JetStream SOFTWARE

JetStream DR

for

Azure VMware Solution

Evaluation Guide

Version 4.0

(June 2026)

Contents

JetStream Software Evaluation Guide

Disaster Recovery from On-Premises vSphere to Microsoft Azure VMware Solution with JetStream DR

Introduction

About this document

The purpose of this document is to provide a guide for evaluating the primary features and benefits of JetStream DR to protect and automate disaster recovery operations for virtual machines.

This evaluation guide contains a set of tests to demonstrate protection, various partial and full recovery operations (Failover, Test Failover and Failback) and JetStream DR resilience that includes DRVA and MSA non-graceful reboot and replication network error events.

This guide recommends a set of specific tests and some example applications to be used for evaluation. The number of failure scenarios can be expanded with physical host, Replication log, uplink and internal network failure and recovery. The evaluator can utilize other applications or additional test cases.

Key Concepts

Concept	Description
Protected Site	The VMware environment where the protected VMs normally run and contains the original infrastructure and data. If considered in terms of data flow, the Protected Site can be thought of as the source.
Recovery Site	The VMware environment where protected virtual machines will run when rehydrated from the Object Store and recovered in the event of a Failover.
NOTE: It is possible for the same site to serve as a Protected Site and Recovery Site when replication is occurring in both directions and virtual machines are protected at both sites.	
Storage Site / Object Store	The Storage Site is the environment where the Object Store for a protected Domain is located. The Object Store maintains continuously updated storage objects containing protected VMs and their data. The Storage Site can be located with the Recovery Site, or it can be in a different location.
Pilot light	A pilot light environment has a minimal set of core components for a site. The pilot light deployment is built to functional equivalency of the production site. This implementation allows you to restore and scale the system quickly and efficiently.
Recovery Point Objective (RPO)	The point in time to which data must be recovered as defined by the organization. In other words, the RPO is what an organization determines is an “acceptable loss” in a disaster situation.
Recovery Time Objective (RTO)	Targeted amount of time a business process should be restored after a disaster or disruption. RTO begins when a disaster hits and does not end until all systems are up and running.
Protected Domain	A Protected Domain contains VMs specified by the user that should be protected and restored together. All VMs of a Protected Domain are replicated to the same bucket on the storage site.

Protected Virtual Machine	A virtual machine that is included in a Protected Domain and replicated to a Storage Site for protection. Failover and Failback.
Failover	The disaster recovery function when the local site becomes appointed the "Recovery Site" for the Protected Domain. It is OK to continue running the Domain at the Recovery Site without failing back to the primary site.
Failback	The process where protected VMs and data are returned from the Recovery Site back to the Protected Site following a Failover. Failback is always live and incremental. After Failback, operations continue back at the Protected Site.
Continuous Failover (CFO)	Continuous Failover is a mode of operation where the Protected and Recovery Sites for a Protected Domain remain asynchronously synchronized during normal operation to minimize the amount time necessary to complete DR recovery.
Planned Failover (PFO)	An extension of the Failover process that can be used for non-disaster events such as moving the location of VMs and workloads while they continue to operate (i.e., "migration").
Test Failover (TFO)	A variant of the Failover process that conducts Failover of actual VMs and workloads but without shifting ownership of them to a Recovery Site. This allows DR and system performance to be fully tested without impacting actual production data.
Runbook	A set of instructions that are followed as part of Failover, Test Failover or Failback to specify VM startup sequence and configuration parameters for a Protected Domain.
Management Server Appliance ("MSA")	The MSA is the JetStream DR virtual appliance that provides a plug-in to vCenter Server. It collects and maintains statistics relevant to the protection of the VMs in the cluster(s) managed through vCenter. It also provides administrative functions, such as selecting VMs for protection, etc. The MSA can be managed using the vSphere Web Client, and its functions can also be accessed directly via CLI or RESTful APIs.
IO Filter	An IO Filter is a virtual machine component that runs in ESXi and intercepts all IO operations between a VM and its corresponding virtual disk(s). IO Filters are used to seamlessly examine currently existing disk data and replicate new data written to virtual disks without impacting system performance.
DR Virtual Appliance ("DRVA")	While the IO Filters capture data for replication, they do not communicate directly with the Object Store. The DRVA is a virtual appliance that maintains the replication log store and manages the transfer of the VMs and their data to the Object Store. The DRVA also manages functions such as in-line compression and garbage collection. There must be at least one DRVA per protected cluster. Additional DRVAs can be added to enhance scalability.
Replication Log	The replication log is the record of data being replicated to the Object Store. Each Protected Domain uses a single replication log for all the VMs belonging to the Protected Domain.
Replication Log Volume	The shared non-volatile memory resource that is dedicated for the use of JetStream DR software. Exposed to the DRVA(s) as an iSCSI LUN or as a VMDK virtual disk, the Replication Log Volume is used to maintain replication logs, garbage collection metadata and other metadata created by the JetStream DR software.

Recovery from Object Cloud Virtual Appliance (RocVA)	A virtual appliance in the data center at the Recovery Site. During a Failover process, the RocVA runs temporarily to facilitate the rehydration of the VMs and their data from the Object Store.
Representation VM (RVM)	During Failover, an RVM is created for each VM being rehydrated. They are created run temporarily during the recovery process (Failover, Failback, Restore) and are automatically deleted when no longer needed.
Protection Modes	Two methods are available to write protected data to primary storage and the replication log store. (1) “Write-through” method: The IO Filter acknowledges completion of a write operation back to a protected VM only after it has received acknowledgement of the write from both the replication log store and the primary storage. (2) “Write-back” method: The IO Filter acknowledges completion of the write operation to the protected VM upon receiving acknowledgement from the replication log store only; the write to primary storage is asynchronous.
Background Replication	The process of reading existing data from the virtual disk at the Protected Site and copying it to the Recovery Site. Background replication is important especially when protection is initiated.
Foreground Replication	The process of continuously identifying newly generated data at the Protected Site and copying it to the appropriate Object Store destination.
Garbage Collection	When invalidated data is no longer needed at the Protected Site it is removed from the Object Store by a "garbage collection" process. This minimizes unnecessary consumption of storage space at the Storage Site.
Domain Ownership (IO Fencing)	To maintain integrity of a Protected Domain, only one JetStream DR site can write to (update) the Object Store for a Protected Domain. Multiple sites can connect to the Protected Domain to read its contents and status, but only the "owning" site DRVA can write to the Protected Domain's bucket in the Object Store. The DRVA of the owning site updates the Protected Domain status to maintain its ownership and the write lock ("fencing out" DRVAs of other sites from writing to the Object Store). Ownership of the Protected Domain can shift between the local protected site or the remote Recovery Site depending upon the action currently being performed.

Table 1 - JetStream DR key concepts

JetStream DR Evaluation Overview

Logical Configuration

The diagram below shows a logical diagram of how the PoC/evaluation environment can be configured. Network connectivity is required between the Storage Site and both the Protected and Recovery Sites, but they do not have to be in separate regions to effectively perform the evaluation tests.

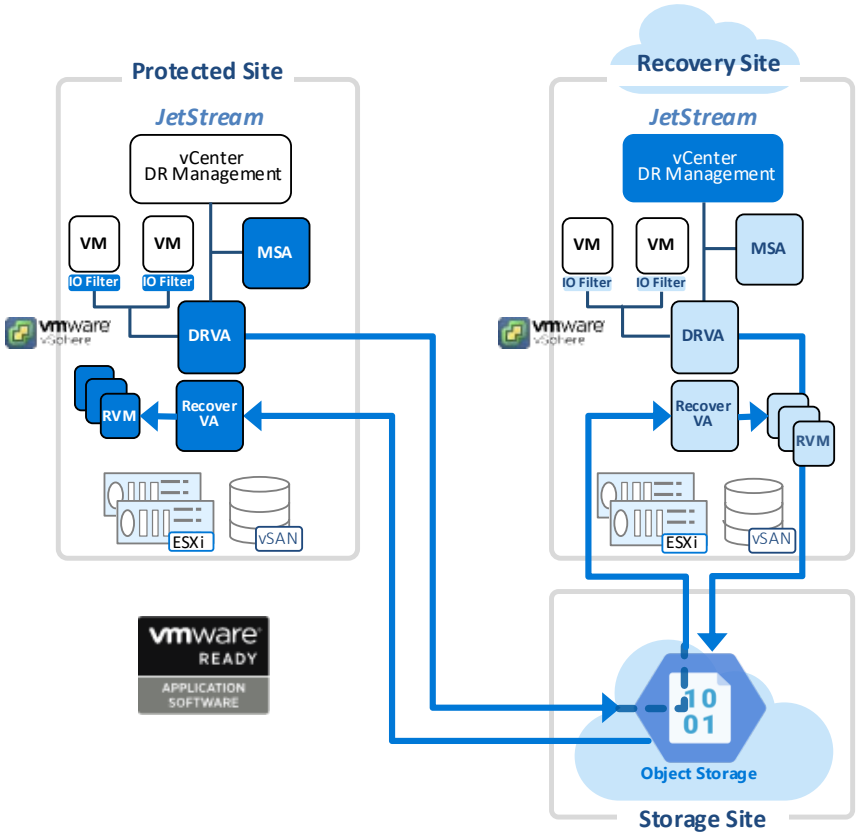


Figure 1- Example evaluation environment

Evaluation Flow

For the best results, the steps in this evaluation guide should be performed in order. Some test operations are dependent on previously completed items.

The PoC/evaluation has the following phases:

- Phase 1: Preparation
  - Microsoft Azure
  - On-premises VMware
- Phase 2: Installation and configuration
  - Storage Site
  - Protected Site
  - Recovery Site
- Phase 3: Evaluation Tests
  - Create a Protected Domain
  - Protect virtual machines
  - Standard Failover of a Protected Domain
  - Continuous Failover of a Protected Domain
  - Planned Failover (migration) of VMs in a Protected Domain

- Failback of a Protected Domain from the Recovery Site back to the Protected Site
- Continuous Failback of VMs in a Protected Domain from the Recovery Site to the Protected Site
- Test Failover of a Protected Domain
- Test Failover of a Protected Domain during Continuous Failover

Phase 1: Preparation

It is assumed that the following items are properly installed and configured in a non-production environment for use during this evaluation:

- DNS server with forward and reverse lookup configured
- VMware vCenter server
- Two or more vSphere 8.x hosts in a vSphere cluster

1. Identify the Microsoft Azure subscription for the Azure VMware Solution Private Cloud. You can use an existing Azure subscription or create a new one.
2. Identify the Azure Region for the Azure VMware Solution Private Cloud. It is recommended to create the Azure Blob Storage Account in the same region as the planned recovery site.
3. Provide JetStream with your Azure Tenant ID so we can provide access to the free JetStream DR for AVS Evaluation Program.
4. Subscribe to *JetStream DR for AVS* from the Azure Marketplace using the free JetStream DR for AVS Evaluation Program private offer and download the software bundle. The JetStream DR for AVS software bundle contains:
   - JetStream DR software
   - JetStream DR Documentation – Release Notes, Admin Guide, REST API guide, etc.
5. Review the JetStream DR documentation – especially the initial chapters of the Admin Guide that describe the prerequisites, infrastructure requirements and steps for installation and configuration. *Note: Additional technical documentation and video tutorials are also available. Review those as needed.*
6. Review and complete the JetStream DR pre-installation/evaluation checklist for the planned PoC scenario:
   a. Hybrid – On-premises vSphere to AVS private cloud
   b. Cloud only – AVS private cloud to AVS private cloud
7. Identify the VMs and applications to run on protected VMs during “normal” operation (no failure events) and for business continuity testing (during Restore, Failover and Failback).
   - Consider using I/O Generators like FIO, IOmeter or JetStress to generate storage workloads during evaluation tests.
   - For this evaluation, plan for a minimum of 6 Linux and/or Windows VMs with VMware tools installed. These VMs will be protected by JetStream DR in three Protected Domains.
   - We suggest a mixture of Linux and Windows VMs.
8. Plan the JetStream DR components and required resources (i.e., number of Protected Domains and their content, number of DR Virtual Appliances and their resources, required Replication Log device capacity and performance; required Object Store capacity and replication bandwidth).
   a. Smaller scale JetStream DR evaluation/PoC testing involving a small number of VMs (10-25 VMs) like what is described in this guide can easily be performed using the JetStream DR UI.
   b. For production deployments or large scale JetStream DR evaluation/PoC testing, it is recommended to use the Capacity Planning Tool (CPT) from the JetStream DR Automation Toolkit to determine resources that will be required for VM protection, both on-prem and in Azure

i. Using statistics captured from vCenter Server, CPT provides recommendations for required DR resources and JetStream components including Protected Domains and their content, DR Virtual Appliances and their resources, Replication Log volume sizing and performance, Object Store capacity, replication bandwidth, and more.

