Zerto

Zerto Virtual Replication Quick Start AWS Environments

Rev01 U3
Jan 2020
ZVR-QSA-7.5

ZVR-QSA-7.5

Zerto Quick Start AWS Environments

Zerto is an IT Resilience Platform™ to provide business continuity (BC) and disaster recovery (DR) in a virtual environment, enabling the replication of mission-critical applications and data as quickly as possible and with minimal data loss. When devising a recovery plan, these two objectives, minimum time to recover and maximum data to recover, are assigned target values: the recovery time objective (RTO) and the recovery point objective (RPO). Zerto enables a virtual-aware recovery with low values for both the RTO and RPO. In addition, Zerto enables protecting virtual machines for extended, longer term, recovery using Long Term Retention.

This document provides a quick guide to setting up Zerto to recover virtual machines in Amazon Web Services (AWS). The virtual machines can be protected by Zerto in either VMware vSphere, Microsoft Hyper-V or Microsoft Azure.

See the following sections:

Introduction on page 4

Recommended Installation Best Practices on page 7

Installation on page 8

Registering the Zerto License on page 10

Pairing Sites to Enable Replicating From One Site to Another Site on page 11

Setting Up the Protected Site on page 12

Protecting Virtual Machines on page 13

Testing Disaster Recovery on page 27

Introduction

Zerto helps customers accelerate IT transformation by eliminating the risk and complexity of modernization and cloud adoption. By replacing multiple legacy solutions with a single IT Resilience Platform™, Zerto is changing the way disaster recovery, retention and cloud are managed. This is done by providing enterprise-class disaster recovery and business continuity software for virtualized infrastructure and cloud environments.

In *on-premise* environments, Zerto (ZVR) is installed with virtual machines to be protected and recovered.

In *public cloud* environments, Zerto Cloud Appliance (ZCA) is installed in the public cloud site that is to be used for recovery.

The installation includes the following:

- *Zerto Virtual Manager* (ZVM): A Windows service that manages everything required for the replication between the protection and recovery sites, except for the actual replication of data. The ZVM interacts with the hypervisor management user interface, such as vCenter Server or Microsoft SCVMM, to get the inventory of VMs, disks, networks, hosts, etc. and then the Zerto User Interface manages this protection. The ZVM also monitors changes in the hypervisor environment and responds accordingly. For example, a VMware vMotion operation, or Microsoft Live Migration of a protected VM from one host to another is intercepted by the ZVM and the Zerto User Interface is updated accordingly.
    - For the maximum number of virtual machines, either being protected or recovered to that site, see Zerto Scale and Benchmarking Guidelines.
- *Virtual Replication Appliance** (VRA): A virtual machine installed on each hypervisor hosting virtual machines to be protected or recovered, to manage the replication of data from protected virtual machines to the recovery site.
    - For the maximum number of volumes, either being protected or recovered to that site, see Zerto Scale and Benchmarking Guidelines.

    > **Note:** *In vSphere installations, OVF to enable installing Virtual Replication Appliances.

- *Virtual Backup Appliance* (VBA): A Windows service that manages File Level Recovery operations within Zerto Virtual Replication.
- ***Zerto User Interface***: Recovery using Zerto is managed in a browser or, in VMware vSphere Web Client or Client console.

When Zerto is installed to work with an on-premise hypervisor it also comprises the following component:

- *Data Streaming Service* (DSS)**:** Installed on the VRA machine, and runs in the same process as the VRA. It is responsible for all the retention data path operations.

Requirements for AWS Environments

For information about requirements and limitations for AWS environments, see Zerto - Prerequisites & Requirements for Amazon Web Services (AWS).

Routable Networks

The instance on which the Zerto Cloud Appliance is installed must use a subnet that is accessible from all Zerto Virtual Managers that may be connected to this instance.

Zerto Virtual Manager does not support NAT (Network Address Translation) firewalls.

Minimum Bandwidth

- The connectivity between sites must have the bandwidth capacity to handle the data to be replicated between the sites. The **minimum** dedicated bandwidth must be at least **5 Mb/sec**.

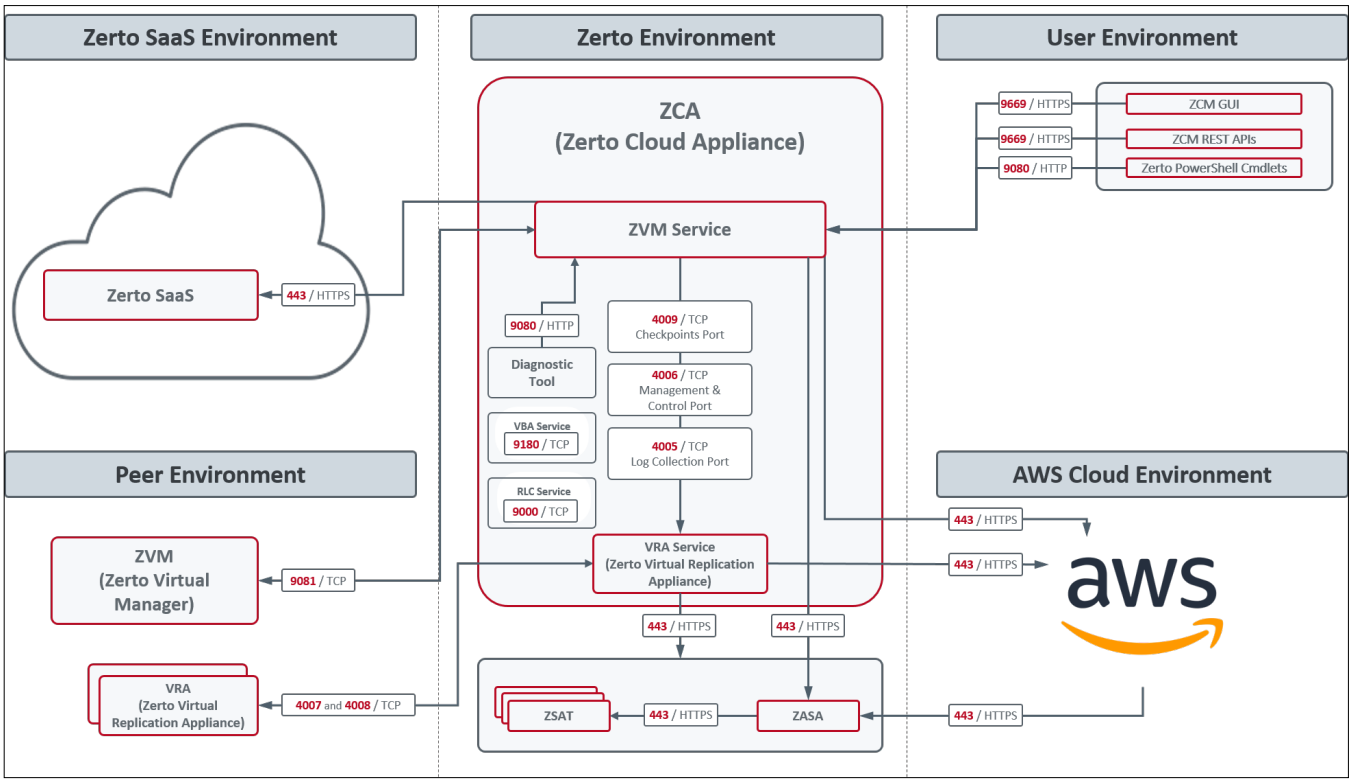
The Zerto User Interface

For supported browsers, see *Interoperability Matrix for All Zerto Versions*, in the section Supported Browsers.

