Zerto Virtual Replication Quick Start Hyper-V Environments

Rev01 U2
July 2019
ZVR-QSH-7.0
© 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-QSH-7.0
Zerto Quick Start Hyper-V 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 in a SCVMM Hyper-V environment to protect virtual machines.

Table of Contents

Introduction on page 3
Recommended Installation Best Practices on page 7
Installation on page 8
Registering the Zerto License on page 10
Installing Virtual Replication Appliances on page 11
Pairing Sites to Enable Replicating From One Site to Another Site on page 15
Setting Up the Second Site on page 15
Enabling Replication to the Same Site on page 16
Protecting Virtual Machines on page 17
Testing Disaster Recovery on page 22

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.

Zerto also supports both the protected and recovery sites being managed by a single SCVMM, to handle small branch offices. When the protected and recovery sites are the same site, only one installation of Zerto Virtual Replication is required.

**Requirements for Each Site**

Click to open and review [prerequisites](#) and [requirements](#): Microsoft Hyper-V environments

** Routable Networks**

The Zerto architecture supports the following network configurations:

- In on-premise environments:
  
  - Flat LAN networks
  
  - VLAN networks, including private VLANs and stretched VLANs
- WAN emulation
- VPN IPsec

- In Cloud environments:
  - The instance (virtual machine) 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.

The Zerto architecture 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.
Zerto can be installed at multiple sites and each of these sites can be paired to any of the other sites. Zerto supports both the protected and recovery sites being managed by a single vCenter Server or System Center Virtual Machine Manager. For example, in the following scenario:

- From a branch office, to the main office, both managed by the same System Center Virtual Machine Manager.
- From one host to a second host, both managed by the same System Center Virtual Machine Manager.
- To the same host but using different storage for recovery.

It is recommended to install Zerto in the main office site where protected machines will be recovered. The following table provides basic information about the ports shown in the above diagram by Zerto.

<table>
<thead>
<tr>
<th>Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td><em>(vSphere only)</em> Required between an ESXi host and the ZVM during installation of a VRA.</td>
</tr>
<tr>
<td>443</td>
<td><em>(vSphere only)</em> Required between the ZVM and the vCenter Server.</td>
</tr>
<tr>
<td>443</td>
<td><em>(vSphere only)</em> Required between an ESXi host and the ZVM during installation of a VRA.</td>
</tr>
<tr>
<td>445</td>
<td>Required between LTR service and a network shared repository on top of SMB protocol.</td>
</tr>
<tr>
<td>2049</td>
<td>Required between LTR service and a network shared repository on top of NFS protocol.</td>
</tr>
<tr>
<td>8100</td>
<td><em>(Hyper-V only)</em> Communication between the ZVM and the SCVMM (System Center Virtual Machine Manager).</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>5672</td>
<td><em>(vSphere only)</em> TCP communication between the ZVM and vCloud Director for access to AMQP messaging.</td>
</tr>
</tbody>
</table>

Note: UDP ports in the 444xx range for DHCP are not required, and can therefore be blocked.
<table>
<thead>
<tr>
<th>Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<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>
<tr>
<td></td>
<td>(Hyper-V only) Communication between every Hyper-V host and the Zerto Virtual Manager.</td>
</tr>
</tbody>
</table>

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

**Note:**
- When a single vCenter Server or SCVMM is used for both protection and recovery, only one ZVM is installed and port 9081 is not used.
- Recovery to a different vCenter Server or SCVMM uses port 9081 between the ZVMs in each site.

If a proxy server is used at the site, specify the IP address of the Zerto Virtual Manager in the exception list in the Proxy Server settings.

### Recommended Installation Best Practices

Zerto recommends the following best practices:

- Install Zerto on a dedicated virtual machine with a dedicated administrator account and with Microsoft failover clustering enabled, and no other applications installed on this machine, and especially not on the machine running SCVMM. If additional applications are installed, the Zerto Virtual Manager service must receive enough resources and HA remain enabled with the VM Restart Policy set to High.

- Install a VRA on every host in a cluster so that if protected virtual machines are moved from one host to another, there is always a VRA to protect the moved virtual machines.

- Install VRAs using static IP addresses and not DHCP.

- Prepare an administrator account for the machine where Zerto is installed.

- 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.

- Synchronize the clocks on the machines where Zerto is installed using NTP.

**Installation**

The Zerto installation deploys the Zerto Virtual Manager (ZVM) and copies the installation software for the Virtual Replication Appliance (VRA).

A complete installation includes installing Zerto on the protected and peer, recovery, sites.

**Note:** When both these sites are managed by a single SCVMM, Zerto is installed on only one site. In this case, Zerto recommends installing Zerto in the main office site where protected machines will be recovered.