For the purposes of this POC/Evaluation guide plan to create:

- *3 Protected Domains, each with 2 or more VMs*
  - *Eval-PD-01*
  - *Eval-PD-02*
  - *Eval-PD-03*
- *6 DRVAs (8 vCPU, 16GB RAM each) – 3 at the Protected Site and 3 at the Recovery Site. For simplicity one DRVA will be used for each Protected Domain. Each DRVA will be configured with a 256 GB Replication log volume.*
  - *Protected Site Protected Domain to DRVA mapping:*
    - *Eval-PD-01 – DRVA-P1 – 64GB Replication Log*
    - *Eval-PD-02 – DRVA-P2 – 64GB Replication Log*
    - *Eval-PD-03 – DRVA-P3 – 64GB Replication Log*

9. Ensure that the following are in place to ensure successful completion of the steps in this guide:
   - Static IP addresses and DNS host (A) records assigned to all vSphere components, JetStream DR components and (optionally) for all virtual machines in the evaluation environment
   - DHCP service configured and available at both the Protected and Recovery Sites.
   - Reliable network connectivity between both the Protected Site, Recovery Site, and the Storage Site.
   - Adequate storage space available for all VMs and JetStream DR components.

Phase 2: Installation and Configuration

This phase of the evaluation includes optional pre-installation validation of the planned evaluation environments and installation and configuration of the components for the Storage Site, Protected Site and Recovery Site.

Pre-Installation

***Optional**, but recommended*:
Deploy the Jetstream DR tools appliance and connect it to the virtual network segment where you plan to install the JetStream DR Management Server Appliance (MSA).

- Run CPT to gather performance and configuration data from the production vCenter server for VM you are planning to protect. Running CPT also provides an opportunity to validate required components.
  - Tests credentials/access to vCenter
  - Tests DNS name resolution of the vCenter server
  - Provides output with estimates of bandwidth required for replication, Object Store size, number and proposed DRVA configuration, replication log volume sizing, etc.

Storage Site – Microsoft Azure Blob Storage

The Storage Site is the environment where the Object Store for a protected Domain is located. The Object Store maintains continuously updated storage objects containing protected VMs and their data. For deployments where an AVS Private Cloud is used as a recovery site, Azure Storage is used.

In the Storage Site, the preparation consists of creating an Azure Storage account to be used as the object storage repository.

1. Create an Azure storage account in the same Azure region as the Azure VMware Solution Private Cloud that will be used to recover or failover the protected VMs.
   The storage account should be configured with the standard performance SKU, hot access tier without hierarchical namespace.
   - ☐ Note the Storage account name and one of the access keys for use later when configuring the Storage Site in the JetStream DR UI.
   - ☐ If CPT was used for planning, note the replication bandwidth recommendation from CPT and compare it to the actual bandwidth available. Actual bandwidth can be measured using the *Object storage performance test tool* (Bandwidth Tester) – another tool available from the Automation Toolkit. The Bandwidth Tester also checks that the Azure Blob Storage account is available.

Protected Site – On-Premises

The Protected Site installation process includes deploying the JetStream DR MSA, registering the VMware vCenter Server, configuring the ESXi hosts with IO Filters, adding the Storage Site, and setting up the DR Virtual Appliances (DRVAs):

1. Create a virtual network segment for JetStream DR (JSDR) virtual appliance VMs (MSA, DRVAs, RocVAs and RVMs).
   - This network segment must be configured with DHCP.
   - Temporary representation virtual machines (RVM) require DHCP assigned IP addresses during Failback or local recovery operations.
2. Create one or more virtual network segments for the workload VMs to be used during testing.
3. Confirm the networking topology and connectivity between the Protected Site and the Azure storage account.
   - Networking and security configuration requirements are documented in the JetStream DR Admin guide.
   - Optionally, run the *Object storage performance test tool* (bandwidth tester) from the JetStream DR Automation Toolkit against the Object Store to:
     i. Test connection to the Object Store
     ii. Test DNS name resolution of the Object Store
     iii. Measure effective bandwidth and latency

4. Deploy the JetStream DR Management Server Appliance (MSA)
   a. Virtual machine name: *PR-MSA-01*
   b. VM location
      i. Datacenter: _____
      ii. Cluster: _____
   c. Select storage

i. Datastore: _____

d. Select network
   i. Select the virtual network you created in step 1.
   ii. Select "**Apply same network settings to all**"

e. Customize template
   i. Hostname – enter MSA FQDN
   ii. Enter root user password
   iii. Networking Properties

5. Register the JetStream DR MSA with vCenter
6. Configure the JetStream service account
   a. Run **manage_iofrest_user.ps1** script from MSA
      i. login to MSA appliance as admin (VM console or SSH)
      ii. **cd /opt/fio/vme2/python/**
      iii. **pwsh ./manage_iofrest_user.ps1**
         1. Use the same vCenter username and password that were used to register the MSA in step 5.
         2. Use the MSA user "admin" and the password that was set during MSA deployment.
7. Configure the IO Filters on the test cluster hosts
8. Create and configure DR Virtual Appliances (DRVA) –
   a. Create 3 DRVAs at the Protected Site for this evaluation plan.
      i. DRVA name(s) = *DRVA-P1, DRVA-P2, DRVA-P3*
      ii. DRVA Location
         1. Datacenter: _____
         2. Cluster: _____
         3. Resource Group (optional): _____
         4. Folder (optional): _____
         5. Datastore: _____
      iii. DRVA VM Settings
         1. 8 vCPU
         2. 16 GB RAM
      iv. DRVA Networking
         1. Management network: Select the virtual network you created in Step 1.
         2. Select "**Apply same network settings to all**"
      v. Summary
         1. Review inputs
         2. Click **Deploy**
9. For each DRVA (*DRVA-P1, DRVA-P2, DRVA-P3*) configure a 2656 GB VMDK Replication Log Volume.
   a. Select a DRVA from the list
   b. Click **+New Replication Log Volume**
      i. Select **VMDK**
      ii. Datacenter: _____
      iii. Datastore: _____

iv. Log Disk Size: 256 GB
v. Click **Configure**

10. Configure the Storage Site (use the same settings for both the Protected Site and Recovery Site)
    a. Log in to vCenter with the vSphere web client and navigate to the Datacenter level
        i. Click the **Configure** tab then select **JetStream DR**
        ii. Click the **Storage Sites** tab in the JetStream UI
        iii. Click **+ Add Storage Site**
        iv. In the "Add Storage Site" window enter the settings for the storage to be used for JetStream DR
            1. Storage site type: *Azure Blob Storage*
            2. Access Type: *Key Access*
            3. Storage Site Name: _____
            4. Azure Blob Storage Account Name: _____
            5. Azure Blob Storage Account Key: _____

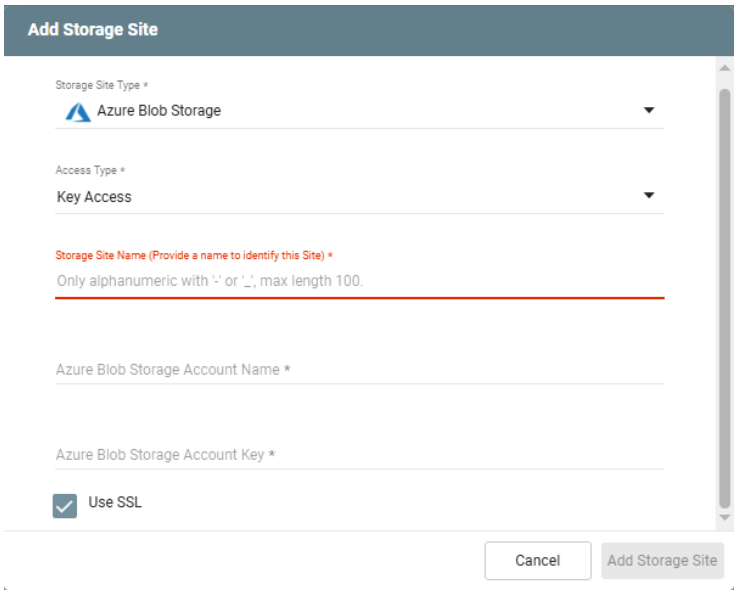


Figure 2 - Add Storage Site

Recovery Site – Azure VMware Solution Private Cloud

1. Create and configure an Azure VMware Solution (AVS) Private Cloud.
2. Configure a DNS forwarder for the AVS private cloud.
3. Create and configure DHCP server or relay for the AVS private cloud. Temporary representation virtual machines (RVM) require DHCP assigned IP addresses during Failover or recovery operations.
4. Create a dedicated NSX network segment for JetStream DR components (MSA, DRVA and RocVAs) and temporary VMs.
    a. Don't overlap addresses with cloud or on-prem IP networks.
    b. Configure sufficient address space and available DHCP IP address range for all VMs that are protected or will be recovered concurrently at the Recovery Site.
    c. Set DNS option to the private cloud's DNS forwarder IP address.
5. Create one or more NSX network segments for the workload VMs to be used during testing.

