Zerto Virtual Replication Installation Guide
Microsoft Hyper-V Environment
Version 5.5
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 v

CHAPTER 1: INSTALLING ZERTO VIRTUAL REPLICATION

Zerto Virtual Replication is installed in every site with virtual machines to be protected and recovered. The installation includes the following:

- **Zerto Virtual Manager (ZVM):** A Windows service that manages the replication at the site level. The ZVM monitors the System Center Virtual Machine Manager (SCVMM) to get the inventory of VMs, disks, networks, hosts, etc. For example, a Microsoft Live Migration of a protected VM from one host to another is monitored by the ZVM and the protection and recovery is updated accordingly.
  
  Each Zerto Virtual Manager can manage up to 5000 virtual machines, either being protected or recovered to that site.

- **Virtual Replication Appliance (VRA):** A virtual machine installed on each Hyper-V hosting virtual machines to be protected or recovered, to manage the replication of data from protected virtual machines to the recovery site.
  
  A VRA can manage a maximum of 1500 volumes, whether these are volumes being protected or recovered.

- **Virtual Backup Appliance (VBA):** A Windows service that manages back-ups within Zerto Virtual Replication.
  
  The VBA service runs on the same machine as the Zerto Virtual Manager service and manages 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 in a browser.

The following topics are described in this section:

- “Zerto Virtual Replication DR Architecture”, below
- “Zerto Virtual Replication Interoperability Matrix”, on page 6
- “Prerequisites and Requirements - Hyper-V with Zerto Virtual Replication”, on page 6
- “Database Requirements in Hyper-V Environments”, on page 7
- “SCVVM Privileges”, on page 7
- “Installing Zerto Virtual Replication in Microsoft Hyper-V Environments”, on page 7
- “Performing a Silent Installation”, on page 17
- “Installing Zerto Virtual Replication Cmdlets”, on page 18
- “Installing the VSS Agent”, on page 19
Zerto Virtual Replication DR Architecture

The following diagram shows how the main Zerto Virtual Replication components are deployed across sites to provide disaster recovery across these sites.

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

Zerto Virtual Replication can be installed at multiple sites and each of these sites can be paired to any of the other sites. Zerto Virtual Replication supports both the protected and recovery sites being managed by a single 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 Virtual Replication 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 Virtual Replication.

<table>
<thead>
<tr>
<th>PORT</th>
<th>PURPOSE</th>
</tr>
</thead>
<tbody>
<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>8100</td>
<td>Communication between the ZVM and the SCVMM (System Center Virtual Machine Manager).</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>
</tbody>
</table>

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

| 9180* | Communication between the ZVM and the VBA. |
| 9669* | Communication between ZVM and ZVM GUI and ZVM REST APIs, and the ZCM. |

Communication between every Hyper-V host and the Zerto Virtual Manager.

*The default port provided during the ZVR installation which can be changed during the installation.
**When the same System Center Virtual Machine Manager is used for both the protected and recovery sites, Zerto Virtual Replication is installed on one site only and this port can be ignored.

---

### Zerto Virtual Replication Interoperability Matrix

For details about what is supported, refer to the [Zerto Virtual Replication Interoperability Matrix](#).

### Prerequisites and Requirements - Hyper-V with Zerto Virtual Replication

For Hyper-V requirements with Zerto Virtual Replication, see [Zerto Virtual Replication Requirements for Microsoft Hyper-V Environments](#).
Database Requirements in Hyper-V Environments

During the Zerto Virtual Manager installation, the user is able to select whether to install and use an **embedded** SQL Server (localdb) as the database.

Alternatively, and also during the installation, the user is able to choose whether to instead select and use an **external** SQL Server instance. To use an externally managed database, during the installation select the **Custom Installation** option.

The larger the environment protected by Zerto Virtual Manager, the larger the database size required to support it.

**Supported Microsoft SQL Server versions:** **2008, and higher.**

Before installing Zerto Virtual Manager, click to thoroughly review the following guides:

- Migrating the Zerto Virtual Replication Database to Microsoft SQL Server.
- Sizing Considerations for Zerto Virtual Replication.

You must have the following **permissions** set:

- Public and dbcreator server roles.
- Permission to connect to the database engine.
- Login enabled.
- In **User Mapping** choose the **master** database under which to create the Zerto Virtual Replication database and set both **db_owner** and **public** for database role membership.

**SCVVM Privileges**

Zerto Virtual Replication utilizes the default SCVMM user, **SCVMM admin**. If Zerto administrators need more granular roles and permissions, they must define Role-based Access Control (RBAC) roles and permissions.

To define RBAC roles and permissions, see the section **Defining Role-based Access Control** in the guide **Zerto Cloud Manager Administration Guide for Cloud Environments**.

**Installing Zerto Virtual Replication in Microsoft Hyper-V Environments**

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

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

When both these sites are managed by a single SCVMM, Zerto Virtual Replication is installed on only one site. In this case, Zerto recommends the following:

- Install Zerto Virtual Replication in the site where protected machines will be recovered.
- Make sure that the machine running SCVMM is also in the site used for the recovery and not protection.

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

- **“To perform an express install of Zerto Virtual Replication:”,** below
- **“Performing a Custom Installation”,** on page 10
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, for example, if the Zerto Virtual Replication for VMware vCenter Server or vCloud Director version was installed on the machine.

**Before you Begin:**
- Make sure you reviewed “Database Requirements in Hyper-V Environments” on page 7

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

1. Run the Zerto Virtual Replication Installer for Hyper-V.
   - 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 Virtual Replication installation package. After .NET is installed, the machine automatically restarts and the Zerto Virtual Replication installation begins.
2. Follow the wizard through the installation until the Installation Type window appears, then select the option **Express Installation**.
3. Click **NEXT**.
   - The SCVMM Server Connectivity window appears.

![SCVMM Server Connectivity]

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 window appears.
   - The installation performs checks to make sure that the installation can proceed successfully.
6. After the checks complete successfully, click **RUN** and continue to the end of the installation.

   As part of the installation, the **Zeus driver (jFLR)** is also installed. This installation is **mandatory** for the Zerto Virtual Replication installation.

   a) During the installation, you are prompted with a Windows Security message to install the **Zerto Storage controller**, which will install the Zeus driver (jFLR).

   b) Click **Install**, and continue with the installation.

