



# 保护**AWS/VMC**上的工作负载

## NetApp Solutions

NetApp  
April 12, 2024

# 目录

- 保护AWS/VMC上的工作负载 ..... 1
  - TR-4931：《在Amazon Web Services和Guest Connect上使用VMware Cloud进行灾难恢复》 ..... 1
  - VMware Cloud中的Veeam备份和还原、采用Amazon FSx for ONTAP ..... 69
  - TR-4955：使用适用于ONTAP 和VMC的FSX进行灾难恢复(AWS VMware Cloud) ..... 100
  - 使用Veeam Replication和FSx for ONTAP将灾难恢复到AWS上的VMware Cloud ..... 114

# 保护AWS/VMC上的工作负载

## TR-4931: 《在Amazon Web Services和Guest Connect上使用VMware Cloud进行灾难恢复》

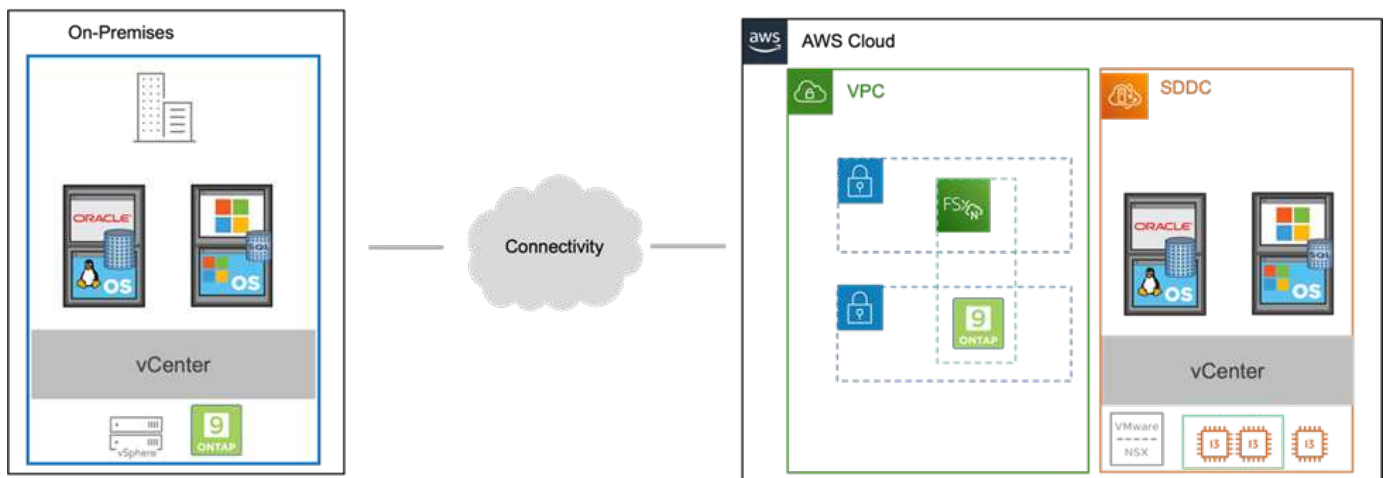
作者: Chris Reno、Josh Powell和Suresh ThopPay—NetApp解决方案工程部

### 概述

对于确保在发生重大中断时快速恢复业务关键型应用程序的企业来说、成熟可靠的灾难恢复(Disaster Recovery、DR)环境和计划至关重要。本解决方案 重点展示灾难恢复使用情形、重点介绍内部部署和AWS上的VMware云中的VMware和NetApp技术。

NetApp与VMware集成的历史很长、成千上万的客户选择NetApp作为其虚拟化环境的存储合作伙伴就证明了这一点。这种集成将继续与云中的子系统连接选项进行、并在近期与NFS数据存储库进行集成。本解决方案 重点介绍通常称为子系统连接存储的使用情形。

在子系统连接的存储中、子系统VMDK部署在VMware配置的数据存储库上、应用程序数据存储在iSCSI或NFS上并直接映射到虚拟机。Oracle和MS SQL应用程序用于演示灾难恢复场景、如下图所示。



### 假设、前提条件和组件概述

在部署此解决方案 之前、请查看组件概述、部署解决方案 所需的前提条件以及在记录此解决方案 时所做的假设。

#### "DR解决方案 要求、要求和规划"

### 使用SnapCenter 执行灾难恢复

在此解决方案 中、SnapCenter 为SQL Server和Oracle应用程序数据提供应用程序一致的快照。此配置与SnapMirror技术相结合、可在内部AFF 和FSX ONTAP 集群之间提供高速数据复制。此外、Veeam Backup & Replication还为我们的虚拟机提供备份和还原功能。

在本节中、我们将介绍用于备份和还原的SnapCenter 、SnapMirror和Veeam的配置。

以下各节介绍了在二级站点完成故障转移所需的配置和步骤：

配置SnapMirror关系和保留计划

SnapCenter 可以更新主存储系统(主存储系统>镜像)和二级存储系统(主存储系统>存储)中的SnapMirror关系、以便进行长期归档和保留。为此、您必须使用SnapMirror在目标卷和源卷之间建立并初始化数据复制关系。

源和目标ONTAP 系统必须位于使用Amazon VPC对等、传输网关、AWS Direct Connect或AWS VPN建立对等关系的网络中。

要在内部ONTAP 系统和FSX ONTAP 之间设置SnapMirror关系、需要执行以下步骤：



请参见 "适用于ONTAP 的FSx—ONTAP 用户指南" 有关使用FSX创建SnapMirror关系的详细信息、请参见。

记录源和目标集群间逻辑接口

对于驻留在内部的源ONTAP 系统、您可以从System Manager或命令行界面检索集群间LIF信息。

- 1. 在ONTAP 系统管理器中、导航到"网络概述"页面、然后检索类型为"集群间"的IP地址、这些IP地址配置为与安装了FSX的AWS VPC进行通信。

Name	Status	Storage VM	IPspace	Address	Current Node	Current Port	Portset	Protocols	Type	Thr
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_vvm_614	✓	ora_vvm	Default	10.61.181.185	E13A300_1	a0a-181		SMB/CIFS, NFS, FL...	Data	0

- 2. 要检索FSX的集群间IP地址、请登录到命令行界面并运行以下命令：

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

```
FsxId0ae40e08acc0dea67::> network interface show -role intercluster
Vserver      Logical      Status      Network      Current      Current      Is
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 和FSX之间建立集群对等关系

要在ONTAP 集群之间建立集群对等关系、必须在另一对等集群中确认在发起ONTAP 集群上输入的唯一密码短语。

1. 使用`cluster peer create`命令在目标FSX集群上设置对等关系。出现提示时、输入一个唯一的密码短语、稍后在源集群上使用该密码短语以完成创建过程。

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

2. 在源集群上、您可以使用ONTAP 系统管理器或命令行界面建立集群对等关系。在ONTAP 系统管理器中、导航到"保护">"概述"、然后选择"对等集群"。

**ONTAP System Manager**

**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

**Peer Cluster**

Generate Passphrase

Manage Cluster Peers

#### Mediator ?

Not configured.

**Configure**

#### Storage VM Peers

PEERED STORAGE VMS

- ✓ 3

3. 在对等集群对话框中、填写所需信息：
  - a. 输入用于在目标FSX集群上建立对等集群关系的密码短语。
  - b. 选择`是`以建立加密关系。

c. 输入目标FSX集群的集群间LIF IP地址。

d. 单击启动集群对等以完成此过程。

### Peer Cluster

Local

STORAGE VM PERMISSIONS

All storage VMs (incl... X

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

Remote

PASSPHRASE ?

.....

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

To generate passphrase,

Intercluster Network Interfaces IP Addresses

172.30.15.42

172.30.14.28

Cancel

+ Add

Initiate Cluster Peering

Cancel

4. 使用以下命令从FSX集群验证集群对等关系的状态：

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

```
FSxId0ae40e08acc0dea67::> cluster peer show
Peer Cluster Name      Cluster Serial Number Availability  Authentication
-----
E13A300                1-80-000011 Available    ok
```

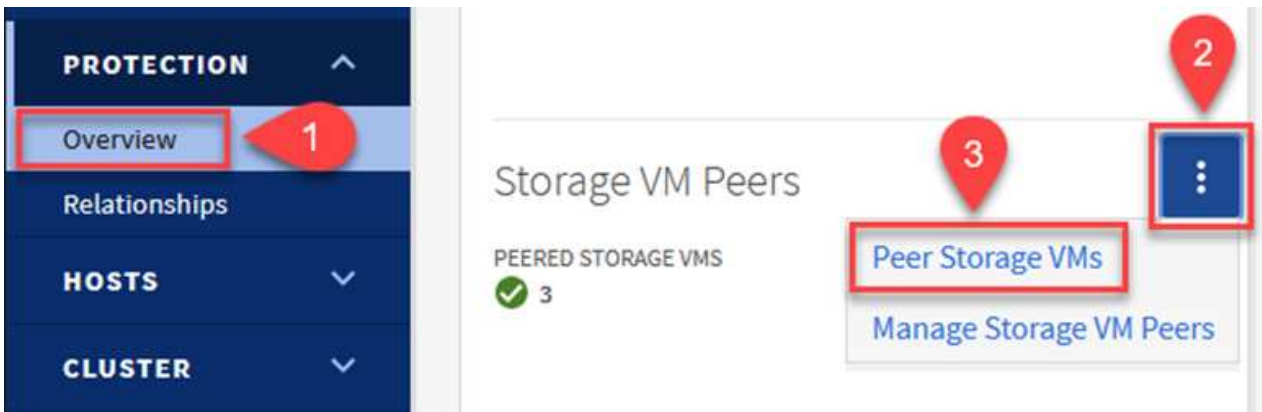
## 建立SVM对等关系

下一步是在目标和源Storage Virtual Machine之间设置SVM关系、这些虚拟机包含将处于SnapMirror关系中的卷。

1. 在源FSX集群中、从CLI使用以下命令创建SVM对等关系：

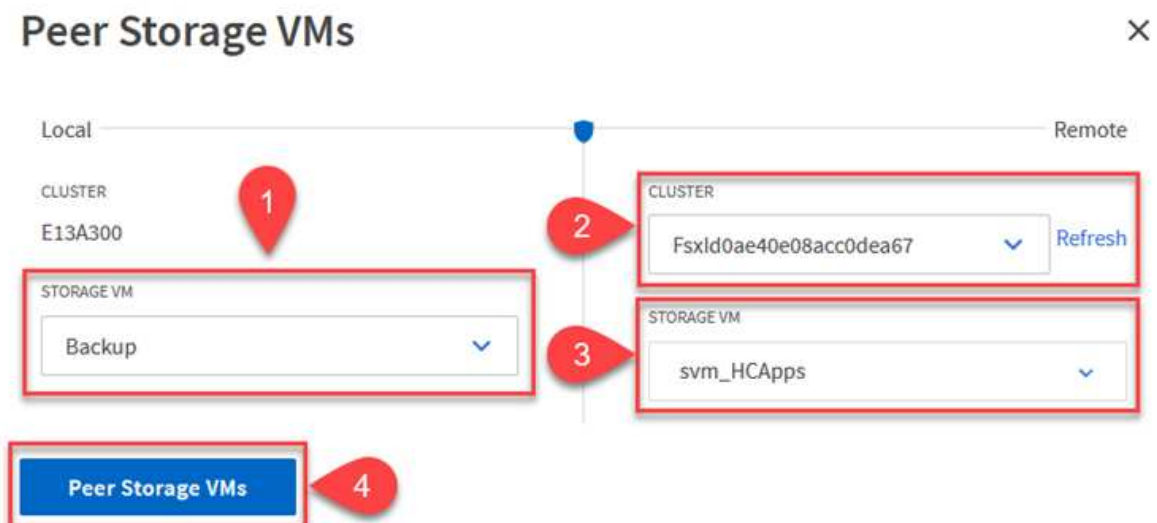
```
FSx-Dest::> vserver peer create -vserver DestSVM -peer-vserver  
Backup -peer-cluster OnPremSourceSVM -applications snapmirror
```

2. 在源ONTAP 集群中、接受与ONTAP 系统管理器或命令行界面的对等关系。
3. 在ONTAP 系统管理器中、转到"保护">"概述"、然后在"Storage VM对等方"下选择"对等Storage VM"。



4. 在对等Storage VM的对话框中、填写必填字段：

- 源Storage VM
- 目标集群
- 目标Storage VM





5. 单击对等Storage VM以完成SVM对等过程。

SnapCenter 管理主存储系统上作为Snapshot副本存在的备份的保留计划。这是在SnapCenter 中创建策略时建立的。SnapCenter 不会管理二级存储系统上保留的备份的保留策略。这些策略通过在二级FSX集群上创建的SnapMirror策略单独管理、并与与源卷具有SnapMirror关系的目标卷相关联。

创建SnapCenter 策略时、您可以选择指定一个二级策略标签、该标签将添加到创建SnapCenter 备份时生成的每个快照的SnapMirror标签中。



在二级存储上、这些标签与与目标卷关联的策略规则匹配、以便强制保留快照。

以下示例显示了一个SnapMirror标签、该标签位于作为SQL Server数据库和日志卷每日备份策略一部分生成的所有快照上。

#### 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 ⓘ

有关为SQL Server数据库创建SnapCenter 策略的详细信息、请参见 "[SnapCenter 文档](#)"。

您必须先创建一个SnapMirror策略、其中包含指定要保留的Snapshot副本数量的规则。

1. 在FSX集群上创建SnapMirror策略。

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

2. 向策略添加SnapMirror标签与SnapCenter 策略中指定的二级策略标签匹配的规则。

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

以下脚本提供了可添加到策略中的规则示例：

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



为每个SnapMirror标签以及要保留的快照数量(保留期限)创建其他规则。

## 创建目标卷

要在FSX上创建一个目标卷、使其成为源卷中Snapshot副本的收件人、请在FSX ONTAP 上运行以下命令：

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

## 在源卷和目标卷之间创建SnapMirror关系

要在源卷和目标卷之间创建SnapMirror关系、请在FSX ONTAP 上运行以下命令：

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

## 初始化SnapMirror关系

初始化SnapMirror关系。此过程将启动从源卷生成的新快照、并将其复制到目标卷。

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

## 在内部部署和配置Windows SnapCenter 服务器。

### 在内部部署Windows SnapCenter 服务器

此解决方案 使用NetApp SnapCenter 为SQL Server和Oracle数据库创建应用程序一致的备份。与用于备份虚拟机VMDK的Veeam备份和复制相结合、可为内部和基于云的数据中心提供全面的灾难恢复解决方案。

SnapCenter 软件可从NetApp支持站点获得、并可安装在位于域或工作组中的Microsoft Windows系统上。有关详细的规划指南和安装说明、请参见 ["NetApp文档中心"](#)。

SnapCenter 软件可从获取 ["此链接"](#)。

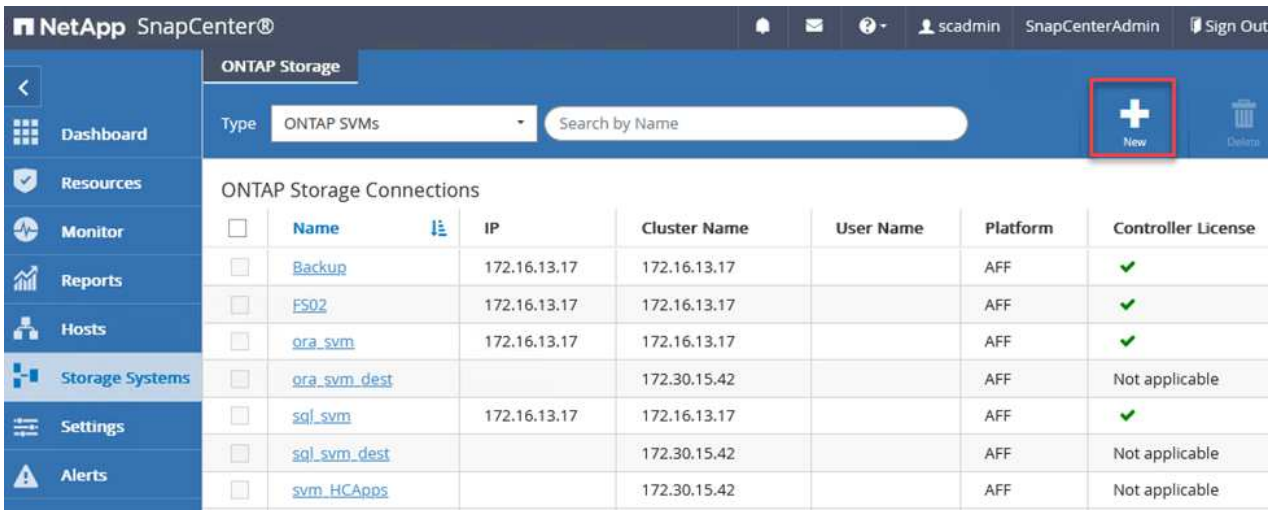
安装后、您可以使用 {https://Virtual\_Cluster\_IP\_or\_FQDN:8146\_} 从Web浏览器访问SnapCenter 控制台。

登录到控制台后、必须为备份SQL Server和Oracle数据库配置SnapCenter。

将存储控制器添加到SnapCenter

要将存储控制器添加到SnapCenter、请完成以下步骤：

- 1. 从左侧菜单中、选择存储系统、然后单击新建开始将存储控制器添加到SnapCenter 的过程。




- 2. 在添加存储系统对话框中、添加本地内部ONTAP 集群的管理IP地址以及用户名和密码。然后单击提交开始发现存储系统。

## 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..

- 重复此过程将FSX ONTAP 系统添加到SnapCenter。在这种情况下、请选择添加存储系统窗口底部的更多选项、然后单击二级复选框、将FSX系统指定为使用SnapMirror副本或主备份快照更新的二级存储系统。

## More Options




Platform FAS

☒ Secondary 

Protocol HTTPS

Port 443

Timeout 60 seconds 

☐ Preferred IP 

Save

Cancel

有关向SnapCenter 添加存储系统的详细信息、请参见中的文档 "[此链接。](#)"。

## 将主机添加到SnapCenter

下一步是将主机应用程序服务器添加到SnapCenter。SQL Server和Oracle的过程都类似。

1. 从左侧菜单中、选择主机、然后单击添加开始向SnapCenter 添加存储控制器的过程。
2. 在添加主机窗口中、添加主机类型、主机名和主机系统凭据。选择插件类型。对于SQL Server、选择Microsoft Windows和Microsoft SQL Server插件。

**NetApp SnapCenter®**

**Managed Hosts**

Search by Name

	Name
<input type="checkbox"/>	<a href="#">oraclesrv_01.sddc.netapp.com</a>
<input type="checkbox"/>	<a href="#">oraclesrv_02.sddc.netapp.com</a>
<input type="checkbox"/>	<a href="#">oraclesrv_03.sddc.netapp.com</a>
<input type="checkbox"/>	<a href="#">oraclesrv_04.sddc.netapp.com</a>
<input type="checkbox"/>	<a href="#">oraclesrv_05.sddc.netapp.com</a>
<input type="checkbox"/>	<a href="#">oraclesrv_06.sddc.netapp.com</a>
<input type="checkbox"/>	<a href="#">oraclesrv_07.sddc.netapp.com</a>
<input type="checkbox"/>	<a href="#">oraclesrv_08.sddc.netapp.com</a>
<input type="checkbox"/>	<a href="#">oraclesrv_09.sddc.netapp.com</a>
<input type="checkbox"/>	<a href="#">oraclesrv_10.sddc.netapp.com</a>

**Add Host**

Host Type:

Host Name:

Credentials:

**Select Plug-ins to Install** SnapCenter Plug-ins Package 4.6 for Windows

- ☒ Microsoft Windows
- ☒ Microsoft SQL Server
- ☐ Microsoft Exchange Server
- ☐ SAP HANA

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

3. 对于Oracle、请在添加主机对话框中填写必填字段、然后选中Oracle数据库插件对应的复选框。然后、单击提交开始发现过程、并将主机添加到SnapCenter。

### Add Host

Host Type Linux ▾

Host Name oraclesrv\_11.sddc.netapp.com

Credentials root ▾



### 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...

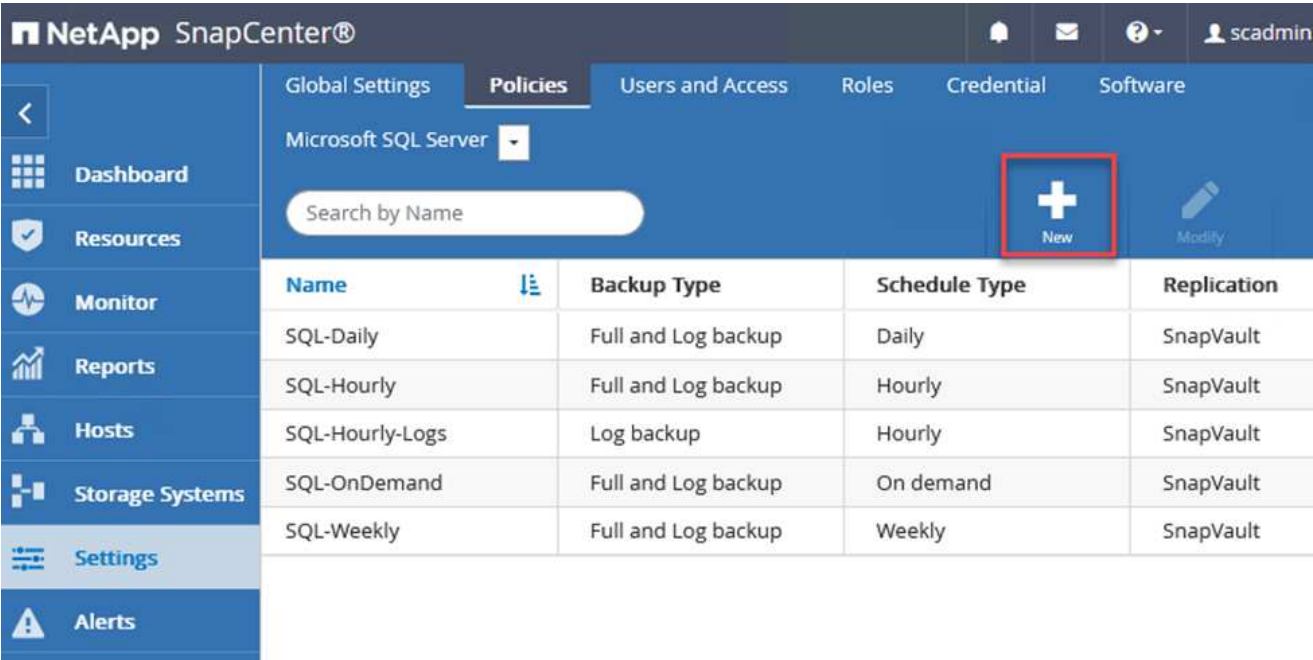
Submit

Cancel



策略用于建立备份作业要遵循的特定规则。它们包括但不限于备份计划、复制类型以及SnapCenter 如何处理备份和截断事务日志。

您可以在SnapCenter Web客户端的"设置"部分访问策略。



有关为SQL Server备份创建策略的完整信息、请参见 ["SnapCenter 文档"](#)。

有关为Oracle备份创建策略的完整信息、请参见 ["SnapCenter 文档"](#)。

- 注： \*
- 在执行策略创建向导期间、请特别注意"复制"部分。在本节中、您将指定要在备份过程中创建的二级SnapMirror副本的类型。
- "创建本地Snapshot副本后更新SnapMirror"设置是指在同一集群中的两个Storage Virtual Machine之间存在SnapMirror关系时更新此关系。
- "创建本地快照副本后更新Snapmirror "设置用于更新两个独立集群之间以及内部ONTAP 系统与Cloud Volumes ONTAP 或FSxN之间的SnapVault 关系。

下图显示了上述选项及其在备份策略向导中的显示方式。

## 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

## 创建SnapCenter 资源组

通过资源组、您可以选择要包含在备份中的数据库资源以及这些资源所遵循的策略。

1. 转到左侧菜单中的"Resources"部分。
2. 在窗口顶部、选择要使用的资源类型(此处为Microsoft SQL Server)、然后单击新建资源组。

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

SnapCenter 文档介绍了为SQL Server和Oracle数据库创建资源组的分步详细信息。

要备份SQL资源、请按照 ["此链接。"](#)。

要备份Oracle资源、请按照 ["此链接。"](#)。

## 部署和配置Veeam Backup Server

解决方案 中使用Veeam Backup & Replication软件来备份我们的应用程序虚拟机、并使用Veeam横向扩展备份存储库(SVBR)将备份副本归档到Amazon S3存储分段。Veeam部署在此解决方案 的Windows服务器上。有关部署Veeam的具体指导、请参见 "[Veeam帮助中心技术文档](#)"。

部署并许可软件后、您可以创建横向扩展备份存储库(SVBR)作为备份作业的目标存储。此外、还应包括一个S3存储分段作为异地VM数据的备份、以便进行灾难恢复。

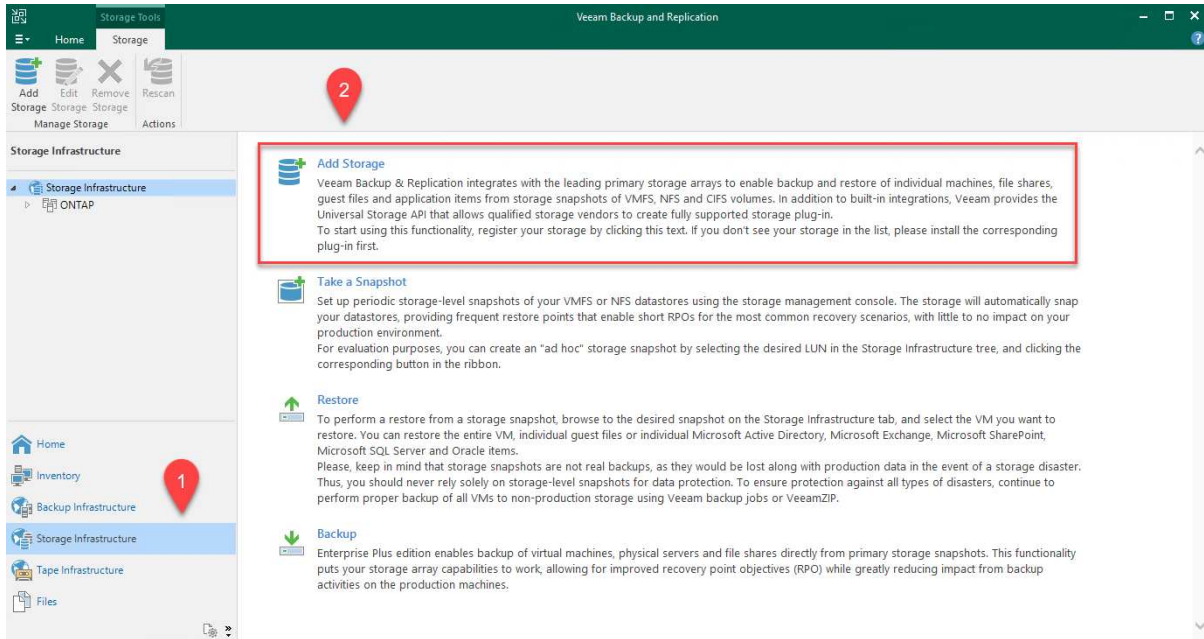
开始使用前、请参见以下前提条件。

1. 在内部ONTAP 系统上创建SMB文件共享、作为备份的目标存储。
2. 创建要包含在SOBR中的Amazon S3存储分段。这是用于异地备份的存储库。

## 将ONTAP 存储添加到Veeam


首先、在Veeam中将ONTAP 存储集群和关联的SMB/NFS文件系统添加为存储基础架构。

1. 打开Veeam控制台并登录。导航到存储基础架构、然后选择添加存储。



2. 在添加存储向导中、选择NetApp作为存储供应商、然后选择Data ONTAP。
3. 输入管理IP地址并选中NAS文件器复选框。单击下一步。

**New NetApp Data ONTAP Storage**×


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

<b>Name</b>	Management server DNS name or IP address: <input type="text" value="10.61.181.180"/>
<b>Credentials</b>	
<b>NAS Filer</b>	Description: <input type="text" value="Created by SDDC\jpowell at 5/17/2022 10:34 AM."/>
<b>Apply</b>	
<b>Summary</b>	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

< Previous Next > Finish Cancel

4. 添加凭据以访问ONTAP 集群。

New NetApp Data ONTAP Storage



**Credentials**  
Specify account with storage administrator privileges.

Name


Credentials

NAS Filer

Apply

Summary

Credentials:

 HCIEUC\Admin (HCIEUC\Admin, last edited: 98 days ago)

▼

Add...

[Manage accounts](#)

Protocol: HTTPS ▼

Port: 443 ▼

< Previous

Next >

Finish

Cancel

5. 在NAS文件管理器页面上、选择要扫描的协议、然后选择下一步。

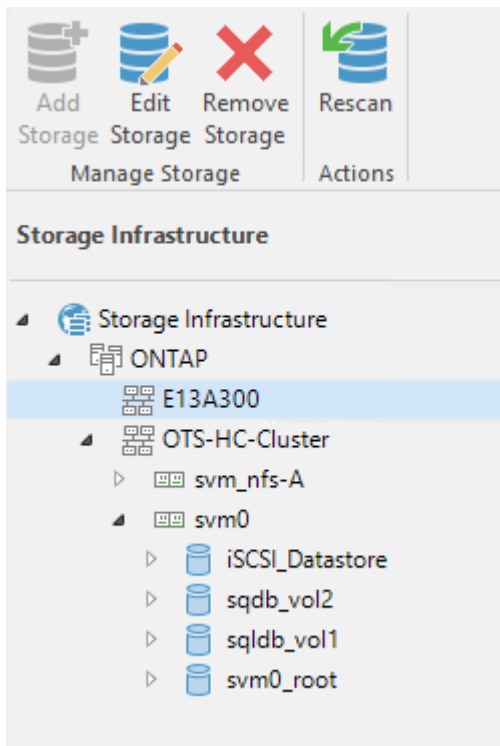
New NetApp Data ONTAP Storage ×

**NAS Filer**

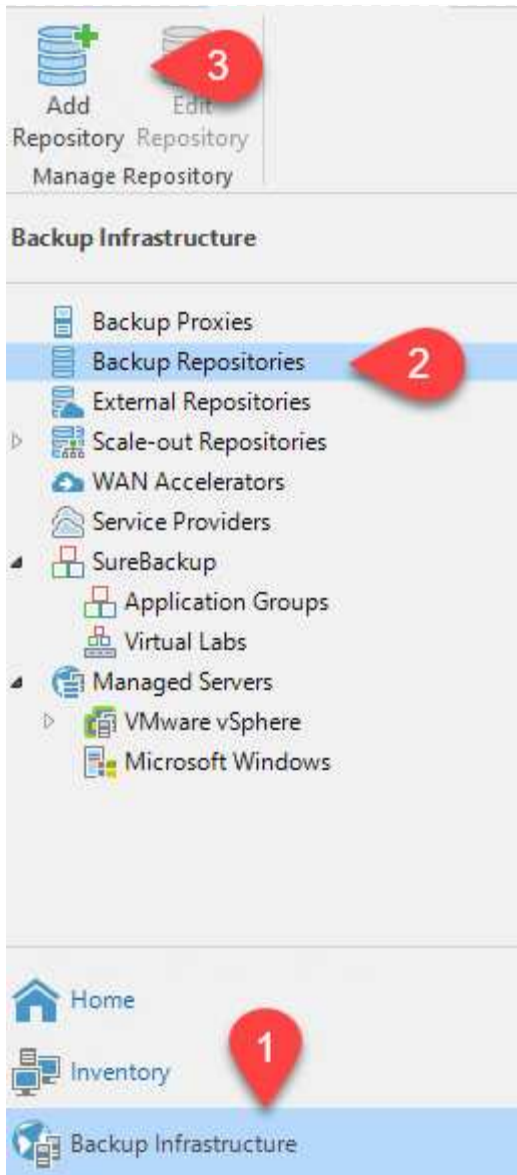
Specify how this storage can be accessed by file backup jobs.

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

6. 完成向导的"Apply"和"Summary"页面、然后单击"Finish"开始存储发现过程。扫描完成后、ONTAP 集群将与NAS存储器一起添加为可用资源。



7. 使用新发现的NAS共享创建备份存储库。从备份基础架构中、选择备份存储库、然后单击添加存储库菜单项。



8. 按照"新建备份存储库向导"中的所有步骤创建存储库。有关创建Veeam备份存储库的详细信息、  
请参见 "[Veeam文档](#)"。



## 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

Share

Repository

Mount Server

Review

Apply

Summary

Shared folder:

Browse...

Use \\server\folder format

☒ This share requires access credentials:

sddc\administrator (sddc\administrator, last edited: 85 days ago)



Add...

[Manage accounts](#)

Gateway server:

☒ Automatic selection☐ The following server:

Use this option to improve performance and reliability of backup to a NAS located in a remote site.

&lt; Previous

Next &gt;

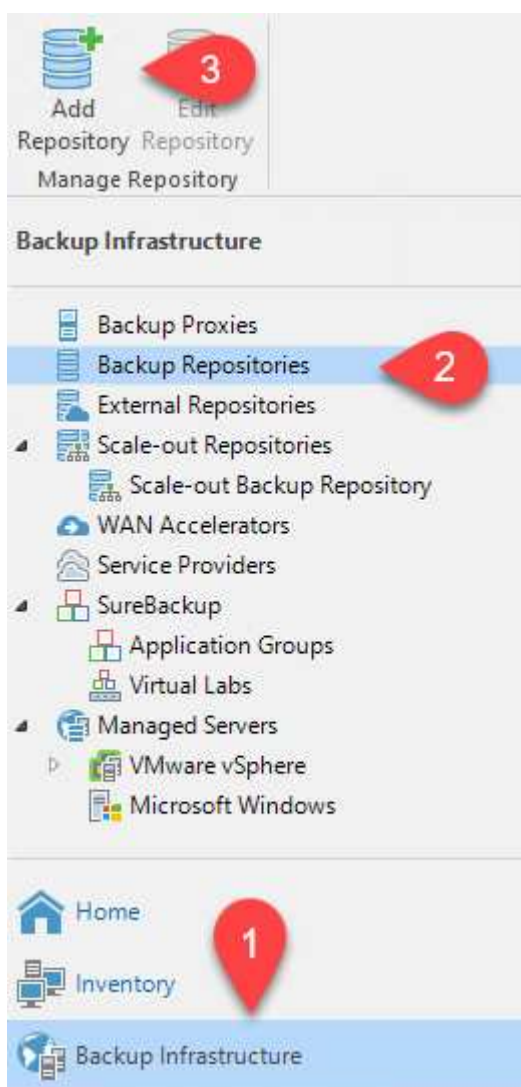
Finish

Cancel

## 将Amazon S3存储分段添加为备份存储库

下一步是将Amazon S3存储添加为备份存储库。

1. 导航到备份基础架构>备份存储库。单击添加存储库。



2. 在添加备份存储库向导中、选择对象存储、然后选择Amazon S3。此时将启动"新建对象存储库"向导。

## 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. 提供对象存储库的名称、然后单击下一步。
4. 在下一节中、提供您的凭据。您需要AWS访问密钥和机密密钥。

## New Object Storage Repository



### Account

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

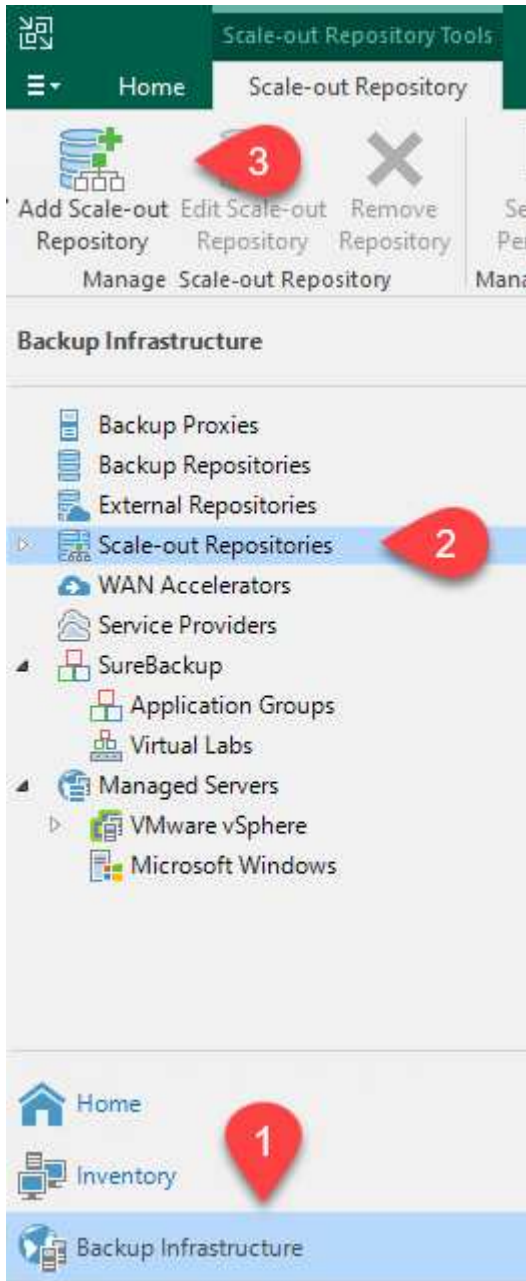
Name	Credentials:
Account	<input type="text" value="AKIAH4H43ZT557HXQT2W (last edited: 107 days ago)"/> <a href="#">Add...</a>
Bucket	<a href="#">Manage cloud accounts</a>
Summary	AWS region:
	<input type="text" value="Global"/>
	<input type="checkbox"/> Use the following gateway server:
	<input type="text" 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=" &lt; Previous"/> <input type="button" value=" Next &gt; "/> <input type="button" value=" Finish "/> <input type="button" value=" Cancel "/>	

5. 加载Amazon配置后、选择您的数据中心、存储分段和文件夹、然后单击应用。最后、单击完成以关闭向导。

## 创建横向扩展备份存储库

现在、我们已将存储库添加到Veeam中、我们可以创建SOBR、以便自动将备份副本分层到异地Amazon S3对象存储以进行灾难恢复。

1. 在备份基础架构中、选择横向扩展存储库、然后单击添加横向扩展存储库菜单项。



2. 在New Scale-Out Backup Repository中、为SOBR提供一个名称、然后单击Next。
3. 对于性能层、选择包含驻留在本地ONTAP 集群上的SMB共享的备份存储库。

## 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	<table border="1"> <thead> <tr> <th>Name</th> </tr> </thead> <tbody> <tr> <td>VBRRepo2</td> </tr> </tbody> </table>	Name	VBRRepo2
Name			
VBRRepo2			
Placement Policy			

- 对于放置策略、根据您的要求选择数据位置或性能。选择"下一步"。
- 对于容量层、我们使用Amazon S3对象存储扩展了SOBR。为了实现灾难恢复、请在创建备份后立即选择将其复制到对象存储、以确保及时交付我们的二级备份。

## 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
Performance Tier
Placement Policy
Capacity Tier
Archive Tier
Summary

☒ Extend scale-out backup repository capacity with object storage:
 

☒ 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.

☒ 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.

Move backup files older than  days (your operational restore window)

☐ Encrypt data uploaded to object storage  
 Password: 


Manage passwords

- 最后、选择应用并完成以完成创建SOBR。

## 创建横向扩展备份存储库作业

配置Veeam的最后一步是使用新创建的SOBR作为备份目标来创建备份作业。创建备份作业是任何存储管理员任务的正常组成部分、我们不会介绍此处的详细步骤。有关在Veeam中创建备份作业的信息、请参见 ["Veeam帮助中心技术文档"](#)。

## BlueXP备份和恢复工具及配置

要将应用程序VM和数据库卷故障转移到AWS中运行的VMware云卷服务、您必须安装并配置SnapCenter 服务器和Veeam备份和复制服务器的正在运行的实例。故障转移完成后、您还必须配置这些工具以恢复正常备份操作、直到计划并执行到内部数据中心的故障恢复为止。

### 部署二级Windows SnapCenter 服务器

SnapCenter 服务器部署在VMware云SDDC中或安装在VPC中的EC2实例上、并通过网络连接到VMware云环境。

SnapCenter 软件可从NetApp支持站点获得、并可安装在位于域或工作组中的Microsoft Windows系统上。有关详细的规划指南和安装说明、请参见 "[NetApp文档中心](#)"。

您可以在以下位置找到SnapCenter 软件： "[此链接](#)"。

### 配置二级Windows SnapCenter 服务器

要还原镜像到FSX ONTAP 的应用程序数据、您必须先完全还原内部SnapCenter 数据库。此过程完成后、将重新建立与VM的通信、现在可以使用FSX ONTAP 作为主存储来恢复应用程序备份。

为此、您必须在SnapCenter 服务器上完成以下各项：

1. 将计算机名称配置为与原始内部SnapCenter 服务器相同。
2. 配置网络以与VMware Cloud和FSX ONTAP 实例进行通信。
3. 完成操作步骤 以还原SnapCenter 数据库。
4. 确认SnapCenter 处于灾难恢复模式、以确保FSX现在成为备份的主存储。
5. 确认已与还原的虚拟机重新建立通信。

有关完成这些步骤的详细信息、请参见第节的 "[SnapCenter 数据库还原过程](#)"。

### 部署二级Veeam Backup & Replication 复制服务器

您可以在AWS上的VMware Cloud中的Windows服务器或EC2实例上安装Veeam Backup & Replication服务器。有关详细的实施指导、请参见 "[Veeam帮助中心技术文档](#)"。

## 配置二级Veeam Backup & amp; 复制服务器

要还原已备份到Amazon S3存储的虚拟机、您必须在Windows服务器上安装Veeam服务器、并将其配置为与VMware Cloud、FSX ONTAP 和包含原始备份存储库的S3存储分段进行通信。此外、还必须在FSX ONTAP 上配置一个新的备份存储库、以便在虚拟机还原后对其执行新备份。

要执行此过程、必须完成以下各项：

1. 配置网络以与VMware Cloud、FSX ONTAP 和包含原始备份存储库的S3存储分段进行通信。
2. 将FSX ONTAP 上的SMB共享配置为新的备份存储库。
3. 在内部挂载用作横向扩展备份存储库一部分的原始S3存储分段。
4. 还原VM后、建立新的备份作业以保护SQL和Oracle VM。

有关使用Veeam还原VM的详细信息、请参见一节 ["使用Veeam Full Restore还原应用程序VM"](#)。

## 用于灾难恢复的SnapCenter 数据库备份

SnapCenter 允许备份和恢复其底层MySQL数据库和配置数据、以便在发生灾难时恢复SnapCenter 服务器。对于解决方案、我们在VPC中的AWS EC2实例上恢复了SnapCenter 数据库和配置。有关此步骤的详细信息、请参见 ["此链接"](#)。

### SnapCenter 备份前提条件

SnapCenter 备份需要满足以下前提条件：

- 在内部ONTAP 系统上创建的卷和SMB共享、用于查找备份的数据库和配置文件。
- 内部ONTAP 系统与AWS帐户中的FSX或CVO之间的SnapMirror关系。此关系用于传输包含备份的SnapCenter 数据库和配置文件的快照。
- Windows Server安装在云帐户中、可以安装在EC2实例上、也可以安装在VMware Cloud SDDC中的VM上。
- SnapCenter 安装在VMware Cloud中的Windows EC2实例或VM上。

## SnapCenter 备份和还原过程摘要

- 在内部ONTAP 系统上创建一个卷、用于托管备份数据库和配置文件。
- 在内部部署和FSX/CVO之间设置SnapMirror关系。
- 挂载SMB共享。
- 检索用于执行API任务的Swagger授权令牌。
- 启动数据库还原过程。
- 使用xcopy实用程序将数据库和配置文件本地目录复制到SMB共享。
- 在FSX上、创建ONTAP 卷的克隆(通过SnapMirror从内部复制)。
- 将SMB共享从FSX挂载到EC2/VMware Cloud。
- 将还原目录从SMB共享复制到本地目录。
- 从Swagger运行SQL Server还原过程。



SnapCenter 提供了一个Web客户端界面、用于执行REST API命令。有关通过Swagger访问REST API的信息、请参见SnapCenter 文档、网址为 ["此链接。"](#)。

## 登录到Swagger并获取授权令牌

导航到Swagger页面后、您必须检索授权令牌以启动数据库还原过程。

1. 访问SnapCenter Swagger API网页、网址为：`//https://<SnapCenter Server IP>: 8146/swagger/_o`。



### SnapCenter API

[ Base URL: /api ]

<https://snapcenter.sddc.netapp.com:8146/Content/swagger/SnapCenter.yaml>

Manage your SnapCenter Server using the SnapCenter API.

To access the swagger documentation of "SnapCenter Plug-in for VMware vSphere" API's, please use  
`https://{SCV_hostname}:{SCV_host_port}/api/swagger-ui.html`

2. 展开"Auth"部分、然后单击Try it out。

#### Auth

POST	/4.6/auth/login	Service login
<p>The login endpoint exposes the method required to log in to the SnapCenter service. The login method returns a token that is used to authenticate subsequent requests.</p>		
Parameters		<button>Try it out</button>

3. 在用户操作文本区域中、填写SnapCenter 凭据和角色、然后单击执行。

Name	Description
TokenNeverExpires	Token never expires
boolean (query)	<div>false</div>
<b>UserOperationContext</b> * required	User credentials
object (body)	<div> <a href="#">Edit Value</a>   <a href="#">Model</a> </div> <div> <pre>{   "UserOperationContext": {     "User": {       "Name": "localhost\\scadmin",       "Passphrase": "NetApp321",       "Rolename": "SnapCenterAdmin"     }   } }</pre> </div> <div> <div>Cancel</div> </div> <div> <div>Parameter content type</div> <div>application/json</div> </div>

Execute

4. 在下面的响应正文中、您可以看到令牌。执行备份过程时、复制令牌文本以进行身份验证。

200 Response body