You can install Zerto using the defaults provided by Zerto or perform a custom install, in which you can 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, for example, if the Zerto for VMware vCenter Server version has been installed on the machine.

➢ **To perform an express install of Zerto:**

---

**Installation**
1. Run the Zerto installation.

   **Note:** If the required version of Microsoft .NET Framework is not installed, you are prompted to install the required version of .NET Framework, which is included as part of the Zerto installation package. After .NET is installed the machine automatically restarts and the Zerto installation begins.

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

3. Click **NEXT**.

   The SCVMM Server and Site Connectivity Type dialog is displayed.

4. Specify the following:

   **IP/Host Name:** The IP address or host name of the machine where the System Center Virtual Machine Manager runs.

   **Domain:** The domain for a user with administrator level privileges to the System Center Virtual Machine Manager.

   **Username:** The user name for a user with administrator level privileges to the System Center Virtual Machine Manager.

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

   **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.

   **Note:** 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 SCVMM connected to the Zerto Virtual Manager.

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.

8. Add the machine to the relevant host boot configuration, so that on starting up the host, this machine, running the Zerto Virtual Manager, is also powered on automatically.

9. Repeat the procedure to install Zerto on peer sites.

### Registering the Zerto License

Access the Zerto User Interface from a browser as follows:

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.

On the very first access to the Zerto User Interface, you must either register your use of Zerto, by entering the license key supplied by Zerto or pair to a site where a license has already been entered.
After entering a valid license, the DASHBOARD tab is displayed with a summary of the site. Before you can start protecting virtual machines in this site, you must configure Zerto Virtual Manager at each site by installing Virtual Replication Appliances on the hosts in the site and pair the protected and recovery sites, as described in the following sections.

**Note:** Complete the configuration of one site at a time.

### Installing Virtual Replication Appliances

The Zerto (VRA) installation includes the installation package for VRAs. A VRA is a Zerto virtual machine that manages the replication of virtual machines across sites. A VRA must be installed on every Hyper-V which hosts virtual machines that require protecting in the protected site and on every Hyper-V that will host the replicated virtual machines in the recovery site. The VRA compresses the data that is passed across the WAN from the protected site to the recovery site. The VRA automatically adjusts the compression level according to CPU usage, including totally disabling it if needed.

A VRA can manage a maximum of 1500 volumes, whether these volumes are being protected or recovered.

The VRA is a custom, very thin, Linux-based virtual machine with a small footprint, disk – memory and CPU – and increased security since there are a minimum number of services installed.

Zerto recommends installing a VRA on every hypervisor host so that if protected virtual machines are moved from one host in the cluster to another host in the cluster there is always a VRA to protect the moved virtual machines.

#### VRA Installation Requirements

To **install** a VRA you require the following on the **host**:

- **15GB** storage space
- At least **1GB** of reserved memory.
- *(vSphere only)* The ESX/ESXi version must be in accordance with supported ESX/ESXi versions in the [Interoperability Matrix](#), and Ports 22 and 443 must be enabled on the host during the installation.
- *(Hyper-V only)* Minimum PowerShell version: **4.0**
- *(Hyper-V only)* Port **8100** must be enabled on **SCVMM**.
• *(Hyper-V only)* The following PowerShell cmdlet has been run:

```
Install-WindowsFeature -Name Hyper-V -IncludeManagementTools -Restart
```

**Before You Begin:**

You must know the following information to install a VRA:

• *(vSphere only)* If the ESXi version is 5.5 or higher and the VRA should connect to the host with user credentials, or if the ESXi version is lower than 5.5 (5.x), the password to access the host root account.

  **Note:** For ESXi versions 5.5 or higher, by default the VRA connects to the host with a vSphere Installation Bundle, VIB. Therefore, it is not necessary to enter the password used to access the host root account.

• The storage the VRA will use, and the local network used by the host.

• The network settings to access the peer site; either the default gateway or the IP address, subnet mask, and gateway.

  **Note:** When the gateway is not required, you can specify 0.0.0.0 as the gateway, for example when performing self replication.

• If a static IP is used, instead of DHCP, which is the Zerto recommendation, you need to know the IP address, subnet mask, and default gateway to be used by the VRA.

  **Note:** In a non-production environment it is often convenient to use DHCP to allocate an IP to the VRA. In a production environment this is not recommended. For example, if the DHCP server changes the IP allocation on a reboot, the VRA does not handle the change.

• If the peer site VRAs are not on the default gateway, you must set up routing to enable the VRAs on this site to communicate with the peer site VRAs before defining the VRAs.

  • Setting up routing after defining VRAs only applies to VRAs installed after the routing is set.
  • Any existing VRA is not affected and access to these VRAs continues via the default gateway.
  • If the default gateway stops being used, you must reinstall the VRAs that were installed before setting up paired site routing.
• *(vSphere only)* For the duration of the installation of the VRA, the Zerto Virtual Manager enables SSH in the vCenter Server.