   If you do not install the additional software when prompted, the **Zerto Virtual Replication installation will fail**.

7. 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. In this user interface you set up Zerto Virtual Replication, as described in “Initial Configuration”, on page 23.

8. You **must 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.

9. 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**.

10. Install Zerto Virtual Replication on peer sites.
Performing a Custom Installation

You can install Zerto Virtual Replication specifying the ports that will be used by Zerto Virtual Replication and full contact details.

Before you Begin:
- Make sure you reviewed “Database Requirements in Hyper-V Environments” on page 7

To perform a custom install of Zerto Virtual Replication:
1. Run the Zerto Virtual Replication Installer for Hyper-V.
   - 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 Virtual Replication installation package. After .NET is installed, the machine automatically restarts and the Zerto Virtual Replication installation begins.
2. Follow the wizard until the Installation Type window appears, then select the option, Custom Installation.
3. Click NEXT. The Windows Service User window appears.
4. Select either Local System account or This account:
   - Local System account: Use the Local System account to run the Zerto Virtual Manager service, which is installed as part of Zerto Virtual Replication. The Local System account has unrestricted access to local resources.
   - This account: Use a specific account as the user account to run the Zerto Virtual Manager service, which is installed as part of Zerto Virtual Replication. The account must have unrestricted access to local resources.
   - Password: The password to use to run the service under the specified account.
   - Confirm Password: Confirmation of the password.
5. Click NEXT.
The Database Type window appears.

- Information required by Zerto Virtual Replication is stored by default in a database embedded in the Zerto Virtual Manager. This information includes details of the site where the Zerto Virtual Manager is installed, details of the Virtual Replication Appliances and the volumes they use, and points-in-time recorded for recovery purposes.
- By default an embedded SQL-based database is installed, but you can use an externally managed database, either Microsoft SQL Server or SQL Server Express.
- Protection and recovery can only be performed when the database is running.
- If you use an external database and it is down for any reason, protection ceases.

6. To use the embedded database, leave the default which is installed with this installation, then continue with Step 9.
7. To use an external database, select the option, Connect to an external Microsoft SQL Server or Microsoft SQL Server Express database.
8. If you selected an external database, the SQL Server Authentication area is enabled. Enter the following authentication details to enable access to the SQL Server database:
   a) Server Name: The domain name and server instance to connect to, with the format: \<server_name>\<instance_name> or \<Server_IP>\<instance_name>
   b) You must specify an authentication method. Select one of the following:
      - Windows Authentication
      - SQL Server Authentication
   c) If you selected Windows Authentication: This option is enabled only if a specific service user account was specified in Windows Service User, in Step 3. In this case, the service account name and password are used.
   d) If you selected SQL Server Authentication, the Test Authentication button is also displayed. After you define the following, click Test Authentication:
      - Username: The user name for the SQL Server database.
      - Password: A valid password for the given user name.
      The installer checks whether it can connect to the specified database with the specified username and password. You can only continue when the authentication is successful.
9. Click NEXT. The SCVMM Server Connectivity window appears.
### SCVMM Server Connectivity

The Zerto Virtual Manager (ZVM) communicates with a SCVMM Server.

Enter connection settings to be used by the Zerto Virtual Manager to communicate with the site SCVMM Server:

<table>
<thead>
<tr>
<th>IP / Host Name</th>
<th>Domain</th>
<th>Username</th>
<th>Password</th>
</tr>
</thead>
</table>

10. Enter connection settings that the **Zerto Virtual Manager** uses to communicate with the **SCVMM Server**:

- **IP/Host name**: The IP address or host name of the machine where the SCVMM 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.
11. Click **NEXT**.

The Zerto Virtual Manager Site Details window appears, where you define general information about the site.

12. Enter the site details:
   - **Site Name**: A name to identify the site. This name is displayed in the Zerto User Interface. **This field is mandatory.**
   - **Location**: Information such as the address, or name of the site to identify it. This field is optional.
   - **Contact Information**: The name of the person to contact if a need arises. This field is optional.
   - **Contact Email**: The email address to contact if a need arises. This field is optional.
   - **Contact Phone**: The phone number to contact if a need arises. This field is optional.

13. Click **NEXT**.
The Online Services and Zerto Mobile Application window appears.

The Online Services and Zerto Mobile Application are enabled by default. You can disable these services by deselecting Enable Online Services and Zerto Mobile Application.

14. Click NEXT.
The Zerto Virtual Manager Communication window appears. In this window you define the connection settings (ports) which are used by Zerto Virtual Manager to communicate with Zerto Virtual Managers on other sites.

### Zerto Virtual Manager Communication

Zerto Virtual Manager (ZVM) communicates with other ZVMs to manage replication between sites.

Enter the connection settings to be used by ZVM to communicate with ZVMs on other sites.

**Warning:** If the protected site recovers to a site maintained by a cloud service provider, do not change the TCP port values.

<table>
<thead>
<tr>
<th>PORT DESCRIPTION (PARAMETER)</th>
<th>DEFAULT PORT NUMBER</th>
<th>COMMUNICATION DIRECTION</th>
<th>BETWEEN...</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Port (ZVM)</td>
<td>9080</td>
<td>Inbound</td>
<td>Zerto Virtual Manager - and - Zerto internal APIs, Cmdlets and a VSS Agent</td>
<td></td>
</tr>
<tr>
<td>HTTPS Port ( clients&lt;-&gt;ZVM)</td>
<td>9669</td>
<td>Inbound</td>
<td>Zerto User Interface - and - Zerto Virtual Manager</td>
<td></td>
</tr>
<tr>
<td>TCP Port (ZVM&lt;-&gt;ZVM)</td>
<td>9081</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP Port (ZVM -&gt; VBA)</td>
<td>1180</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
15. Click **NEXT**.

   The installation performs checks to verify that the installation can proceed successfully.

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

   As part of the installation, the **Zeus driver (jFLR)** is also installed. This installation is **mandatory** for the Zerto Virtual Replication installation.

   a) During the installation, you are prompted with a Windows Security message to install the **Zerto Storage controller**, which will install the Zeus driver (jFLR).

   b) Click **Install**, and continue with the installation.