The lowest supported screen resolution is **1366x768**.

Open Firewall Ports

The following diagram shows Zerto components deployed on one site and the ports and communication protocols used between the components.



Zerto Cloud Appliance requires the following ports to be open in the AWS site firewall, set in the Amazon security group:

Port	Description
443	Required between the ZVM and the AWS Cloud environment.
443	Required between ZVM Service and ZASA.
4005	Log collection between the ZVM and site VRAs.
4006	Communication between the ZVM and local site VRAs and the site VBA.
4007	Control communication between protecting and peer VRAs.
4008	Communication between VRAs to pass data from protected virtual machines to a VRA on a recovery site.
4009	Communication between the ZVM and local site VRAs to handle checkpoints.
7073	Internal port, used only on the ZVM VM. Used for communication with the service in charge of collecting data for the Zerto Resource Planner. **Note:** Unless you select the checkbox 'Enable Support notification and product improvement feedback', data is **not** transmitted to Zerto Analytics.
9080*	Communication between the ZVM, Zerto Powershell Cmdlets, and Zerto Diagnostic tool.
9081*	Communication between paired ZVMs**
9180*	Communication between the ZVM and the VBA.
9669*	Communication between ZVM and ZVM GUI and ZVM REST APIs, and the ZCM.
9779	Communication between ZVM and ZSSP (Zerto Self Service Portal).
9989	Communication between ZCM, and ZCM GUI and ZCM REST APIs.

*The **default** port provided during the ZVR installation which can be changed during the installation.
When the same vCenter Server is used for both the **protected and **recovery** sites, ZVR is installed on one site only and this port can be ignored.

Recommended Installation Best Practices

Zerto recommends the following best practices:

- Install Zerto on a dedicated virtual machine with a dedicated administrator account.
- You must **exclude**the following folders from **antivirus scanning**:

Zerto Virtual Replication
%ProgramData%\Zerto\Data\zvm_db.mdf
C:\Program Files\Zerto\Zerto Virtual Replication\Zerto.Zvm.Service.exe
C:\Program Files\Zerto\Zerto Virtual Replication\Zerto.Vba.VbaService.exe
C:\Program Files\Zerto\Zerto Virtual Replication\Zerto Online Services Connector\Zerto.Online.Services.Connector.exe
C:\Program Files\Zerto\Zerto Virtual Replication\Embedded DB Manager Service\Zerto.LocalDbInstanceManagerService.exe

Failure to do so may lead to the Zerto Virtual Replication folder being incorrectly identified as a threat and in some circumstances corrupt the Zerto Virtual Replication folder.

Installation

The Zerto installation deploys the Zerto Cloud Appliance (ZCA) on the recovery site. A complete installation includes installing Zerto on the protected site.

You can install Zerto using the defaults provided by Zerto or perform a custom install, in which you define the ports that will be used by Zerto.

Performing an Express Installation

You can install Zerto using the defaults provided by Zerto. Site information can be provided, if required, after the installation in the Zerto User Interface.

Make sure the permission level of the VM running the ZCA is set using IAM Roles. See Setting EC2 Instance Permissions in AWS on page 1.

> **Note:** You cannot install Zerto on the same machine where another version of Zerto has been installed.

To perform an express install of Zerto:

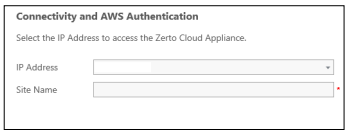
1. Run the Zerto installation executable for Amazon Web Services (AWS). It has a format like:

   `Zerto.Zvm.Zca.Installer_N.NuN_pNNN.exe` where *N.NuN_pNNN* represents the version and build number.

2. Follow the wizard through the installation until the dialog for the Installation Type and select the `Express Installation` option.

3. Click **NEXT**.

   The Connectivity and AWS Authentication dialog is displayed.



4. Specify the following:

   IP / Host Name: The IP address or host name of the machine on which you are installing the Zerto Cloud Appliance. The protected site accesses the recovery site using this IP.

   Site Name: A name to identify the site.

5. Click **NEXT**.

   The Validation dialog is displayed.

   The installation performs checks to make sure that the installation can proceed successfully.

6. After the checks complete successfully, click **NEXT** and continue to the end of the installation.
7. You must **exclude** the following folders from **antivirus scanning**:

Zerto Virtual Replication
%ProgramData%\Zerto\Data\zvm_db.mdf
C:\Program Files\Zerto\Zerto Virtual Replication\Zerto.Zvm.Service.exe
C:\Program Files\Zerto\Zerto Virtual Replication\Zerto.Vba.VbaService.exe
C:\Program Files\Zerto\Zerto Virtual Replication\Zerto Online Services Connector\Zerto.Online.Services.Connector.exe
C:\Program Files\Zerto\Zerto Virtual Replication\Embedded DB Manager Service\Zerto.LocalDbInstanceManagerService.exe

Failure to do so may lead to the Zerto Virtual Replication folder being incorrectly identified as a threat and in some circumstances corrupt the Zerto Virtual Replication folder.

Registering the Zerto License

Access the Zerto User Interface from a browser as follows:

To use the Zerto Virtual Manager Web Client:

1. In a browser, enter the following URL:
   `https://zvm_IP:9669`

   where **zvm_IP** is the IP address of the Zerto Virtual Manager for the AWS site. Ensure that port 9669 is open and set as an inbound rule in the security group of the instance where Zerto is installed.

2. Log in using the user name and password of the instance on AWS on which you installed the Zerto Cloud Appliance.

When you first access the Zerto User Interface, you must register your use of Zerto by entering the ZCA license supplied by Zerto.

> **Note:** The license is different from the license you use for your protected site.

After entering a valid license, the DASHBOARD tab is displayed with a summary of the site.

In order to protect virtual machines to AWS, you must first pair the protected site containing the virtual machines that you want to protect with the AWS site on which you installed the Zerto Cloud Appliance. This is described in Pairing Sites to Enable Replicating From One Site to Another Site on page 11.

Pairing Sites to Enable Replicating From One Site to Another Site

Zerto is installed on both the protected and AWS sites and these two sites are paired to enable disaster recovery across the sites.

To pair sites:

1. In the Zerto User Interface, in the **SITES** tab click **PAIR**.

   The `Add Site` dialog is displayed.

2. Specify the following:

   - **Remote Site ZVM IP Address:** IP address or fully qualified DNS host name of the remote site Zerto Virtual Manager to pair to.
   - **Port:** The TCP port communication between the sites. Enter the port that was specified during installation. The default port during the installation is 9081.

3. Click **PAIR**.

   The sites are paired, meaning that the Zerto Virtual Manager on the protected site is connected to - paired with - the Zerto Virtual Manager on the AWS site.

After the pairing completes the content of the SITES tab changes to include summary information about the paired site.

