Zerto Virtual Replication Test Plan
Microsoft Azure Environment
Version 5.5
The Zerto Virtual Replication test plan environment should be designed to support the required software components and TCP connectivity described in the Zerto Virtual Replication Installation Guide.

Accessing the Zerto User Interface

You manage replication in your protected site environment, including the protection and replication of virtual machines between the protected and recovery sites, using the Zerto User Interface.

You can test Zerto Virtual Replication using the Zerto User Interface, which can be accessed from either the protected site or the recovery site.

To access the Zerto User Interface in an Azure recovery site:
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 Azure site. Ensure that port 9669 is open and set as an inbound rule in the security group of the instance where Zerto Virtual Replication is installed.

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

To access the Zerto User Interface in a VMware vSphere protected site:
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 site you want to manage.
2. Log in using the user name and password for the vCenter Server connected to the Zerto Virtual Manager.

To access the Zerto User Interface in a Microsoft SCVMM protected site:
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 site you want to manage.
2. Log in using the user name and password for the machine where you installed Zerto Virtual Replication.

   **Username** – The user name of the user for the machine where the Zerto Virtual Manager is installed. If the user is part of a domain, you must also specify the domain, with the following format: domain\username

   **Password** – A valid password for the given user name.

Continue with Zerto Virtual Replication Tests.

Zerto Virtual Replication Tests

This document includes the following tests:

- **Test 1**: Create a VPG
- **Test 2**: Test failing over the VPG
- **Test 3**: Add a VM to an existing VPG
- **Test 4**: Configure a recovery VM IP address
- **Test 5**: Restore a file from the recovery site

These tests demonstrate the basic Zerto Virtual Replication functionality.

Before you begin the tests, make sure you review Requirements for Microsoft Azure Environments.
These tests demonstrate the basic Zerto Virtual Replication functionality.

### TEST 1: CREATE A VPG

**Procedure**

- In the Zerto User Interface for the protected site, select **ACTIONS > CREATE VPG**.

  ![Create VPG screen](image1)

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

  - Specify the name of the VPG. Leave the default value for the **Priority**.

  ![Create VPG wizard](image2)

  - Click **NEXT** and select the virtual machine to be protected and click the arrow pointing right to include this machine in the VPG.

    ![Select VMs screen](image3)

  - To select virtual machines that are already protected in other VPGs, click **Select VMs**.
TEST 1: CREATE A VPG (CONTINUED)

- Click NEXT.

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

  ![Create VPG dialog]

- Click NEXT to select the default recovery settings.

  ![Create VPG settings]

  Select the settings for both failover/move and failover test operations.

  - **VNet** - The virtual network dedicated to your Azure subscription.
  - **Subnet** - The subnet or the VNet network.
  - **Network Security Group** - The Azure network security to be associated with the virtual machines in this VPG. You can associate one network security group with the virtual machines. The NIC will be associated with the network security group defined at the virtual machine level.
  - **Instance Family** - The instance family from which to select the size. Azure instance families are optimized for different types of applications. Choose the instance family appropriate for the application being protected in the VPG.
  - **Instance Size** - The instance size, within the instance family, to assign to recovered instances. Different sizes within an instance family vary, for example in a number of cores, RAM, and local storage size. Choose the instance size appropriate for the application being protected in the VPG. The price per instance is related to the instance configuration.

- Continue clicking NEXT to review the remaining settings (BACKUP and SUMMARY) but leave these with the default values and click DONE.

**Expected result**  A VPG is created with initial syncing, resulting in Meeting SLA, protecting, status.
### Notes

When creating a VPG, add the virtual machines that are part of an application to the VPG such as the machine hosting the application as well as the web server and database machines, if these are required to successfully run the application. Only virtual machines that are supported by Azure can be protected by Zerto Virtual Replication. Refer to Azure documentation for the supported operating systems, which include the following:

- **Windows (32- and 64-bit)**
  
  **Note:** .NET 3.5 or higher must be installed on the Windows machine.

- **Linux/Unix (64-bit)**

  **Note:** By default, every Azure virtual machine is created with additional temporary disk. This disk is in addition to the disks associated with each protected virtual machine.