   If you do not install the additional software when prompted, **the Zerto Virtual Replication installation will fail**.

17. 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. In this user interface you set up Zerto Virtual Replication, as described in “Initial Configuration”, on page 23.

18. You **must 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.

19. 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.

20. Install Zerto Virtual Replication on peer sites.

   ■ The installation creates the Zerto Virtual Manager and Virtual Backup Appliance as services, and the installation package to enable installing Virtual Replication Appliances on hosts.

   ■ Zerto Virtual Replication creates folders, such as C:\ZertoAgent, which **must not be removed**.
Performing a Silent Installation

You can perform a silent installation of Zerto Virtual Replication, by running the installation executable in a script with the -s option.

```
<installation>.exe [-s] [-uninstall] [-l <logfile>] [[PROPERTY=VALUE] ...]
```

Where:
- **uninstall** Runs the uninstall procedure.
- **-l <logfile>** Writes log entries to the specified file.
- **-s** Runs the installation, uninstall, repair or upgrade silently.

If Zerto Virtual Replication does **not exist** on the machine, an installation is performed.

If the **same version** of Zerto Virtual Replication exists on the machine, a repair is performed.

If a **previous version** of Zerto Virtual Replication exists on the machine, an upgrade is performed.

- **PROPERTY=VALUE** Sets the property PROPERTY to VALUE. The PROPERTY can be any of the following:

<table>
<thead>
<tr>
<th>PROPERTY</th>
<th>DESCRIPTION</th>
<th>MANDATORY</th>
</tr>
</thead>
<tbody>
<tr>
<td>ScvmmDomain</td>
<td>The domain name for an administrator.</td>
<td>Yes</td>
</tr>
<tr>
<td>ScvmmHost</td>
<td>The host name of the machine on which Zerto Virtual Replication is installed.</td>
<td>Yes</td>
</tr>
<tr>
<td>ScvmmPassword</td>
<td>A valid password for the given user name.</td>
<td>Yes</td>
</tr>
<tr>
<td>ScvmmUsername</td>
<td>The user name for an administrator.</td>
<td>Yes</td>
</tr>
<tr>
<td>AutoRestart</td>
<td>When running on Windows 2012 platforms, you might need to restart the computer to complete the installation. To automatically restart the computer after the installation, set this value to 1.</td>
<td>No</td>
</tr>
<tr>
<td>DBType</td>
<td><strong>Embedded database</strong> (default)</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>- or -</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>External Microsoft SQL Server</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Value: <strong>DBType=sqlserver</strong></td>
<td></td>
</tr>
<tr>
<td>IsWindowsAuthentication</td>
<td>Use Windows authentication.</td>
<td>No</td>
</tr>
<tr>
<td>ServiceAccount</td>
<td>The user account to run the Zerto Virtual Manager service.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Default value: '\LocalSystem'</td>
<td></td>
</tr>
<tr>
<td>ServicePassword</td>
<td>The password to use to run the service under the specified account.</td>
<td>No</td>
</tr>
<tr>
<td>SiteCertificatePassword</td>
<td>The default is taken from Zerto.</td>
<td>No</td>
</tr>
<tr>
<td>SiteContactEmail</td>
<td>The email address to contact if a need arises.</td>
<td>No</td>
</tr>
<tr>
<td>SiteContactInfo</td>
<td>The name of the person to contact if a need arises.</td>
<td>No</td>
</tr>
<tr>
<td>SiteContactPhone</td>
<td>The phone number to contact if a need arises.</td>
<td>No</td>
</tr>
<tr>
<td>SiteHttpPort</td>
<td>The port used for inbound communication between the Zerto Virtual Manager and Zerto internal APIs, Cmdlets and a VSS Agent.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Default value: <strong>9080</strong></td>
<td></td>
</tr>
<tr>
<td>SiteHttpPort</td>
<td>The port used for inbound communication between the Zerto User Interface and the Zerto Virtual Manager.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Default value: <strong>9669</strong></td>
<td></td>
</tr>
<tr>
<td>SiteAddress</td>
<td>The IP address, or host name of the machine where SCVMM runs.</td>
<td>No</td>
</tr>
<tr>
<td>SiteKeepPreviousIdentifier</td>
<td>Default value: <strong>true</strong></td>
<td>No</td>
</tr>
<tr>
<td>SiteLocation</td>
<td>Information to identify the site location.</td>
<td>No</td>
</tr>
</tbody>
</table>
Installing Zerto Virtual Replication Cmdlets

Windows PowerShell is a command-line shell running under Windows for system administrators. The Windows PowerShell includes both an interactive command line prompt and a scripting environment. Each can be used independently or they can be used together.

Windows PowerShell is built on top of the .NET Framework common language runtime (CLR), enabling it to accept and return .NET Framework objects.

To run the Zerto Virtual Replication cmdlets you must first run the installation package supplied by Zerto.

Note: You must have both Microsoft .NET Framework 4 and Windows PowerShell installed.

To install the Zerto Virtual Replication cmdlets:
1. Make sure that Windows PowerShell is closed.
2. Run the installation file.

After installing the Zerto Virtual Replication cmdlets, either add the cmdlets each time you open the Windows PowerShell or create a Windows PowerShell profile. The following procedure describes how to add the Zerto Virtual Replication cmdlets to every Windows PowerShell session.

To add the Zerto Virtual Replication cmdlets to the current session:
- Open Windows PowerShell with the following arguments:

```powershell
Add-PSSnapIn Zerto.PS.Commands
```

The Add-PSSnapin cmdlet adds registered Windows PowerShell snap-ins to the current session.

To add the Zerto Virtual Replication cmdlets to every session, in the Properties dialog for a PowerShell shortcut specify a Target value similar to the following:

```bash
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -NoExit -Command Add-PSSnapIn Zerto.PS.Commands
```

Note: You can create a Windows PowerShell profile, as described in the Windows PowerShell Help, to add the snap-in to all future Windows PowerShell sessions.

For more details, see Zerto Virtual Replication PowerShell Cmdlets Guide.