Setting Up the Protected Site

Refer to the Zerto documentation for the relevant hypervisor.

Protecting Virtual Machines

You can protect virtual machines to an AWS recovery site from either VMware vSphere, Microsoft Hyper-V or Microsoft Azure. The procedure is the same whether you intend to protect one virtual machine or multiple virtual machines.

When creating a VPG to AWS the data is stored in S3 and all replicated data from protected virtual machines to AWS is encrypted in S3. All recovery operations bring up the recovered machines in EC2 in AWS.

Before replicating from a protected site to a recovery AWS site, review the following guidelines for AWS environments, and considerations when protecting to AWS: Zerto - Prerequisites & Requirements for Amazon Web Services (AWS)

See also:

- Import Methods for AWS on page 1
- ZertoTools for Windows on page 1
- Creating a Virtual Protection Group on page 21

Import Methods for AWS

During recovery operations, Zerto uses a combination of the following APIs and methods to convert the Amazon S3 objects into recovery disks in EC2 as EBS disks:

- **AWS Import:**
  - **Import-instance:** for the boot volume
  - **Import-volume:** for data volumes

  For more information see the relevant AWS documentation:
  - API_ImportInstance
  - API_ImportVolume

  > **Note:** The ImportImage API is not used by Zerto.

- **Zerto Import - zImport:** an import method that does not have the same limitations as the AWS APIs. It creates an AWS EC2 instance per protected VM volume, called zImporter, to convert the S3 objects and write them to a zImport local disk. When all the data has been imported and its disk has been attached to the recovered instance, the zImport instance is terminated.

  > **Notes:**
  >
  > - zImporter is based on an official AWS Linux AMI (Amazon Machine Image), into which a script is injected to perform the import.

- To ensure that the zImport instance cannot be accessed from the outside world, a security group is created. During a recovery operation the zImport instance is connected to this security group. All inbound traffic is blocked and only outbound traffic to access the script online is allowed. The security group is deleted at the end of the recovery operation.
- Zerto can set default encryption on the S3 bucket so that all objects are encrypted when they are stored in the bucket. To enable S3 encryption please contact support.
- The default zImporter instance type is c5.4xlarge and the AWS EC2 default maximum instance quota is 10. If during the creation of zImport instances the maximum EC2 instance quota is reached, the creation of the next and subsequent zImport instances will be queued, increasing the RTO. If during recovery operations, the ZVM identifies a VPG with the potential to exceed the EC2 instance quota, the user will receive an alert with advice to contact AWS support to increase the service limits in order to improve RTO.
  - Each zImporter VM is responsible for the import process of a single volume. Therefore, it is recommended to contact AWS and increase the maximum instance quota of the c5.4xlarge instance type to the maximum number of volumes you are planning to failover to AWS at once.
- GPT formatted disks are supported for data volumes only, when using either of the zImport methods.
- When using either of the zImport methods, each volume is created with EBS disk of type io1 with maximum 1000 EBS Provision IOPS allocated. EBS disk type can be changed post recovery without downtime, see the relevant for more information see the relevant AWS documentation. The minimum disk size for io1 is 4GB.
- The default Max EBS Provision IOPS quota in a region across all io1 disks is 40000 EBS Provision IOPS, meaning that with 1000 EBS Provision IOPS per volume, the maximum possible number of volumes is 40. If the Max EBS Provision IOPS quota is reached, the failover process will switch to using slower gp2 disks. An event will notify the user of this, and recommend that the user contact AWS support to increase the Max EBS Provision IOPS quota.

- Depending on the desired RTO during recovery operations, or when testing failover, the user can select an import method per VPG or per virtual machine from the following options:
  - Zerto Import for Data Volumes on page 14
  - Zerto Import for All Volumes on page 15
  - AWS Import on page 16

Zerto Import for Data Volumes

This method is the **default setting** and has a faster RTO than AWS Import. This method uses a **combination** of the **AWS import-instance** API for the boot volume, and the **zImport**method for data volumes. To use this method when creating or editing a VPG, an **Access Key ID** and a **Secret Access Key** is required. Both fields can be set in the **Site Settings** window, see Site Settings on page 1.

- **Each machine that you intend to protect** must have at least **250MB free space.** This is because AWS adds files to the recovered machines during failover, move, test failover, and clone operations.
- **Protected boot volumes** are recovered in EC2 as EBS disks with magnetic disk type. Virtual machines with disks that are less than 1GB are recovered with disks of 1GB. Temporary disks may be created based on the selected instance size.
- Temporary disks may be created based on the selected instance size.
- The **maximum** protected **data volume** size is **16TB**, while the **boot volume** can be up to **1TB**.
- The AWS ImportInstance API only supports single volume VMs. The boot volume of the protected virtual machine should not be attached to any other volume to successfully boot. For more information, see http://docs.aws.amazon.com/AWSEC2/latest/APIReference/API_ImportInstance.html

Zerto Import for All Volumes

This method uses the **zImport**method for all volumes and ensures the fastest RTO.

This method creates an AWS EC2 instance per protected VM volume, called zImporter, to convert the S3 objects and write them to a zImport local disk. When all the data has been imported and its disk have been attached to the recovered instance, the zImport instance is terminated.

- Temporary disks may be created based on the selected instance size.
- The **maximum** protected **data volume** size is **16TB**, while the **boot volume** can be up to **2047GiB**.

> **Note:** Some VMs use the MBR partitioning scheme, which only supports up to 2047 GiB boot volumes. If your instance does not boot with a boot volume that is 2TB or larger, the VM you are using may be limited to a 2047 GiB boot volume size. Non-boot volumes do not have this limitation. See AWS Documentation for more information: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html

When recovering to AWS instance types listed below using Zerto Import for All Volumes import method, **Windows 2012**, **Windows 2012R2**, **Windows 2016** or **Windows 2019** are supported.

- C3
- C4
- D2
- I2
- R3
- M4 (excluding M4.16xlarge)

The following drivers are installed on the recovered virtual machine:

- AWS PV Drivers
- Windows ENA (Elastic Network Adapter) Drivers

When recovering to **C5/M5** instances using Zerto Import for All Volumes import method, **Windows 2008R2**, **Windows 2012**, **Windows 2012R2**, **Windows 2016** and **Windows 2019** are supported.

- For **Windows 2012R2**, **Windows 2016** and **Windows 2019**, the following drivers are downloaded on the **protected** virtual machine. ZertoTools installs these drivers on the **recovered** virtual machine:
  - Windows ENA (Elastic Network Adapter) Drivers
  - NVMe driver
- For **Windows 2008R2** and **Windows 2012**, Windows ENA (Elastic Network Adapter) drivers and NVMe driver are downloaded on the **protected** virtual machine. ZertoTools installs these drivers on the **protected** virtual machine and executes the below command:

```
start rundll32.exe sppnp.dll,Sysprep_Generalize_Pnp -wait
```

This command removes computer-specific information for the drivers. When recovering to C5/M5, the instance will boot on AWS and install all the drivers again.

> **Note:** If these drivers are installed on a VM running **Windows 2012**, **Windows 2012R2**, **Windows 2016** or **Windows 2019**, the other AWS import methods will fail. To overcome this, you must uninstall the drivers before using the other AWS import methods.

