Zerto Virtual Replication provides a business continuity (BC) and disaster recovery (DR) solution in a virtual environment, enabling the replication of mission-critical applications and data as quickly as possible, 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 Virtual Replication enables a virtual-aware recovery with low values for both the RTO and RPO. In addition, Zerto Virtual Replication enables protecting virtual machines for extended, longer term recovery from an offsite backup.

This document provides a quick guide to setting up Zerto Virtual Replication to recover virtual machines in Microsoft Azure (MA). The virtual machines can be protected by Zerto Virtual Replication in either VMware vSphere or Microsoft Hyper-V.

To learn about replicating from Azure, see the Azure Zerto Virtual Manager Administration Guide.

---

**Table of Contents**

- **Introduction** ................................................................. 1
- **Recommended Installation Best Practices** .......................... 3
- **Installation** ..................................................................... 3
- **Registering the Zerto Virtual Replication License** ................. 7
- **Pairing Sites to Enable Replicating From One Site to Another Site** ................................................................. 8
- **Setting Up the Protected Site** .............................................. 8
- **Protecting Virtual Machines** ............................................... 8
- **Testing Disaster Recovery** .................................................. 14

---

**Introduction**

You install a Zerto Cloud Appliance (ZCA) in the Microsoft Azure site that is to be used for recovery. The Zerto Cloud Appliance is comprised of the following:

- **Zerto Virtual Manager** (ZVM) - A Windows service that manages everything required for the replication between the protected site and Azure, except for the actual replication of data. Each Zerto Virtual Manager can manage up to 5000 virtual machines, either being protected or recovered to that site.

- **Virtual Replication Appliance** (VRA) - A Windows service that manages the replication of data from protected virtual machines to Azure. A Virtual Replication Appliance can manage a maximum of 500 volumes.

- **Virtual Backup Appliance** (VBA) - A Windows service that manages back-ups within Zerto Virtual Replication and is responsible for the repositories where offsite backups are stored. These repositories can be local or on a shared network.

- **Zerto User Interface** - Recovery using Zerto Virtual Replication is managed by the Zerto User Interface in a web browser.

**Requirements for the Azure Site**

For information about requirements and restrictions, see Zerto Virtual Replication Requirements for Microsoft Azure Environments.

**Routable Networks**

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

Zerto Virtual Replication 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

Microsoft Windows Explorer 9 is not supported and version 10 does not work well with the user interface. Zerto recommends using Chrome, Firefox, or later versions of Internet Explorer. The minimum recommended screen resolution is 1024*768.

Open Firewall Ports

The following architecture diagram shows the **ports** that must be opened in the firewalls on all sites.

The following table provides basic information about the ports shown in the above diagram by Zerto Virtual Replication. Zerto Cloud Appliance (ZCA) requires the following **ports** to be open in the **Azure site firewall**, set in the **Azure network security group**:

<table>
<thead>
<tr>
<th>PORT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>Required between the ZVM and the Azure Cloud environment.</td>
</tr>
<tr>
<td>443</td>
<td>Required between the Azure REST Service and the ZVM during installation of a VRA.</td>
</tr>
<tr>
<td>4005</td>
<td>Log collection between the ZVM and site VRAs.</td>
</tr>
<tr>
<td>4006</td>
<td>Communication between the ZVM and local site VRAs and the site VBA.</td>
</tr>
<tr>
<td>4007</td>
<td>Control communication between protecting and peer VRAs.</td>
</tr>
<tr>
<td>4008</td>
<td>Communication between VRAs to pass data from protected virtual machines to a VRA on a recovery site.</td>
</tr>
<tr>
<td>4009</td>
<td>Communication between the ZVM and local site VRAs to handle checkpoints.</td>
</tr>
<tr>
<td>9779</td>
<td>Communication between ZVM and ZSSP (Zerto Self Service Portal).</td>
</tr>
</tbody>
</table>

*The default port provided during the ZVR installation which can be changed during the installation.*
Recommended Installation Best Practices

Zerto recommends the following best practices:

- Install Zerto Virtual Replication on a dedicated virtual machine with a dedicated administrator account.
- It is required to exclude the Zerto Virtual Replication folder from antivirus scanning. Failure to do so may lead to the ZVR folder being incorrectly identified as a threat and in some circumstances corrupt the ZVR folder.

**Installation**

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

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

**Performing an Express Installation**

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

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

**To perform an express install of Zerto Virtual Replication:**

1. Run the Zerto installation executable for Azure. It has a format like:
   

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

3. Click **NEXT**.
4. Click **AUTHENTICATE**.
An external Microsoft Azure authentication window is displayed.

5. In the **external Microsoft Azure authentication page**, specify the following:
   a) The email or phone number of the account who is the Azure subscription User Access Administrator.
For instruction on how to add a user as a subscription User Access Administrator, see https://azure.microsoft.com/en-us/documentation/articles/role-based-access-built-in-roles/.

b) The password of the account.
c) Click Sign in.