---

<table>
<thead>
<tr>
<th>PROPERTY</th>
<th>DESCRIPTION</th>
<th>MANDATORY</th>
</tr>
</thead>
<tbody>
<tr>
<td>SiteName</td>
<td>A name to identify the site. This name is displayed in the Zerto User Interface.</td>
<td>No</td>
</tr>
<tr>
<td>SiteTcpPort</td>
<td>The port used for communication between Zerto Virtual Managers.</td>
<td>No</td>
</tr>
<tr>
<td>SiteTcpPortVba</td>
<td>The port used for communication between the Zerto Virtual Manager and the Virtual Backup Appliance.</td>
<td>No</td>
</tr>
<tr>
<td>SqlPassword</td>
<td>A valid password for the given user name.</td>
<td>No</td>
</tr>
<tr>
<td>SqlServerName</td>
<td>The domain name and server instance to connect to, with the format: domain\instance</td>
<td>No</td>
</tr>
<tr>
<td>SqlUserName</td>
<td>The user name for the SQL Server database.</td>
<td>No</td>
</tr>
</tbody>
</table>

"Zerto Virtual Replication Hyperv Installer.exe" -s ScvmmHost=199.10.10.20 ScvmmDomain=MyDomain ScvmmUsername=Administrator ScvmmPassword=mypassword SiteName=site1_199.10.10.20
Installing the VSS Agent

The Microsoft Volume Shadow Copy Service (VSS) enables taking manual or automatic backup copies or snapshots of data, even if it has a lock, on a specific volume at a specific point-in-time over regular intervals. This ensures not just that the data is crash consistent but also application consistency if recovery is needed.

Zerto Virtual Replication enables adding checkpoints to the journal that are synchronized with VSS snapshots.

To use Zerto Virtual Replication with VSS and to ensure application consistency, you must install the ZertoVssAgent on every virtual machine that uses VSS, and that you want to protect with Zerto Virtual Replication.

You can install the ZertoVssAgent on the following supported Windows operating systems:

<table>
<thead>
<tr>
<th>OPERATING SYSTEMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Server 2008, all versions (SPs and R2)</td>
</tr>
<tr>
<td>Windows Server 2012, all versions (SPs and R2)</td>
</tr>
<tr>
<td>Windows Server 2016</td>
</tr>
</tbody>
</table>

Consider the following:

- Only a single virtual machine in a VPG can have application consistent checkpoints, and the VSS checkpoint is only applied to the virtual machine where the ZertoVssAgent is installed.
- Thus, even if more than one virtual machine runs VSS, you only install the Zerto VssAgent on one of the virtual machines in the VPG.
- Also, the virtual machine where the ZertoVssAgent is installed must have network connectivity to the local Zerto Virtual Manager in order to be able to add VSS checkpoints successfully.

To install the ZertoVssAgent:

1. Download the ZertoVssAgent, ZertoVss64Agent.msi, from the Zerto Support Portal downloads page, to the virtual machines that use VSS, and which you want to protect with Zerto Virtual Replication.
2. Log in as an Administrator to the virtual machine that uses VSS, and which you want to protect.
3. Navigate to and run the ZertoVss64Agent.msi file.
   - Only a single virtual machine in a VPG can have application consistent checkpoints.
   - The VSS checkpoint is only applied to the virtual machine where the ZertoVssAgent is installed.
   - Even if more than one virtual machine runs VSS, you only install the Zerto VSSAgent on one of the virtual machines in the VPG.
   - The virtual machine where the ZertoVssAgent is installed must have network connectivity to the local Zerto Virtual Manager in order to add VSS checkpoints successfully.
4. Enter the license key and click Validate.
5. Run the ZertoVssAgent on the virtual machines that use VSS and that you want to protect.
6. Follow the wizard through the installation.
   The Zerto Virtual Manager Connections Settings dialog is displayed.

7. Specify the IP address and HTTP port number for the Zerto Virtual Managers managing the protection of the virtual machines, both for the local site and optionally, for the paired, remote site.
   ■ If the same hypervisor manager is used both for protecting and recovering virtual machines, specify the IP address and HTTP port number for the single Zerto Virtual Manager installed.
   ■ The default HTTP port number when Zerto Virtual Replication is installed is 9080.
   ■ If you enter a wrong IP address or port you can correct the address or port after the installation completes by editing the ZertoVssAgentGUI.exe.conf file in the ZertoVssAgent folder under the folder where the ZertoVssAgent is installed, for example, C:\Program Files\Zerto.

8. Click OK.
   The ZertoVssAgent is installed and the Add VSS Checkpoint icon is placed on the desktop. The agent runs as a Windows service, ZertoVssprovider.

For more details about the ZertoVssAgent, see the Zerto Virtual Manager Administration Guide.
CHAPTER 2: ACCESSING THE ZERTO USER INTERFACE

You manage the protection and replication of virtual machines in Microsoft System Center Virtual Machine Manager (SCVMM), between the protected and recovery sites, using the Zerto User Interface. On first access to the user interface, you might have to add a security certificate to set up secure communication, as described in “Adding a Security Certificate for the Zerto User Interface”, on page 21. Zerto also provides a set of RESTful APIs and PowerShell cmdlets to enable incorporating some of the disaster recovery functionality within scripts or programs.

Note: 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.

Note: 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.

The following topics are described in this chapter:

■ “Using the Zerto User Interface From a Browser”, below
■ “Adding a Security Certificate for the Zerto User Interface”, on page 21

Using the Zerto User Interface From a Browser

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. Login using the user name and password for the machine where you installed Zerto Virtual Replication.
   Username: The user name for the user for the machine where the Zerto Virtual Manager is installed. If the user is part of a domain, you must also specify the domain, with the following format:
   domain\username
   Password: A valid password for the given user name.

Adding a Security Certificate for the Zerto User Interface

Communication between the Zerto Virtual Manager and the user interface uses HTTPS.

On the first login to the Zerto User Interface, you must install a security certificate in order to be able to continue working without each login requiring acceptance of the security.

On first access to the Zerto User Interface, if you haven’t installed the security certificate, a security alert is issued.

Note the following:

■ To run this procedure run Microsoft Internet Explorer as administrator. The procedure is similar for Google Chrome and for Mozilla Firefox.
■ Access the Zerto User Interface using the IP and not the name of the machine where Zerto Virtual Replication is installed.