6. Create one or more NSX network segments to be used as an isolated test network for Test Failover.
7. Confirm the networking topology and connectivity between the Azure storage account and the AVS private cloud.
    a. Create a VM in the AVS private cloud and connect it to the network segment created in step 4.
        i. Look up the DNS name of the Azure Storage account.
        ii. Ping the IP address of the Azure Storage account.
        iii. Try tools like the Azure Storage Explorer to check connectivity from the VM to the Azure Storage account.
    b. Networking and security configuration requirements are documented in the Admin Guide.
    c. Optionally, run the *Object storage performance test tool* (bandwidth tester) from the Automation Toolkit against the Object Store to:
        i. Test connection to the Object Store
        ii. Test DNS name resolution of the Object Store
        iii. Measure effective bandwidth and latency
8. Install JetStream DR for AVS – Follow the instructions in the online document.
    a. Log in to Azure portal (portal.azure.com)
    b. Navigate to the AVS private cloud where JetStream DR software is intended to be deployed.
    c. In the left panel, locate and expand **Operations**, then click **Run command**.
    d. Under **Packages**, select **JSDR.Configuration** (Version 8.0.3).
    e. From the list select **Install-JetDRWithStaticIP,** then click **Run command**.
    f. Complete the input form with the necessary inputs, then click **Run**.
        i. Network: _____ (VM network name from step 4)
        ii. HostName: *RE-MSA-01* (Enter the FQDN of the MSA VM)
        iii. MSA Credential
            1. Username: *Admin*
            2. Password: _____
        iv. Gateway: _____
        v. DNS: _____ (comma separated)
        vi. MSA IP: _____ (MSA Static IP address)
        vii. Netmask: _____ (nnn.nnn.nnn.nnn format)
        viii. VLAN Id: _____ (leave blank unless VNIC level tagging is required)
        ix. Cluster: *Cluster-1*
        x. VM Name: *RE-MSA-01*
        xi. Datastore: ***vsanDatastore***
        xii. Protected Cluster: *Cluster-1*
        xiii. Register With IP: Set to "*True*"
    g. The Run command status can be monitored under Run execution status.
    h. Additional details can be found by selecting the Execution name.
    i. After the run command execution completes, use the vSphere Web Client to log in to the AVS private cloud vCenter as cloudadmin@vsphere.local. If prompted, refresh the client session.
    j. The JetStream DR plug-in UI is available at **vCenter -> Datacenter -> Configure -> JetStream DR**.

9. Configure the Storage Site (use the same settings for both the Protected Site and Recovery Site)
    a. Log in to vCenter with the vSphere web client and navigate to the Datacenter level
        i. Click the **Configure** tab then select **JetStream DR**

ii. Click the **Storage Sites** tab in the JetStream UI
iii. Click **+ Add Storage Site**
iv. In the "Add Storage Site" window enter the settings for the storage to be used for JetStream DR
    1. Storage site type: *Azure Blob Storage*
    2. Access Type: *Key Access*
    3. Storage Site Name: _____
    4. Azure Blob Storage Account Name: _____
    5. Azure Blob Storage Account Key: _____

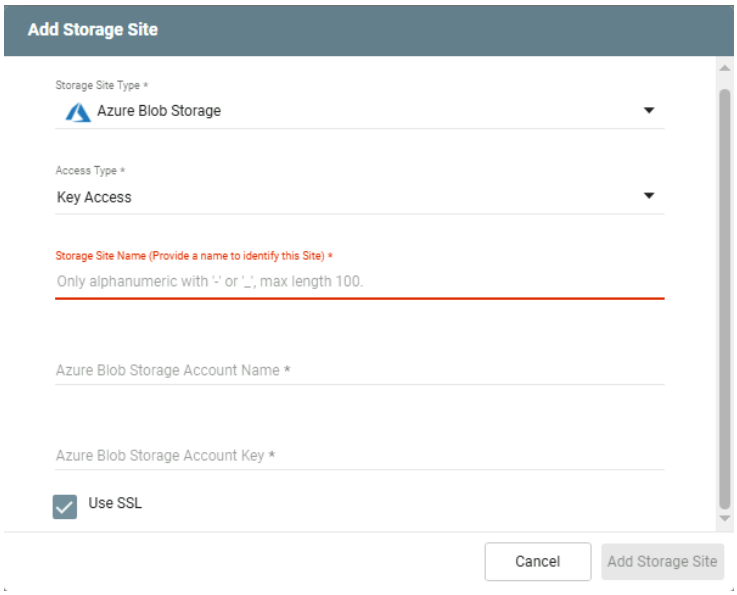


Figure 3 - Add Storage Site

10. Create and configure 3 DR Virtual Appliances (DRVA) in the Recovery Site AVS Private Cloud.
    a. DRVA Name – <DRVA-R1, DRVA-R2, DRVA-R3>
    b. DRVA location
        i. Datacenter: *SDDC-Datacenter*
        ii. Cluster: *Cluster-1*
        iii. Resource Group (optional): _____
        iv. Folder (optional): _____
        v. Datastore: ***vsanDatastore***
    c. DRVA VM settings
        i. 8 vCPU
        ii. 16 GB RAM
    d. DRVA Network
        i. Management network: Select the virtual network you created in step 4.
        ii. Select "**Apply same network settings to all**"
11. After the DRVAs status shows "Running," configure a New Replication Log Volume for each DRVA
        i. Replication Log type: **VMDK**
        ii. Datacenter: *SDDC-Datacenter*

iii. Datastore: *vsanDatastore*
iv. Log disk size - 256 GB

Phase 3: Evaluation Tests

The following JetStream DR operations are covered in this phase:

1. Create a Protected Domain
2. Protect virtual machines
3. Partial Failover
4. Standard Failover of VMs in a Protected Domain
5. Continuous Failover of VMs in a Protected Domain
6. Planned Failover (migration) of VMs in a Protected Domain
7. Failback of VMs in a Protected Domain from the Recovery Site back to the Protected Site
8. Continuous Failback of VMs in a Protected Domain from the Recovery Site back to the Protected Site
9. Continuous Failback of VMs in a Protected Domain from the Recovery Site with Resume Continuous Failover
10. Test Failover of VMs in a Protected Domain
11. Test Failover of VMs in a Protected Domain with Continuous Failover

Evaluation Activities

Evaluation Activities	Result
Create a Protected Domain	
Protect Virtual Machines	
Partial Failover and Force Failover of Protected Domain	
Standard Failover of Protected Domain	
Continuous Failover of Protected Domain	
Planned Failover of Protected Domain	
Failback of Protected Domain	
Continuous Failback of Protected Domain	
Continuous Failback of Protected Domain with Resume Continuous Failover	
Test Failover	
Test Failover with Continuous Failover	

Create a Protected Domain

A Protected Domain is a set of VMs sharing common protection policies and Recovery Time Objective (RTO). The VMs in a Protected Domain may be either independent of each other (“Independent VMs”) or may be in groups of inter-dependent VMs (“Runbook Groups”). All Protection, Recovery, Failover or Failback operations are performed with a Protected Domain.

In this evaluation guide you will create three Protected Domains (Eval-PD-01, Eval-PD-02, and Eval-PD-03). All three Protected Domains use to the same Object Store (“Storage Site”) in the same Azure Region as Recovery Site but each will have a unique destination container.

Once the Protected Domains have been created, starting DR protection for the VMs is simple and can be initiated immediately.

Create three Protected Domains (Eval-PD-01, Eval-PD-02, Eval-PD-03)

Following the Admin Guide, create Protected Domains at the Protected Site.

1. Create 3 Protected Domains (Eval-PD-01, Eval-PD-02, Eval-PD-03)
    a. General
        i. Name: *<Eval-PD-01, Eval-PD-02 or Eval-PD-03>*
        ii. Storage Site: *<Azure Storage site name>*
        iii. Total estimated data size: 200GB (minimum value allowed)
        iv. Priority Level: Default
        v. Leave "Enable PITR" unchecked
    b. Primary Site
        i. DRVA: *<DRVA-P1, DRVA-P2, or DRVA-P3>*
        ii. Replication Log Storage: select the volume from the dropdown list
        iii. Replication Log Size: **64GB**
        iv. Primary Site Datacenter: *<vCenter inventory datacenter name>*
        v. Primary Site Cluster: *<Name of "configured cluster" where VMs to be protected are located>*
2. Repeat Step 1 two more times to create Eval-PD-02 and Eval-PD-03.

Protect Virtual Machines

Multiple VMs can be assigned to a single Protected Domain for protection. JetStream DR continuously replicates data generated by the VMs in a Protected Domain. In this evaluation guide, 2 VMs will be protected in Eval-PD-01, 2 VMs in Eval-PD-02, and 2 VMs in Eval-PD-03.

When protection is started for a VM, a "background replication" process is initiated to replicate pre-existing data from the VM's virtual disks to the Object Store. While this is taking place, the VM's applications continue to run, and a "foreground replication" process replicates newly generated data to the Object Store. If the protected VM is running when protection is started, the background and foreground replication processes run concurrently. If the VM is not running, all data is copied from the VM's virtual disks via background replication, with no foreground replication. The amount of data replicated in the background and foreground is reflected in the JetStream DR runtime statistics and is visible in the JetStream DR user interface.

Once the VMs are protected, we will confirm that key VMware vSphere capabilities (e.g., snapshots, vMotion, etc.) are fully supported and data consistency is as expected.

Select VMs for protection in Protected Domains Eval-PD-01, Eval-PD-02 and Eval-PD-03.

Following the Admin Guide, select VMs for protection in each Protected Domain (*Eval-PD-01, Eval-PD-02, Eval-PD-03*)

1. Go to the **Protected Domains** menu
2. Select the Protected Domain *Eval-PD-01* from the dropdown list
3. Click the **Start Protection** button.

a. Select the VMs in the Start Protection screen
b. Set the Protection Mode to **Write-back**
c. Click the **Start Protection** button.

4. Repeat steps 1 through 3 for each of the remaining Protected Domains (*Eval-PD-02, Eval-PD-03*)

Note: The JetStream DR Automation Toolkit tools can be used to create and execute a *Protection Plan.* This can be used to automate the creation and configuration of DRVAs, Protected Domains, and start VM protection.

Observe the DR statistics through the GUI (incoming/outgoing data rates, RPO, garbage collection, replication logging). It may be helpful to observe statistics as VM protection is initiated, as well as after the VMs' status have changed to "recoverable." In the latter case, note the RPO data to confirm it meets your target RPO.

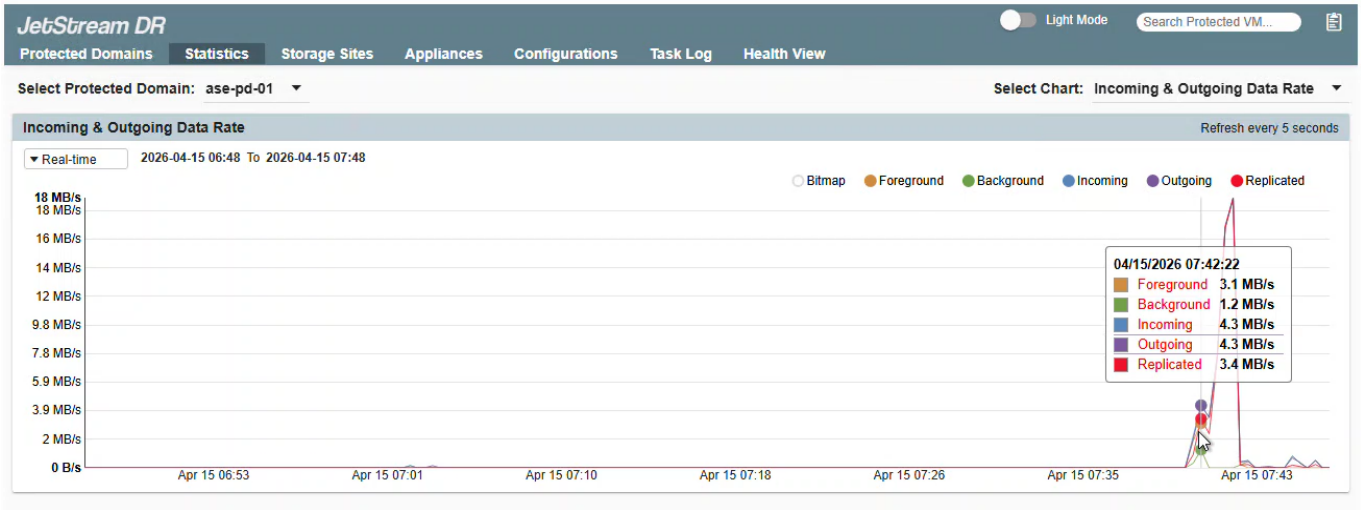


Figure 4- IO Statistics

Virtual machine operation tests

These tests demonstrate that data replication is not adversely impacted when various vSphere operations are performed in the Protected Site.