```
{
  "PluginName": null,
  "HostId": 0,
  "RoleId": null,
  "JobIds": null
},
{
  "User": {
    "Token": "KlYxOg==tsV6EOtdtAmAYpe8q5SG6wcoGaSjwME6jrNy5CsY63HRQ5LkoZLIESRNAhpGJJ0UUQynEMdgtVGDZnvx+I/ZJZIn5M1NZrj6CLfGTApplGmcagT08bqb5bMTx07EcdRAidzAXUDb3GyLQKtW0GdwKzSeUwKj3uVupnk1E3lslK6PRBv9RS8j0qHQvo4v4RL0hhThwFhV9/23nFeJVP/p1Ev4vrV/zeZVTUHFHUM069XRe5cuW9nwyj4b0I5Y5FN3XDkjq=",
    "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": ""
  }
}
```

Download

接下来、转到Swagger页面上的灾难恢复区域、开始SnapCenter 备份过程。

1. 单击"Disaster Recovery"区域、将其展开。

### Disaster Recovery

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. 展开`/4.6/disasterrecovery/server/backup`部分、然后单击Try it out。

POST

/4.6/disasterrecovery/server/backup

Starts the SnapCenter Server DR backup.

Starts and creates a new SnapCenter Server DR backup.

Parameters

Try it out

3. 在SmDRBackupRequest部分中、添加正确的本地目标路径并选择执行以启动SnapCenter 数据库和配置的备份。



备份过程不允许直接备份到NFS或CIFS文件共享。

Name	Description
<b>Token</b> * required string (header)	User authorization token <div>TUHFHUM069XRe5cuW9nwyj4b0l5Y5FN3XDkjQ==</div>
<b>SmDRBackupRequest</b> * required object (body)	Parameters to take Backup <div>Edit Value   Model</div> <div><pre>{   "TargetPath": "C:\\\\SnapCenter_Backups\\\\" }</pre></div> <div>Cancel</div> <div>Parameter content type application/json</div>

Execute

在启动数据库还原过程时、登录到SnapCenter 以查看日志文件。在"Monitor"部分下、您可以查看SnapCenter 服务器灾难恢复备份的详细信息。

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'

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

36

## 使用XCOPY实用程序将数据库备份文件复制到SMB共享

接下来、您必须将备份从SnapCenter 服务器上的本地驱动器移动到用于SnapMirror将数据复制到AWS中FSX实例上的二级位置的CIFS共享。使用带有保留文件权限的特定选项的xcopy。

以管理员身份打开命令提示符。在命令提示符处、输入以下命令：

