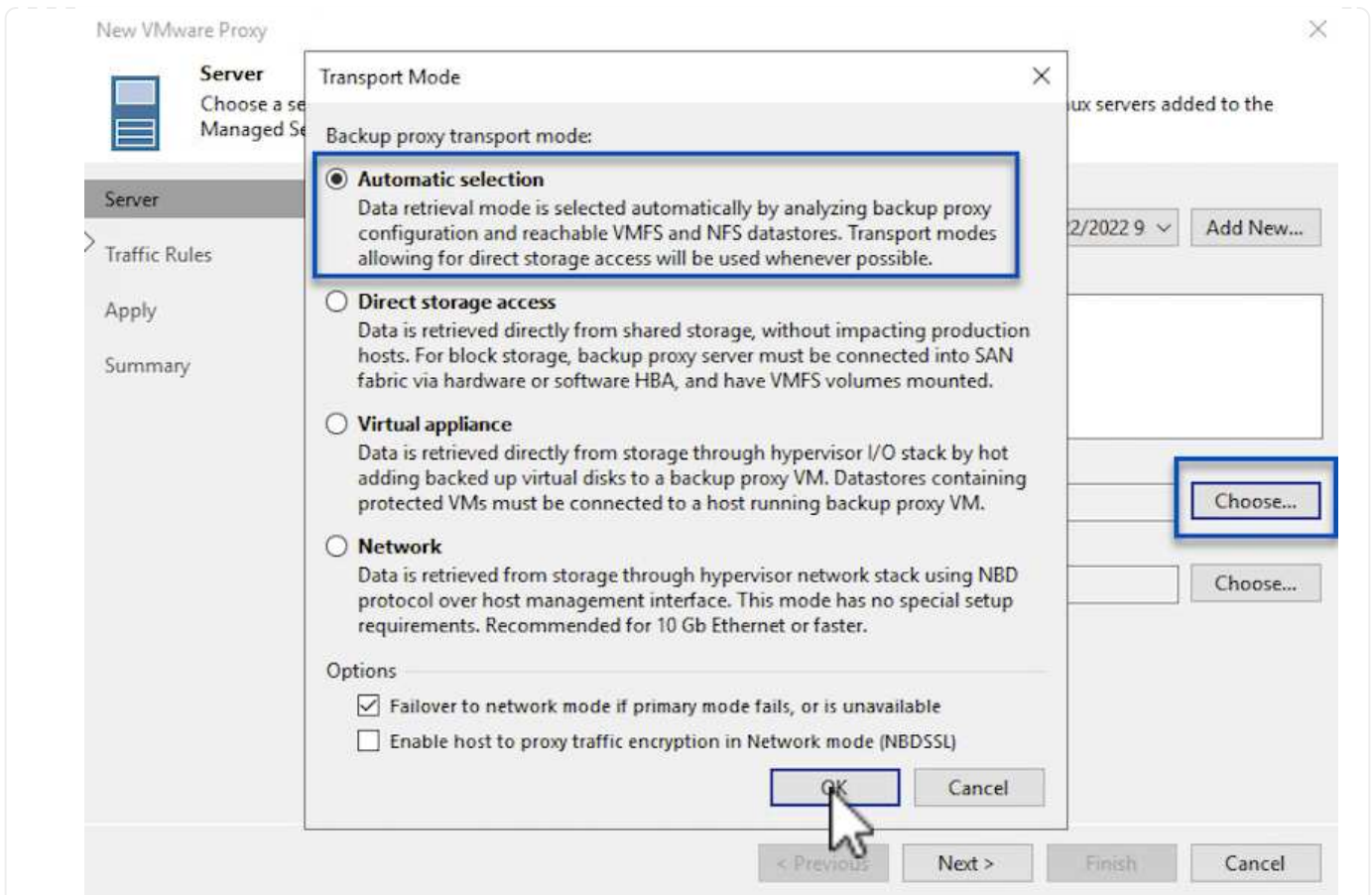


4. 選取以新增 Microsoft Windows、然後依照提示新增伺服器：

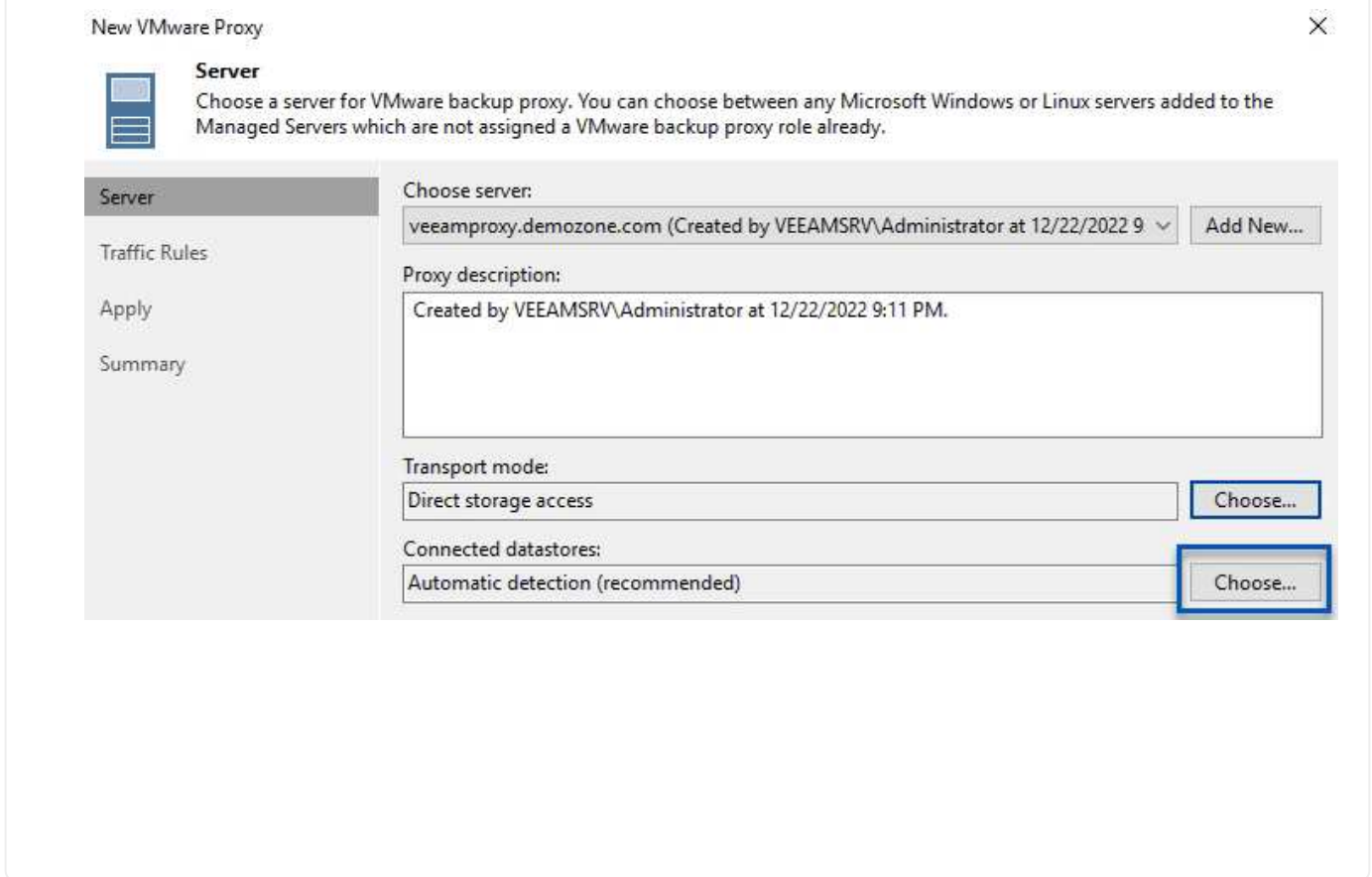
- 填寫 DNS 名稱或 IP 位址
- 選取要用於新系統上認證的帳戶、或新增認證
- 檢閱要安裝的元件、然後按一下 * 套用 * 開始部署

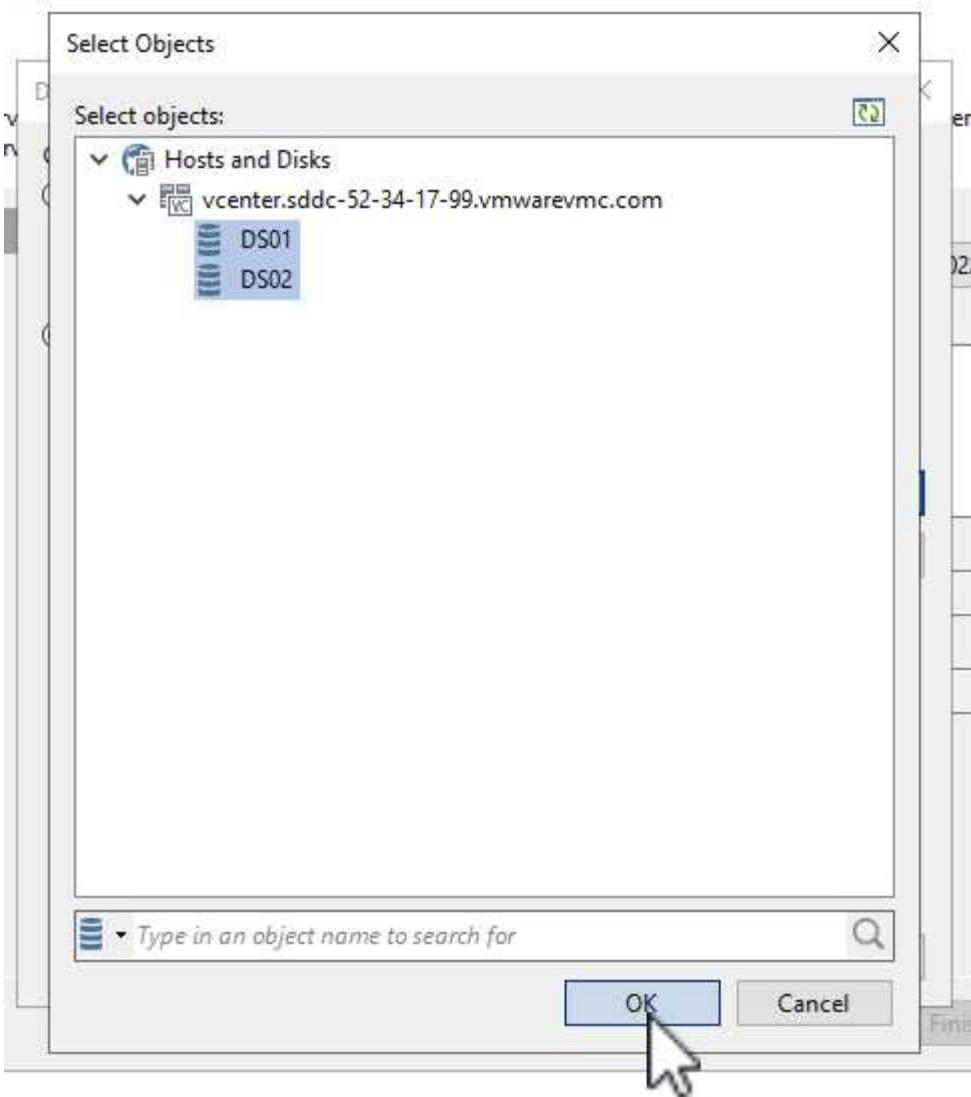


5. 回到 * 新增 VMware Proxy* 精靈、選擇傳輸模式。在我們的案例中、我們選擇 * 自動選擇* 。

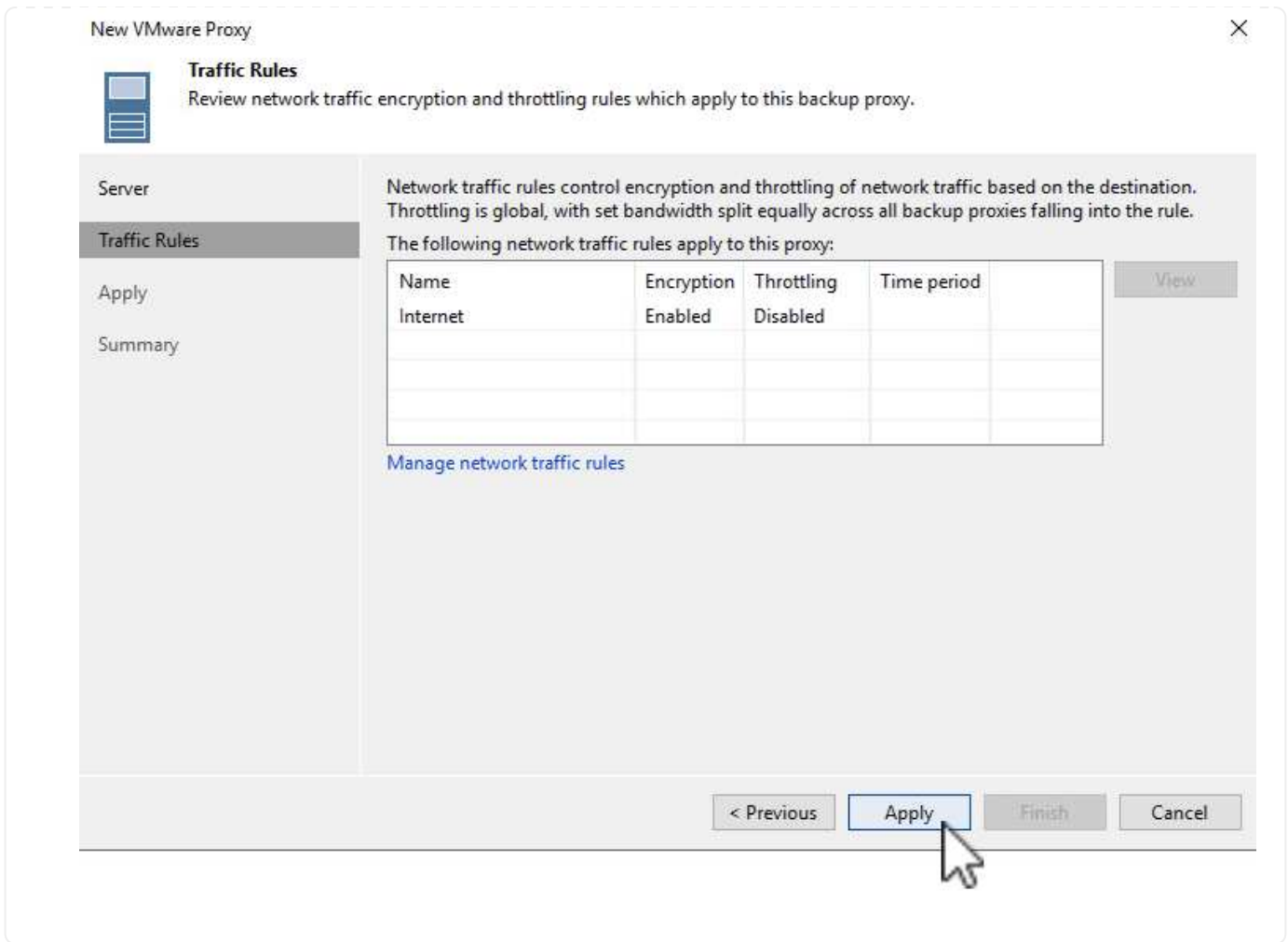


6. 選取您要 VMware Proxy 直接存取的連線資料存放區。





7. 設定並套用任何特定的網路流量規則、例如所需的加密或節流。完成後、按一下 * 套用 * 按鈕以完成部署。



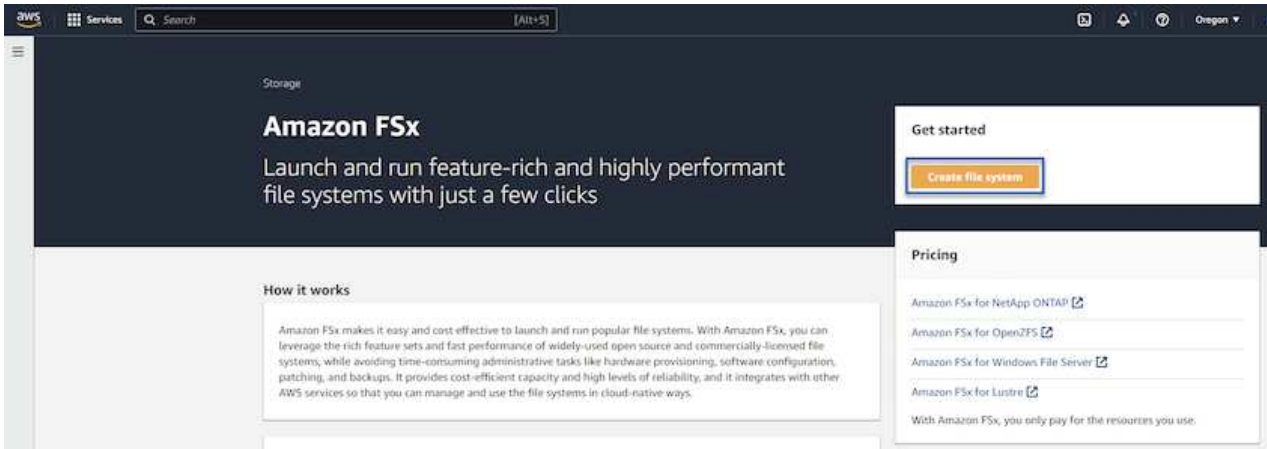
設定儲存與備份儲存庫

主要 Veeam 備份伺服器 and Veeam Proxy 伺服器可以直接連線儲存設備的形式存取備份儲存庫。在本節中、我們將介紹如何為 ONTAP 檔案系統建立 FSX、將 iSCSI LUN 掛載至 Veeam 伺服器、以及建立備份儲存庫。

為 ONTAP 檔案系統建立 FSX

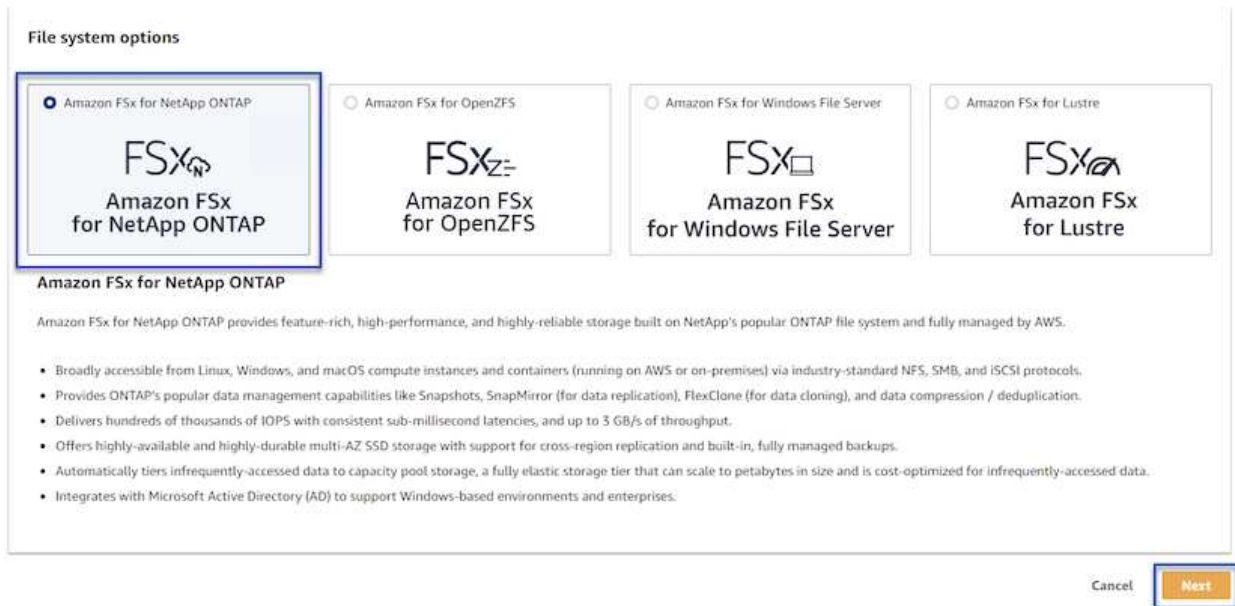
為 ONTAP 檔案系統建立一個 FSX、用於裝載 Veeam 備份儲存庫的 iSCSI 磁碟區。

1. 在 AWS 主控台、前往 FSX、然後 * 建立檔案系統 *



2. 選擇 * Amazon FSX for NetApp ONTAP *、然後選擇 * Next* 繼續。

Select file system type



3. 填寫檔案系統名稱、部署類型、SSD 儲存容量、以及 ONTAP 叢集的 FSX 所在的 VPC。這必須是設定為與 VMware Cloud 中的虛擬機器網路通訊的 VPC。按一下 * 下一步 *。

Create file system

Creation method

Quick create

Use recommended best-practice configurations. Most configuration options can be changed after the file system is created.

Standard create

You set all of the configuration options, including specifying performance, networking, security, backups, and maintenance.

Quick configuration

File system name - optional info

BackupFSxN

1

Maximum of 256 Unicode letters, whitespace, and numbers, plus + - = . _ : /

Deployment type info

Multi-AZ

Single-AZ

2

SSD storage capacity info

4096 GiB

3

Minimum 1024 GiB; Maximum 192 TiB

Virtual Private Cloud (VPC) info

Specify the VPC from which your file system is accessible.

Demo-FsxforONTAP-VPC | vpc-05596abe79cb653b7

4

Storage efficiency

Select whether you would like to enable ONTAP's storage efficiency features: deduplication, compression, and compaction

Enabled (recommended)

Disabled

Cancel

Back

Next

4. 檢閱部署步驟、然後按一下 * 建立檔案系統 *、開始建立檔案系統的程序。

設定及掛載 iSCSI LUN

在適用於 ONTAP 的 FSX 上建立和設定 iSCSI LUN、並掛載至 Veeam 備份和 Proxy 伺服器。這些 LUN 稍後將用於建立 Veeam 備份儲存庫。



在適用於 ONTAP 的 FSX 上建立 iSCSI LUN 是一個多步驟程序。建立磁碟區的第一步可以在 Amazon FSX 主控台或 NetApp ONTAP CLI 中完成。



如需使用適用於 ONTAP 的 FSX 的詳細資訊、請參閱 "[適用於 ONTAP 的 FSX 使用者指南](#)"。

1. 從 NetApp ONTAP CLI 使用下列命令建立初始磁碟區：

```
FSx-Backup::> volume create -vserver svm_name -volume vol_name  
-aggregate aggregate_name -size vol_size -type RW
```

2. 使用上一步建立的磁碟區建立 LUN：

```
FSx-Backup::> lun create -vserver svm_name -path  
/vol/vol_name/lun_name -size size -ostype windows -space-allocation  
enabled
```

3. 建立包含 Veeam 備份和 Proxy 伺服器 iSCSI IQN 的啟動器群組、以授予對 LUN 的存取權：

```
FSx-Backup::> igroup create -vserver svm_name -igroup igroup_name  
-protocol iSCSI -ostype windows -initiator IQN
```

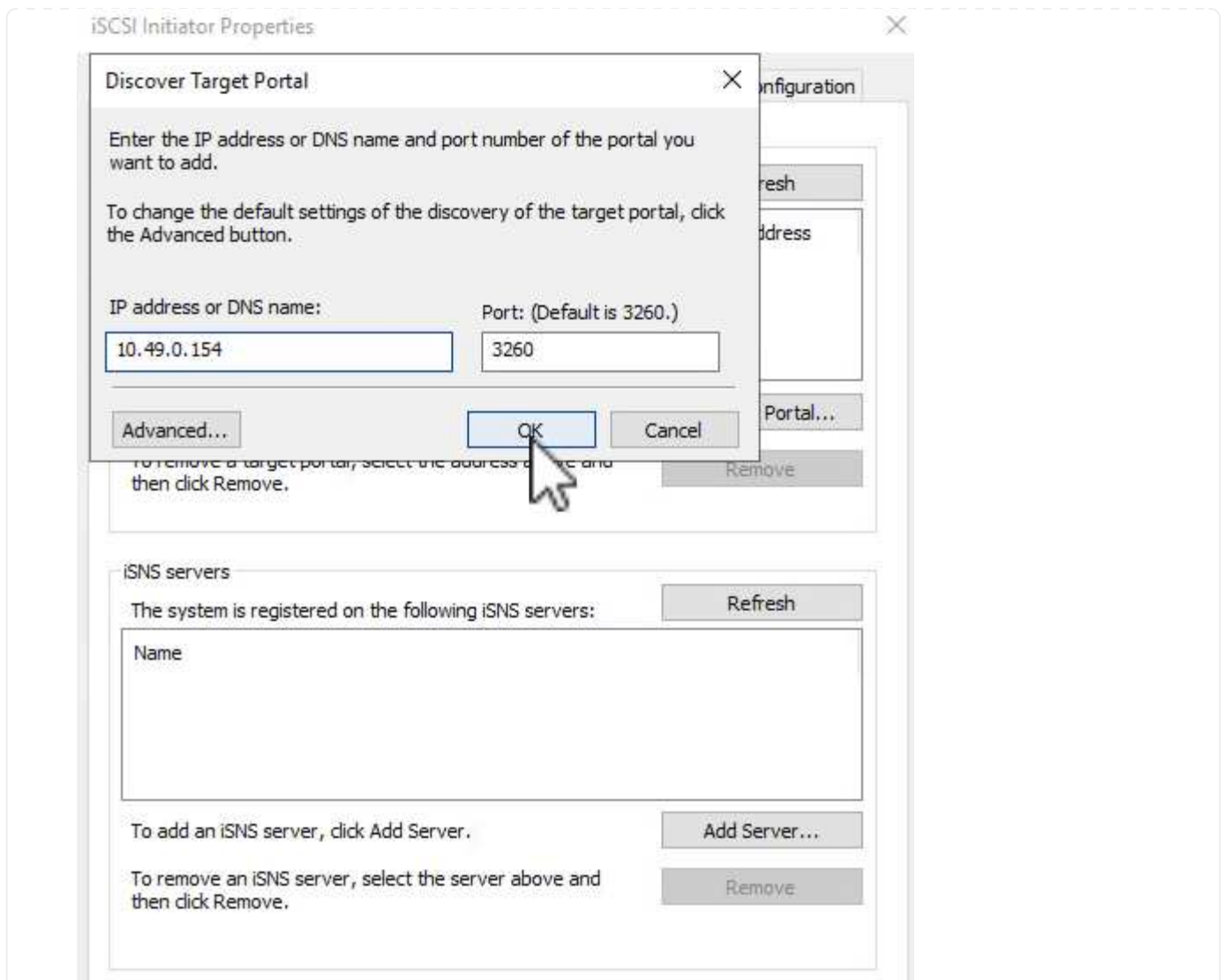


若要完成上述步驟、您必須先從 Windows 伺服器上的 iSCSI 啟動器內容擷取 IQN。

4. 最後、將 LUN 對應至您剛建立的啟動器群組：

```
FSx-Backup::> lun mapping create -vserver svm_name -path  
/vol/vol_name/lun_name igroup igroup_name
```

5. 若要掛載 iSCSI LUN、請登入 Veeam 備份與複寫伺服器、然後開啟 iSCSI 啟動器內容。移至 * Discover (探索) * 標籤、然後輸入 iSCSI 目標 IP 位址。



6. 在 * 目標 * 索引標籤上、反白非作用中的 LUN 、然後按一下 * 連線 * 。勾選 * 啟用多重路徑 * 方塊、然後按一下 * 確定 * 以連線至 LUN 。

Targets Discovery Favorite Targets Volumes and Devices RADIUS Configuration

Quick Connect
To discover and log on to a target using a basic connection, type the IP address or DNS name of the target and then click Quick Connect.

Target: Quick Connect...

Discovered targets

Refresh

Name	Status
iqn.1992-08.com.netapp:sn.d9aad3cd818011edbfcd87a...	Inactive

To connect using advanced options, select a target and then click Connect.

To completely disconnect a target, select the target and then click Disconnect.

For target properties, including configuration of sessions, select the target and click Properties.

For configuration of devices associated with a target, select the target and then click Devices.

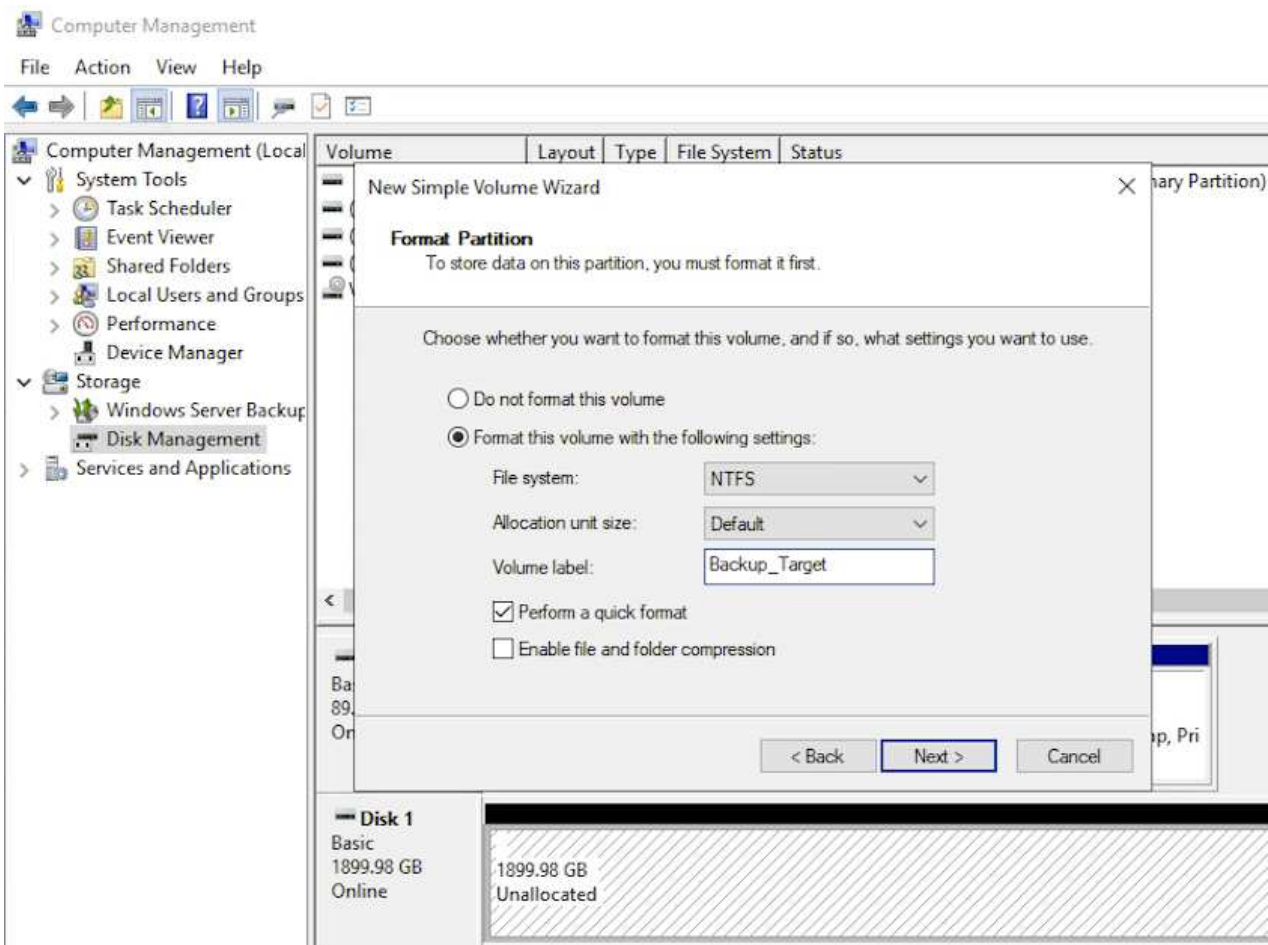
Connect

Disconnect

Properties...

Devices...