Substitute operating systems and workloads according to your preferences.

Initial Background Replication and VM running status

- ☐ Start protection and complete "initial sync" while the Windows VM is powered off; then power on the VM
- ☐ Start protection and complete "initial sync" while the Linux VM is powered on (use *fio* as an I/O generator)
- ☐ Final VMs state should be "Recoverable"

Shutdown / Power-off and Reboot of a protected VM while it is running a workload

- ☐ Shutdown and reboot a protected Linux VM running *fio*; restart *fio*
- ☐ Power off and power on a protected Linux VM running *fio*; restart *fio*
- ☐ Notice that the VM state remains "Recoverable"

- ☐ Stop *fio*

vMotion

- ☐ Start *IOmeter* or *fio* in a protected Windows VM
- ☐ Initiate vMotion of the Windows VM
- ☐ Wait for vMotion to complete
- ☐ Observe replication resuming smoothly after the vMotion has completed
- ☐ Wait for *IOmeter* or *fio* to complete

Create and Delete Snapshot

- ☐ Start *fio* in the protected Linux VM
- ☐ Create a VM snapshot
- ☐ Wait for a few minutes, then delete the snapshot
- ☐ Observe replication running continuously and smoothly during these operations
- ☐ Stop *fio*

Change VM Configuration

- ☐ Change VM configuration (vCPU or memory)
- ☐ Observe updated VM configuration in upcoming Failover and Failback tests

Create a Full Clone

- ☐ Start *fio* in the protected Linux VM
- ☐ Create a VM clone from one of the protected VMs (wait for completion). Do not add the clone VM to a Protected Domain
- ☐ Wait for a few minutes, then delete the clone
- ☐ Observe replication running continuously for the protected VM during these operations
- ☐ Stop *fio*

JetStream DR Garbage Collection Functionality

Power off the VMs in both Domain 1 and Eval-PD-02 then observe the garbage collection historical statistics. The amount of "garbage" should continue to decrease over time. After a few hours, check the garbage collection historical statistics.

JetStream DR appliance resilience tests

In this section, some of the most common failure events are simulated. Some large failure scenarios like whole cluster failure or specific host failure are difficult to reproduce. However, the events and failure scenarios provided are a representative sample.

DR Virtual Appliance (DRVA) Failure Event

- □ Start *IOmeter* or *fio* in the Windows VM (the Linux VM can be stopped) in a Protected Domain.
- □ Power off the DRVA for a Protected Domain. Wait 5 minutes, then power on the DRVA (optionally, vMotion and Stop & Reboot DRVA could also be evaluated)

- Notice that *IOmeter* or *fio* continues running in the protected VMs without interruption
- Observe the impact on Replication Log usage statistics
- Observe the impact on RPO and replication network activity through historical statistics

☐ Stop *IOmeter* or *fio*

Management Server (MSA) Failure Event

☐ Power off the MSA, then after 5 minutes, power the MSA back on.

- Notice that the protected VMs and both Protected Domains continue running without interruption
- After reboot, the MSA fully restores the previous protection state. It includes Object Store, DRVA, Domains and VMs state.

Replication Link Error Event

A replication network failure can be simulated by bringing down the DRVA network used for data replication.

☐ Start *fio* in the Linux VM in Eval-PD-02
☐ Break the network link to the Object Store (Azure Storage account). Keep it down for 15 minutes – after 15 minutes, the DRVA replication log will be getting full, and the running Protected Domains will switch to bitmap mode
☐ Allow *fio* to run continuously – no application-level actions are required

- Notice that *IOmeter* or *fio* continues running in the protected VMs without interruption

☐ Observe the historical statistics (RPO value and replication log space utilization) and the changes in Eval-PD-02 state – all VMs' IO filters will have switched to bitmap mode and the RPO value will grow. However, all the VMs stay in recoverable mode with higher RPO
☐ Simulate network recovery by restoring the network link
☐ Observe the amount of background (from the bitmap) and foreground data being replicated
☐ Wait until synchronization with the Object Store is complete and the Protected Domains return to the 'Recoverable' state
☐ Stop *fio* in the Linux VM.

Fio performance may drop during background replication. Background replication actively reads data from the primary storage.

Failover Testing – Import Protected Domains

Prior to performing disaster recovery operations at the Recovery Site, Protected Domains must be imported from the Storage Site.

Import Protected Domains Eval-PD-01, Eval-PD-02 and Eval-PD-03 at the Recovery Site.

Following the Admin Guide, Import Protected Domains for Failover at the Recovery Site

1. Log in to vCenter with the vSphere web client and navigate to the Datacenter level
2. Click the **Configure** tab then select **JetStream DR**
3. Click the **Storage Sites** tab in the JetStream UI
4. Click **Scan Domains**
5. Select Eval-PD-01
6. Click **Import**
7. Repeat steps 1 through 6 for Eval-PD-02, and Eval-PD-03

The Protected Domains are now imported on the Recovery Site and available for Recovery or Failover operations.

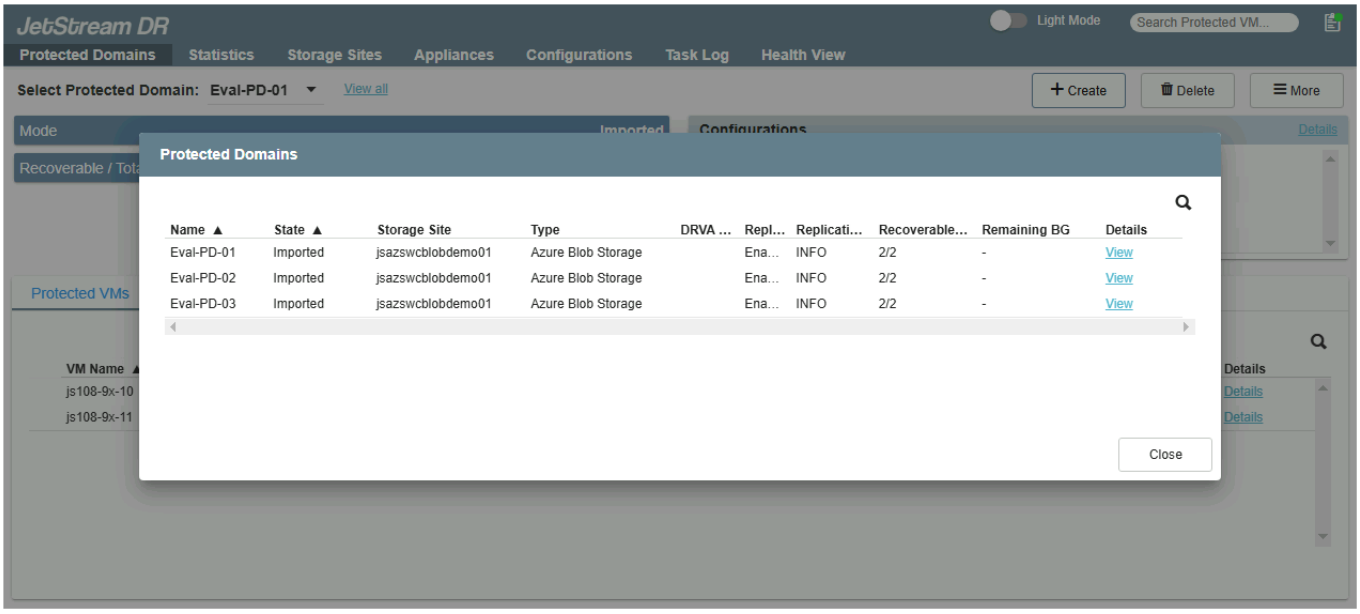


*Figure 5-**View all** showing all 3 Protected Domains imported*

Failover – Partial Failure

This partial failure test will use Eval-PD-02 to demonstrate the recovery of VMs in a particular Protected Domain when the entire Protected Site has not failed. In the process you will see how JetStream DR enforces Protected Domain ownership with IO Fencing to protect the integrity of the Object Store. The initial attempt fails because DRVA-P2 at the Protected Site continues running and updating the heartbeats in the Object Store container related to Eval-PD-02. Failover of Eval-PD-02 to the Recovery Site in AVS will be completed using the Force Failover capability. When the Force Failover option is used, ownership of Eval-PD-02 is seized and transferred to the Recovery Site JetStream DR installation, locking out the original Protected Site DRVA from writing to the Object Store container for Eval-PD-02. Once the Failover is complete, DRVA-R2 in the Recovery Site is responsible for updating the Object Store for Eval-PD-02.

Start Failover for Protected Domain Eval-PD-02 at the Recovery Site while there is no failure at the Protected Site.

Following the Admin Guide, Start Failover of VMs for Eval-PD-02 from the Recovery Site.

1. Select Protected Domain: “Eval-PD-02”
2. Click the “**More**” button
3. Select “**Failover**”
4. In the “Failover Protected Domain” screen
    a. General
        i. Review domain settings
    b. Failover Settings
        i. Datacenter: *SDDC-Datacenter*
        ii. Cluster: *Cluster-1*
        iii. Resource Group (optional): _____
        iv. Folder (optional): _____
        v. Datastore: *vsanDatastore*

vi. Failover Type: **Regular**

c. VM Settings
   i. VM Network Mapping
d. Recovery VA
   i. Management Network
   ii. Select **Apply same network settings to all**
e. DR Settings
   i. Select *DRVA-R2*
   ii. Select Replication Log Volume
   iii. Replication Log Size: 64 GB
f. Summary
   i. Review inputs
   ii. Click **Failover**

☐ Failover for Eval-PD-02 is attempted from Recovery Site.
- The attempt failed at the "Take Protected Domain ownership" step due to Protected Domain ownership violation because the Protected Site DRVA continued to maintain the ownership claim by updating the heartbeat in Eval-PD-02's Object Store bucket.