The following limitations apply when protecting to Azure:

- You cannot protect machines that have a disk larger than 1TB.
- The protected virtual machines needs to have at least one NIC.
- The supported number of data disks per virtual machine is dependent on the selected instance size. For example, instance size D3_v2 allows up to eight data disks per virtual machine.
- Virtual machines with UEFI Firmware cannot be protected.

To create a VPG that will be recovered to Azure, you must have a virtual machine in Azure with a Zerto Cloud Appliance installed on it. This ZCA must be paired with the protected site.

### Actual Result

*Replace with actual result.*
TEST 2: TEST FAILING OVER THE VPG

Procedure

- In the Zerto User Interface for either the protected or recovery sites set the operation to TEST and click FAILOVER.

- In the Failover Test wizard, select the VPG to test.
- Click NEXT to review the test setting that are available but leave the defaults.

- Click NEXT and to start the test, click START FAILOVER TEST.

  **Note:** If any of the VPGs have at least one VM configured with a static IP, but the static IP is in use on the recovery site, a warning message appears enabling you to choose whether to continue with a dynamic IP, or to cancel the failover process.

- Verify that the test virtual machine was recovered successfully by checking that the virtual machine files are up to date.

- Click the Stop test icon to stop the test in the specific VPG tab or via the TASKS popup dialog in the status bar, or in the TASKS tab under the MONITORING tab.

- In the Stop Test dialog, in the Result field, specify whether the test succeeded or failed.
- Optionally, in the Notes field, add a description of the test. For example, specify where external files that describe the tests performed are saved.
- Click STOP.
TEST 2: TEST FAILING OVER THE VPG (CONTINUED)

- Create a text file on each protected virtual machine. After creating the text file wait a few minutes before creating a second text file on each machine.
- In the Zerto User Interface, set the operation to TEST and click FAILOVER. The Failover Test wizard is displayed.
- In the Failover Test wizard, select the VPG to test.
- Click NEXT to set the checkpoint for the test.

![Failover Test Wizard](image)

- Click the Checkpoint link.
The {VPG-Name}: Checkpoints dialog is displayed.

![Checkpoint Dialog](image)

- Select a checkpoint to recover to. Specify a checkpoint between the times the two text files on each machine were created.
- Click OK.
- Click NEXT and to start the test, click START FAILOVER TEST.

**Note:** If any of the VPGs have at least one VM configured with a static IP, but the static IP is in use on the recovery site, a warning message appears enabling you to choose whether to continue with a dynamic IP, or to cancel the failover process.

- Verify that the protected test virtual machines were recovered successfully to the desired points-in-time by verifying the text file contents of the recovered virtual machines files.
- Click the Stop test icon to stop the test as described above and in the Stop Test dialog in the Result field specify whether the test succeeded or failed and then click STOP.

<table>
<thead>
<tr>
<th>Expected result</th>
<th>The recovery virtual machine is created in the recovery site with the name <code>vmname - failover test</code>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notes</td>
<td>Zerto Virtual Replication enables recovering to any checkpoint that is displayed, even as soon as 10 seconds after the disaster. This provides an almost zero RPO.</td>
</tr>
<tr>
<td>Actual Result</td>
<td>Replace with actual result.</td>
</tr>
</tbody>
</table>
### TEST 3: ADD A VM TO AN EXISTING VPG

**Procedure**
- In the Zerto User Interface for either the protected or recovery sites, select the VPG in the VPGs tab and click **MORE > Edit VPG**. You can also select the VPG to display the VPG details and click **EDIT VPG**. The **Edit VPG** wizard is displayed, enabling editing the VPG, including adding and removing virtual machines from the VPG.
- In the **VMs** step, select the virtual machine to be added to the VPG and click the arrow pointing right to include this machine in the VPG.
- Click **DONE**.

**Expected result**
The VPG definition is updated, and then the additional virtual machine is synced with the recovery site. When the sync process for the virtual machine is complete, Zerto Virtual Manager adds a checkpoint: **VM ‘XXX’ is fully synced** where XXX is the name of the virtual machine that was synced.