7. 在磁碟管理公用程式中、初始化新的 LUN 、並建立具有所需名稱和磁碟機代號的磁碟區。勾選 * 啟用多重路徑 * 方塊、然後按一下 * 確定 * 以連線至 LUN 。

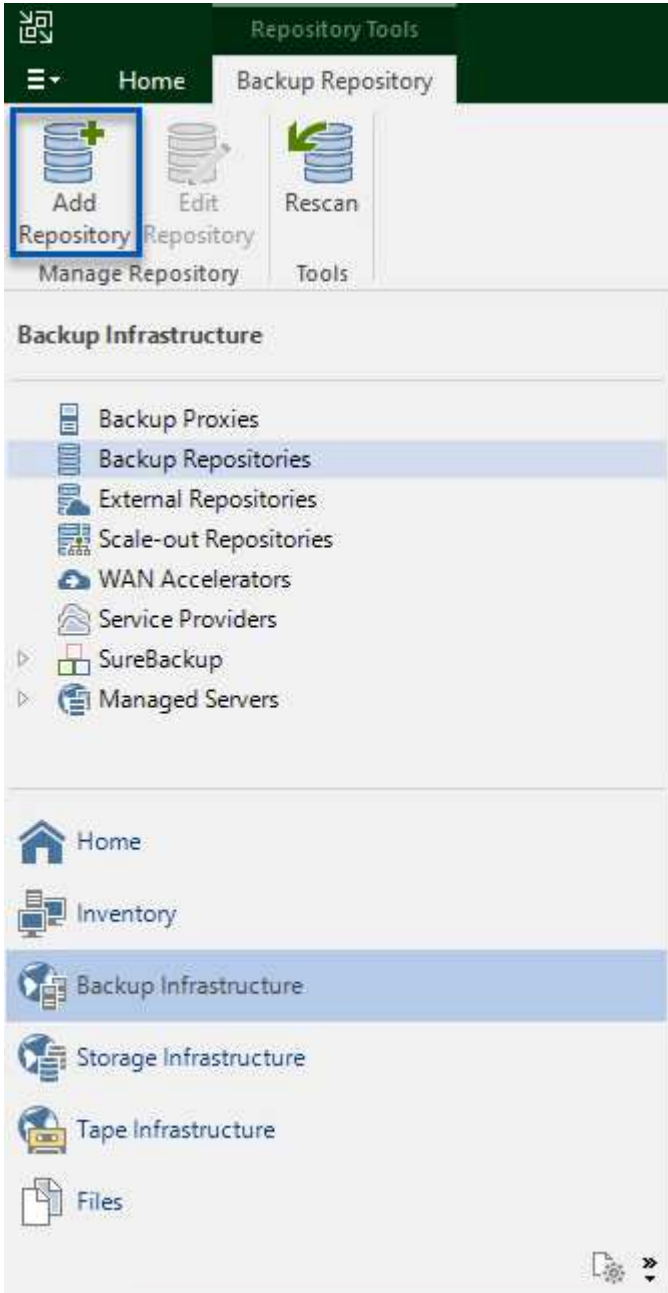


8. 重複這些步驟、在 Veeam Proxy 伺服器上掛載 iSCSI 磁碟區。

建立 Veeam 備份儲存庫

在 Veeam Backup and Replication 主控台中、為 Veeam Backup 和 Veeam Proxy 伺服器建立備份儲存庫。這些儲存庫將作為虛擬機器備份的備份目標。

1. 在 Veeam Backup and Replication 主控台中、按一下左下角的 * Backup Infrastructure* 、然後選取 * 新增儲存庫 *



2. 在「新增備份儲存庫」精靈中、輸入儲存庫的名稱、然後從下拉式清單中選取伺服器、然後按一下「* 填入 *」按鈕以選擇要使用的 NTFS 磁碟區。

**Server**


Choose repository server. You can select server from the list of managed servers added to the console.

Name	Repository server:																																																									
Server	veeamproxy.demozone.com (Created by VEEAMSRV\Administrator at 12/22/2022 9) Add New...																																																									
Repository	<table border="1"><thead><tr><th>Path</th><th>Capacity</th><th>Free</th></tr></thead><tbody><tr><td>C:\</td><td>89.4 GB</td><td>74 GB</td></tr><tr><td>E:\</td><td>1.9 TB</td><td>1.9 TB</td></tr><tr><td> </td><td> </td><td> </td></tr><tr><td> </td><td> </td><td> </td></tr><tr><td> </td><td> </td><td> </td></tr><tr><td> </td><td> </td><td> </td></tr><tr><td> </td><td> </td><td> </td></tr><tr><td> </td><td> </td><td> </td></tr><tr><td> </td><td> </td><td> </td></tr><tr><td> </td><td> </td><td> </td></tr><tr><td> </td><td> </td><td> </td></tr><tr><td> </td><td> </td><td> </td></tr><tr><td> </td><td> </td><td> </td></tr><tr><td> </td><td> </td><td> </td></tr><tr><td> </td><td> </td><td> </td></tr><tr><td> </td><td> </td><td> </td></tr><tr><td> </td><td> </td><td> </td></tr><tr><td> </td><td> </td><td> </td></tr></tbody></table>	Path	Capacity	Free	C:\	89.4 GB	74 GB	E:\	1.9 TB	1.9 TB																																																
Path	Capacity	Free																																																								
C:\	89.4 GB	74 GB																																																								
E:\	1.9 TB	1.9 TB																																																								
Mount Server	Populate																																																									
Review																																																										
Apply																																																										
Summary																																																										

< Previous Next > Finish Cancel

3. 在下一頁中、選擇在執行進階還原時、用來將備份掛載到的掛載伺服器。依預設、這是連接儲存庫儲存設備的相同伺服器。
4. 檢閱您的選擇、然後按一下 * 套用 * 以開始建立備份儲存庫。

New Backup Repository ✕

 **Review**
Please review the settings, and click Apply to continue.

Name
Server
Repository
Mount Server
Review
Apply
Summary

The following components will be processed on server veeamproxy.demozone.com:

Component name	Status
Transport	already exists
vPower NFS	will be installed
Mount Server	will be installed

Search the repository for existing backups and import them automatically
 Import guest file system index data to the catalog

< Previous **Apply** Finish Cancel

5. 對任何其他 Proxy 伺服器重複這些步驟。

設定 Veeam 備份工作

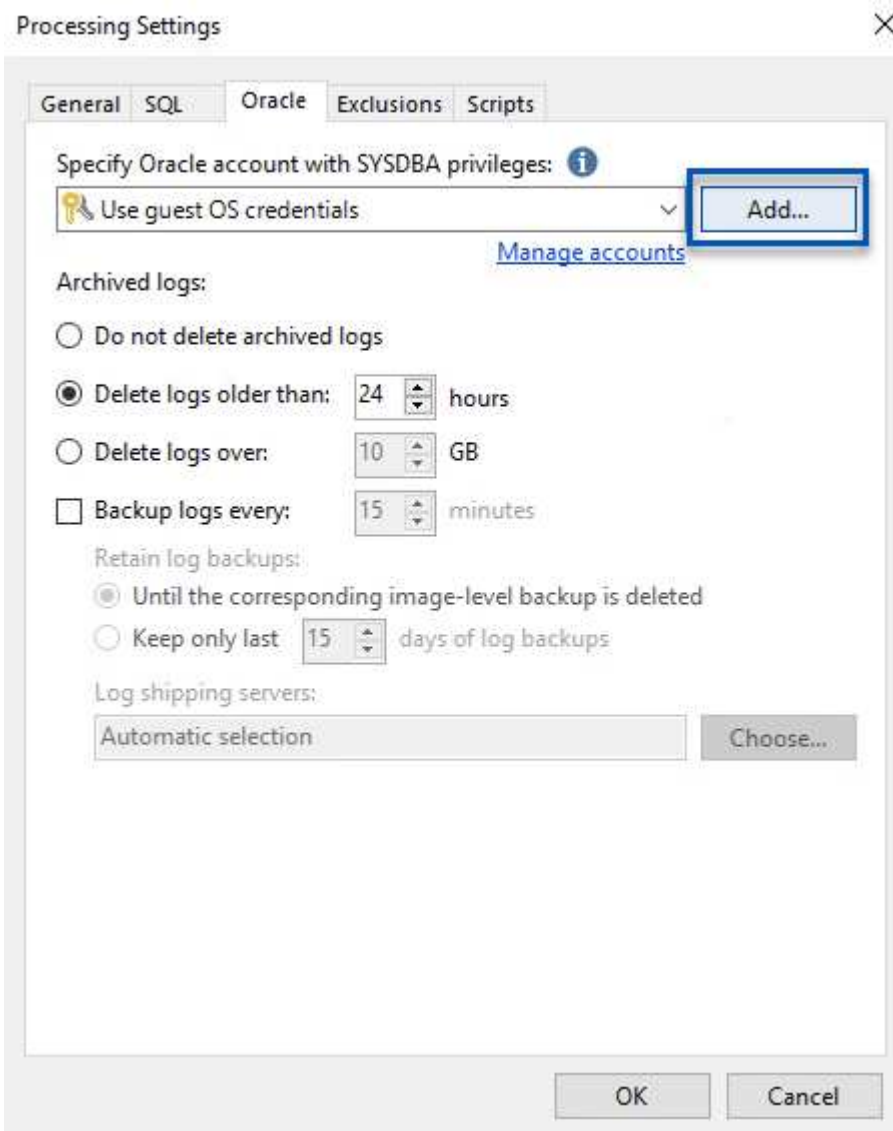
應使用上一節的備份儲存庫來建立備份工作。建立備工作務是任何儲存系統管理員的正常作業、我們並未涵蓋此處的所有步驟。如需在Veeam中建立備份工作的完整資訊、請參閱 "[Veeam說明中心技術文件](#)"。

在本解決方案中、會針對下列項目分別建立備份工作：

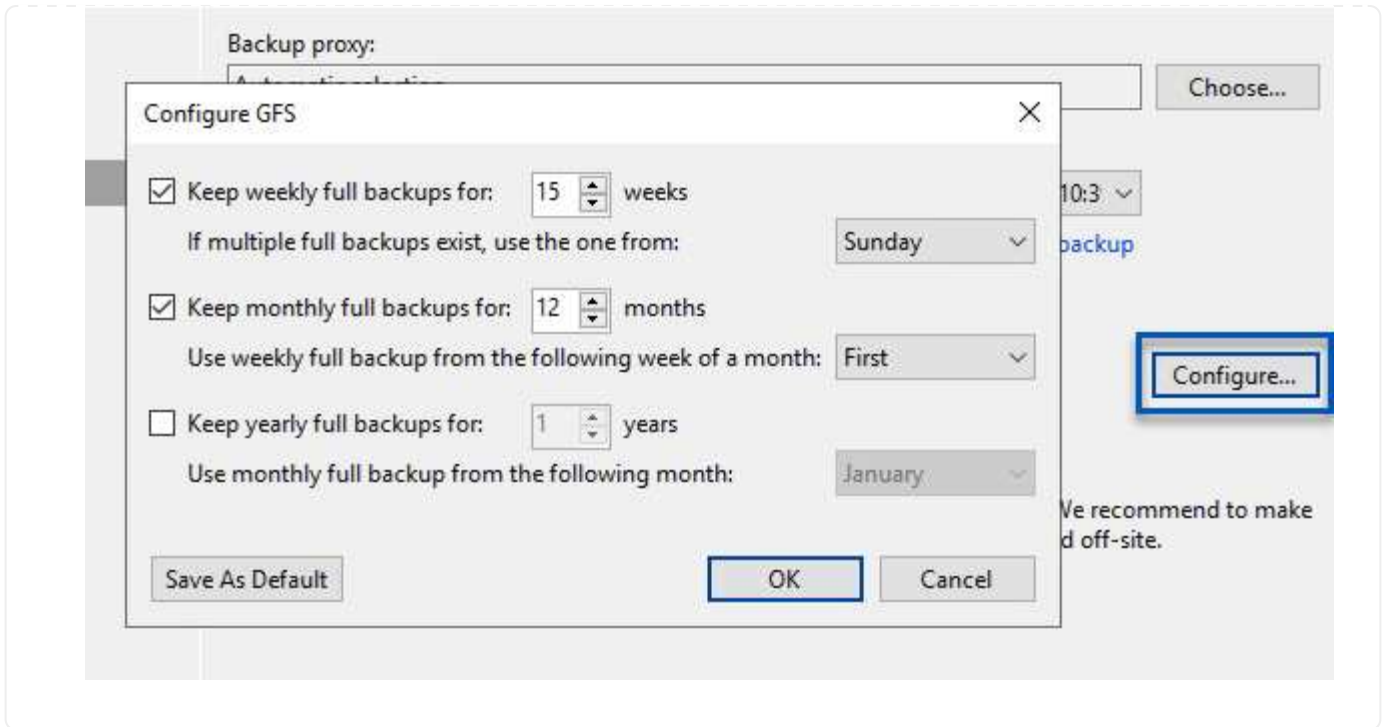
- Microsoft Windows SQL Server
- Oracle 資料庫伺服器
- Windows 檔案伺服器
- Linux 檔案伺服器

設定 Veeam 備份工作時的一般考量

1. 啟用應用程式感知處理、以建立一致的備份並執行交易記錄處理。
2. 啟用應用程式感知處理後、請將具有管理員權限的正確認證新增至應用程式、因為這可能與來賓作業系統認證不同。



3. 若要管理備份的保留原則、請勾選 * 保留某些完整備份以供歸檔之用 *、然後按一下 * 組態 ... * 按鈕以設定原則。



使用 Veeam 完整還原還原應用程式 VM

使用 Veeam 執行完整還原是執行應用程式還原的第一步。我們驗證了 VM 的完整還原功能已開啟、而且所有服務都正常執行。

還原伺服器是任何儲存系統管理員的常用項目之一、我們並未涵蓋此處的所有步驟。如需在 Veeam 中執行完整還原的完整資訊、請參閱 "[Veeam說明中心技術文件](#)"。

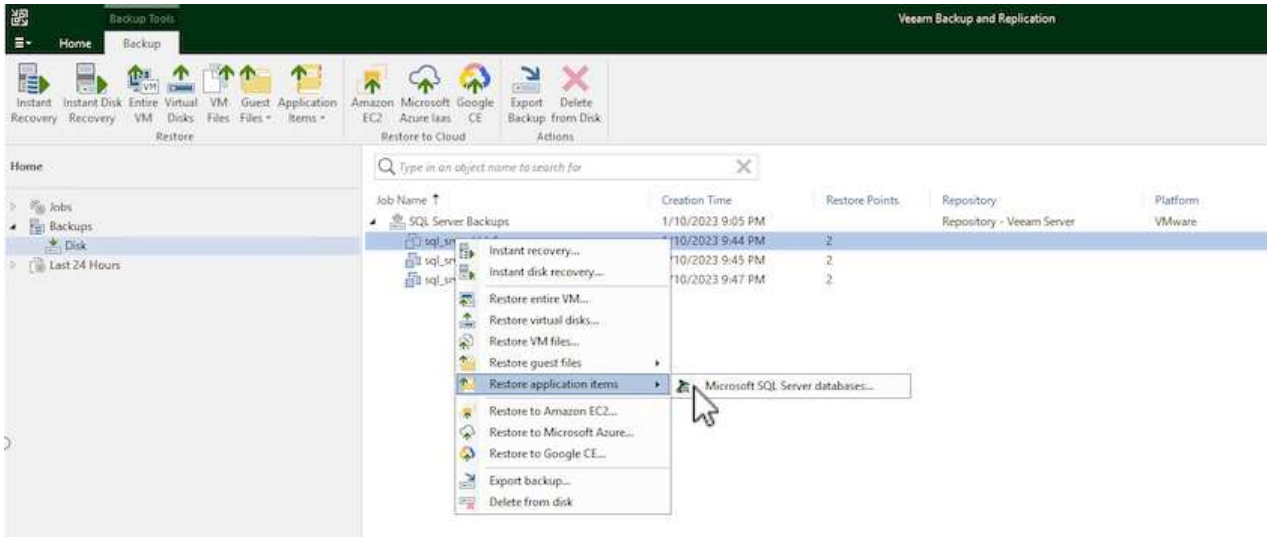
還原 SQL Server 資料庫

Veeam 備份與複寫提供數種還原 SQL Server 資料庫的選項。在此驗證中、我們使用 Veeam Explorer for SQL Server 搭配 Instant Recovery 來執行 SQL Server 資料庫的還原。SQL Server Instant Recovery 是一項功能、可讓您快速還原 SQL Server 資料庫、而無需等待完整的資料庫還原。這項快速恢復程序可將停機時間降至最低、並確保業務持續運作。其運作方式如下：

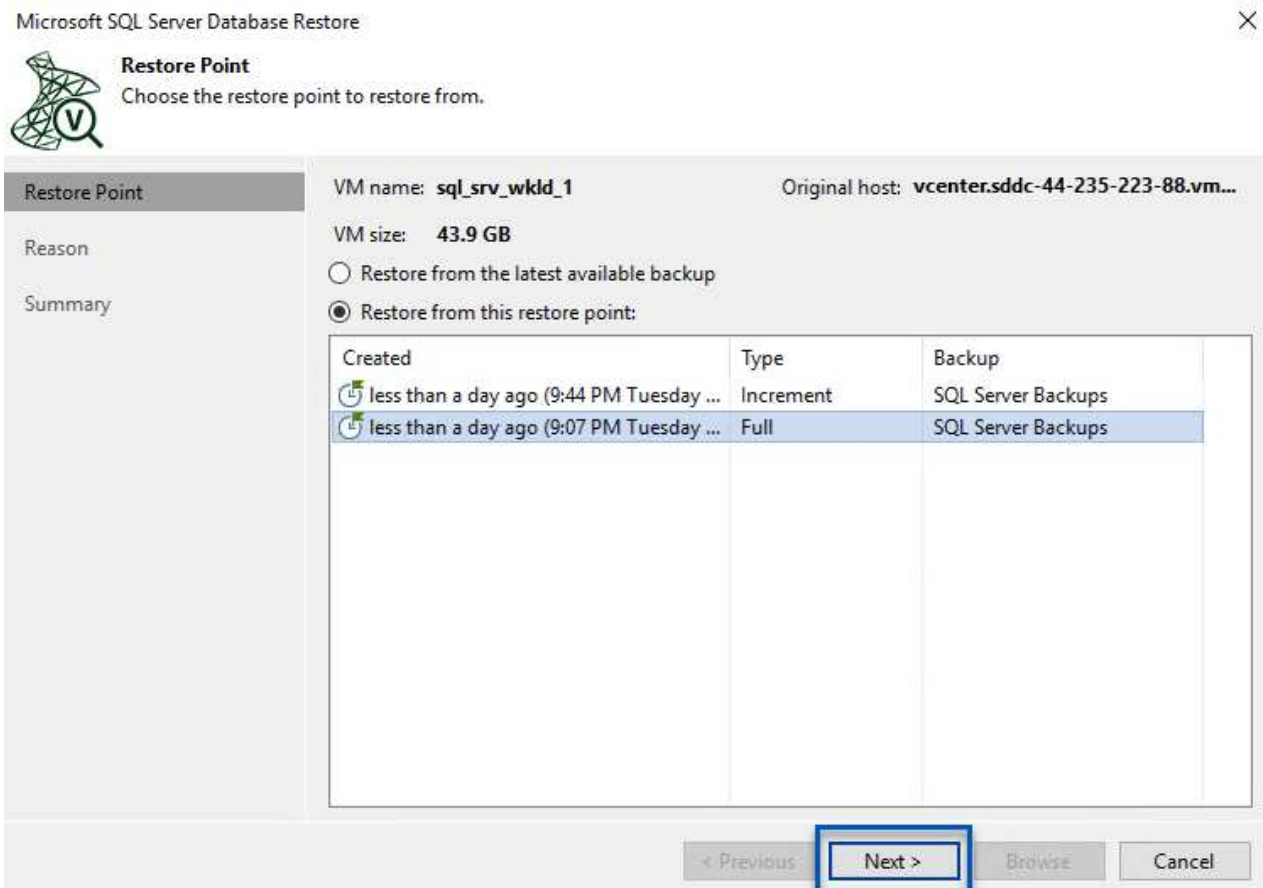
- Veeam Explorer * 裝載包含要還原的 SQL Server 資料庫的備份 * 。
- 軟體 * 直接從掛載的檔案發佈資料庫 * 、使其可在目標 SQL Server 執行個體上作為暫存資料庫存取。
- 在使用暫存資料庫時、Veeam Explorer * 會將使用者查詢 * 重新導向至此資料庫、確保使用者可以繼續存取及使用資料。
- 在背景中、Veeam * 會執行完整的資料庫還原 * 、將資料從暫存資料庫傳輸到原始資料庫位置。
- 完整資料庫還原完成後、Veeam Explorer * 會將使用者查詢切換回原始 * 資料庫、並移除暫存資料庫。

使用 Veeam Explorer Instant Recovery 還原 SQL Server 資料庫

1. 在 Veeam 備份與複寫主控台中、瀏覽至 SQL Server 備份清單、在伺服器上按一下滑鼠右鍵、然後選取 * 還原應用程式項目 *、再選取 * Microsoft SQL Server 資料庫 ... *。



2. 在 Microsoft SQL Server 資料庫還原精靈中、從清單中選取還原點、然後按一下 * 下一步 *。



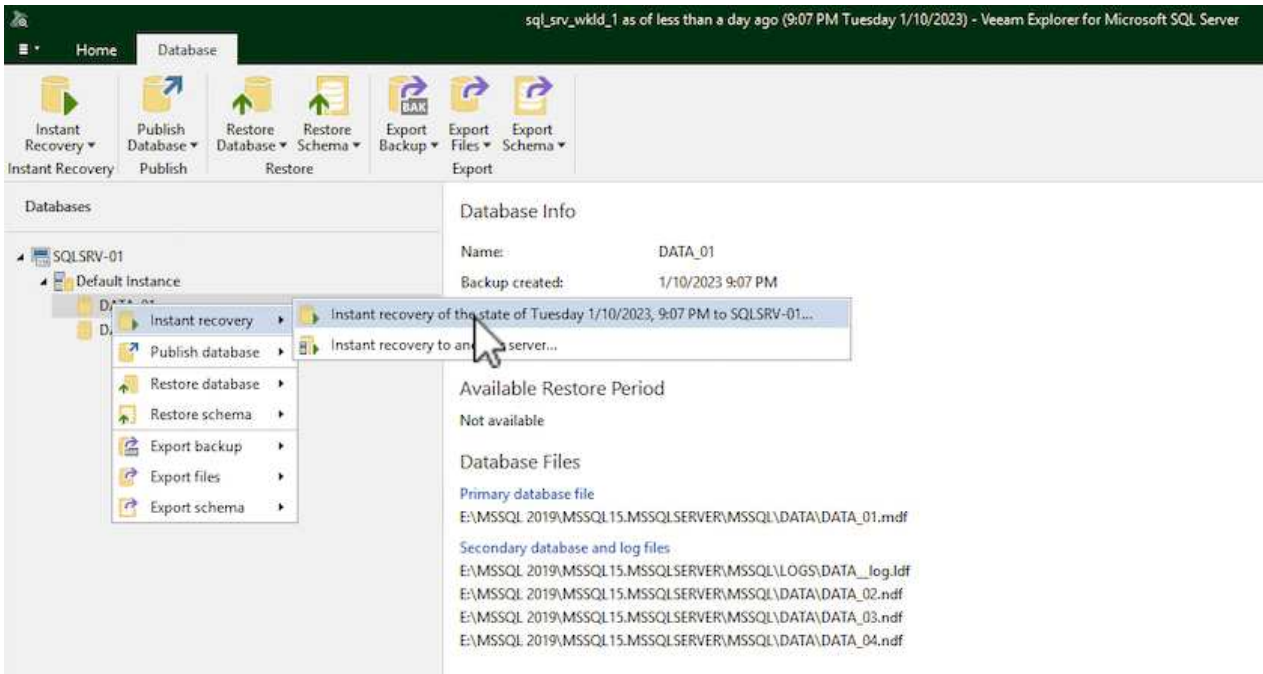
3. 如有需要、請輸入 * 還原原因 *、然後按一下「摘要」頁面上的 * 瀏覽 * 按鈕、啟動適用於 Microsoft SQL Server 的 Veeam Explorer。

**Summary**

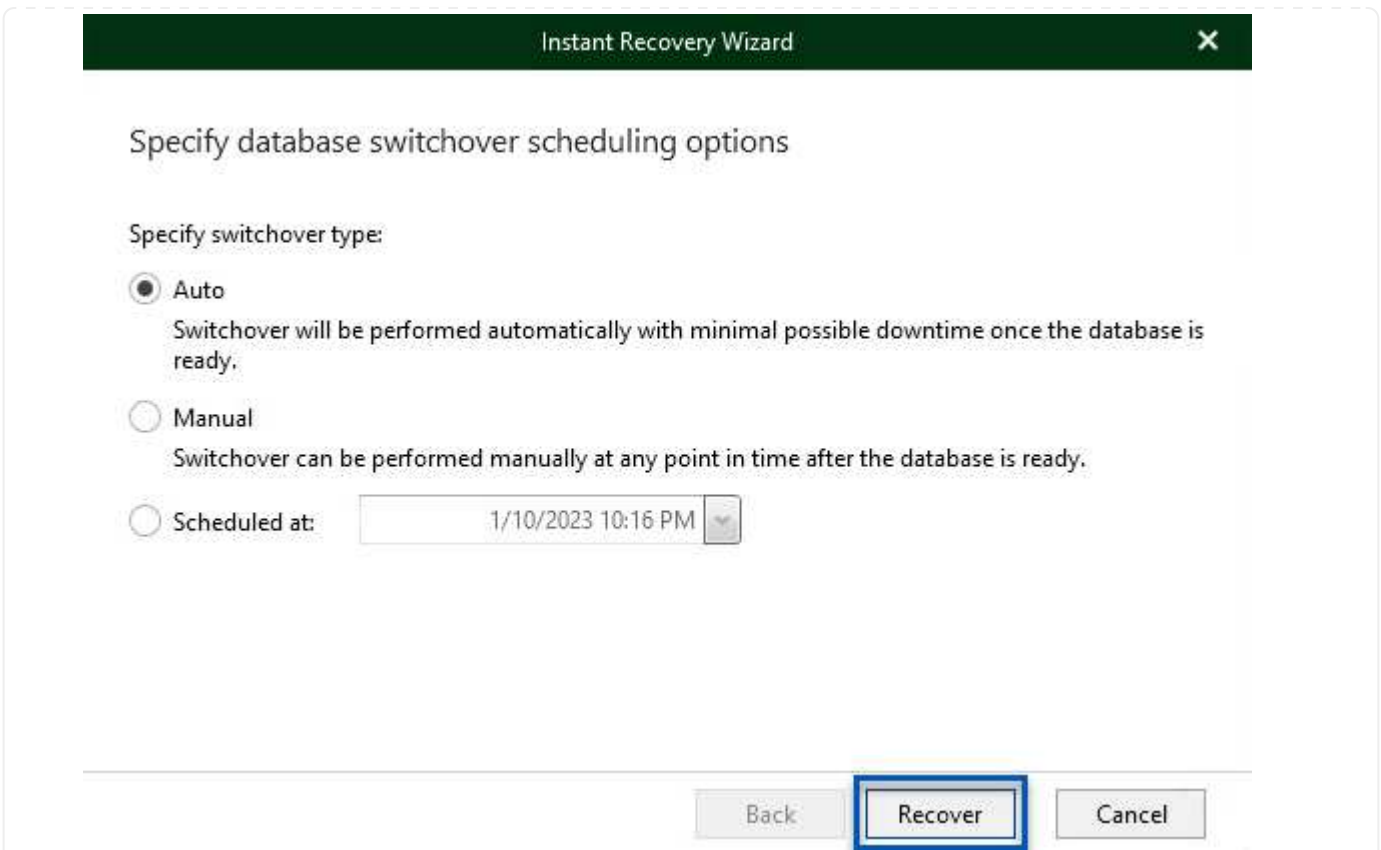
Review the restore settings, and click Browse to exit the wizard and open Veeam Explorer for SQL Server, where you will select databases to restore.

Restore Point	Summary: VM name: sql_srv_wkld_1 Restore point: Current: sql_srv_wkld_1 less than a day ago (9:07 PM Tuesday 1/10/2023)
Reason	
Summary	

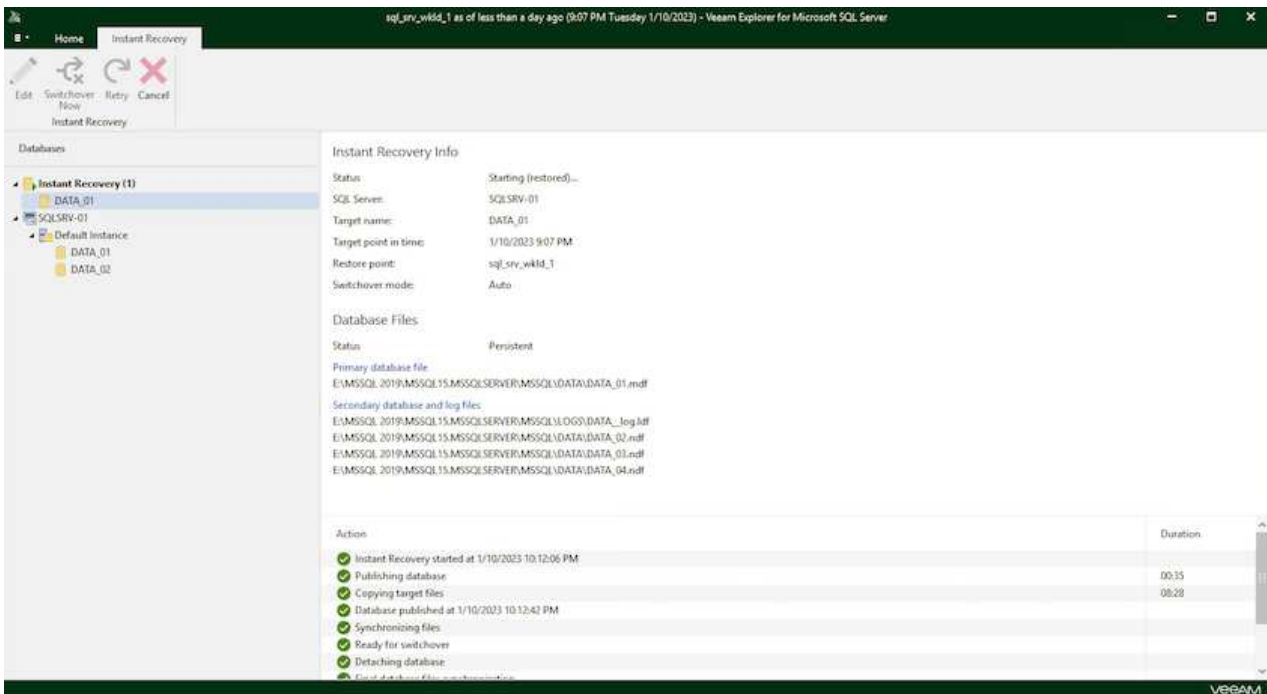
- 在 Veeam Explorer 中展開資料庫執行個體清單、按一下滑鼠右鍵並選取 * 立即還原 * 、然後選取要還原的特定還原點。



- 在即時恢復嚮導中指定轉換類型。這可以在最短停機時間內自動進行、手動或在指定時間進行。然後按一下 * 恢復 * 按鈕開始還原程序。



6. 可從 Veeam Explorer 監控還原程序。



如需使用 Veeam Explorer 執行 SQL Server 還原作業的詳細資訊、請參閱中的 Microsoft SQL Server 一節 "Veeam Explorers 使用者指南"。

使用 Veeam Explorer 還原 Oracle 資料庫

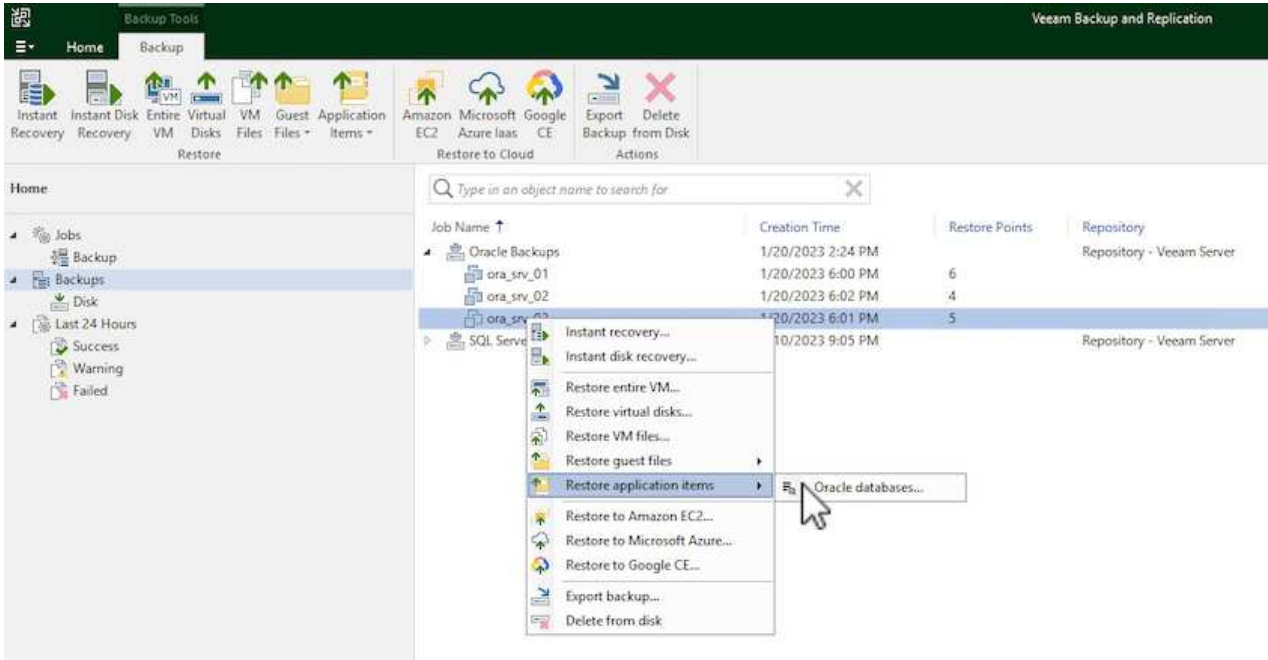
Veeam Explorer for Oracle 資料庫提供使用 Instant Recovery 執行標準 Oracle 資料庫還原或不中斷還原的功能。它也支援發佈資料庫、可快速存取、還原 Data Guard 資料庫、以及從 RMAN 備份還原。

如需使用 Veeam Explorer 執行 Oracle 資料庫還原作業的詳細資訊、請參閱中的 Oracle 一節 "[Veeam Explorers 使用者指南](#)"。

使用 Veeam Explorer 還原 Oracle 資料庫

在本節中、使用 Veeam Explorer 將 Oracle 資料庫還原至不同的伺服器。

1. 在 Veeam 備份與複寫主控台中、瀏覽至 Oracle 備份清單、在伺服器上按一下滑鼠右鍵、然後選取 * 還原應用程式項目 *、再選取 * Oracle 資料庫 ... *。