> **Note:** C5/M5 instance types are supported with the Zerto Import for All Volumes import method only.

> **Important:**
>
> When using this import method for Windows machines, **ZertoTools for Windows** needs to be run on the **protected** Windows virtual machine in VMware **before VPG creation**. For more information, see ZertoTools for Windows on page 17.

AWS Import

This method uses a combination of the **AWS import-instance** and **import-volume** APIs for the boot and data volumes respectively. This was the only method supported until version 5.5. To use this method when creating or editing a VPG, an **Access Key ID** and a **Secret Access Key** is required. Both fields can be set in the **Site Settings** window, see Site Settings on page 1.

- **Each machine that you intend to protect** must have at least **250MB free space.** This is because AWS adds files to the recovered machines during failover, move, test failover, and clone operations.
- **Protected boot volumes** are recovered in EC2 as EBS disks with General Purpose SSD (gp2). Virtual machines with disks that are less than 1GB are recovered with disks of 1GB. Additional volumes might be created in the recovered instance, dependent on the instance type used for the recovery. These volumes can be ignored.
- **Protected volumes** are recovered in EC2 as EBS disks with General Purpose SSD (gp2). Virtual machines with disks that are less than 1GB are recovered with disks of 1GB. Additional volumes might be created in the recovered instance, dependent on the instance type used for the recovery. These volumes can be ignored. Temporary disks may be created based on the selected instance size.
- The **maximum** protected **data volume** and **boot disk** size is **1TB**.
- The AWS ImportInstance API only supports single volume VMs. The boot volume of the protected virtual machine should not be attached to any other volume to successfully boot. For more information, see http://docs.aws.amazon.com/AWSEC2/latest/APIReference/API_ImportInstance.html

ZertoTools for Windows

ZertoTools for Windows is required for protecting VMs running Windows operating system in VMware, while AWS is the recovery site platform. The tool enables the following:

- re-IP for Windows machines upon failback to VMware site when using **Zerto Import for Data Volumes** import method. (Due to AWS expected behavior, VMware tools are removed for virtual machines that were imported from VMware.)
- Supporting **Zerto Import for All Volumes** import method for Windows machines for failover and upon failback to VMware site.

BEST PRACTICE:

It is recommended to install ZertoTools before VPG creation. This ensures that all checkpoints are valid when failing over.

If you install ZertoTools after VPG creation, make sure you select a checkpoint **after** the installations are completed.

ZertoTools Requirements

- ZertoTools supports the following operating systems:
  - 2008R2
  - 2012
  - 2012R2
  - 2016

  - Windows 2019* (*Windows 2019 is supported only if using Zerto Import for All Volumes)
- Run ZertoTools from C: Windows OS drive only.
- .Net Framework 4.5 and up must be installed.

ZertoTools Limitations

- When using the Zerto Import for All Volumes import method, ZertoTools should not be installed on machines with Windows that are **Domain Controllers**.

  When failing over machines with Windows 2012, 2012R2 and 2016 that are Domain Controllers, the Windows Citrix PV drivers need to be downloaded **manually** on the protected machines.

  To download and install Windows PV drivers:

  a. Go to https://www.xenproject.org/downloads/windows-pv-drivers/winpv-drivers-81/winpv-drivers-820.html

  b. Follow the instructions for downloading and installing all Windows PV drivers.
- To failover Windows 2008R2 with Domain Controller, contact Zerto Support.
- Failback for Windows machines with Domain Controller is not supported.

ZertoTools Execution Options

- When recovering to the AWS instance types listed below using Zerto Import for All Volumes import method, **Windows 2012**, **Windows 2012R2**, **Windows 2016** and **Windows 2019** are supported.

  - C3
  - C4
  - D2
  - I2
  - R3
  - M4 (excluding M4.16xlarge)

  - The following drivers are downloaded on the **protected** virtual machine. When recovering to these AWS instance types, ZertoTools installs these drivers on the **recovered** virtual machine:
    - AWS PV Drivers
    - Windows ENA (Elastic Network Adapter) Driver
- When recovering to **C5/M5** instances using Zerto Import for All Volumes import method, **Windows 2008R2**, **Windows 2012**, **Windows 2012R2**, **Windows 2016** and **Windows 2019** are supported.
  - For **Windows 2012R2**, **Windows 2016** and **Windows 2019**, the following drivers are downloaded on the **protected** virtual machine. ZertoTools installs these drivers on the **recovered** virtual machine:
    - Windows ENA (Elastic Network Adapter) Drivers
    - NVMe driver

For **Windows 2008R2** and **Windows 2012**, Windows ENA (Elastic Network Adapter) drivers and NVMe driver are downloaded on the **protected** virtual machine. ZertoTools installs these drivers on the **protected** virtual machine and executes the below command:

```
start rundll32.exe sppnp.dll,Sysprep_Generalize_Pnp -wait
```

This command removes computer-specific information for the drivers. When recovering to C5/M5, the instance will boot on AWS and install all the drivers again.

> **Note:** If these drivers are installed on a VM running **Windows 2012**, **Windows 2012R2**, **Windows 2016** and **Windows 2019**, the other AWS import methods will fail. To overcome this, you must uninstall the drivers before using the other AWS import methods.

> **Note:** C5/M5 instance types are supported with the Zerto Import for All Volumes import method only.

AWS PV Driver

When an instance is created in AWS or when performing Failover using the Zerto Import for Data Volumes and AWS Import methods, by default, Amazon will install the latest version of the AWS PV driver.

When using the **Zerto Import for All Volumes** import method, only the AWS PV driver version **7.4.6** is supported when failing back from AWS to vSphere. ZertoTools installs AWS PV driver version **7.4.6** by default. You can install ZertoTools with the latest AWS PV driver manually but you will be required to downgrade the AWS PV driver before performing Failback to vSphere.

> **Note:** AWS PV driver is not installed when recovering to C5/M5 instance types.

To execute the ZertoTools script:

1. Login to myZerto to access ZertoTools from **myZerto > Support & Downloads > Tools > ZertoTools for Windows**
2. Extract the zip file and copy the **Zerto Tools.bat** to each **protected** Windows virtual machine in VMware.
3. Execute the batch files with one of the following arguments:
   - **-d** (default): ZertoTools will automatically install AWS PV driver version 7.4.6 upon failover to AWS.
   - **-l** (latest): ZertoTools will install the latest version of the AWS PV driver on the instance using the Zerto Import for All Volumes import method. The latest version tested by Zerto is AWS PV driver **version 8.3.1**. **Before failback from AWS to vSphere, you will need to downgrade the AWS PV driver**. For more information on the Downgrade Script, see

Downgrade Script on page 21. (For instances using Zerto Import for Data Volumes and AWS Import methods, the latest AWS PV driver will be installed by Amazon).

- **-q** (quiet mode): Install ZertoTools without any prompt. The default for prompt will be Yes. This argument is relevant only when recovering to C5/M5 instance types with Windows 2008R2 and Windows 2012.
- **-v**: Verify that all required components are downloaded and your machine is ready for failover.
- **-u**: Uninstall ZertoTools.

> **Important:**
>
> When recovering to C5/M5 instances, ZertoTools for Windows can be executed with either **-d** or **-I** arguments.

