Zerto Virtual Replication Quick Start Azure Environments

Rev01 U2
Dec 2019
ZVR-QSZ-7.5
© 2019 Zerto All rights reserved.

Information in this document is confidential and subject to change without notice and does not represent a commitment on the part of Zerto Ltd. Zerto Ltd. does not assume responsibility for any printing errors that may appear in this document. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, without the prior written permission of Zerto Ltd. All other marks and names mentioned herein may be trademarks of their respective companies.

The scripts are provided by example only and are not supported under any Zerto support program or service. All examples and scripts are provided "as-is" without warranty of any kind. The author and Zerto further disclaim all implied warranties including, without limitation, any implied warranties of merchantability or of fitness for a particular purpose.

In no event shall Zerto, its authors, or anyone else involved in the creation, production, or delivery of the scripts be liable for any damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or other pecuniary loss) arising out of the use of or inability to use the sample scripts or documentation, even if the author or Zerto has been advised of the possibility of such damages. The entire risk arising out of the use or performance of the sample scripts and documentation remains with you.

ZVR-QSZ-7.5
Zerto Quick Start Azure 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 Microsoft Azure (MA). The virtual machines can be protected by Zerto in either VMware vSphere or Microsoft Hyper-V.

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

See the following sections:

- Introduction on page 4
- Recommended Installation Best Practices on page 8
- Installation on page 9
- Registering the Zerto License on page 13
- Pairing Sites to Enable Replicating From One Site to Another Site on page 14
- Setting Up the Protected Site on page 17
- Protecting Virtual Machines on page 18
- Testing Disaster Recovery on page 26
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 the Azure Site

Click to open and review prerequisites and requirements: [Zerto 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

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 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.
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>
<tr>
<td>9989</td>
<td>Communication between ZCM, and ZCM GUI and ZCM REST APIs.</td>
</tr>
<tr>
<td>9080*</td>
<td>Communication between the ZVM, Zerto Powershell Cmdlets, and Zerto Diagnostic tool.</td>
</tr>
<tr>
<td>9081*</td>
<td>Communication between paired ZVMs**</td>
</tr>
<tr>
<td>9180*</td>
<td>Communication between the ZVM and the VBA.</td>
</tr>
<tr>
<td>9669*</td>
<td>Communication between ZVM and ZVM GUI and ZVM REST APIs, and the ZCM.</td>
</tr>
</tbody>
</table>

*The default port provided during the ZVR installation which can be changed during the installation.*

**Access to Azure Cloud Environment**

The followings list contains the endpoints required to set up replication to and from Azure:

- management.azure.com
- 168.63.129.16:32526
- 169.254.169.254
- *.blob.core.windows.net
- *.management.azure-api.net
- login.microsoftonline.com
- secure.*.microsoftonline-p.com
- *.store.core.windows.net
• portal.azure.com
• graph.windows.net
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 from antivirus scanning:

<table>
<thead>
<tr>
<th>Zerto Virtual Replication</th>
</tr>
</thead>
<tbody>
<tr>
<td>%ProgramData%\Zerto\Data\zvm_db.mdf</td>
</tr>
<tr>
<td>C:\Program Files\Zerto\Zerto Virtual Replication\Zerto.Zvm.Service.exe</td>
</tr>
<tr>
<td>C:\Program Files\Zerto\Zerto Virtual Replication\Zerto.Vba.VbaService.exe</td>
</tr>
<tr>
<td>C:\Program Files\Zerto\Zerto Virtual Replication\Zerto Online Services Connector\Zerto.Online.Services.Connector.exe</td>
</tr>
<tr>
<td>C:\Program Files\Zerto\Zerto Virtual Replication\Embedded DB Manager Service\Zerto.LocalDbInstanceManagerService.exe</td>
</tr>
</tbody>
</table>

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.

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

Before you Begin:

• Make sure you deployed Zerto Cloud Appliance.
• Make sure you reviewed Database Requirements in Microsoft Azure Environments.
• Make sure Managed Identities on the VM running the ZCA is enabled and the permission level is set to Contributor, or greater, at the Subscription level. See Enabling Managed Identities and Setting Mandatory Permissions in Azure on page 1.