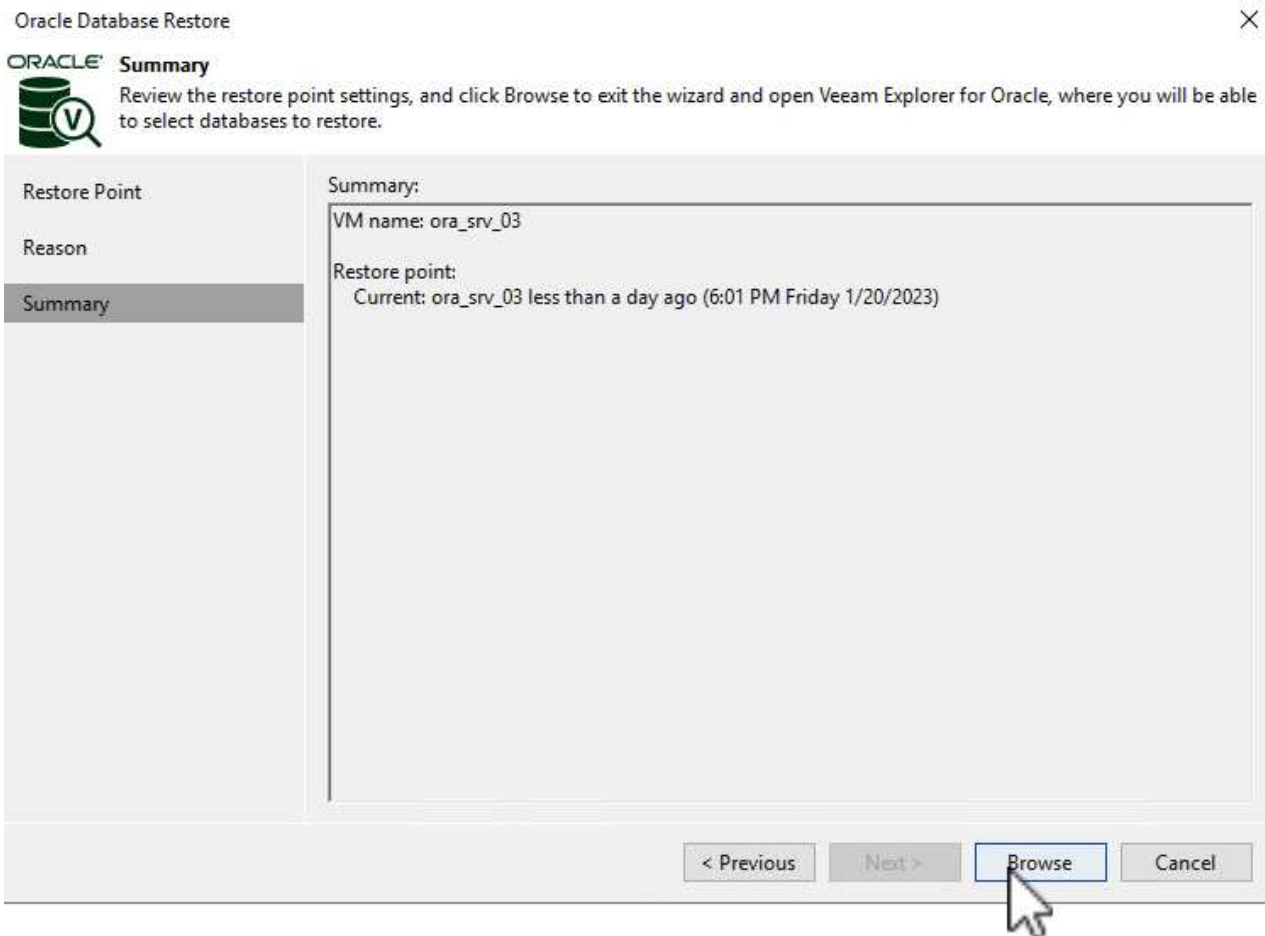
2. 在 Oracle 資料庫還原精靈中、從清單中選取還原點、然後按一下 * 下一步 *。

**Restore Point**

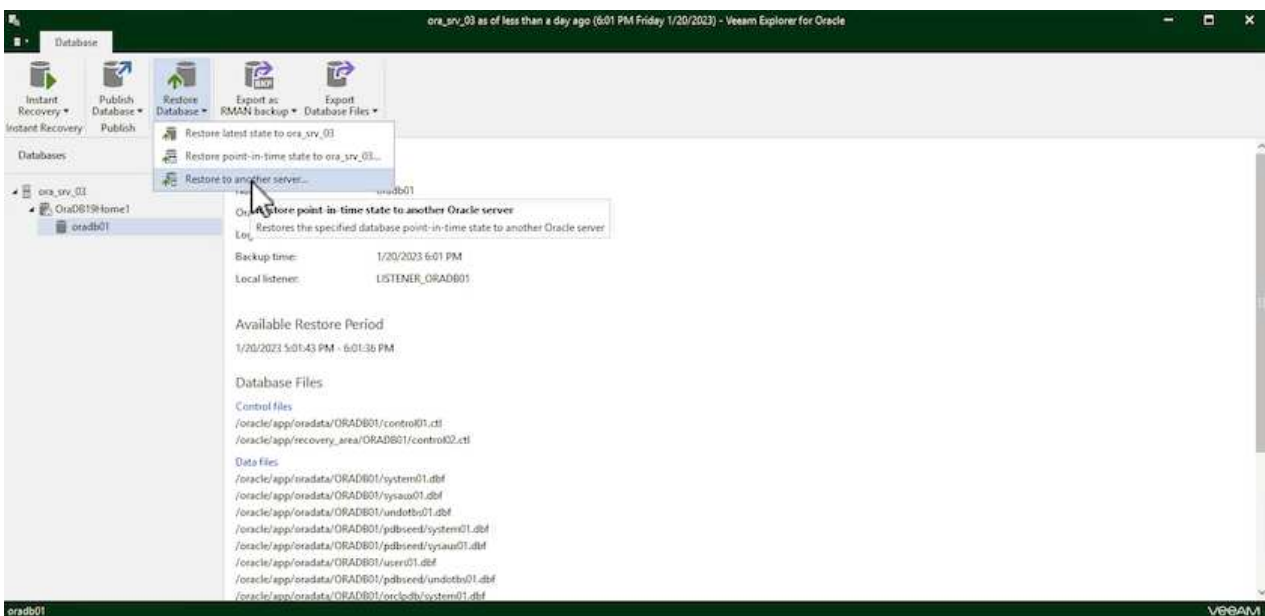
Choose the restore point to restore from.

Restore Point	VM name: ora_srv_03	Original host: vcenter.sddc-44-235-223-88.vm...																		
Reason	VM size: 38.5 GB																			
Summary	<input checked="" type="radio"/> Restore from the latest available backup																			
	<input type="radio"/> Restore from this restore point:																			
	<table border="1"><thead><tr><th>Created</th><th>Type</th><th>Backup</th></tr></thead><tbody><tr><td> less than a day ago (6:01 PM Friday 1/...</td><td>Increment</td><td>Oracle Backups</td></tr><tr><td> less than a day ago (5:01 PM Friday 1/...</td><td>Increment</td><td>Oracle Backups</td></tr><tr><td> less than a day ago (4:02 PM Friday 1/...</td><td>Increment</td><td>Oracle Backups</td></tr><tr><td> less than a day ago (3:47 PM Friday 1/...</td><td>Increment</td><td>Oracle Backups</td></tr><tr><td> less than a day ago (2:47 PM Friday 1/...</td><td>Full</td><td>Oracle Backups</td></tr></tbody></table>	Created	Type	Backup	less than a day ago (6:01 PM Friday 1/...	Increment	Oracle Backups	less than a day ago (5:01 PM Friday 1/...	Increment	Oracle Backups	less than a day ago (4:02 PM Friday 1/...	Increment	Oracle Backups	less than a day ago (3:47 PM Friday 1/...	Increment	Oracle Backups	less than a day ago (2:47 PM Friday 1/...	Full	Oracle Backups	
Created	Type	Backup																		
less than a day ago (6:01 PM Friday 1/...	Increment	Oracle Backups																		
less than a day ago (5:01 PM Friday 1/...	Increment	Oracle Backups																		
less than a day ago (4:02 PM Friday 1/...	Increment	Oracle Backups																		
less than a day ago (3:47 PM Friday 1/...	Increment	Oracle Backups																		
less than a day ago (2:47 PM Friday 1/...	Full	Oracle Backups																		
	<input type="button" value=" < Previous"/>	<input type="button" value=" Next >"/>																		
	<input type="button" value=" Browse"/>	<input type="button" value=" Cancel"/>																		

3. 如有需要、請輸入 * 還原原因 *、然後在「摘要」頁面上按一下 * 瀏覽 * 按鈕、啟動 Veeam Explorer for Oracle。



4. 在 Veeam Explorer 中展開資料庫執行個體清單、按一下要還原的資料庫、然後從頂端的 * 還原資料庫 * 下拉式功能表中選取 * 還原至其他伺服器 ... * 。



5. 在還原精靈中指定還原點、然後按一下 * 下一步 * 。

Specify restore point


Specify point in time you want to restore the database to:

 Restore to the point in time of the selected image-level backup Restore to a specific point in time (requires redo log backups)5:01 PM
1/20/20236:01 PM
1/20/2023

Friday, January 20, 2023 6:01 PM

 Perform restore to the specific transaction

Enables you to review major database transactions around the selected time, and restore the database to the moment in time right before the unwanted change.

 To enable this functionality, specify the staging Oracle server under Menu > Options.

Back

Next

Cancel

6. 指定要還原資料庫的目標伺服器 and 帳戶認證、然後按一下 * 下一步 * 。

Specify target Linux server connection credentials

Server: ora_srv_01

SSH port: 22

Account: oracle

Advanced...

Password: [Click here to change the password]

 Private key is required for this connection

Private key:

Browse...

Passphrase:

Back

Next

Cancel

7. 最後、指定資料庫檔案的目標位置、然後按一下 * 還原 * 按鈕開始還原程序。

Specify database files target location

Control files

- /oracle/app/oradata/oradb01/control01.ctl
- /oracle/app/recovery_area/oradb01/control02.ctl

Data files

- /oracle/app/oradata/oradb01/system01.dbf
- /oracle/app/oradata/oradb01/sysaux01.dbf
- /oracle/app/oradata/oradb01/undotbs01.dbf
- /oracle/app/oradata/oradb01/pdbseed/system01.dbf
- /oracle/app/oradata/oradb01/pdbseed/sysaux01.dbf
- /oracle/app/oradata/oradb01/users01.dbf

Back

Restore

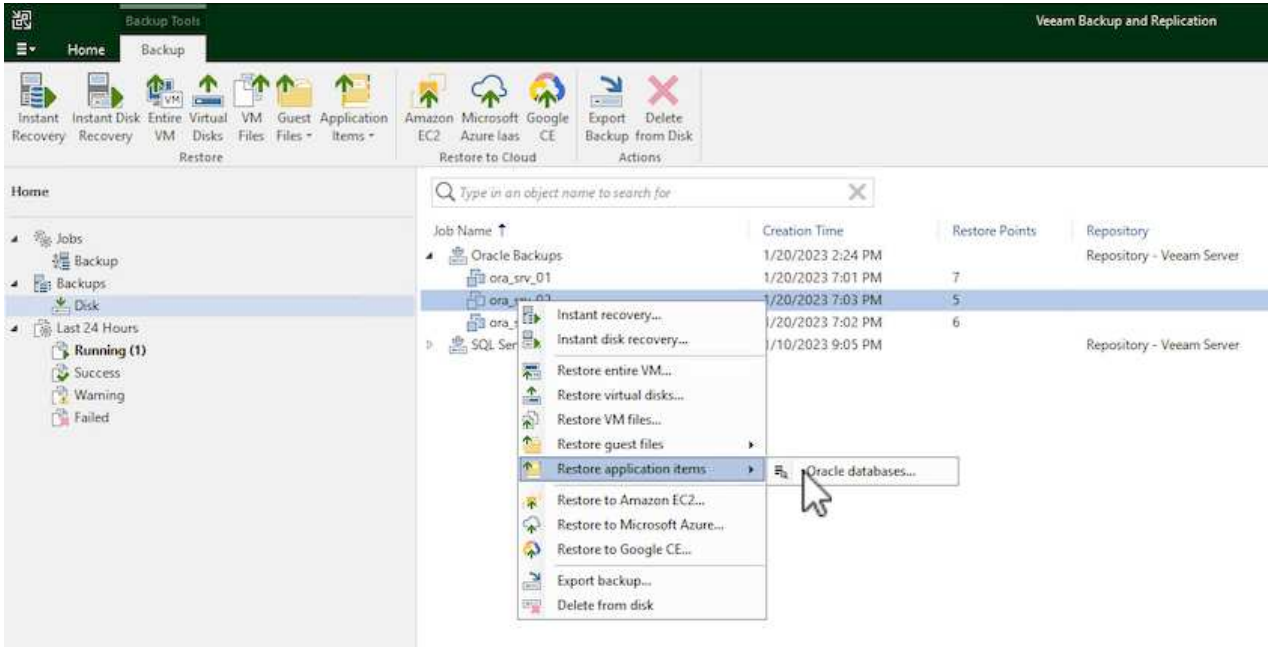
Cancel

8. 資料庫恢復完成後、請檢查伺服器上的 Oracle 資料庫是否正確啟動。

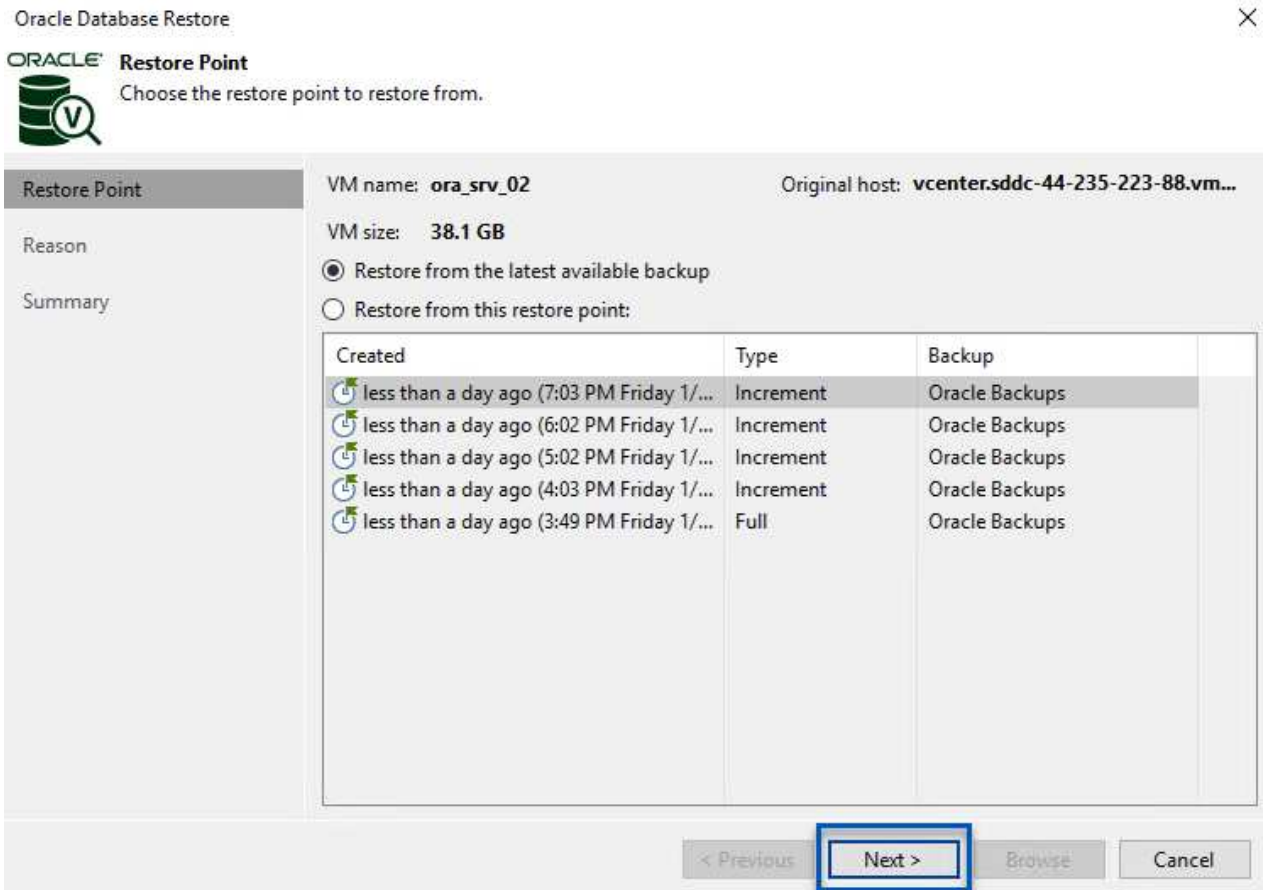
將 Oracle 資料庫發佈至替代伺服器

在本節中、資料庫會發佈到替代伺服器、以便在不啟動完整還原的情況下快速存取。

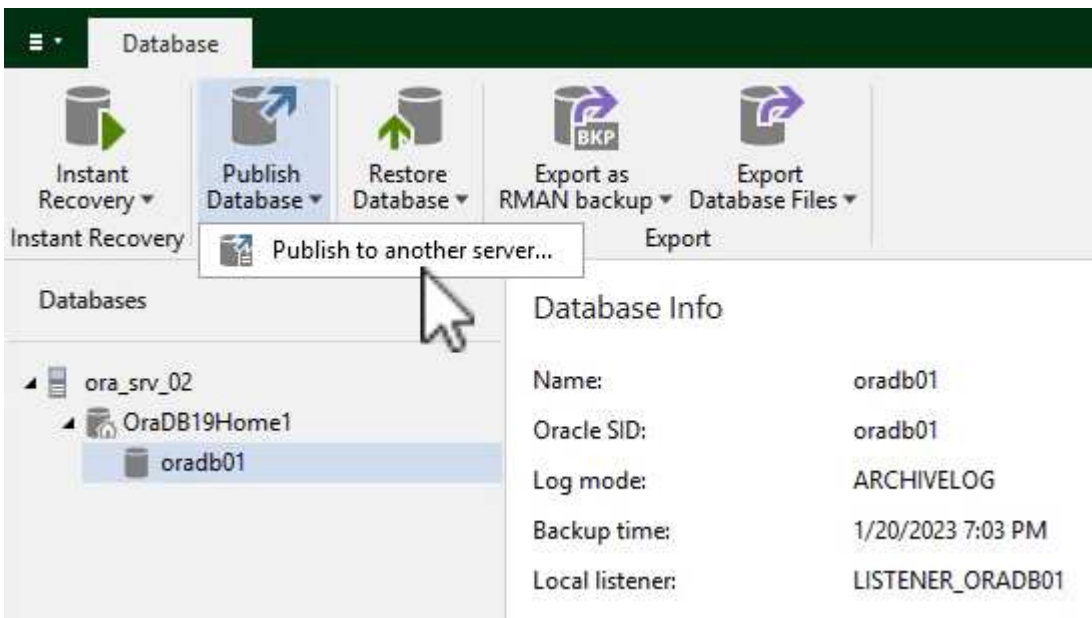
1. 在 Veeam 備份與複寫主控台中、瀏覽至 Oracle 備份清單、在伺服器上按一下滑鼠右鍵、然後選取 * 還原應用程式項目 *、再選取 * Oracle 資料庫 ... *。



2. 在 Oracle 資料庫還原精靈中、從清單中選取還原點、然後按一下 * 下一步 *。



3. 如有需要、請輸入 * 還原原因 *、然後在「摘要」頁面上按一下 * 瀏覽 * 按鈕、啟動 Veeam Explorer for Oracle。
4. 在 Veeam Explorer 中展開資料庫執行個體清單、按一下要還原的資料庫、然後從頂端的 * 發佈資料庫 * 下拉式功能表中選取 * 發佈至其他伺服器 ... *。



5. 在發佈精靈中、指定要發佈資料庫的還原點、然後按一下 * 下一步 *。
6. 最後、指定目標 Linux 檔案系統位置、然後按一下 * Publish * 開始還原程序。

Specify Oracle settings

 Restore to the original location Restore to a different location:Oracle Home: Global Database Name: Oracle SID:

7. 當發佈完成後、請登入目標伺服器並執行下列命令、以確保資料庫正在執行：

```
oracle@ora_srv_01> sqlplus / as sysdba
```

```
SQL> select name, open_mode from v$database;
```



```
oracle@ora_srv_01:~  
File Edit View Search Terminal Help  
[oracle@ora_srv_01 ~]$ sqlplus / as sysdba  
  
SQL*Plus: Release 19.0.0.0.0 - Production on Fri Jan 20 16:46:39 2023  
Version 19.3.0.0.0  
  
Copyright (c) 1982, 2019, Oracle. All rights reserved.  
  
Connected to:  
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production  
Version 19.3.0.0.0  
  
SQL> select name, open_mode from v$database;  
  
NAME          OPEN_MODE  
-----  
ORADB01      READ WRITE
```

結論

VMware Cloud 是執行業務關鍵應用程式及儲存敏感資料的強大平台。對於仰賴 VMware Cloud 的企業而言、安全的資料保護解決方案是不可或缺的、可確保業務持續運作、並協助防範網路威脅和資料遺失。選擇可靠且健全的資料保護解決方案、企業就能確信關鍵資料安全無虞、不受任何影響。

本文件中的使用案例著重於備受肯定的資料保護技術、強調 NetApp、VMware 和 Veeam 之間的整合。FSX for ONTAP 在 AWS 中支援做為 VMware Cloud 的補充 NFS 資料存放區、並用於所有虛擬機器和應用程式資料。Veeam 備份與複寫是一套全方位的資料保護解決方案、旨在協助企業改善、自動化及簡化備份與還原程序。Veeam 與 ONTAP 的 FSX 上託管的 iSCSI 備份目標磁碟區搭配使用、可為位於 VMware Cloud 的應用程式資料提供安全且易於管理的資料保護解決方案。

其他資訊

若要深入瞭解本解決方案所提供的技術、請參閱下列其他資訊。

- ["適用於 ONTAP 的 FSX 使用者指南"](#)
- ["Veeam說明中心技術文件"](#)
- ["VMware Cloud on AWS 支援。考量與限制"](#)

TR-4955：使用FSX進行災難恢復ONTAP、以利實現VMware vCenter與VMC（AWS VMware Cloud）

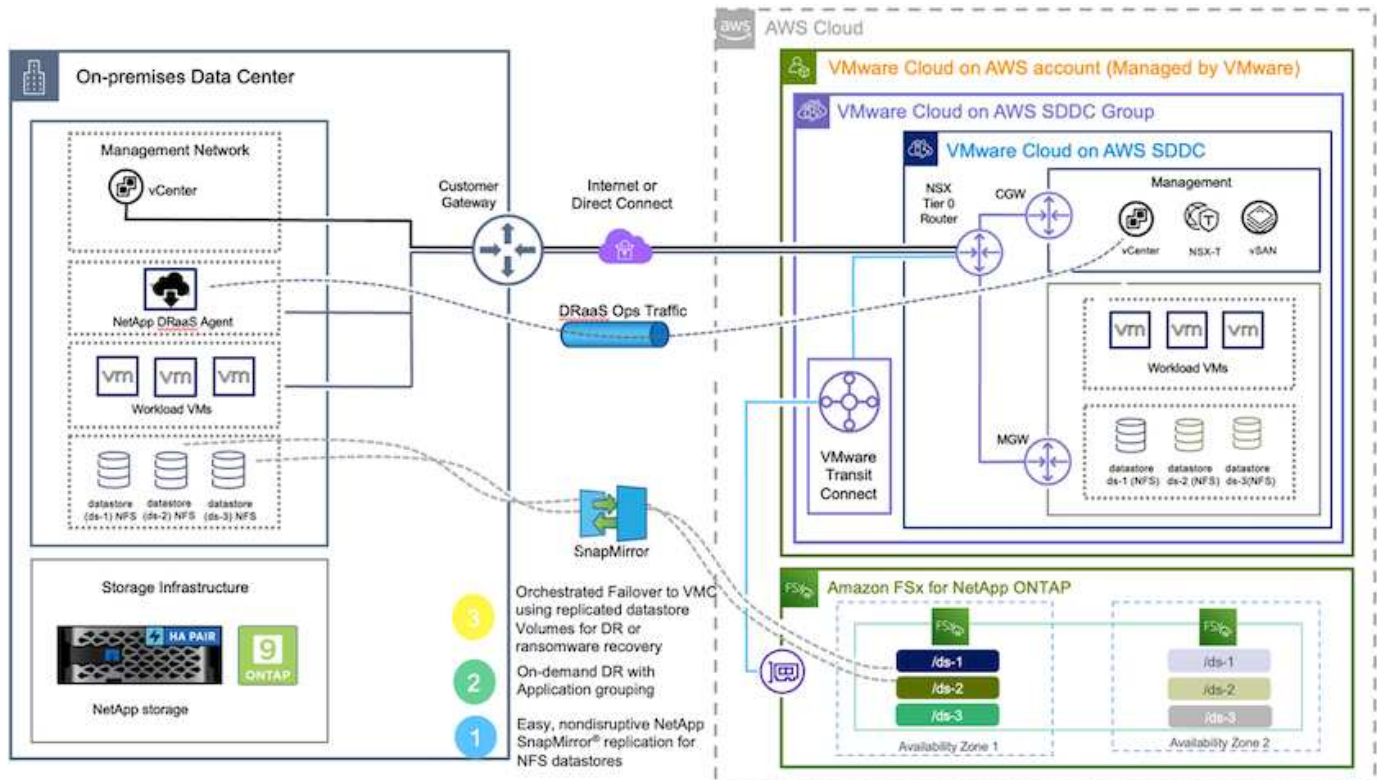
災難恢復協調程式（DRO；含UI的指令碼解決方案）可用來無縫恢復從內部部署複寫到FSX以ONTAP 供支援的工作負載。DRO透過VM登錄到VMC、將SnapMirror層級的還原作業自動化、並直接在NSS-T上進行網路對應所有VMC環境均隨附此功能。

NetApp公司Niyazz Mohamed

總覽

災難恢復至雲端是一種彈性且具成本效益的方法、可保護工作負載免受站台停機和資料毀損事件（例如勒索軟體）的影響。有了NetApp SnapMirror技術、內部部署的VMware工作負載可以複寫到FSX、ONTAP 以便在AWS中執行。

災難恢復協調程式（DRO；含UI的指令碼解決方案）可用來無縫恢復從內部部署複寫到FSX以ONTAP 供支援的工作負載。DRO透過VM登錄到VMC、將SnapMirror層級的還原作業自動化、並直接在NSS-T上進行網路對應所有VMC環境均隨附此功能。



快速入門

在AWS上部署及設定VMware Cloud

"AWS上的VMware Cloud" 為AWS生態系統中的VMware工作負載提供雲端原生體驗。每個VMware軟體定義資料中心（SDDC）都會在Amazon Virtual Private Cloud（VPC）上執行、並提供完整的VMware堆疊（包括vCenter Server）、NSX-T軟體定義網路、vSAN軟體定義儲存設備、以及一或多個ESXi主機、為工作負載提供運算與儲存資源。若要在AWS上設定VMC環境、請執行下列步驟 "連結"。也可將一個指示燈式叢集用於DR用途。



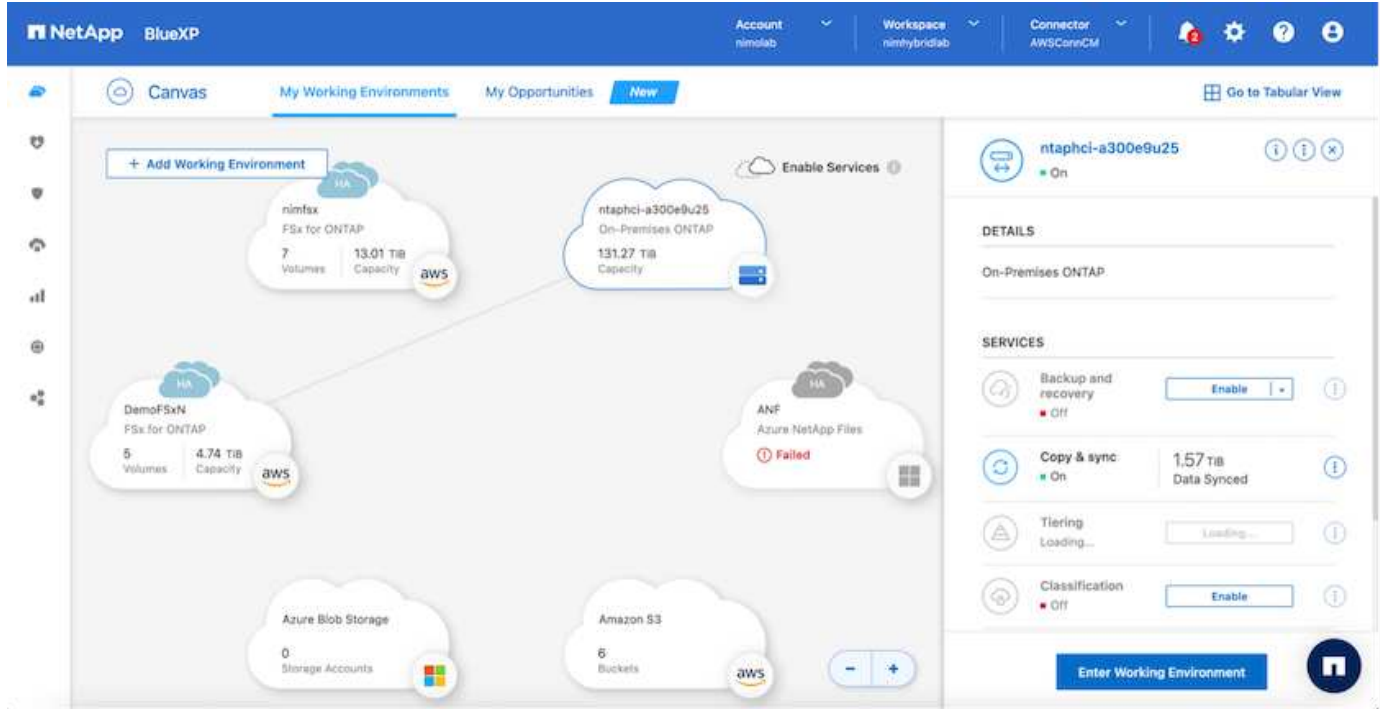
在初始版本中、DRO支援現有的指示燈叢集。隨需建立SDDC將於即將推出的版本中提供。

配置和設定FSXfor ONTAP Sf

Amazon FSX for NetApp ONTAP Sfing是一項全託管服務、以熱門的NetApp ONTAP Sfor NetApp文件系統為基礎、提供高度可靠、可擴充、高效能且功能豐富的檔案儲存設備。請依照下列步驟操作 "連結" 配置和設定FSXfor ONTAP Sf。

部署SnapMirror並將其設定為FSXfor ONTAP Sfor Sfor

下一步是使用NetApp BlueXP、探索AWS ONTAP 執行個體上已配置的FSX、並以ONTAP 適當的頻率將所需的資料存放區磁碟區從內部部署環境複寫到FSX以供使用、並保留NetApp Snapshot複本：



請遵循此連結中的步驟來設定BlueXP。您也可以使用NetApp ONTAP 的CLI來排程此連結的複寫作業。



SnapMirror關係是先決條件、必須事先建立。

DRO安裝

若要開始使用DRO、請在指定的EC2執行個體或虛擬機器上使用Ubuntu作業系統、以確保符合先決條件。然後安裝套件。

先決條件

- 請確定已連線至來源和目的地vCenter及儲存系統。
- 如果您使用DNS名稱、則應該已有DNS解析。否則、您應該使用vCenter和儲存系統的IP位址。
- 建立具有root權限的使用者。您也可以將Sudo與EC2執行個體搭配使用。

作業系統需求

- Ubuntu 20.04 (LTS) 、至少2 GB和4個vCPU
- 下列套件必須安裝在指定的代理VM上：
 - Docker
 - Docker編寫
 - Jq