```
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
```

## 故障转移

### 主站点发生灾难

对于主内部数据中心发生的灾难、我们的方案包括使用VMware Cloud on AWS故障转移到位于Amazon Web Services基础架构上的二级站点。我们假定虚拟机和内部ONTAP 集群不再可访问。此外、SnapCenter 和Veeam虚拟机将无法再访问、必须在我们的二级站点上进行重建。

本节将介绍基础架构故障转移到云的问题、我们将介绍以下主题：

- SnapCenter 数据库还原。建立新的SnapCenter 服务器后、请还原MySQL数据库和配置文件、并将数据库切换到灾难恢复模式、以使二级FSX存储成为主存储设备。
- 使用Veeam Backup & Replication还原应用程序虚拟机。连接包含VM备份的S3存储、导入备份并将其还原到AWS上的VMware Cloud。
- 使用SnapCenter 还原SQL Server应用程序数据。
- 使用SnapCenter 还原Oracle应用程序数据。

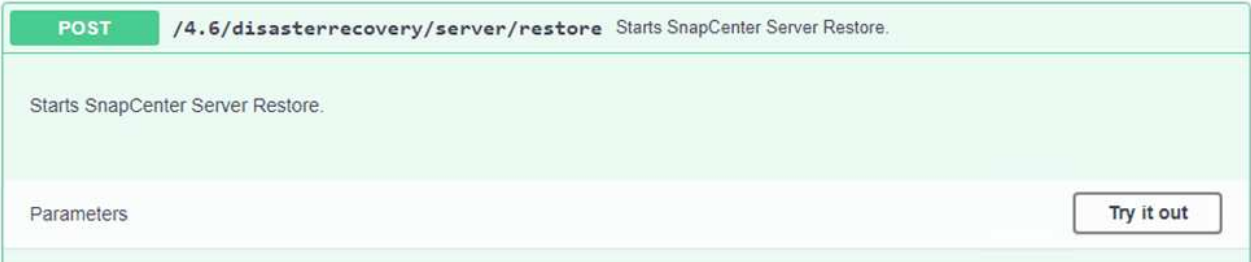
SnapCenter 允许备份和还原其MySQL数据库和配置文件、从而支持灾难恢复场景。这样、管理员便可以在内部数据中心对SnapCenter 数据库进行定期备份、然后将该数据库还原到二级SnapCenter 数据库。

要访问远程SnapCenter 服务器上的SnapCenter 备份文件、请完成以下步骤：

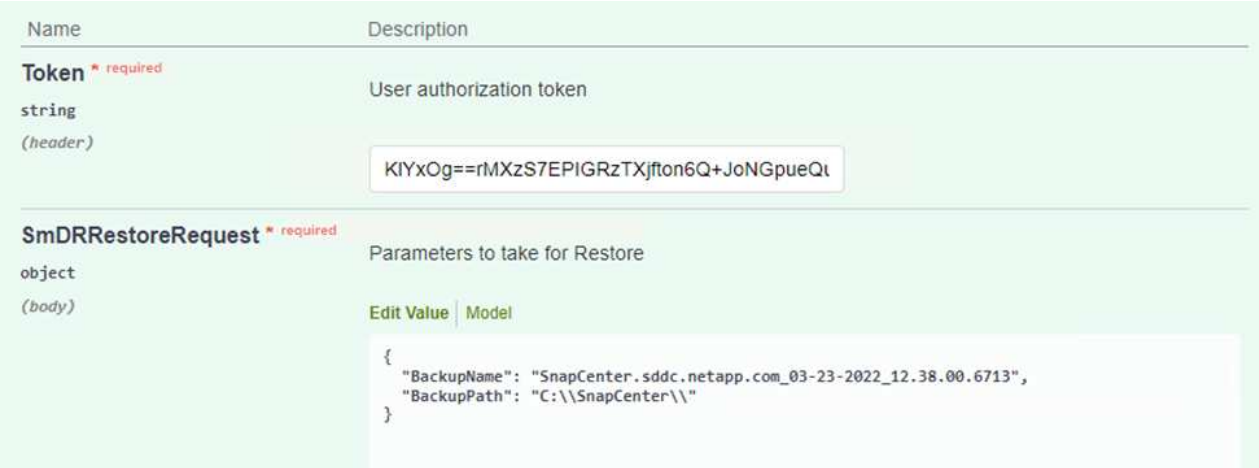
1. 从FSX集群中断SnapMirror关系、从而使卷变为读/写卷。
2. 创建CIFS服务器(如有必要)并创建指向克隆卷的接合路径的CIFS共享。
3. 使用xcopy将备份文件复制到二级SnapCenter 系统上的本地目录。
4. 安装SnapCenter v4.6。
5. 确保SnapCenter 服务器与原始服务器具有相同的FQDN。要成功还原数据库、必须执行此操作。

要启动还原过程、请完成以下步骤：

1. 导航到二级SnapCenter 服务器的Swagger API网页、然后按照前面的说明获取授权令牌。
2. 导航到Swagger页面的Disaster Recovery部分、选择`/4.6/disasterrecovery/server/restore`、然后单击Try it out。



3. 粘贴您的授权令牌、然后在"SmDRResterRequest"部分中、将备份名称和二级SnapCenter 服务器上的本地目录粘贴。




4. 选择执行按钮以启动还原过程。
5. 在SnapCenter 中、导航到Monitor部分以查看还原作业的进度。



**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. 要从二级存储启用SQL Server还原、必须将SnapCenter 数据库切换为灾难恢复模式。此操作将作为单独的操作执行、并在Swagger API网页上启动。
  - a. 导航到Disaster Recovery部分、然后单击`/4.6/disasterrecovery/storage`。
  - b. 粘贴用户授权令牌。
  - c. 在SmSetDisasterRecoverySettingsRequest部分中、将`EnableDisasterRecover`更改为`true`。
  - d. 单击执行为SQL Server启用灾难恢复模式。

Name	Description
<b>Token</b> * required string (header)	User authorization token <div>KIYxOg==rMXzS7EPIGRzTXjfton6Q+JoNGpueQt</div>
<b>SmSetDisasterRecoverySettingsRequest</b> * required object (body)	Parameters to enable or disable the DR mode <div> Edit Value   Model  <pre>{   "EnableDisasterRecovery": true }</pre> </div>



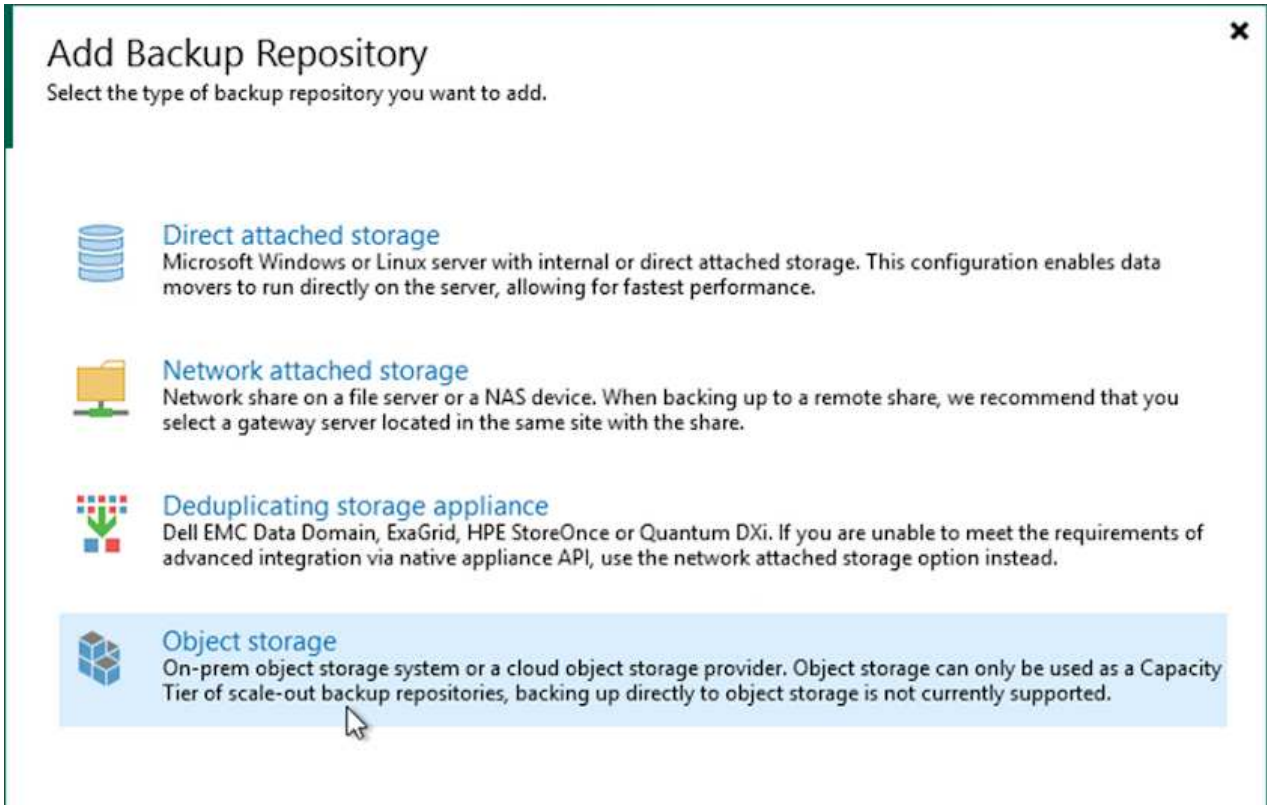
请参见有关其他过程的注释。

使用Veeam完全还原还原应用程序VM


从二级Veeam服务器导入S3存储的备份、并将SQL Server和Oracle VM还原到VMware Cloud集群。

要从内部横向扩展备份存储库中的S3对象导入备份、请完成以下步骤：

1. 转到备份存储库、然后单击顶部菜单中的添加存储库以启动添加备份存储库向导。在向导的第一页上、选择对象存储作为备份存储库类型。




2. 选择Amazon S3作为对象存储类型。




## 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. 从Amazon Cloud Storage Services列表中、选择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. 从下拉列表中选择预先输入的凭据、或者添加用于访问云存储资源的新凭据。单击下一步继续。

New Object Storage Repository ✕

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

Name	Credentials:
Account	 AKIA4H43ZT53YJXPY2Y (last edited: 33 days ago) <span>▼</span> <span>Add...</span>
	<a href="#">Manage cloud accounts</a>
Bucket	AWS region:
Summary	Global <span>▼</span>

☐ Use the following gateway server:


EC2AMAZ-3POTKQV (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.

< Previous Next > Finish Cancel

5. 在存储分段页面上、输入数据中心、存储分段、文件夹以及任何所需选项。单击应用。

New Object Storage Repository

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

Name	Data center: US East (N. Virginia)
Account	
Bucket	Bucket: ehcveeamrepo <span>Browse...</span>
Summary	Folder: RTP <span>Browse...</span>

☐ 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.

☐ Make recent backups immutable for: 30 days  
Protects backups from modification or deletion by ransomware, hackers or malicious insiders using native object storage capabilities.

☐ 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.

☐ Store backups in a single availability zone (even lower price per GB, reduced resilience)

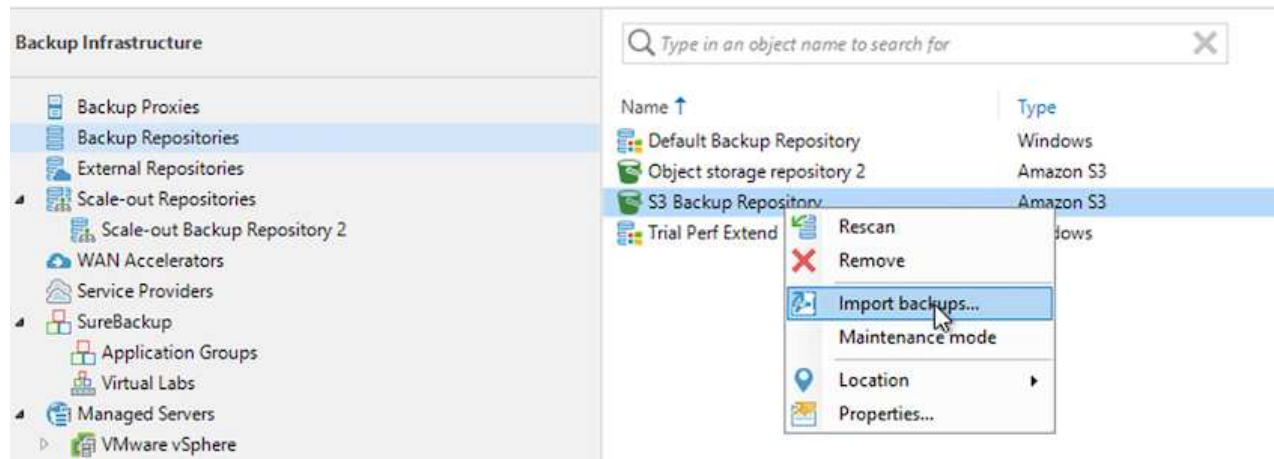
< Previous **Apply** Finish Cancel

6. 最后、选择完成以完成此过程并添加存储库。

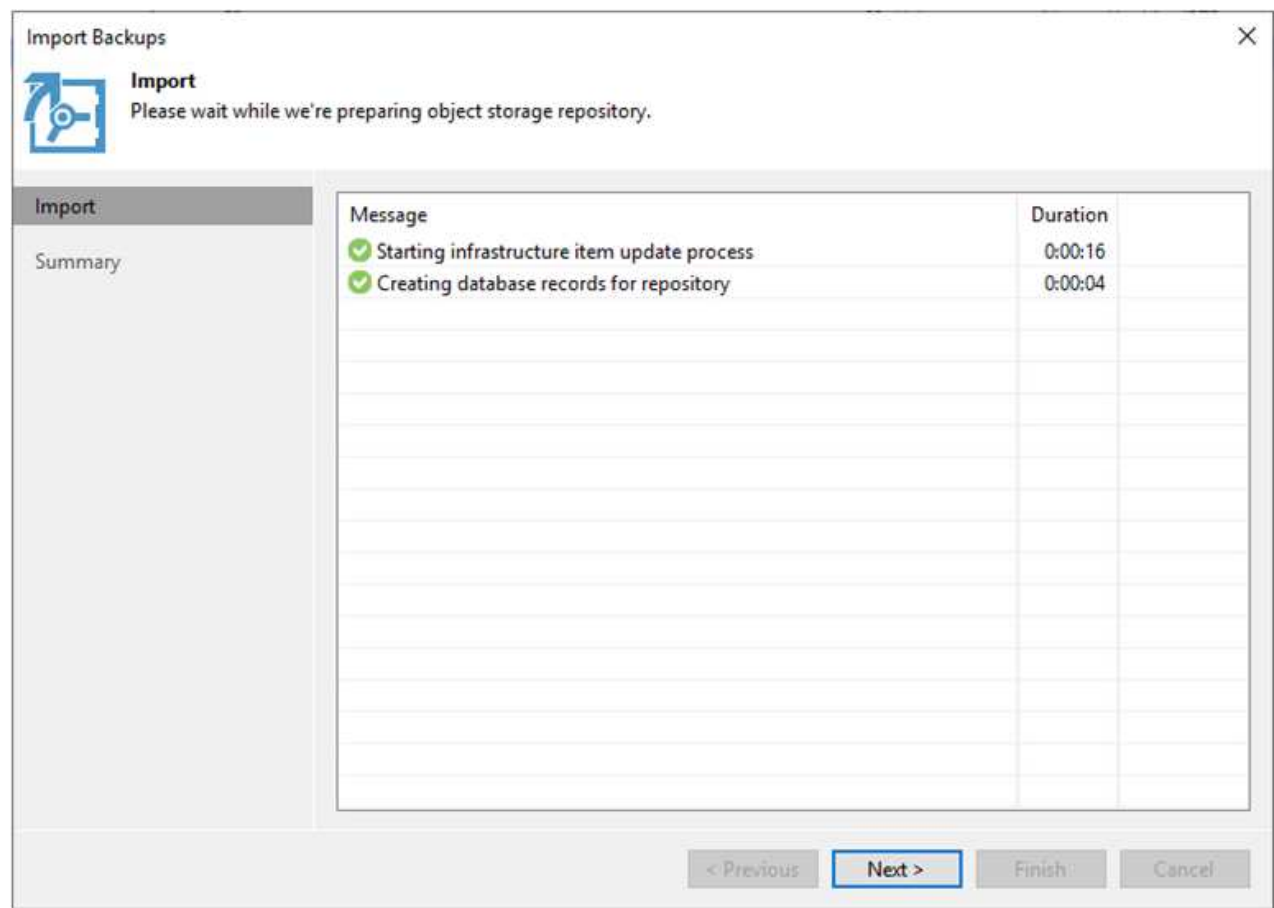
从S3对象存储导入备份

要从上一节中添加的S3存储库导入备份、请完成以下步骤。

1. 在S3备份存储库中、选择导入备份以启动导入备份向导。



2. 为导入创建数据库记录后、在摘要屏幕上选择下一步、然后选择完成以启动导入过程。



3. 导入完成后、您可以将虚拟机还原到VMware Cloud集群中。



## 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	

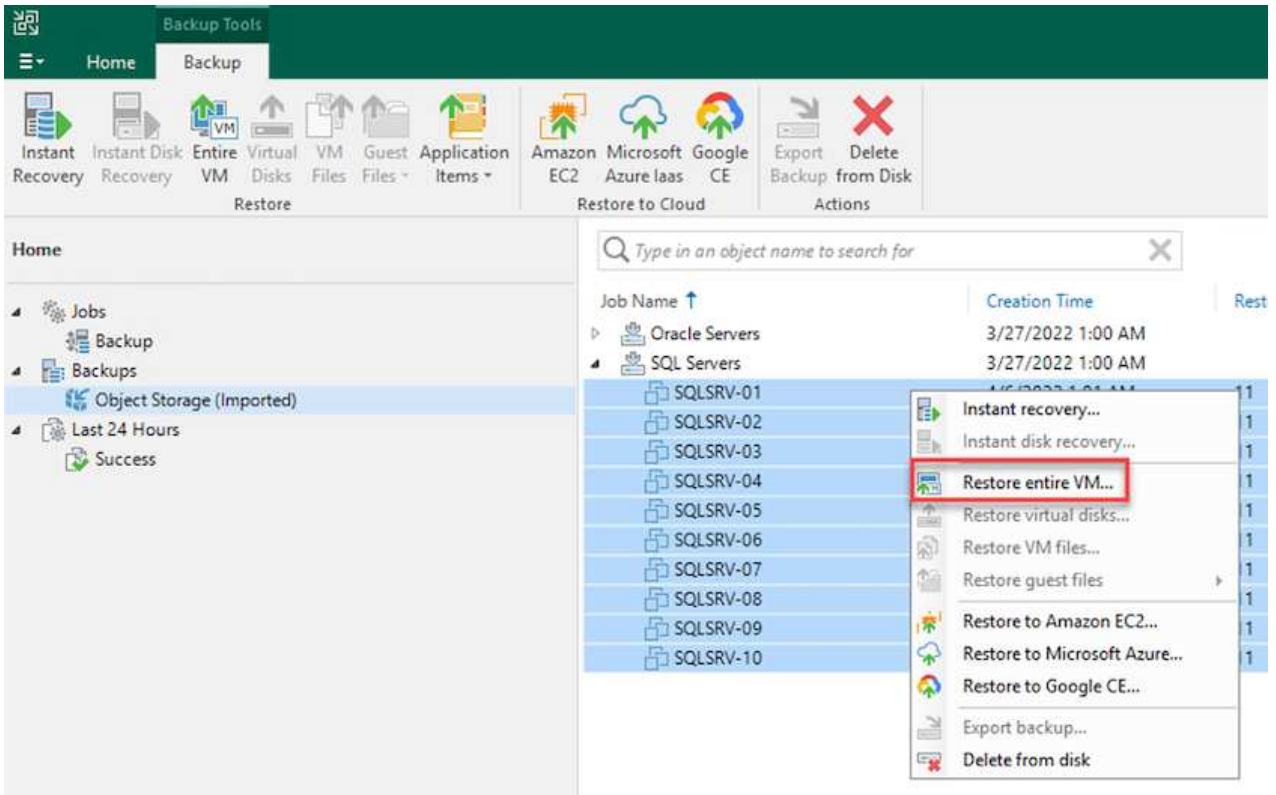
Close



## 通过Veeam完全还原到VMware Cloud来还原应用程序VM

要将SQL和Oracle虚拟机还原到AWS工作负载域/集群上的VMware Cloud、请完成以下步骤。


1. 从Veeam主页页面中、选择包含导入备份的对象存储、选择要还原的VM、然后右键单击并选择还原整个VM。



2. 在完整虚拟机还原向导的第一页上、根据需要修改要备份的虚拟机、然后选择下一步。



Full VM Restore



Restore Mode

Specify whether selected VMs should be restored back to the original location, or to a new location or with different settings.

Virtual Machines

Restore Mode

Host

Resource Pool

Datastore

Folder

Network

Secure Restore

Summary

☐ Restore to the original location

Quickly initiate the restore of selected VM to its original location, with the original name and settings. This option minimizes the chance of user input error.

☒ Restore to a new location, or with different settings

Customize the restored VM location, and change its settings. The wizard will automatically populate all controls with the original VM settings as the defaults.

☐ Staged restore

Run the selected VM directly from backup files in the isolated DataLab to make changes to the guest OS or applications prior to placing the VM into production environment.

[Pick proxy to use](#)

☐ Quick rollback (restore changed blocks only)

Allows for quick VM recovery in case of guest OS software problem, or user error. Do not use this option when recovering from disaster caused by hardware or storage issue, or power loss.

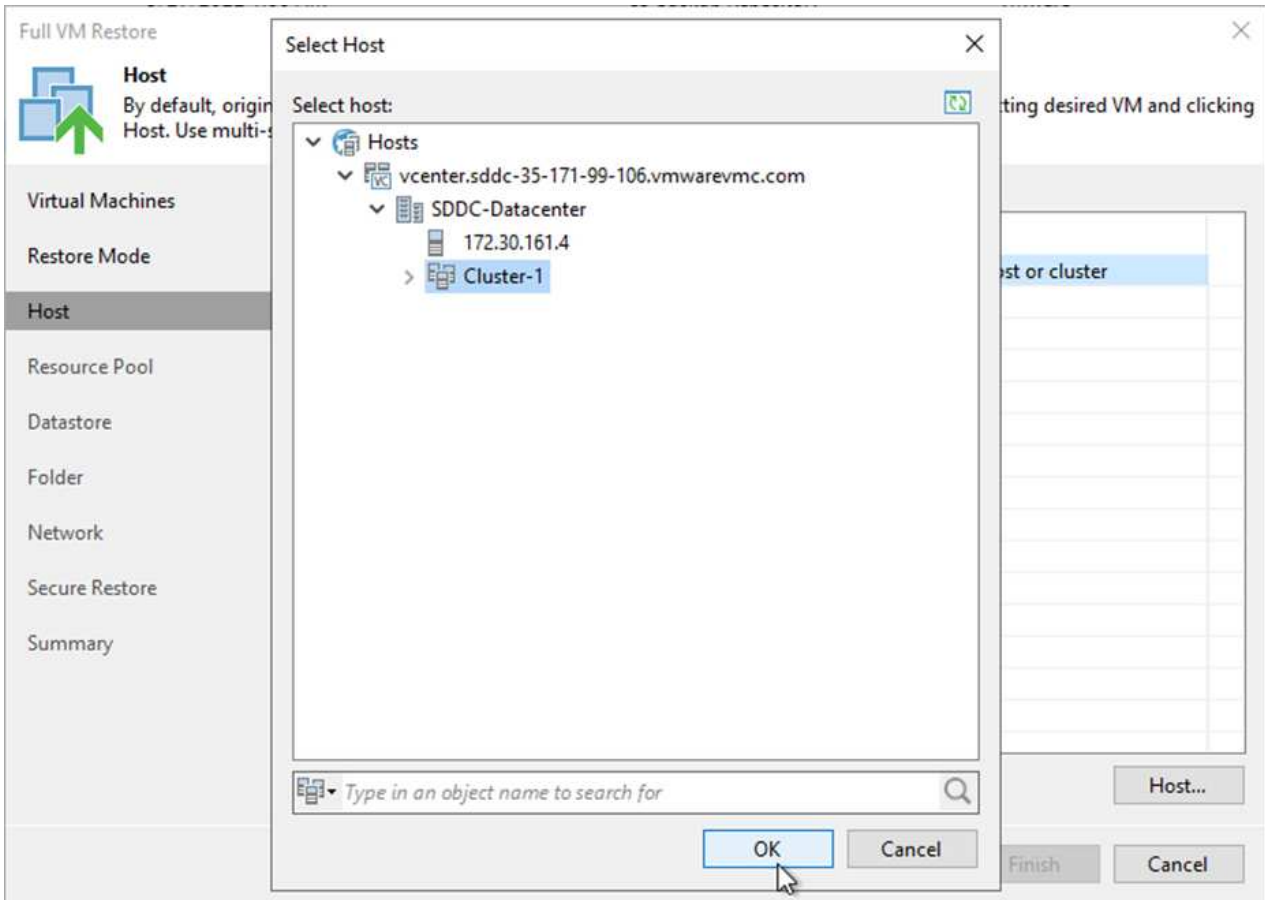
< Previous

Next >

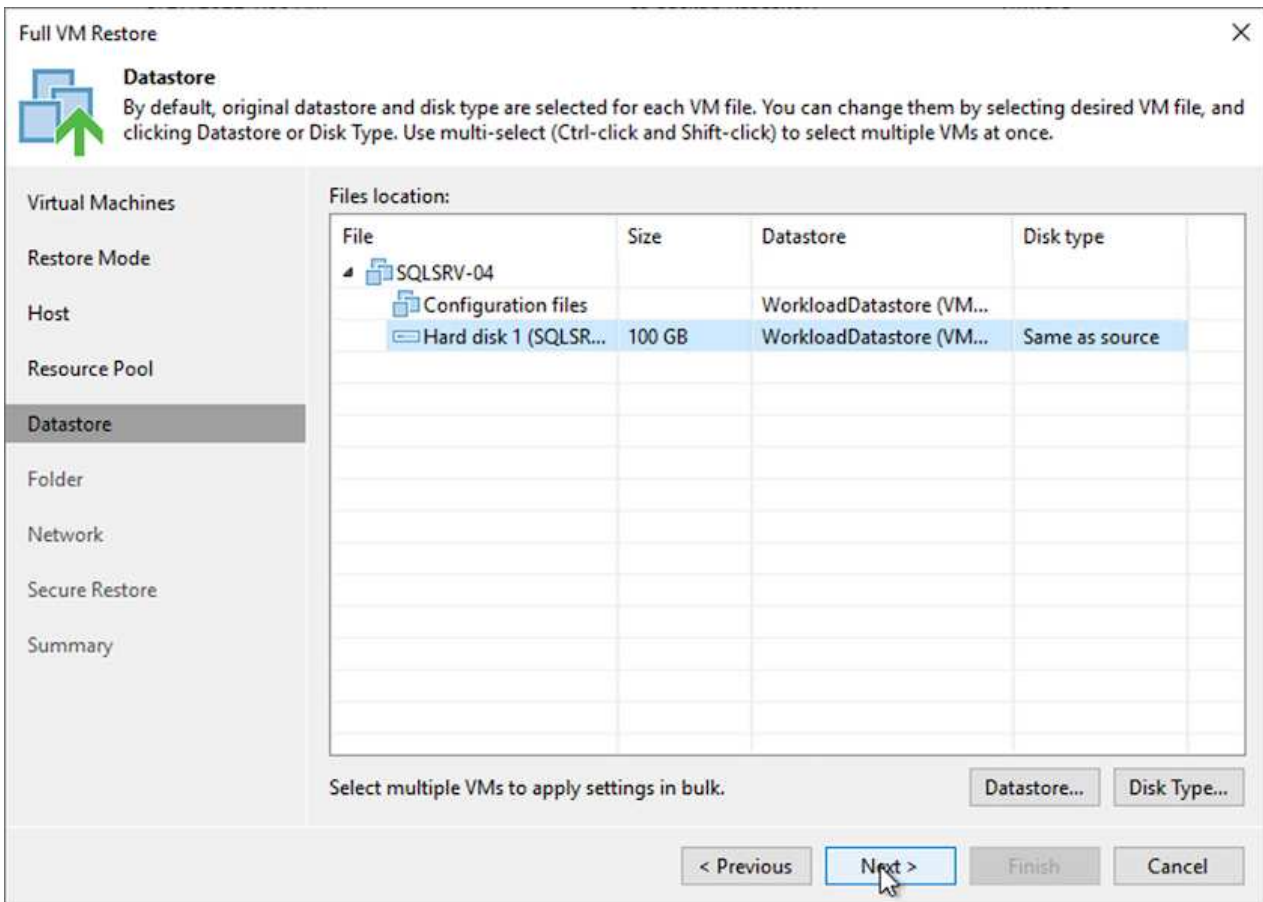
Finish

Cancel

4. 在主机页面上、选择要将虚拟机还原到的目标ESXi主机或集群。

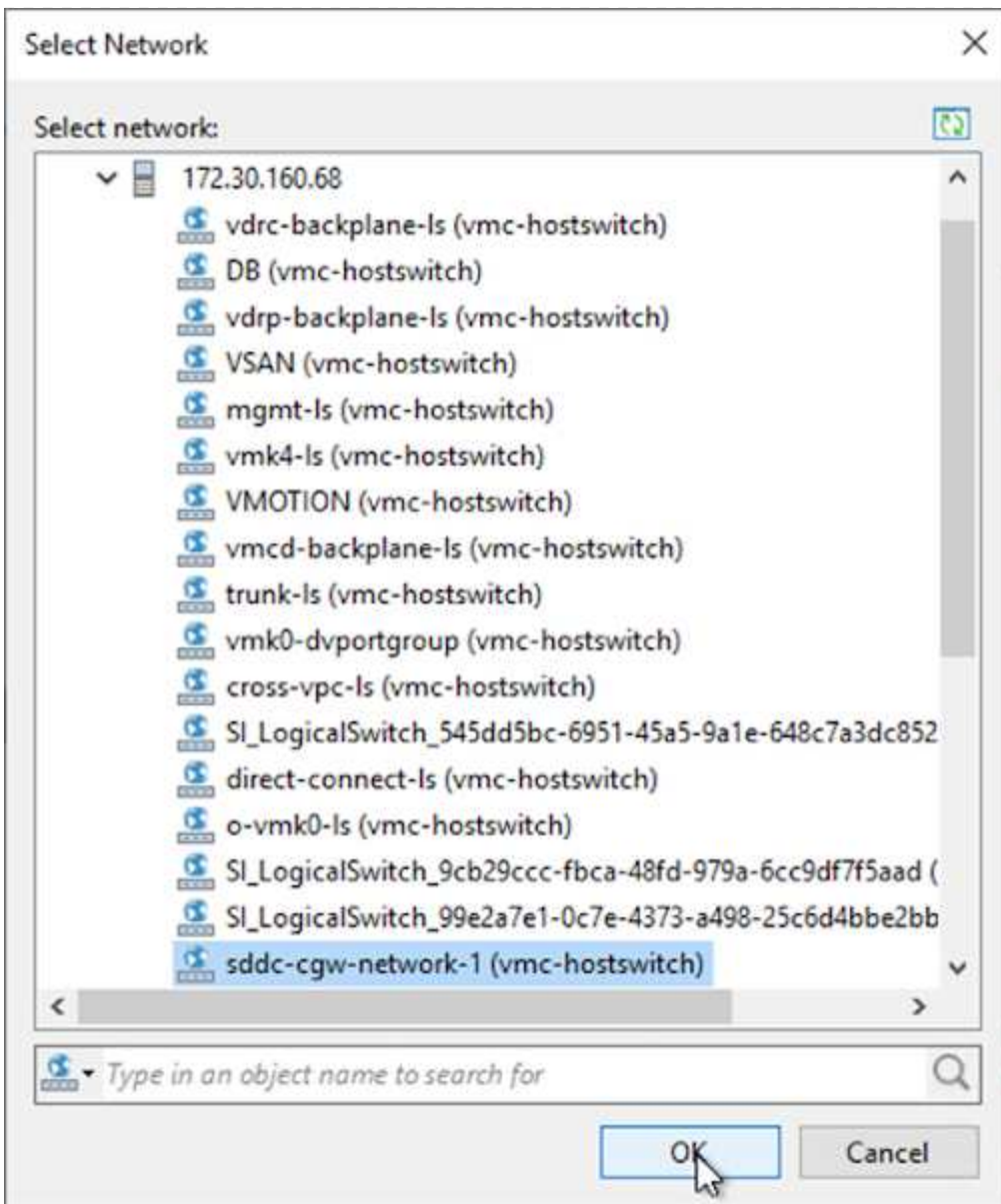


5. 在Datastores页面上、为配置文件和硬盘选择目标数据存储库位置。



6. 在网络页面上、将虚拟机上的原始网络映射到新目标位置中的网络。





7. 选择是否扫描已还原的虚拟机中的恶意软件、查看摘要页面、然后单击完成以开始还原。

## 还原SQL Server应用程序数据

以下过程提供了有关在发生灾难导致内部站点无法运行时如何在AWS的VMware云服务中恢复SQL Server的说明。

假定已完成以下前提条件、才能继续执行恢复步骤：

1. 已使用Veeam Full Restore将Windows Server VM还原到VMware Cloud SDDC。
2. 已建立二级SnapCenter 服务器、并已使用一节中所述的步骤完成SnapCenter 数据库还原和配置 "[SnapCenter 备份和还原过程摘要。](#)"

## VM: SQL Server VM的还原后配置

虚拟机还原完成后、您必须配置网络连接和其他项目、以便在SnapCenter 中重新发现主机虚拟机。

1. 为管理和iSCSI或NFS分配新的IP地址。
2. 将主机加入Windows域。
3. 将主机名添加到DNS或SnapCenter 服务器上的hosts文件中。



如果部署SnapCenter 插件时使用的域凭据与当前域不同、则必须在SQL Server VM上更改适用于Windows服务的插件的登录帐户。更改登录帐户后、重新启动SnapCenter SMCore、适用于Windows的插件和适用于SQL Server的插件服务。



要在SnapCenter 中自动重新发现还原的VM、FQDN必须与最初添加到内部SnapCenter 中的VM相同。

## 为SQL Server还原配置FSX存储

要完成SQL Server VM的灾难恢复还原过程、您必须断开与FSX集群的现有SnapMirror关系并授予对卷的访问权限。为此，请完成以下步骤：

1. 要中断SQL Server数据库和日志卷的现有SnapMirror关系、请从FSX命令行界面运行以下命令：

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

2. 通过创建包含SQL Server Windows VM的iSCSI IQN的启动程序组来授予对LUN的访问权限：

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

3. 最后、将LUN映射到刚刚创建的启动程序组：

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

4. 要查找路径名称、请运行`lun show`命令。



## 设置Windows VM以进行iSCSI访问并发现文件系统

1. 在SQL Server VM中、设置iSCSI网络适配器、以便在VMware端口组上进行通信、该端口组已建立、并可连接到FSX实例上的iSCSI目标接口。
2. 打开iSCSI启动程序属性实用程序、并清除发现、收藏的目标和目标选项卡上的旧连接设置。
3. 找到用于访问FSX实例/集群上的iSCSI逻辑接口的IP地址。您可以在AWS控制台中的Amazon FSx > ONTAP > Storage Virtual Machine下找到此选项。

### Endpoints

Management DNS name

svm-045c077375d3d9799.fs-0ae40e08acc0dea67.fsx.us-east-1.amazonaws.com

NFS DNS name

svm-045c077375d3d9799.fs-0ae40e08acc0dea67.fsx.us-east-1.amazonaws.com

iSCSI DNS name

iscsi.svm-045c077375d3d9799.fs-0ae40e08acc0dea67.fsx.us-east-1.amazonaws.com

Management IP address

198.19.254.53

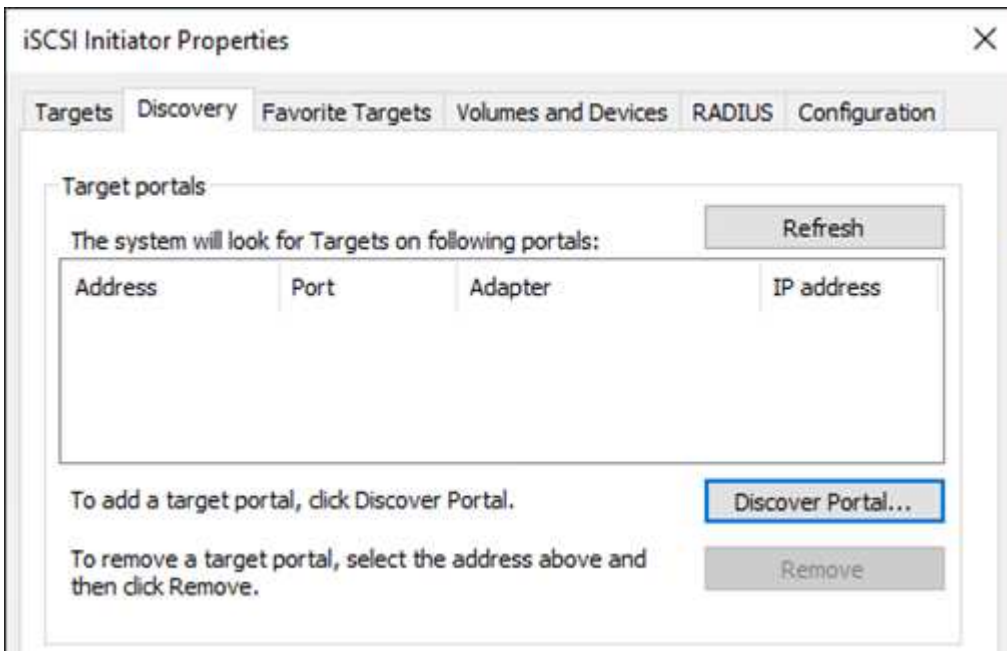
NFS IP address

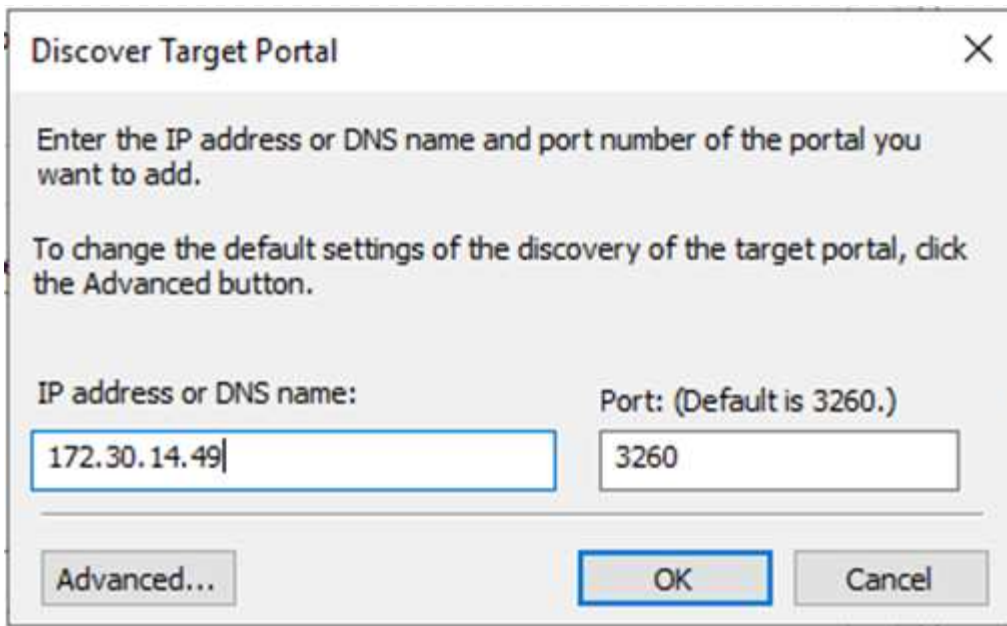
198.19.254.53

iSCSI IP addresses

172.30.15.101, 172.30.14.49

4. 在发现选项卡中、单击发现门户、然后输入FSX iSCSI目标的IP地址。





The image shows a 'Discover Target Portal' dialog box. It has a title bar with a close button (X). The main area contains two paragraphs of text: 'Enter the IP address or DNS name and port number of the portal you want to add.' and 'To change the default settings of the discovery of the target portal, click the Advanced button.' Below the text are two input fields. The first is labeled 'IP address or DNS name:' and contains the text '172.30.14.49'. The second is labeled 'Port: (Default is 3260.)' and contains the text '3260'. At the bottom of the dialog are three buttons: 'Advanced...', 'OK', and 'Cancel'. The 'OK' button is highlighted with a blue border.

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. 在目标选项卡上、单击连接、根据您的配置选择启用多路径、然后单击确定连接到目标。

# iSCSI Initiator Properties

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.5918b03f9ef411ecb007495...	Inactive

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

Connect

## Connect To Target

Target name:

iqn.1992-08.com.netapp:sn.5918b03f9ef411ecb0074956fb75f45c:vs.6

☒ Add this connection to the list of Favorite Targets.

This will make the system automatically attempt to restore the connection every time this computer restarts.

☒ Enable multi-path

Advanced...

OK

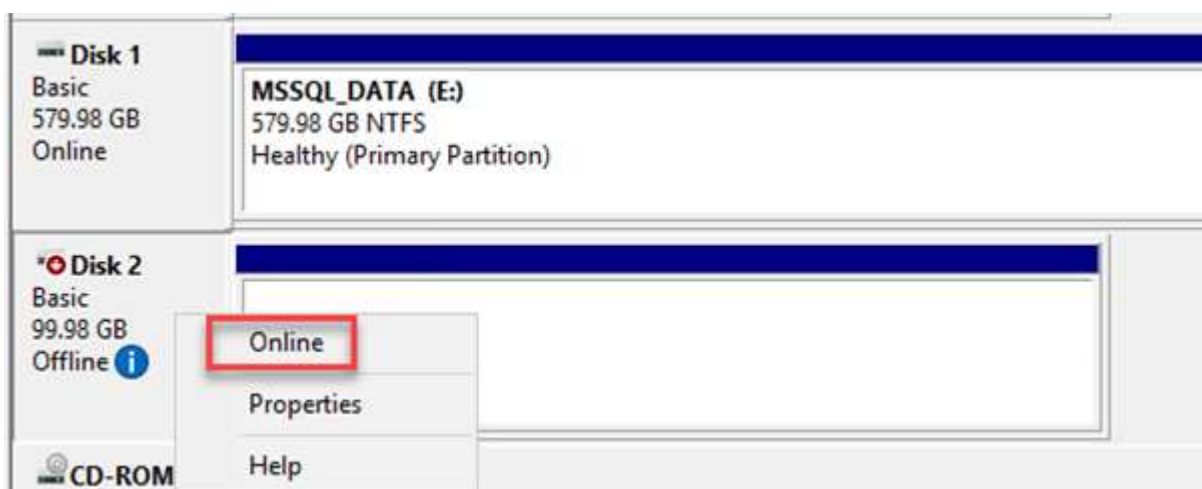
Cancel

OK

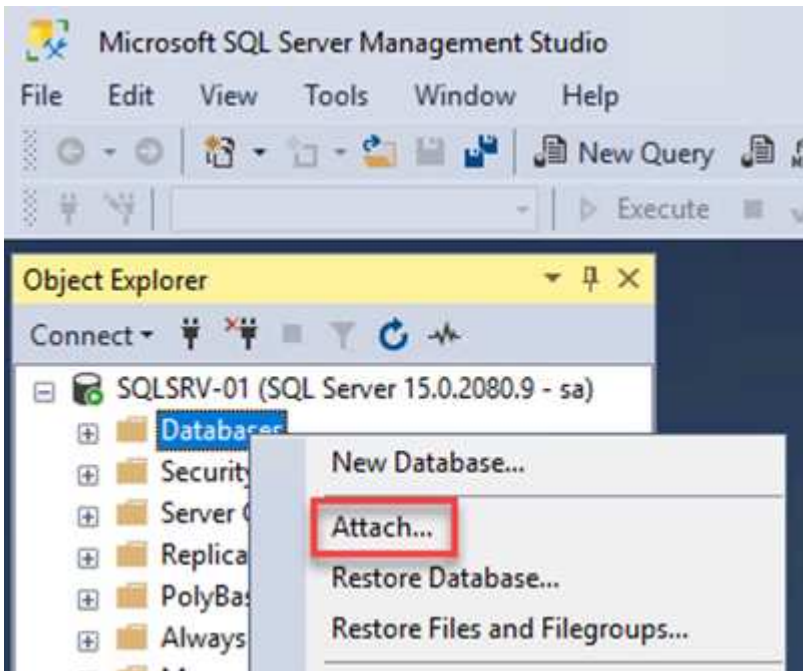
Cancel

Apply

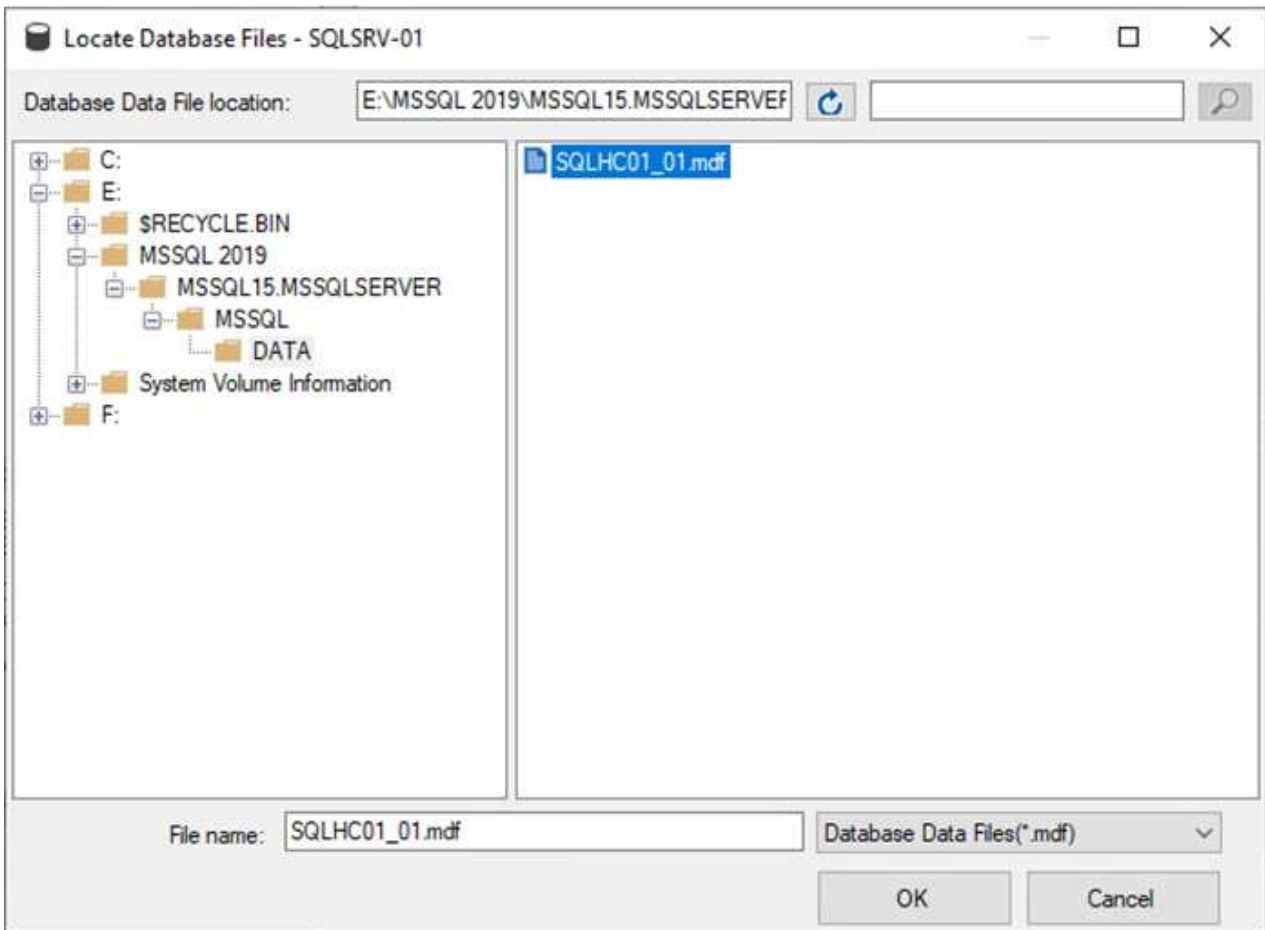
6. 打开计算机管理实用程序并使磁盘联机。确认它们保留的驱动器号与先前相同。



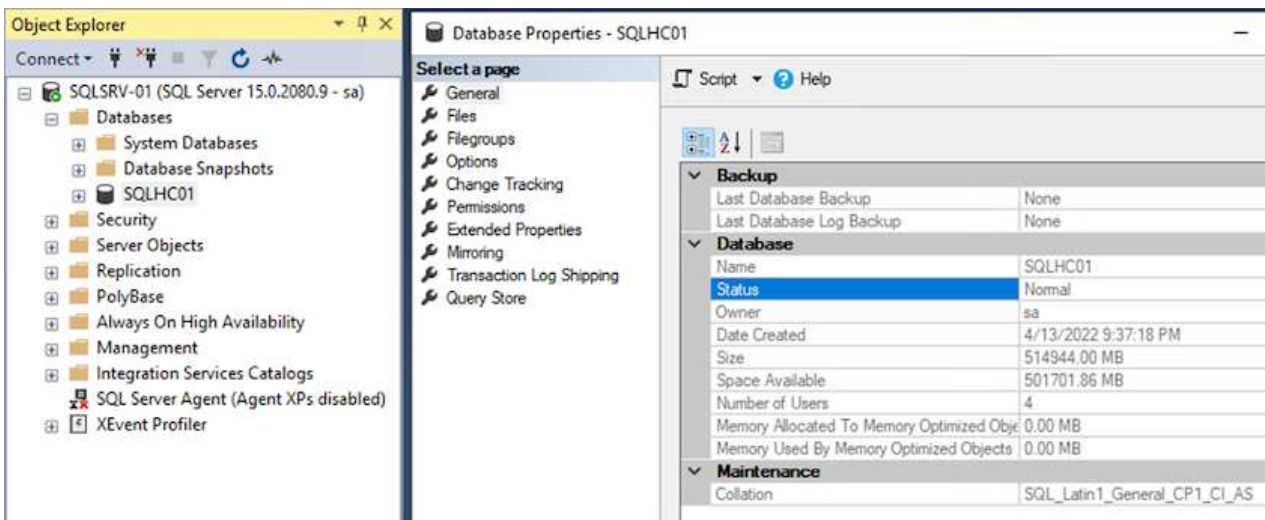
1. 从SQL Server VM中、打开Microsoft SQL Server Management Studio并选择Attach以开始连接到数据库的过程。



2. 单击添加并导航到包含SQL Server主数据库文件的文件夹、将其选中、然后单击确定。



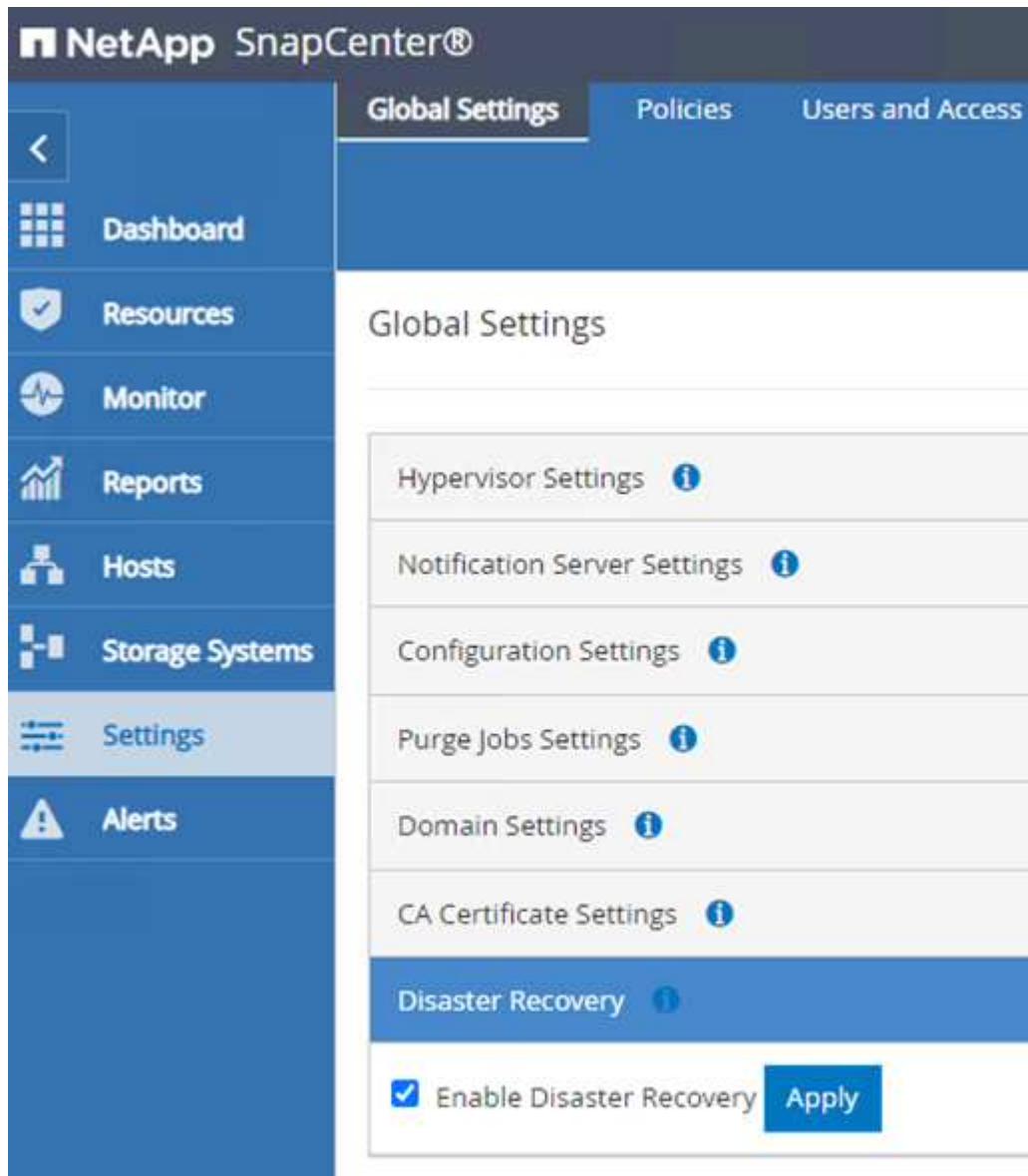
3. 如果事务日志位于单独的驱动器上、请选择包含事务日志的文件夹。
4. 完成后、单击确定以连接数据库。



将SnapCenter 数据库还原到其先前状态后、它会自动重新发现SQL Server主机。要使此操作正常运行、请记住以下前提条件：

- 必须将SnapCenter 置于灾难恢复模式。可以通过Swagger API或Disaster Recovery下的Global Settings实现此目的。
- SQL Server的FQDN必须与内部数据中心中运行的实例相同。
- 必须断开原始SnapMirror关系。
- 必须将包含数据库的LUN挂载到SQL Server实例、并连接数据库。

要确认SnapCenter 处于灾难恢复模式、请在SnapCenter Web客户端中导航到设置。转到全局设置选项卡、然后单击灾难恢复。确保启用"启用灾难恢复"复选框。



## 还原Oracle应用程序数据

以下过程提供了有关在发生灾难导致内部站点无法运行时如何在AWS的VMware云服务中恢复Oracle应用程序数据的说明。

完成以下前提条件以继续执行恢复步骤：

1. Oracle Linux服务器VM已使用Veeam Full Restore还原到VMware Cloud SDDC。
2. 已建立二级SnapCenter 服务器、并已使用本节所述的步骤还原SnapCenter 数据库和配置文件 "[SnapCenter 备份和还原过程摘要](#)。"



要使FSxN实例上托管的二级存储卷可供Oracle服务器访问、必须先中断现有的SnapMirror关系。

1. 登录到FSX命令行界面后、运行以下命令以查看使用正确名称筛选的卷。