To perform an express install of Zerto:

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


   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 Verification of Azure Roles and Permissions window is displayed.
4. Click **VERIFY PERMISSIONS**.
   - On success, proceed to Step 8. The Subscription field will be automatically populated. on page 10
   - On failure, verify that the VM running the ZCA has Managed Identities enabled and has been set to the role of **Contributor**, or greater, at the Subscription level.

5. The Subscription field will be automatically populated.

6. Select the desired **Region**. If you do not select a region, the default is the VM’s Region.

7. 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.

   By default, the Create new storage account option is selected.
**Important:**

Each ZCA requires a separate storage account. Multiple ZCAs using the same account is not supported.

a. By using the default option **Create new** in the **Storage Account** field, the installation creates a **new** resource group and a **Standard** storage account.

b. Click **Use existing** to select an existing storage account. When you select this option, the drop down menu becomes active.

  • Only **Standard storage accounts** which exist in the **selected region and subscription** are displayed in the storage account drop down menu.

  • General-purpose v1 (GPv1) accounts are supported.

  • Blob Storage accounts are not displayed for selection since the Blob Storage account type is not supported.

  • When you select an **existing** storage account, the account is automatically **tagged** with a **Zerto unique tag**.

**Note:**

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.

8. Click **NEXT**.

9. The Connectivity page is displayed.

10. 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.

11. Specify a name to identify this site.
12. Click **NEXT**.

The Online Services and Zerto Mobile Application dialog is displayed.

13. Click **NEXT**.

14. 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**.

15. 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.

16. 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:

1. **To use the Zerto Virtual Manager Web Client:**
   - 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 is installed.
   - 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 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 on page 14.
Pairing Sites to Enable Replicating From One Site to Another Site

See the following sections:

- Pair to Another Site on page 14
- Unpairing Sites on page 15

Pair to Another Site

You can pair to any site where Zerto is installed.

Zerto can be installed at multiple sites and each of these sites can be paired to any other site on which Zerto has been installed. Virtual machines that are protected on one site can be recovered to any paired site.

➢ To pair to a site:

1. From the remote site to which you will pair, in Zerto Virtual Manager > Sites tab, click the button Generate Pairing Token.

2. The Generate Pairing Token window opens.

3. Click Copy, to copy the token.

   The token expires when the earliest of one of the following conditions is met:
   - 48 hours after clicking Copy
   - At the next ZVM process termination
   - After the token is used to authenticate the pairing request

4. From the site which will initiate the pairing, in the Zerto Virtual Manager > Sites tab, click PAIR.

   The Add Site window is displayed.
5. Specify the following:

- **Host name/IP**: 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 the installation. The default port during the installation was 9081.
- **Token**: Paste the token which you copied above.

6. Click **PAIR**.

The sites are paired, meaning that the Zerto Virtual Manager for the local site is connected to the Zerto Virtual Manager at the remote site.

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

### Unpairing Sites

You can unpair any two sites that are paired to each other.

**Important**: If there is a VPG on either of the sites you are unpairing, the VPGs will be deleted.

### To unpair two sites:

1. In the Zerto User Interface, in the SITES tab, select the site which you want to unpair.

2. Click **UNPAIR**.

   A message appears warning the user that the sites are about to unpair.

   If there are either protected or recovered VPGs on the paired sites, a message appears warning the user that the VPGs will be deleted.
3. For vSphere, Hyper-V and Azure platforms, you can select to keep disks to use for preseeding if the VMs are re-protected. If you select this option, the disks are not removed from the recovery site.

4. To unpair, click **CONTINUE**.

   The sites are no longer paired. If there are VPGs on either site, they are deleted.

   The VRA on the recovery site that handles the replication for the VPG is updated including keeping or removing the replicated data for the deleted VPG, depending if you selected to keep disks to use for preseeding.