變更權限 `docker.sock` : `sudo chmod 666 /var/run/docker.sock`。



◦ `deploy.sh` 指令碼會執行所有必要的先決條件。

安裝套件

1. 在指定的虛擬機器上下載安裝套件：

```
git clone https://github.com/NetApp/DRO-AWS.git
```



代理程式可安裝在內部部署或AWS VPC內。

2. 解壓縮套件、執行部署指令碼、然後輸入主機IP（例如、10.10.10.10）。

```
tar xvf DRO-prereq.tar
```

3. 瀏覽至目錄並執行部署指令碼、如下所示：

```
sudo sh deploy.sh
```

4. 使用下列項目存取UI：

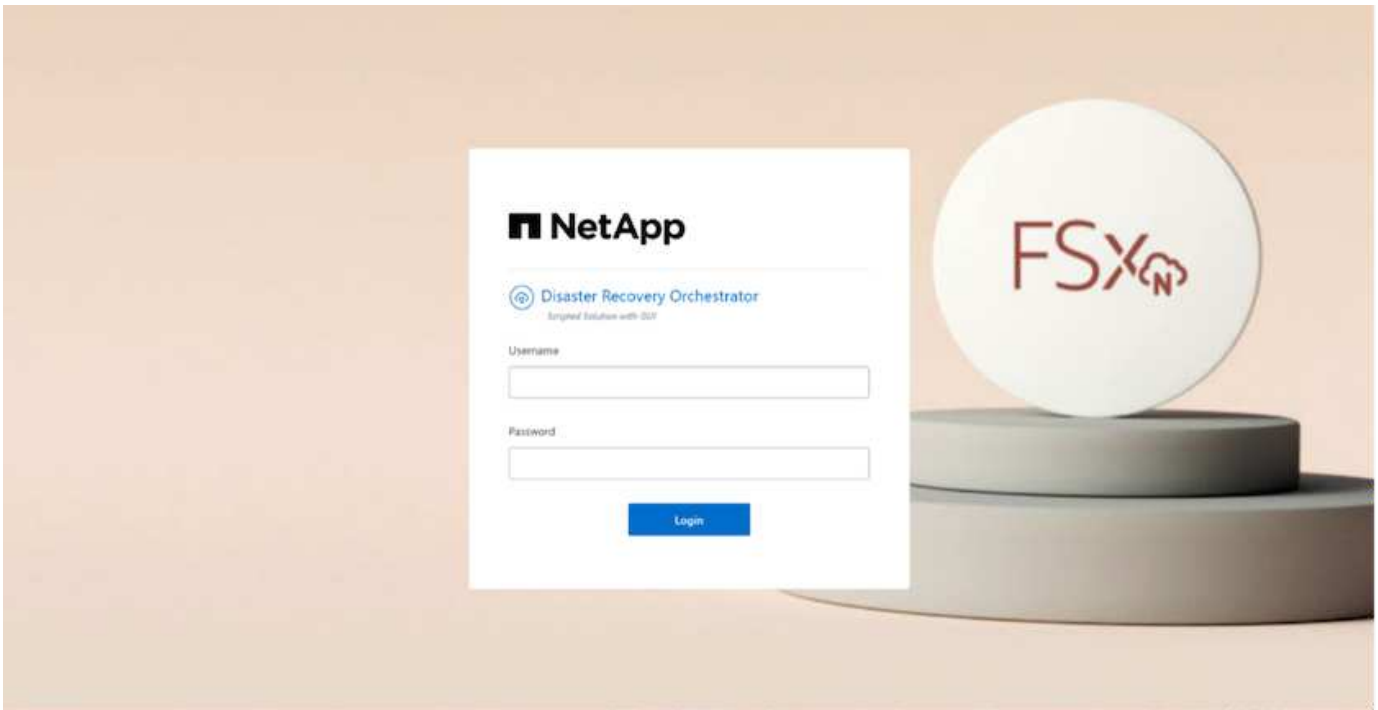
```
https://<host-ip-address>
```

使用下列預設認證：

```
Username: admin  
Password: admin
```



您可以使用「變更密碼」選項來變更密碼。



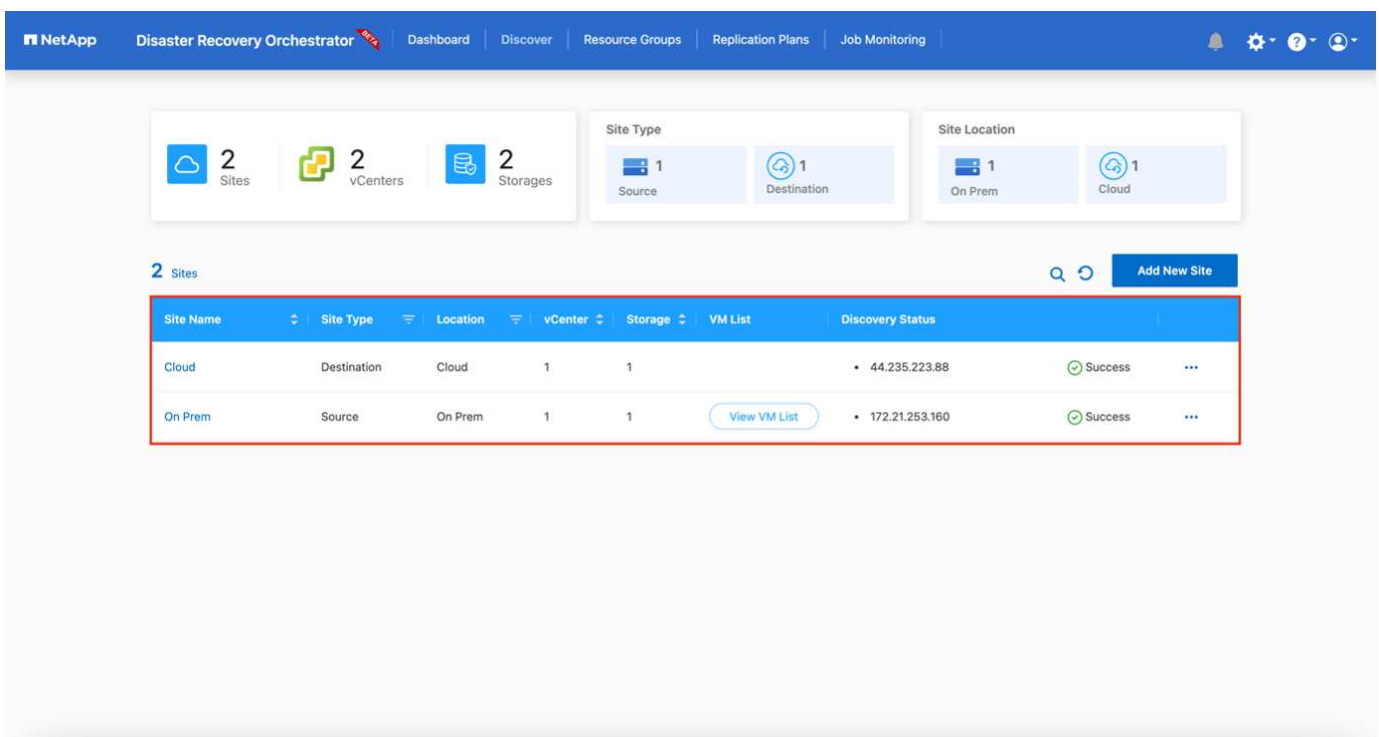
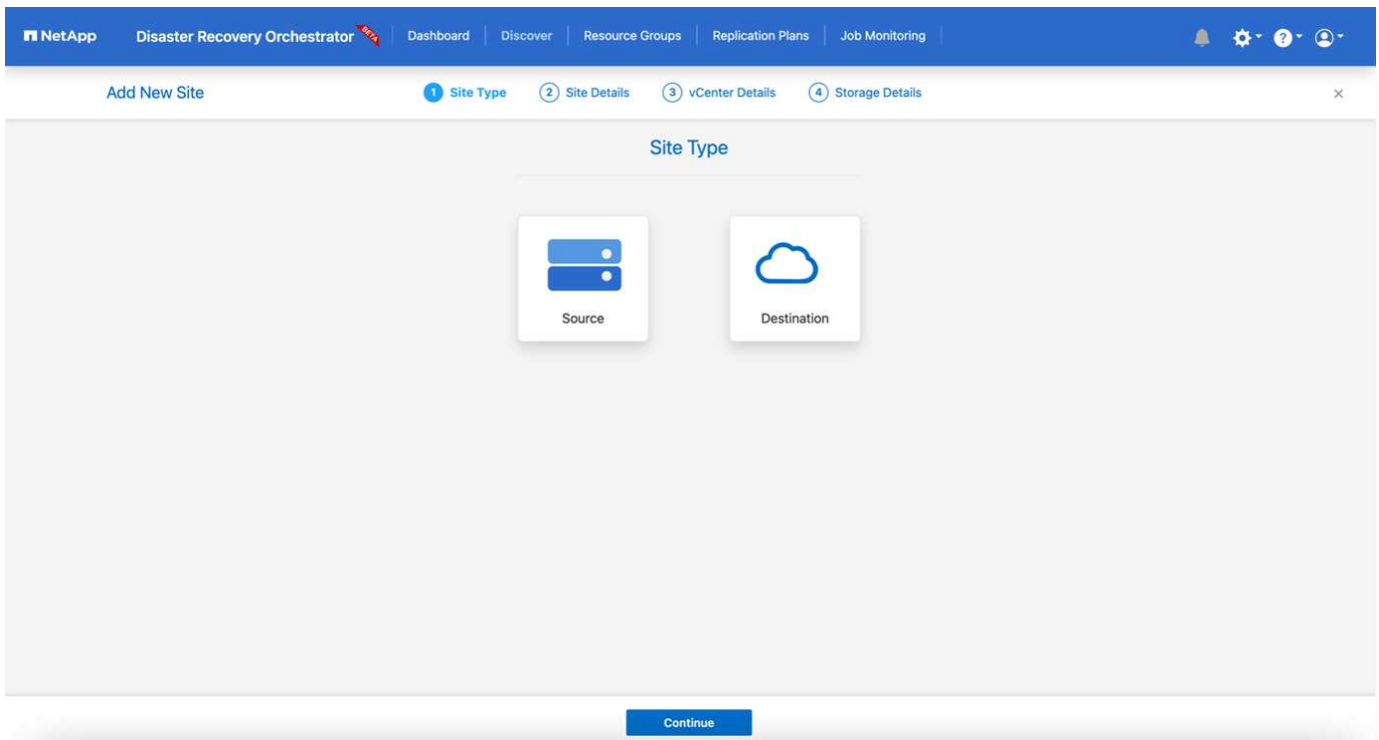
DRO組態

FSXfor ONTAP VMware和VMC設定正確之後、您可以開始設定DRO、使用FSXfor ONTAP Sfor VMware上的唯讀SnapMirror複本、將內部部署工作負載自動還原至VMC。

NetApp建議將DRO代理程式部署在AWS中、也部署到ONTAP 部署FSX for Sf2的相同VPC（也可連接對等端點）、因此DRO代理程式可以透過網路與內部部署元件、以及使用FSXfor ONTAP VMware和VMC資源進行通訊。

第一步是探索內部部署和雲端資源（vCenter和儲存設備）、並將其新增至DRO。在支援的瀏覽器中開啟DRO、然後使用預設的使用者名稱和密碼（admin/admin）和新增站台。您也可以使用「探索」選項來新增站台。新增下列平台：

- 內部部署
 - 內部部署vCenter
 - 儲存系統ONTAP
- 雲端
 - VMC vCenter
 - FSX ONTAP



新增後、DRO會執行自動探索、並顯示從來源儲存設備到FSX ONTAP for Sf0具有對應SnapMirror複本的VM。DRO會自動偵測VM所使用的網路和連接埠群組、並填入這些群組。

NetApp Disaster Recovery Orchestrator Dashboard | Discover | Resource Groups | Replication Plans | Job Monitoring

Back VM List Site: On Prem | vCenter: 172.21.253.160

10 Datastores | 219 Virtual Machines | VM Protection: 3 Protected, 216 Unprotected

38 VMs Create Resource Group

VM Name	VM Status	VM State (1)	DataStore	CPU	Memory (MB)
a300-vcsa02	Not Protected	Powered On	A300_NFS_DS04	16	65536
PFSense	Not Protected	Powered On	A300_NFS_DS04	4	8192
PFsense260	Not Protected	Powered On	A300_NFS_DS04	4	16384
NimDC02	Not Protected	Powered On	A300_NFS_DS04	4	8192
jRBhoja-187	Not Protected	Powered On	A300_NFS_DS04	4	16384
jNimo-187	Not Protected	Powered On	A300_NFS_DS04	4	16384
NimMSdesktop	Not Protected	Powered On	A300_NFS_DS04	8	12288

下一步是將所需的虛擬機器分成功能群組、做為資源群組。

資源群組

新增平台之後、您可以將想要恢復的VM群組為資源群組。DRO資源群組可讓您將一組相依的虛擬機器分組至邏輯群組、其中包含開機順序、開機延遲、以及可在恢復時執行的選用應用程式驗證。

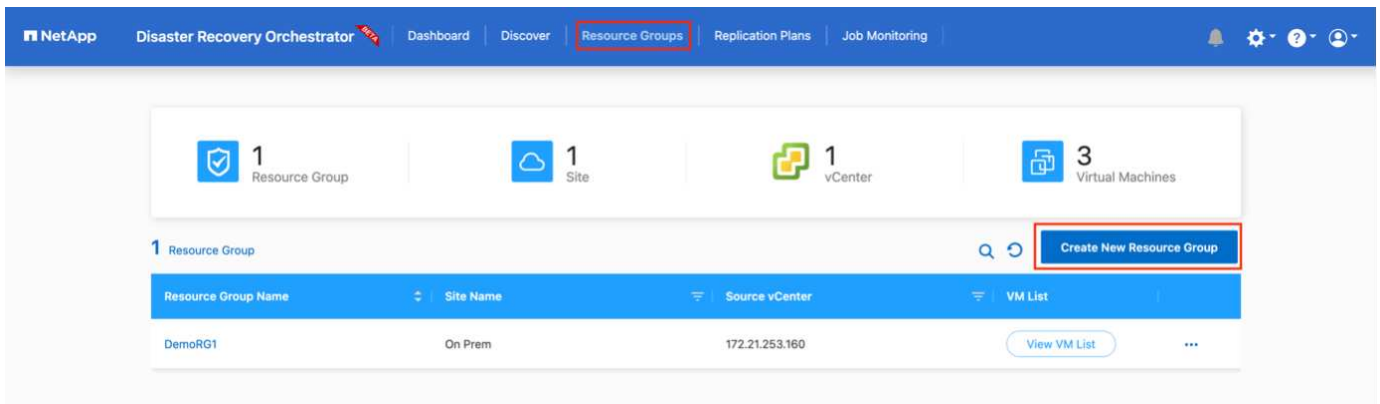
若要開始建立資源群組、請完成下列步驟：

1. 存取*資源群組*、然後按一下*建立新的資源群組*。
2. 在「新資源群組」下、從下拉式清單中選取來源網站、然後按一下「建立」。
3. 提供*資源群組詳細資料*、然後按一下*繼續*。
4. 使用搜尋選項選取適當的VM。
5. 選取所選VM的開機順序和開機延遲（秒）。選取每個VM並設定其優先順序、以設定開機順序。三個是所有VM的預設值。

選項如下：

1-第一台開機的虛擬機器 3-預設 5-最後一台開機的虛擬機器

6. 按一下「建立資源群組」。

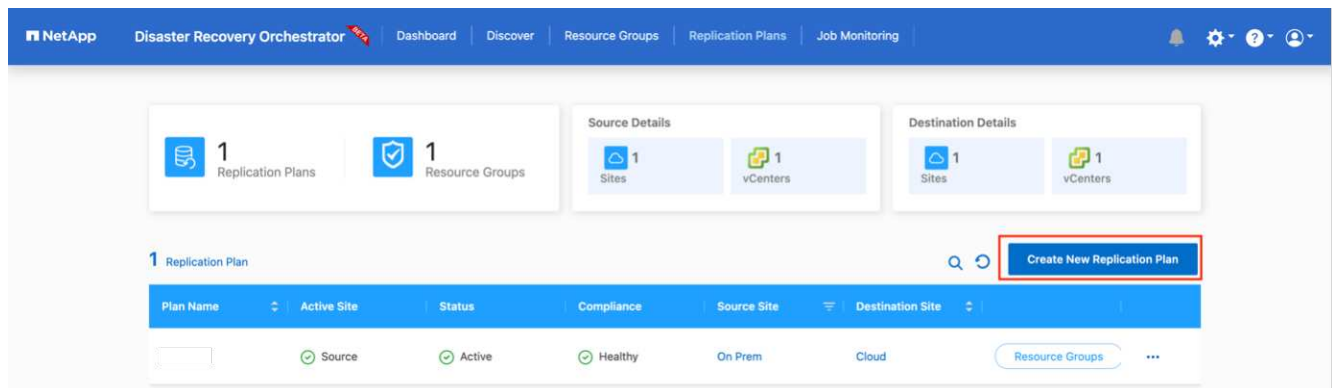


複寫計畫

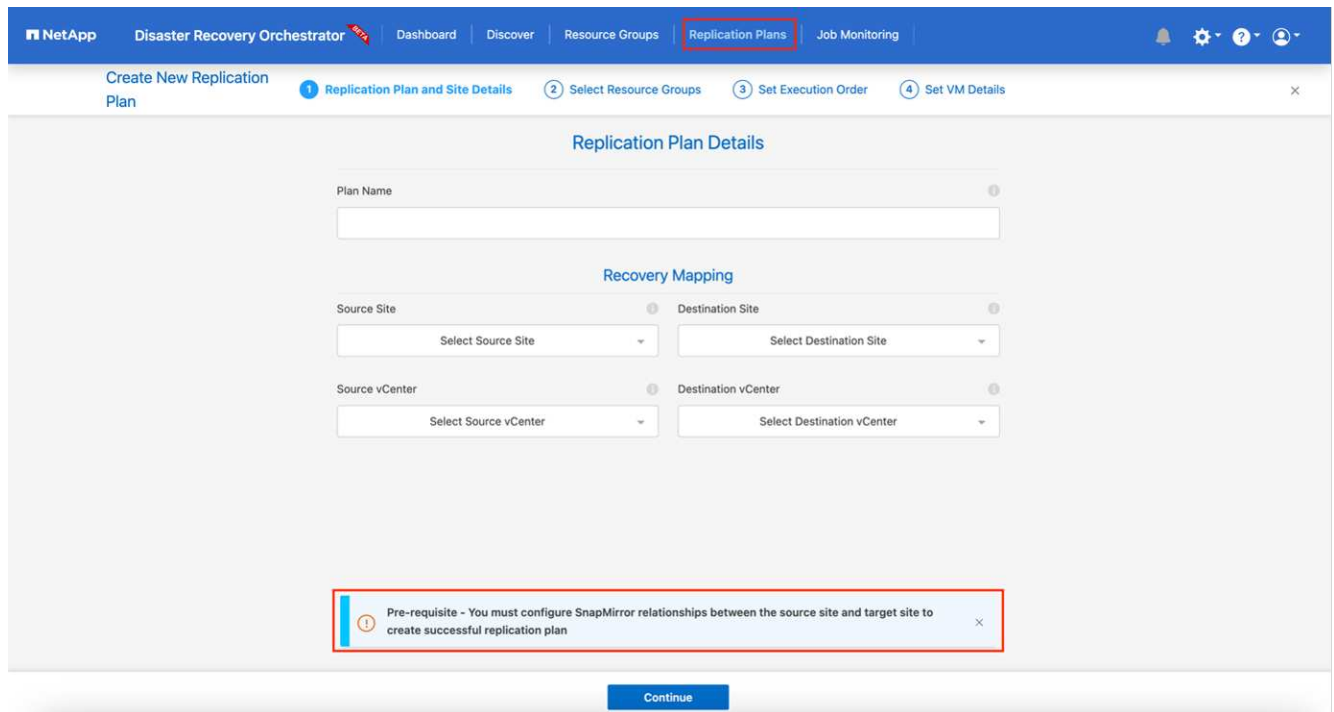
在發生災難時、您需要一套恢復應用程式的計畫。從下拉式清單中選取來源和目的地vCenter平台、然後選取要納入此計畫的資源群組、以及應用程式應如何還原和開啟的分組（例如、網域控制器、層級1、層級2等）。這類計畫有時也稱為藍圖。若要定義恢復計畫、請瀏覽至*複寫計畫*索引標籤、然後按一下*新增複寫計畫*。

若要開始建立複寫計畫、請完成下列步驟：

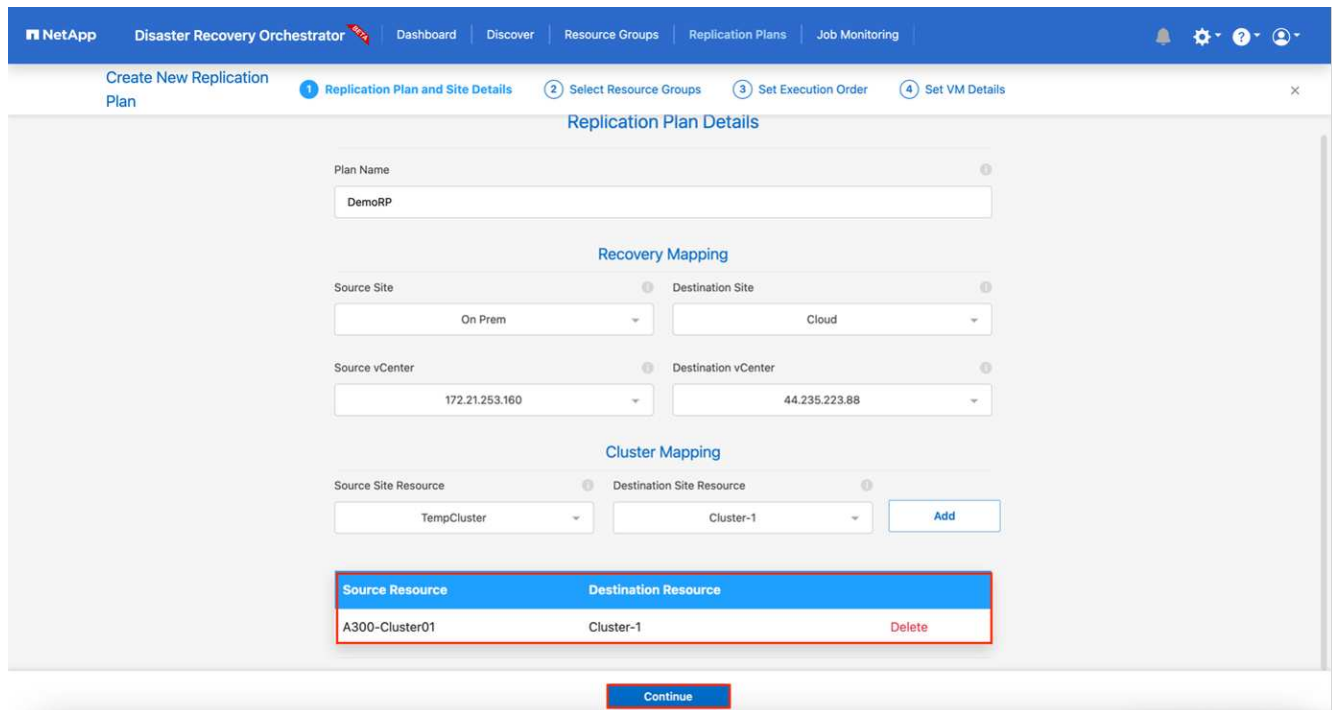
1. 存取*複寫計畫*、然後按一下*建立新的複寫計畫*。



2. 在「新的複寫計畫」下、提供計畫名稱、並選取來源站台、相關聯的vCenter、目的地站台及相關的vCenter來新增還原對應。



3. 完成恢復對應後、選取叢集對應。



4. 選擇*資源群組詳細資料*、然後按一下*繼續*。

5. 設定資源群組的執行順序。此選項可讓您在存在多個資源群組時、選取作業順序。

6. 完成後、選取網路對應至適當的區段。區段應已在VMC中進行資源配置、因此請選取適當的區段來對應 VM。

7. 根據VM的選擇、會自動選取資料存放區對應。



SnapMirror位於磁碟區層級。因此、所有VM都會複寫到複寫目的地。請務必選取屬於資料存放區一部分的所有VM。如果未選取、則只會處理屬於複寫計畫一部分的VM。

Replication Plan Details

Select Execution Order

Resource Group Name	Execution Order
DemoRG1	3

Network Mapping

No more Source/Destination network resources available for mapping

Source Resource	Destination Resource	
VLAN 3375	sddc-cgw-network-1	Delete

DataStore Mapping

Source DataStore	Destination Volume
DRO_Mini	DRO_Mini_copy

Previous Continue

- 在VM詳細資料下、您可以選擇調整VM的CPU和RAM參數大小、這對於將大型環境還原至較小的目標叢集或執行DR測試而不需配置一對一的實體VMware基礎架構而言、非常有幫助。此外、您也可以針對資源群組中所有選取的VM、修改開機順序和開機延遲（秒）。如果在資源群組開機順序選擇期間所選取的項目有任何變更、則還有其他選項可修改開機順序。依預設、系統會使用在資源群組選取期間選取的開機順序；不過、在此階段可以執行任何修改。

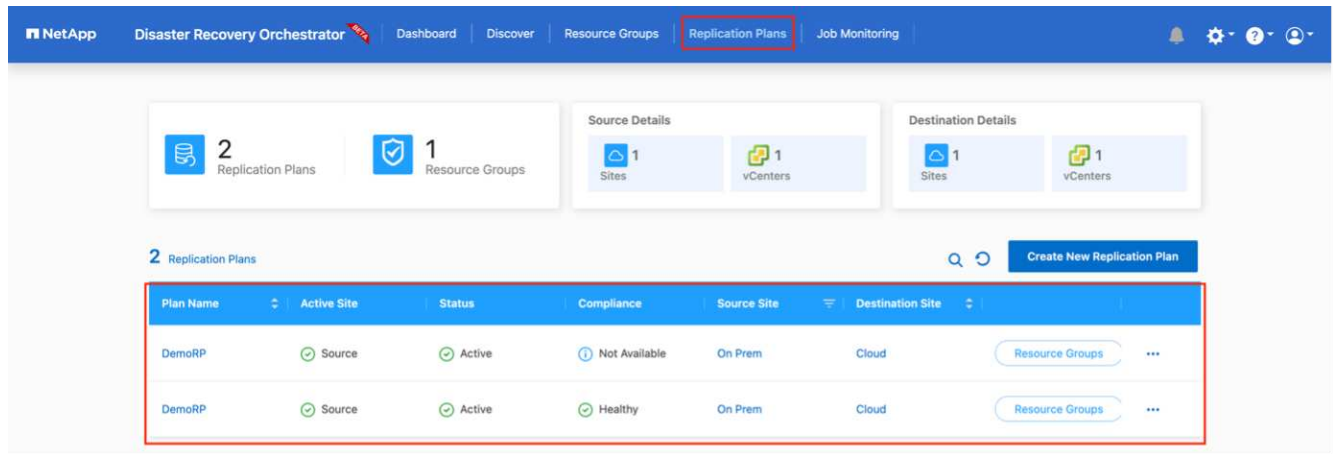
VM Details

3 VMs

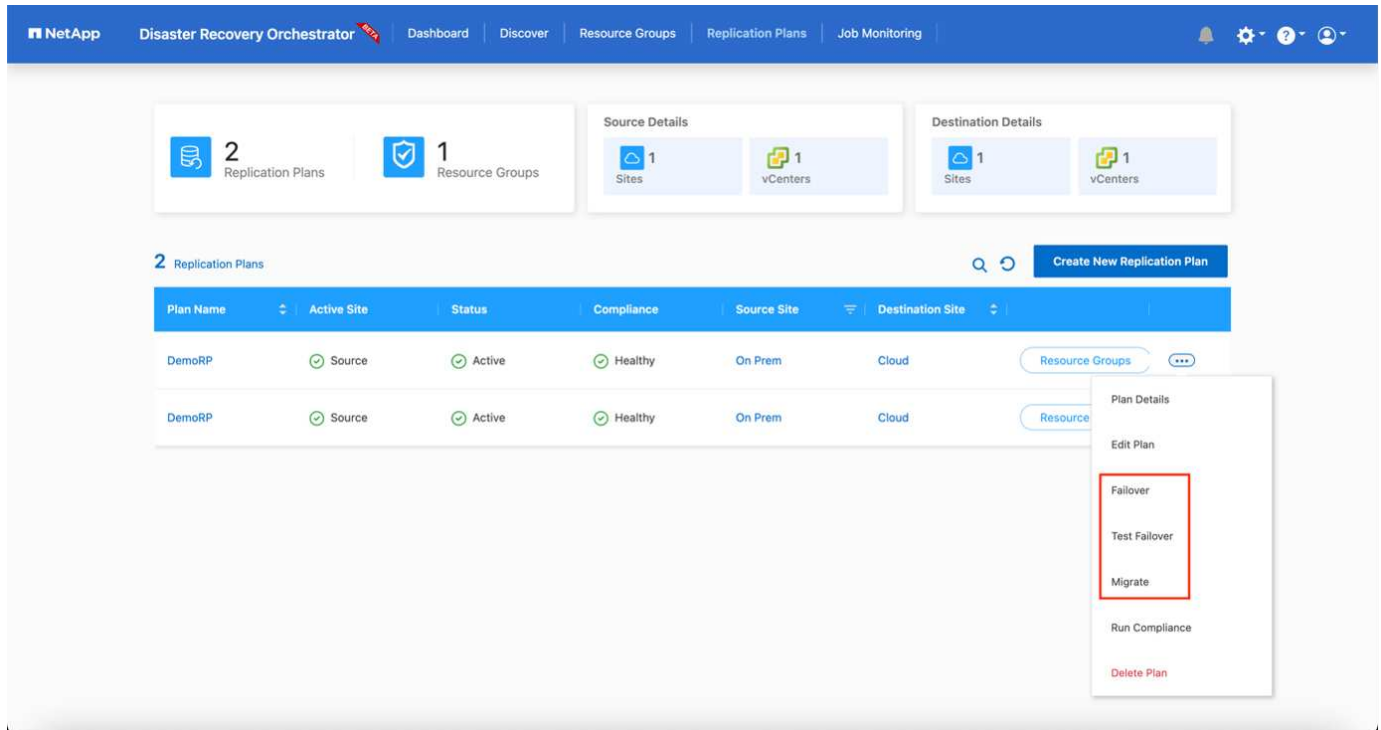
VM Name	No. of CPUs	Memory (MB)	NIC/IP	Boot Order
Resource Group : DemoRG1				
Mini_Test01	1	2048	<input type="radio"/> Static <input checked="" type="radio"/> Dynamic	3
Mini_Test02	1	2048	<input type="radio"/> Static <input checked="" type="radio"/> Dynamic	2
Mini_Test03	1	2048	<input type="radio"/> Static <input checked="" type="radio"/> Dynamic	1

Previous Create Replication Plan

- 按一下「建立複寫計畫」。



建立複寫計畫之後、即可根據需求來執行容錯移轉選項、測試容錯移轉選項或移轉選項。在容錯移轉和測試容錯移轉選項期間、會使用最新的SnapMirror Snapshot複本、或從時間點Snapshot複本（根據SnapMirror的保留原則）選取特定的Snapshot複本。如果您面臨勒索軟體之類的毀損事件、最近的複本已遭入侵或加密、則時間點選項可能非常實用。DRO會顯示所有可用的時間點。若要以複寫計畫中指定的組態觸發容錯移轉或測試容錯移轉、您可以按一下*容錯移轉*或*測試容錯移轉*。