4. Wait a few minutes and verify you get the following message: **Process successfully finished.**

> **Important:**
>
> If you receive an error message, **DO NOT** perform failover.

5. The script downloads the drivers and installs them upon failover on the AWS machine. If the download of these drivers **fails**, manually download them from the following links:
   - AWS PV driver version **7.4.6**: https://s3.amazonaws.com/ec2-windows-drivers-downloads/AWSPV/7.4.6/AWSPVDriver.zip
   - AWS PV driver version <**Latest**>: https://s3.amazonaws.com/ec2-windows-drivers-downloads/AWSPV/8.3.1/AWSPVDriver.zip
   - Download ENA (Enhanced Network Adapter): https://s3.amazonaws.com/ec2-windows-drivers-downloads/ENA/Latest/AwsEnaNetworkDriver.zip
   - Download the NVMe driver: https://s3.amazonaws.com/ec2-windows-drivers-downloads/NVMe/Latest/AWSNVMe.zip

> **Note:** If you need to download the drivers manually, the zip file name of each driver **should not be changed**.

ZertoTools will also backup the VMtools to ensure re-IP works upon Failback to the protected VMware site.

When running ZertoTools, note the following:

- A folder named **ZertoTools** is created on C:/ProgramData folder.
  This folder must not be deleted.

- Upon failover to AWS, the AWS PV driver update may force reboot of the recovered instances in AWS.

Downgrade Script

If you decide to install the latest AWS PV driver, you will need to downgrade it before failing back to vSphere.

To execute the downgrade script:

1. Login to the **protected AWS instance** and locate the AWS PV driver version.
2. Backup the AWS instance on which you're going to downgrade the AWS PV driver.
3. Copy the entire directory from **myZerto > Support & Downloads > Tools > Downgrade Script** to the AWS protected instance.
4. Execute the batch file (not the MSI file).

> **Important:**
>
> Your AWS machine may need to reboot a few times upon execution of the batch files.

5. After a few minutes, connect to the AWS instance and verify that the AWS PV driver is **version 7.4.6**.

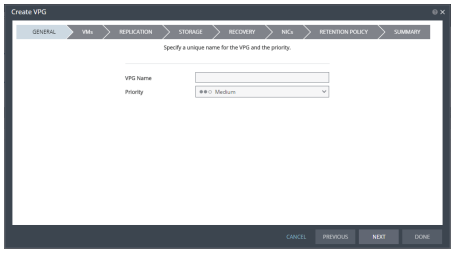
If you installed ZertoTools after VPG creation, wait for the next checkpoint to be created before performing failover.

Creating a Virtual Protection Group

To create a virtual protection group (VPG):

1. In the Zerto User Interface on the protected site, either VMware vSphere or Microsoft Hyper-V, select **ACTIONS > CREATE VPG**.

   The **NEW VPG** step of the Create VPG wizard is displayed.



2. Specify the name of the VPG and the priority of the VPG.

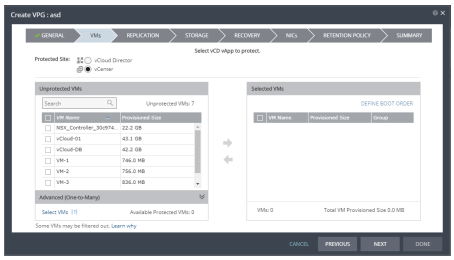
   VPG Name: The VPG name must be unique.

   Priority: Determine the priority for transferring data from the protected site to the recovery site when there is limited bandwidth and more than one VPG is defined on the protected site. When

there are updates to virtual machines protected in VPGs with different priorities, first the updates from the VPG with the highest priority are passed over the WAN. Medium priority VPGs will only be able to use whatever bandwidth is left after the high priority VPGs have used it. This is also true between medium and low priorities.

3. Click **NEXT**.

   The VMs step is displayed.



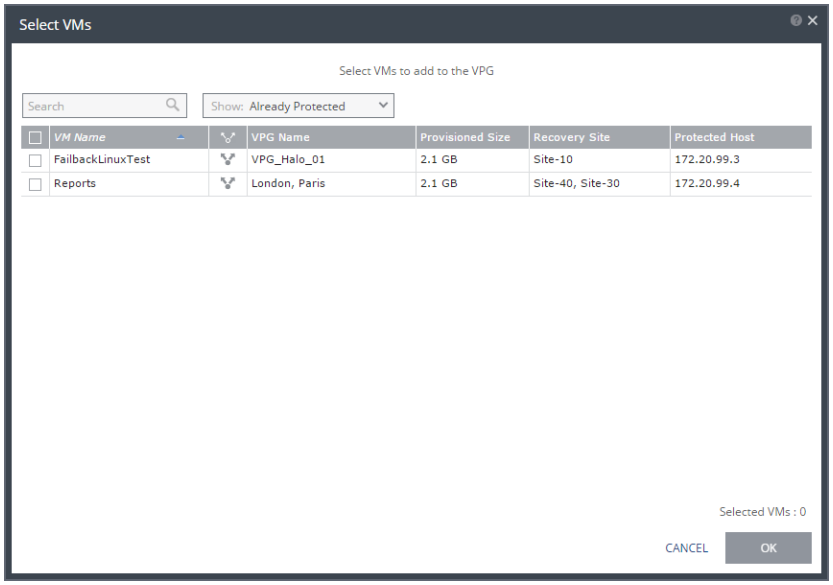
4. Select the VMs that will be part of this VPG and click the right-pointing arrow to include these VMs in the VPG.

   - Zerto uses the SCSI protocol. Only virtual machines with disks that support this protocol can be specified.
   - When using the **Search** field, you can use the wildcards; ***** or **?**

   Virtual machines that are not yet protected are displayed in the list. A VPG can include virtual machines that are not yet protected and virtual machines that are already protected.

5. You can view protected virtual machines in the **Advanced (One-to-Many)** section, by clicking **Select VMs**.

   The Select VMs dialog is displayed.



> **Note:** Virtual machines can be protected in a maximum of three VPGs. These VPGs cannot be recovered to the same site. Virtual machines protected in the maximum number of VPGs are not displayed in the Select VMs dialog.

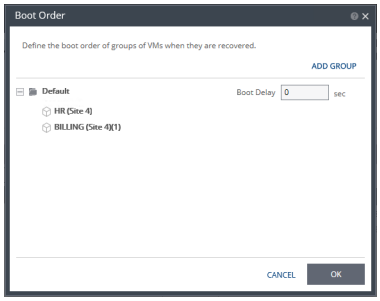
In on-premise environments, protecting virtual machines in several VPGs is enabled only if both the protected site and the recovery site, as well as the VRAs installed on these sites, are of version 5.0 and higher.

6. To define the boot order of the virtual machines in the VPG, click **DEFINE BOOT ORDER**, otherwise go to the next step.

   When virtual machines in a VPG are started in the recovery site, by default these machines are not started up in a particular order. If you want specific virtual machines to start before other machines, you can specify a boot order. The virtual machines are defined in groups and the boot order applies to the groups and not to individual virtual machines in the groups. You can specify a delay between groups during startup.