   The locations of the saved target disks are specified in the **Events** tab in the ZVM application on the **Recovery** site.
Setting Up the Protected Site

Refer to the Zerto 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. 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, see [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.
- The ZCA VM must have Managed Identities enabled and permissions must be set to Contributor, or greater, at the Subscription level. For further details, see [https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview](https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview).
- Only General-purpose v1 (GPv1) accounts are supported.
- It is recommended to use a separate storage account for each ZCA.
- For **Linux** distribution, refer to Azure documentation:
- **Ultra SSD** storage is not supported.

**Requirements for Replication From Azure**

Zerto supports replication of VMs with the following types of Managed disks:

- Managed Premium SSD
- Managed Standard SSD
- Managed Standard HDD

**Requirements for Replication To Azure**

Zerto uses the cloud native Azure Scale Set service to reduce RTO when failing over to Azure. When ZCA is installed in Azure, and the ZVM is up and running, an Azure scale set with one virtual machine is created.
in your Azure environment. The new virtual machine, created by the Scale Set, is prefixed with the site ID. When failing over to Azure, multiple VMs in the Scale Set are deployed for the recovery process and created in the ZCA VNet. When recovery is completed, these VMs are terminated.

The following requirements apply when protecting 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.

  \[\textbf{Note:} \quad \text{For some instance sizes, the Azure virtual machine is created with a Local SSD disk which is a temporary disk. This disk is in addition to the disks associated with each protected virtual machine.}\]

- The protected virtual machines needs to have at least one NIC.
- The Azure scale out instances require access to a set of URLs. Zerto reduced the set of URLs required to the following:
  - azure.archive.ubuntu.com
  - security.ubuntu.com
- ZCA primary NIC subnet requires minimum 50 IP addresses for the Azure Scale Set VMs.
- Increase CPU quota, per Ds1_v2 SKU family, to at least 50 for the Azure Scale Set service.
- Increase CPU quota, per region, to at least 100 for the Azure Scale Set service and for recovering VMs to Azure.
- When failing over, up to 40 VMs are created of type Ds1_v2; with Ubuntu server 18.04 LTS.

The following limitations apply when protecting to Azure:

- Virtual machines with UEFI Firmware cannot be protected.
- Reserve at least 2 CPUs and 4GB RAM for the machine using a subnet accessible by other Zerto 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

Protecting Virtual Machines
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**, where the maximum amount is 250.

Default Azure Limitations which Affect Recovery

<table>
<thead>
<tr>
<th>Virtual Machines Limitations</th>
<th># of VMs per region per subscription:</th>
<th>Default is 20. Increase this default to at least 50.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td># of VMs per series, cores per region:</td>
<td>Increase default to at least 50 for Ds1_v2 series.</td>
</tr>
<tr>
<td></td>
<td>Resource groups per subscription:</td>
<td>800</td>
</tr>
<tr>
<td>Networking</td>
<td>Network interfaces per region:</td>
<td>350</td>
</tr>
<tr>
<td></td>
<td>NICs per instance:</td>
<td>Depends on instance size:</td>
</tr>
<tr>
<td></td>
<td>Private IP Addresses per VNET per subscription per region:</td>
<td>4096</td>
</tr>
<tr>
<td></td>
<td>Cloning of IP addresses during recovery operations:</td>
<td>Due to an Azure limitation, failing over Linux VMs with static IP is not supported.</td>
</tr>
</tbody>
</table>
Storage

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

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 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.

6. Click **NEXT**
   The REPLICATION step 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.
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.

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.

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:
    \textit{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 \textit{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.

\textbf{Note:} You can initiate the failover test from either the protected site or recovery site.

\begin{itemize}
\item To test failover:
\item 1. In the Zerto User Interface set the operation to \textbf{TEST} and click \textbf{FAILOVER}.
   
   The Failover Test wizard is displayed.
\end{itemize}
2. Click NEXT. 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.

   ![Select VMs to Failover dialog]

   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 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**.

![Image of Zerto User Interface](image)

**Stopping a Failover Test**

➤ **To stop a failover test:**

1. Click the **Stop test** icon to stop the test in the specific VPG tab.

![Image of Zerto User Interface showing Stop Test dialog](image)

You can also stop the test via the **TASKS** popup dialog in the status bar or under **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**.

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 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.

© 2019 Zerto Ltd. All rights reserved.