**Actual Result**
*Replace with actual result.*
TEST 4: CONFIGURE A RECOVERY VM IP ADDRESS

Procedure

■ In the Zerto User Interface, in the VPGs tab, select the VPG and click MORE > Edit VPG.
■ In the Edit VPG wizard, in the RECOVERY step, specify network details to use for the recovered virtual machines after a live failover, a test failover, or migration.

![Image showing the Edit VPG wizard](https://via.placeholder.com/150)

■ Click ADVANCED VM SETTINGS to set a specific private IP address for each virtual machine.

![Image showing Advanced VM Settings](https://via.placeholder.com/150)

■ Select a virtual machine and click EDIT SELECTED. The Edit VM Settings dialog is displayed.

![Image showing Edit VM Settings](https://via.placeholder.com/150)

■ In the Failover Test column, specify a private IP to use for the recovered virtual machine when testing replication and click SAVE and then in the Edit VPG wizard, click DONE.
■ Check that recovered virtual machines will have the IP you defined by running Test 2: Test failing over the VPG.

Expected result

The VPG is updated. In a failover test, the IP address of the virtual machines will be the settings that were defined.

Notes

You can use the same procedure for a failover or move operation via the Failover/Move Recovery column.

Actual Result

Replace with actual result.
TEST 5: RESTORE A FILE FROM THE RECOVERY SITE

Procedure

- In the Zerto User Interface select ACTIONS > RESTORE FILE.
  The File and Folder Restore: Select VM wizard is displayed.
- Select the virtual machine on which the file or folder to be restored is located and click NEXT.

The CHECKPOINT step is displayed. By default, all available checkpoints are displayed.

- Select the checkpoint from which to recover the file or folder and click NEXT.
  The DISK step is displayed. All disks associated with the selected virtual machine are displayed.

- Select a disk to mount and click NEXT.
TEST 5: RESTORE A FILE FROM THE RECOVERY SITE (CONTINUED)

The MOUNT step is displayed with the settings you selected.

- Click START MOUNT to mount the disk.

  Mounting the disk may take some time, depending on the selected checkpoint and the number of files and folders on the disk. When the disk is mounted, icons appear next to the completed task.

- Click the folder icon ( ) to browse the files and folders on the disk.

  **Note:** Click the unmount icon ( ) to unmount the disk without restoring any files or folders.

The File and Folder Restore: Download wizard is displayed.

- Click NEXT.

  The FILE/FOLDER step is displayed.

- Select the files and folders you want to download.

  The selected files or folders are displayed in the right pane.
Click NEXT.
The DOWNLOAD step is displayed with details of the files and folders to restore.

**Note:** By default, when you select multiple files or one or more folders, the data is compressed before it is downloaded. If you select only one file, for download, you can choose whether or not the file is compressed.

3. Click START DOWNLOAD.
   The files and folders are downloaded to the downloads folder on the computer where you ran the download.

<table>
<thead>
<tr>
<th><strong>Expected result</strong></th>
<th>The file or folder you selected to restore is downloaded to the computer from which you ran the restore. The file is restored with its name unless it is zipped, in which case it is in the ZertoDownloads.zip file.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Notes</strong></td>
<td>Zerto recommends that you unmount the disk after the files or folders are downloaded.</td>
</tr>
<tr>
<td><strong>Actual Result</strong></td>
<td>Replace with actual result.</td>
</tr>
</tbody>
</table>
Requirements for Microsoft Azure Environments

- Azure ZCA can be installed only on Windows Server 2012 R2 and higher.
- Only virtual machines that are supported by Azure can be protected by Zerto Virtual Replication. All Windows operating systems are supported.
  
  **Note:** Microsoft does not support operating systems that are past the **End of Support date**, without a **Custom Support Agreement (CSA)**. For more information about Microsoft operating systems support for Microsoft Azure, refer to [https://support.microsoft.com/en-us/kb/2721672](https://support.microsoft.com/en-us/kb/2721672).

- To replicate between Azure and your site, you must have a virtual machine in Azure with a Zerto Cloud Appliance installed on it. This ZCA **must be paired with your site**.
- For **Linux** distribution, refer to Azure documentation:

Requirements for Replication From Azure

- For Virtual Machines to be protected from Azure, the VM volumes must reside in the Standard storage account defined during ZCA installation.
  