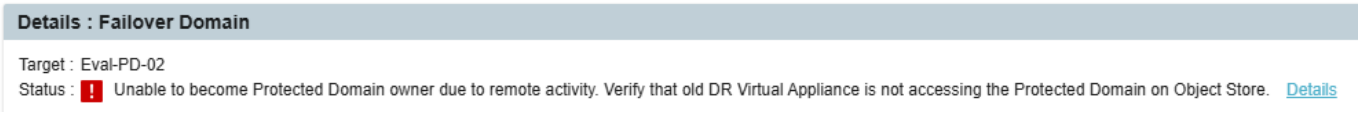


Figure 6 – Task Log: Failover failed because the Protected Site is still running

Repeat the Failover steps above, but this time select "**Force**" as the Failover Type.

Following the Admin Guide, Start Failover of VMs for Eval-PD-02 from the Recovery Site.

a. Select Protected Domain: "Eval-PD-02"
b. Click the "**More**" button
c. Select "**Failover**"
d. In the "Failover Protected Domain" screen
   i. General
      1. Review domain settings
   ii. Failover Settings
      1. Datacenter: *SDDC-Datacenter*
      2. Cluster: *Cluster-1*
      3. Resource Group (optional): _____
      4. Folder (optional): _____
      5. Datastore: *vsanDatastore*
      6. Failover Type: **Force**
      7. Click **Confirm**
   iii. VM Settings
      1. VM Network Mapping
   iv. Recovery VA
      1. Management Network
      2. Select **Apply same network settings to all**

v. DR Settings
    1. Select *DRVA-R2*
    2. Select Replication Log Volume
    3. Replication Log Size: 64 GB
vi. Summary
    1. Review inputs
    2. Click **Failover**

☐ Force Failover is applied from the Recovery Site. The Force Failover message is sent to the Protected Site through the Protected Domain's Object Store container.
- The Protected site DRVA receives this message and stops Eval-PD-02. As a result, the DRVA stops updating heartbeats.
- The Recovery Site MSA recognizes that heartbeat updates have stopped. It acquires Protected Domain ownership and initiates Failover.

☐ Failover starts and completes successfully.

☐ Eval-PD-02's VMs Failover and are restarted at the Recovery Site. Eval-PD-02's VMs are immediately protected and continue running.

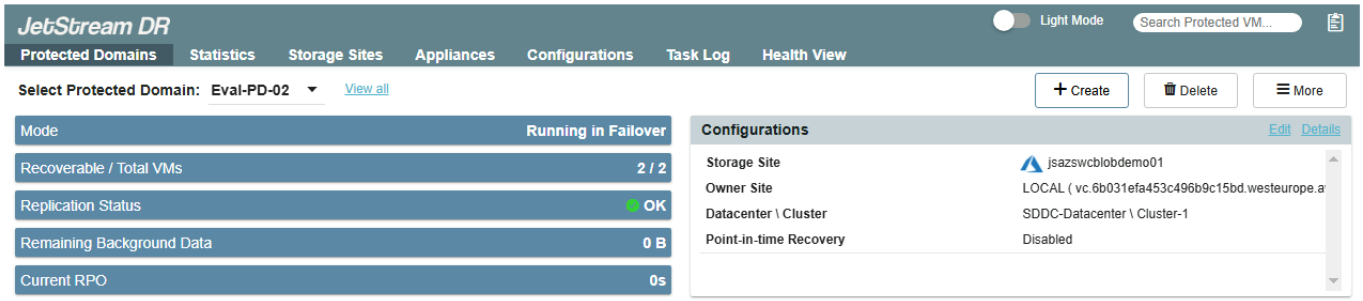


Figure 7- Eval-PD-02 Running in Failover

Failover – Standard Failover

☐ At the Protected Site, power off DRVA-P1. DRVA-P1 will lose connectivity with the Object Store.

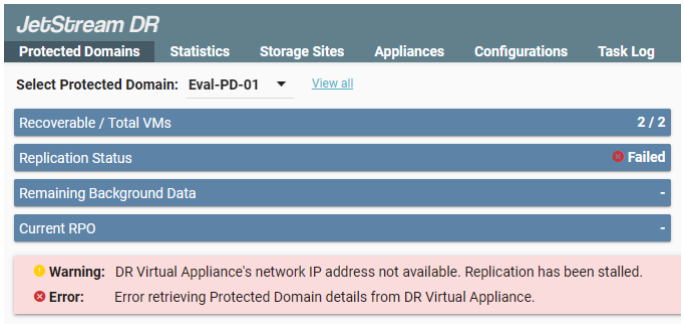


Figure 8- Eval-PD-01 replication stopped after DRVA-P! is powered off

Following the Admin Guide, Start Failover of VMs for Eval-PD-01 from the Recovery Site.

1. Select Protected Domain: "Eval-PD-01"
2. Click the "**More**" button
3. Select "**Failover**"
4. In the "Failover Protected Domain" screen
    a. General

i. Review domain settings

b. Failover Settings
   i. Datacenter: *SDDC-Datacenter*
   ii. Cluster: *Cluster-1*
   iii. Resource Group (optional): _____
   iv. Folder (optional): _____
   v. Datastore: *vsanDatastore*
   vi. Failover Type: **Regular**

c. VM Settings
   i. VM Network Mapping (Select the network for the recovered VMs)

d. Recovery VA
   i. Management Network
   ii. Select **Apply same network settings to all**

e. DR Settings
   i. Select DRVA-R1
   ii. Select Replication Log Volume
   iii. Replication Log Size: **64 GB**

f. Summary
   i. Review inputs
   ii. Click **Failover**

☐ Because DRVA-P1 has been powered off and not communicating with the Object Store, the heartbeats are not updated by the Protected Site, and the Failover is started successfully. The Eval-PD-01 ownership is transferred to the Recovery Site.

☐ Eval-PD-01 Failover completes successfully.

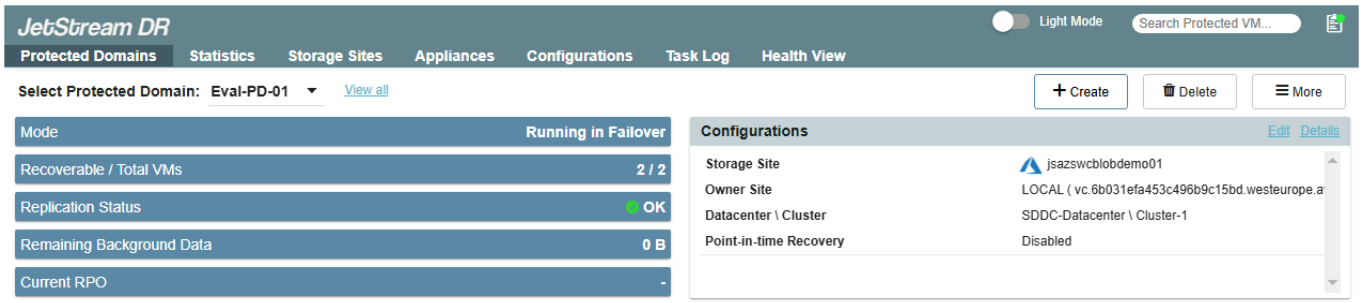


Figure 9- Eval-PD-01 Running in Failover

☐ Now both Eval-PD-01 and Eval-PD-02 Protected Domains are running at the Recovery Site.

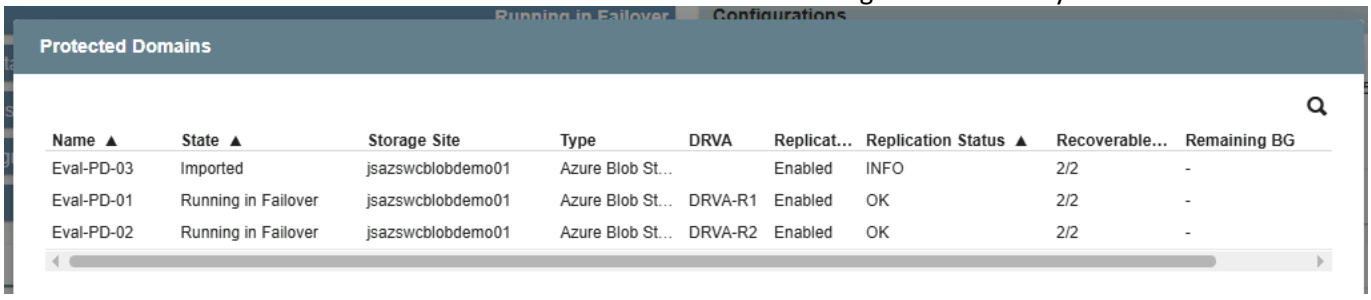


Figure 10- Current Protected Domain status at the Recovery Site after Eval-PD-01 and Eval-PD-02 have been recovered

- □ Observe RPO and data consistency. Notice that protection is resumed automatically and replication continues into the appropriate containers in Azure Storage.

Failover – Continuous Failover

"Continuous Failover" can be initiated at any time to replicate resources to the Recovery Site prior to any disaster. The replicated resources will become synchronized with the Protected Site during normal operation and can be recovered quickly, minimizing Failover recovery time when disaster does strike.

Continuous Failover can be configured at any time and then allowed to run in the background during normal system operation. After a disaster event has occurred, Continuous Failover is "completed" to transfer ownership of the protected VMs to the Recovery Site (near-zero RTO).

Start "Continuous Failover" for Eval-PD-03

Following the Admin Guide, Start Continuous Failover of VMs for Eval-PD-03 from the Recovery Site.

1. Select Protected Domain: "Eval-PD-03"
2. Click the "**More**" button
3. Select "**Continuous Failover**"
    a. In the "Failover Protected Domain" screen
        i. General
            1. Review domain settings
        ii. Failover Settings
            1. Datacenter: *SDDC-Datacenter*
            2. Cluster: *Cluster-1*
            3. Resource Group (optional): _____
            4. Folder (optional): _____
            5. Datastore: *vsanDatastore*
        iii. VM Settings
            1. VM Network Mapping (Select the network for the recovered VMs)
        iv. Recovery VA
            1. Management Network
            2. Select **Apply same network settings to all**
        v. DR Settings
            1. Select DRVA-R3
            2. Select Replication Log Volume
            3. Replication Log Size: **64 GB**
        vi. Summary
            1. Review inputs
            2. Click **Continuous Failover**

- □ Notice that the Protected VMs in Eval-PD-03 continue to run at the Protected Site.

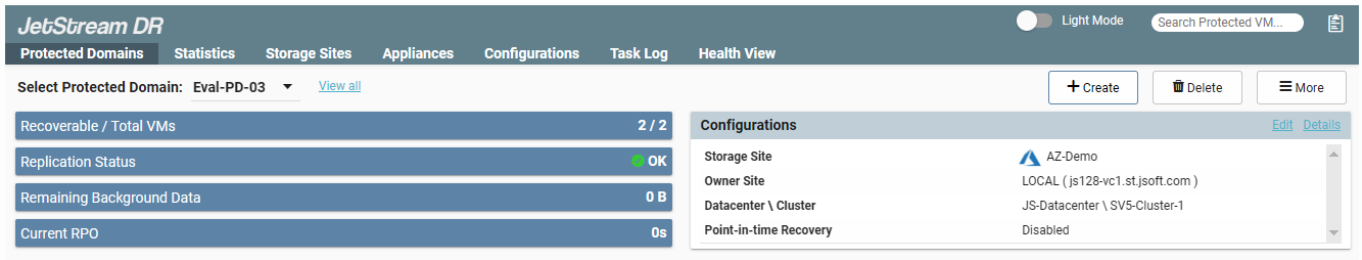


Figure 11- Eval-PD-03 still running at Protected Site

- ☐ After most of the background data has been processed, proceed to the next test to "complete" the in-progress Continuous Failover.