Failover Details



Volume Snapshot Details

- Use latest snapshot ⓘ
- Select specific snapshot ⓘ

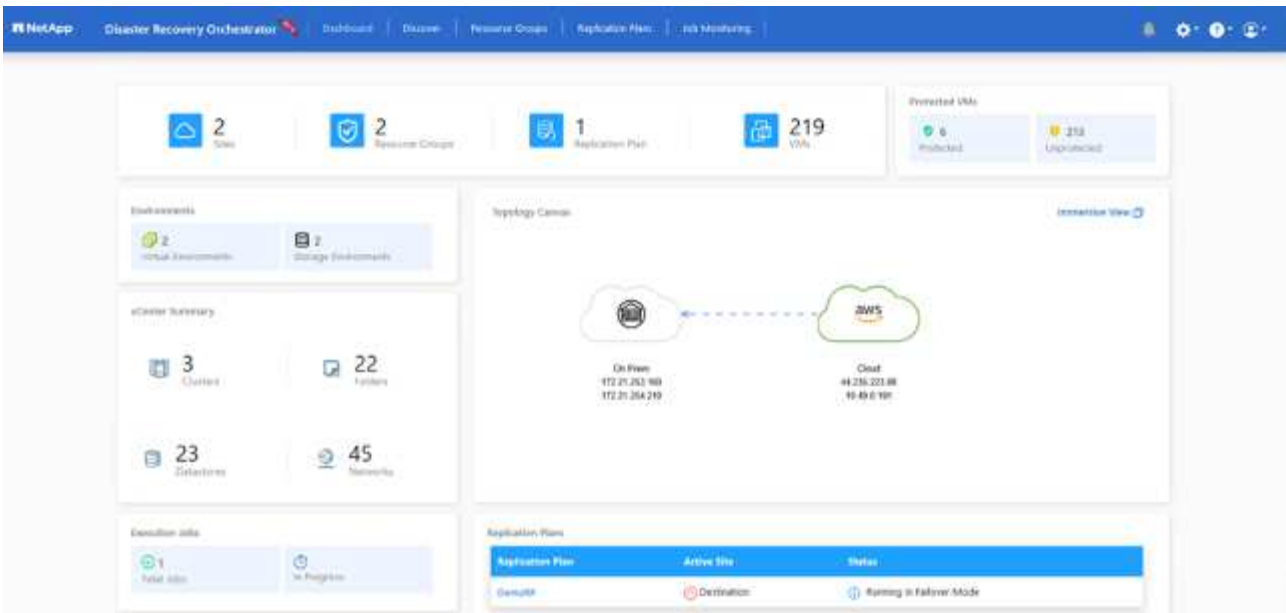
Start Failover

複寫計畫可在工作功能表中監控：

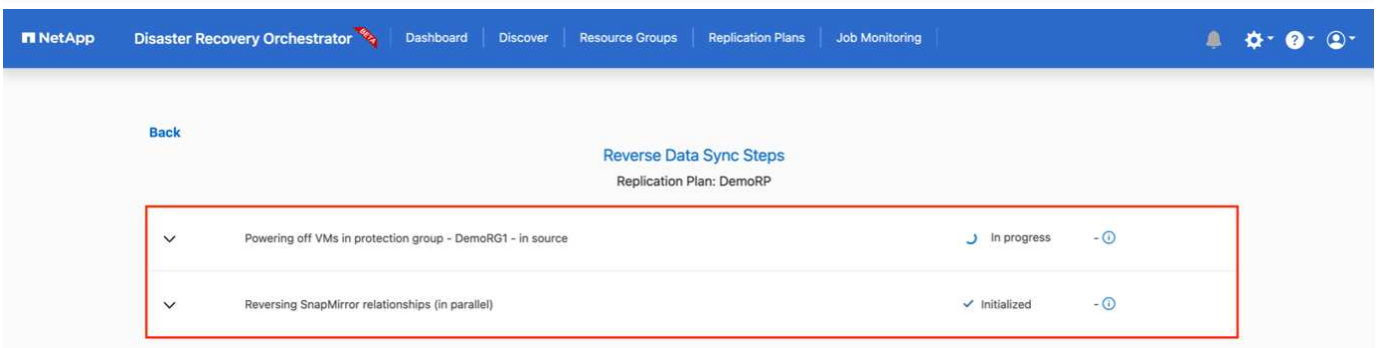
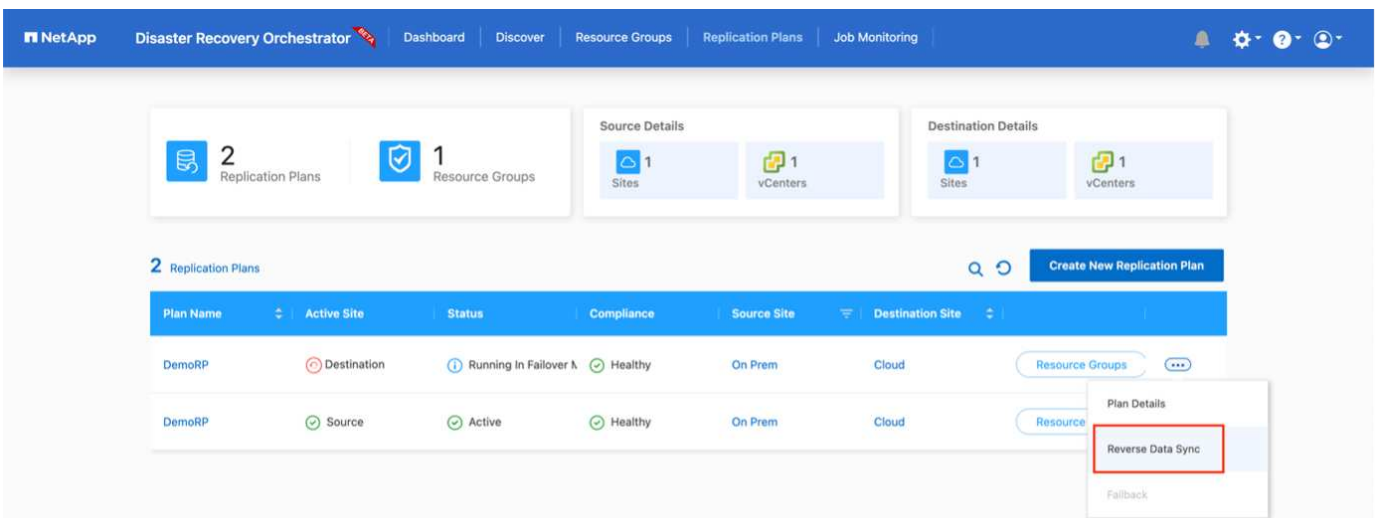
The screenshot shows the NetApp Disaster Recovery Orchestrator interface. The top navigation bar includes 'NetApp', 'Disaster Recovery Orchestrator', 'Dashboard', 'Discover', 'Resource Groups', 'Replication Plans', and 'Job Monitoring'. The 'Job Monitoring' tab is active. Below the navigation bar, there is a 'Back' link and a 'Failover Steps' section for 'Replication Plan: DemoRP'. The steps are listed in a table:

Step	Status	Duration
Breaking SnapMirror relationships (in parallel)	Success	11.3 Seconds
Mounting volumes and creating datastores (in parallel)	Success	34.7 Seconds
Registering VMs (in parallel)	Success	13.2 Seconds
Powering on VMs in protection group - DemoRG1 - in target	Success	95.8 Seconds
Updating replication status	Success	0.5 Seconds

在觸發容錯移轉之後、可在VMC vCenter (VM、網路、資料存放區) 中看到還原的項目。根據預設、虛擬機器會還原至工作負載資料夾。



容錯回復可在複寫計畫層級觸發。對於測試容錯移轉、可利用「切換」選項來復原變更、並移除FlexClone關係。與容錯移轉相關的容錯回復是兩個步驟的程序。選取複寫計畫、然後選取*反轉資料同步*。



完成後、您可以觸發容錯回復、將其移回原始正式作業站台。

NetApp Disaster Recovery Orchestrator

2 Replication Plans

Plan Name	Active Site	Status	Compliance	Source Site	Destination Site
DemoRP	Destination	Active	Healthy	On Prem	Cloud
DemoRP	Source	Active	Healthy	On Prem	Cloud

Plan Details

- Fallback

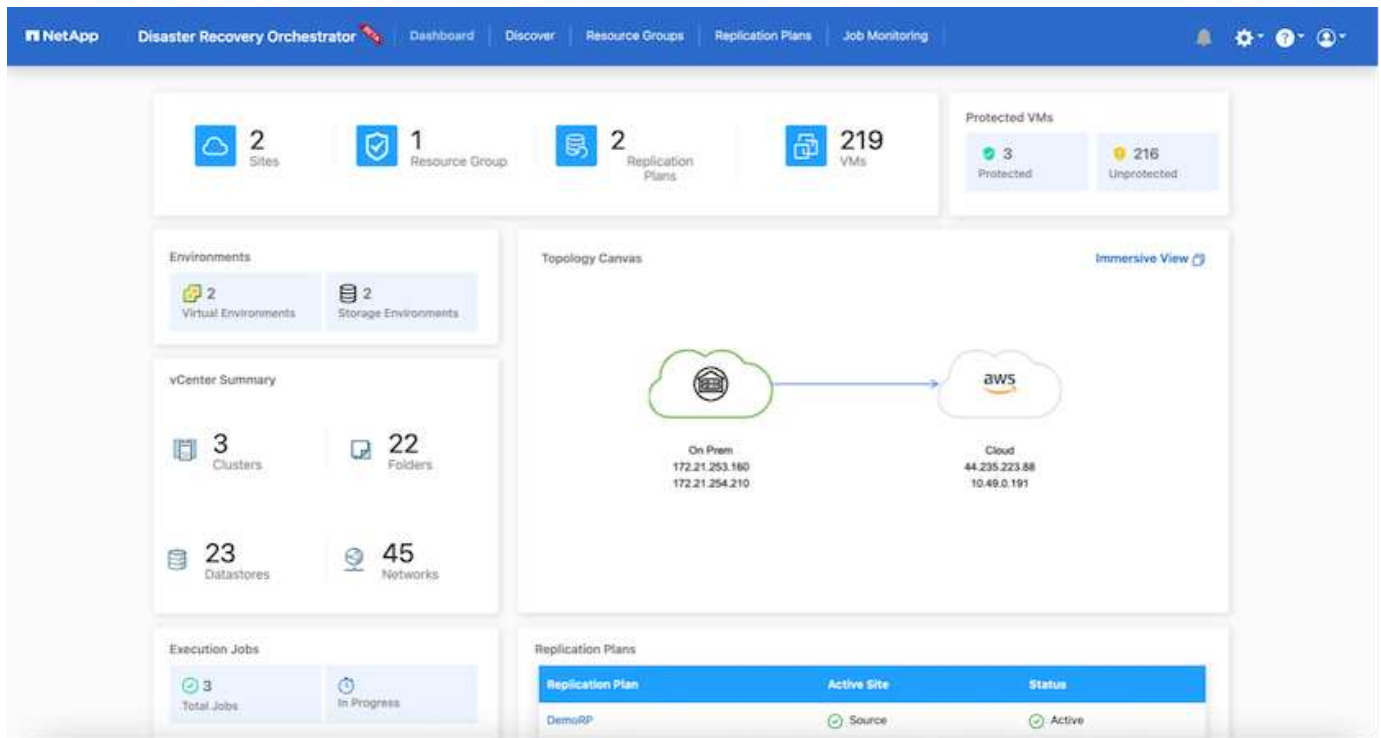
Back

Fallback Steps

Replication Plan: DemoRP

Powering off VMs in protection group - DemoRG1 - in target	In progress
Unregistering VMs in target (in parallel)	Initialized
Unmounting volumes in target (in parallel)	Initialized
Breaking reverse SnapMirror relationships (in parallel)	Initialized
Updating VM networks (in parallel)	Initialized
Powering on VMs in protection group - DemoRG1 - in source	Initialized
Deleting reverse SnapMirror relationships (in parallel)	Initialized
Resuming SnapMirror relationships to target (in parallel)	Initialized

從NetApp BlueXP中、我們可以看到適當磁碟區（對應至VMC的磁碟區為讀寫磁碟區）的複寫健全狀況已經中斷。在測試容錯移轉期間、DRO不會對應目的地或複本磁碟區。相反地、它會製作所需SnapMirror（或Snapshot）執行個體的FlexClone複本、並公開FlexClone執行個體、而FlexClone執行個體不會耗用額外的實體容量來ONTAP 進行FSXfor Sf2。此程序可確保磁碟區未被修改、即使在DR測試或分類工作流程期間、複本工作仍可繼續執行。此外、此程序可確保在發生錯誤或恢復毀損的資料時、能夠清除還原作業、而不會造成複本遭到破壞的風險。



勒索軟體恢復

從勒索軟體中恢復可能是一項艱鉅的任務。具體而言、IT組織很難鎖定安全回報點所在的位置、一旦確定了安全回報點、就能保護恢復的工作負載、避免遭受例如睡眠中的惡意軟體或易受影響的應用程式等重複發生的攻擊。

DRO可讓您從任何可用時間點恢復系統、藉此解決這些疑慮。您也可以將工作負載還原至功能性且隔離的網路、以便應用程式在不受北南流量影響的位置彼此運作和通訊。這可讓您的安全團隊安全進行鑑識、並確保沒有隱藏或睡眠中的惡意軟體。

效益

- 使用高效且彈性的SnapMirror複寫。
- 利用Snapshot複本保留功能、將資料恢復到任何可用的時間點。
- 從儲存、運算、網路及應用程式驗證步驟中、將所有必要步驟完全自動化、以恢復數百至數千部VM。
- 使用不變更複寫磁碟區的方法、使用ONTAP FlexClone技術來恢復工作負載。
 - 避免磁碟區或Snapshot複本的資料毀損風險。
 - 避免災難恢復測試工作流程期間的複寫中斷。
 - 災難恢復資料與雲端運算資源可能用於災難恢復以外的工作流程、例如DevTest、安全性測試、修補或升級測試、以及補救測試。
- CPU與RAM最佳化、可將還原作業移至較小的運算叢集、協助降低雲端成本。

使用 Veeam Replication 和 FSX for ONTAP 在 AWS 上進行災難恢復至 VMware Cloud

Amazon FSx for NetApp ONTAP 與 AWS 上的 VMware Cloud 整合、是以 NetApp ONTAP 檔案系統為基礎的 AWS 託管外部 NFS 資料存放區、可附加至 SDDC 中的叢集。它為客戶提供靈活、高效能的虛擬化儲存基礎架構、可在運算資源之外進行擴充。

總覽

對於那些希望使用 VMware Cloud on AWS SDDC 做為災難恢復目標的客戶、ONTAP 資料存放區的 FSX 可用於使用任何驗證的協力廠商解決方案、提供 VM 複寫功能、從內部部署複寫資料。透過新增適用於 ONTAP 資料存放區的 FSX、相較於在 AWS SDDC 上建置 VMware 雲端、它將可實現成本最佳化的部署、並提供大量的 ESXi 主機以容納儲存設備。

此方法也可協助客戶在 VMC 中使用試驗性光叢集、以及將 ONTAP 資料存放區的 FSX 來裝載 VM 複本。同樣的程序也可透過正常容錯移轉複寫計畫、以作為移轉選項延伸至 VMware Cloud on AWS。

問題陳述

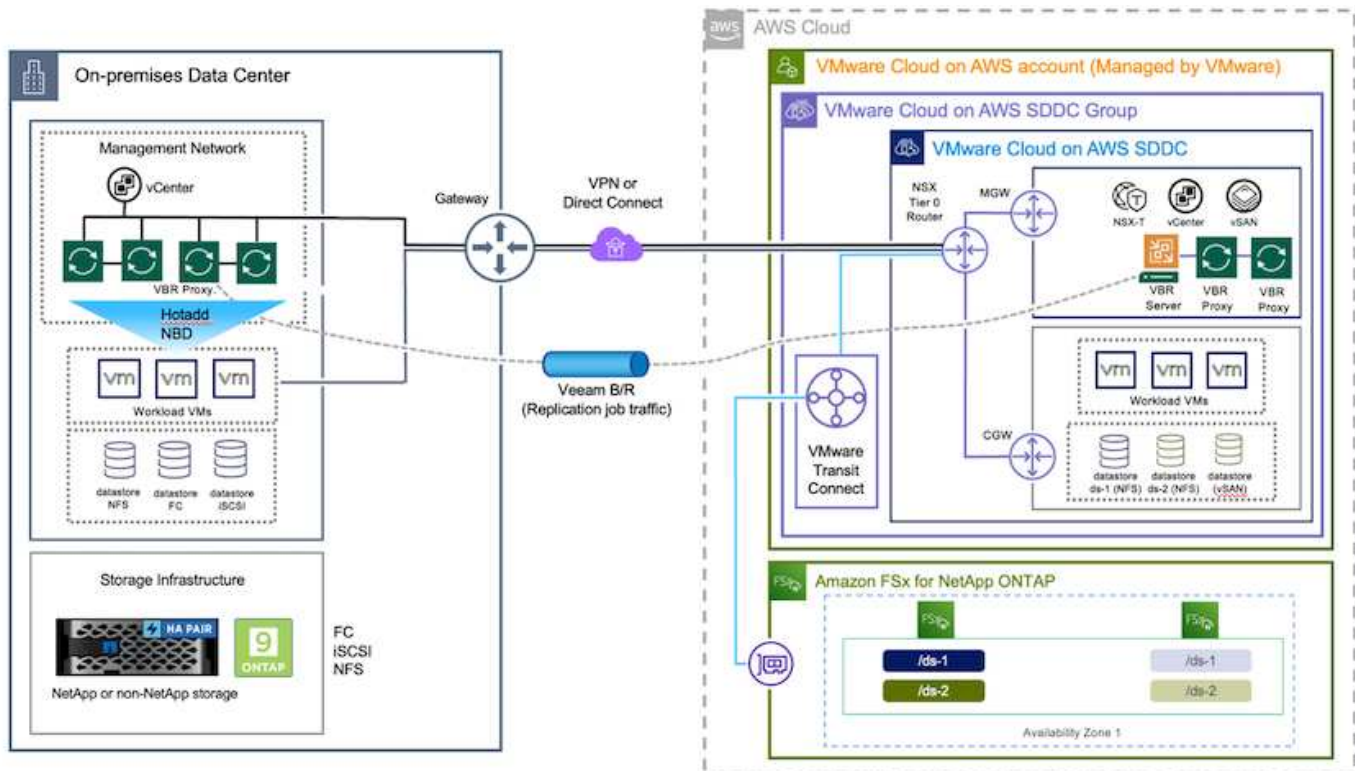
本文件說明如何使用適用於 ONTAP 資料存放區和 Veeam 備份與複寫的 FSX、以使用 VM 複寫功能、為內部部署的 VMware VM 設定災難恢復至 VMware Cloud on AWS。

Veeam 備份與複寫功能可在現場及遠端複寫災難恢復 (DR)。複寫虛擬機器時、Veeam 備份與複寫會在 AWS SDDC 叢集上的目標 VMware Cloud 上、以原生 VMware vSphere 格式建立 VM 的精確複本、並使複本與原始 VM 保持同步。

複寫可提供最佳的恢復時間目標 (RTO) 值、因為虛擬機器的複本處於就緒啟動狀態。這種複寫機制可確保工作負載在發生災難事件時、可在 AWS SDDC 上的 VMware Cloud 上快速啟動。Veeam 備份與複寫軟體也能最佳化流量傳輸、以便透過 WAN 進行複寫、並降低連線速度。此外、它也會篩選出重複的資料區塊、零資料區塊、交換檔案和排除的 VM 來賓作業系統檔案、並壓縮複本流量。

為了避免複寫工作佔用整個網路頻寬、可以制定 WAN 加速器和網路節流規則。Veeam Backup & Replication 中的複寫程序是由工作所驅動、這表示複寫是透過設定複寫工作來執行。發生災難事件時、可觸發容錯移轉、藉由容錯移轉至複本來恢復 VM。

執行容錯移轉時、複寫的 VM 會接管原始 VM 的角色。容錯移轉可以執行至複本的最新狀態、或是任何已知的還原點。如此一來、就能視需要進行勒索軟體恢復或隔離測試。在 Veeam 備份與複寫中、容錯移轉與容錯回復是暫時的中繼步驟、應進一步完成。Veeam 備份與複寫提供多種選項來處理不同的災難恢復案例。



解決方案部署

高階步驟

1. Veeam 備份與複寫軟體是在內部環境中執行、並具備適當的網路連線能力。
2. 在 AWS 上設定 VMware Cloud、請參閱 VMware Cloud Tech Zone 文章 ["VMware Cloud on AWS 與 Amazon FSx for NetApp ONTAP 部署指南整合"](#) 若要部署、請在 AWS SDDC 上設定 VMware Cloud、將 ONTAP 的 FSx 設定為 NFS 資料存放區。（以最小組態設定的試行環境可用於 DR 用途。發生事件時、VM 會容錯移轉至此叢集、並可新增其他節點）。
3. 設定複寫工作、以使用 Veeam 備份與複寫建立 VM 複本。
4. 建立容錯移轉計畫並執行容錯移轉。
5. 災難事件完成且主站台正常運作後、切換回正式作業的 VM。

Veeam VM 複寫至 VMC 和 ONTAP 資料存放區的 FSX 的先決條件

1. 確保 Veeam 備份與複寫備份虛擬機器已連線至來源 vCenter、以及 AWS SDDC 叢集上的目標 VMware 雲端。
2. 備份伺服器必須能夠解析簡短名稱、並連線至來源和目標 vCenter。
3. ONTAP 資料存放區的目標 FSX 必須有足夠的可用空間來儲存複寫 VM 的 VMDK

如需其他資訊、請參閱涵蓋的「考量與限制」 ["請按這裡"](#)。

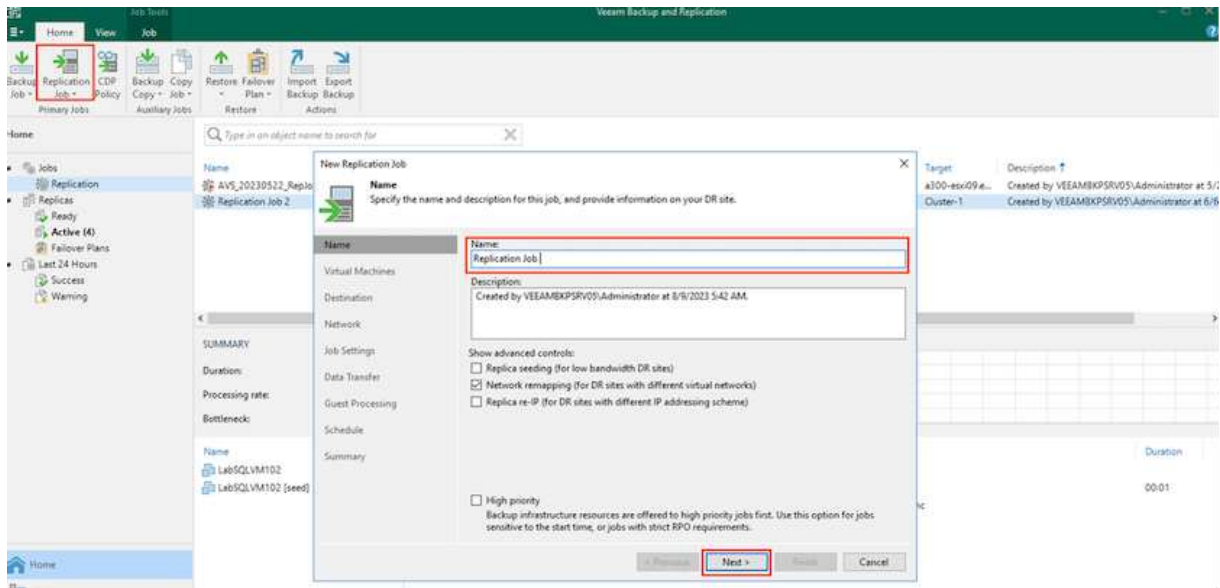
部署詳細資料

步驟 1：複寫 VM

Veeam 備份與複寫利用 VMware vSphere 快照功能、並在複寫期間、Veeam 備份與複寫要求 VMware vSphere 建立 VM 快照。VM 快照是 VM 的時間點複本、其中包括虛擬磁碟、系統狀態、組態等。Veeam 備份與複寫會使用快照做為複寫資料來源。

若要複寫 VM、請依照下列步驟進行：

1. 開啟 Veeam 備份與複寫主控台。
2. 在首頁檢視中、選取複寫工作 > 虛擬機器 > VMware vSphere。
3. 指定工作名稱並選取適當的進階控制核取方塊。按一下「下一步」
 - 如果內部部署和 AWS 之間的連線頻寬有限、請選取複本植入核取方塊。
 - 如果 AWS SDDC 上 VMware Cloud 上的區段與內部部署站台網路不相符、請選取「網路重新對應（適用於具有不同網路的 AWS VMC 站台）」核取方塊。
 - 如果內部生產站台的 IP 定址方案與 AWS VMC 站台的配置不同、請選取複本重新 IP（適用於具有不同 IP 定址方案的 DR 站台）核取方塊。



4. 在 * 虛擬機器 * 步驟中、選取需要複寫至 FSX 的 VM、以將 ONTAP 資料存放區附加至 AWS SDDC 上的 VMware Cloud。虛擬機器可放置在 vSAN 上、以填滿可用的 vSAN 資料存放區容量。在試驗性光叢集中、3 節點叢集的可用容量將會受到限制。其餘資料可複寫至 ONTAP 資料存放區的 FSX。按一下 * 新增 *、然後在 * 新增物件 * 視窗中選取必要的 VM 或 VM 容器、然後按一下 * 新增 *。單擊 * 下一步 *。



Virtual Machines

Select one or more VMs to replicate. Use exclusion settings to exclude specific VMs and virtual disks from replication.

Name	Virtual machines to replicate:																																																						
Virtual Machines	<table border="1"><thead><tr><th>Name</th><th>Type</th><th>Size</th></tr></thead><tbody><tr><td>TestVeeam21</td><td>Virtual Machine</td><td>873 MB</td></tr><tr><td>TestVeeam22</td><td>Virtual Machine</td><td>890 MB</td></tr><tr><td>TestVeeam23</td><td>Virtual Machine</td><td>883 MB</td></tr><tr><td>TestVeeam24</td><td>Virtual Machine</td><td>879 MB</td></tr><tr><td>TestVeeam25</td><td>Virtual Machine</td><td>885 MB</td></tr><tr><td>TestVeeam26</td><td>Virtual Machine</td><td>883 MB</td></tr><tr><td>TestVeeam27</td><td>Virtual Machine</td><td>879 MB</td></tr><tr><td>TestVeeam28</td><td>Virtual Machine</td><td>880 MB</td></tr><tr><td>TestVeeam29</td><td>Virtual Machine</td><td>878 MB</td></tr><tr><td>TestVeeam30</td><td>Virtual Machine</td><td>876 MB</td></tr><tr><td>TestVeeam31</td><td>Virtual Machine</td><td>888 MB</td></tr><tr><td>TestVeeam32</td><td>Virtual Machine</td><td>881 MB</td></tr><tr><td>TestVeeam33</td><td>Virtual Machine</td><td>877 MB</td></tr><tr><td>TestVeeam34</td><td>Virtual Machine</td><td>875 MB</td></tr><tr><td>TestVeeam35</td><td>Virtual Machine</td><td>882 MB</td></tr><tr><td>WinSQL401</td><td>Virtual Machine</td><td>20.3 GB</td></tr><tr><td>WinSQL405</td><td>Virtual Machine</td><td>24.2 GB</td></tr></tbody></table>	Name	Type	Size	TestVeeam21	Virtual Machine	873 MB	TestVeeam22	Virtual Machine	890 MB	TestVeeam23	Virtual Machine	883 MB	TestVeeam24	Virtual Machine	879 MB	TestVeeam25	Virtual Machine	885 MB	TestVeeam26	Virtual Machine	883 MB	TestVeeam27	Virtual Machine	879 MB	TestVeeam28	Virtual Machine	880 MB	TestVeeam29	Virtual Machine	878 MB	TestVeeam30	Virtual Machine	876 MB	TestVeeam31	Virtual Machine	888 MB	TestVeeam32	Virtual Machine	881 MB	TestVeeam33	Virtual Machine	877 MB	TestVeeam34	Virtual Machine	875 MB	TestVeeam35	Virtual Machine	882 MB	WinSQL401	Virtual Machine	20.3 GB	WinSQL405	Virtual Machine	24.2 GB
Name	Type	Size																																																					
TestVeeam21	Virtual Machine	873 MB																																																					
TestVeeam22	Virtual Machine	890 MB																																																					
TestVeeam23	Virtual Machine	883 MB																																																					
TestVeeam24	Virtual Machine	879 MB																																																					
TestVeeam25	Virtual Machine	885 MB																																																					
TestVeeam26	Virtual Machine	883 MB																																																					
TestVeeam27	Virtual Machine	879 MB																																																					
TestVeeam28	Virtual Machine	880 MB																																																					
TestVeeam29	Virtual Machine	878 MB																																																					
TestVeeam30	Virtual Machine	876 MB																																																					
TestVeeam31	Virtual Machine	888 MB																																																					
TestVeeam32	Virtual Machine	881 MB																																																					
TestVeeam33	Virtual Machine	877 MB																																																					
TestVeeam34	Virtual Machine	875 MB																																																					
TestVeeam35	Virtual Machine	882 MB																																																					
WinSQL401	Virtual Machine	20.3 GB																																																					
WinSQL405	Virtual Machine	24.2 GB																																																					
Destination																																																							
Network																																																							
Job Settings																																																							
Data Transfer																																																							
Guest Processing																																																							
Schedule																																																							
Summary																																																							

Buttons: Add... (highlighted), Remove, Exclusions..., Source..., Up, Down, Recalculate, Total size: 120 GB

Navigation: < Previous, Next > (highlighted), Finish, Cancel

5. 之後、將目的地選取為 AWS SDDC 叢集 / 主機上的 VMware Cloud、以及 VM 複本適用的資源集區、VM 資料夾和 ONTAP 資料存放區的 FSX。然後按一下 * 下一步 *。



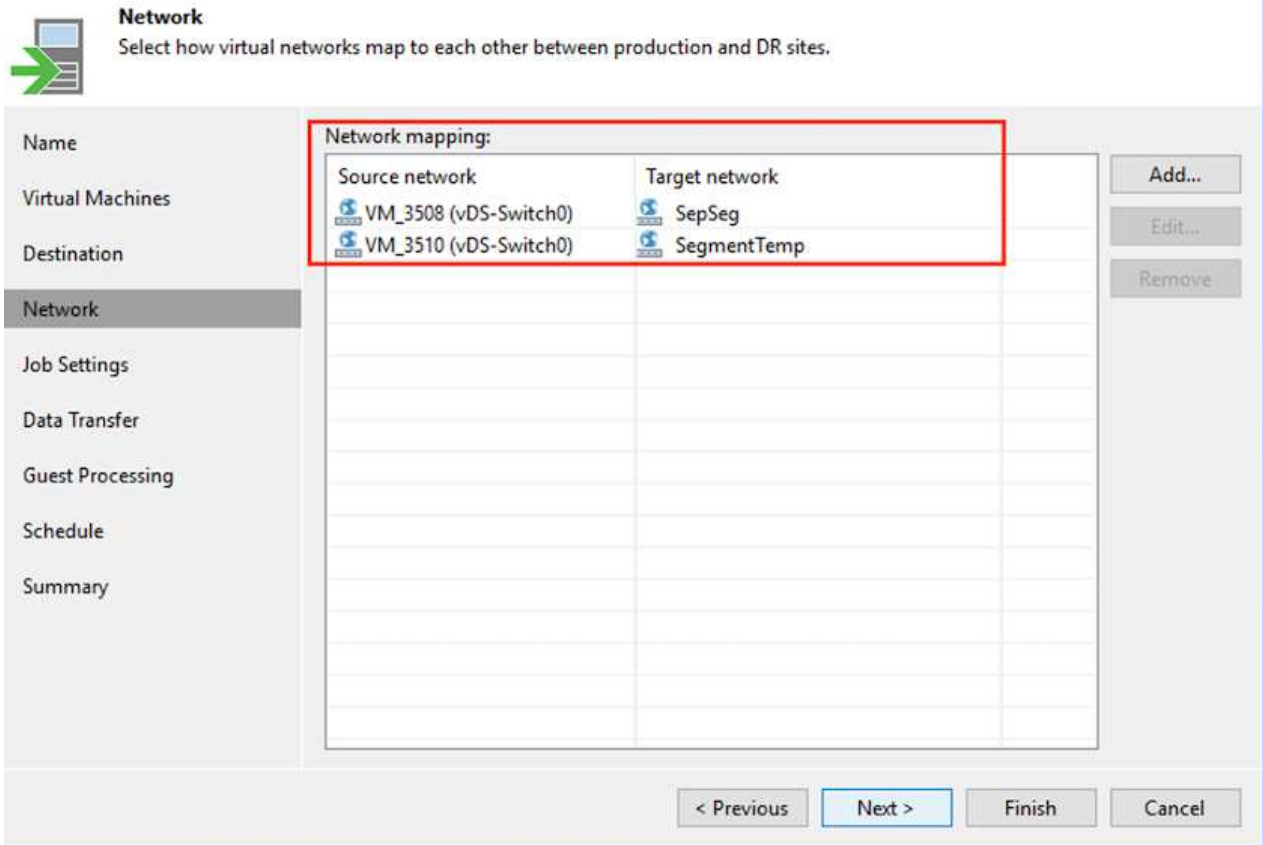
Destination

Specify where replicas should be created in the DR site.