```
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. 运行以下命令以中断现有SnapMirror关系。

```
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客户端中的接合路径：

## 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. 添加接合路径名称、然后单击更新。从Oracle服务器挂载NFS卷时、请指定此接合路径。

## 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Cloud Manager中、您可以使用正确的NFS LIF IP地址获取mount命令、以便挂载包含Oracle数据库文件和日志的NFS卷。

1. 在Cloud Manager中、访问FSX集群的卷列表。

FSx

HCApps

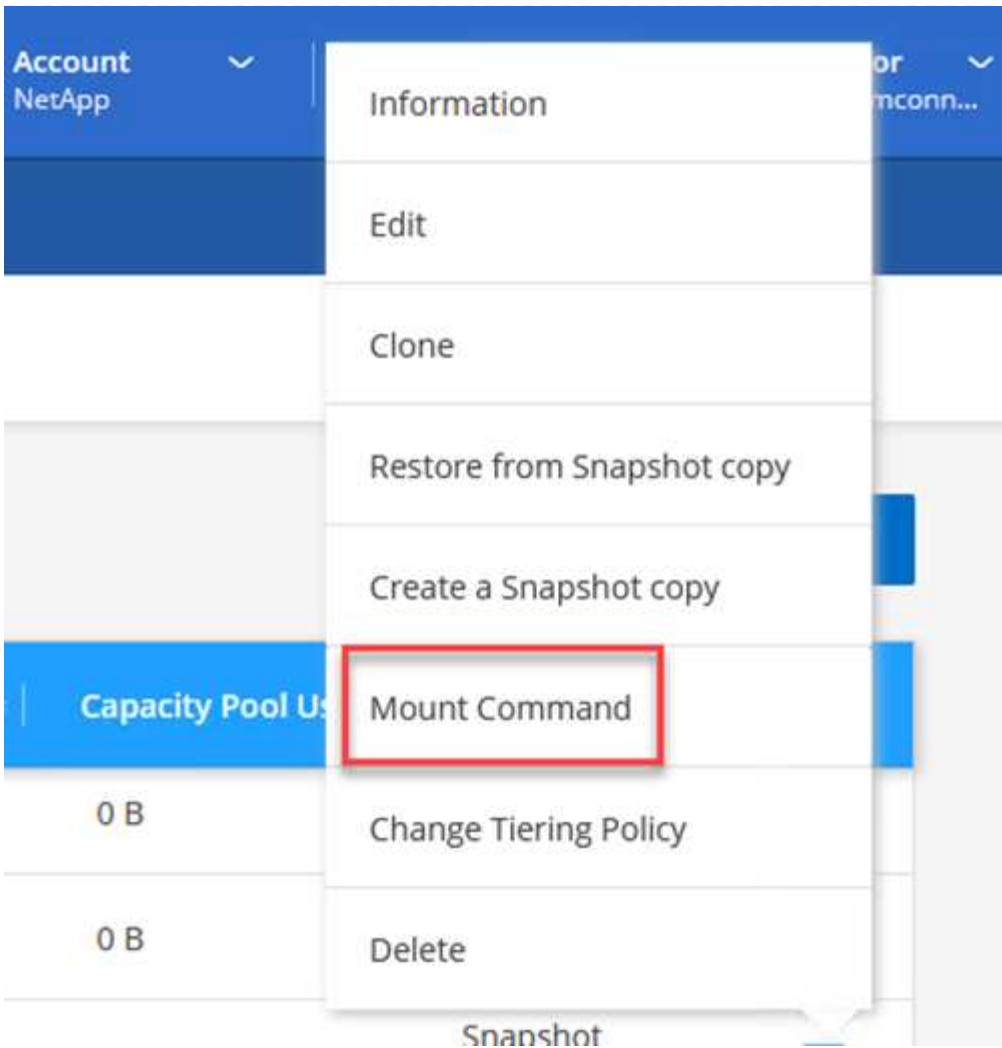
Overview

Volumes

50 volumes

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. 从操作菜单中、选择挂载命令以查看并复制要在Oracle Linux服务器上使用的挂载命令。



### 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. 将NFS文件系统挂载到Oracle Linux Server。Oracle Linux主机上已存在用于挂载NFS共享的目录。
4. 在Oracle Linux服务器上、使用mount命令挂载NFS卷。

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

对与Oracle数据库关联的每个卷重复此步骤。



要在重新启动时使NFS挂载持久、请编辑`/etc/fstab`文件以包含mount命令。

5. 重新启动Oracle服务器。Oracle数据库应正常启动并可供使用。

## 故障恢复

成功完成此解决方案 中所述的故障转移过程后、SnapCenter 和Veeam将恢复在AWS中运行的备份功能、而适用于ONTAP 的FSX现在已指定为主存储、并且与原始内部数据中心没有SnapMirror关系。在内部恢复正常功能后、您可以使用与本文档所述过程相同的过程将数据镜像回内部ONTAP 存储系统。

如本文档中所述、您还可以配置SnapCenter 、以便将应用程序数据卷从适用于ONTAP 的FSx镜像到驻留在内部的ONTAP 存储系统。同样、您也可以将Veeam配置为使用横向扩展备份存储库将备份副本复制到Amazon S3、以便驻留在内部数据中心的Veeam备份服务器可以访问这些备份。

故障恢复不在本文档的讨论范围内、但故障恢复与此处所述的详细过程差别不大。

## 结论

本文档中介绍的使用情形侧重于经过验证的灾难恢复技术、这些技术突出了NetApp与VMware之间的集成。NetApp ONTAP 存储系统提供经验证的数据镜像技术、使企业能够设计涵盖领先云提供商所采用的内部和ONTAP 技术的灾难恢复解决方案。

AWS上的ONTAP FSX就是这样一种解决方案 、它可以与SnapCenter 和SyncMirror 无缝集成、以便将应用程序数据复制到云。Veeam备份和复制是另一项众所周知的技术、可与NetApp ONTAP 存储系统完美集成、并可提供到vSphere原生 存储的故障转移。

此解决方案 使用托管SQL Server和Oracle应用程序数据的ONTAP 系统中的子系统连接存储提供了一个灾难恢复解决方案。采用SnapMirror的SnapCenter 提供了一个易于管理的解决方案、用于保护ONTAP 系统上的应用程序卷、并将其复制到驻留在云中的FSX或CVO。SnapCenter 是一种支持灾难恢复的解决方案、用于将所有应用程序数据故障转移到AWS上的VMware Cloud。

## 从何处查找追加信息

要了解有关本文档中所述信息的更多信息，请查看以下文档和 / 或网站：

- 指向解决方案 文档的链接

["采用VMware解决方案的NetApp混合多云"](#)

["NetApp 解决方案"](#)

# VMware Cloud中的Veeam备份和还原、采用Amazon FSx for ONTAP

作者：Jsh Powell—NetApp解决方案工程部

## 概述

Veeam Backup & Replication是一款高效可靠的解决方案、用于保护VMware Cloud中的数据。此解决方案 演示了使用Veeam备份和复制在VMware Cloud中备份和还原FSx for ONTAP NFS数据存储库上的应用程序VM的正确设置和配置。

VMware Cloud (在AWS中)支持使用NFS数据存储库作为补充存储、而FSx for NetApp ONTAP 是一款安全解决方案、适用于需要为云应用程序存储大量数据的客户、该数据存储库可以独立于SDDC集群中的ESXi主机数量进行扩展。这项集成的AWS存储服务可提供具有所有传统NetApp ONTAP 功能的高效存储。

## 用例

此解决方案 可解决以下使用情形：

- 使用FSx for NetApp ONTAP 作为备份存储库、备份和还原VMC中托管的Windows和Linux虚拟机。
- 使用FSx for NetApp ONTAP 作为备份存储库来备份和还原Microsoft SQL Server应用程序数据。
- 使用FSx for NetApp ONTAP 作为备份存储库来备份和还原Oracle应用程序数据。

## 使用Amazon FSx for ONTAP 的NFS数据存储库

此解决方案 中的所有虚拟机都位于FSx上、用于ONTAP 补充NFS数据存储库。使用FSx for ONTAP 作为补充NFS数据存储库具有若干优势。例如、它允许您：

- 在云中创建可扩展且高度可用的文件系统、而无需复杂的设置和管理。
- 与现有VMware环境集成、支持您使用熟悉的工具和流程来管理云资源。
- 利用ONTAP 提供的高级数据管理功能(例如快照和复制)保护数据并确保其可用性。

## 解决方案 部署概述

此列表简要介绍了配置Veeam备份和复制、使用FSx for ONTAP 作为备份存储库执行备份和还原作业以及还原SQL Server和Oracle VM和数据库所需的步骤：

1. 创建FSx for ONTAP 文件系统、用作Veeam Backup & Replication的iSCSI备份存储库。
2. 部署Veeam代理以分布备份工作负载并挂载FSx for ONTAP 上托管的iSCSI备份存储库。
3. 配置Veeam备份作业以备份SQL Server、Oracle、Linux和Windows虚拟机。
4. 还原SQL Server虚拟机和各个数据库。
5. 还原Oracle虚拟机和各个数据库。

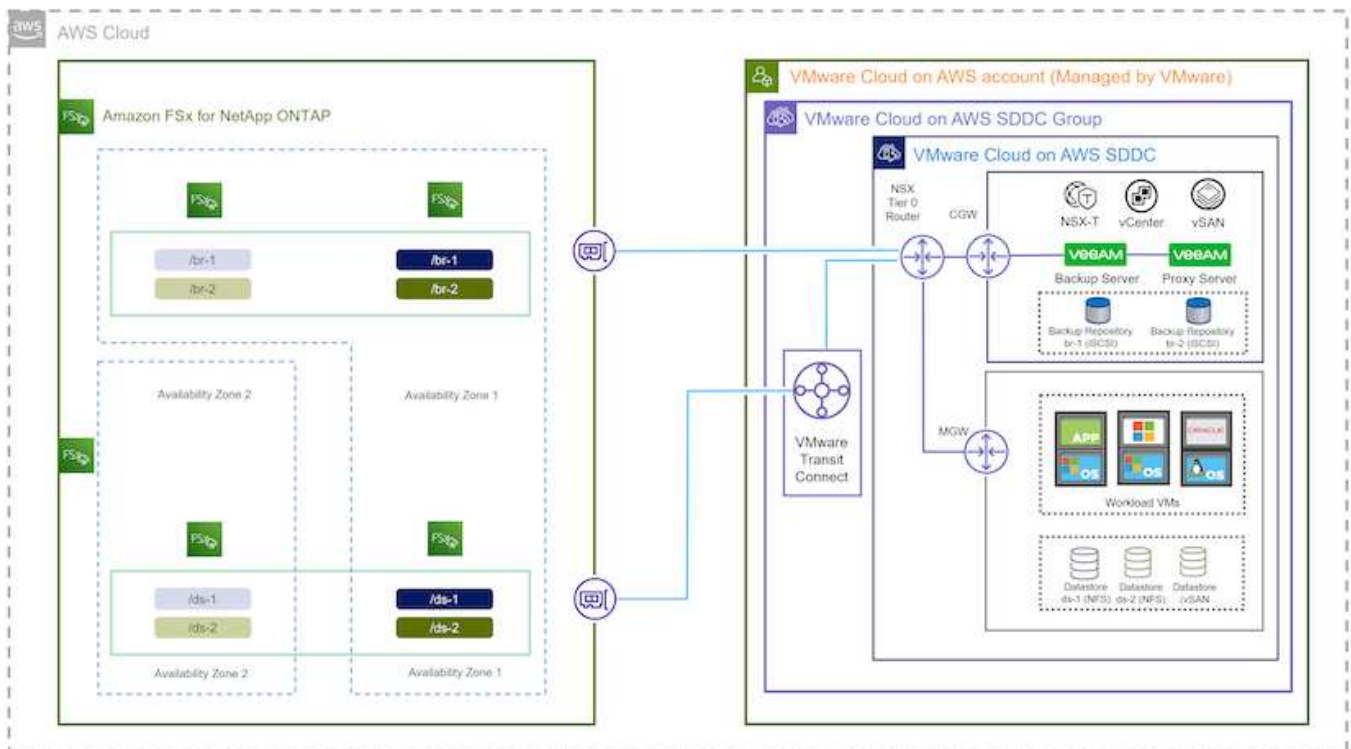
## 前提条件

本解决方案 的目的是演示在VMware Cloud中运行的虚拟机以及由FSx for NetApp ONTAP 托管的NFS数据存储库中的虚拟机的数据保护。此解决方案 假定已配置以下组件并可供使用：

1. 一个或多个NFS数据存储库连接到VMware Cloud的FSx for ONTAP 文件系统。
2. 安装了Veeam Backup & Replication软件的Microsoft Windows Server VM。
  - Veeam Backup & Replication服务器已使用其IP地址或完全限定域名发现vCenter Server。
3. 在解决方案 部署期间、要与Veeam备份代理组件一起安装的Microsoft Windows Server VM。
4. VMDK和应用程序数据驻留在FSx for ONTAP NFS数据存储库上的Microsoft SQL Server VM。对于此解决方案、我们在两个单独的VMDK上有两个SQL数据库。
  - 注意：作为最佳实践、数据库和事务日志文件应放置在单独的驱动器上、因为这样可以提高性能和可靠性。这部分是由于事务日志是按顺序写入的、而数据库文件是随机写入的。
5. 包含VMDK和应用程序数据的Oracle数据库VM驻留在FSx上、用于ONTAP NFS数据存储库。
6. VMDK驻留在FSx上的Linux和Windows文件服务器VM、用于ONTAP NFS数据存储库。
7. Veeam需要使用特定的TCP端口在备份环境中的服务器和组件之间进行通信。在Veeam备份基础架构组件上、系统会自动创建所需的防火墙规则。有关网络端口要求的完整列表、请参阅的端口部分 ["适用于VMware vSphere的Veeam备份和复制用户指南"](#)。

## 高级架构

此解决方案 的测试/验证是在可能与最终部署环境匹配或可能不匹配的实验室中执行的。有关详细信息、请参见以下各节。





本解决方案 的目的是演示在VMware Cloud中运行的虚拟机以及由FSx for NetApp ONTAP 托管的NFS数据存储库中的虚拟机的数据保护。此解决方案 假定已配置以下组件并可供使用：

- Microsoft Windows VM位于FSx for ONTAP NFS数据存储库上
- Linux (CentOS) VM位于FSx for ONTAP NFS数据存储库上
- Microsoft SQL Server VM位于FSx for ONTAP NFS数据存储库上