   > **Note:** Up to 20 virtual machines may boot on a host simultaneously. Following the boot, a 15 second (default) delay occurs until the next boot batch.

   Initially, virtual machines in the VPG are displayed together under the Default group. If you want specific machines to start before other virtual machines, define new groups with one or more virtual machines in each group.



   a. Click **ADD GROUP** to add a new group.

   b. To change the name of a group, click the Pencil icon next to the group. To delete a group, click the delete icon on the right side. You cannot delete the `Default` group nor a group that contains a virtual machine.

   c. Drag virtual machines to move them from one group to another.

   d. Drag groups to change the order the groups are started.

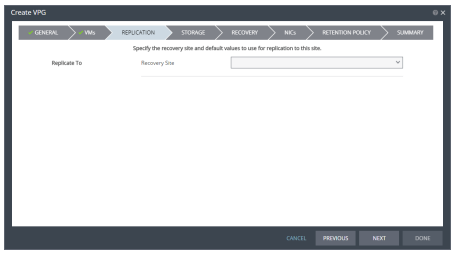
   e. Optionally, in `Boot Delay`, specify a time delay between starting up the virtual machines in the group and starting up the virtual machines in the next group. For example, assume three groups, Default, Server, and Client, defined in this order. The boot delay defined for the Default group is 10, for the Server group is 100, and for the Client group 0. The virtual machines in the

Default group are started together and after 10 seconds the virtual machines in the Server group are started. After 100 seconds the virtual machines in the Client group are started.

f. Click **OK**.

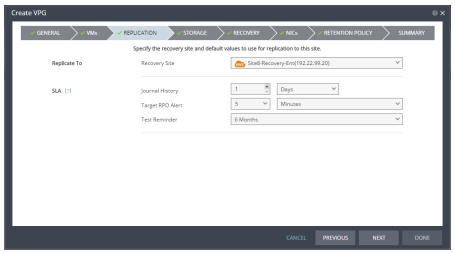
7. Click **NEXT**.

The REPLICATION step is displayed.



> **Note:** If the protected site is paired with only one recovery site, the recovery step is displayed with the `Recovery Site` field automatically filled in and defaults set for the fields that are relevant for AWS.

8. Specify the recovery site and the values to use when replicating to this site.

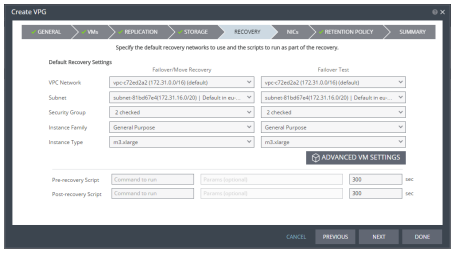


Recovery Site: The site to which you want to recover the virtual machines.

As soon as you specify that the recovery site is on AWS, the display changes to show only fields that are relevant for AWS.

9. The following settings can be changed later by editing the VPG definition. For your first VPG, leave the default values and click **NEXT**.

After clicking NEXT, the RECOVERY step is displayed. Recovery details include the networks to use for failover, move, and testing failover, and whether scripts should run as part of the recovery process.



> **Note:** Steps that do not require input are marked with a check mark. You can jump directly to a step that has been marked with a check mark to edit the values for that step. Every step must be marked with a check mark before you can click **DONE** to create the VPG.

10. Select recovery settings for failover/move and failover testing.

    VPC Network: The virtual network dedicated to your AWS account.

    Subnet: The subnet mask for the VPC network.

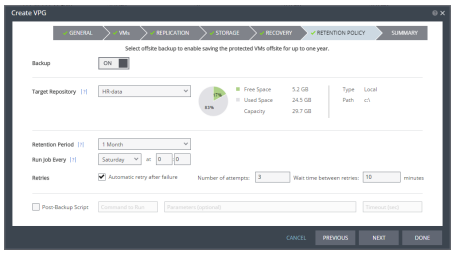
    Security Group: The AWS security to be associated with the virtual machines in this VPG.

    Instance Family: The instance family from which to select the type. (AWS instance families are optimized for different types of applications. Choose the instance family appropriate for the application in the VPG.)

    Instance Type: The instance type, within the instance family, to assign to recovered instances. Different types within an instance family vary primarily in vCPU, ECU, RAM, and local storage size. The price per instance is directly related to the instance size.

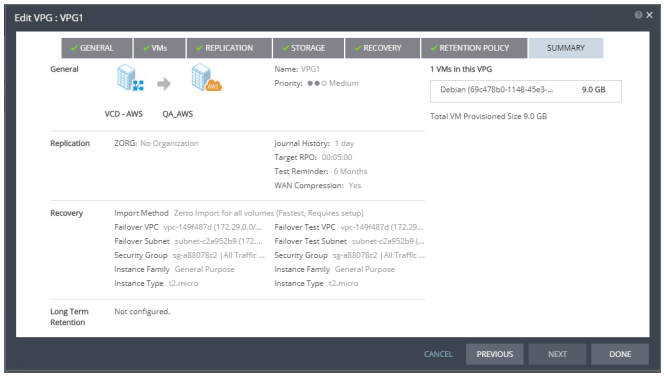
11. Click **NEXT**.

    The BACKUP step is displayed. Backup properties govern the VPG backup, including the repository where the backups are saved. Backup extends the ability to recover virtual machines in a VPG going back one year.



12. Again, leave the defaults and click **NEXT**.

    The SUMMARY step is displayed. It shows the VPG configuration that you defined in previous tabs.



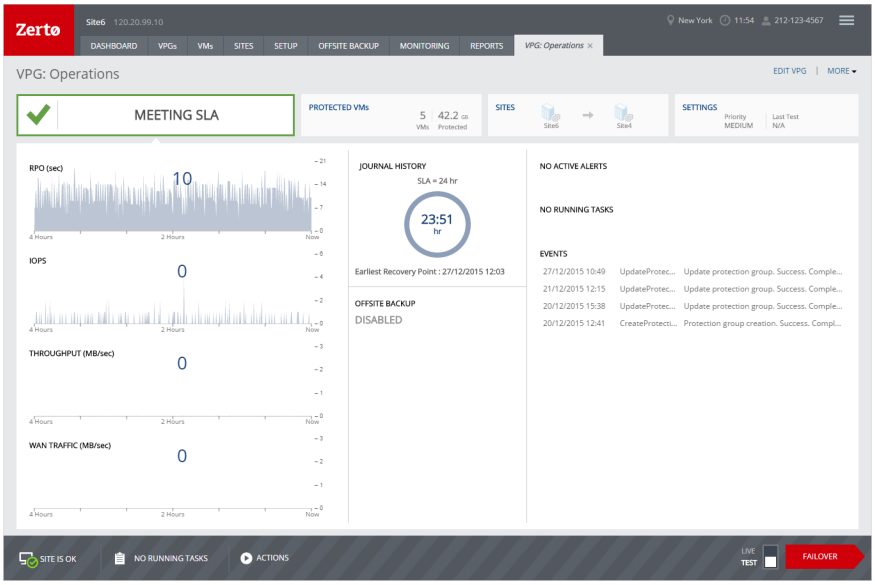
13. Click **DONE**.

    The VPG is created.