  A Standard storage account is created or selected upon ZCA installation.
  - Type: Standard storage
  - Recovery and journal volumes reside on this Zerto Storage Account
  - Azure VMs with all disks on this Zerto Storage Account can be protected by Zerto.
  - Blob Storage is not supported.
  - VMs which are not deployed via the Azure Resource Manager cannot be protected from Azure.

Requirements for Replication To Azure

- Protected volumes are recovered in Azure as **VHD disks** in a page blob. Virtual machines with disks that are less than 1GB are recovered with disks of 1GB.
  
  **Note:** For some instance sizes, the Azure virtual machine is created with a Local SSD disk which is a temporary disk. This disk is in addition to the disks associated with each protected virtual machine.

- The following **limitations** apply when protecting to Azure
  - Virtual machines with **UEFI Firmware** cannot be protected.
  - You **cannot** protect machines that have a disk **larger than 4 TB**.
  - The **protected** virtual machines needs to have **at least one NIC**.
  - Reserve at least **2 CPUs** and **4GB RAM** for the machine using a subnet accessible by other Zerto Virtual Replication sites.
  - The **supported** number of **data disks and NICs per virtual machine** is dependent on the selected instance size. For example, instance size D3_v2 allows up to eight data disks per virtual machine.

Additional Azure Considerations

For additional considerations, see **Azure subscription and service limits, quotas and constraints**: [https://docs.microsoft.com/en-us/azure/azure-subscription-service-limits](https://docs.microsoft.com/en-us/azure/azure-subscription-service-limits).

For example from the link, see the following default values:

- There can be multiple Zerto Cloud Appliances per Azure subscription and region.
- **20 cores per subscription**
- **200 Storage accounts per subscription**
- **20 VMs per region per subscription**
- **20 VMs per series (Dv2, F, etc.) cores per subscription per Region**

Additionally, see the following example for **maximum** values:
- A Standard storage account has a maximum total request rate of 20,000 IOPS. The total IOPS across all of your virtual machine disks in a Standard storage account should not exceed this limit.

<table>
<thead>
<tr>
<th>VM TIER</th>
<th>BASIC TIER VM</th>
<th>STANDARD TIER VM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk size</td>
<td>4 TB</td>
<td>4 TB</td>
</tr>
<tr>
<td>Max 8 KB IOPS per persistent disk</td>
<td>300</td>
<td>500</td>
</tr>
<tr>
<td>Max number of disks performing max IOPS</td>
<td>66</td>
<td>50</td>
</tr>
</tbody>
</table>

See also "Azure Limitations Which Affect Installation and Recoverability", on page 15.

**Azure Limitations Which Affect Installation and Recoverability**

Below are the default Azure limitations which affect installation and recovery.

**Default Azure limitations which Affect Installation**

- **Storage Limitations:**
  - Number of storage accounts: **200 per subscription** (note: max is 250)

**Default Azure Limitations which Affect Recovery**

<table>
<thead>
<tr>
<th>Virtual Machines Limitations</th>
<th>VMs per subscription per region: 20 (max: 10K)</th>
<th>VM total cores per subscription per region: 20</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance sizes:</td>
<td>Limited per region.</td>
<td>Many of them are 20 cores per region per subscription</td>
</tr>
<tr>
<td>Resource groups per subscription: 800</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Networking</th>
<th>Network interfaces per region: 350</th>
<th>NICs per instance: Depends on instance size:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private IP Addresses per VNET per subscription per region: 4096</td>
<td></td>
<td>Cloning of IP addresses during recovery operations: A different static IP should not be configured for virtual machines with a Linux operating system. Configuring a different static IP for these machines <strong>will cause them not to boot.</strong></td>
</tr>
</tbody>
</table>

**Requirements for Microsoft Azure Environments**
### Requirements for Microsoft Azure Environments

| Storage | Storage account total size limitation: 500 TB  
(# of entities (blobs, containers etc) within a storage account: unlimited) |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Max size of a page blob (vhd): 4 TB</td>
</tr>
<tr>
<td></td>
<td>Min size of a page blob (vhd): 20 MB</td>
</tr>
<tr>
<td></td>
<td>Max number of data disks: Depends on instance size</td>
</tr>
</tbody>
</table>