  - 两个数据库托管在不同的VMDK上
- Oracle VM位于FSx for ONTAP NFS数据存储库上

## 解决方案 部署

在本解决方案 中、我们详细说明了如何使用Veeam备份和复制软件部署和验证解决方案 、以便在AWS上的VMware Cloud SDDC中对SQL Server、Oracle以及Windows和Linux文件服务器虚拟机执行备份和恢复。此解决方案 中的虚拟机位于FSx for ONTAP 托管的补充NFS数据存储库中。此外、还会使用一个单独的FSx for ONTAP 文件系统来托管要用于Veeam备份存储库的iSCSI卷。

我们将通过FSx创建ONTAP 文件系统、挂载要用作备份存储库的iSCSI卷、创建和运行备份作业以及执行VM和数据库还原。

有关FSx for NetApp ONTAP 的详细信息、请参见 ["FSx for ONTAP 用户指南"](#)。

有关Veeam备份和复制的详细信息、请参见 ["Veeam帮助中心技术文档"](#) 站点

有关将Veeam Backup and Replication与VMware Cloud on AWS结合使用时的注意事项和限制、请参见 ["基于AWS的VMware Cloud和基于Dell EMC支持的VMware Cloud。注意事项和限制"](#)。

### 部署Veeam代理服务器

Veeam代理服务器是Veeam Backup & Replication软件的一个组件、充当源与备份或复制目标之间的中介。代理服务器通过在本机处理数据来帮助优化和加速备份作业期间的数据传输、并且可以使用不同的传输模式通过VMware vStorage API进行数据保护或通过直接存储访问来访问数据。

在选择Veeam代理服务器设计时、请务必考虑并发任务的数量以及所需的传输模式或存储访问类型。

有关代理服务器数量的规模估算及其系统要求、请参见 ["Veeam VMware vSphere最佳实践指南"](#)。

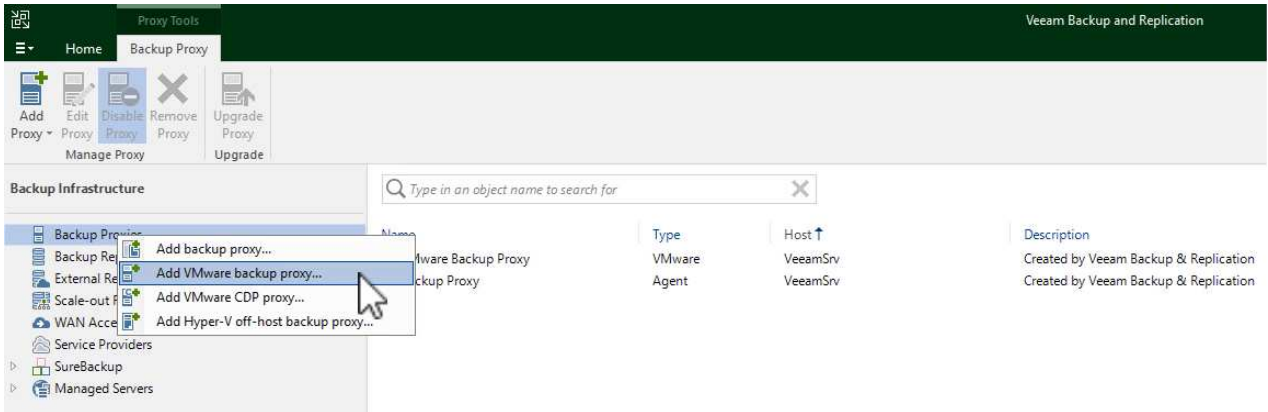
Veeam Data Mover是Veeam代理服务器的一个组件、它利用传输模式从源获取VM数据并将其传输到目标。传输模式是在配置备份作业期间指定的。通过使用直接存储访问、可以提高从NFS数据存储库备份的效率。

有关传输模式的详细信息、请参阅 ["适用于VMware vSphere的Veeam备份和复制用户指南"](#)。

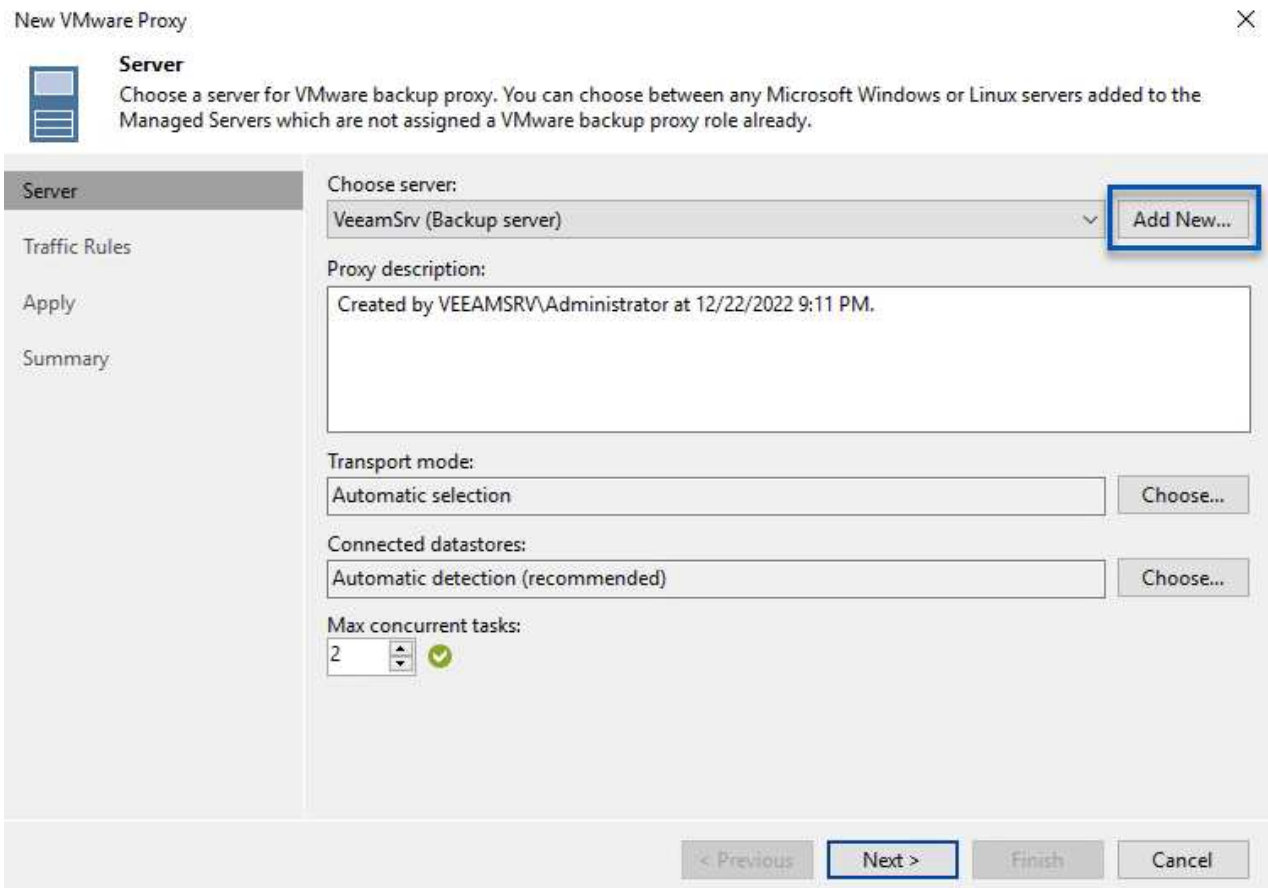
在下面的步骤中、我们将介绍如何在VMware Cloud SDDC中的Windows VM上部署Veeam代理服务器。

在此步骤中、Veeam代理将部署到现有Windows VM。这样便可在主Veeam备份服务器和Veeam代理之间分布备份作业。

1. 在Veeam Backup and Replication服务器上、打开管理控制台并选择左下方菜单中的\*备份基础架构\*。
2. 右键单击\*备份代理\*，然后单击\*添加VMware备份代理...\*以打开向导。

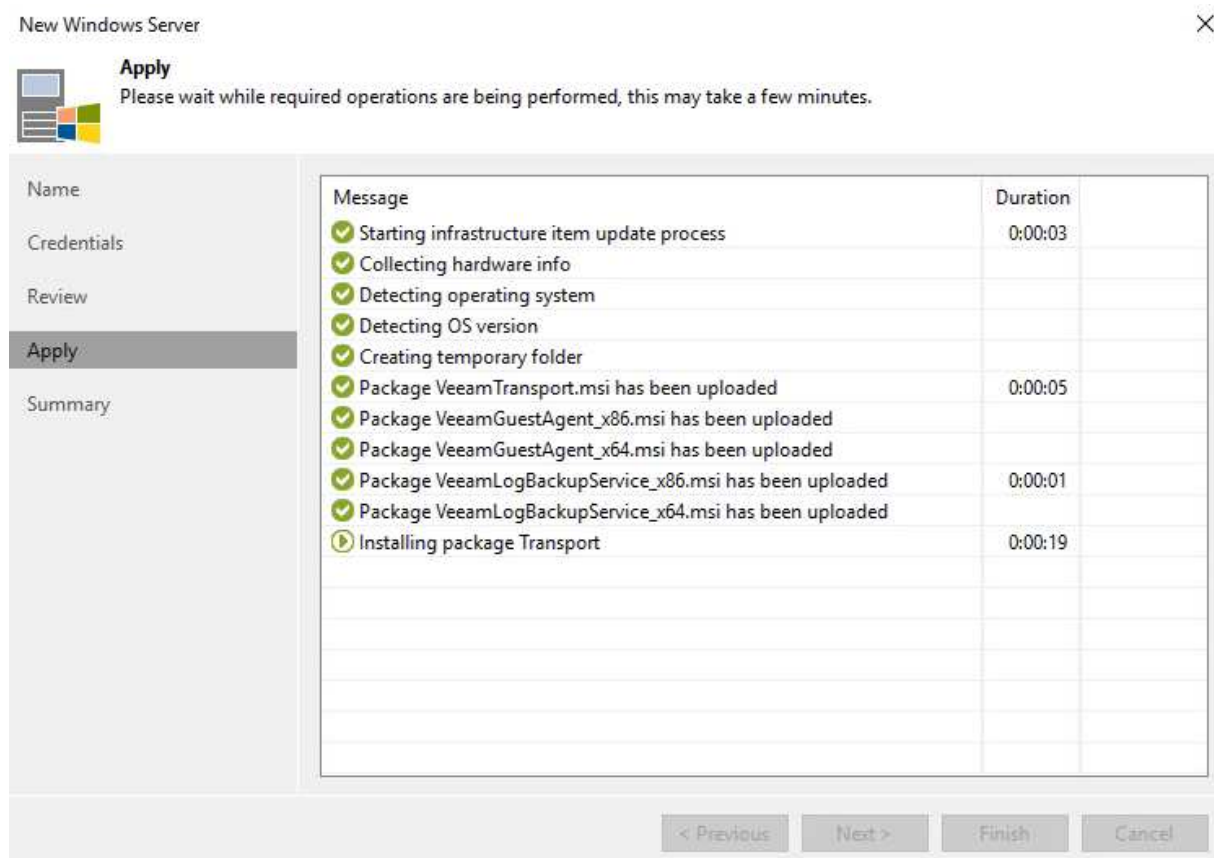


3. 在\*Add VMware Proxy\*向导中，单击\*Add New...\*按钮以添加新的代理服务器。

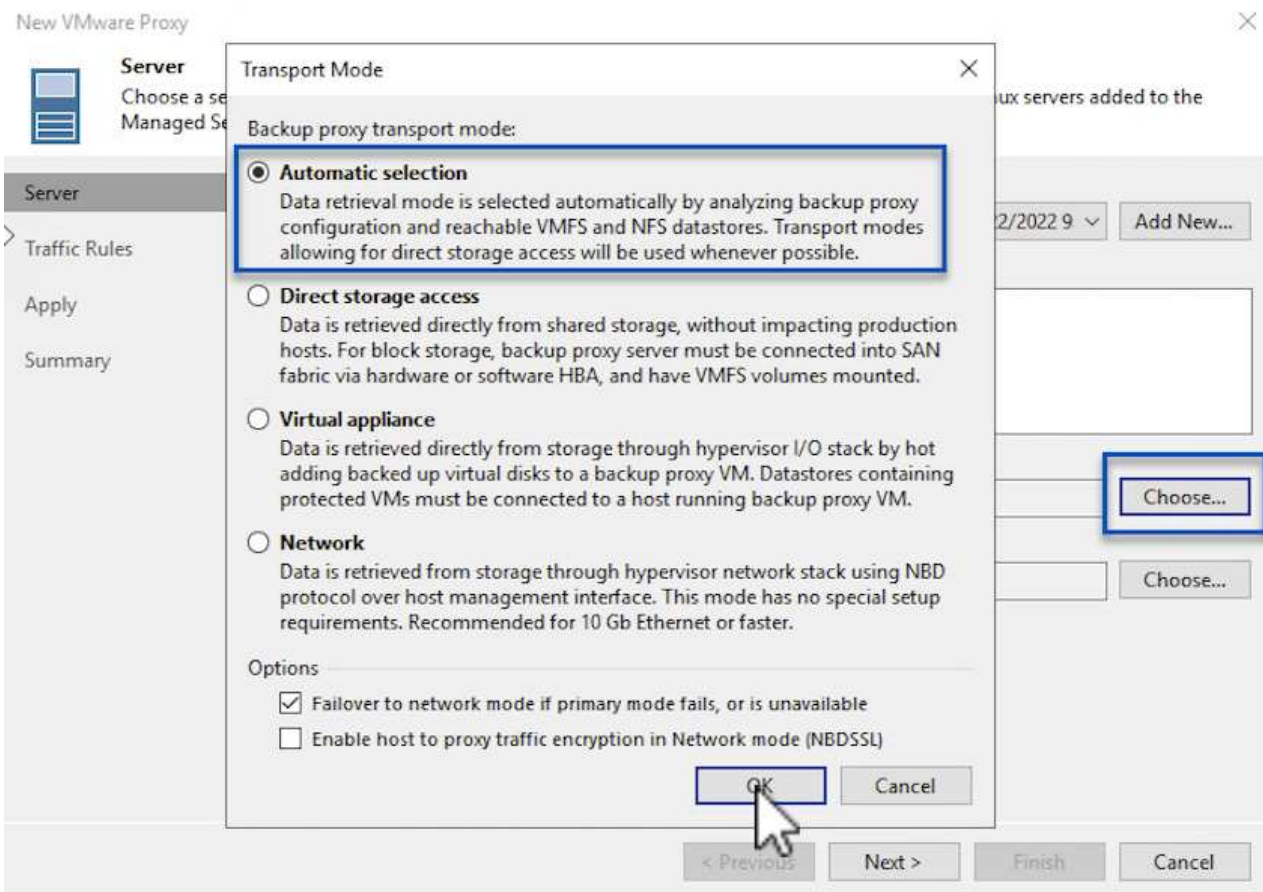


4. 选择以添加Microsoft Windows、然后按照提示添加服务器：
  - 填写DNS名称或IP地址

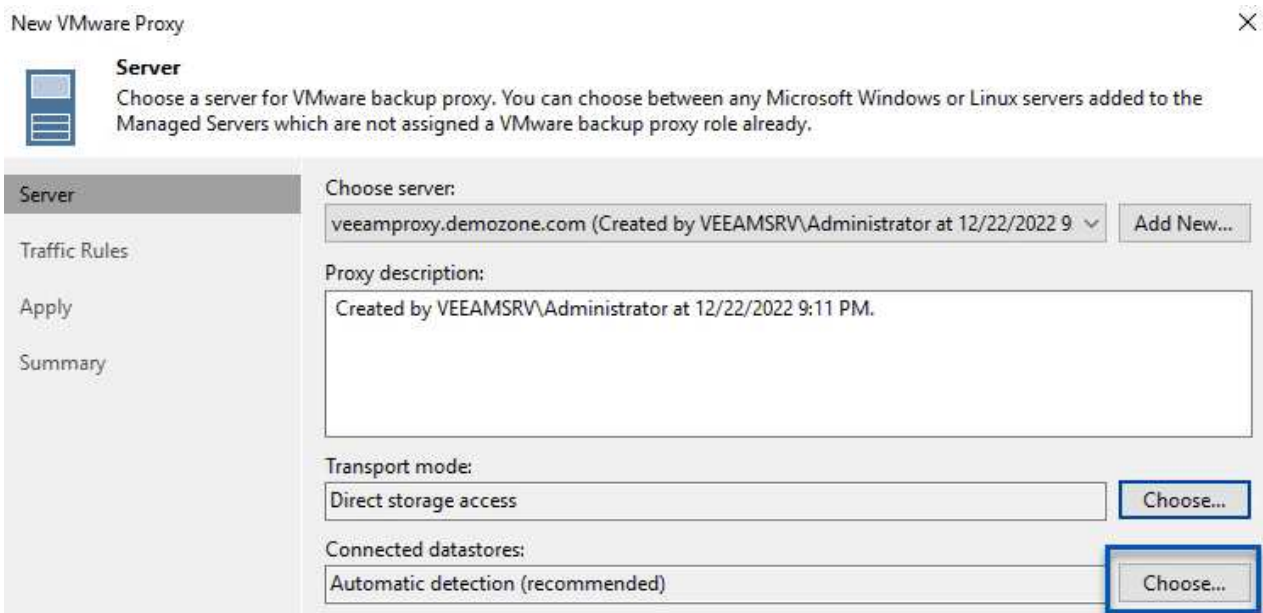
- 选择要用于新系统上的凭据的帐户或添加新凭据
- 查看要安装的组件，然后单击\*Apply\*开始部署

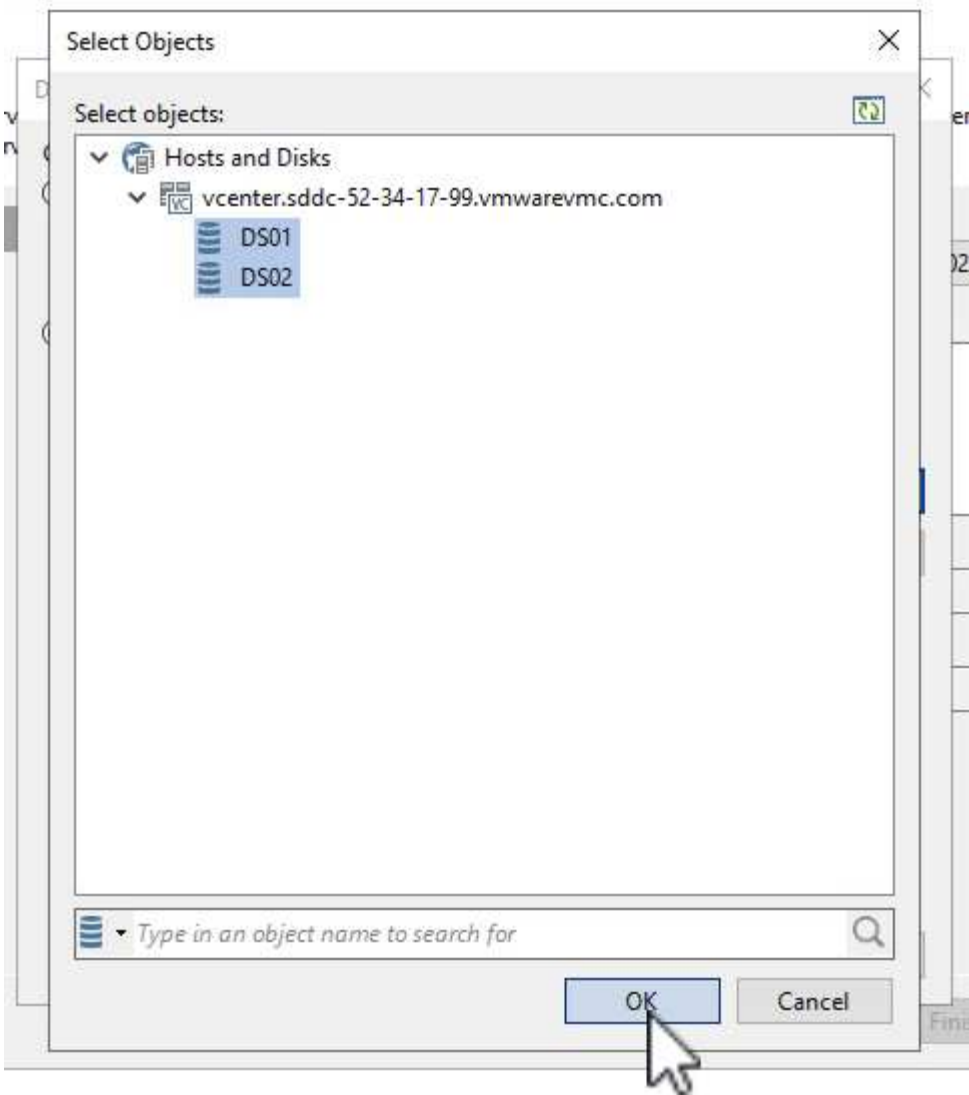


5. 返回“新建VMware代理”向导，选择传输模式。在本例中，我们选择了\*自动选择\*。

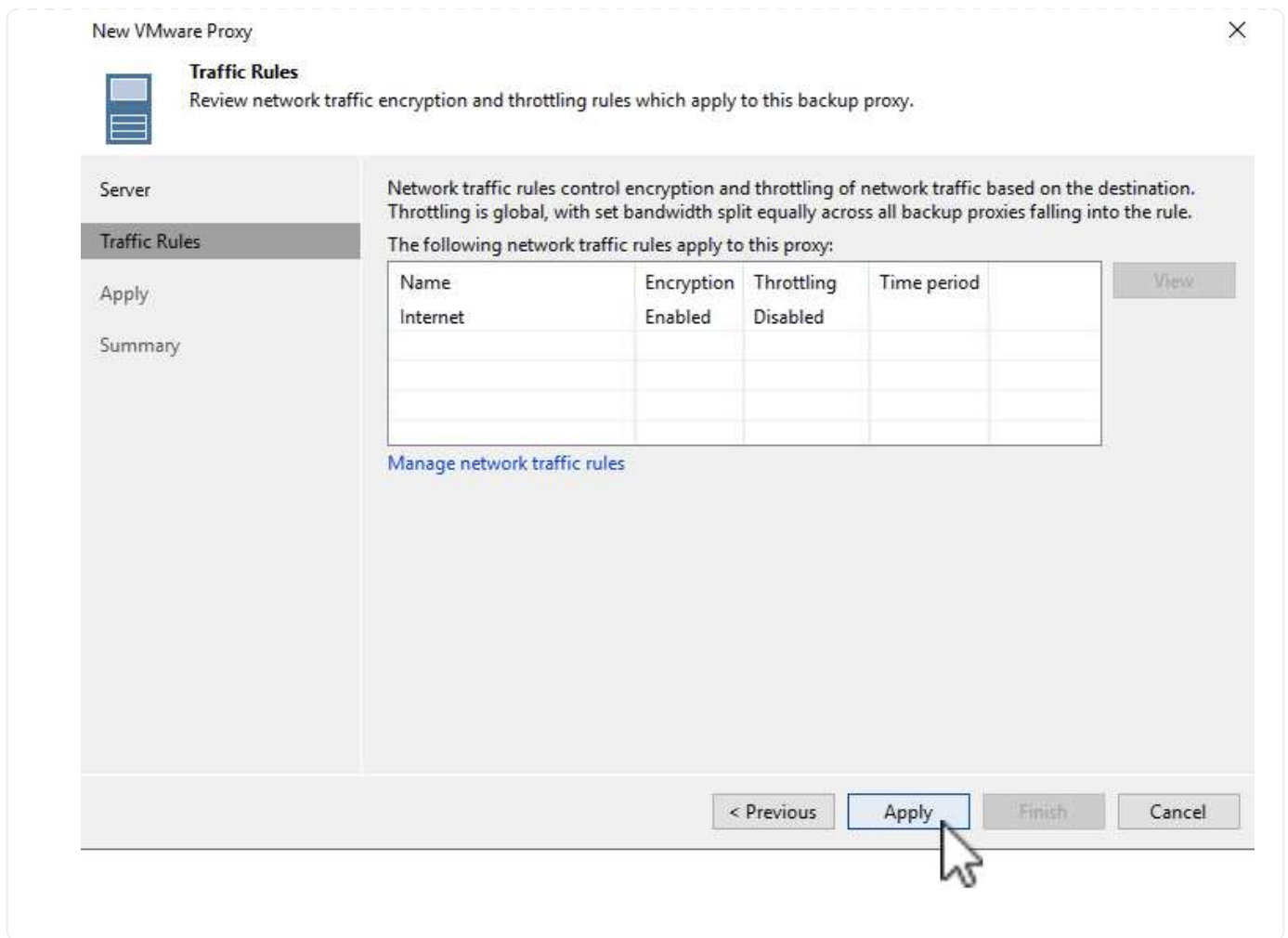


6. 选择希望VMware代理直接访问的已连接数据存储库。





7. 根据需要配置和应用任何特定网络流量规则、例如加密或限制。完成后，单击\*Apply\*按钮完成部署。



## 配置存储和备份存储库

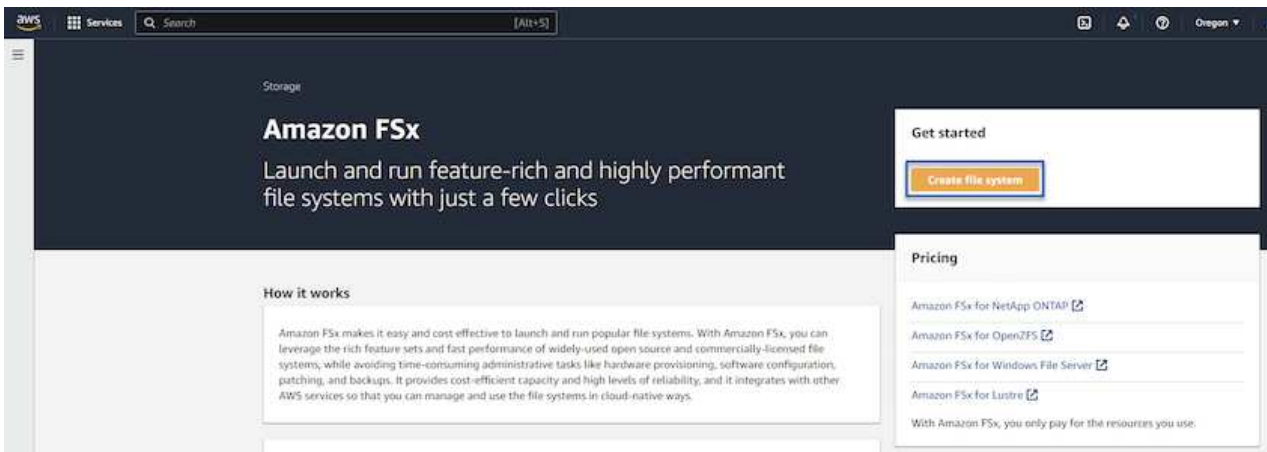
主Veeam备份服务器和Veeam代理服务器可访问直连存储形式的备份存储库。在本节中、我们将介绍如何创建适用于ONTAP 文件系统的FSx、如何将iSCSI LUN挂载到Veeam服务器以及如何创建备份存储库。



## 为ONTAP 文件系统创建FSx

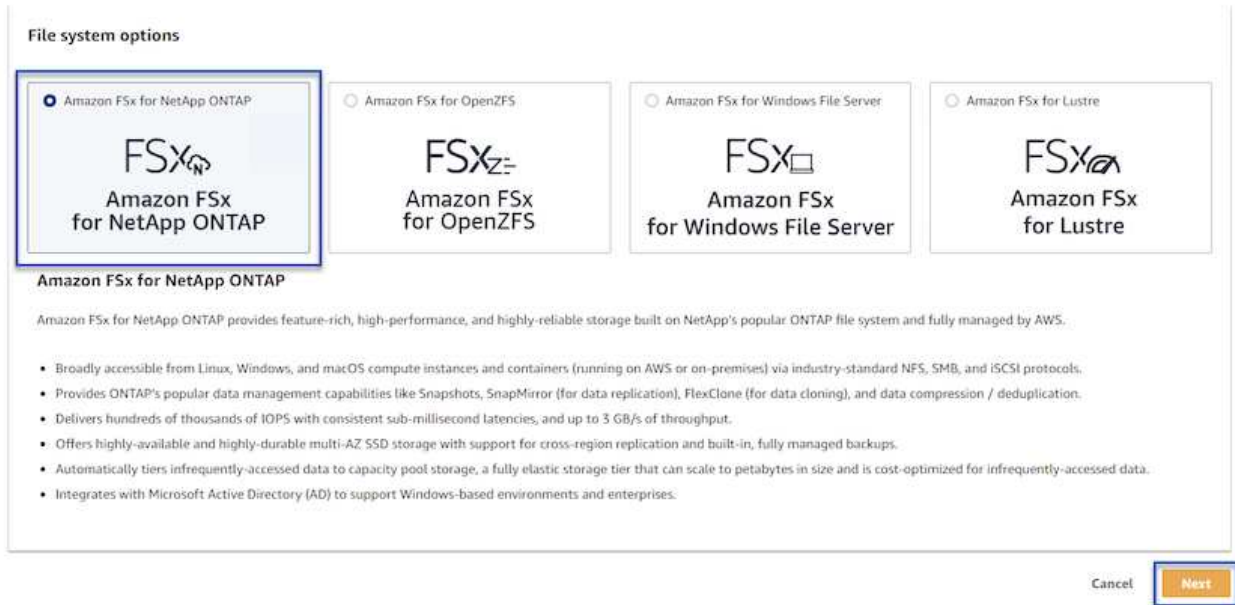
创建FSx for ONTAP 文件系统、用于托管Veeam备份存储库的iSCSI卷。

1. 在AWS控制台中，转到FSx，然后选择\*Create file system\*



2. 选择\*Amazon FSx for NetApp ONTAP FS\*，然后选择\*Next\*继续。

### Select file system type



3. 填写文件系统名称、部署类型、SSD存储容量以及FSx for ONTAP 集群将驻留的VPC。此VPC必须配置为与VMware Cloud中的虚拟机网络进行通信。单击“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. 查看部署步骤，然后单击\*Create File System\*开始文件系统创建过程。



## 配置和挂载iSCSI LUN

在FSx for ONTAP 上创建和配置iSCSI LUN、然后挂载到Veeam备份和代理服务器。这些LUN稍后将用于创建Veeam备份存储库。



在FSx for ONTAP 上创建iSCSI LUN是一个多步骤过程。创建卷的第一步可以在Amazon FSx控制台中完成、也可以使用NetApp ONTAP 命令行界面完成。



有关使用FSx for ONTAP 的详细信息、请参见 ["FSx for ONTAP 用户指南"](#)。

1. 在NetApp ONTAP 命令行界面中、使用以下命令创建初始卷：

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

2. 使用上一步中创建的卷创建LUN：

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

3. 通过创建包含Veeam备份和代理服务器的iSCSI IQN的启动程序组来授予对LUN的访问权限：

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

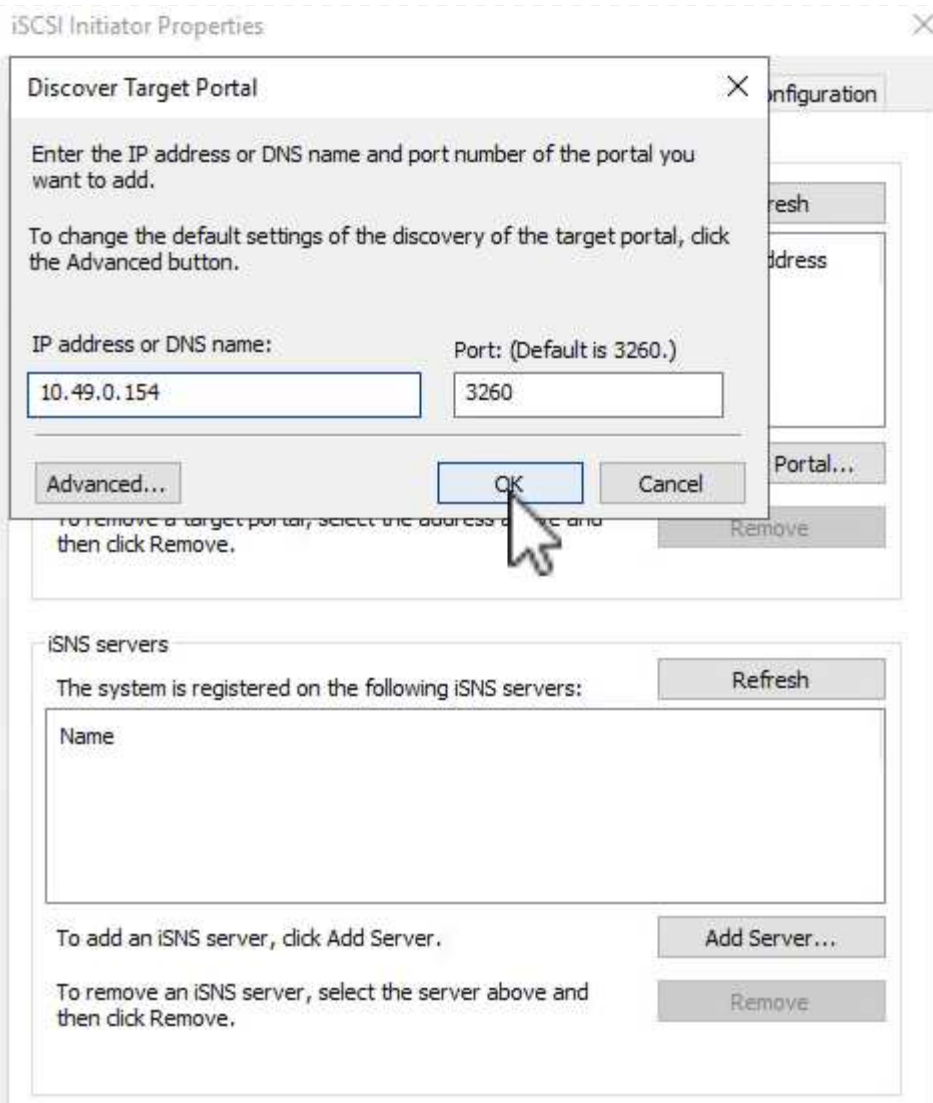


要完成上述步骤、您需要先从Windows服务器上的iSCSI启动程序属性检索IQN。

4. 最后、将LUN映射到刚刚创建的启动程序组：

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

5. 要挂载iSCSI LUN、请登录到Veeam Backup & Replication Server并打开iSCSI启动程序属性。进入\*Discover (\*发现)\*选项卡并输入iSCSI目标IP地址。



6. 在\*目标\*选项卡上，突出显示非活动LUN并单击\*Connect\*。选中\*启用多路径\*框，然后单击\*确定\*以连接到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:

Discovered targets

Name	Status
iqn.1992-08.com.netapp:sn.d9aad3cd818011edbfc87a...	Inactive

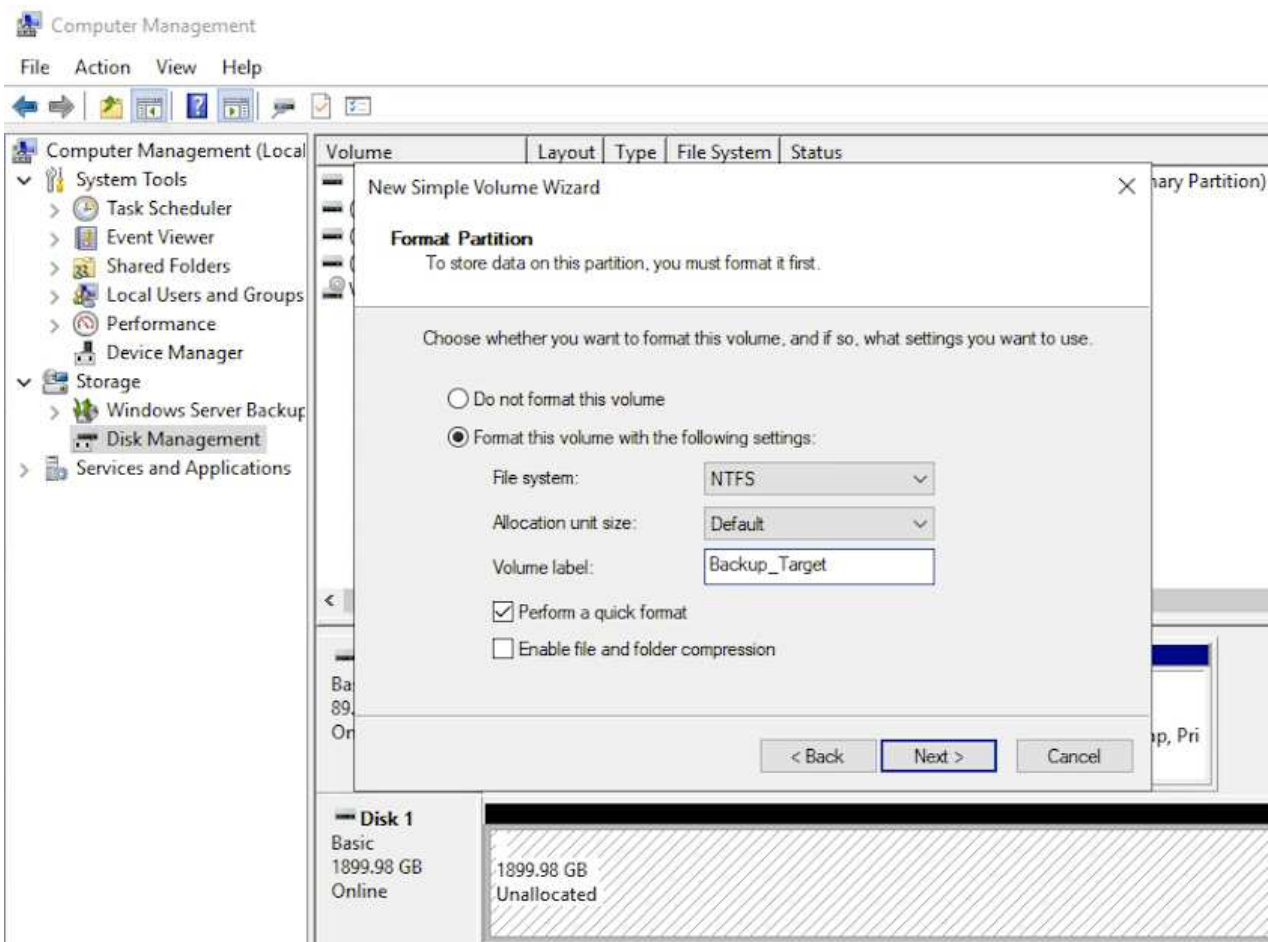
To connect using advanced options, select a target and then click Connect.

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...

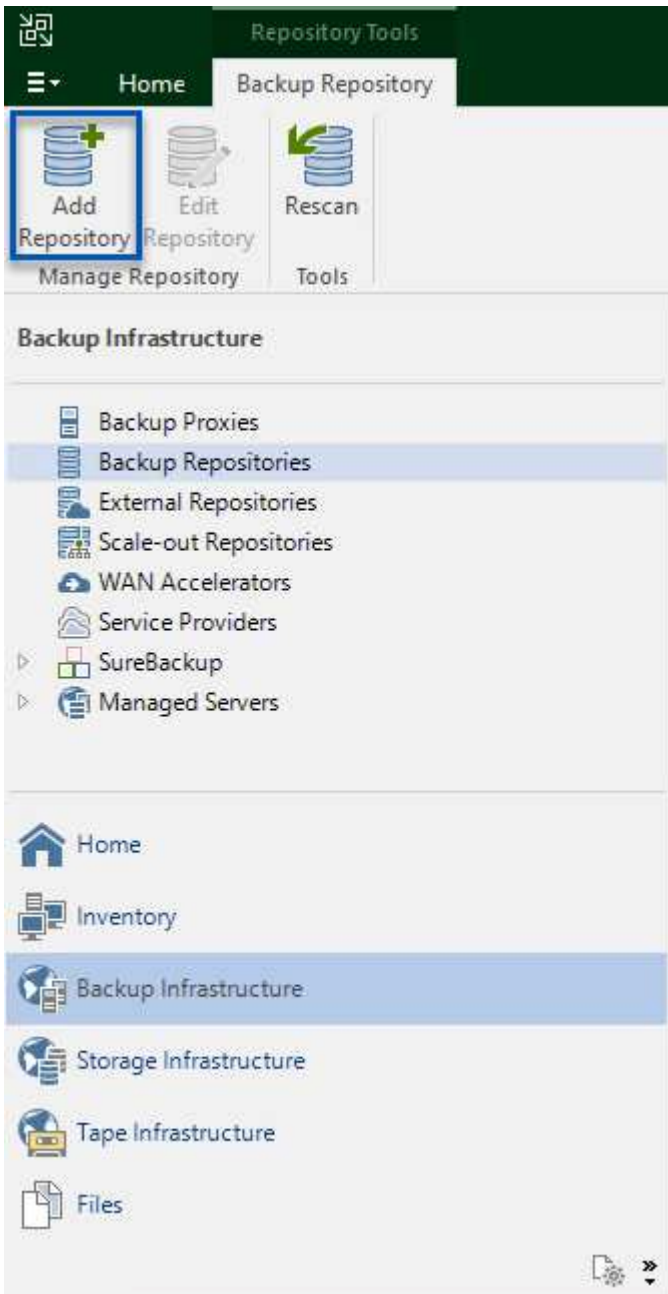
7. 在磁盘管理实用程序中、初始化新的LUN并使用所需的名称和驱动器盘符创建卷。选中\*启用多路径\*框，然后单击\*确定\*以连接到LUN。



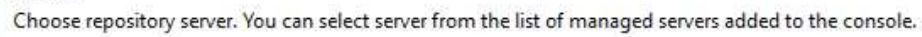
8. 重复上述步骤、将iSCSI卷挂载到Veeam代理服务器上。

在Veeam Backup and Replication控制台中、为Veeam Backup和Veeam Proxy服务器创建备份存储库。这些存储库将用作虚拟机备份的备份目标。

1. 在Veeam Backup and Replication控制台中、单击左下方的\*备份基础架构\*、然后选择\*添加存储库\*




2. 在"New Backup Repository (新建备份存储库)"向导中、输入存储库的名称、然后从下拉列表中选择服务器、并单击\*填充\*按钮以选择要使用的NTFS卷。



3. 在下一页上、选择执行高级还原时用于挂载备份的挂载服务器。默认情况下、此服务器与存储库存储连接在一起。