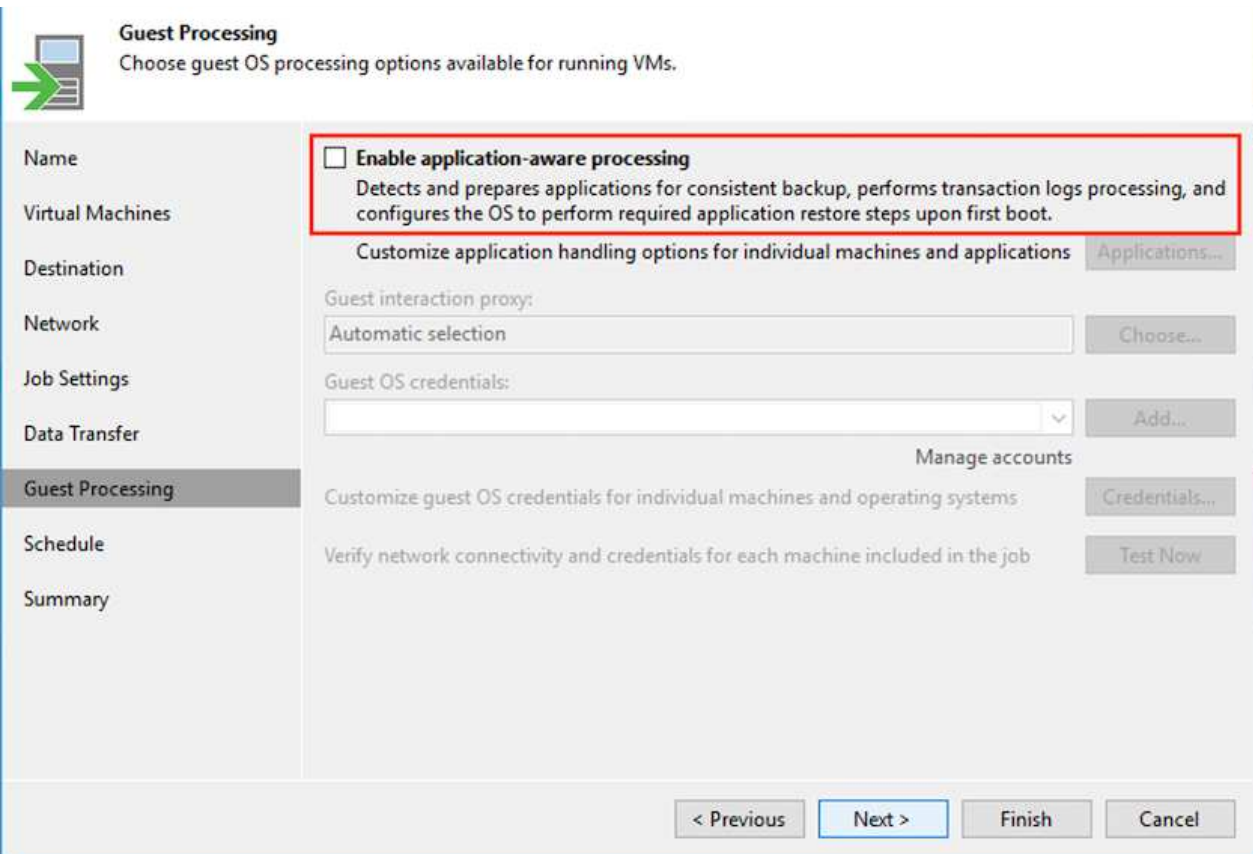
Name	Host or cluster: <input type="text"/>	Choose...	
Virtual Machines			
Destination	Resource pool: Resources	Choose...	
Network	Pick resource pool for selected replicas		
Job Settings	VM folder: vm	Choose...	
Data Transfer	Pick VM folder for selected replicas		
Guest Processing			
Schedule	Datastore: _Veeam [5.6 TB free]		Choose...
Summary	Pick datastore for selected virtual disks		

Navigation: < Previous, Next > (highlighted), Finish, Cancel

6. 在下一個步驟中、視需要在來源和目的地虛擬網路之間建立對應。

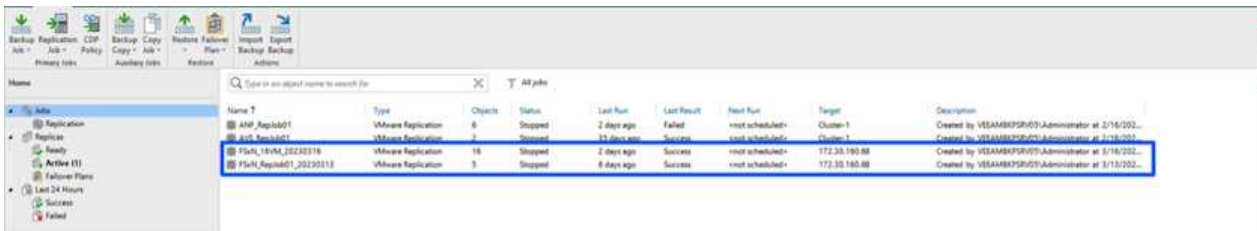


7. 在 * 工作設定 * 步驟中、指定將儲存 VM 複本中繼資料、保留原則等的備份儲存庫。
8. 在 **Data Transfer** 步驟中更新 **Source** 和 **Target** 代理服務器，並保留 **Automatic** 選擇（默認）並保持 **Direct** 選項，然後單擊 **Next**（下一步）。
9. 在 * 來賓處理 * 步驟中、視需要選取 * 啟用應用程式感知處理 * 選項。單擊 * 下一步 *。



10. 選擇複寫排程以定期執行複寫工作。

11. 在精靈的 * 摘要 * 步驟中、檢閱複寫工作的詳細資料。若要在精靈關閉後立即啟動工作、請選取 * 按一下「完成」時執行工作 * 核取方塊、否則請取消選取核取方塊。然後按一下 * 完成 * 以關閉精靈。



複寫工作啟動後、會在目的地 VMC SDDC 叢集 / 主機上填入具有指定尾碼的虛擬機器。

The screenshot displays the Veeam Backup and Replication interface. The top navigation bar includes Home, View, and Job. Below this, there are icons for Start, Stop, Retry, Statistics, Report, Edit, Clone, Disable, and Delete. The main area is divided into several sections:




- Home:** A sidebar on the left with navigation options like Replication, Ready, Failover Plans, Last 24 Hours, Success, Home, Inventory, Backup Infrastructure, Storage Infrastructure, Tape Infrastructure, and Files.
- Table:** A table listing jobs with columns for Name, Type, Objects, Status, Last Run, Last Result, Next Run, Target, and Description. The selected job is 'FSxN_16VM_20230316'.
- SUMMARY:** A section showing job details such as Duration (01:21:27), Processing rate (494 MB/s), Bottleneck (Proxy), Processed (256 GB (100%)), Read (256 GB), Transferred (38.9 MB (-99%)), Success (16), Warnings (0), and Errors (0).
- THROUGHPUT (ALL TIME):** A bar chart showing the throughput of the job over time, with a speed of 594 MB/s.
- Table of Test VMs:** A table listing 16 test VMs (TestVeeam01 to TestVeeam16) with their status (Success) and the action being performed (Processing TestVeeam01 to TestVeeam16). The duration for each VM is listed in the final column.

如需 Veeam 複寫的其他資訊、請參閱 ["複寫的運作方式"](#)。

步驟 2：建立容錯移轉計畫

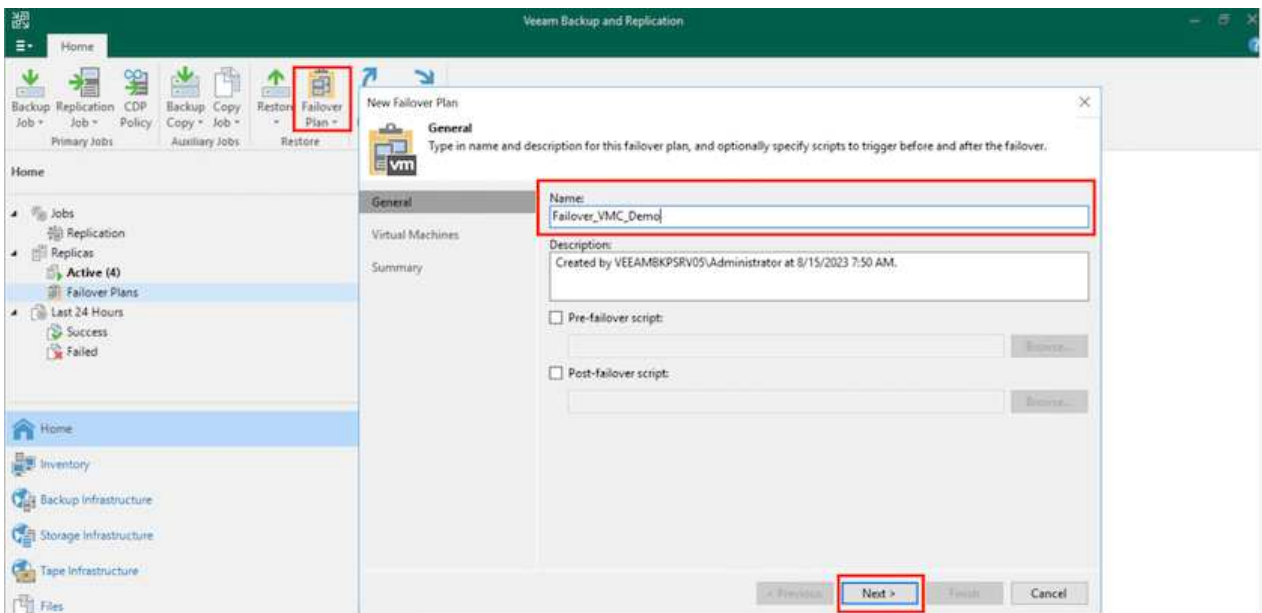
當初始複寫或植入完成時、請建立容錯移轉計畫。容錯移轉計畫有助於自動逐一或以群組的方式、為相關的 VM 執行容錯移轉。容錯移轉計畫是 VM 處理順序的藍圖、包括開機延遲。容錯移轉計畫也有助於確保關鍵相依的 VM 已經在執行中。

若要建立計畫、請瀏覽至稱為複本的新子區段、然後選取容錯移轉計畫。選擇適當的 VM。Veeam 備份與複寫會尋找最接近此時間點的還原點、並使用它們來啟動 VM 複本。

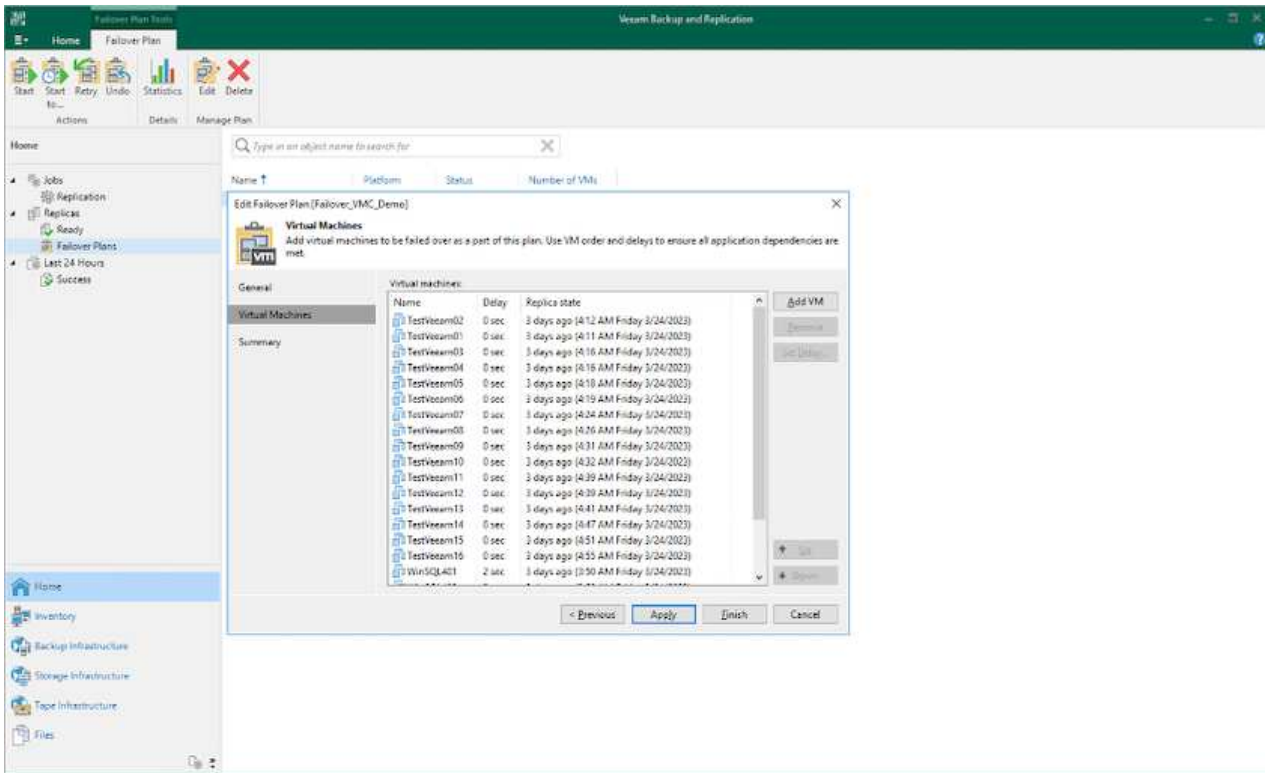
-  只有在初始複寫完成且 VM 複本處於就緒狀態時、才能新增容錯移轉計畫。
-  執行容錯移轉計畫時可同時啟動的虛擬機器數量上限為 10 個。
-  在容錯移轉過程中、來源 VM 將不會關閉。

若要建立 * 容錯移轉計畫 *、請執行下列步驟：

1. 在主畫面上、選取 * 容錯移轉計畫 > VMware vSphere *。
2. 接下來、請提供計畫的名稱和說明。可視需要新增容錯移轉前後指令碼。例如、在啟動複寫的虛擬機器之前、請先執行指令碼來關閉虛擬機器。



3. 將 VM 新增至計畫、並修改 VM 開機順序和開機延遲、以符合應用程式相依性。



如需建立複寫工作的其他資訊、請參閱 ["建立複寫工作"](#)。

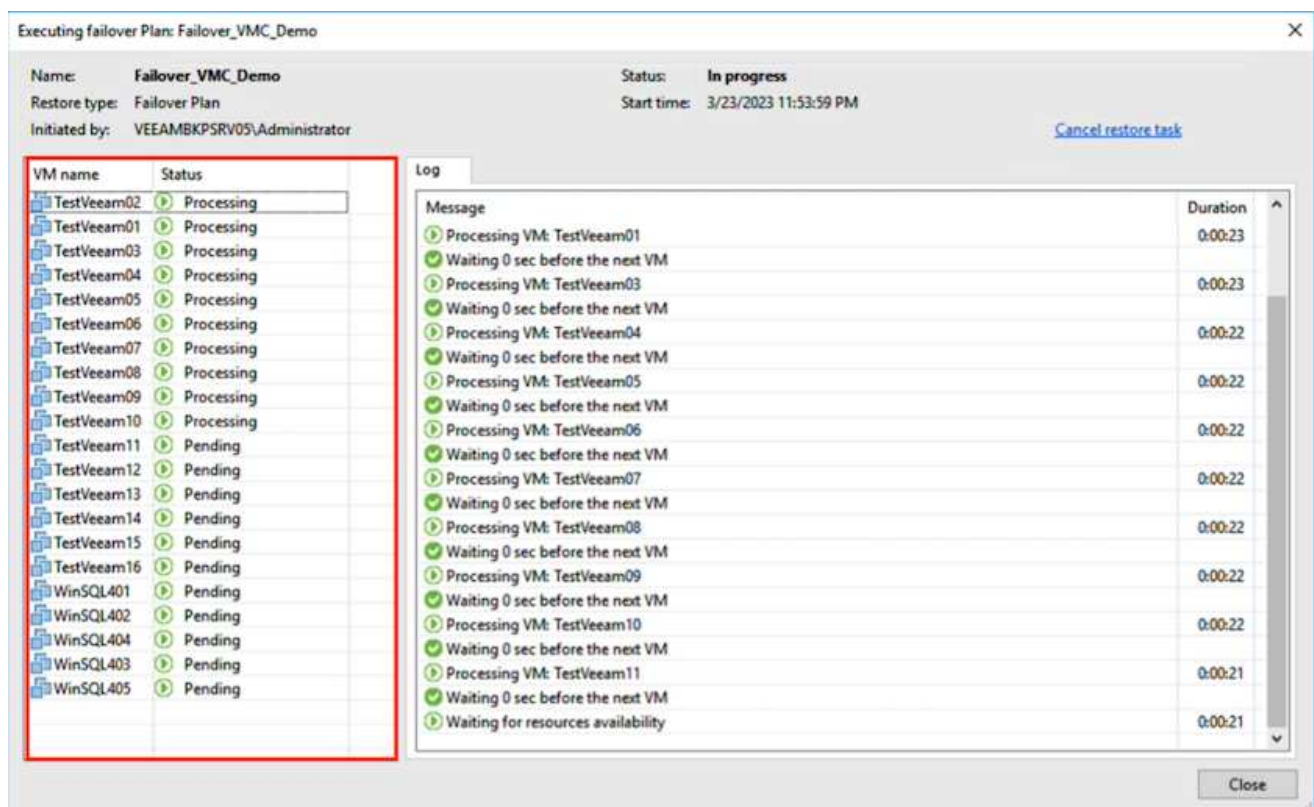
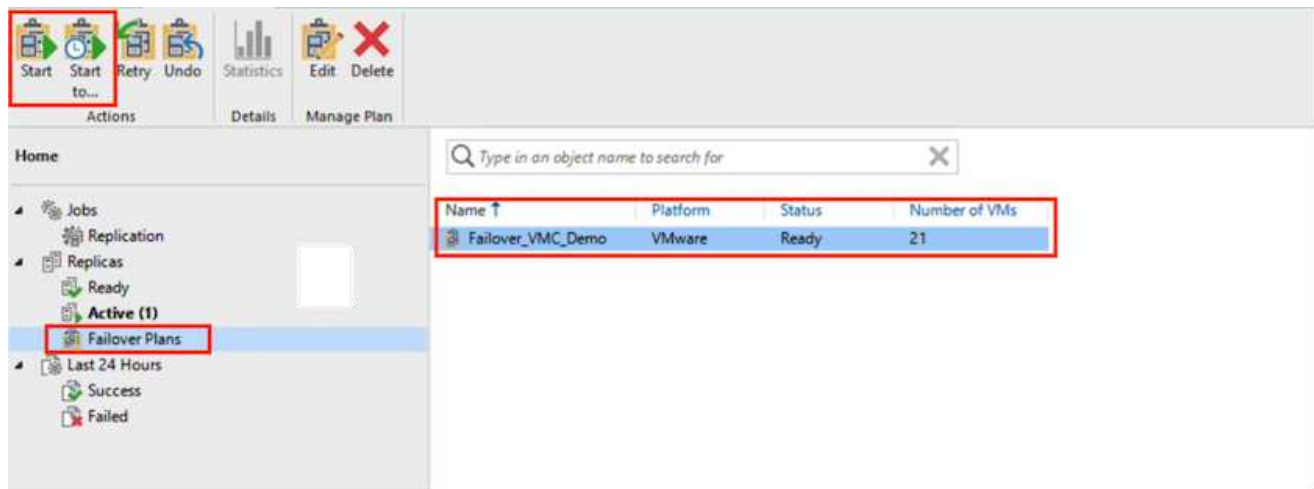
步驟 3：執行容錯移轉計畫

在容錯移轉期間、正式作業站台中的來源 VM 會切換至災難恢復站台上的複本。在容錯移轉程序中、Veeam 備份與複寫會將 VM 複本還原至所需的還原點、並將所有 I/O 活動從來源 VM 移至複本。複本不僅可在發生災難時使用、也可用於模擬災難恢復訓練。在容錯移轉模擬期間、來源 VM 仍在執行中。完成所有必要的測試後、即可復原容錯移轉並恢復正常作業。

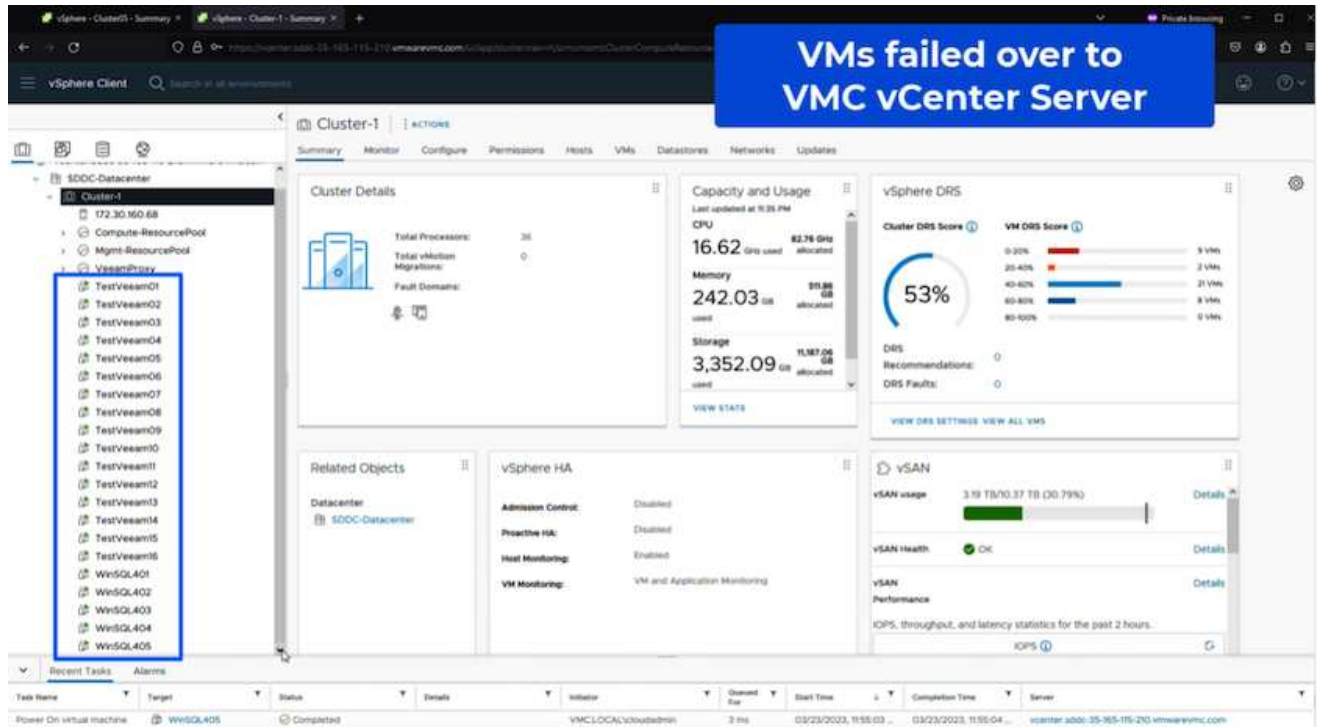


確保已建立網路區段、以避免災難恢復訓練期間發生 IP 衝突。

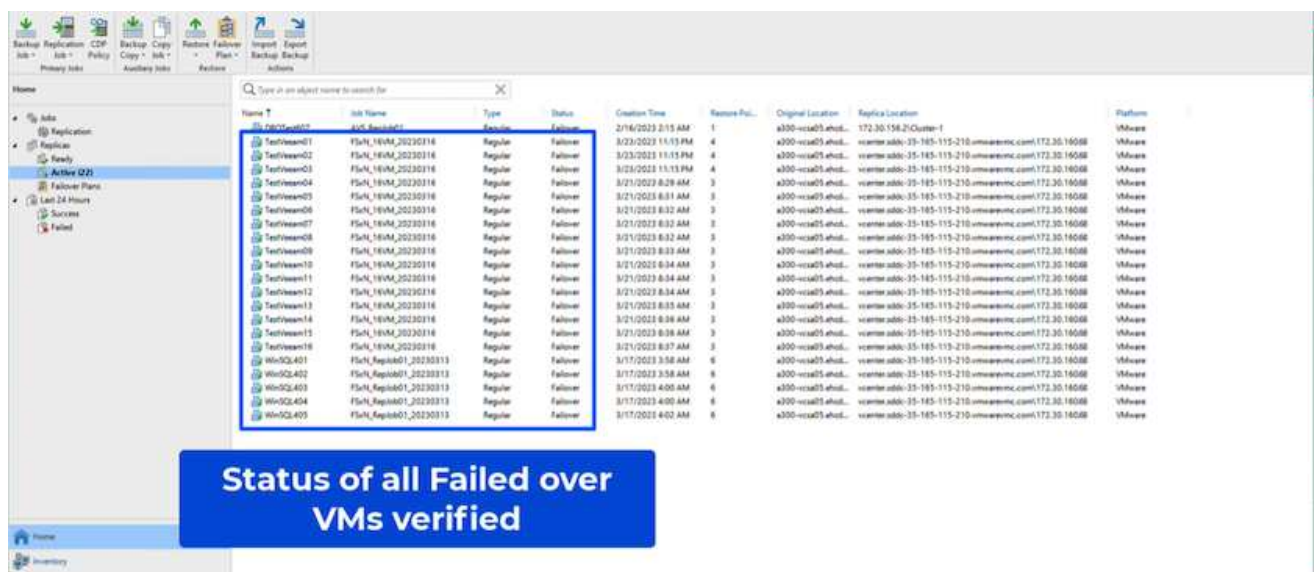
若要開始進行容錯移轉計畫、只要按一下 * 容錯移轉計畫 * 索引標籤、然後在容錯移轉計畫上按一下滑鼠右鍵即可。選擇 * Start*。這會使用最新的 VM 複本還原點進行容錯移轉。若要容錯移轉至虛擬機器複本的特定還原點、請選取 * 開始至 *。



VM 複本的狀態會從「準備就緒」變更為「容錯移轉」、而 VM 會在 AWS SDDC 叢集 / 主機上的目的地 VMware Cloud 上啟動。



容錯移轉完成後、VM 的狀態會變更為「容錯移轉」。



Veeam 備份與複寫會停止來源 VM 的所有複寫活動、直到其複本回到「就緒」狀態為止。

如需容錯移轉計畫的詳細資訊、請參閱 "容錯移轉計畫"。

步驟 4：容錯回復至正式作業網站

當容錯移轉計畫執行時、它會被視為中間步驟、需要根據需求完成。選項包括：

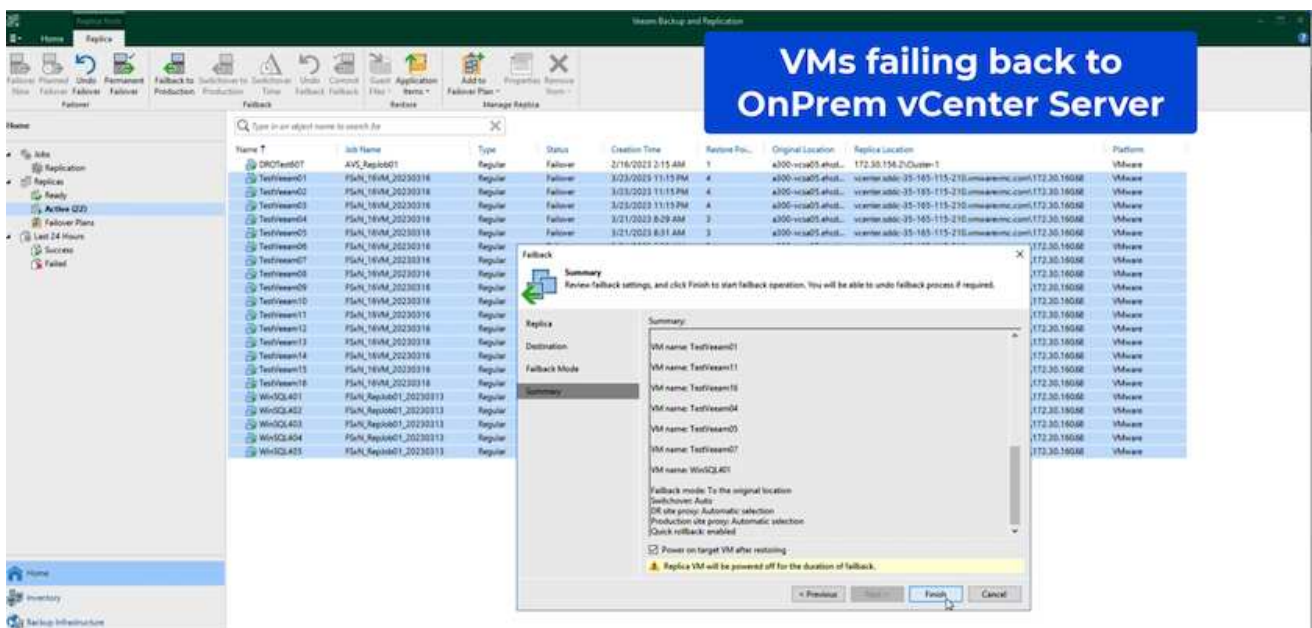
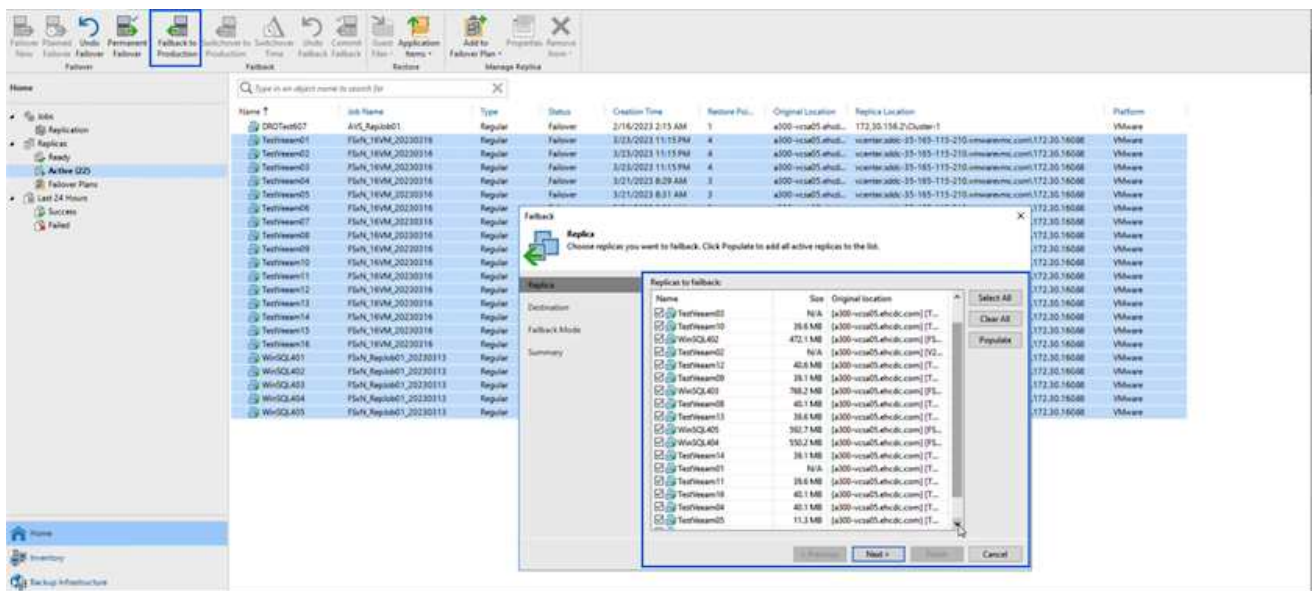
- * 容錯回復至正式作業 *：切換回原始 VM、並將 VM 複本執行時發生的所有變更傳輸至原始 VM。



當您執行容錯回復時、變更只會傳輸但不會發佈。選擇 * 提交容錯回復 * (確認原始 VM 正常運作後) 或 * 復原容錯回復 *、以在原始 VM 未如預期運作時返回 VM 複本。

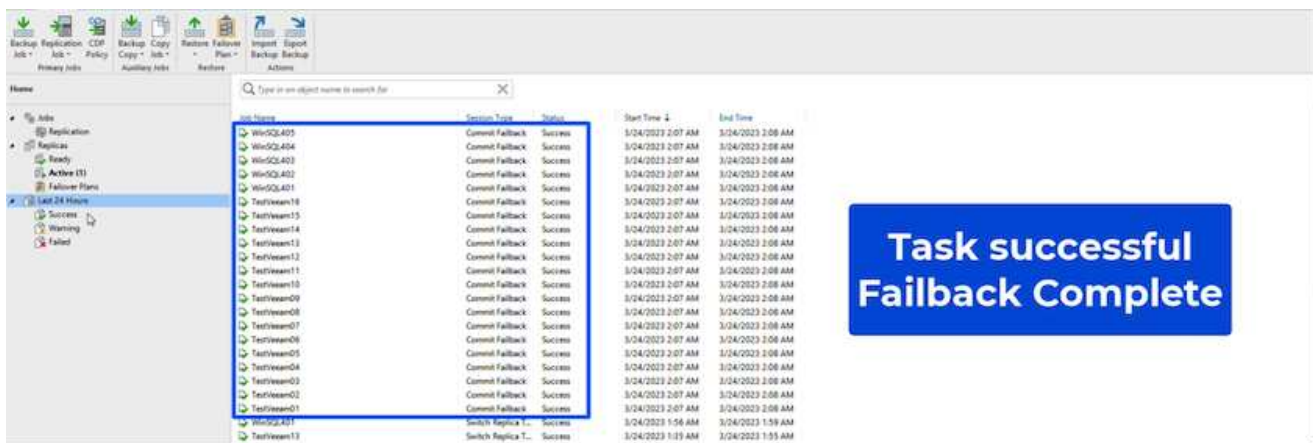
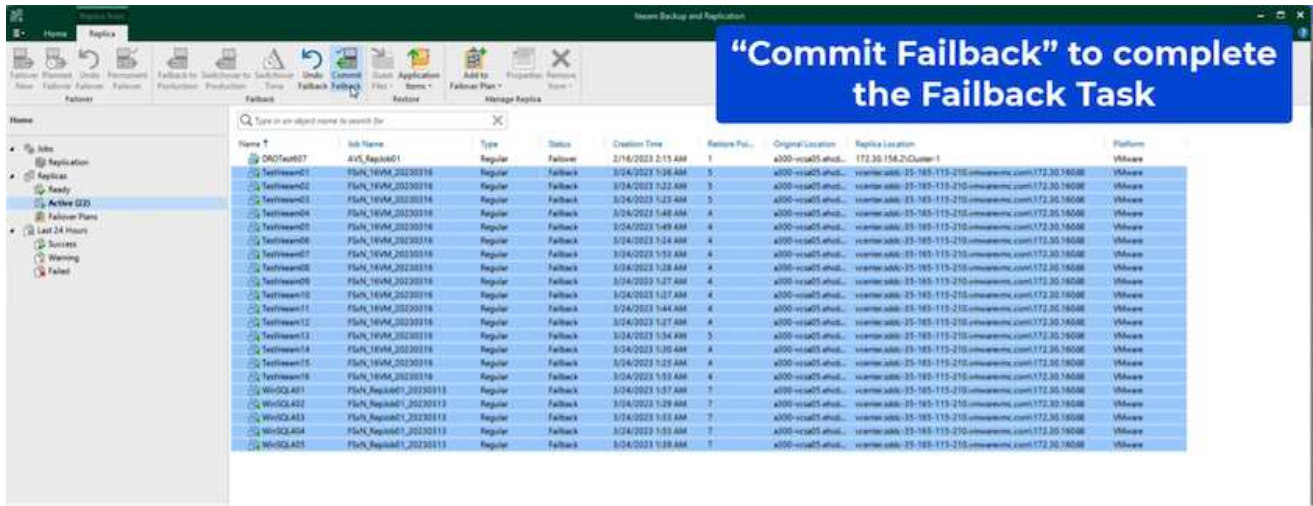
- * 復原容錯移轉 *：切換回原始 VM、並在 VM 複本執行時捨棄對其所做的所有變更。
- * 永久容錯移轉 *：從原始 VM 永久切換至 VM 複本、並將此複本作為原始 VM 使用。