To install a security certificate for the Zerto User Interface:

2. Click Install Certificate. The Certificate Import wizard window appears.
3. Follow the wizard, taking note to place all the certificates in the Trusted Root Certification Authorities store. To do this, in the relevant window, select the option Place all certificates in the following store and browse to select the store Trusted Root Certification Authorities.
4. Continue to the end of the wizard.
5. When the Security Warning appears, click Yes.

6. Click OK to confirm that the installation was successful.
7. Click OK when prompted, and then Yes in the Security Alert window to continue.
CHAPTER 3: INITIAL CONFIGURATION

After installing Zerto Virtual Replication, you must configure the site.
Zerto Virtual Replication is configured and managed from within the Zerto User Interface.
This section describes the initial configuration required after installing Zerto Virtual Replication.

The following topics are described in this section:
- “Registering the Zerto Virtual Replication License”, below
- “Installing Virtual Replication Appliances”, on page 24
- “Pairing Sites”, on page 27
- “Setting Up a Remote Site”, on page 28

Registering the Zerto Virtual Replication License

On the very first access to the Zerto User Interface, you must do one of the following:
- Either register your use of Zerto Virtual Replication, by entering the license key supplied by Zerto,
- Or, pair to a site where a license has already been entered.

A customer using a Cloud Service Provider (CSP) to manage the disaster recovery, pairs to the CSP using the IP address supplied by the CSP and does not enter a license key.

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 install Virtual Replication Appliances on the hosts in the site and then pair the protected and recovery sites, as described in the following sections:
- “Installing Virtual Replication Appliances”, on page 24
- “Pairing Sites”, on page 27
Installing Virtual Replication Appliances

The Zerto Virtual Replication installation includes the installation package for Virtual Replication Appliances (VRAs).

A VRA is a Zerto Virtual Replication 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.

See also:
- “VRA Installation Requirements”, on page 24
- “Setting Up Routing”, on page 25
- “Installing a Zerto Virtual Replication Appliance (VRA) on a Host”, on page 25

VRA Installation Requirements

To install a VRA you require the following on the Hyper-V host:

- 15GB storage space
- At least 1GB of reserved memory.
- Port 8100 must be enabled on SCVMM.
- Minimum PowerShell version: 4.0
- The following PowerShell cmdlet has been run:
  ```powershell
  Install-WindowsFeature -Name Hyper-V -IncludeManagementTools -Restart
  ```

You must 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.
- 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.

Before You Begin:

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, instead of DHCP, 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

Use the following procedure to set up routing to enable the VRAs on the site to communicate with the peer site VRAs before defining the VRAs.

To set up routing:
1. In the SETUP > VRAs tab, select MORE > Paired Site Routing. The Configure Paired Site Routing window appears.

2. Click Enable Paired Site Routing.
3. Specify the following and then click SAVE:
   - Address: The IP address of the next hop at the local site, the router or gateway address, that is used to access the peer site network.
   - Subnet Mask: The subnet mask for the peer site network.
   - Gateway: The gateway for the peer site network.

   These access details are used to access all VRAs installed on the peer site after the information is saved.

Installing a Zerto Virtual Replication Appliance (VRA) on a Host

Use the following procedure to install a Zerto Virtual Replication Appliance on a host.

To install a Zerto Virtual Replication Appliance (VRA) on a host:
1. In the Zerto User Interface, click SETUP > VRAs.
2. Select a host which requires a VRA and click NEW VRA.
The **Configure and Install VRA** window appears.

![Configure and Install VRA Window](image)

**Note:** If you selected a **cluster** or **multiple hosts**, the VRA is installed on the **first host in the displayed list**.

3. In the **Host Details** area, specify the following:
   - **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.
   - **Host Root Password**: For future use.
   - **Storage**: The storage that the VRA will use for mirror virtual machines and for its journal. You can install more than one VRA on the same storage.
   - **Network**: The network used to access the VRA.
   - **VRA RAM**: The amount of memory to allocate to the VRA.
     - The amount determines the **maximum buffer size for the VRA**, for buffering IOs written by the protected virtual machines, **before the writes are sent** over the network to the recovery VRA.
     - The recovery VRA also buffers the incoming IOs until they are written to the journal.
     - If a buffer becomes full, a **Bitmap Sync** is performed after space is freed up in the buffer.

<table>
<thead>
<tr>
<th>AMOUNT OF VRA RAM</th>
<th>VRA BUFFER POOL SIZE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1GB</td>
<td>450MB</td>
</tr>
<tr>
<td>2GB</td>
<td>1450MB</td>
</tr>
<tr>
<td>3GB</td>
<td>2300MB</td>
</tr>
<tr>
<td>4GB</td>
<td>3,300MB</td>
</tr>
<tr>
<td>5GB</td>
<td>4,300MB</td>
</tr>
<tr>
<td>6GB</td>
<td>5,300MB</td>
</tr>
<tr>
<td>7GB</td>
<td>6,300MB</td>
</tr>
<tr>
<td>8GB</td>
<td>7,300MB</td>
</tr>
<tr>
<td>9GB</td>
<td>8,300MB</td>
</tr>
<tr>
<td>10GB</td>
<td>9,300MB</td>
</tr>
<tr>
<td>11GB</td>
<td>10,300MB</td>
</tr>
<tr>
<td>12GB</td>
<td>11,300MB</td>
</tr>
</tbody>
</table>
The protecting VRA can use 90% of the buffer for IOs to send over the network and the recovery VRA can use 75% of the buffer.

For Example: A protecting VRA defined with **2GB of RAM** can buffer approximately **1305MB** before the buffer is full and a Bitmap Sync is required.

The number of virtual machines that a VRA can support is not dependent on the amount of VRA RAM.

- **VRA Group:** Select the **VRA Group** from the dropdown list.
  - To create a new VRA group, type in the name of the new group and click **CREATE**. You can then choose the new group from the dropdown list.
  
  You group VRAs together when VRAs use different networks so they can be grouped by network, for example when the protected and recovery sites are managed by the same SCVMM and you want to replicate from the branch site to the main site. Within a group the priority assigned to a VPG dictates the bandwidth used and is applicable within a group and not between groups. Thus, a VPG with a high priority is allocated bandwidth before VPGs with lower priorities. VPGs that are on VRAs with different VRA groups, for example, VPG1 on VRA1 in group1 and VPG2 on VRA2 in group2, do not affect each other, as the priority is relevant only within each group.