4. 查看您的选择，然后单击\*Apply\*开始创建备份存储库。

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. 对任何其他代理服务器重复上述步骤。

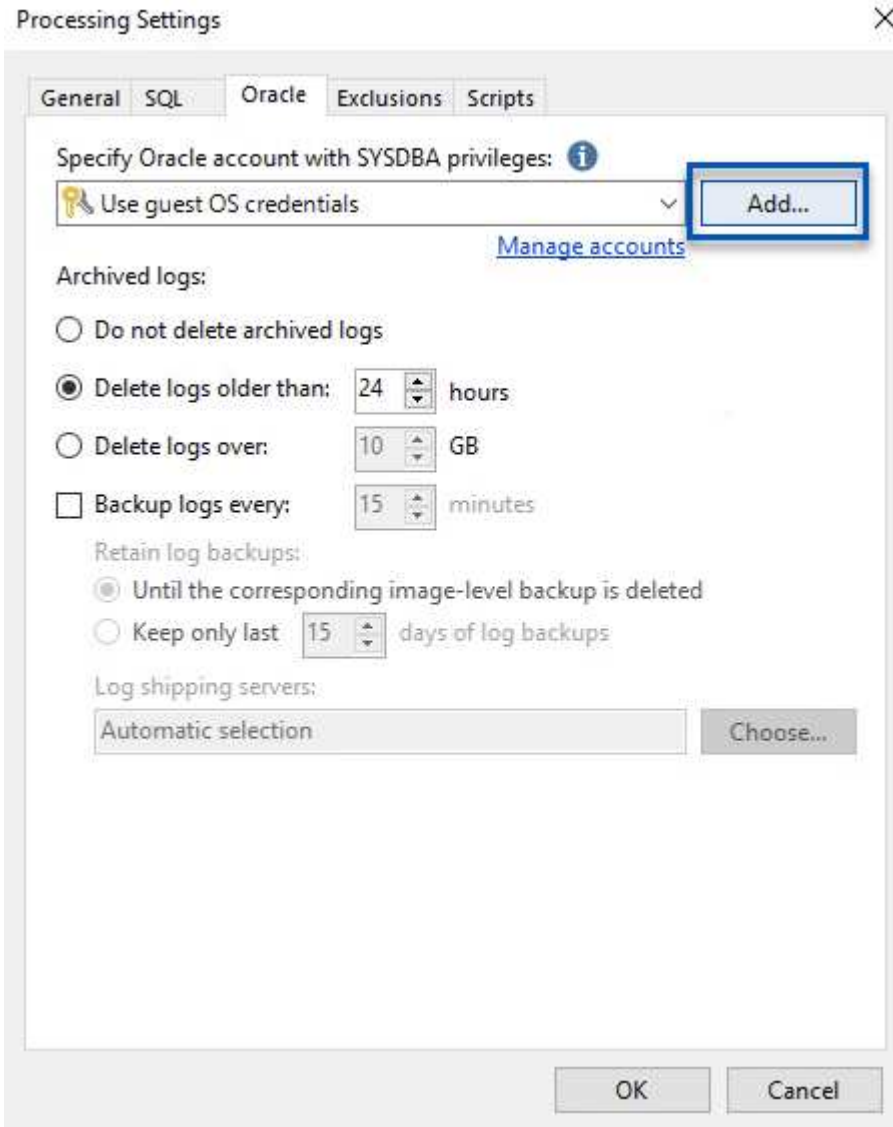
配置Veeam备份作业

应使用上一节中的备份系统信息栏创建备份作业。创建备份作业是任何存储管理员的常规任务、此处不会介绍所有步骤。有关在Veeam中创建备份作业的详细信息、请参见 ["Veeam帮助中心技术文档"](#)。

在此解决方案 中、为以下项创建了单独的备份作业：

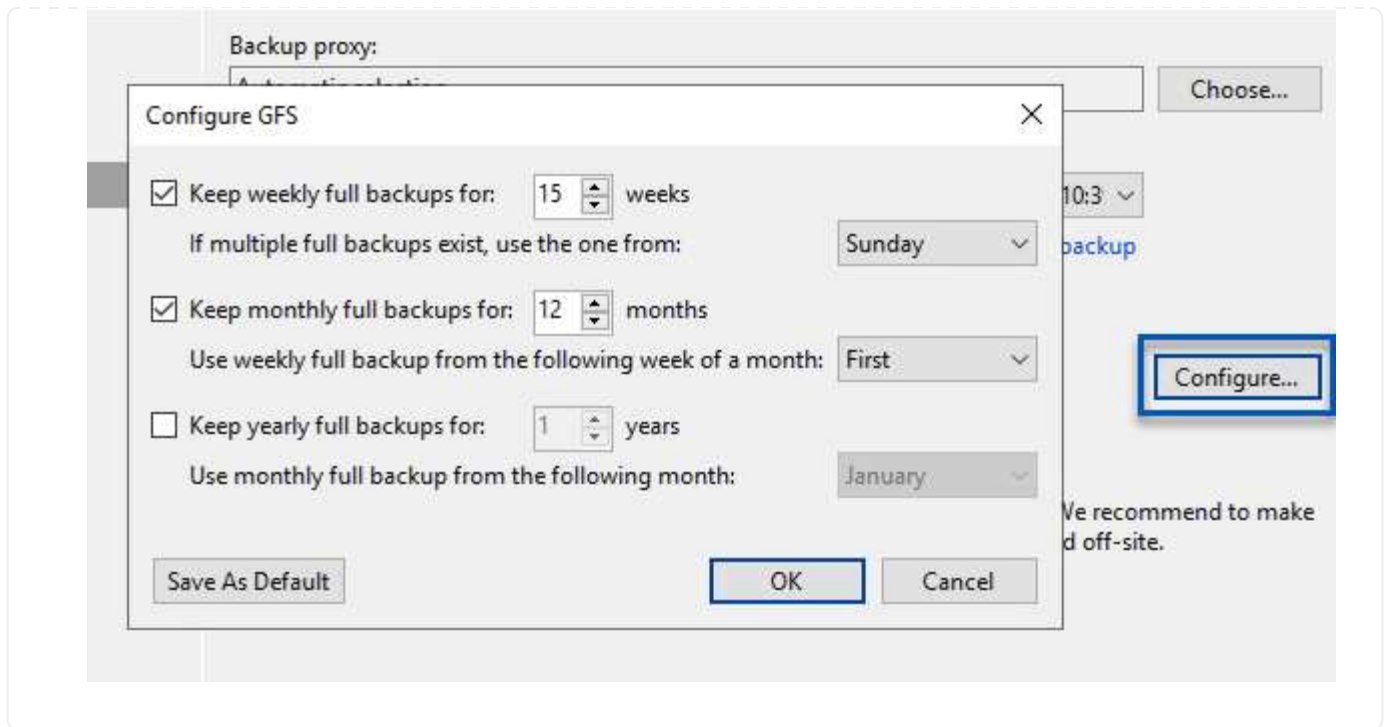
- Microsoft Windows SQL Server
- Oracle数据库服务器
- Windows文件服务器
- Linux文件服务器

1. 启用应用程序感知型处理、以创建一致的备份并执行事务日志处理。
2. 启用应用程序感知型处理后、请向应用程序添加具有管理员权限的正确凭据、因为此凭据可能与子操作系统凭据不同。



3. 要管理备份的保留策略，请选中\*将某些完整备份保留更长的时间以供归档使用\*，然后单击\*配置...\*按钮以配置策略。





## 使用Veeam完全恢复还原应用程序VM

使用Veeam执行完全还原是执行应用程序还原的第一步。我们验证了已启动的VM的完全恢复以及所有服务均正常运行。

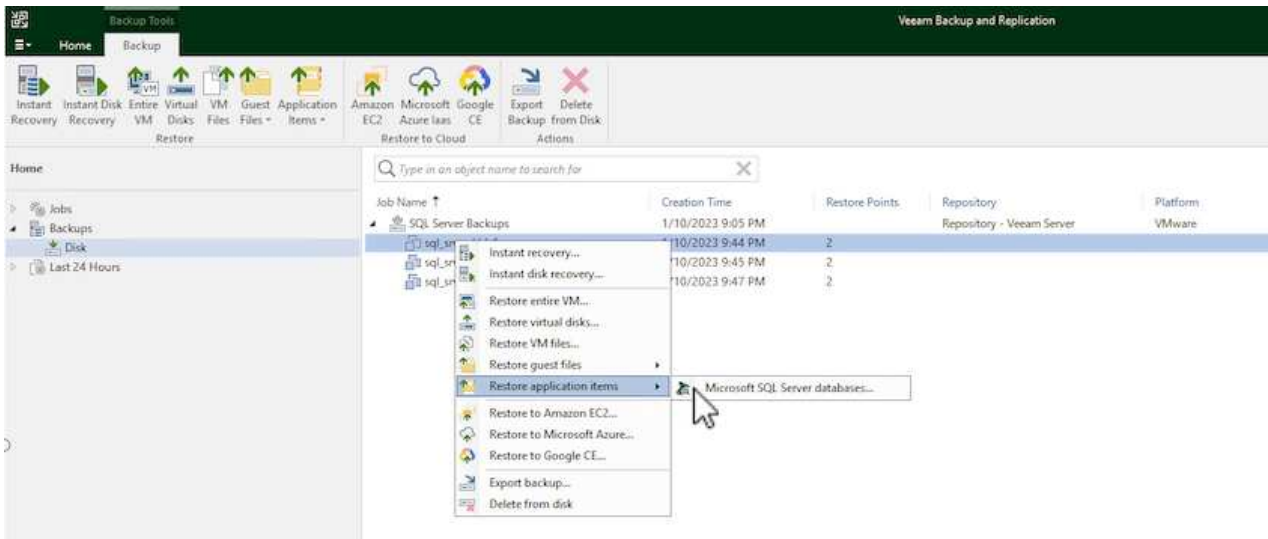
还原服务器是任何存储管理员职责的正常组成部分、此处不会介绍所有步骤。有关在Veeam中执行完全恢复的更多完整信息、请参见 ["Veeam帮助中心技术文档"](#)。

## 还原SQL Server数据库

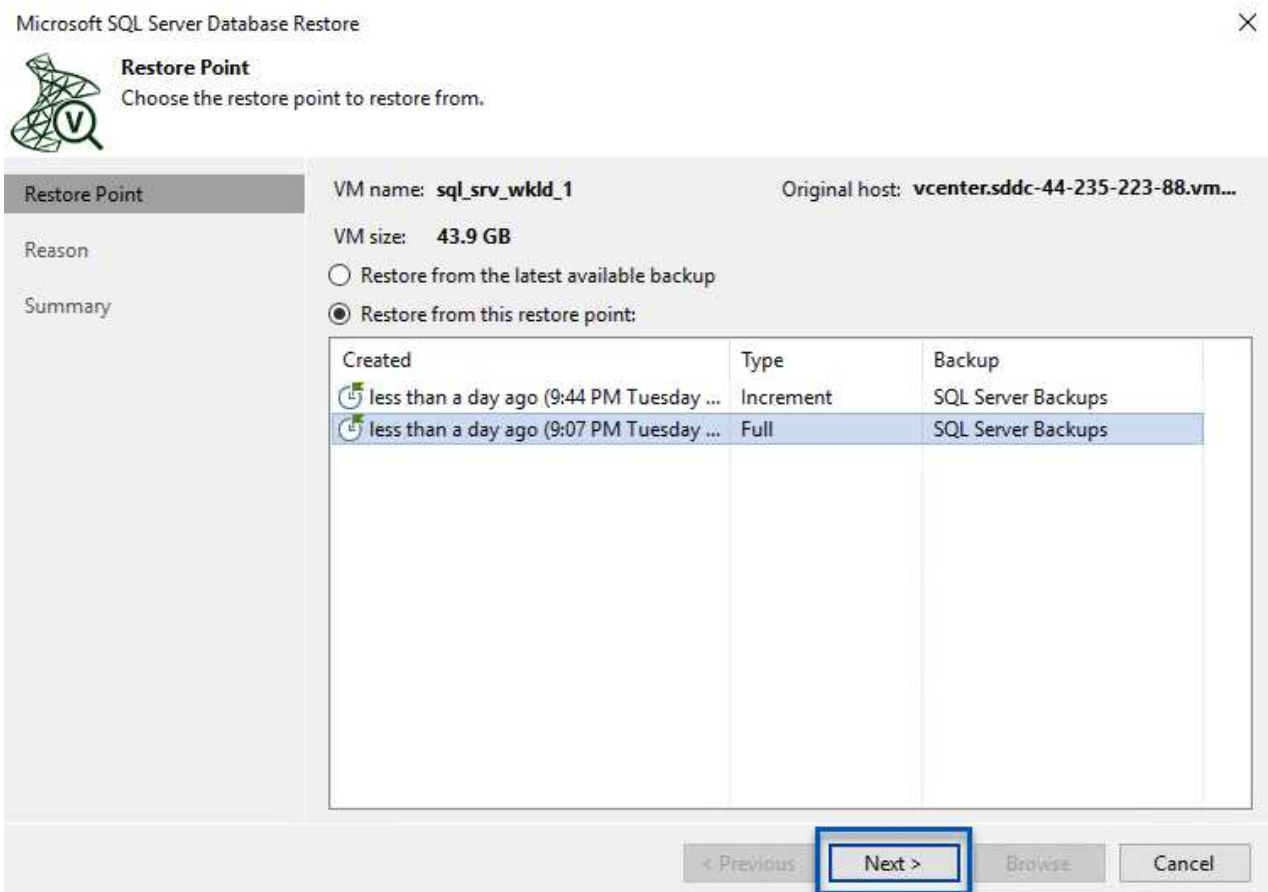
Veeam Backup & Replication提供了多种还原SQL Server数据库的选项。在此验证中、我们使用Veeam Explorer for SQL Server with Instant Recovery执行SQL Server数据库还原。SQL Server即时恢复是一项功能、可用于快速还原SQL Server数据库、而无需等待完整的数据库还原。这种快速恢复过程可最大限度地减少停机时间并确保业务连续性。工作原理如下：

- Veeam Explorer 挂载包含要还原的**SQL Server**数据库的备份。
- 软件\*直接从装载的文件发布数据库\*，使其可作为目标SQL Server实例上的临时数据库访问。
- 在使用临时数据库时、Veeam Explorer \*将用户查询\*重定向到此数据库、以确保用户可以继续访问和使用数据。
- 在后台、Veeam 执行完整数据库还原、将数据从临时数据库传输到原始数据库位置。
- 完整数据库还原完成后、Veeam Explorer \*将用户查询切换回原始\*数据库并删除临时数据库。

1. 在Veeam备份和复制控制台中、导航到SQL Server备份列表、右键单击某个服务器并选择\*还原应用程序项\*、然后选择\* Microsoft SQL Server数据库...\*。



2. 在Microsoft SQL Server数据库还原向导中，从列表中选择还原点，然后单击\*Next\*。



3. 如果需要、输入\*恢复原因\*、然后在摘要页面上、单击\*浏览\*按钮以启动Veeam Explorer for Microsoft SQL Server。

**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

Reason

Summary

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)

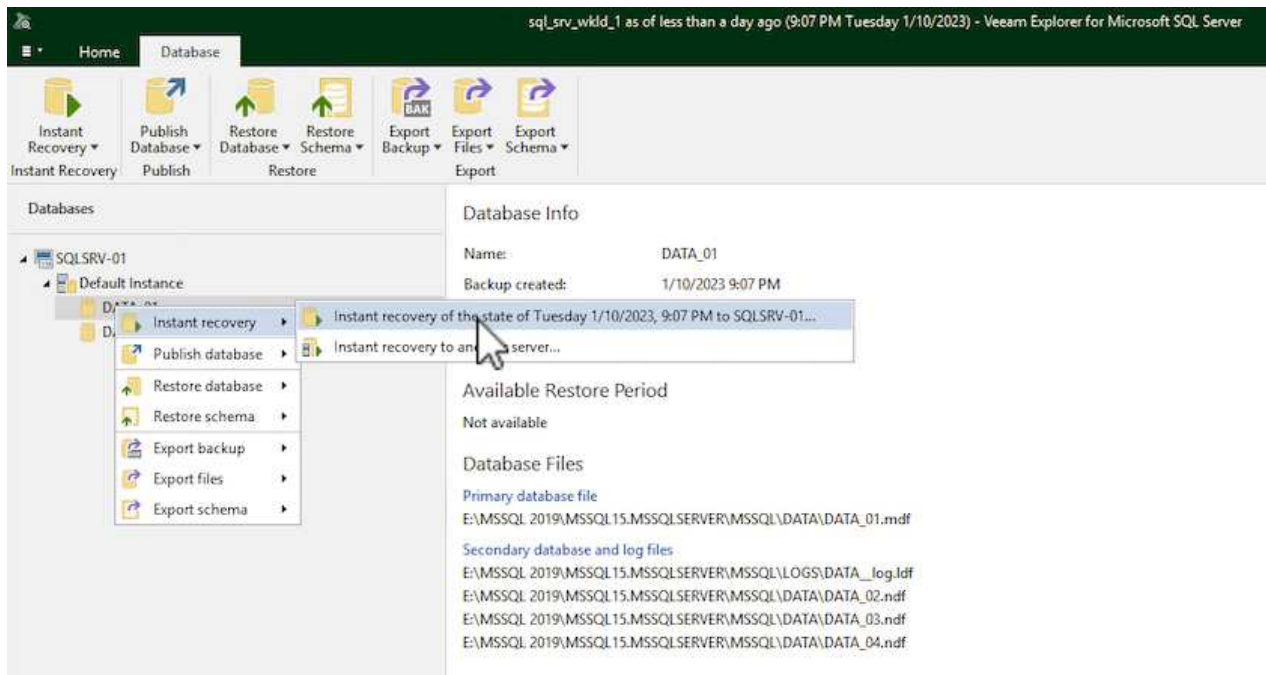
&lt; Previous

Next &gt;

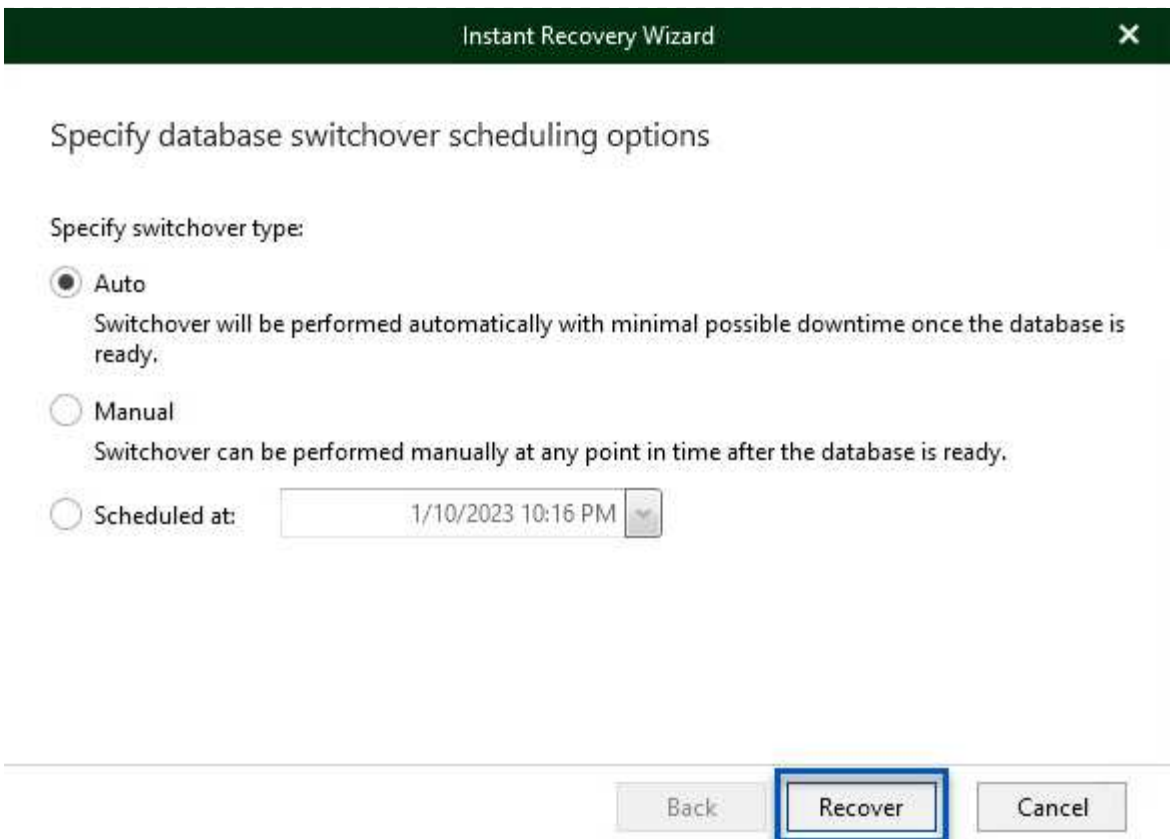
Browse

Cancel

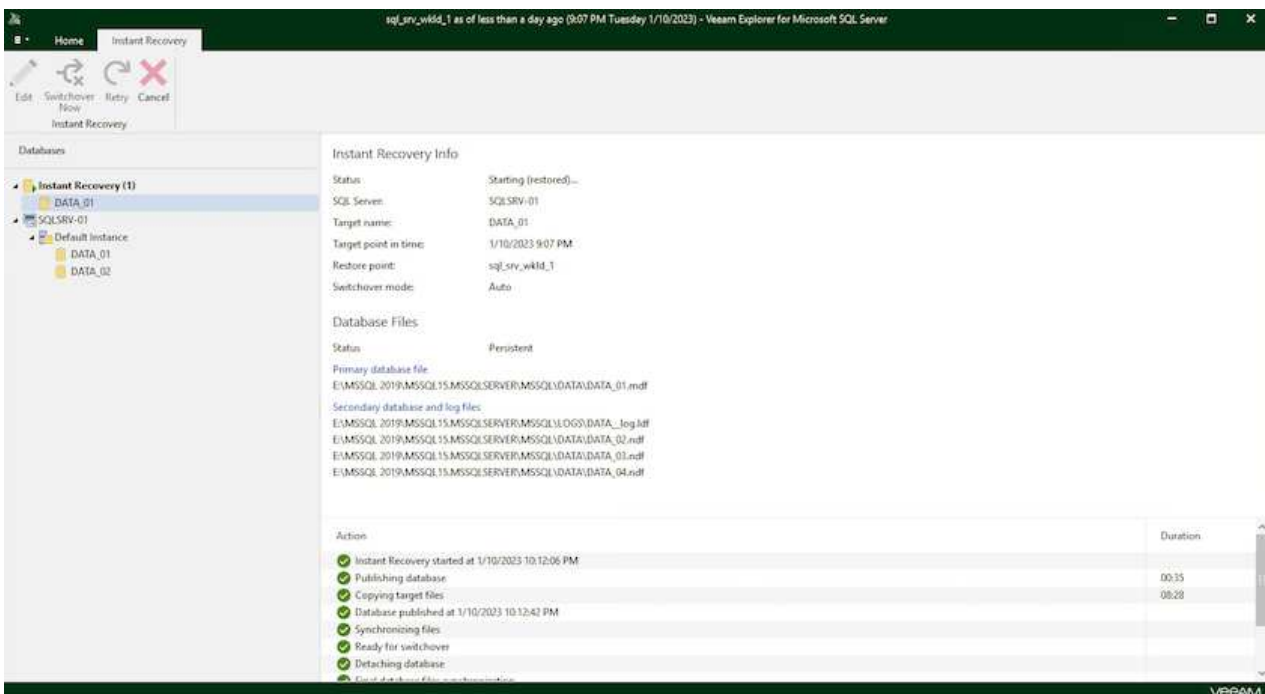
4. 在Veeam Explorer中展开数据库实例列表、右键单击并选择\*即时恢复\*、然后选择要恢复到的特定还原点。



5. 在即时恢复向导中、指定切换类型。这可以是自动执行的、停机时间最短、也可以是手动执行的、也可以是在指定时间执行的。然后单击\*recover (恢复)\*按钮开始恢复过程。



6. 可以从Veeam Explorer监控恢复过程。



有关使用Veeam Explorer执行SQL Server还原操作的详细信息，请参阅中的Microsoft SQL Server一节 "《Veeam Explorers用户指南》"。

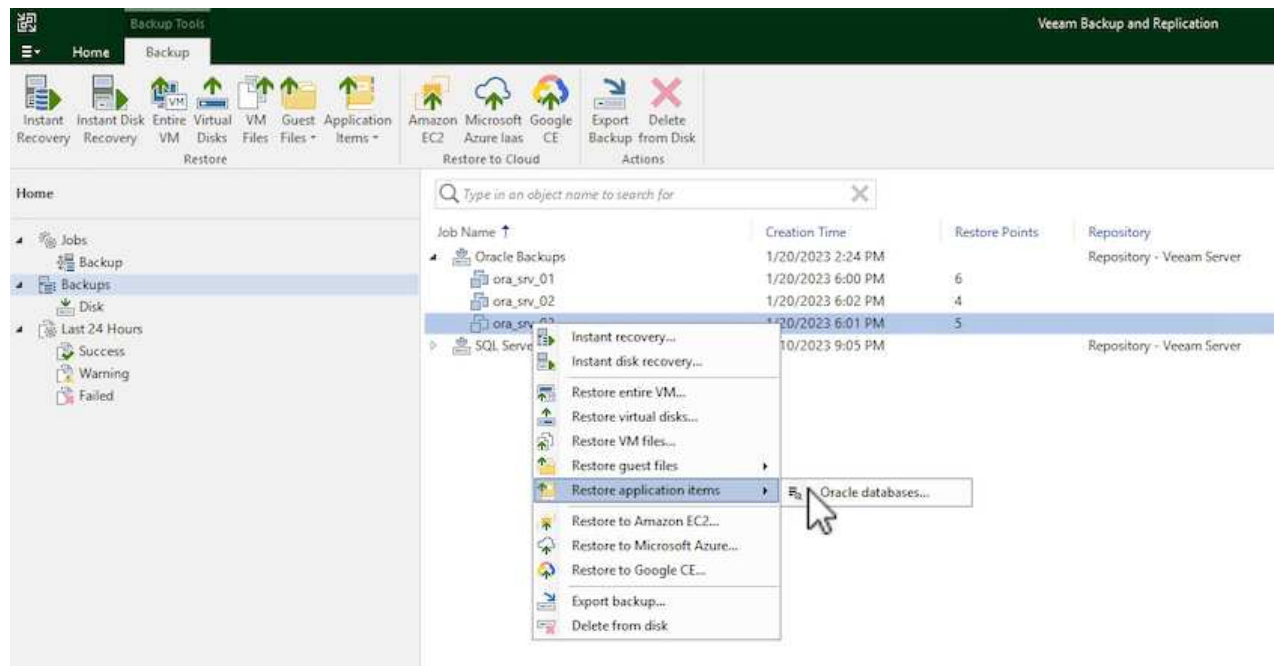
## 使用Veeam Explorer还原Oracle数据库

Veeam Explorer for Oracle数据库支持使用即时恢复执行标准Oracle数据库还原或无中断还原。它还支持发布数据库、以便快速访问、恢复Data Guard数据库以及从RMAN备份中恢复。

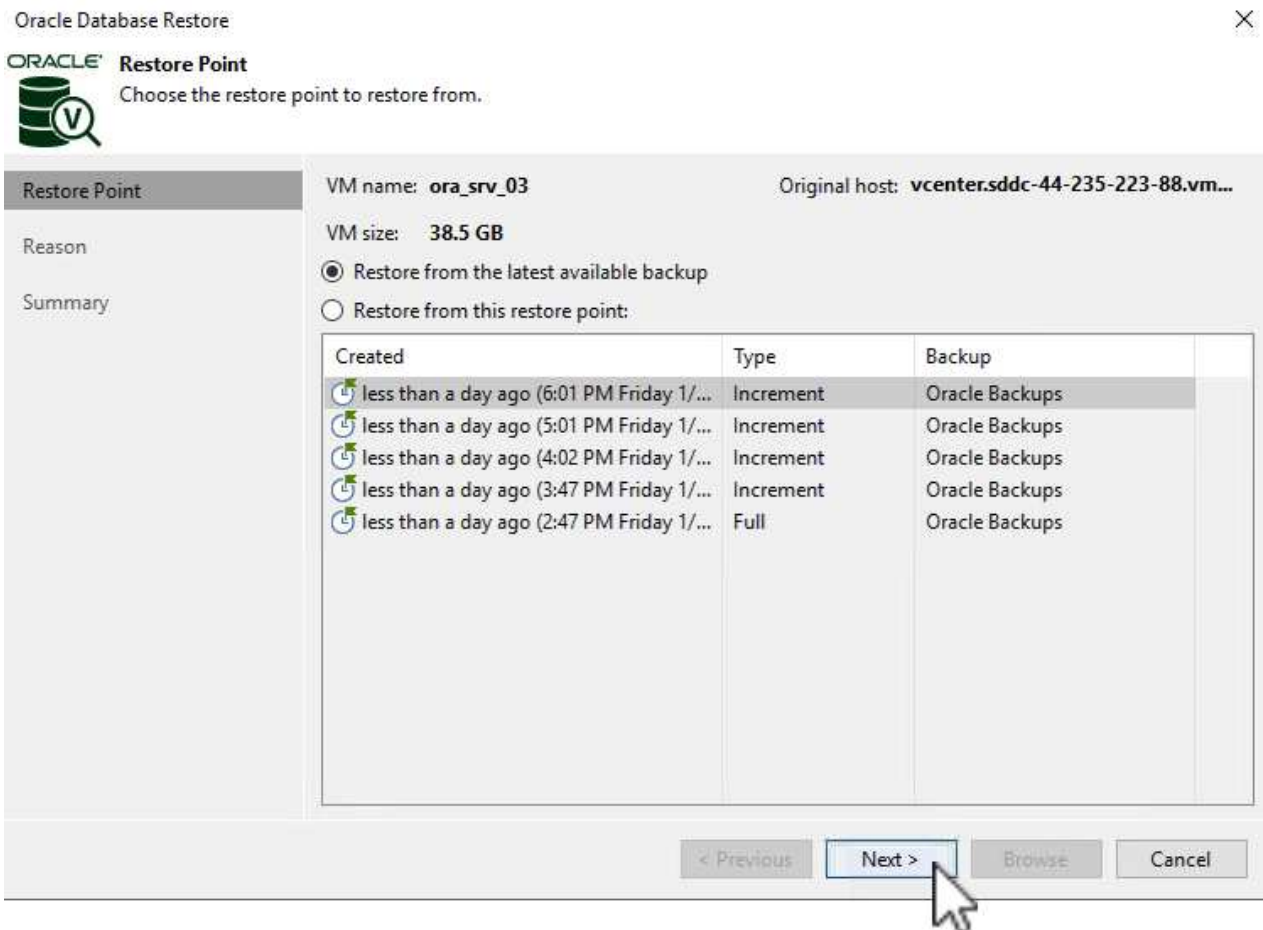
有关使用Veeam Explorer执行Oracle数据库还原操作的详细信息、请参阅中的Oracle一节 "[《Veeam Explorers 用户指南》](#)"。

本节将介绍如何使用Veeam Explorer将Oracle数据库还原到其他服务器。

1. 在Veeam Backup and Replication控制台中、导航到Oracle备份列表、右键单击某个服务器并选择\*还原应用程序项\*、然后选择\* Oracle数据库... \*。

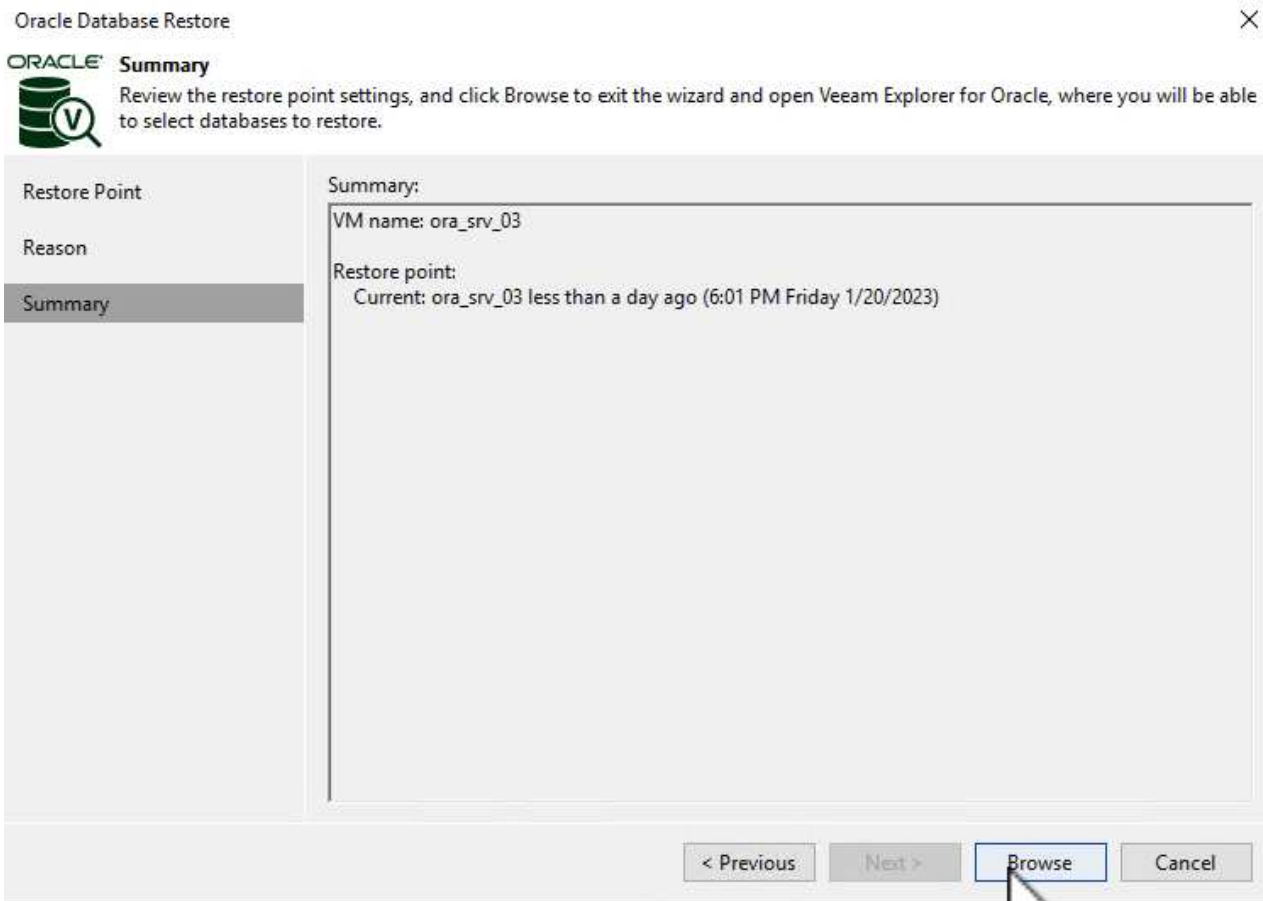


2. 在Oracle数据库恢复向导中，从列表选择一个还原点，然后单击\*Next\*。

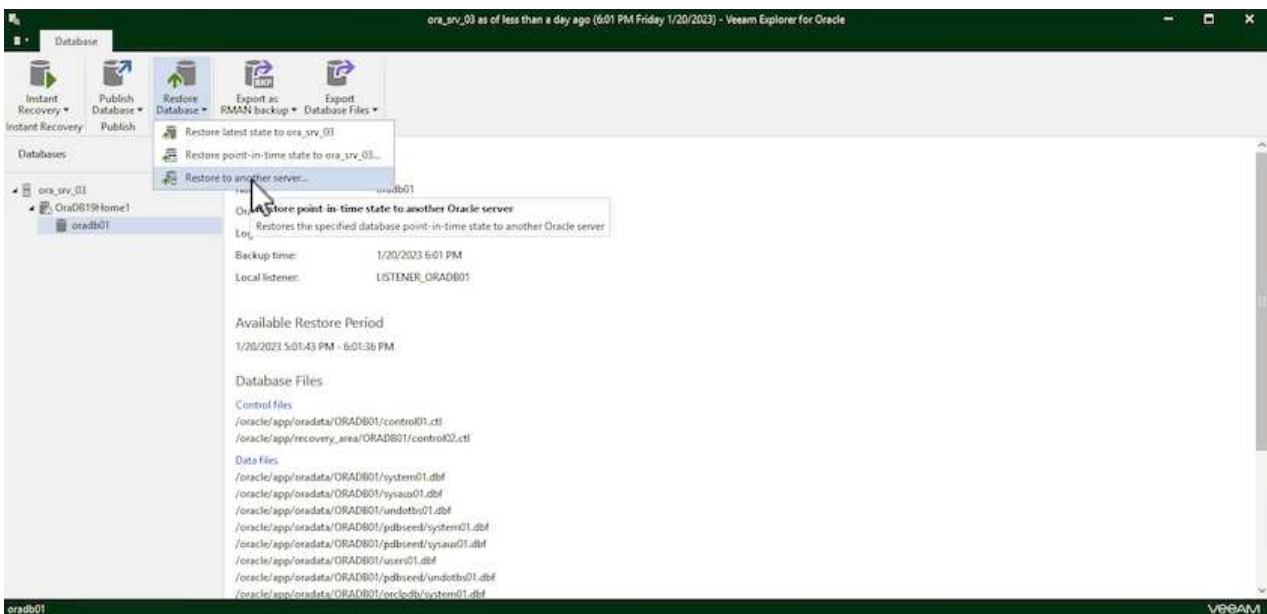


3. 如果需要、输入\*恢复原因\*、然后在摘要页面上、单击\*浏览\*按钮以启动Veeam Explorer for Oracle。





4. 在Veeam Explorer中展开数据库实例列表、单击要还原的数据库、然后从顶部的\*还原数据库\*下拉菜单中选择\*还原到另一台服务器...\*。



5. 在“恢复向导”中，指定要从中恢复的还原点，然后单击“下一步”。



Restore Wizard

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  
1/20/2023

6:01 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

- 指定数据库将还原到的目标服务器和帐户凭据，然后单击\*Next\*。

Restore Wizard

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

- 最后，指定数据库文件的目标位置，然后单击\*Restore\*按钮开始恢复过程。

## 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

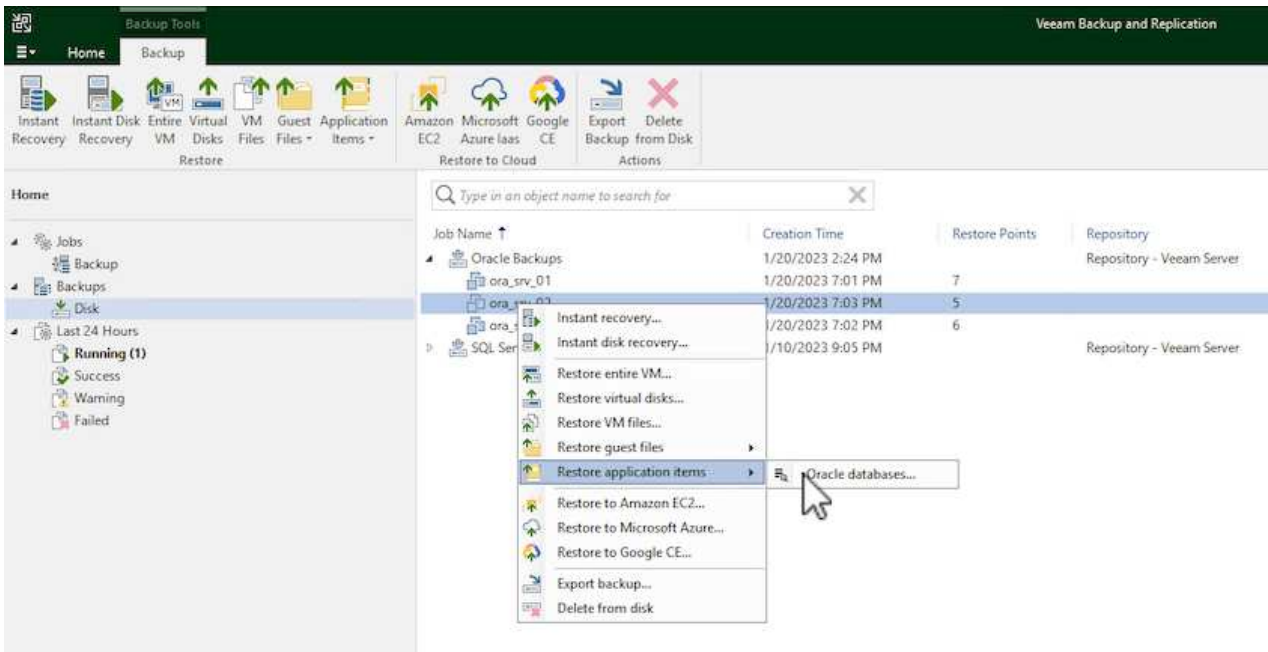
Cancel

8. 数据库恢复完成后、请检查Oracle数据库是否在服务器上正确启动。

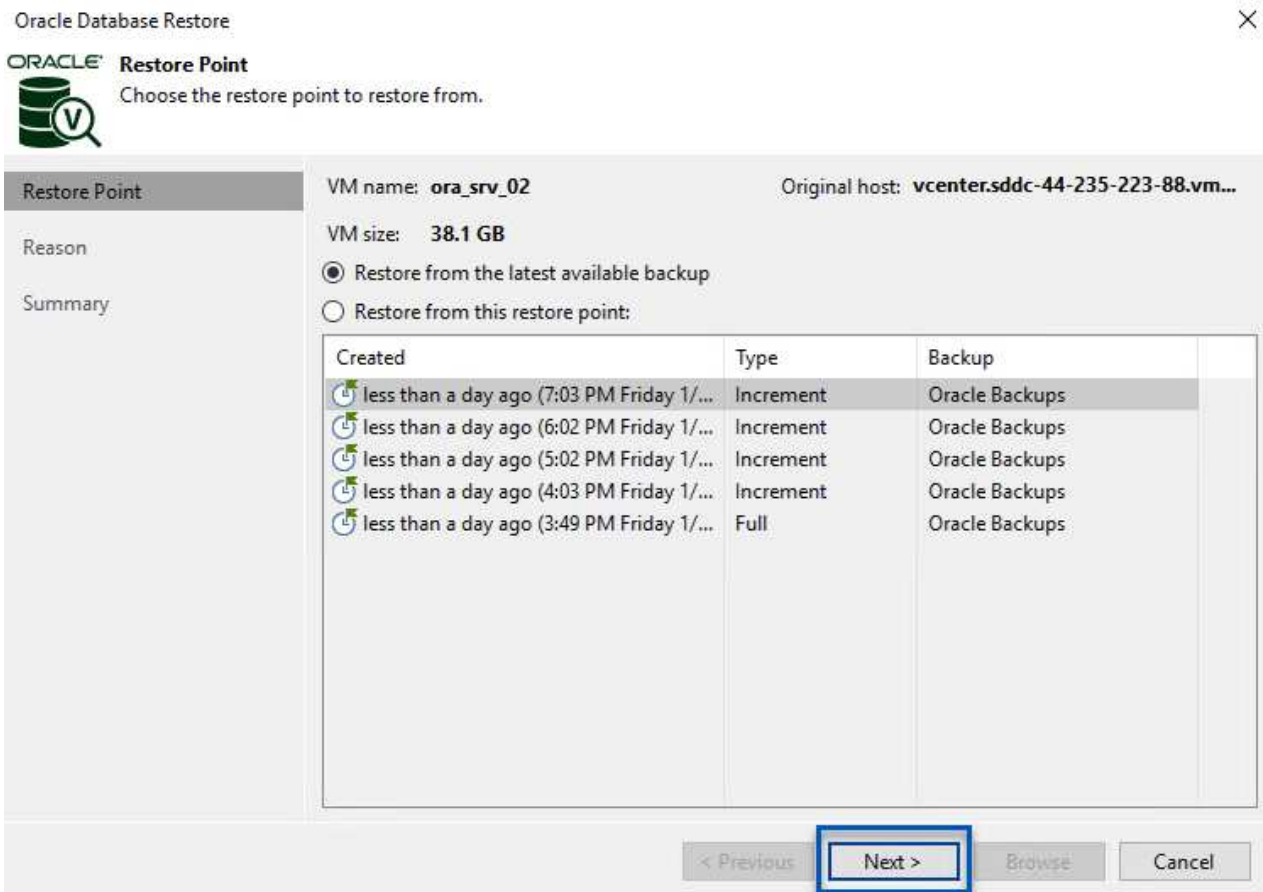
将Oracle数据库发布到备用服务器

在本节中、数据库会发布到备用服务器、以便在不启动完全还原的情况下快速访问。

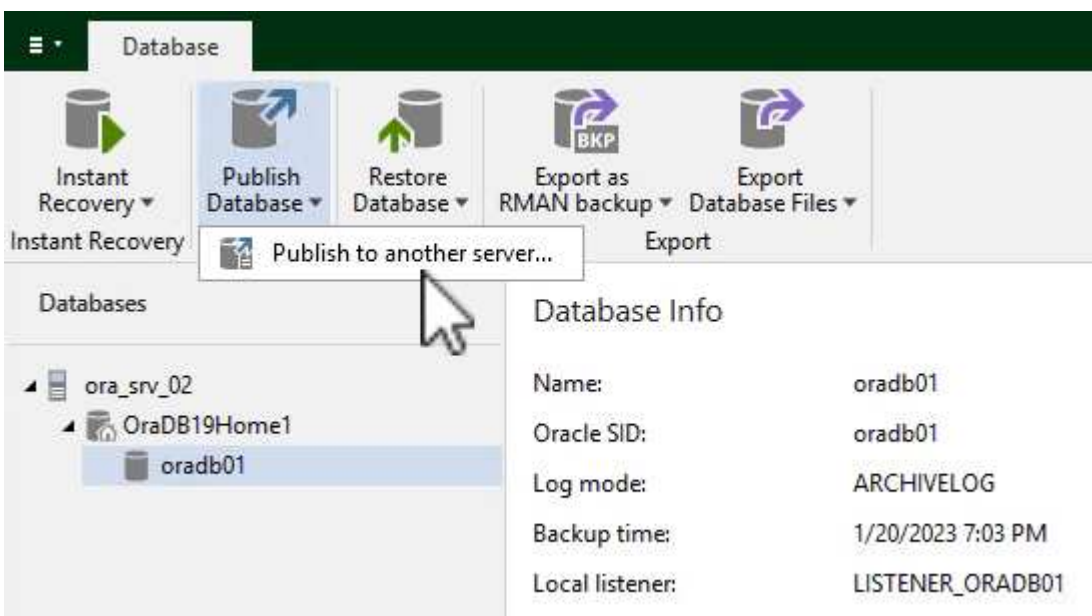
- 1. 在Veeam Backup and Replication控制台中、导航到Oracle备份列表、右键单击某个服务器并选择\*还原应用程序项\*、然后选择\* Oracle数据库... \*。



- 2. 在Oracle数据库恢复向导中、从列表选择一个还原点，然后单击\*Next\*。



3. 如果需要、输入\*恢复原因\*、然后在摘要页面上、单击\*浏览\*按钮以启动Veeam Explorer for Oracle。
4. 在Veeam Explorer中展开数据库实例列表、单击要还原的数据库、然后从顶部的\*发布数据库\*下拉菜单中选择\*发布到另一台服务器...\*。



5. 在发布向导中、指定发布数据库的还原点、然后单击\*Next\*。
6. 最后、指定目标Linux文件系统位置、然后单击\*发布\*开始恢复过程。

## Specify Oracle settings

☒ Restore to the original location☐ Restore to a different location:

Oracle Home: /oracle/app/product/19c

Browse...

Global Database Name: oradb01.demozone.com

Oracle SID: oradb01

Back

Publish

Cancel

7. 发布完成后、登录到目标服务器并运行以下命令、以确保数据库正在运行：