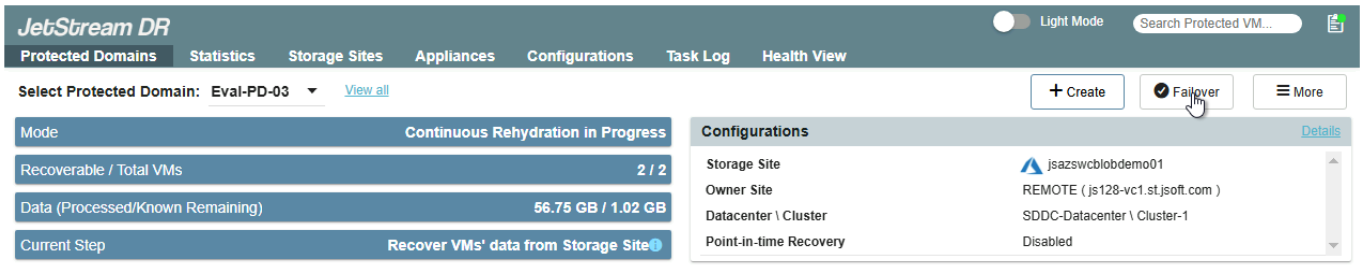


Figure 12- Eval-PD-03 with Continuous Failover in Progress at the Recovery Site

Failover – Planned Failover

Planned Failover is an option for either Standard (on-demand) or Continuous (near-zero RTO) Failover types. In this example we will “Complete” a Continuous Failover with the Planned Failover option.

Planned Failover shuts down the Protected Domain at the Protected Site (gracefully) before transferring ownership to the Recovery Site.

For this test Eval-PD-03’s in progress Continuous Failover will be “Completed” with the Planned Failover option.

Complete the in-progress Continuous Failover to recover the VMs in Eval-PD-03 from Azure Storage to the AVS Private Cloud at the Recovery Site.

Following the Admin Guide, Complete the Continuous Failover of VMs for Eval-PD-03.

1. Select Protected Domain: “Eval-PD-03”
2. Click the “**More**” button
3. Click “**Failover**”
4. In the “Complete Continuous Failover for Protected Domain…” screen
    a. VM Network Mapping
    b. Other Settings
        i. Select “**Planned**”
        ii. Select “**Destroy Protected Domain’s VMs at the Remote Site**”
        iii. Click **Complete Failover**

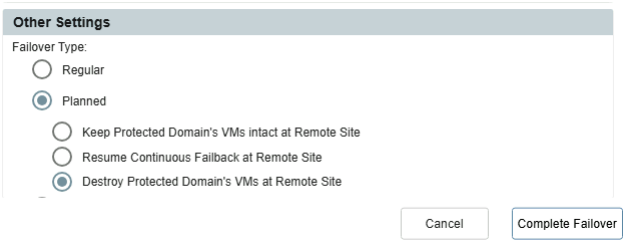


Figure 13- Completing Continuous Failover with the Planned option

☐ Now Eval-PD-01, Eval-PD-02 and Eval-PD-03 are Running in Failover at the Recovery Site

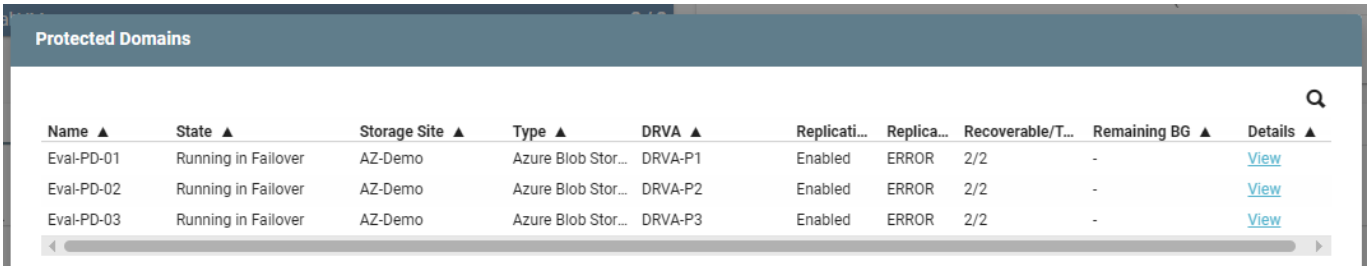


Figure 14- All 3 Protected Domains are Running in Failover

☐ Observe RPO and data consistency.
☐ Notice that the protected VMs are automatically protected when the Failover is complete.
☐ Notice the recovered VMs in AVS continue to replicate their data into the appropriate bucket in the Azure Storage.
☐ Notice that the Protected VMs in Eval-PD-03 are no longer registered in the Protected Site vCenter inventory.

Failback preparation

☐ Power on and/or reconnect the virtual network connections of the DRVAs at the Protected Site. All stale VMs and DRVAs are running at the Protected Site.
☐ Clean up Protected Site with JetStream cleaning procedure. It includes
  - Delete the stale VMs from Eval-PD-01 and Eval-PD-02
  - Delete the Protected Domains – Eval-PD-01 and Eval-PD-02
  - Delete the related replication log sections on DRVA-P1 and DRVA-P2. The MSA and DRVAs continue running but they do not have Eval-PD-01 or Eval-PD-02.
☐ After the Protected Site cleanup for Eval-PD-01 and Eval-PD-02 is complete, only Eval-PD-03 remains:

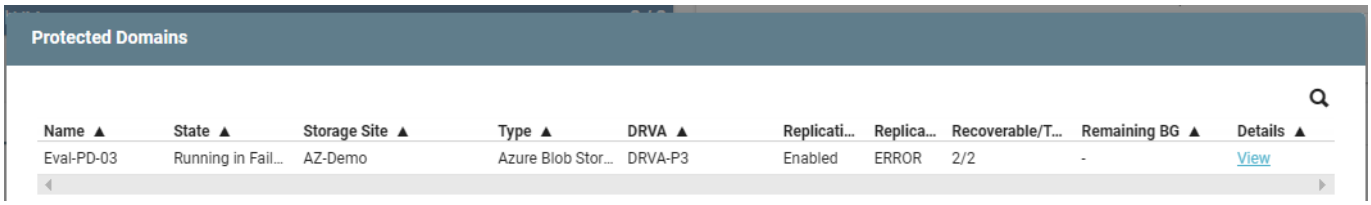


Figure 15- After Protected Site clean up only Eval-PD-03 remains

☐ Start Failback procedure while Eval-PD-01 and Eval-PD-02 are still running at the Recovery Site.

☐ Import Eval-PD-01 and Eval-PD-02 at the Protected Site in preparation for Failback

Following the Admin Guide, Import Protected Domains for Failback at the Protected Site

1. Log in to vCenter with the vSphere web client and navigate to the Datacenter level
2. Click the Configure tab then select JetStream DR

3. Click the Storage Sites tab in the JetStream UI
4. Click **Scan Domains**
5. Select Eval-PD-01
6. Click **Import**
7. Repeat steps 4 through 6 for Eval-PD-02

The Protected Domains are now imported on the Protected Site and available for Failback operations.

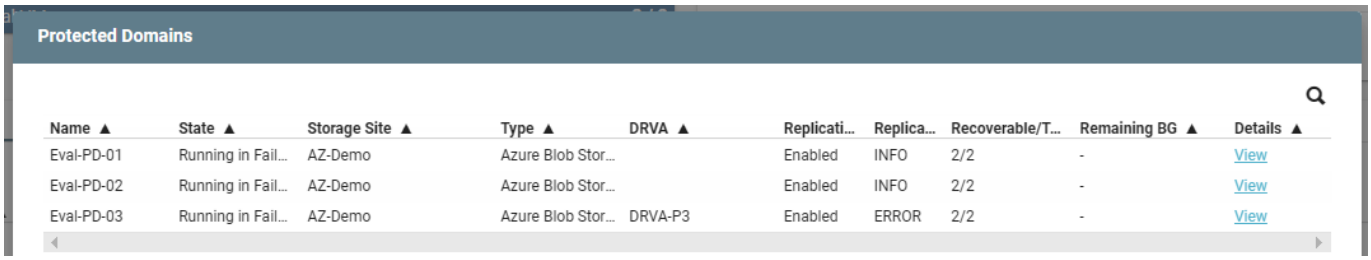


Figure 16- Eval-PD-01 and Eval-PD-02 are available for Failback after being imported at the Protected Site

Failback

- ☐ Failback Eval-PD-01 from the Recovery Site back to the original Protected Site.
    - Failback includes:
        - Stopping the VMs that are running in Failover at the Recovery Site and restarting them at the original Protected Site.
        - Protected Domain ownership switches back to the original Protected Site.
        - The Failed back VMs will be started at the original Protected Site.
        - Data protection is resumed smoothly with replication resuming to the same Object Store container.
        - Recovery site resources used by the failed over VMs are released.

Following the Admin Guide, Start Failback of VMs for Eval-PD-01 from the Protected Site.

1. Select Protected Domain: “Eval-PD-01”
2. Click the “**More**” button
3. Select “**Failback**”
4. In the “Failback Protected Domain” screen
    a. General
        i. Review domain settings
    b. Failback Settings
        i. Datacenter: _____
        ii. Cluster: _____
        iii. Resource Group (optional): _____
        iv. Folder (optional): _____
        v. Datastore: _____
        vi. Select “**Delete Protected Domain’s VMs at Remote Site**”
    c. VM Settings
        i. VM Network Mapping

ii. Set a Maximum Delay Value – 10 minutes is the minimum.

d. Recovery VA
   i. Management Network
   ii. Select **Apply same network settings to all**

e. DR Settings
   i. Select DRVA-P1
   ii. Select Replication Log Volume
   iii. Replication Log Size: **64 GB**

f. Summary
   i. Review inputs
   ii. Click **Failback**

- ☐ Notice that the VMs in Eval-PD-01 are no longer running at the Recovery Site in AVS and are now running again at the original Protected Site.
- ☐ Notice that after Failback is completed, the Protected Domain continues to be protected, and data is replicated into the appropriate container in the Azure Storage account.

Failback – Continuous Failback

"Continuous Failback" can be used to at any time to replicate resources to the Recovery Site prior to any disaster. The replicated resources will become synchronized with the Protected Site during normal operation and can be recovered quickly, minimizing Failover recovery time when disaster does strike.

Continuous Failback can be configured at any time and then allowed to run in the background during normal system operation. After a disaster event has occurred, Continuous Failover is "completed" to transfer ownership of the protected VMs to the Recovery Site (near-zero RTO).

Failback Eval-PD-02 from the Recovery Site back to the original Protected Site using Continuous Failback.

Following the Admin Guide, Start Failback of VMs for Eval-PD-02 from the Protected Site.