4. In the **VRA Network Details** area, specify the following:
   - **Configuration:** Either have the IP address allocated via a **static IP address** or a **DHCP server**.
     - If you select the **Static** recommended option, enter the following:
       - **Address:** The IP address for the VRA.
       - **Subnet Mask:** The subnet mask for the network. The default value is **255.255.255.0**.
       - **Default Gateway:** The default gateway for the network.

5. 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.

6. Repeat this procedure to **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.
   - A VRA can manage a maximum of **1500 volumes**, whether these are volumes being protected or recovered.
   - VRAs are configured and managed by the Zerto Virtual Manager. You **cannot take snapshots** of VRAs as snapshots cause operational problems for the VRAs.
   - The following folder is created as part of the VRA installation and **must not be removed**:
     - C:\zerto-temp-<storage_name> - VRA installation files
     - Where <storage_name> signifies the target host. When a VRA is installed using the local storage (c:\), there is only one folder with this name. When a VRA is installed on remote storage, a second folder with the same name is also created where the VRA is installed.

**Pairing Sites**

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

To pair sites:
1. In the Zerto User Interface, in the SITES tab click PAIR.
   The Add Site window appears.

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, 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 a Remote Site

When you are recovering to a **remote site**, and not the same site, you set up a remote site by pairing to the site as described in “Pairing Sites”, on page 27 and then installing VRAs in the site.

To install VRAs on Hyper-V hosts in the remote site:
1. Repeat the procedure, “Installing Virtual Replication Appliances”, on page 24, via the Zerto User Interface for the remote site.
2. If you install a VRA on a remote site before pairing the site, you have to enter the license to use Zerto Virtual Replication, as described in “Registering the Zerto Virtual Replication License”, on page 23.
   **Note**: You can install VRAs on all the sites from within the Zerto Cloud Manager user interface.
You uninstall Zerto Virtual Replication via the *Uninstall a program* in the Windows Control Panel.

When you uninstall Zerto Virtual Replication the following are also removed:

- The Virtual Replication Appliances.
- All the virtual protection groups defined to protect virtual machines, including all the target disks managed by the VRA for the virtual machines that were being protected.
- The Zerto Virtual Backup Appliance.
- Any Zerto Cloud Connectors.

If, for any reason, a Virtual Replication Appliance cannot be removed, for example, in a Microsoft Hyper-V environment, when the SCVMM is down, you can continue with the uninstall and later remove the Virtual Replication Appliance manually from within SCVMM. If this does not work, contact Zerto support.

**Note:** You can uninstall Zerto Virtual Replication silently, by running the silent installation with the `-uninstall` switch, as described in "Performing a Silent Installation", on page 17.
Zerto Virtual Replication releases regular updates. Microsoft also release new versions of their products which can impact Zerto Virtual Replication. This section describes different options for different upgrade scenarios.

The following topics are described in this section:
- “Guidelines to Upgrading Zerto Virtual Replication”, on page 30
- “Upgrading Multiple Sites Running Different Versions”, on page 33
- “Upgrading To More Than One Version Higher”, on page 33
- “Upgrading VRAs”, on page 36
- “Upgrading Zerto Virtual Replication PowerShell Cmdlets”, on page 36
- “Upgrading Zerto Cloud Connectors”, on page 38

You can upgrade Zerto Virtual Replication silently, by running the silent installation, as described in “Performing a Silent Installation”, on page 17.

### Guidelines to Upgrading Zerto Virtual Replication

**Before upgrading**, review the following documents:
- Product Version Lifecycle Matrix for Zerto Virtual Replication
- Sizing Considerations for Zerto Virtual Replication

Then, review the following considerations:
- Zerto recommends upgrading to the latest version of Zerto Virtual Replication that supports the environment you are using. See the Zerto Virtual Replication Interoperability Matrix for the list of environments supported by this version of Zerto Virtual Replication.
- The order you upgrade the sites, protected or recovery, is not relevant as long as paired sites remain only one version apart, that is, only one version higher or lower.

*Note:* Upgrade releases are considered to be upgrades of the same version. Releases 5.5, 5.5U1, etc., are the same version.

- The following table shows what version you can upgrade to, based on the current version running at the site.

<table>
<thead>
<tr>
<th>CURRENT VERSION:</th>
<th>CAN UPGRADE TO:</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0, 4.0Ux</td>
<td>4.5Ux</td>
</tr>
<tr>
<td>4.5, 4.5Ux</td>
<td>5.0Ux</td>
</tr>
<tr>
<td>5.0, 5.0Ux</td>
<td>5.5</td>
</tr>
</tbody>
</table>

- You do not need to move workloads during an upgrade.
- When upgrading a protected vSphere or Hyper-V environment, after the upgrade, a bitmap sync is performed for VPGs on the protected VRA.
- In a Hyper-V environment, SCVMM 2016 is supported on ZVR clean installations only.
- Zerto Cloud Appliance is supported for Azure and AWS (ZCA) on:
  - Windows 2016
  - Windows 2012R2
- A Zerto Virtual Manager can be used with a different version on another site, as long as the other version is only one version higher or lower.
- You can upgrade from version N to the next version (N+1) of Zerto Virtual Replication including to any update within the current version. You cannot do an N+2 upgrade directly.
The following table shows what versions can be used on a peer site, based on the version on the current site.

<table>
<thead>
<tr>
<th>VERSION (N-1)</th>
<th>CURRENT VERSION (N)</th>
<th>VERSION (N+1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.5, 3.5Ux</td>
<td>4.0, 4.0Ux</td>
<td>4.5, 4.5Ux</td>
</tr>
<tr>
<td>4.0, 4.0Ux</td>
<td>4.5, 4.5Ux</td>
<td>5.0, 5.0Ux</td>
</tr>
<tr>
<td>4.5, 4.5Ux</td>
<td>5.0, 5.0Ux</td>
<td>5.5, 5.5Ux</td>
</tr>
</tbody>
</table>

- When upgrading Zerto Virtual Replication, the VRAs that were installed in the previous version are not upgraded automatically.
- If a newer version of the installed VRAs exists, you can continue to use the current VRAs with the new version of Zerto Virtual Replication, or upgrade these VRAs from within the Zerto User Interface, as described in “Upgrading VRAs”, on page 36.