在本示範中、選擇了「容錯回復至正式作業」。在精靈的「目的地」步驟中選取容錯回復至原始 VM、並啟用「還原後開啟 VM」核取方塊。

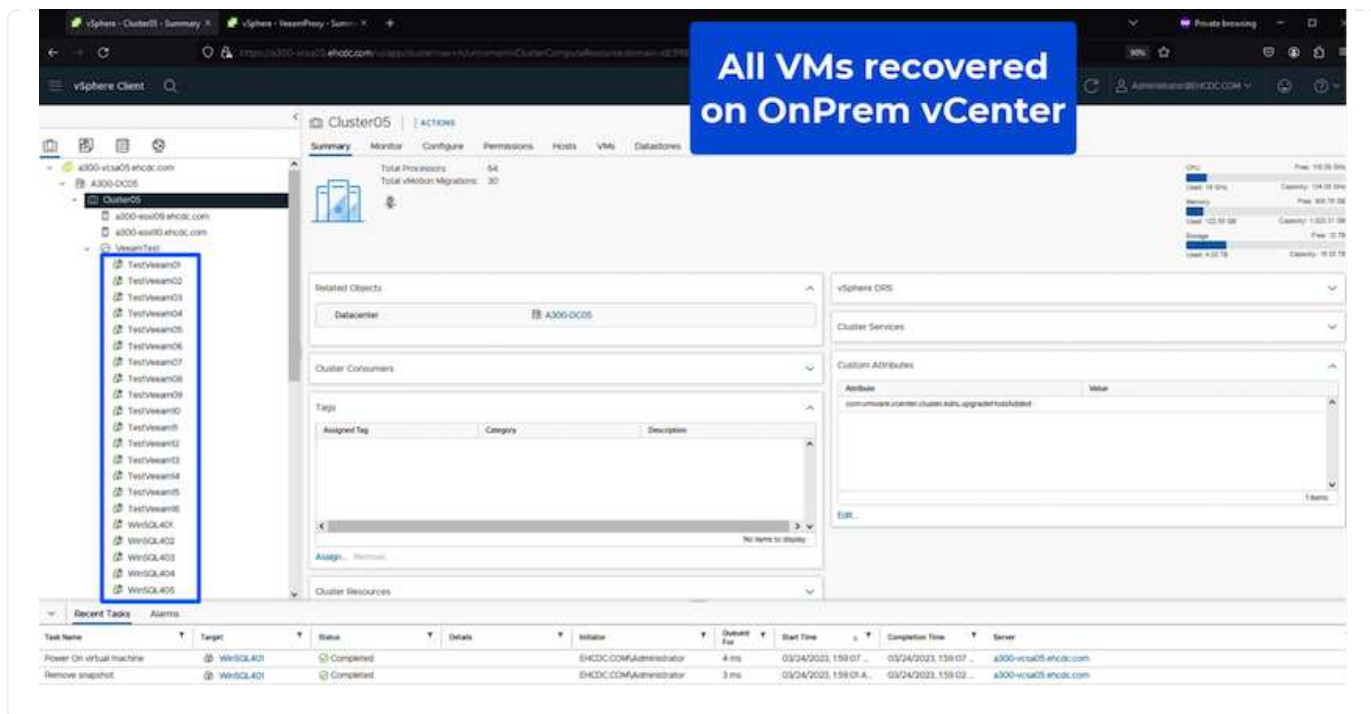


容錯回復認可是完成容錯回復作業的方法之一。提交容錯回復時、會確認傳送至容錯回復的 VM（正式作業 VM）所做的變更、均如預期運作。提交作業完成後、Veeam 備份與複製寫會恢復正式作業 VM 的複製活動。

如需容錯回復程序的詳細資訊、請參閱的 Veeam 文件 "[容錯移轉和容錯回復以進行複製](#)"。



在容錯回復至正式作業後、虛擬機器都會還原回原始正式作業站台。



結論

ONTAP 資料存放區功能的 FSX 可讓 Veeam 或任何經過驗證的協力廠商工具、使用 Pilot Light 叢集提供低成本的 DR 解決方案、而無需在叢集中直立放置大量主機、只需容納 VM 複本即可。這是一套強大的解決方案、可處理量身打造的自訂災難恢復計畫、並可重複使用內部現有的備份產品以滿足災難恢復需求、進而透過內部部署的災難恢復資料中心、實現雲端型災難恢復。當發生災難時、只要按一下按鈕、即可依照計畫進行容錯移轉或容錯移轉、並決定啟動 DR 站台。

若要深入瞭解此程序、歡迎觀看詳細的逐步解說影片。

<https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=15fed205-8614-4ef7-b2d0-b061015e925a>

在 AWS / VMC 上移轉工作負載

TR 4942 : ONTAP 使用VMware HCX將工作負載移轉至FSx支援資料存放區

Amazon Web Services (AWS) 上的VMware Cloud (VMC) 的常見使用案例、其補充NFS資料存放區位於Amazon FSx for NetApp ONTAP 的NetApp功能區上、就是移轉VMware工作負載。VMware HCX是首選選項、提供多種移轉方法、可將內部部署虛擬機器 (VM) 及其資料 (在任何VMware支援的資料存放區上執行) 移至VMC資料存放區、其中包括FSXfor ONTAP VMware上的補充NFS資料存放區。

作者：NetApp解決方案工程

總覽：使用VMware HCX、FSx ONTAP 補充資料存放區和VMware Cloud移轉虛擬機器

VMware HCX主要是一個行動平台、其設計旨在簡化跨雲端的工作負載移轉、工作負載重新平衡及營運不中斷。它是AWS上VMware Cloud的一部分、提供許多移轉工作負載的方法、可用於災難恢復 (DR) 作業。

本文件提供部署及設定VMware HCX的逐步指引、包括內部部署及雲端資料中心端的所有主要元件、可實現各種VM移轉機制。

如需詳細資訊、請參閱 ["HCX部署簡介"](#) 和 ["在AWS SDDC目的地環境上安裝檢查清單B - HCX搭配VMware Cloud"](#)。

高階步驟

此清單提供安裝及設定VMware HCX的高階步驟：

1. 透過VMware Cloud Services Console啟動VMC軟體定義資料中心（SDDC）的HCX。
2. 在內部部署的vCenter Server中下載並部署HCX Connector OVA安裝程式。
3. 使用授權金鑰啟動HCX。
4. 將內部部署的VMware HCX Connector與VMC HCX Cloud Manager配對。
5. 設定網路設定檔、運算設定檔和服務網格。
6. （選用）執行「Network Extension（網路延伸）」以延伸網路並避免重新IP。
7. 驗證應用裝置狀態、並確保可以進行移轉。
8. 移轉VM工作負載。

先決條件

開始之前、請先確定符合下列先決條件。如需詳細資訊、請參閱 ["準備安裝HCX"](#)。在具備連線能力等先決條件之後、從VMC的VMware HCX主控台產生授權金鑰、即可設定及啟動HCX。啟用HCX之後、就會部署vCenter外掛程式、並可透過vCenter主控台進行管理來存取。

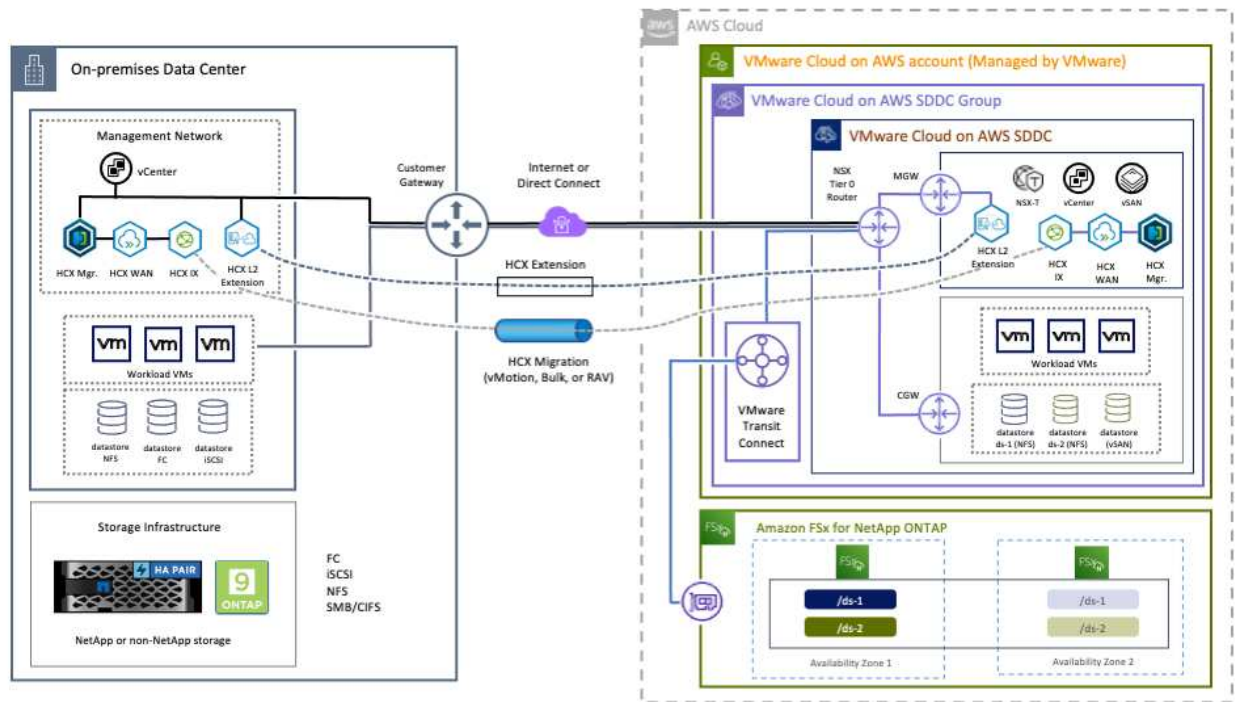
在繼續執行HCX啟動與部署之前、必須先完成下列安裝步驟：

1. 請使用現有的VMC SDDC、或在這之後建立新的SDDC ["NetApp連結"](#) 或是這種情況 ["VMware連結"](#)。
2. 從內部部署vCenter環境到VMC SDDC的網路路徑、必須使用vMotion來支援VM移轉。
3. 請確定所需的 ["防火牆規則和連接埠"](#) 允許內部部署vCenter Server與SDDC vCenter之間的VMotion流量。
4. FSx for ONTAP SforiNFS Volume應安裝為VMC SDDC的補充資料存放區。若要將NFS資料存放區附加至適當的叢集、請遵循本文所述的步驟 ["NetApp連結"](#) 或是這種情況 ["VMware連結"](#)。

高層架構

為了進行測試、此驗證所使用的內部部署實驗室環境是透過站台對站台VPN連線至AWS VPC、因此可透過外部傳輸閘道、在內部部署連線至AWS和VMware Cloud SDDC。HCx移轉與網路延伸流量會透過網際網路在內部部署與VMware雲端目的地SDDC之間傳輸。此架構可修改為使用Direct Connect私有虛擬介面。

下圖說明高層架構。



解決方案部署

請依照一系列步驟完成本解決方案的部署：

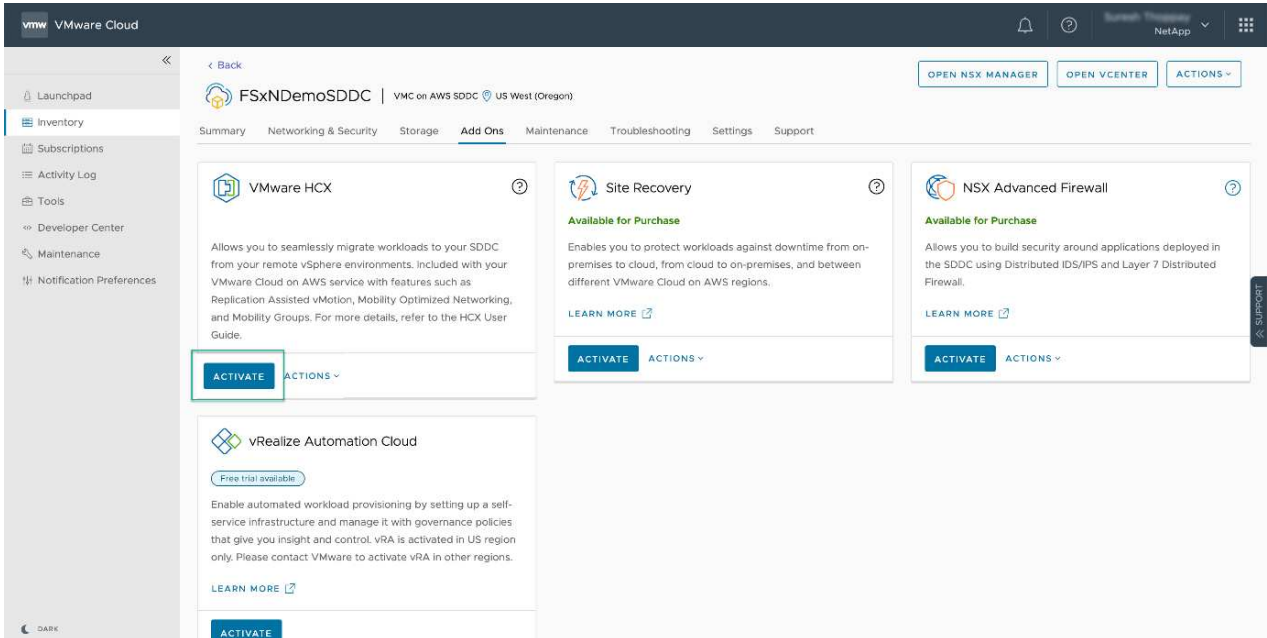
步驟1：使用附加元件選項透過VMC SDDC啟動HCX

若要執行安裝、請完成下列步驟：

1. 登入VMC主控台：["vmc.vmware.com"](https://vmc.vmware.com) 並存取庫存。
2. 若要選取適當的SDDC並存取附加元件、請按一下「View Details on SDDC（在SDDC上檢視詳細資料）」、然後選取「Add Ons（新增附加元件）」索引標籤。
3. 按一下「啟用VMware HCX」。



完成此步驟最多需要25分鐘。

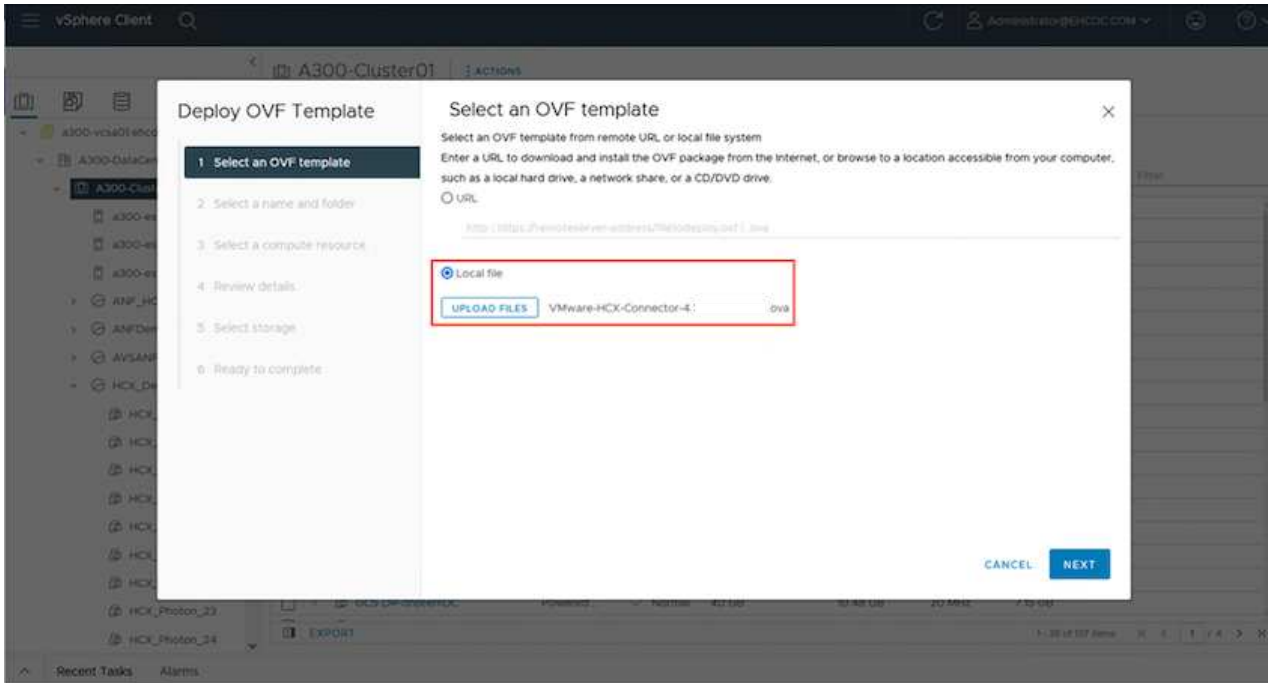


4. 部署完成後、確認vCenter Console中有可用的HCX Manager及其相關外掛程式、以驗證部署。
5. 建立適當的管理閘道防火牆、以開啟存取HCX Cloud Manager所需的連接埠。HCX Cloud Manager現在已可開始執行HCX作業。

步驟2：在內部部署vCenter Server中部署安裝程式OVA

若要讓內部部署連接器與VMC中的HCX Manager通訊、請確定內部部署環境中已開啟適當的防火牆連接埠。

1. 從VMC主控台瀏覽至HCX儀表板、移至「Administration」（管理）、然後選取「Systems Update」（系統更新）索引標籤。按一下「Request a Download Link for the HCX Connector OVA image」（申請HCX Connector OVA映像的下載連結）
2. 下載HCX Connector之後、在內部部署的vCenter Server中部署OVA。以滑鼠右鍵按一下vSphere叢集、然後選取部署OVF範本選項。

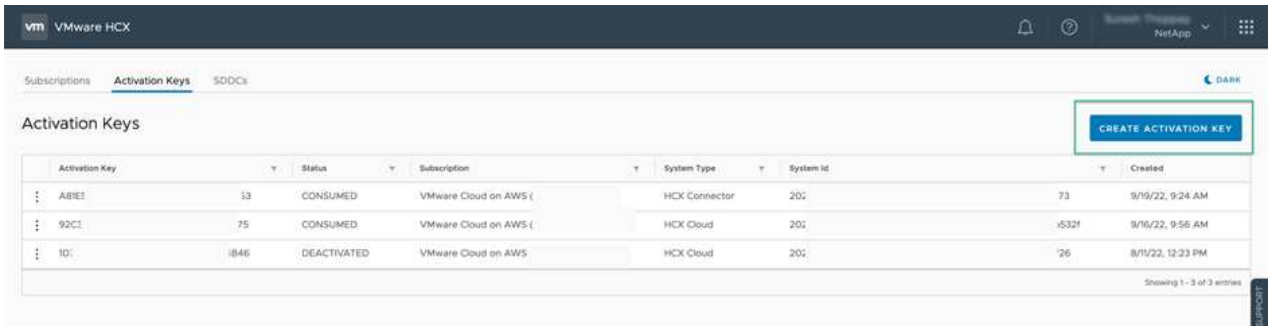


3. 在「部署OVF範本」精靈中輸入必要資訊、按一下「下一步」、然後按一下「完成」以部署VMware HCX Connector OVA。
4. 手動開啟虛擬應用裝置電源。如需逐步指示、請前往 "[VMware HCX使用者指南](#)"。

步驟3：使用授權金鑰啟動HCX Connector

在內部部署VMware HCX Connector OVA並啟動應用裝置之後、請完成下列步驟以啟動HCX Connector。從VMC的VMware HCX主控台產生授權金鑰、並在VMware HCX Connector安裝期間輸入授權。

1. 從VMware Cloud Console移至「Inventory（資源清冊）」、選取SDDC、然後按一下「View Details（檢視詳細資料）」。在「Add Ons（新增選項）」索引標籤的VMware HCX動態磚中、按一下「Open HCX（開啟HCX）」。
2. 在「啟用金鑰」索引標籤中、按一下「建立啟動金鑰」。選取「System Type（系統類型）」作為HCX Connector、然後按一下「Confirm（確認）」以產生金鑰。複製啟動金鑰。



部署在內部部署的每個HCX Connector都需要個別的金鑰。

3. 登入內部部署的VMware HCX Connector、網址為 "https://hcxconnectorIP:9443" 使用系統管理員認證。



使用在OVA部署期間定義的密碼。

4. 在「授權」區段中、輸入從步驟2複製的啟動金鑰、然後按一下「啟動」。



內部部署的HCX Connector必須能存取網際網路、才能成功完成啟動。

5. 在「資料中心位置」下、提供在內部部署環境中安裝VMware HCX Manager所需的位置。按一下「繼續」。
6. 在「System Name（系統名稱）」下、更新名稱、然後按「Continue（繼續）」。
7. 選取「Yes（是）」、然後繼續。
8. 在「Connect your vCenter（連線vCenter）」下、提供vCenter Server的IP位址或完整網域名稱（FQDN）和認證、然後按一下「Continue（繼續）」。



使用FQDN以避免稍後發生通訊問題。

9. 在「Configure SSO/PSC（設定SSO/PSC）」下、提供Platform Services Controller的FQDN或IP位址、然後按一下「Continue（繼續）」。



輸入vCenter Server的IP位址或FQDN。

10. 確認輸入的資訊正確無誤、然後按一下「重新啟動」。

11. 完成後、vCenter Server會顯示為綠色。vCenter Server和SSO都必須具有正確的組態參數、此參數應與上一頁相同。



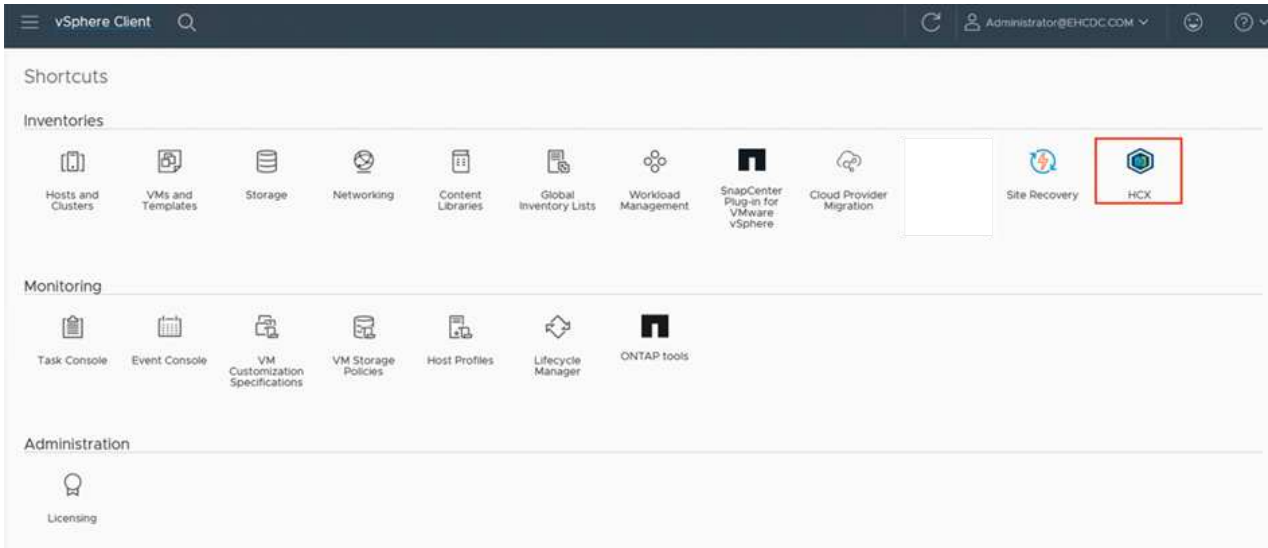
此程序大約需要10–20分鐘、而外掛程式則要新增至vCenter Server。

The screenshot displays the VMware HCX Manager dashboard for a device named VMware-HCX-440. The top navigation bar includes 'Dashboard', 'Appliance Summary', 'Configuration', and 'Administration'. The main content area is divided into several sections:

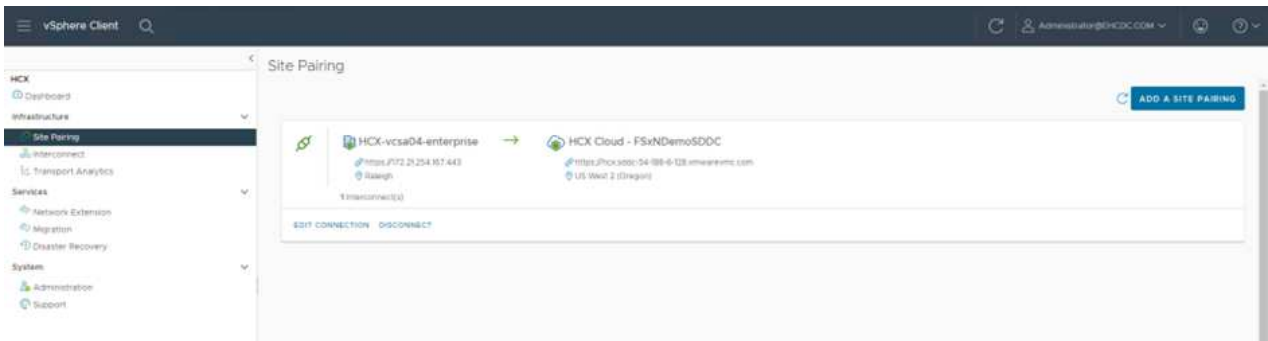
- System Information:** FQDN: VMware-HCX-440.ehcdc.com, IP Address: 172.2, Version: 4.4.1.0, Uptime: 20 days, 21 hours, 9 minutes, Current Time: Tuesday, 13 September 2022 07:44:11 PM UTC.
- Resource Usage:** Three bar charts showing CPU (67% used), Memory (81% used), and Storage (23% used).
- Configuration Grid:** A table with three columns: NSX, vCenter, and SSO. The vCenter and SSO rows contain the URL 'https://a300-vcxa01.ehcdc.com' and a green status indicator.

步驟4：將內部部署的VMware HCX Connector與VMC HCX Cloud Manager配對

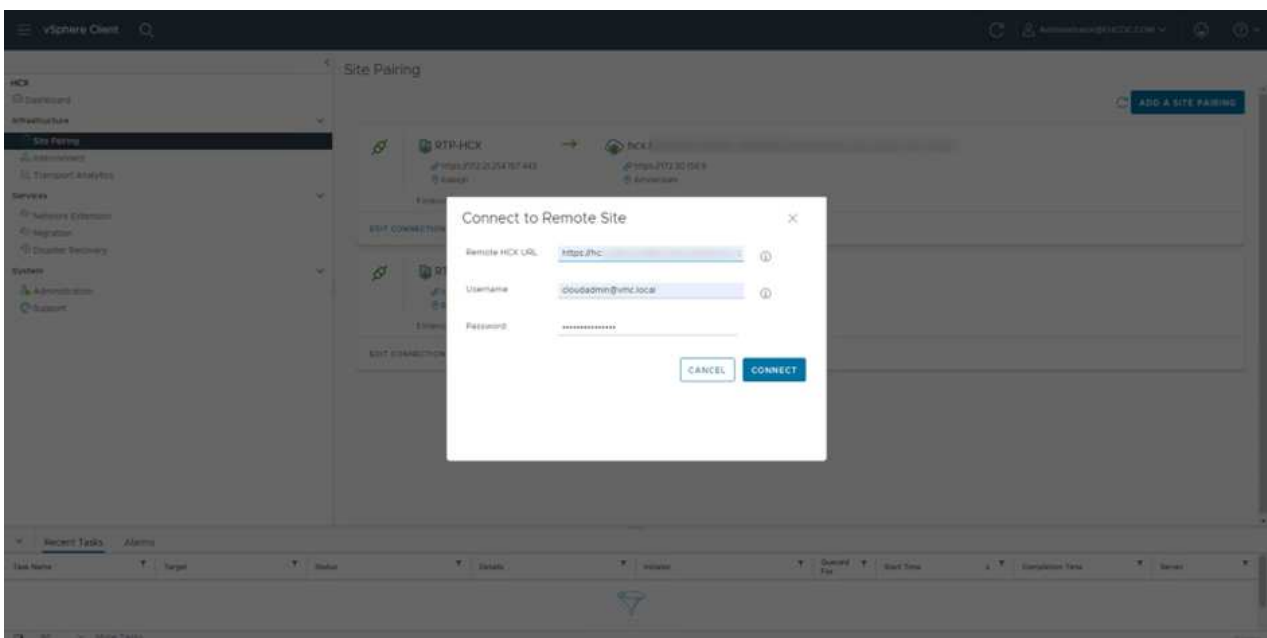
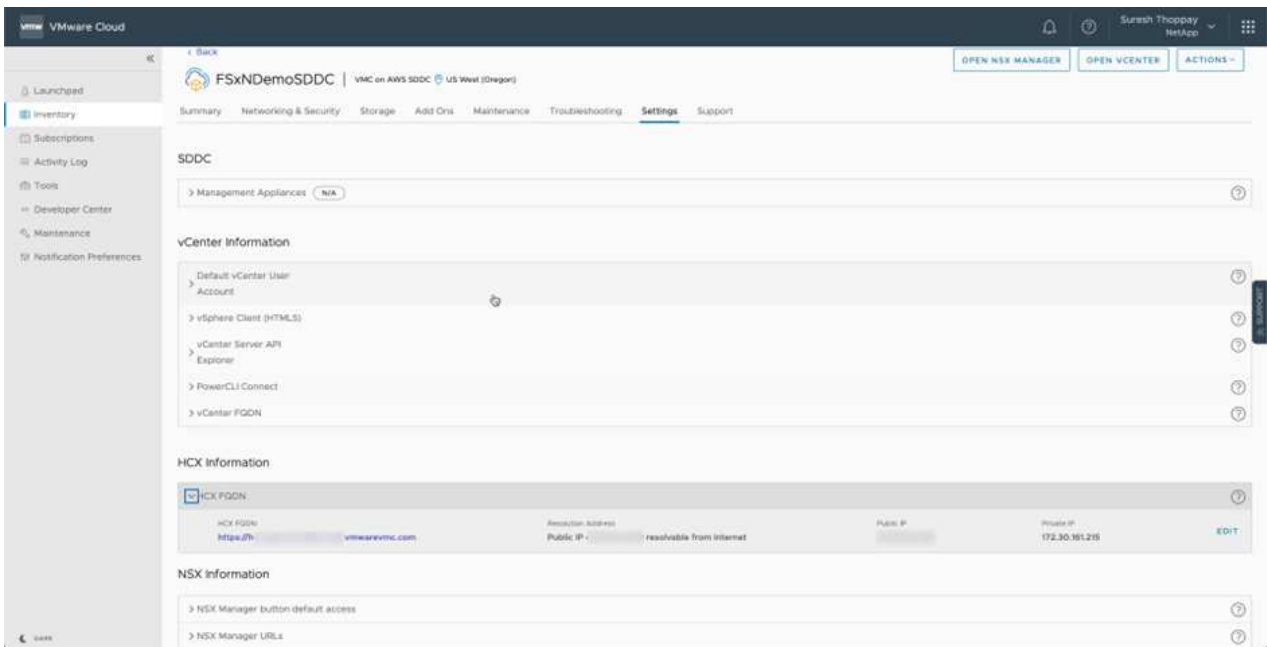
1. 若要在內部部署vCenter Server和VMC SDDC之間建立站台配對、請登入內部部署vCenter Server、然後存取HCX vSphere Web Client外掛程式。



2. 按一下「基礎架構」下的「新增站台配對」。若要驗證遠端站台、請輸入VMC HCX Cloud Manager URL或IP位址、以及CloudAdmin角色的認證資料。



HCx資訊可從SDDC設定頁面擷取。



3. 若要啟動站台配對、請按一下「Connect (連線)」。



VMware HCX Connector 必須能夠透過連接埠 443 與 HCX Cloud Manager IP 通訊。

4. 建立配對之後、即可在 HCX 儀表板上取得新設定的站台配對。

步驟5：設定網路設定檔、運算設定檔和服務網格

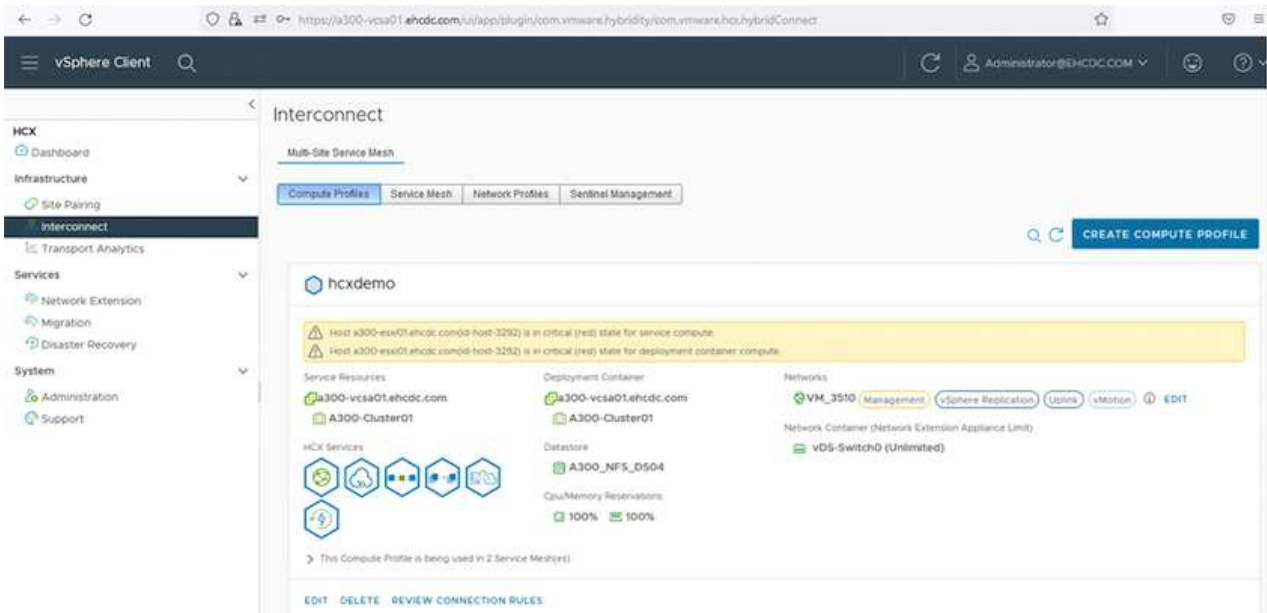
VMware HCX互連（HCX-IX）應用裝置可透過網際網路提供安全通道功能、並可透過私有連線至目標站台、以啟用複製和VMotion型功能。互連提供加密、流量工程和SD-WAN。若要建立HCI IX-IX互連設備、請完成下列步驟：