• *(vSphere only)* You must know the following information to install a VRA:
  - The **password** to access the **host root account**, for ESXi 5.x and higher.
  - The **datastore** the VRA will use and the **local network** used by the host.
  - The **network settings** to access the **peer** site; either the default gateway or the IP address, subnet mask, and gateway.
  - If a **static IP** is used, instead of DHCP, which is the Zerto recommendation, you need to know the IP address, subnet mask, and default gateway to be used by the VRA.

  **Note:** In a non-production environment it is often convenient to use DHCP to allocate an IP to the VRA. In a production environment this is not recommended. For example, if the DHCP server changes the IP allocation on a reboot, the VRA does not handle the change.

You must also know the following information to install a VRA:

• The storage the VRA will use and the local network used by the host.

• The network settings to access the peer site; either the default gateway or the IP address, subnet mask and gateway.

  **Note:** When the gateway is not required, you can specify 0.0.0.0 as the gateway, for example when performing self replication.

• If a static IP is used, which is the Zerto recommendation\(^1\), instead of DHCP, the IP address, subnet mask and default gateway to be used by the VRA.

If the peer site VRAs are not on the same network as the peer site Zerto Virtual Manager, you must set up routing to enable the Zerto Virtual Manager to communicate with the peer site VRAs, as described in the Zerto Virtual Manager Administration Guide for the Microsoft Hyper-V Environment.

**To install a Zerto Virtual Replication Appliance (VRA) on a host:**

1. In the Zerto User Interface, click **SETUP > VRAs**.
2. Select a host that needs a VRA and click **NEW VRA**.
   
   The Configure and Install VRA dialog is displayed.

\(^1\) In a non-production environment it is often convenient to use DHCP to allocate an IP to the VRA. In a production environment this is not recommended. For example, if the DHCP server changes the IP allocation on a reboot, the VRA does not handle the change.
3. Specify the following in the Host Details section:

**Host:** The host under which the VRA is installed. The drop-down displays the hosts which do not have a VRA installed, with the selected host displayed by default.

**Storage:** The storage that contains the OS disks of the VRA VM. You can install more than one VRA on the same storage.

**Network:** The network used to access the VRA.

4. Leave the Host Root Password, VRA RAM and VRA Group values with their defaults.

5. Specify the following in the VRA Network Details section:

**Configuration:** Specify DHCP.

**Note:** In a production environment the Static option is the recommended option.

6. Click INSTALL.

The VRA installation starts and the status is displayed in the TASKS popup dialog in the status bar and under **MONITORING > TASKS.**

The VRA displayed name and DNS name is **Z-VRA-hostname.** If a virtual machine with this name exists, for example when a previous VRA was not deleted, the VRA name has a number appended to it.

Add a VRA to every Hyper-V host that hosts virtual machines for which you want replication. Zerto recommends installing a VRA on every listed Hyper-V host. An alert is issued after the first VRA is installed.
in a cluster because Zerto recommends installing a VRA on every host in the cluster. The alert is automatically removed when all the hosts in the cluster have VRAs installed.

**Note:** VRAs are configured and managed by the Zerto Virtual Manager. You cannot take snapshots of VRAs as snapshots cause operational problems for the VRAs.

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

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

If a single SCVMM is used, for example with remote branch offices, when replicating from one datacenter to another datacenter, both managed by the same SCVMM, you must enable replication to the same SCVMM and pairing is not required. For details, see Enabling Replication to the Same Site on page 16.

#### To pair sites:

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

   The Add Site dialog is displayed.

   ![Add Site Dialog](image)

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 for the local SCVMM site is connected to the Zerto Virtual Manager on the remote SCVMM site.

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

### Setting Up the Second Site

After pairing the sites you can access the second site without entering a license and then install VRAs in the site.
Install VRAs on hosts in the second site by repeating the procedure, Installing Virtual Replication Appliances on page 11.

Enabling Replication to the Same Site

When a single SCVMM is used, for example with remote branch offices, when replicating from one datacenter to another datacenter, both managed by the same SCVMM, you must enable replication to the same SCVMM and pairing is not required. In this case, replication to the same SCVMM must be set in the Site Settings dialog.

To enable replication to the same SCVMM:

1. In the Zerto User Interface, click SETTINGS ( ) in the top right of the header and select Site Settings.

   The Site Settings dialog is displayed.

2. Click Policies.

3. Select the Enable Replication to Self checkbox.

4. Click APPLY or SAVE.

   The Zerto Virtual Manager, when used to protect to itself, can manage the protection of up to 5000 virtual machines.
Protecting Virtual Machines

You can protect virtual machines to a recovery site SCVMM. The procedure is the same whether you intend to protect one virtual machine or multiple virtual machines. Virtual machines are protected in virtual protection groups. A virtual protection group (VPG) is a group of virtual machines that you group together for recovery purposes.