6. The Region where ZCA is installed is automatically populated in the Azure Authentication window.

7. Select a Subscription. Only subscriptions related to the region where the ZCA is installed are displayed.

8. Once you select a subscription, a Directory related to the subscription is populated.

9. Define a new storage account that will be used for replication and recovery or select one from a list of existing storage accounts in the drop down menu.

10. Selecting an existing storage account is available under the following conditions:
   ■ The site where the Zerto Virtual Replication is installed is of version 5.5.1 and higher.
   ■ The site paired to the site where Zerto Virtual Replication is installed is of version 5.5 and higher.

11. By default, the Create new storage account option is selected.

12. To select an existing storage account, click Use existing. When you select this option, the drop down menu becomes active.

13. Only Standard storage accounts existing in the selected region and subscription are displayed in the storage account drop down menu.

14. If you selected an existing storage account, the account is automatically tagged with a Zerto unique tag.

15. If you selected Create New in the Storage Account field, the installation creates a new resource group and a Standard storage account.

16. When a storage account is either created or selected, the following occurs:
   ■ The journal and recovery disks are created in the storage account.
   ■ The selected storage account appears in Site Settings, in the Site Information tab.

17. Click NEXT.

18. The Connectivity page is displayed.
19. Select the IP address of the machine on which you are installing the Zerto Cloud Appliance. The protected site accesses the Azure site through VPN using this IP.

20. Specify a name to identify this site.

21. Click **NEXT**.

   The *Online Services and Zerto Mobile Application* dialog is displayed.
22. Click NEXT.

23. If you reached the subscription’s maximum limit of storage accounts, a message appears informing the user that creating a new storage account has failed.

24. After the checks complete successfully, click RUN and continue to the end of the installation.

If you intend managing your disaster recovery from this machine, you can select to open the Zerto Virtual Manager (ZVM) Interface at the end of the installation, logging in with the user name and password for the Azure instance on which you installed the Zerto Virtual Manager. In this user interface you set up Zerto Virtual Replication.

25. It is required to exclude the Zerto Virtual Replication folder from antivirus scanning. Failure to do so may lead to the ZVR folder being incorrectly identified as a threat and in some circumstances corrupt the ZVR folder.

Registering the Zerto Virtual Replication 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 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.

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

When you first access the Zerto User Interface, you must register your use of Zerto Virtual Replication 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 Azure, you must first pair the protected site containing the virtual machines that you want to protect with the Azure site on which you installed the Zerto Cloud Appliance. This is described in “Pairing Sites to Enable Replicating From One Site to Another Site”, below.

**Pairing Sites to Enable Replicating From One Site to Another Site**

Zerto Virtual Replication is installed on both the protected and Microsoft Azure 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 Azure 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 Virtual Replication documentation for the relevant hypervisor.

**Protecting Virtual Machines**

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

- **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.

- 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.

Requirements for Replication within Azure
- Azure ZCA on both Azure sites need to be version 6.0 and higher.
- The following limitations apply when protecting within Azure:
  - Self replication is not supported.

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.

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

| Networking       | Network interfaces per region: | 350               |
|                  | NICs per instance: | Depends on instance size: |
|                  | Private IP Addresses per VNET per subscription per region: | 4096               |
|                  | 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 will cause them not to boot. |

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

1. In the Zerto User Interface on the protected site, either VMware vSphere, Microsoft Hyper-V, Amazon Web Service (AWS), or Azure, 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 Virtual Replication 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.

6. 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 Azure.

7. 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 Azure, the display changes to show only fields that are relevant for Azure.

8. 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.
9. Select recovery settings for failover/move and failover testing.

   **VNet** – The virtual network dedicated to your Azure account.

   **Subnet** – The subnet mask for the VNet.

   **Network Security Group** – The Azure security to be associated with the virtual machines in this VPG.

   **Instance Family** – The series from which to select the type. (Azure instance families are optimized for different types of applications. Choose the series appropriate for the application in the VPG.)

   **Instance Size** – The instance size, within the series, to assign to recovered instances. Different sizes within a series vary primarily in vCPU, ECU, RAM, and local storage size. The price per instance is directly related to the instance size.

10. 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.

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

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

12. 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 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 machines are created in Microsoft Azure and configured to the checkpoint specified for the recovery.
  - The new virtual machines 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 in a sandbox and powered on for testing.
- **Stopping the test.**
  - The virtual machines in Azure 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 set the operation to TEST and click **FAILOVER**.
   The Failover Test wizard is displayed.

2. Select the VPGs to test. By default, all VPGs are listed.
   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 **EXECUTION PARAMETERS** step is displayed. 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**.

5. 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.

The test starts for the selected VPGs. The test begins with an initialization period during which the new virtual machines are created in Azure. The protected virtual machines are created as new instances in instances group. These instances are defined as D1 instances. If D1 instances do not meet your needs, you can manually stop the instance, change the instance size, 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 Azure 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 Azure. In the Azure 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 Failover test when a failover test is being performed.
- In the Zerto User Interface, click the VPGs tab, and then click on 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 under RUNNING TASKS.

Stopping a Failover Test

To stop a failover test:
1. Click the Stop test icon 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 under MONITORING > TASKS.
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.

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.