1. 在「基礎架構」下、選取「互連」>「多站台服務網狀架構」>「運算設定檔」>「建立運算設定檔」。



運算設定檔包含部署互連虛擬應用裝置所需的運算、儲存和網路部署參數。他們也會指定HCX服務可以存取VMware資料中心的哪個部分。

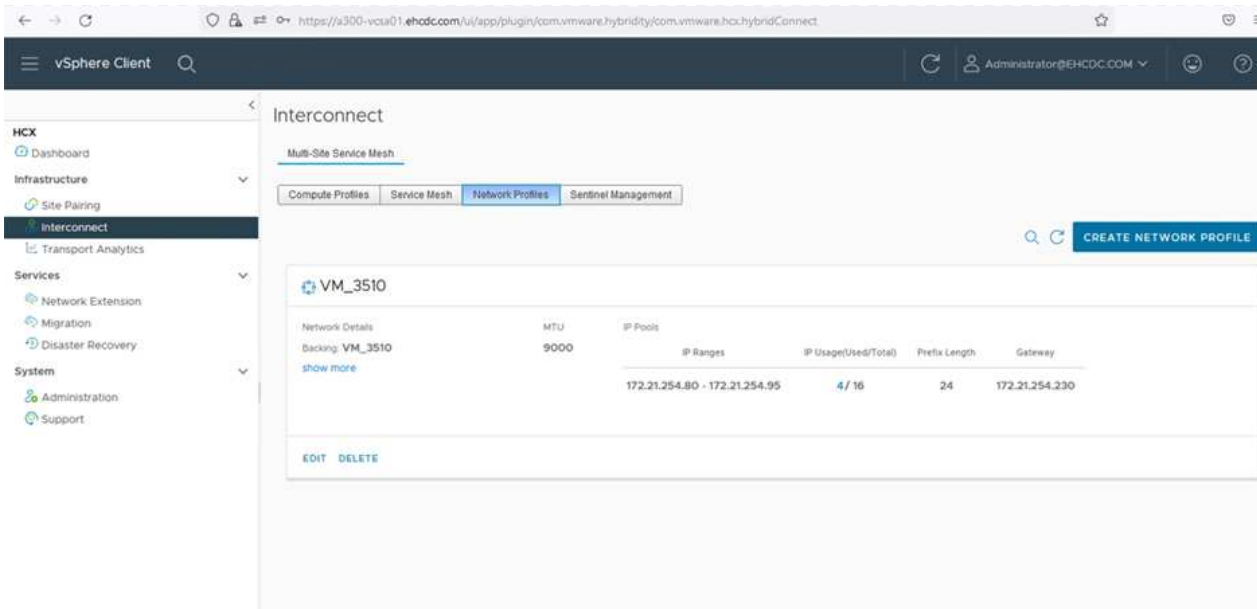
如需詳細指示、請參閱 ["建立運算設定檔"](#)。



2. 建立運算設定檔之後、選取「Multi-Site Service Mesh」（多站台服務網格）>「Network Profiles」（網路設定檔）>「Create Network Profile」（建立網路設定檔）、即可建立網路設定檔。
3. 網路設定檔會定義一系列IP位址和網路、以供HCX用於其虛擬應用裝置。



這需要兩個以上的IP位址。這些IP位址將從管理網路指派給虛擬應用裝置。



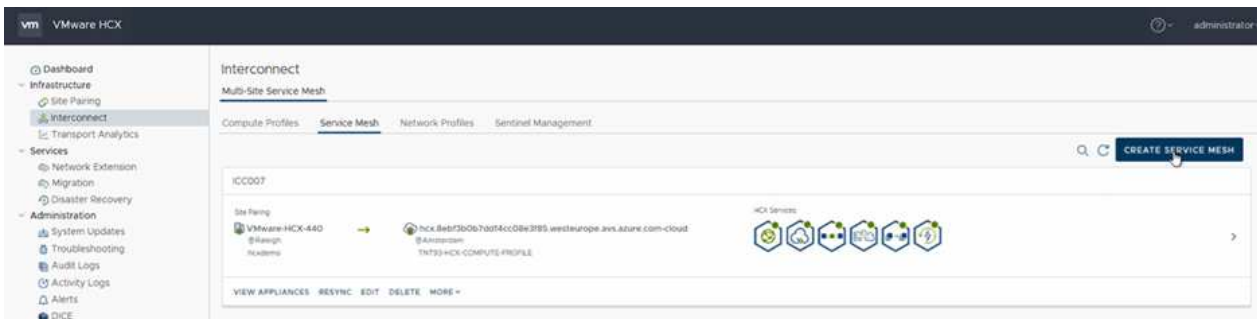
如需詳細指示、請參閱 ["建立網路設定檔"](#)。



如果您透過網際網路連線至SD-WAN、則必須在「網路與安全性」區段下保留公用IP。

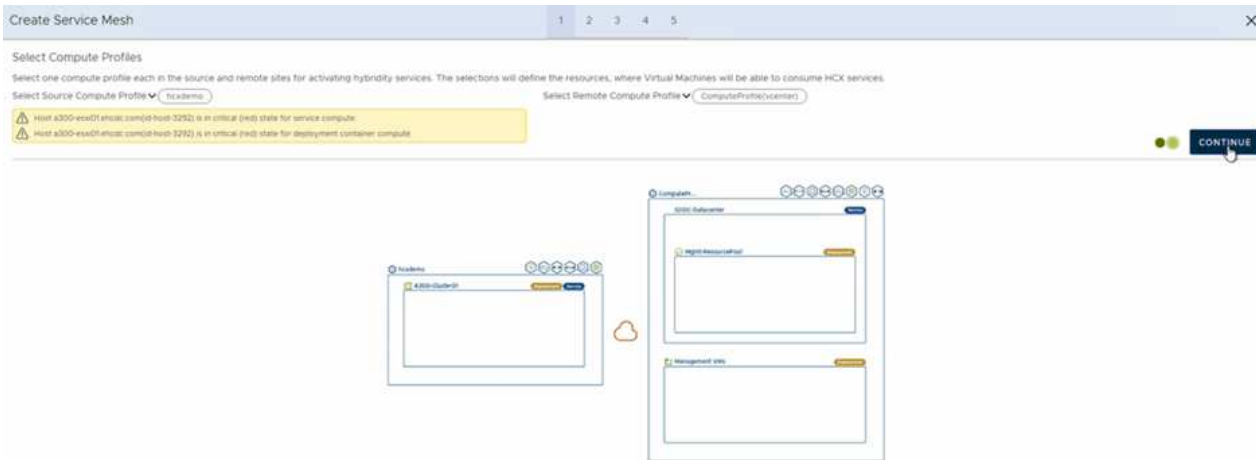
- 若要建立服務網格、請選取Interconnect選項中的Service Mesh（服務網格）索引標籤、然後選取內部部署和VMC SDDC站台。

服務網格會建立本機和遠端運算和網路設定檔配對。

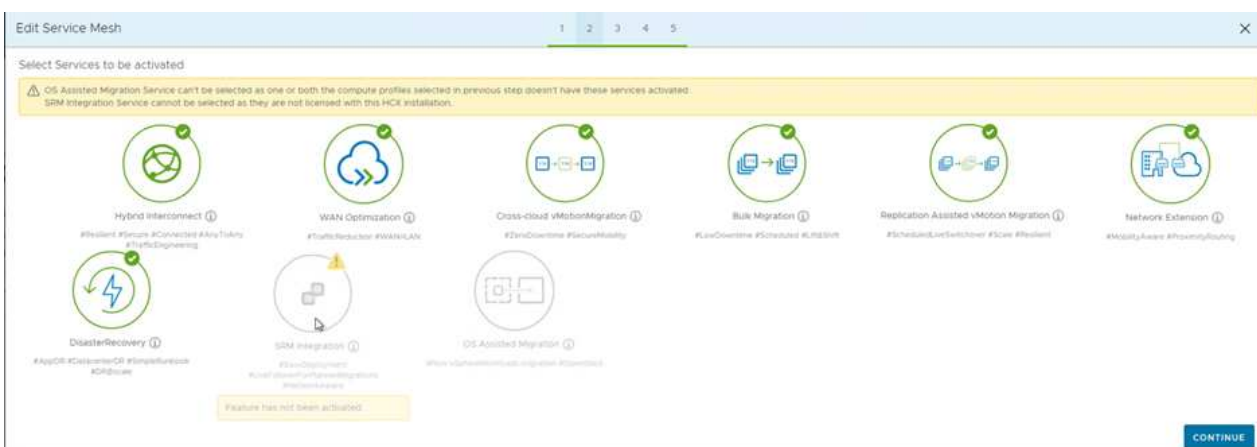


此程序的一部分涉及部署HCX應用裝置、這些裝置將會自動設定在來源和目標站台上、以建立安全的傳輸架構。

- 選取來源和遠端運算設定檔、然後按一下「Continue（繼續）」。



6. 選取要啟動的服務、然後按一下「Continue (繼續)」。



複寫輔助VMotion移轉、SRM整合及OS輔助移轉需要HCX Enterprise授權。

7. 建立服務網格的名稱、然後按一下「完成」開始建立程序。完成部署約需30分鐘。設定好服務網格後、就會建立移轉工作負載VM所需的虛擬基礎架構和網路。

- HCI**
- Dashboard
- Infrastructure
- Interconnect**
- Transport Analytics
- Services
 - Network Extension
 - Migration
 - Disaster Recovery
- System
 - Administration
 - Support

Interconnect

Multi-Service View

Configure Profiles | **Service View** | Select Profiles | Service Management

← KCC007 | EDIT SERVICE MESH

🔍 📄 🔄

Appliance Name	Appliance Type	IP Address	Current Status	Current Version	Appliance Version
KCC007-40-0 w/ 8551a7b1-812d-4f31-8121-8122b6a6d036 Endpoint: K300-Customer01 Storage: K300_MPL_C204	HCI-INGRESS	172.21.28.81	🟢 View Refresh	4.4.0.0	4.4.1.0 View
KCC007-40-1 w/ 1f75a7b1-812d-4f31-8121-8122b6a6d036 Endpoint: K300-Customer01 Storage: K300_MPL_C204 Network Controller: NS-1-0-0-0-0 Extended Network: 0.0.0.0	HCI-NET-EXT	172.21.28.8	🟢 View Refresh	4.4.0.0	4.4.1.0 View
KCC007-40-4 w/ 84817742-7561-4684-c036-468444d7561 Endpoint: K300-Customer01 Storage: K300_MPL_C204	HCI-INGRESS-OUT			7.3.0.0	N/A

1 Appliance(s)

Appliances on hcx.8ebf3b0a7daf4cc08e3f85.westeurope.azure.com-cloud

Appliance Name	Appliance Type	IP Address	Current Version
KCC007-40-1	HCI-INGRESS	172.21.28.87 172.21.28.148 172.21.28.17 172.21.28.3	4.4.0.0
KCC007-40-1	HCI-NET-EXT	172.21.28.88 172.21.28.2	4.4.0.0
KCC007-40-1	HCI-INGRESS-OUT		7.3.0.0

步驟6：移轉工作負載

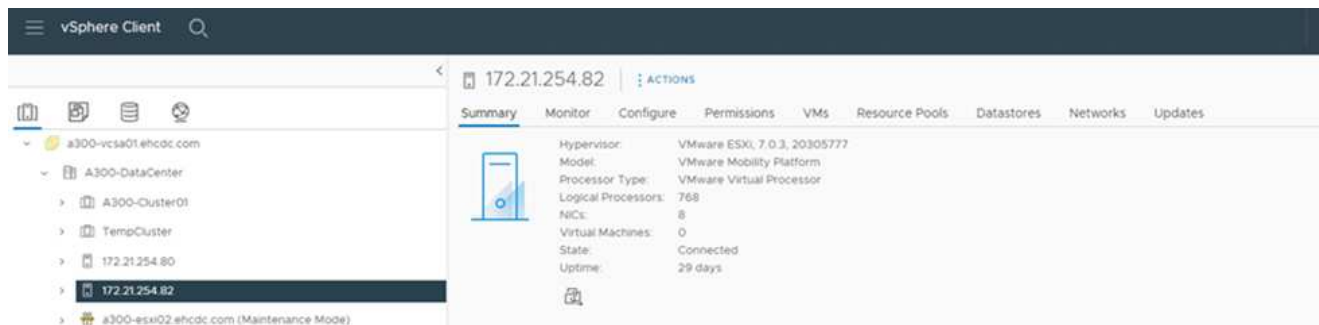
HCx可在兩個或多個不同的環境（例如內部部署環境和VMC SDDC）之間提供雙向移轉服務。應用程式工作負載可使用各種移轉技術、例如HCX大量移轉、HCX vMotion、HCX冷移轉、HCX複寫輔助vMotion（可搭配HCX Enterprise版本使用）、以及HCX OS輔助移轉（可搭配HCX Enterprise版本使用）、移轉至或移轉至HCX啟動的站台。

若要深入瞭解可用的HCX移轉技術、請參閱 "[VMware HCX移轉類型](#)"

HCX-IX應用裝置使用行動代理程式服務來執行VMotion、Cold和Replication輔助VMotion（RAV）移轉。



HCX-IX應用裝置會將行動代理程式服務新增為vCenter Server中的主機物件。此物件上顯示的處理器、記憶體、儲存設備和網路資源、並不代表裝載IX應用裝置的實體Hypervisor實際使用量。



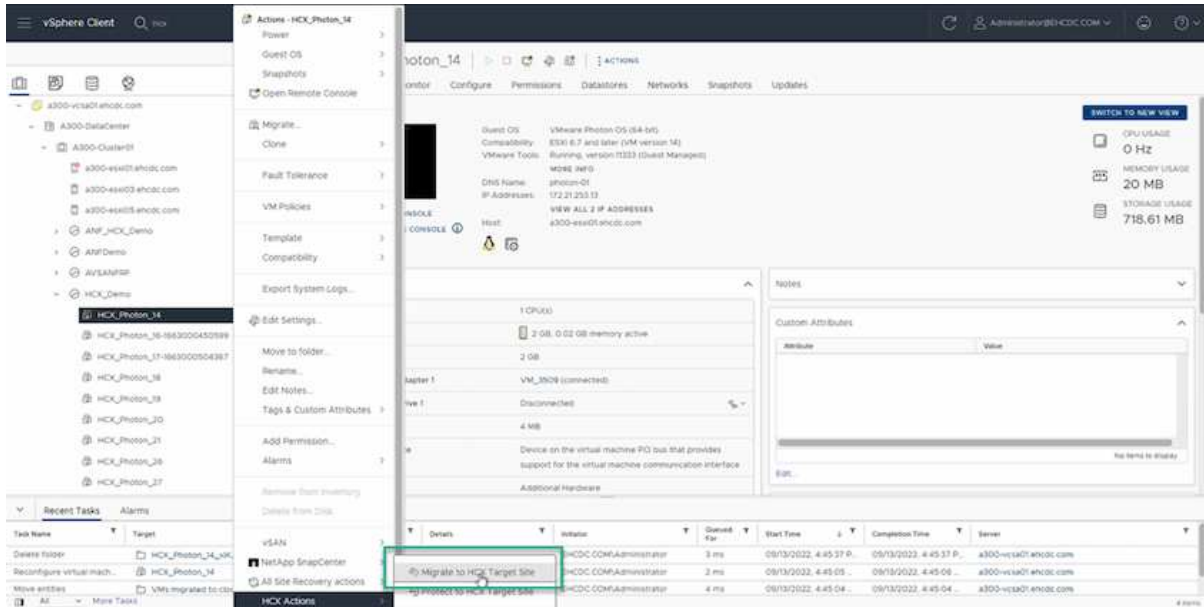
VMware HCX vMotion

本節說明HCX vMotion機制。此移轉技術使用VMware vMotion傳輸協定將VM移轉至VMC SDDC。
◦ vMotion移轉選項可用於一次移轉單一VM的VM狀態。此移轉方法不會中斷服務。

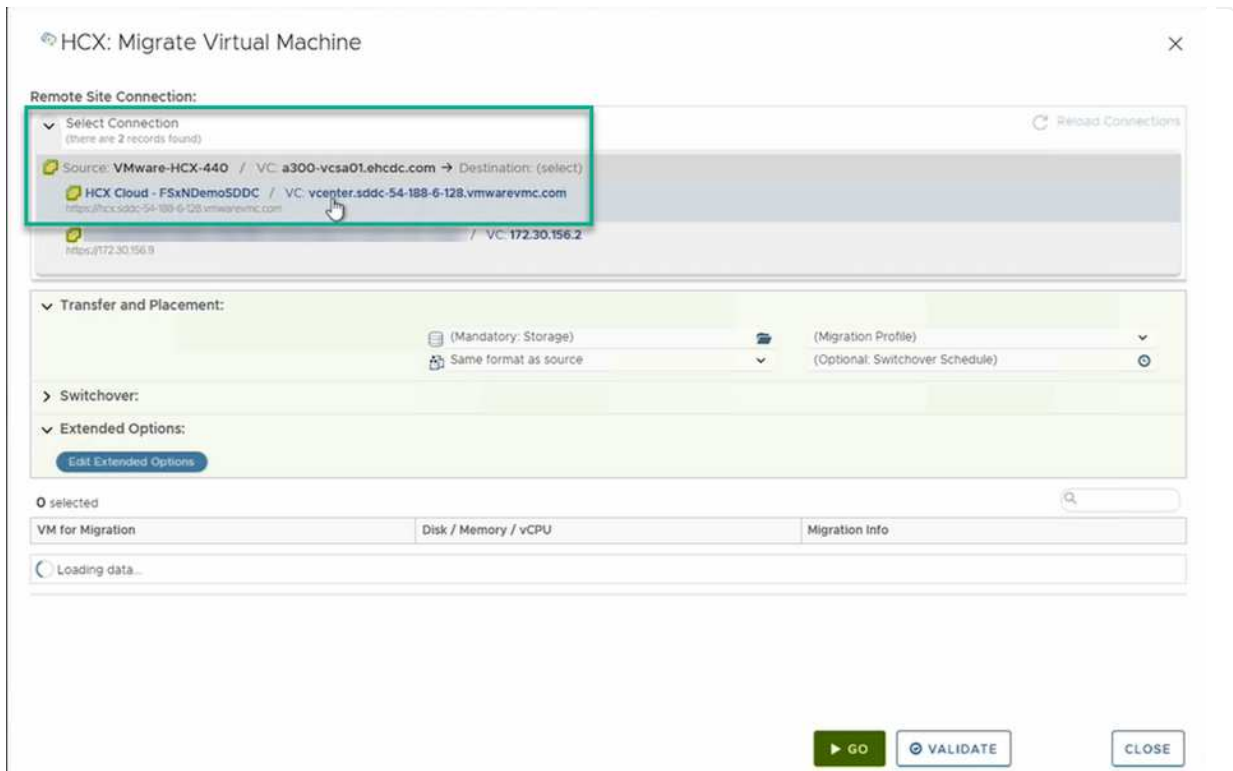


網路擴充功能應已就緒（適用於連接VM的連接埠群組）、以便在不需要變更IP位址的情況下移轉VM。

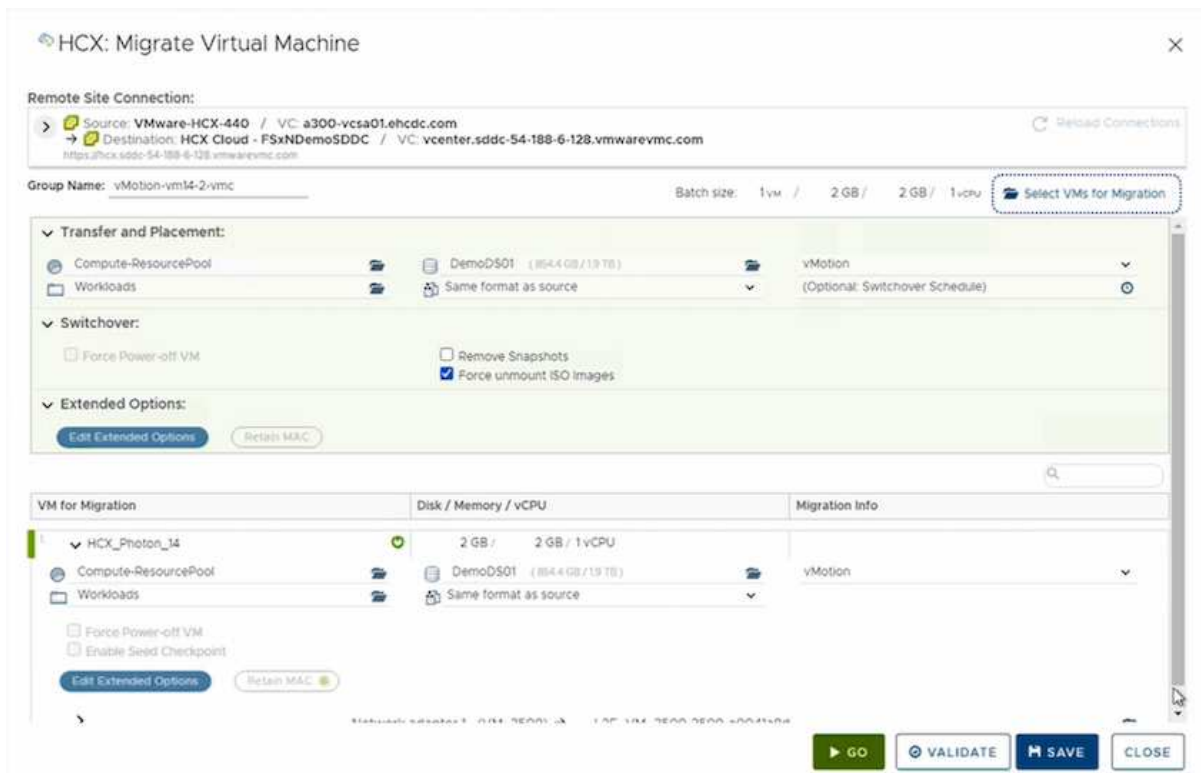
1. 從內部部署vSphere用戶端移至「Inventory」、在要移轉的VM上按一下滑鼠右鍵、然後選取「HCX Actions」（HCX動作）>「移轉至HCX目標站台」。



2. 在移轉虛擬機器精靈中、選取遠端站台連線（目標VMC SDDC）。



3. 新增群組名稱、並在「Transfer and Placement (傳輸和放置)」下更新必填欄位 (叢集、儲存設備和目的地網路)、然後按一下「Validate (驗證)」。



4. 驗證檢查完成後、按一下「Go (執行)」以啟動移轉。



VMotion傳輸會擷取VM作用中記憶體、其執行狀態、IP位址及其MAC位址。如需有關HCX VMotion需求與限制的詳細資訊、請參閱 "[瞭解VMware HCX VMotion和冷移轉](#)"。

5. 您可以從HCX >移轉儀表板監控VMotion的進度 and 完成。

The screenshot shows the vSphere Client interface with the Migration dashboard. The dashboard displays a table of migration tasks and their progress. The main task, VM_3005, is shown as 'Migrating Virtual Machine' with a progress bar at 100%. Below this, a table lists other migration tasks, all of which are 'Migration Complete'.

Task Name	Target	Status	Details	Initiator	Duration	Start Time	Completion Time	Server
Reocate virtual machine	HCX_Photon_14	100%	Migrating Virtual Machine ac...	EHCDC.COM\Administrator	3 ms	09/13/2022, 4:59:08...		a300-vc3a01.ehcdc.com
Refresh host storage i...	172.21.254.82	Completed		EHCDC.COM\Administrator	3 ms	08/13/2022, 4:57:43 P...	08/13/2022, 4:57:43 P...	a300-vc3a01.ehcdc.com

VMware複寫輔助vMotion

您可能從VMware文件中看到、VMware HCX Replication輔助VMotion (RAV) 結合了大量移轉與VMotion的優點。大量移轉使用vSphere Replication平行移轉多個VM、而VM會在切換期間重新開機。HCx vMotion可在不中斷的情況下進行移轉、但會在複寫群組中一次連續執行一部VM。RAV會平行複寫VM、並保持同步、直到切換期間為止。在切換過程中、它一次移轉一個VM、而不會停機。

下列快照顯示移轉設定檔為「複寫輔助vMotion」。

Workload Mobility

Remote Site Connection: Reverse Migration

Destination: RTP-HCX / VC: a300-vcsa01.ehcdc.com ← Source: HCX Cloud - FSXDemoSDCC / VC: vcenter.sddc-54-188-6-128.vmwarevmc.com

Group Name: ToRTP

Batch size: 4 vms / 8 GB / 8 GB / 4 vCPU

Transfer and Placement:

- VMC_Demo
- A300 NFS_D503 (1.9 TB / 4 TB)
- Same format as source

Switchover:

Extended Options:

Migration Profile: Replication-assisted vMotion

VM for Migration	Disk / Memory / vCPU	Migration Info
> HCX_Photon_11	2 GB / 2 GB / 1 vCPU	(Migration profile is not specified)
> HCX_Photon_12	2 GB / 2 GB / 1 vCPU	(Migration profile is not specified)
> HCX_Photon_13	2 GB / 2 GB / 1 vCPU	(Migration profile is not specified)
> HCX_Photon_14	2 GB / 2 GB / 1 vCPU	(Migration profile is not specified)

GO VALIDATE SAVE CLOSE

與少數VM的vMotion相比、複寫的持續時間可能會更長。使用RAV時、只能同步差異並納入記憶體內容。以下是移轉狀態的快照、顯示移轉的開始時間與每個VM的結束時間如何相同。

vSphere Client

Migration

Name	VM(s) / Storage / Memory / CPU(s)	Progress	Start	End	Status
vcenter.sddc-54-188-6-128.vmwarevmc.com → a300-vcsa01.ehcdc.com					
ToRTP					
1	HCX_Photon_11	100%	03:20 PM Tue 03	03:21 PM Tue 03	Migration completed
2	HCX_Photon_12	100%	03:20 PM Tue 03	03:24 PM Tue 03	Migration completed
3	HCX_Photon_13	100%	03:20 PM Tue 03	03:26 PM Tue 03	Migration completed
4	HCX_Photon_14	100%	03:20 PM Tue 03	03:28 PM Tue 03	Migration completed
2023-09-22 15:44:07 UTC					
vcenter.sddc-54-188-6-128.vmwarevmc.com ← a300-vcsa01.ehcdc.com					
FromRTP					

Recent Tasks

Task Name	Target	Status	Details	Initiator	Duration	Start Time	Completion Time	Server
Create virtual machine	HCX_Photon_11_Shadow	Completed		VMC.LOCAL\Administrator	2 ms	09/23/2022, 4:03:09	09/23/2022, 4:03:10	vcenter.sddc-54-188-6-128.vmwarevmc.com
Unregister virtual machine	HCX_Photon_11	Completed		VMC.LOCAL\Administrator	3 ms	09/23/2022, 4:03:09	09/23/2022, 4:03:09	vcenter.sddc-54-188-6-128.vmwarevmc.com
Refresh virtual machine s...	HCX_Photon_11	Completed		VMC.LOCAL\Administrator	4 ms	09/23/2022, 4:03:09	09/23/2022, 4:03:09	vcenter.sddc-54-188-6-128.vmwarevmc.com
Resync virtual machine	HCX_Photon_11	Completed	Migrating Virtual Machine ac...	VMC.LOCAL\Administrator	4 ms	09/23/2022, 4:00:55	09/23/2022, 4:01:02 PM	vcenter.sddc-54-188-6-128.vmwarevmc.com
Create virtual machine	SDCC-Datacenter	Completed		VMC.LOCAL\Administrator	3 ms	09/23/2022, 3:59:47	09/23/2022, 3:59:47	vcenter.sddc-54-188-6-128.vmwarevmc.com
Refresh host storage ops	172.30.40.128	Completed		VMC.LOCAL\Administrator	4 ms	09/23/2022, 3:59:17 P.	09/23/2022, 3:59:17 P.	vcenter.sddc-54-188-6-128.vmwarevmc.com

如需HCX移轉選項的其他資訊、以及如何使用HCX將工作負載從內部部署移轉至AWS上的VMware Cloud、請參閱 ["VMware HCX使用者指南"](#)。



VMware HCX VMotion需要100Mbps或更高的處理量能力。



目標VMC FSX for ONTAP VMware資料存放區必須有足夠的空間來容納移轉作業。

結論

無論您是針對全雲端或混合雲、或是內部部署中任何類型/廠商儲存設備上的資料、Amazon FSx for NetApp ONTAP 支援HCX都能提供絕佳的選項來部署和移轉工作負載、同時將資料需求無縫接軌至應用程式層、進而降低TCO。無論使用案例為何、請選擇VMC搭配使用FSXfor ONTAP VMware資料存放區、以快速實現雲端效益、一致的基礎架構、以及跨內部部署和多個雲端的作業、工作負載的雙向可攜性、以及企業級容量和效能。使用VMware vSphere複寫、VMware vMotion或甚至是NFC-複本來連接儲存設備及移轉VM的程序與程序、都是相當熟悉的程序。

重點摘要

本文件的重點包括：

- 現在您可以將Amazon FSx ONTAP 支援資料存放區與VMC SDDC搭配使用。
- 您可以輕鬆地將資料從任何內部部署資料中心移轉至使用FSXfor ONTAP VMware資料存放區執行的VMC
- 您可以輕鬆擴充和縮減FSX- ONTAP 支援資料存放區、以滿足移轉活動期間的容量和效能需求。

何處可找到其他資訊

若要深入瞭解本文所述資訊、請參閱下列網站連結：

- VMware Cloud文件

["https://docs.vmware.com/en/VMware-Cloud-on-AWS/"](https://docs.vmware.com/en/VMware-Cloud-on-AWS/)

- Amazon FSX for NetApp ONTAP 的支援文件

["https://docs.aws.amazon.com/fsx/latest/ONTAPGuide"](https://docs.aws.amazon.com/fsx/latest/ONTAPGuide)

VMware HCX使用者指南

- ["https://docs.vmware.com/en/VMware-HCX/4.4/hcx-user-guide/GUID-BFD7E194-CFE5-4259-B74B-991B26A51758.html"](https://docs.vmware.com/en/VMware-HCX/4.4/hcx-user-guide/GUID-BFD7E194-CFE5-4259-B74B-991B26A51758.html)

區域可用度–VMC的補充NFS資料存放區

深入瞭解AWS、VMC和FSX ONTAP 支援全球區域的相關資訊。



NFS資料存放區可在同時ONTAP 提供兩項服務（VMC和FSX支援）的區域中使用。

AWS / VMC上的補充NFS資料存放區可用度由Amazon定義。首先、您需要判斷VMC和FSxN是否在指定的區域中可用。接下來、您需要判斷該區域是否支援FSxN補充NFS資料存放區。

- 檢查VMC的可用度 ["請按這裡"](#)。
- Amazon定價指南提供FSxN（FSx ONTAP）的可用位置資訊。您可以找到這些資訊 ["請按這裡"](#)。

- VMC的FSxN補充NFS資料存放區即將推出。

在資訊仍在發佈期間、下表將目前對VMC、FSxN和FSxN的支援識別為補充NFS資料存放區。

美洲

* AWS地區*	* VMC可用度*	* FSX ONTAP 不間斷供應*	* NFS資料存放區可用度*
美國東部（北維吉尼亞州）	是的	是的	是的
美國東部（俄亥俄州）	是的	是的	是的
美國西部（北加州）	是的	否	否
美國西部（俄勒岡州）	是的	是的	是的
GovCloud（美國西部）	是的	是的	是的
加拿大（中部）	是的	是的	是的
南美洲（聖保羅）	是的	是的	是的

最後更新日期：2022年6月2日。

EMEA

* AWS地區*	* VMC可用度*	* FSX ONTAP 不間斷供應*	* NFS資料存放區可用度*
歐洲（愛爾蘭）	是的	是的	是的
歐洲（倫敦）	是的	是的	是的
歐洲（法蘭克福）	是的	是的	是的
歐洲（巴黎）	是的	是的	是的
歐洲（米蘭）	是的	是的	是的
歐洲（斯德哥爾摩）	是的	是的	是的

最後更新日期：2022年6月2日。

亞太地區

* AWS地區*	* VMC可用度*	* FSX ONTAP 不間斷供應*	* NFS資料存放區可用度*
亞太地區（悉尼）	是的	是的	是的
亞太地區（東京）	是的	是的	是的
亞太地區（大阪）	是的	否	否
亞太地區（新加坡）	是的	是的	是的
亞太地區（首爾）	是的	是的	是的
亞太地區（Mumbai）	是的	是的	是的
亞太地區（雅加達）	否	否	否
亞太地區（香港）	是的	是的	是的

最後更新日期：2022年9月28日。

版權資訊

Copyright © 2024 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。