1. Select Protected Domain: "Eval-PD-02"
2. Click the **More** button
3. Select "**Continuous Failback**"
   a. In the "Failback Protected Domain" screen
      i. General
         1. Review domain settings
      ii. Failback Settings
         1. Datacenter: _____
         2. Cluster: _____
         3. Resource Group (optional): _____
         4. Folder (optional): _____
         5. Datastore: _____
      iii. VM Settings
         1. VM Network Mapping
         2. Set a Maximum Delay Value – **10 minutes** is the minimum.
      iv. Recovery VA

1. Management Network
2. Select **Apply same network settings to all**

v. DR Settings
1. Select DRVA-P1
2. Select Replication Log Volume
3. Replication Log Size: 64 GB

vi. Summary
1. Review inputs
2. Click **Continuous Failback**

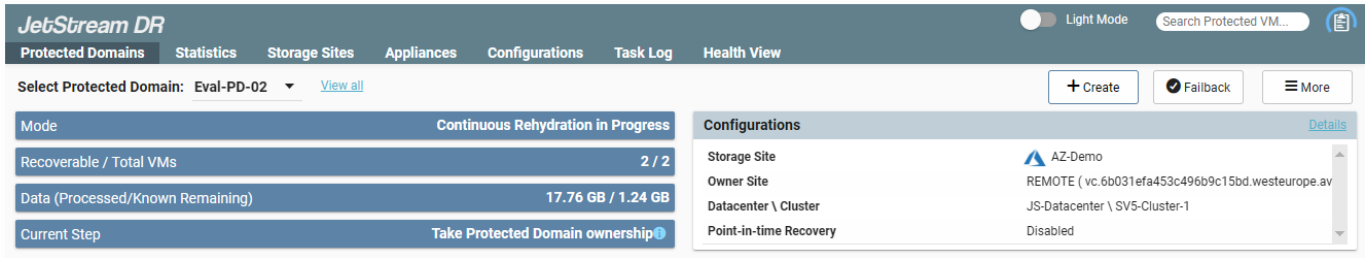


Figure 17- Continuous Failback in Progress at the Protected Site

☐ Notice that the VM in Eval-PD-02 continue to run at the Recovery Site while the Continuous Failback operation is running at the Protected Site.

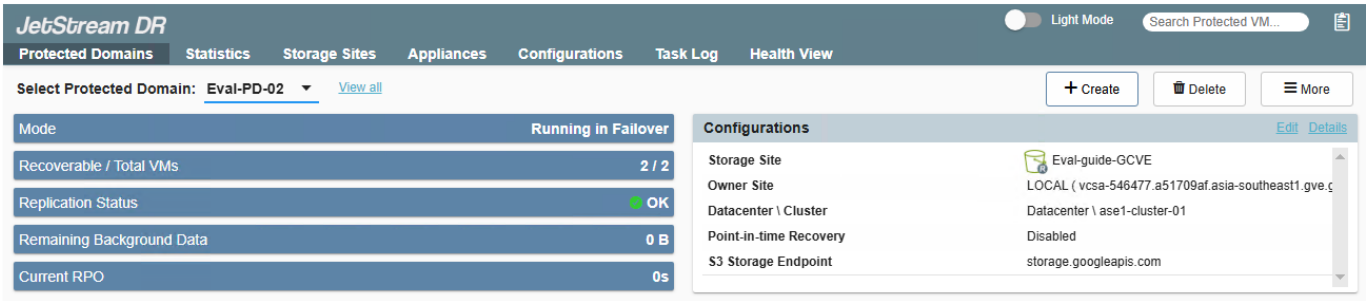


Figure 18- Eval-PD-02 VMs continue to run at the Recovery Site

☐ The VMs will continue to run at the Recovery Site until the Continuous Failback completion is initiated.

Complete the Continuous Failback for Eval-PD-02

Following the Admin Guide, Complete the Continuous Failback of VMs for Eval-PD-02.

1. Select Protected Domain: “Eval-PD-02”
2. Click “**Failback**”
    a. In the “Complete Continuous Failover for Protected Domain…” screen
    b. Other Settings
        i. Select “**Planned**”
        ii. Select “**Destroy Protected Domain’s VMs at the Remote Site**”
    c. Click **Complete Failback**

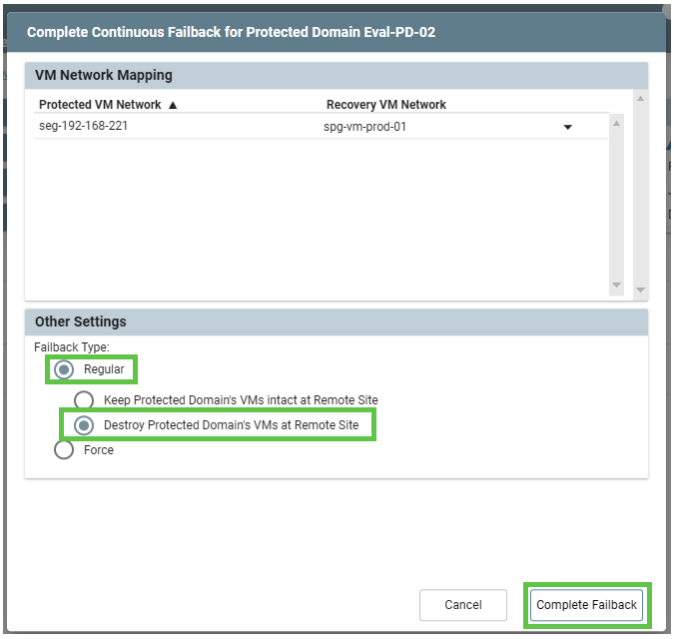


Figure 19- Complete Continuous Failback for Eval-PD-02

- ☐ Observe RPO and data consistency.
- ☐ Notice that the VMs in Eval-PD-02 are no longer running at the Recovery Site in AVS and are now running again at the original Protected Site.
- ☐ Notice that after Failback is completed, the Protected Domain continues to be protected, and data is replicated into the appropriate container in the Azure Storage account.
- ☐ Protected Domains Eval-PD-01 and Eval-PD-02 are now running again at the Protected Site:

Failback – Continuous Failback with Resume Continuous Failover

Failback Eval-PD-03 from the Recovery Site back to the original Protected Site using Continuous Failback.

Following the Admin Guide, Start Failback of VMs for Eval-PD-02 from the Protected Site.

1. Select Protected Domain: "Eval-PD-03"
2. Click the **More** button
3. Select "**Continuous Failback**"
4. In the "Failback Protected Domain" screen
    a. General
        i. Review domain settings
    b. Failback Settings
        i. Datacenter: _____
        ii. Cluster: _____
        iii. Resource Group (optional): _____
        iv. Folder (optional): _____
        v. Datastore: _____
    c. VM Settings
        i. VM Network Mapping
    d. Recovery VA

i. Management Network
ii. Select **Apply same network settings to all**

e. DR Settings
i. Select DRVA-P3
ii. Select Replication Log Volume
iii. Replication Log Size: 64 GB

f. Summary
i. Review inputs
ii. Click **Continuous Failback**

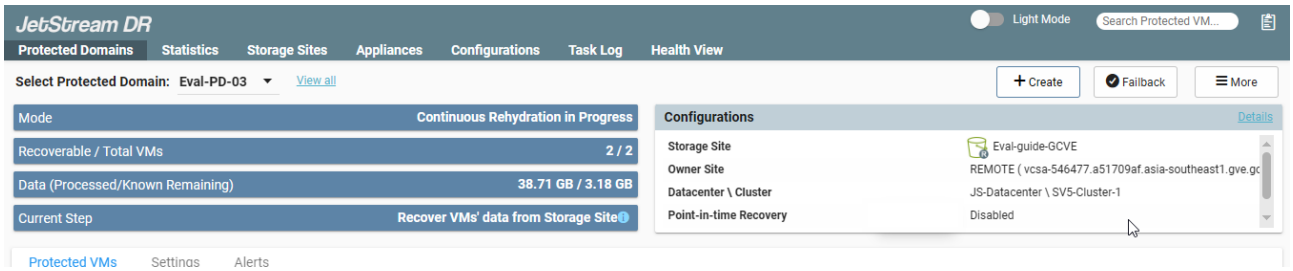


Figure 20- Continuous Failback in Progress at the Protected Site

- ☐ Notice that the VMs in Eval-PD-02 continue to run at the Recovery Site while the Continuous Failback operation is running at the Protected Site.
- ☐ The VMs will continue to run at the Recovery Site until the Continuous Failback completion is initiated.

Complete the Continuous Failback for Eval-PD-03

When the bulk of the VM data for Eval-PD-03 has been recovered back to the Protected Site, complete the Failback with the Regular option.

Following the Admin Guide, Complete the Continuous Failback of VMs for Eval-PD-03.

1. Select Protected Domain: “Eval-PD-03”
2. Click “**Failback**”
3. In the “Complete Continuous Failover for Protected Domain…” screen
    a. Other Settings
        i. Select “**Regular**”
        ii. Select “**Resume Continuous Failover using existing disks**”

b. Click **Complete Failback**

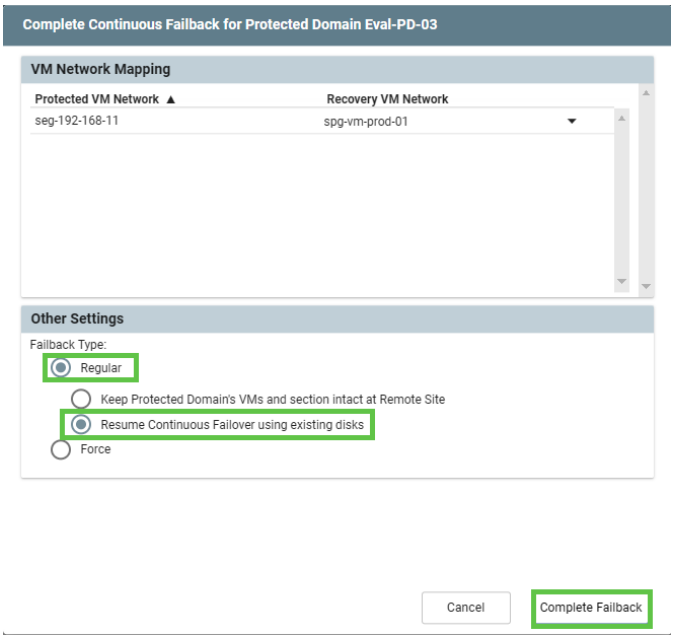
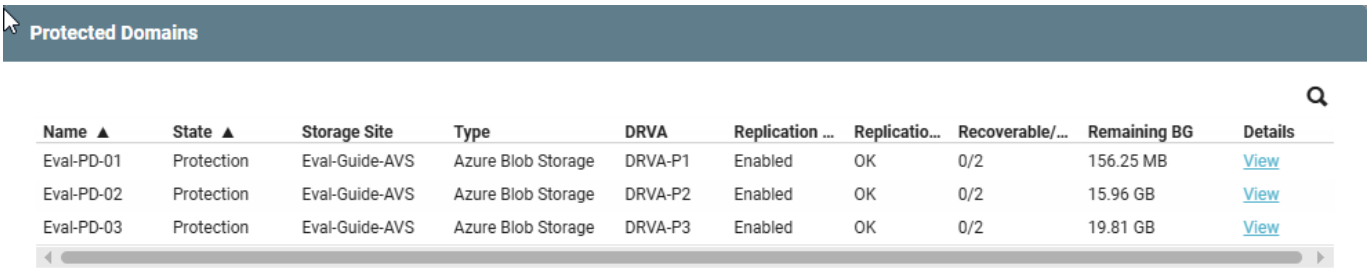