The VRA in the recovery site is updated with information about the VPG and then the data on the protected virtual machines are synchronized with the replication virtual machines managed by the VRA on the recovery site. This process can take some time, depending on the size of the VMs and the bandwidth between the sites.

> **Note:** For synchronization to work, the protected virtual machines must be powered on.

Once synchronized, the VRA on the recovery site includes a complete copy of every virtual machine in the VPG. After synchronization, the virtual machines in the VPG are fully protected, meeting their SLA, and the delta changes to these virtual machines are sent to the recovery site.



To verify that the disaster recovery that you have planned is the one that will be implemented, Zerto recommends testing the recovery of the VPGs defined in the protected site to the recovery site.

Testing Disaster Recovery

Use the *Failover Test* operation to test that during recovery the virtual machines are correctly replicated at the recovery site. The Failover Test operation creates test virtual machines - instances - in a sandbox, using the test network specified in the VPG definition.

The Failover Test operation has the following basic steps:

- Starting the test.
  - The test virtual machine instances are created in AWS and configured to the checkpoint specified for the recovery.
  - The new instances are powered on, making them available to the user. If applicable, the boot order defined in the VPG settings is used to power on the machines.
- Testing. The virtual machines in the VPG are created as instances in a sandbox and powered on for testing.
- Stopping the test.
  - The instances in AWS are powered off and removed from the inventory.
  - The following tag is added to the checkpoint specified for the test: `Tested at` *startDateAndTimeOfTest*
  - The updated checkpoint can be used to identify the point-in-time to restore the virtual machines in the VPG during a failover.

Testing that recovery is accomplished successfully should be done periodically so that you can verify that a failover will work. Zerto also recommends testing all the VPGs being recovered to the same cluster together.

When configuring a VPG, specify the period between tests for that VPG in the `Test Reminder` field in the REPLICATION step of the Create VPG wizard.

Starting a Failover Test

You can test a single VPG or multiple VPGs to make sure that if an actual failover is needed, the failover will perform as expected.

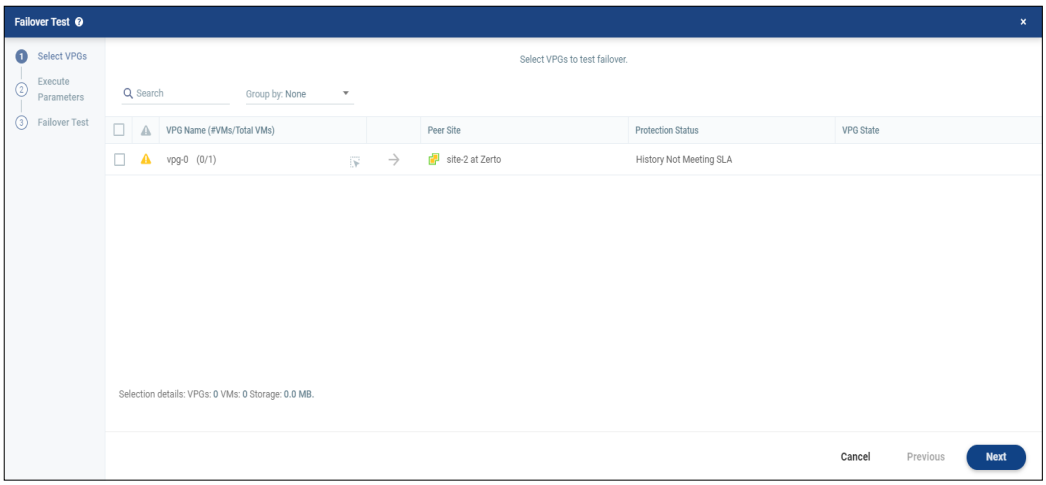
> **Note:** You can initiate the failover test from either the protected site or recovery site.

To test failover:

1. In the Zerto User Interface click 

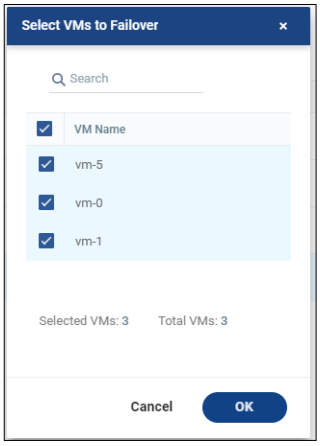
.

   The Failover Test wizard is displayed.



2. Select the VPGs to test. By default, all VPGs are listed.

   a. To select specific VMs in a VPG, click the icon next to each VPG to get a list of VMs. The Select VMs to Failover dialog is displayed. By default, all VMs are selected.



   b. Select the VMs to test.

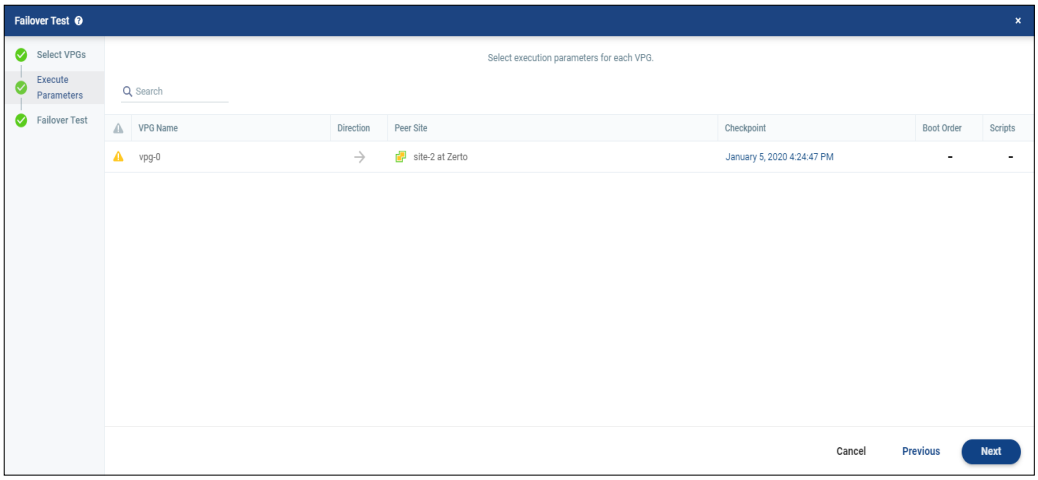
> **Note:** Selecting specific VMs in a VPG to failover is not supported when replicating from a **vCD site**.

   At the bottom, the selection details show the amount of data and the total number of virtual machines selected.

   The **Direction** arrow shows the direction of the process: from the protected site to the peer, recovery, site.