To create a virtual protection group (VPG):

1. In the Zerto User Interface, select ACTIONS>CREATE VPG.

   The GENERAL 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 arrow pointing right to include these VMs in the VPG.

   • 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.

![Select VMs dialog](image)

**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 five (5) virtual machines may boot on a host simultaneously. Following the boot, a 300 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**.

Click **NEXT**.

The **REPLICATION** step is displayed.

7. Specify the values to use when replicating to this site.

**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 SLA and Advanced settings, as shown below.

**Recovery Site:** The site to which you want to recover the virtual machines. After specifying the recovery site, the host and storage on the site to use for replication can be specified. If you
specified that replication is possible to the same site, as described in Enabling Replication to the Same Site on page 16, then you can specify the local site here.

- **Host:** The default cluster or host, in the recovery site that handles the replicated data.
- **Storage:** The default storage volume to use for the recovered virtual machine files and for their data volumes. Every storage for the recovery host is included in the drop-down list. If a cluster is selected for the host, only storage accessible by every host in the cluster are displayed.

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 STORAGE step is displayed. By default the storage used for the virtual machine definition is also used for the virtual machine data. For each virtual machine in the VPG, Zerto displays its storage-related information.

```
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. For your first VPG, leave the default values. These settings can be changed later by editing the VPG definition. Click NEXT.

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

10. Select the recovery settings.

- **Failover/Move Network:** The network to use during a failover or move operation in which the recovered virtual machines will run.
• **Failover Test Network**: The network to use when testing the failover of virtual machines in the recovery site. Zerto recommends using a fenced-out network so as not to impact the production network at this site.

11. You can run scripts as part of the recovery process, and these scripts are defined in the VPG. Script settings can be added later by editing the VPG definition. For your first VPG, leave the default values and click **NEXT**.

The NICs step is displayed. In this step, you can specify the NIC details to use for the recovered virtual machines after a failover, a test failover, or migration.

**NICs step in on-premise environments:**

12. Again, leave the defaults and 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.

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

The **SUMMARY** step is displayed. It shows the VPG configuration that you defined in previous tabs.
14. 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.

In order 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, as opposed to creating virtual machines in a production network, to a specified point-in-time, using the virtual disks managed by the VRA. All testing is written to scratch volumes. The longer the test period the more scratch volumes are used, until the maximum size is reached, at which point no more testing can be done. The maximum size of all the scratch volumes is determined by the journal size hard limit and cannot be changed. The scratch volumes reside on the storage defined for the journal.

The Failover Test operation has the following basic steps:

1. Starting the test.
   a. The test virtual machines are created at the remote site using the network specified for testing in the VPG settings and configured to the checkpoint specified for the recovery.
   b. The 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.

2. Testing. The virtual machines in the VPG are created as test machines in a sandbox and powered on for testing using the test network specified in the VPG definition and using the virtual disks managed by the VRA. All testing is written to scratch volumes. The longer the test period the more scratch volumes are used, until the maximum size is reached, at which point no more testing can be done. The maximum size of all the scratch volumes is determined by the journal size hard limit and cannot be changed. The scratch volumes reside on the storage defined for the journal. Using scratch volumes makes cleaning up the test failover more efficient.

   **Note:** You must not delete, clone, migrate to another host or change the disk properties of any of the test virtual machines.

3. Stopping the test.
   a. The test virtual machines are powered off and removed from the inventory.
   b. The following tag is added to the checkpoint specified for the test:
      
      Tested at startDateAndTimeOfTest

      The tagged 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. For example, in a cluster, if the HA configuration in a cluster includes admission control to prevent virtual machines being started if they violate availability constraints, testing the failover of every VPG configured for recovery to this cluster, at the same time, will show whether the constraints are violated or not.

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.
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.

After Starting a Test, What Happens?

During the initiation phase, the virtual machines in the virtual protection group are created at the recovery site with the suffix testing recovery.

All testing is written to scratch volumes. The longer the test period the more scratch volumes are used, until the maximum size is reached, at which point no more testing can be done. The maximum size of all the scratch volumes is determined by the journal size hard limit and cannot be changed. The scratch volumes reside on the storage defined for the journal. Using these test scratch volumes makes cleaning up the test failover more efficient.

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 take a snapshot of a test machine, since the virtual machine volumes are still managed by the VRA and not by the virtual machine. Using a snapshot of a test machine will create a corrupted virtual machine.
- 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**.

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.
NEW Zerto 7.0 enhances the Zerto IT Resilience Platform by converging disaster recovery and backup to deliver continuous availability within a simple, scalable platform. Zerto 7.0 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.