```
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 |


```

## 结论

VMware Cloud是一个功能强大的平台、用于运行业务关键型应用程序和存储敏感数据。对于依赖VMware Cloud的企业来说、安全的数据保护解决方案 对于确保业务连续性并帮助抵御网络威胁和数据丢失至关重要。通过选择可靠且强大的数据保护解决方案、企业可以确信无论什么情况、其关键数据都是安全可靠的。

本文档中提供的使用情形重点介绍经验证的数据保护技术、这些技术重点介绍了NetApp、VMware和Veeam之间的集成。在AWS中、FSx for ONTAP 可用作VMware Cloud的补充NFS数据存储库、并可用于所有虚拟机和应用程序数据。Veeam Backup & Replication是一款全面的数据保护解决方案、旨在帮助企业改进、自动化和简化备份和恢复流程。Veeam可与FSx for ONTAP 上托管的iSCSI备份目标卷结合使用、为驻留在VMware Cloud中的应用程序数据提供安全且易于管理的数据保护解决方案。

## 追加信息

要详细了解此解决方案 中提供的技术、请参阅以下追加信息。

- ["FSx for ONTAP 用户指南"](#)
- ["Veeam帮助中心技术文档"](#)
- ["VMware Cloud on AWS支持。注意事项和限制"](#)

# TR-4955：使用适用于ONTAP 和VMC的FSX进行灾难恢复(AWS VMware Cloud)

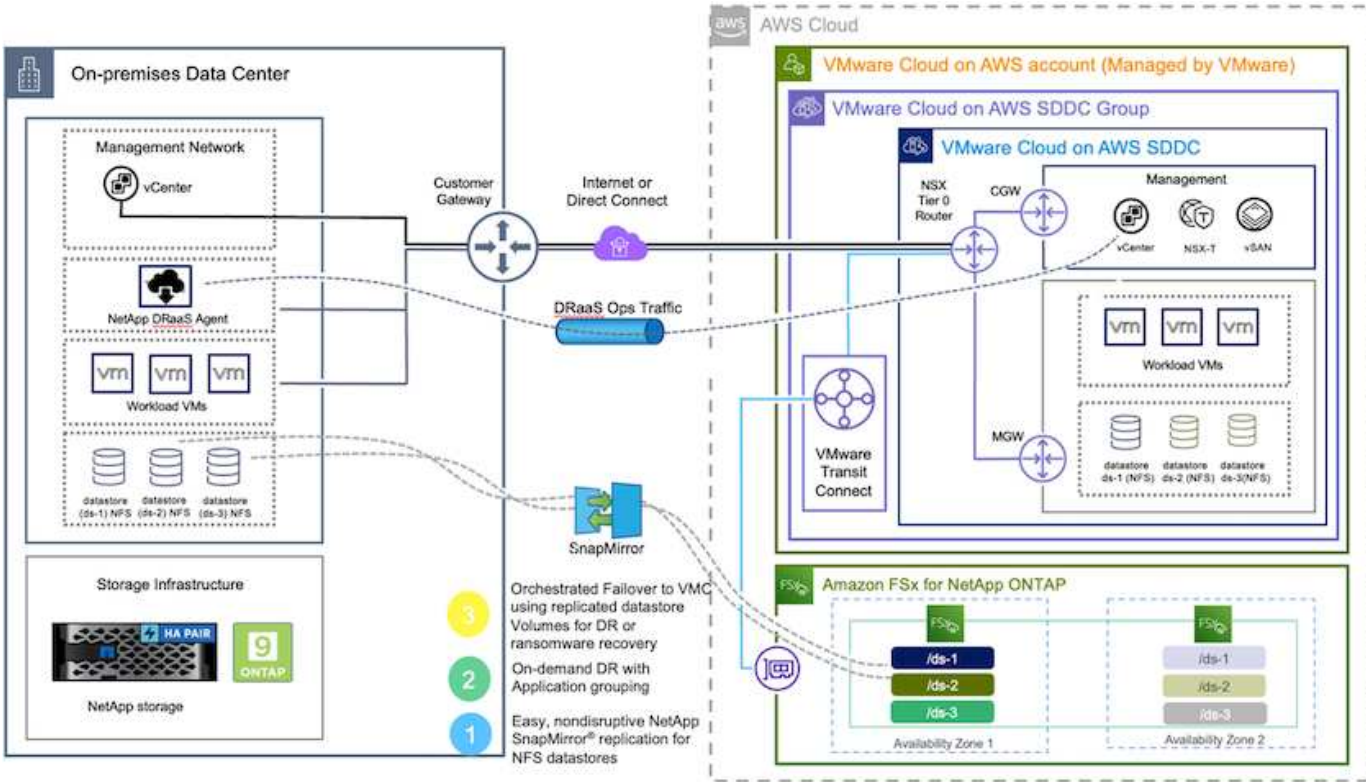
NetApp 公司 Niyaz Mohamed



概述

将灾难恢复到云是一种弹性且经济高效的方式、可保护工作负载免受站点中断和数据损坏事件(例如勒索软件)的影响。借助NetApp SnapMirror技术、可以将内部VMware工作负载复制到在AWS中运行的FSX for ONTAP。

可以使用灾难恢复协调器(DRO; 具有UI的脚本式解决方案)无缝恢复从内部复制到FSX for ONTAP 的工作负载。DRO可通过VM注册到VMC自动从SnapMirror级别恢复到直接在NSX-T上进行的网络映射所有VMC环境都包含此功能。



入门

在AWS上部署和配置VMware Cloud

"基于 AWS 的 VMware Cloud" 为AWS生态系统中基于VMware的工作负载提供云原生体验。每个VMware软件定义的数据中心(SDDC)均在Amazon Virtual Private Cloud (VPC)中运行、并提供完整的VMware堆栈(包括vCenter Server)、NSX-T软件定义的网络连接、vSAN软件定义的存储以及一个或多个ESXi主机、这些主机可为工作负载提供计算和存储资源。要在AWS上配置VMC环境、请按照此处的步骤进行操作 ["链接"](#)。此外、还可以使用引导灯集群进行灾难恢复。



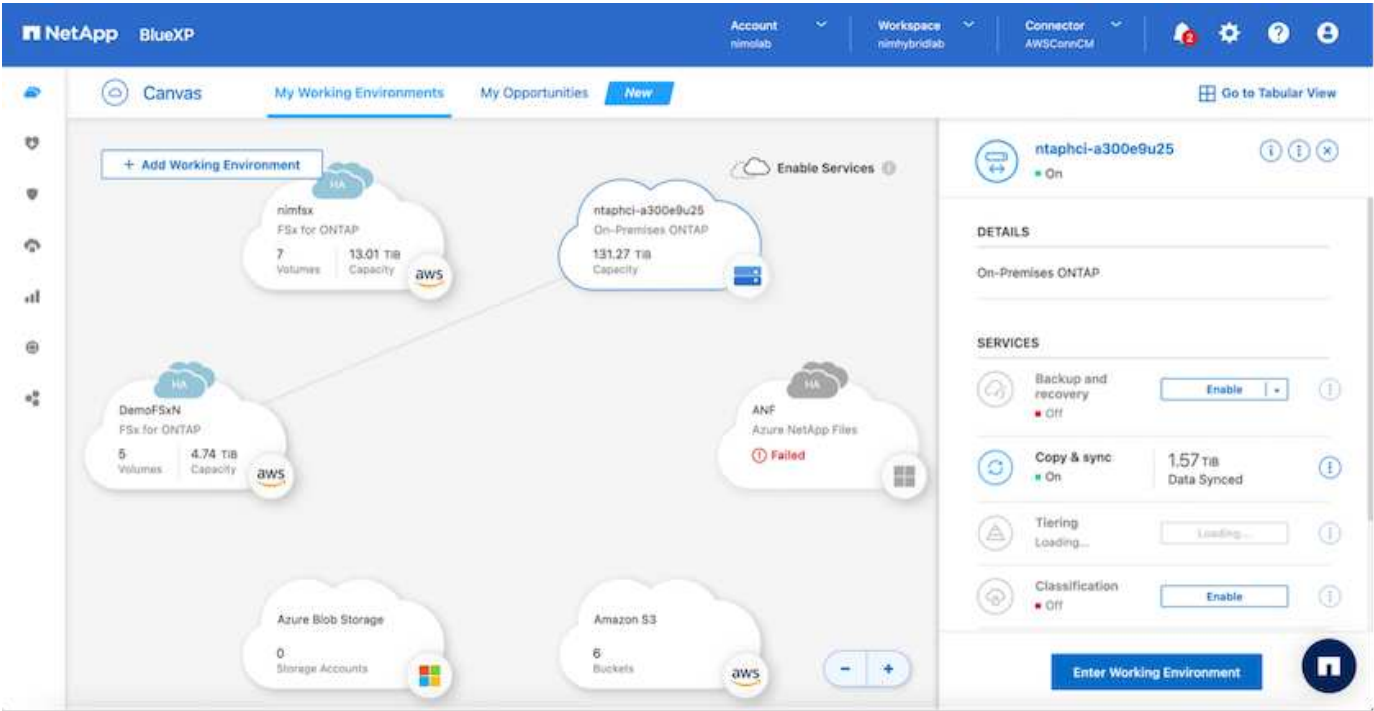
在初始版本中、DRO支持现有的试用集群。即将发布的版本将提供按需创建SDDC的功能。

为ONTAP 配置和配置FSX

适用于NetApp ONTAP 的Amazon FSX是一种完全托管的服务、可提供基于常见NetApp ONTAP 文件系统构建的高度可靠、可扩展、高性能和功能丰富的文件存储。请按照此处的步骤进行操作 ["链接"](#)。为ONTAP 配置和配置FSX。

为适用于ONTAP 的FSX部署和配置SnapMirror

下一步是使用NetApp BlueXP并发现在AWS实例上为ONTAP 配置的FSX、并以适当的频率将所需的数据存储库卷从内部环境复制到适用于ONTAP 的FSX并保留NetApp Snapshot副本：



按照此链接中的步骤配置BlueXP。您也可以使用NetApp ONTAP 命令行界面计划通过此链接进行复制。



SnapMirror关系是前提条件、必须事先创建。

DRO安装

要开始使用DRO、请在指定EC2实例或虚拟机上使用Ubuntu操作系统、以确保满足前提条件。然后安装软件包。

前提条件

- 确保与源和目标vCenter以及存储系统建立连接。
- 如果使用的是DNS名称、则应进行DNS解析。否则、您应使用vCenter和存储系统的IP地址。
- 创建具有root权限的用户。您也可以将sudo与EC2实例结合使用。

操作系统要求

- Ubuntu 20.04 (LTS)、至少具有2 GB和4个vCPU
- 指定代理VM上必须安装以下软件包：
  - Docker
  - Docker构成
  - JQ



更改上的权限 `docker.sock`: `sudo chmod 666 /var/run/docker.sock`。



。 `deploy.sh` 此脚本将执行所有必需的前提条件。

## 安装软件包

1. 在指定虚拟机上下载安装包：

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



该代理可以安装在内部环境中、也可以安装在AWS VPC中。

2. 解压缩软件包、运行部署脚本、然后输入主机IP (例如10.10.10.10)。

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

3. 导航到目录并按如下所示运行Deploy脚本：