Figure 21- Complete Continuous Failback for Eval-PD-03

- ☐ Observe RPO and data consistency.
- ☐ Notice that the VMs in Eval-PD-03 are no longer running at the Recovery Site in GCVE and are now running again at the original Protected Site.
- ☐ Notice that after Failback is completed, the Protected Domain continues to be protected, and data is replicated into the appropriate bucket in Google Cloud Storage.
- ☐ Protected Domains Eval-PD-01, Eval-PD-02 and Eval-PD-03 are now running again at the Protected Site:



Name ▲	State ▲	Storage Site	Type	DRVA	Replication ...	Replicatio...	Recoverable/...	Remaining BG	Details
Eval-PD-01	Protection	Eval-Guide-AVS	Azure Blob Storage	DRVA-P1	Enabled	OK	0/2	156.25 MB	View
Eval-PD-02	Protection	Eval-Guide-AVS	Azure Blob Storage	DRVA-P2	Enabled	OK	0/2	15.96 GB	View
Eval-PD-03	Protection	Eval-Guide-AVS	Azure Blob Storage	DRVA-P3	Enabled	OK	0/2	19.81 GB	View

Figure 22 - Eval-PD-01, Eval-PD-02 and Eval-PD-03 are all running at the Protected Site

Failover – Test Failover

- ☐ Identify an isolated "test" network segment on the Recovery Site for the VMs involved in the test Failover.
- ☐ If Eval-PD-01 has not been failed back to the Protected Site, use a different Protected Domain, or create a new Protected Domain and import it on the Recovery Site to be used for the Test Failover test.
- ☐ Start a "Test Failover" of the protected VMs from The Object Store to the AVS Private Cloud Recovery Site.

Following the Admin Guide, start test Failover of VMs for Eval-PD-01 from the Recovery Site.

a. Select Protected Domain: "Eval-PD-01"
b. Click **More**
c. Select "**Test Failover**"
d. In the "Test Failover Protected Domain" screen

iii. General
    1. Review domain settings
iv. Failover Settings
    1. Datacenter: *SDDC-Datacenter*
    2. Cluster: *Cluster-1*
    3. Resource Group (optional): _____
    4. Folder (optional): _____
    5. Datastore: *vsanDatastore*
    6. Accept the default settings
v. VM Settings
    1. VM Network Mapping – Select the appropriate test network segment
vi. Recovery VA
    1. Management Network
    2. Select **Apply same network settings to all**
vii. Summary
    1. Review inputs
    2. Click **Test Failover**

When the Test Failover is ready a message will be displayed: "*Protected Domain's VM(s) recovery completed. Verify VMs and click Complete to complete the Test Failover Operation*"

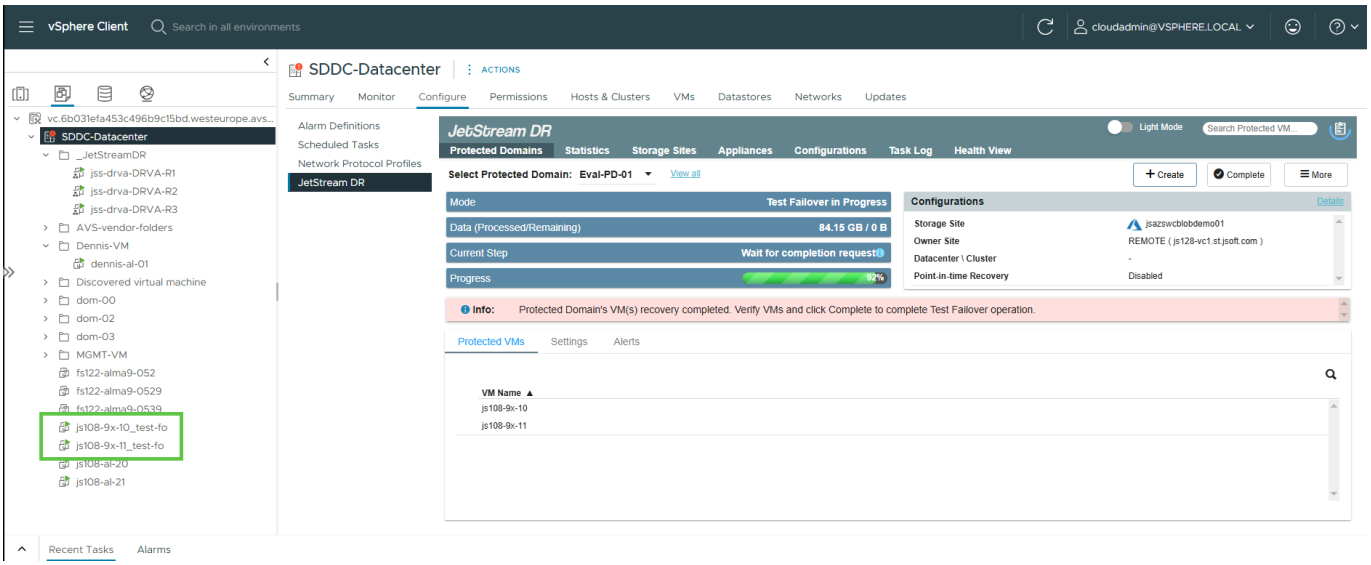


Figure 23- Protected Domain's VM(s) recovery completed... Ready for validation.

- ☐ Notice this task does not affect the continued operation and protection of the VMs at the Protected Site. Observe RPO and data consistency of the recovered VMs at the AVS Recovery Site, as well as the continued operation of JetStream DR in the protected on-premises cluster.
- ☐ Verify the operation of the VMs.

When the VM operations tests are finished. Click "**Complete**" to finish the test failover and the system will automatically power off the VMs and cleanup the Recovery Site.

Failover – Test Failover with Continuous Failover in Progress

- ☐ Identify an isolated "test" network segment on the Recovery Site for the VMs involved in the test Failover.

- ☐ If Eval-PD-03 has been failed back to the Protected Site and Continuous Failover was resumed, then use Eval-PD-03 for this Test Failover test.
- ☐ Start a "Test Failover" of the protected VMs from Google Cloud Storage into the GCVE private cloud Recovery Site.

Following the Admin Guide, start test Failover of VMs for Eval-PD-03 from the Recovery Site.

1. Select Protected Domain: "Eval-PD-03"
2. Click **Failover**
3. Select "**Test Failover**"
4. In the "Test Failover Protected Domain" screen
    a. General
        i. Review domain settings
    b. Failover Settings
        i. Datacenter: _____
        ii. Cluster: _____
        iii. Resource Group (optional): _____
        iv. Folder (optional): _____
        v. Datastore: *vsanDatastore*
        vi. Accept the default settings
    c. VM Settings
        i. VM Network Mapping – Select the appropriate test network segment
    d. Recovery VA
        i. Management Network
        ii. Select **Apply same network settings to all**
    e. Summary
        i. Review inputs
        ii. Click **Test Failover**

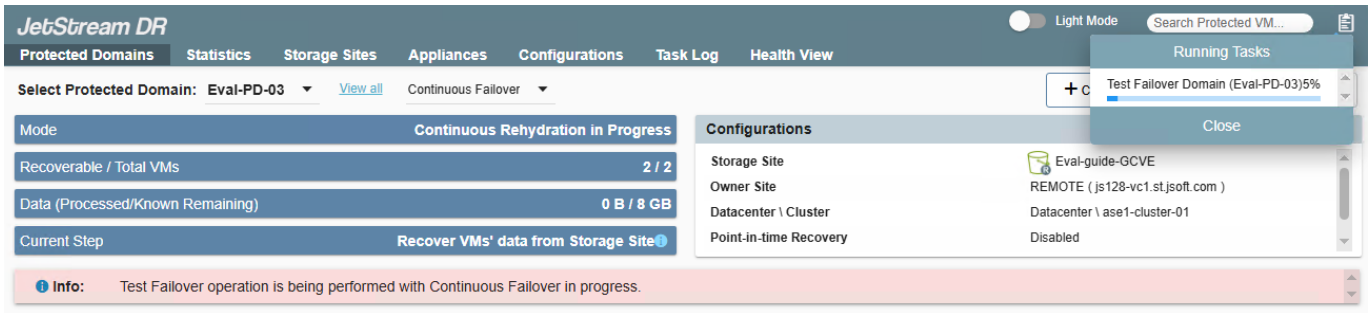


Figure 24- Eval-PD-03 Test Failover starting

- ☐ When the Test Failover is ready a message will be displayed: "*Protected Domain's VMs recovery completed. Verify VMs and click Complete to complete the Test Failover Operation*"

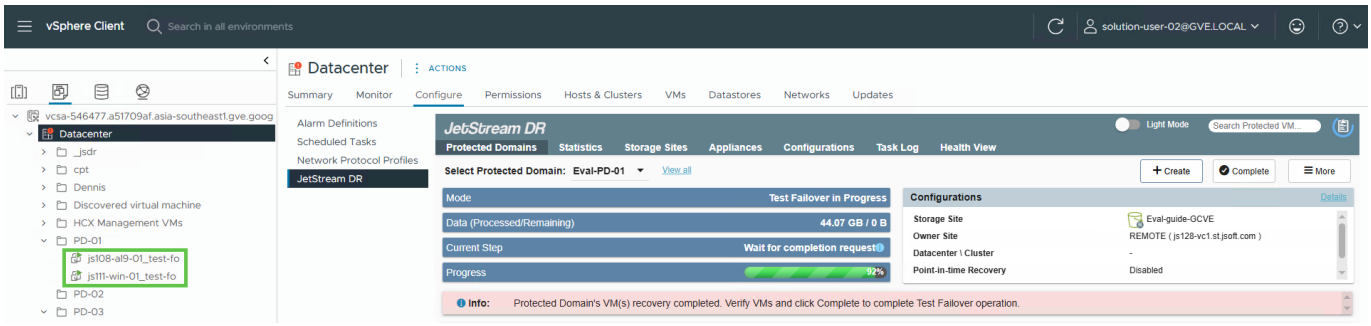


Figure 25- Protected Domain's VM(s) recovery completed... Ready for validation.

- ☐ Notice this task does not affect the continued operation and protection of the VMs at the Protected Site. Observe RPO and data consistency of the recovered VMs at the GCVE Recovery Site, as well as the continued operation of JetStream DR in the protected on-premises cluster.
- ☐ Verify the operation of the VMs.
- ☐ When the VM operations tests are finished. Click "**Complete**" to finish the test and the system will automatically power off the VMs and cleanup the Recovery Site.

Summary

JetStream DR with Continuous Data Protection is a sophisticated product that consists of multiple components. Testing various recovery methods is critical to make sure that all elements of protection are operating correctly. This guide provides an example of a complete evaluation plan that tests failure of each of the components and elements of the VM environment. Confirmation of the expected results demonstrates that JetStream DR will provide full VM protection through multiple modes of failure. This test plan can be modified to reflect specific use cases of the product as well.