See the following sections:
- “Before Upgrading Zerto Virtual Replication”, on page 31
- “Upgrading the Current Installation”, on page 31

**Before Upgrading Zerto Virtual Replication**

Before upgrading to a new version, either by installing the new version over the existing version or by uninstalling the existing version and then installing the new version, Zerto recommends doing the following:

- Clear the Microsoft Internet Explorer cache of temporary Internet files. Not clearing the cache of temporary files can result in problems when accessing the Zerto Virtual Manager.
- Make sure that all VPGs are in the state Protecting, and not in a sync state, such as Delta Sync, or in an error state, such as Needs Configuration.
- Complete any recovery operation before starting the upgrade.
- Stop the Zerto Virtual Manager service.
- Create a backup of the machine where the Zerto Virtual Manager runs, which you will use if the upgrade fails. Zerto recommends taking a snapshot of the machine after stopping the Zerto Virtual Manager service.

**Note:** The snapshot should only be used to rollback to the pre-upgrade state immediately after the upgrade has completed. The snapshot should not be used after the protection of virtual machines has restarted.

The installation procedure checks for an existing installation that is either one version lower than the new version or is the same version. If an installation is found you can upgrade the installation.

**Upgrading the Current Installation**

The existing Virtual Replication Appliances and protected virtual machines, together with all other information, such as checkpoints, journals, sites, and pairing details, are retained and are available in the upgraded installation.

The upgrade is performed without disrupting the protection, but no new checkpoints are written to the journal during the actual upgrade.

This temporarily causes alerts to be issued, even if only a single site was affected, stating that the journal history and RPO do not meet their specified target settings.

**To upgrade the version:**

1. Run the Zerto Virtual Replication installation executable for your environment.
   The Zerto Replication Installation Wizard is displayed.
2. Click NEXT to continue.
   Zerto Virtual Replication validates that your system meets the upgrade requirements.
3. Select the checkbox to accept the license agreement, and click **NEXT** to continue.

   The VRAs Upgrade window is displayed.

   ![VRAs Upgrade Window]

   The Auto-Upgrade Virtual Replication Appliances checkbox is selected by default, meaning that all the VRAs will be automatically upgraded once the upgrade completes successfully.

   - Optionally, deselect the checkbox if you want to manually upgrade VRAs after the version upgrade completes.

   **Note:** *(For Hyper-V environments only)* After the upgrade, a **delta sync** is performed at the protected site, and a **bitmap sync** is performed at the recovered site.

4. Click **Next**.

   - The version upgrade proceeds automatically, displaying a Validation box followed by an Upgrade progress box.
   - The Upgrade Complete window is displayed, with the checkbox **Open the Zerto Virtual Manager interface** already selected.
   - It is highly recommended that you track the VRA upgrade via the Zerto Virtual Manager interface. You may, however, deselect the checkbox if you do not want to track the VRA upgrade progress.

5. Click **DONE** to close the wizard.

   The Zerto Virtual Manager interface opens at the **Setup > VRAs** tab, displaying the Upgrading VRA tasks.

   **Note:** If during the upgrade, system requirements are identified that require a restart, a window is displayed informing the user that the upgrade is complete and whether to restart the computer.
Upgrading Multiple Sites Running Different Versions

A Zerto Virtual Manager can be installed on a site running a different version, as long as each version is only one version higher or lower than the other.

When you have multiple sites, make sure that the version of Zerto Virtual Manager is never more than one version higher or lower than any of the versions running on the paired sites.

To upgrade Zerto Virtual Replication installed on multiple sites:
1. Upgrade a site whose version is lower than the required version. Start the upgrades with the site whose version is lowest. Make sure, at all times, that no site is more or less than one version higher or lower than any of the paired sites.
2. If the VRAs on the site need upgrading, upgrade these VRAs to ensure that they are no less than one version higher or lower than any of the VRAs on any of the paired sites.
3. Repeat the above step for all sites.

For Example:
- You have sites running versions 4.0U3, which are paired to a site running 4.5U4.
- You are planning to upgrade to 5.0U2.
- Upgrade first the 4.0U3 site to a 4.5U4 version, and then both of the sites to 5.0U2.

Upgrading To More Than One Version Higher

Before upgrading to a new version, make sure that all VPGs are in Protecting state and not in a sync state, such as Delta Sync, or an error state, such as Needs Configuration.

If you need to upgrade more than one version higher, do one of the following:
1. Upgrade versions stepwise, one version at a time, as described above in Upgrading Multiple Sites Running Different Versions, until you reach the required version.
   - or -
2. Use the Zerto Diagnostics utility’s export option to export the existing VPG definitions, then uninstall the old version of Zerto Virtual Replication. Install the new version, then use the Zerto Diagnostics utility’s import option to re-create the VPGs. Use the following procedure.

Upgrading Zerto Virtual Replication Using the Zerto Diagnostics Utility

To upgrade Zerto Virtual Replication using the Zerto Diagnostics utility:
1. Click Start > Programs > Zerto Virtual Replication > Zerto Diagnostics. The Zerto Virtual Replication Diagnostics menu dialog is displayed.
2. Select the **Export Virtual Protection Group (VPG)** settings option and click **Next**.

   **Note:** Zerto Virtual Replication regularly exports settings to the folder `<Zerto_Installation_Folder>\Zerto Virtual Replication\ExportedSettings`. You can use the last exported file. The default location of Zerto_Installation_Folder is `C:\Program Files\Zerto`.

3. Select the destination for the file that will contain the exported settings and enter the Zerto Virtual Manager IP address and port for the protected site.

4. Click **Next**.
   
   The list of exported VPGs is displayed.

5. Click **Done**.

6. In the Zerto User Interface delete the VPGs, and keep their target disks.

   **Note:** If you did not export the settings, Zerto Virtual Replication regularly exports settings to the folder `<Zerto_Installation_Folder>\Zerto Virtual Replication\ExportedSettings`. You can use the last exported file as input to recreate the VPGs to this point in time. The default location of Zerto_Installation_Folder is `C:\Program Files\Zerto`.