```
sudo sh deploy.sh
```

4. 使用以下命令访问UI：

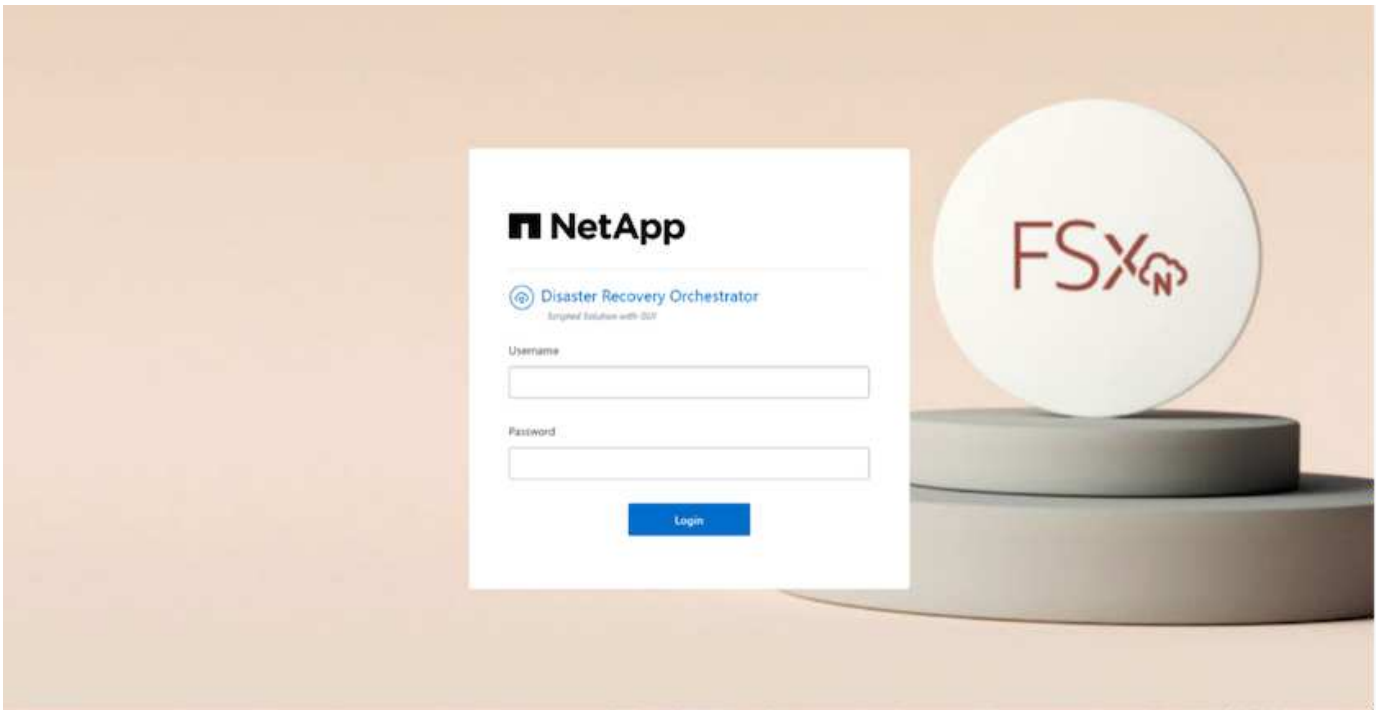
```
https://<host-ip-address>
```

使用以下默认凭据：

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



可以使用"更改密码"选项更改密码。



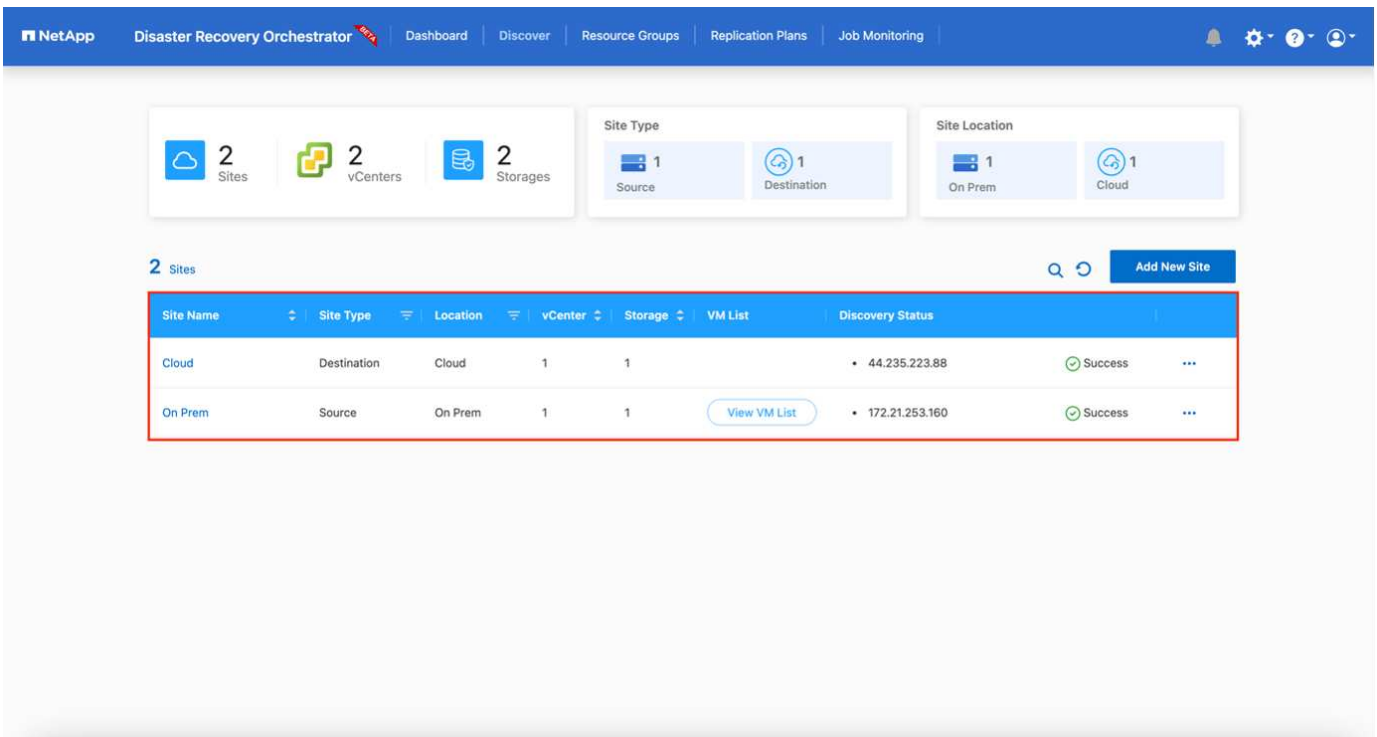
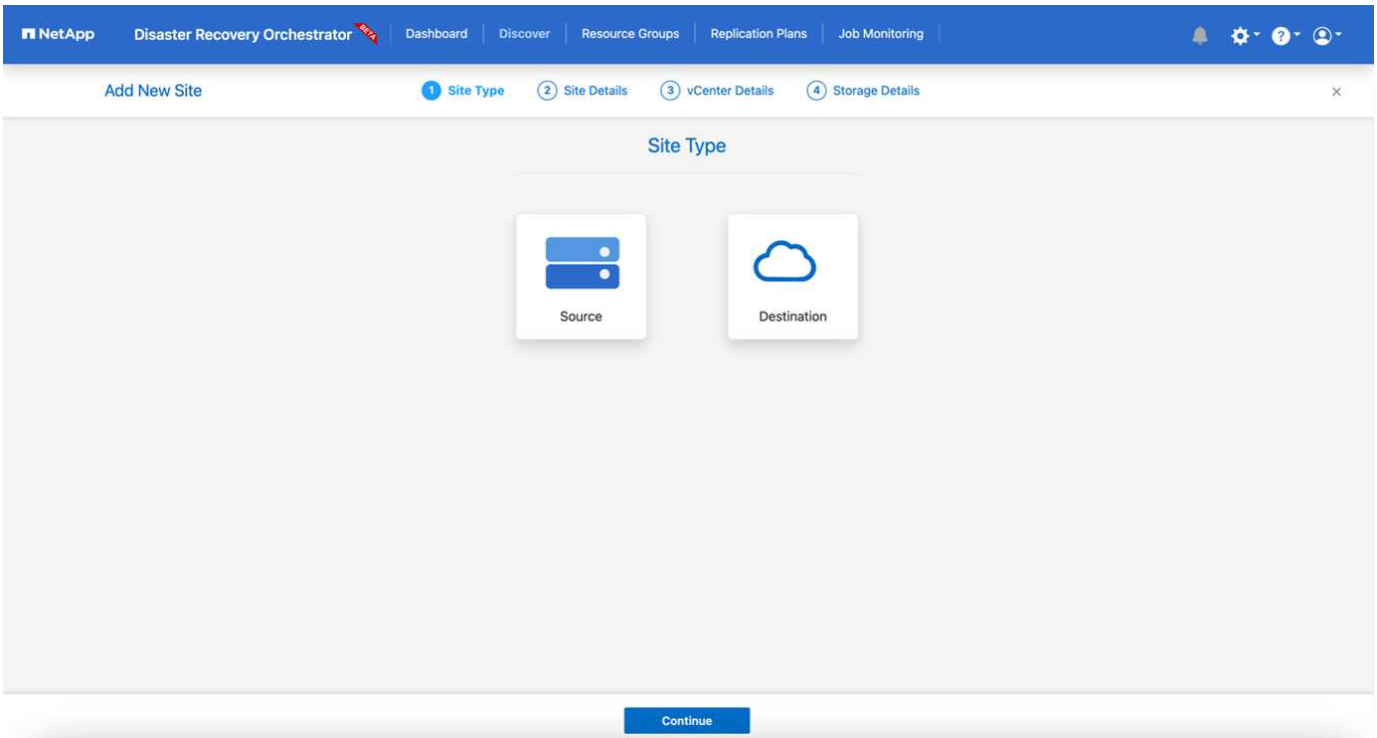
## DRO配置

正确配置适用于ONTAP 的FSX和VMC之后、您可以开始配置DRO、以便使用适用于ONTAP 的FSX上的只读SnapMirror副本自动将内部工作负载恢复到VMC。

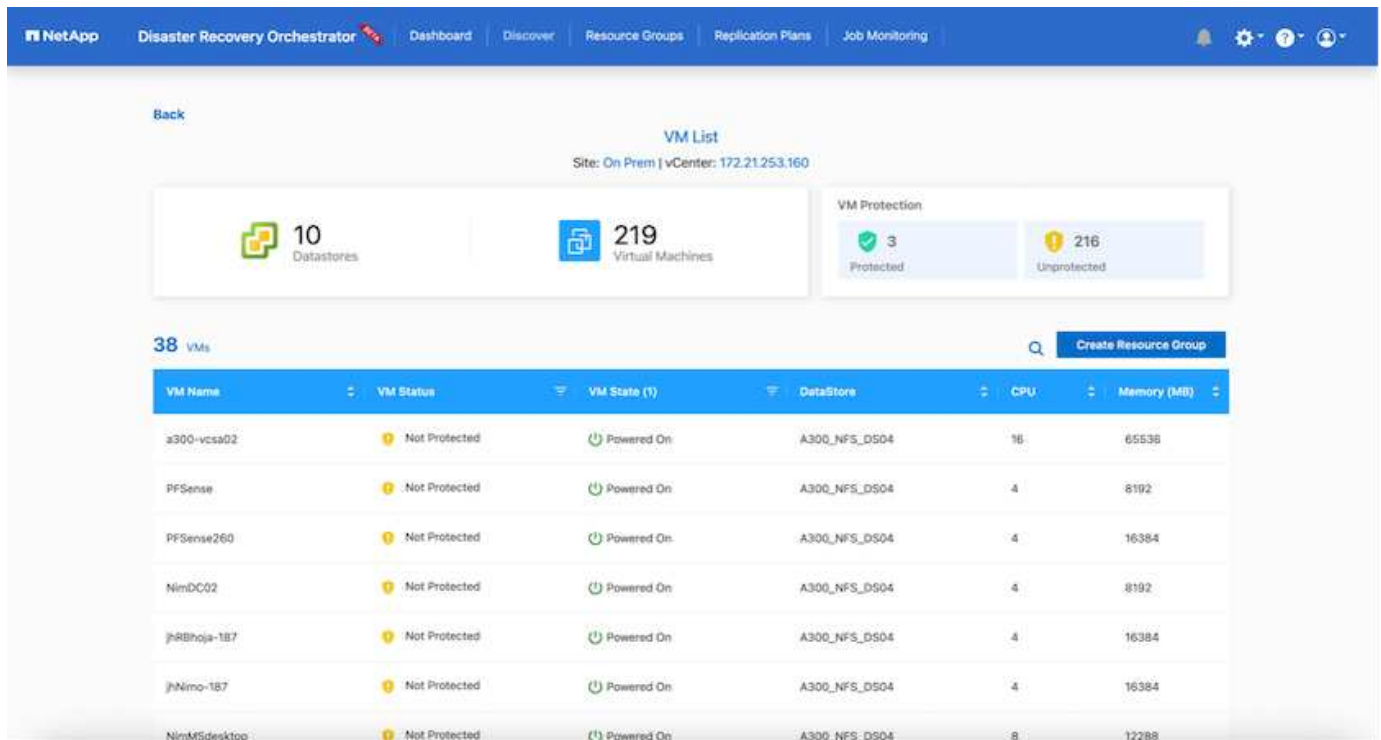
NetApp建议在AWS中部署DRO代理、并将其部署到部署了FSX for ONTAP 的同一VPC上(也可以通过对等连接)。这样、DRO代理便可通过网络与内部组件以及适用于ONTAP 的FSX和VMC资源进行通信。

第一步是发现内部资源和云资源(vCenter和存储)并将其添加到DRO中。在支持的浏览器中打开DRO、并使用默认用户名和密码(admin/admin)以及添加站点。也可以使用发现选项添加站点。添加以下平台：

- 内部部署
  - 内部vCenter
  - ONTAP 存储系统
- 云
  - VMC vCenter
  - 适用于 ONTAP 的 FSX



添加后、DRO将执行自动发现、并显示具有从源存储到适用于ONTAP 的FSX的相应SnapMirror副本的VM。DRO会自动检测VM使用的网络和端口组并对其进行填充。



下一步是将所需的VM分组到功能组中、以用作资源组。

## 资源分组

添加平台后、您可以将要恢复的VM分组到资源组中。使用DRO资源组、您可以将一组依赖虚拟机分组到逻辑组中、这些逻辑组包含启动顺序、启动延迟以及可在恢复时执行的可选应用程序验证。

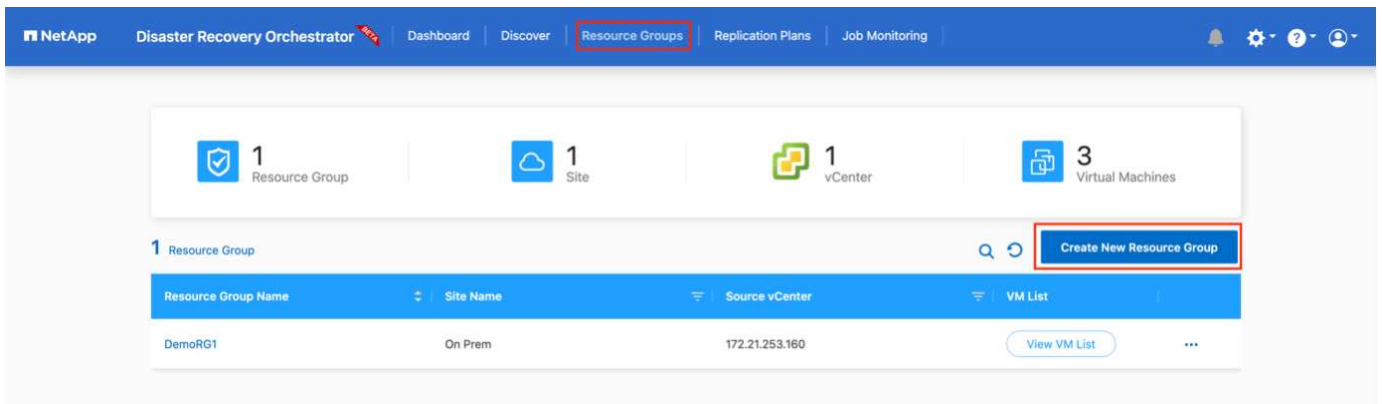
要开始创建资源组、请完成以下步骤：

1. 访问\*资源组\*、然后单击\*创建新资源组\*。
2. 在\*新建资源组\*下、从下拉列表中选择源站点、然后单击\*创建\*。
3. 提供\*资源组详细信息\*并单击\*继续\*。
4. 使用搜索选项选择相应的VM。
5. 选择选定虚拟机的启动顺序和启动延迟(秒)。通过选择每个VM并设置其优先级来设置启动顺序。所有VM的默认值均为3。

选项如下：

1—第一个启动的虚拟机 3—默认值 5—最后一个启动的虚拟机

6. 单击\*创建资源组\*。

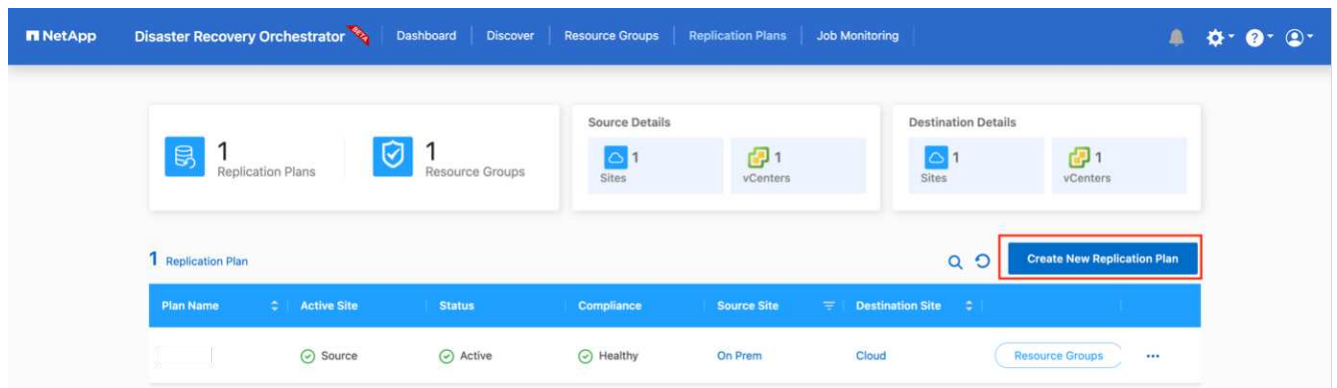


## 复制计划

您需要制定计划、以便在发生灾难时恢复应用程序。从下拉列表中选择源和目标vCenter平台、然后选择要包含在此计划中的资源组、以及应用程序应如何还原和启动的分组(例如、域控制器、第1层、第2层等)。此类计划有时也称为蓝图。要定义恢复计划、请导航到\*复制计划\*选项卡、然后单击\*新建复制计划\*。

要开始创建复制计划、请完成以下步骤：

1. 访问\*复制计划\*、然后单击\*创建新复制计划\*。



2. 在\*新复制计划\*下、为计划提供一个名称、并通过选择源站点、关联的vCenter、目标站点和关联的vCenter来添加恢复映射。

NetApp Disaster Recovery Orchestrator

Dashboard | Discover | Resource Groups | **Replication Plans** | Job Monitoring

Create New Replication Plan

1 Replication Plan and Site Details | 2 Select Resource Groups | 3 Set Execution Order | 4 Set VM Details

### Replication Plan Details

Plan Name

Recovery Mapping

Source Site: Select Source Site

Destination Site: Select Destination Site

Source vCenter: Select Source vCenter

Destination vCenter: Select Destination vCenter

**Pre-requisite - You must configure SnapMirror relationships between the source site and target site to create successful replication plan**

Continue

3. 恢复映射完成后、选择集群映射。

NetApp Disaster Recovery Orchestrator

Dashboard | Discover | Resource Groups | **Replication Plans** | Job Monitoring

Create New Replication Plan

1 Replication Plan and Site Details | 2 Select Resource Groups | 3 Set Execution Order | 4 Set VM Details

### Replication Plan Details

Plan Name: DemoRP

Recovery Mapping

Source Site: On Prem

Destination Site: Cloud

Source vCenter: 172.21.253.160

Destination vCenter: 44.235.223.88

Cluster Mapping

Source Site Resource	Destination Site Resource	
TempCluster	Cluster-1	Add

Source Resource	Destination Resource	
A300-Cluster01	Cluster-1	Delete

Continue

4. 选择\*资源组详细信息\*、然后单击\*继续\*。

5. 设置资源组的执行顺序。使用此选项可以选择存在多个资源组时的操作顺序。

6. 完成后、选择指向相应网段的网络映射。应已在VMC中配置这些区块、因此请选择适当的区块以映射虚拟机。

7. 根据VM的选择、系统会自动选择数据存储库映射。



SnapMirror处于卷级别。因此、所有VM都会复制到复制目标。确保选择属于数据存储库的所有VM。如果未选择这些虚拟机、则仅会处理属于复制计划的虚拟机。

Resource Group Name	Execution Order
DemoRG1	3

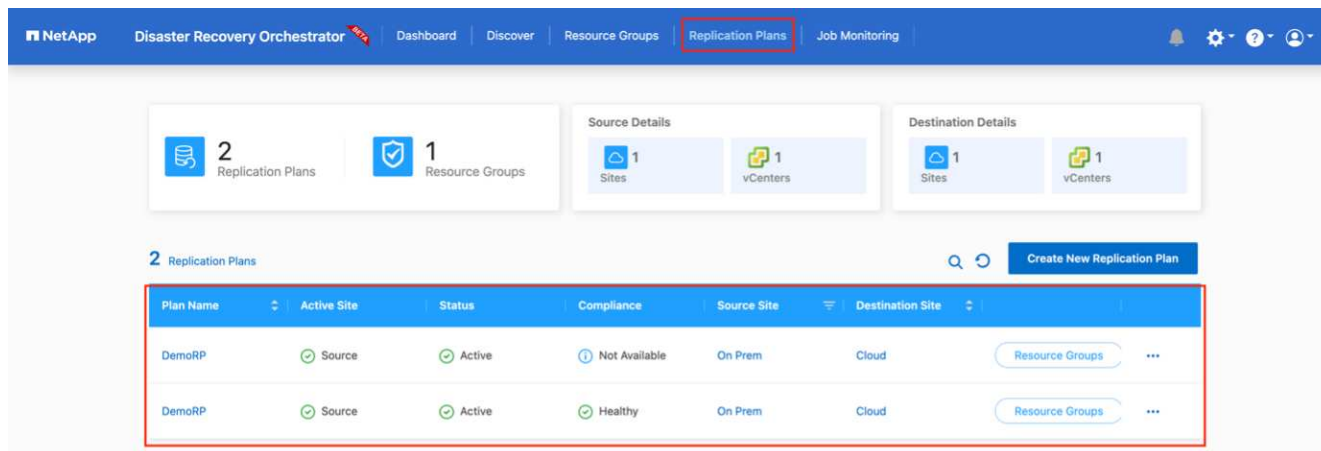
Source Resource	Destination Resource	
VLAN 3375	sddc-cgw-network-1	Delete

Source DataStore	Destination Volume
DRO_Mini	DRO_Mini_copy

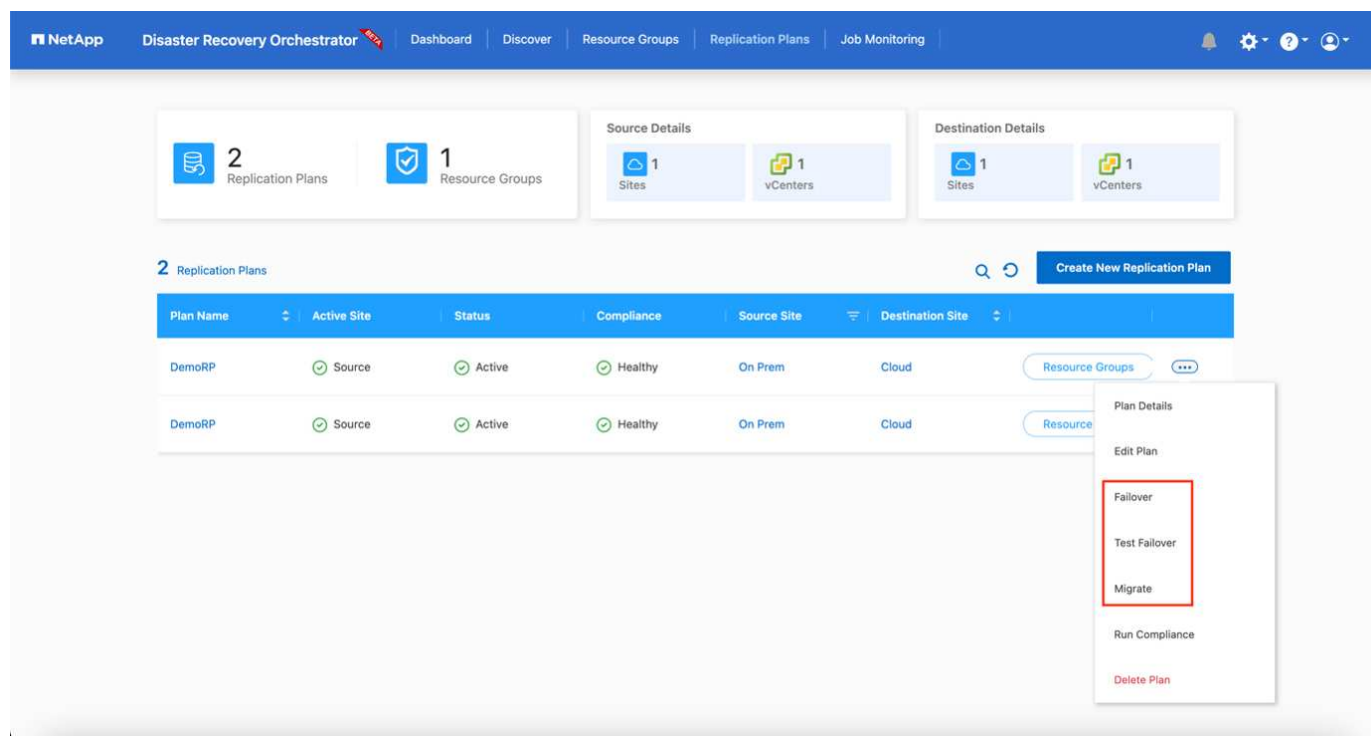
- 在VM详细信息下、您可以选择调整VM的CPU和RAM参数大小；在将大型环境恢复到较小的目标集群或执行灾难恢复测试而无需配置一对一物理VMware基础架构时、这会非常有用。此外、您还可以修改资源组中所有选定虚拟机的启动顺序和启动延迟(秒)。如果需要对资源组启动顺序选择期间选择的启动顺序进行任何更改、还可以选择修改启动顺序。默认情况下、系统会使用在选择资源组期间选择的启动顺序；但是、在此阶段可以执行任何修改。

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

- 单击\*创建复制计划\*。



创建复制计划后、可以根据需要使用故障转移选项、test-failover选项或migrate选项。在故障转移和测试-故障转移选项期间、将使用最新的SnapMirror Snapshot副本、或者可以从时间点Snapshot副本中选择特定的Snapshot副本(按照SnapMirror的保留策略)。如果您遇到勒索软件等损坏事件、而最新副本已被泄露或加密、则时间点选项可能会非常有用。DRO显示所有可用时间点。要使用复制计划中指定的配置触发故障转移或测试故障转移、可以单击\*故障转移\*或\*测试故障转移\*。





## Failover Details



### Volume Snapshot Details

- ☒ Use latest snapshot ⓘ
- ☐ Select specific snapshot ⓘ

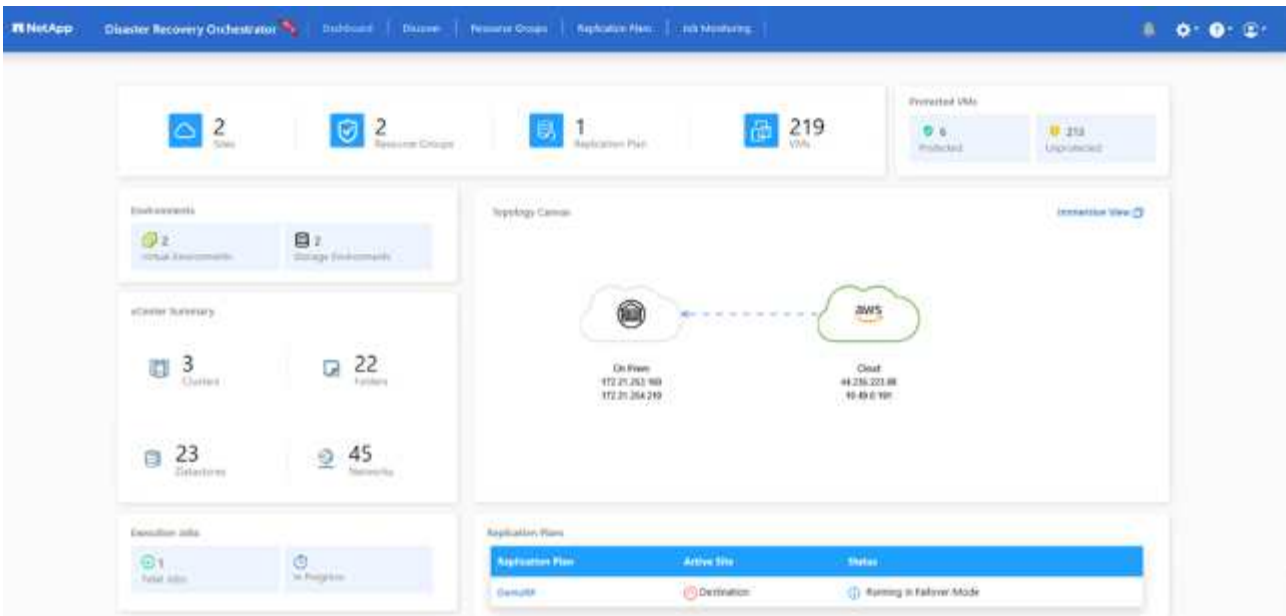
Start Failover

可以在任务菜单中监控复制计划：

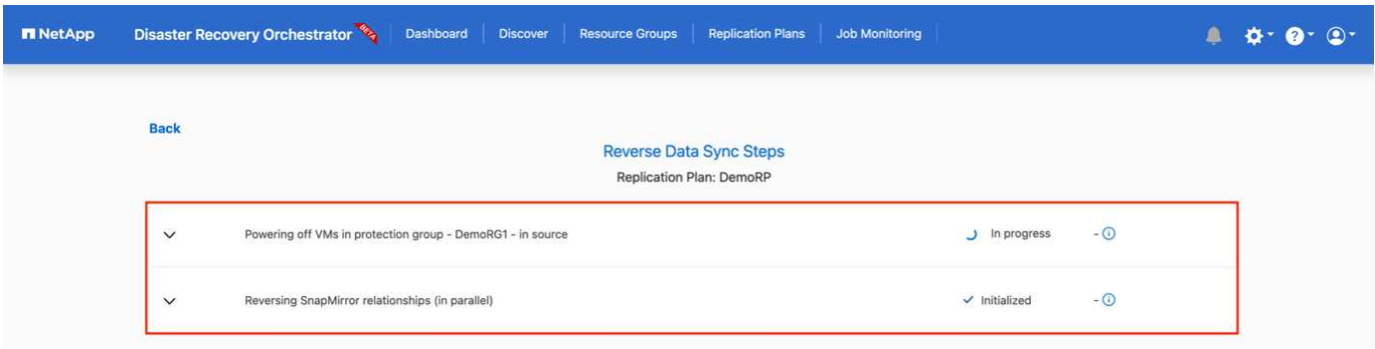
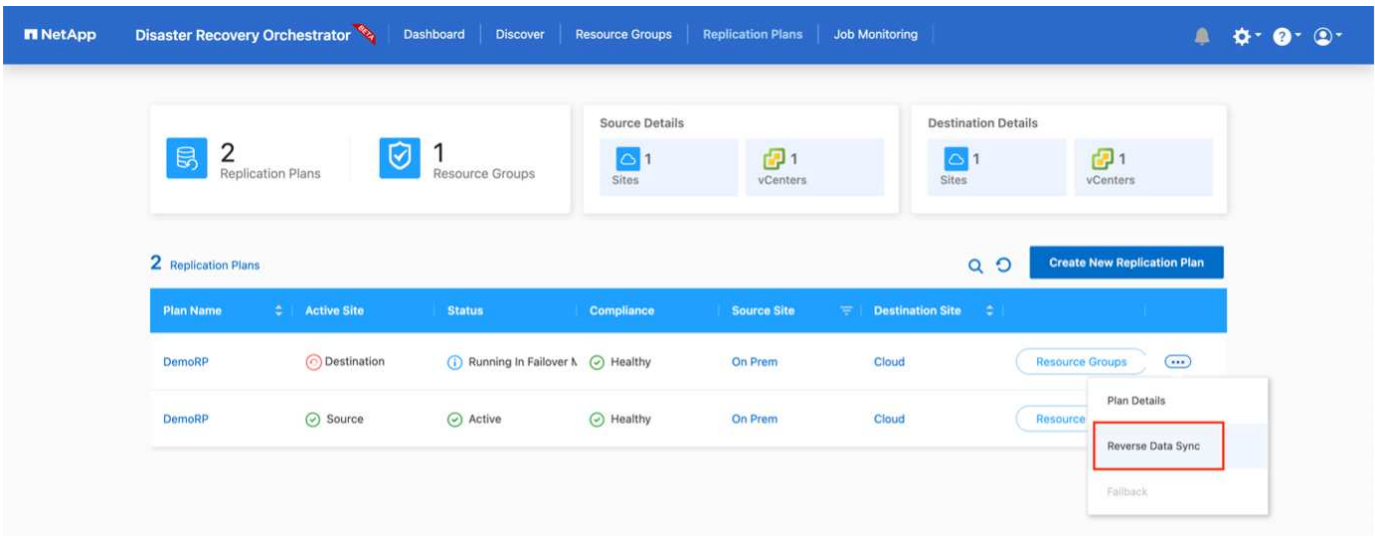
The screenshot shows the NetApp Disaster Recovery Orchestrator interface. The top navigation bar includes 'NetApp', 'Disaster Recovery Orchestrator', and several menu items: 'Dashboard', 'Discover', 'Resource Groups', 'Replication Plans', and 'Job Monitoring' (which is highlighted with a red box). On the right side of the navigation bar are icons for notifications, settings, help, and user profile. Below the navigation bar, the main content area has a 'Back' link on the left. In the center, there is a section titled 'Failover Steps' with a subtitle 'Replication Plan: DemoRP' (this section is also highlighted with a red box). Below this title is a table showing the progress of five failover steps, each with a dropdown arrow on the left, a description, a status icon and text, and a duration with an information icon.

▼	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 ⓘ

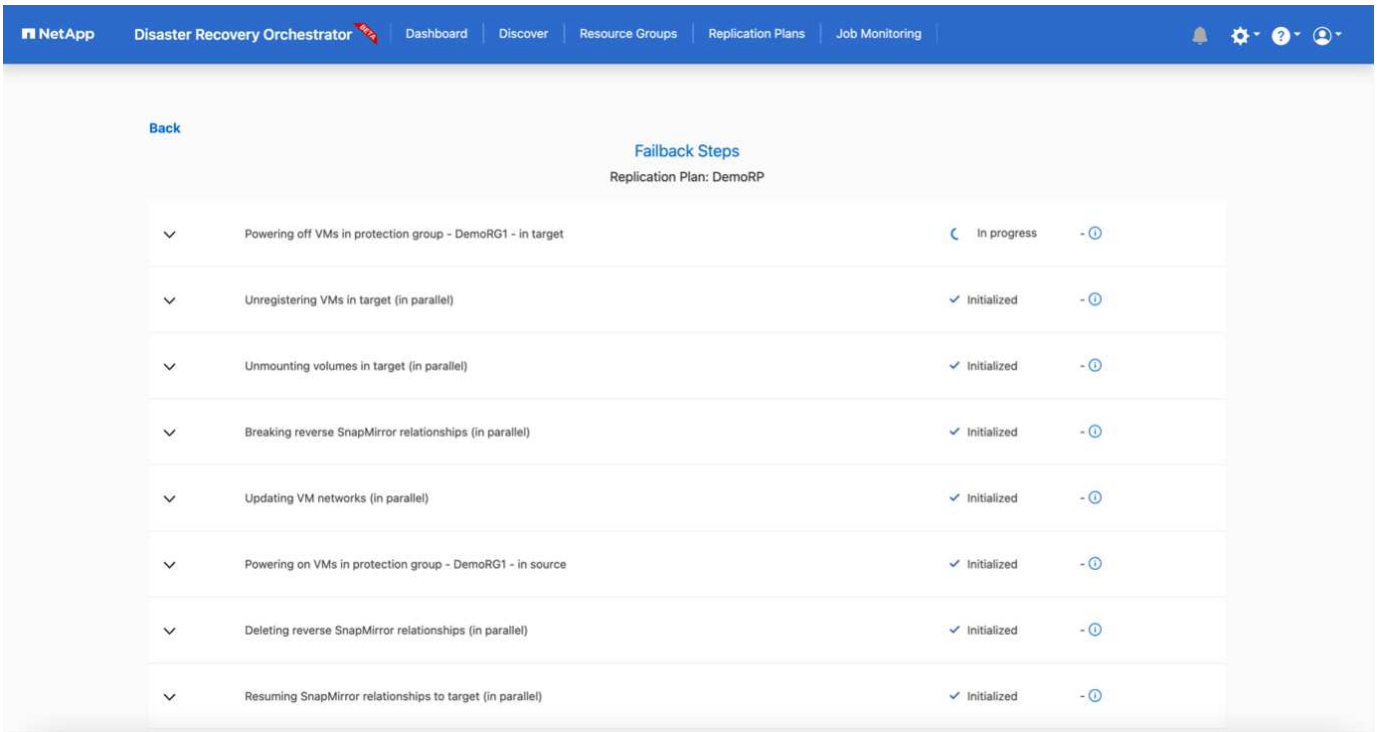
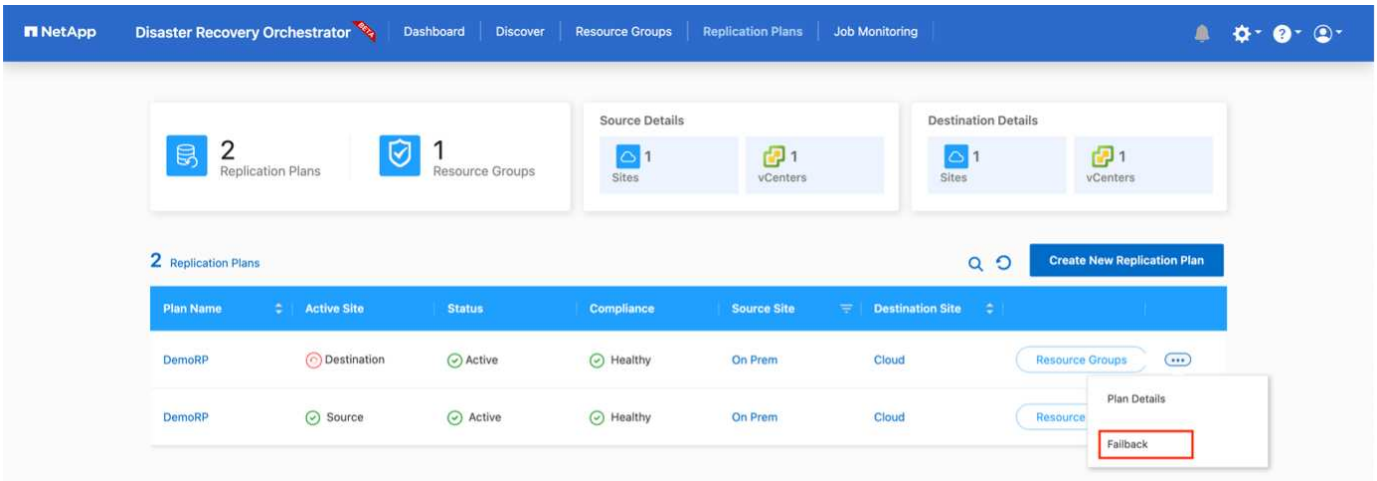
触发故障转移后、可以在VMC vCenter中看到恢复的项目(VM、网络、数据存储空间)。默认情况下、VM将恢复到工作负载文件夹。



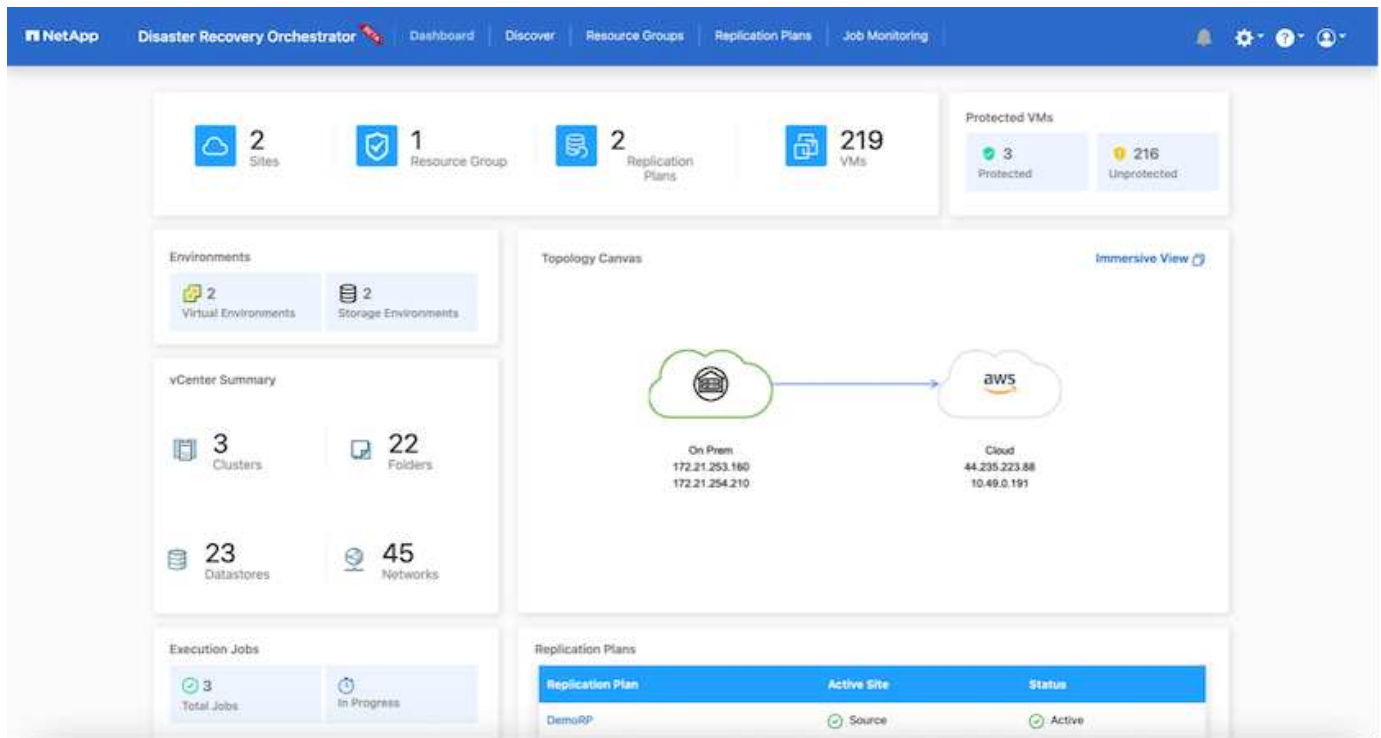
可以在复制计划级别触发故障恢复。对于测试故障转移、可以使用卸载选项回滚更改并删除FlexClone关系。与故障转移相关的故障恢复过程分为两步。选择复制计划并选择\*反向数据同步\*。



完成后、您可以触发故障恢复以移回原始生产站点。



在NetApp BlueXP中、我们可以看到相应卷(已映射到VMC的读写卷)的复制运行状况已中断。在测试故障转移期间、DRO不会映射目标卷或副本卷。相反、它会为所需的SnapMirror (或Snapshot)实例创建一个FlexClone副本、并公开FlexClone实例、这样不会占用适用于ONTAP 的FSX的额外物理容量。此过程可确保卷不会被修改、并且即使在灾难恢复测试或鉴别 workflow 期间、副本作业也可以继续执行。此外、此过程还可确保在发生错误或恢复损坏的数据时、可以清理恢复过程、而不会造成副本被销毁的风险。



## 勒索软件恢复

从勒索软件中恢复可能是一项艰巨的任务。具体而言、IT组织很难确定安全的返回点、一旦确定、就很难保护已恢复的工作负载、防止再次发生攻击、例如、休眠的恶意软件或容易受到攻击的应用程序。

DRO可帮助您从任何可用时间点恢复系统、从而解决这些问题。您还可以将工作负载恢复到正常运行且彼此隔离的网络、以便应用程序可以在不受北-南流量影响的位置彼此运行和通信。这样、您的安全团队就可以安全地进行取证、并确保没有隐藏或休眠的恶意软件。

## 优势

- 使用高效且具有故障恢复能力的SnapMirror复制。
- 使用Snapshot副本保留功能恢复到任何可用时间点。
- 完全自动化执行从存储、计算、网络 and 应用程序验证步骤中恢复成百上千个VM所需的所有步骤。
- 使用ONTAP FlexClone技术执行工作负载恢复、方法不会更改复制的卷。
  - 避免卷或Snapshot副本发生数据损坏的风险。
  - 在灾难恢复测试 workflow 期间避免复制中断。
  - 将灾难恢复数据与云计算资源一起用于灾难恢复以外的工作流、例如DevTest、安全测试、修补或升级测试以及修复测试。
- CPU和RAM优化、可通过恢复到较小的计算集群来帮助降低云成本。

## 使用Veeam Replication和FSx for ONTAP将灾难恢复到AWS上的VMware Cloud

作者：Niyaz Mohamed - NetApp解决方案工程部



5. 灾难事件完成且主站点启动后、切换回生产VM。

将**Veeam VM**复制到适用于**ONTAP**数据存储库的**VMC**和**FSx**的前提条件

1. 确保Veeam Backup & Replication备份VM已连接到源vCenter以及AWS SDDC集群上的目标VMware云。
2. 备份服务器必须能够解析短名称并连接到源和目标vCenter。
3. 适用于ONTAP数据存储库的目标FSx必须具有足够的可用空间来存储已复制VM的VMDK

对于追加信息、请参阅介绍的"注意事项和限制" ["此处"](#)。

部署详细信息

## 第1步：复制VM

Veeam Backup & Replication利用VMware vSphere快照功能、在复制期间、Veeam Backup & Replication会请求VMware vSphere创建VM快照。VM快照是VM的时间点副本、其中包括虚拟磁盘、系统状态、配置等。Veeam Backup & Replication使用快照作为复制数据源。

要复制VM、请执行以下步骤：

1. 打开Veeam Backup & Replication Console。
2. 在主页视图中、选择复制作业>虚拟机> VMware vSphere。
3. 指定作业名称并选中相应的高级控制复选框。单击下一步。
  - 如果内部和AWS之间的连接带宽受限、请选中副本传播复选框。
  - 如果AWS SDDC上VMware Cloud上的区块与内部站点网络不匹配、请选中网络重新映射(适用于具有不同网络的AWS VMC站点)复选框。
  - 如果内部生产站点中的IP地址方案与AWS VMC站点中的方案不同、请选中"副本重新IP (适用于具有不同IP地址方案的灾难恢复站点)"复选框。

[灾难恢复Veeam FSx版本2] | *dr-veeam-fsx-image2.png*

4. 在\*虚拟机\*步骤中、选择需要复制到连接到AWS SDDC上的VMware Cloud的FSx for ONTAP数据存储库的VM。可以将虚拟机放置在vSAN上、以填满可用的vSAN数据存储库容量。在指示灯集群中、3节点集群的可用容量将受到限制。其余数据可以复制到FSx for ONTAP数据存储库。单击\*Add\*，然后在\*Add Object\*窗口中选择所需的VM或VM容器，然后单击\*Add\*。单击 \* 下一步 \*。

[灾难恢复Veeam FSx版本3] | *dr-veeam-fsx-image3.png*

5. 之后、选择目标作为AWS SDDC上的VMware Cloud集群/主机、并为VM副本选择相应的资源池、VM文件夹和FSx for ONTAP数据存储库。然后单击\*Next\*。

[灾难恢复Veeam FSx版本4] | *dr-veeam-fsx-image4.png*

6. 在下一步中、根据需要创建源虚拟网络与目标虚拟网络之间的映射。

[灾难恢复Veeam FSx版本5] | *dr-veeam-fsx-image5.png*

7. 在\*作业设置\*步骤中，指定要存储VM副本元数据、保留策略等的备份存储库。
8. 在“数据传输”步骤中更新\*Source\*和\*Target\*代理服务器，保留“自动\*选择”(默认)并保持“\*直接”选项处于选中状态，然后单击“下一步”。
9. 在\*Guest Processing\*步骤中，根据需要选择\*Enable application-aware processing\*选项。单击 \* 下一步 \*。

[灾难恢复Veeam FSx版本6] | *dr-veeam-fsx-image6.png*

10. 选择复制计划以定期运行复制作业。
11. 在向导的\*摘要\*步骤中，查看复制作业的详细信息。要在关闭向导后立即启动作业，请选中\*单击完成时运行作业\*复选框，否则不要选中该复选框。然后单击\*完成\*关闭向导。

[灾难恢复Veeam FSx版本7] | *dr-veeam-fsx-image7.png*

复制作业启动后、目标VMC SDDC集群/主机上将填充具有指定后缀的VM。

[灾难恢复Veeam FSx版本8] | [dr-veeam-fsx-image8.png](#)

有关追加信息for Veeam复制的信息、请参见 ["复制的工作原理"](#)。

## 第2步：创建故障转移计划

初始复制或传播完成后、创建故障转移计划。故障转移计划有助于逐个或以组的形式自动对相关VM执行故障转移。故障转移计划是VM处理顺序(包括启动延迟)的蓝图。故障转移计划还有助于确保关键的相关VM已在运行。

要创建计划、请导航到名为副本的新子部分、然后选择故障转移计划。选择适当的VM。Veeam Backup & Replication将查找最接近此时间点的还原点、并使用它们启动VM副本。



只有在初始复制完成且虚拟机副本处于就绪状态时、才能添加故障转移计划。



在运行故障转移计划时、最多可同时启动10个VM。



在故障转移过程中、源VM不会关闭。

要创建\*故障转移计划\*，请执行以下操作：

1. 在主页视图中，选择\*故障转移计划> VMware vSphere。
2. 接下来、提供计划的名称和问题描述。可以根据需要添加故障转移前和故障转移后脚本。例如、在启动复制的VM之前、请运行一个脚本来关闭VM。

[灾难恢复Veeam FSx版本9] | [dr-veeam-fsx-image9.png](#)

3. 将VM添加到计划中、并修改VM启动顺序和启动延迟、以满足应用程序依赖关系。

[灾难恢复Veeam FSx版本10] | [dr-veeam-fsx-image10.png](#)

有关用于创建复制作业的追加信息、请参见 ["正在创建复制作业"](#)。



### 第3步：运行故障转移计划

在故障转移期间、生产站点中的源VM将切换到灾难恢复站点上的副本。在故障转移过程中、Veeam Backup & Replication会将VM副本还原到所需的还原点、并将所有I/O活动从源VM移至其副本。不仅可以发生在灾难时使用副本、还可以用于模拟灾难恢复演练。在模拟故障转移期间、源VM将保持运行状态。执行完所有必要的测试后、您可以撤消故障转移并恢复正常操作。



确保网络分段到位、以避免灾难恢复期间发生IP冲突。

要启动故障转移计划，只需单击\*故障转移计划\*选项卡，然后右键单击故障转移计划。选择 \* 开始 \*。此操作将使用虚拟机副本的最新还原点进行故障转移。要故障转移到VM副本的特定还原点，请选择\*Start to \*。

[灾难恢复Veeam FSx image11] | *dr-veeam-fsx-image11.png*

[DR Veeam FSx版本12] | *dr-veeam-fsx-image12.png*

VM副本的状态将从"准备就绪"更改为"故障转移"、VM将在AWS SDDC集群/主机上的目标VMware Cloud上启动。

[灾难恢复Veeam FSx版本13.] | *dr-veeam-fsx-image13.png*

故障转移完成后、VM的状态将更改为"故障转移"。

[DR Veeam FSx版本14.] | *dr-veeam-fsx-image14.png*



Veeam Backup & Replication会停止源VM的所有复制活动、直到其副本恢复到就绪状态为止。

有关故障转移计划的详细信息、请参见 ["故障转移计划"](#)。

## 第4步：故障恢复到生产站点

当故障转移计划正在运行时、它会被视为一个中间步骤、需要根据需要最终确定。选项包括：

- 故障恢复到生产环境-切换回原始虚拟机并将虚拟机副本运行期间发生的所有更改传输至原始虚拟机。



执行故障恢复时、只会传输更改、但不会发布更改。如果原始虚拟机未按预期工作，请选择\*commit failback\*(确认原始虚拟机按预期工作后)或\*Undo failback\*(撤消故障恢复)返回到虚拟机副本。

- 撤消故障转移-切换回原始虚拟机并放弃在虚拟机副本运行期间对其所做的所有更改。
- 永久故障转移-从原始虚拟机永久切换到虚拟机副本，并将此副本用作原始虚拟机。

在此演示中、我们选择了故障恢复到生产环境。在向导的目标步骤中选择了故障恢复到原始虚拟机、并启用了"Power On VM after Restoring"(还原后启动虚拟机)复选框。

[灾难恢复Veeam FSx版本15] | *dr-veeam-fsx-image15.png*

[DR Veeam FSx版本16] | *dr-veeam-fsx-image16.png*

提交故障恢复是完成故障恢复操作的方法之一。提交故障恢复后、它会确认发送到故障恢复虚拟机(生产虚拟机)的更改是否按预期工作。完成提交操作后、Veeam Backup & Replication将恢复生产虚拟机的复制活动。

有关故障恢复过程的详细信息、请参见Veeam文档 "[故障转移和故障恢复以进行复制](#)"。

[DR Veeam FSx版本17.] | *dr-veeam-fsx-image17.png*

[DR Veeam FSx版本18.] | *dr-veeam-fsx-image18.png*

成功故障恢复到生产环境后、所有VM都会还原回原始生产站点。

[DR Veeam FSx版本19] | *dr-veeam-fsx-image19.png*

## 结论

借助FSx for ONTAP数据存储库功能、Veeam或任何经过验证的第三方工具可以使用Pilot Light集群提供低成本的DR解决方案、而无需在集群中建立大量主机来容纳VM副本。这样可以提供一个功能强大的解决方案来处理定制的自定义灾难恢复计划、还可以重复使用内部现有备份产品来满足灾难恢复需求、从而通过在内部部署现有灾难恢复数据中心实现基于云的灾难恢复。发生灾难时、只需单击一个按钮、即可按计划进行故障转移或故障转移、并决定激活灾难恢复站点。

要了解有关此过程的更多信息、请随时观看详细的演练视频。

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

## 版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

## 商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。