3. Click **NEXT**.

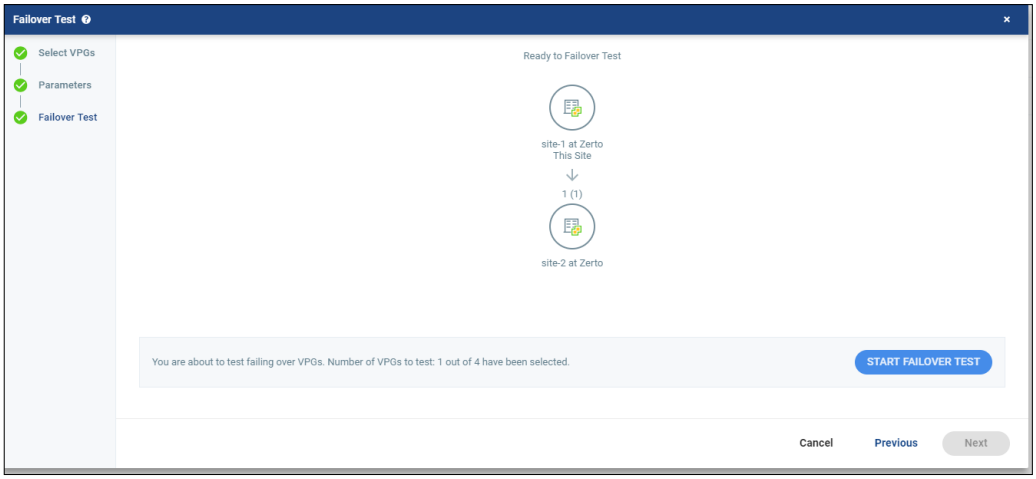
   The **PARAMETERS** step is displayed.



You can select the checkpoint to use for the recovery and see if a boot order and scripts are defined for the VPG.
By default, the last checkpoint added to the journal is displayed. The checkpoints determine the RPO and ensure crash consistency and write-fidelity when the virtual machines in a VPG are recovered. These checkpoints are written every few seconds and you can recover to any of the available checkpoints.

4. Click **NEXT**.

   The FAILOVER TEST step is displayed. The topology shows the number of VPGs and virtual machines being tested to failover to each recovery site.



5. To start the test, click **START FAILOVER TEST**.

   The test starts for the selected VPGs. The test begins with an initialization period during which the virtual machines are created in the recovery site.

The test starts for the selected VPGs. The test begins with an initialization period during which the new instances are created in AWS. The protected virtual machines are created as new instances in EC2. These instances are defined as m3.xlarge instances except in the Asia Pacific (Seoul) region where they are defined as m4.xlarge instances. If these instances do not meet your needs, you can manually stop the instance, change the instance type, and restart the instance. For more information, contact Zerto Support.

If you did not define a private IP for a virtual machine in the VPG definition, during recovery AWS sets the private IP from the defined subnet range.

After Starting a Test, What Happens?

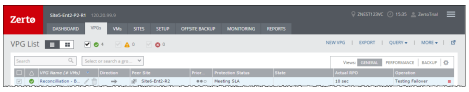
The virtual machines in the virtual protection group are created in AWS. In the AWS console, the new virtual machines appear with their original names and the suffix *testing recovery*.

While a test is running:

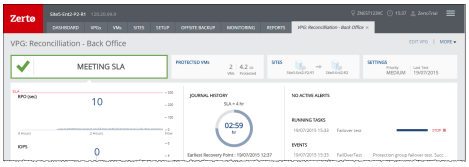
- The virtual machines in the VPGs continue to be protected.
- You can add checkpoints to the VPGs, and if necessary fail over the VPGs.
- You cannot move VPGs being tested.
- You cannot initiate a failover while a test is being initialized or closed.

Monitor the status of a failover test by doing the following:

- In the Zerto User Interface, click the VPGs tab. The `Operation` field in the GENERAL view displays Testing Failover when a failover test is being performed.



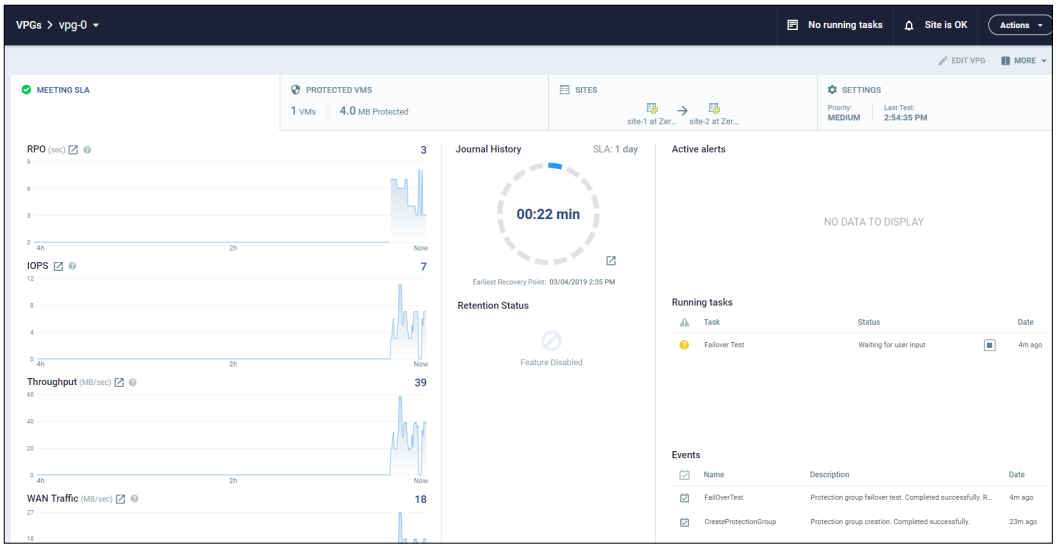
- In the Zerto User Interface, click the **VPGs** tab, and then click the name of a VPG you are testing. A dynamic tab is created displaying the specific VPG details including the status of the failover test.



Stopping a Failover Test

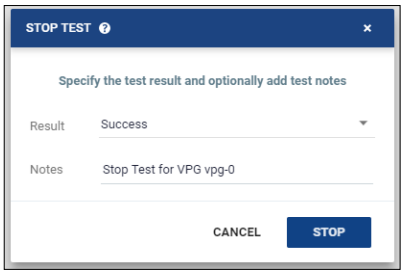
To stop a failover test:

1. Click the **Stop** icon, in either the Dashboard or the dynamic tab, to stop the test in the specific VPG tab.



You can also stop the test via the TASKS popup dialog in the status bar, or by selecting **MONITORING > TASKS**.

The Stop Test dialog is displayed.



2. In the Result field specify whether the test succeeded or failed.
3. Optionally, in the Notes field, add a description of the test. For example, specify where external files that describe the tests performed are saved. Notes are limited to 255 characters.
4. Click **STOP**.

5. In the Result field specify whether the test succeeded or failed.
6. Optionally, in the Notes field, add a description of the test. For example, specify where external files that describe the tests performed are saved. Notes are limited to 255 characters.
7. Click **STOP**.

After stopping a test, the following occurs:

- Virtual machines in the recovery site are powered off and removed.
- The resource group created for the operation is deleted.
- The checkpoint that was used for the test has the following tag added to identify the test: Tested at startDateAndTimeOfTest.

This checkpoint can be used to identify the point-in-time to use to restore the virtual machines in the VPG during a failover.

Zerto

Zerto enhances the Zerto IT Resilience Platform by converging disaster recovery and backup to deliver continuous availability within a simple, scalable platform. Zerto delivers enhanced analytics, platform improvements and cloud performance upgrades required in the future of IT resilience.

Learn more at Zerto.com.

For assistance using Zerto's Solution, contact: @Zerto Support.