7. Uninstall the existing Zerto Virtual Replication version.

8. Install the new Zerto Virtual Replication version, as described in the **Zerto Virtual Replication Installation Guide**.

9. Install the VRAs on the hosts in the site and pair the sites, as described in **Zerto Virtual Replication Installation Guide**.
Note: If the protected site and recovery site are the same for any of the VPGs that were exported, set Enable replication to Self in the Advanced Settings dialog, as described in Zerto Virtual Manager Administration Guide for the VMware vSphere Environment.

10. Click Start > Programs > Zerto Virtual Replication > Zerto Diagnostics.
   The Zerto Virtual Replication Diagnostics menu dialog is displayed.
11. Select Import Virtual Protection Group (VPG) settings.
12. Click Next.

   ![Zerto Diagnostics Collection](image)

13. Select the file previously exported and enter the Zerto Virtual Manager IP address and port for the protected site.
14. Click Next.
   The list of exported VPGs is displayed.

   ![Zerto Diagnostics Collection](image)

15. Select the VPGs to import. You cannot import VPGs that have the same name as a VPG that is already defined in current installation. If a VPG in the import file has the same name as an existing VPG, it is disabled and is grayed-out.
16. Click Next.
   The list of imported VPGs is displayed. If the VPG cannot not be imported, the reason is specified.
17. Click Done.
Upgrading VRAs

This section is applicable if Auto-Upgrade Virtual Replication Appliances was not selected when upgrading Zerto Virtual Replication, or if a manual VRA upgrade is required.

- If a newer version of the installed VRAs exists, you can continue to use the current VRAs with the new version of Zerto Virtual Replication, or you can upgrade these VRAs from within the Zerto User Interface.
- VRAs installed with the previous version of Zerto Virtual Replication can work with VRAs installed with the current version of Zerto Virtual Replication in any combination (all from one version or a mix of VRA versions) as long as the VRAs are only one version lower than the version of Zerto Virtual Replication installed on the site.
- Zerto recommends that you always upgrade the VRAs on your site to the latest version.
- Not all new installations of Zerto Virtual Replication require upgrading VRAs. If your VRA is outdated relative to your current version of Zerto Virtual Replication and an upgrade is available, the VRA version will be reported in the column as outdated. In addition, an alert is issued on the site using the old VRA and on any site that is paired with it.
  
  Note: You can move the mouse over the Outdated value to display the VRA version as a tooltip.

Site Specific Considerations when Upgrading VRAs

- (For Hyper-V Environments) VRAs managing protected virtual machines: Either live migrate the protected virtual machines and storage managed by the VRA to another host with a VRA, or upgrade the VRA without migrating the virtual machines and a delta sync will be performed following the upgrade.
- Upgrading a VRA that manages the recovery of virtual machines results in a bitmap sync being performed after the upgrade. Note that the time to upgrade a VRA is short so the bitmap sync should also be quick.

Procedure: Upgrading VRAs

Use the following procedure to upgrade your VRAs.

To upgrade VRAs:

1. For Hyper-V Environments: For a VRA protecting virtual machines, if live migrating the protected virtual machines:
   a) Remove affinity rules for protected virtual machines on the host with the VRA to be upgraded.
   b) Live migrate these protected machines from the host to another host with a VRA.
2. In the Zerto User Interface, click SETUP > VRAs, select the VRAs to upgrade, and then click MORE > Upgrade.
   The Upgrade VRAs dialog is displayed, listing the selected VRAs, and whether an upgrade is available.
3. Review the list for the VRAs that you want to upgrade. Deselect any VRAs that you decide not to upgrade.
4. Click Upgrade Selected VRAs.
5. The upgrade progress is displayed in the VRAs tab.
   - (For Hyper-V Environments) After the upgrade, a delta sync is performed at the protected site, and a bitmap sync is performed at the recovered site.
   
   Note: The VRA name does not change, even if the naming convention in the latest version is different.

Upgrading Zerto Virtual Replication PowerShell Cmdlets

When upgrading Zerto Virtual Replication PowerShell cmdlets, make sure that Windows PowerShell is closed before installing the new version.

Upgrading or Reinstalling Microsoft SCVMM/Hyper-V Components
Upgrading or Reinstalling Microsoft SCVMM/Hyper-V Components

Refer to Microsoft documentation for complete information regarding installation and upgrading of Microsoft products prior to installation or upgrade.

Verify that your version of Zerto Virtual Replication supports the new Microsoft version before beginning the installation or upgrade.

Refer to the Zerto Virtual Replication Interoperability Matrix for the list of Hyper-V environments supported by this version of Zerto Virtual Replication.

See the following sections:

- Reinstalling VMM
- Upgrading or Reinstalling a Host
- Upgrading Integration Services
- Restarting Zerto Virtual Manager After SCVMM Upgrade

Reinstalling VMM

If you need to reinstall the VMM, including rebuilding the database, contact Zerto support for help throughout the reinstallation.

Upgrading or Reinstalling a Host

When upgrading, including applying patches, or reinstalling a host with an active VRA:

1. First, change the recovery host of every virtual machine in every VPG that recovers to this host, to avoid a Delta Sync after the host has been upgraded and the VRA started up.
2. Then upgrade the host. You can move the virtual machines to a different host from within the Zerto User Interface, as described below, or by using cmdlets, as described in Zerto Virtual Replication PowerShell Cmdlets Guide.

To change a recovery VRA:

1. In the Zerto User Interface, click SETUP > VRAs.
2. Select the VRA to change and click MORE > Change VM Recovery VRA.

   The Change VM Recovery VRA dialog is displayed, listing all the virtual machines being recovered on that host.

   3. Review the list and select the virtual machines to change the target host to another specified target host.
   4. From the Select the replacement host drop-down list, select the target host for these virtual machines.

      You can move some virtual machines to one replacement target host, and then by repeating the operation, you can move other virtual machines to a different target host.

      - Validation is performed to make sure the selected target host can be used. For example, the datastores used by both the VRAs are accessible from both hosts.
      - Any implications of the change, such as whether synchronization might be required after the change is also displayed.
   5. Click SAVE.
Upgrading Zerto Virtual Replication

- The VPG recovery host definitions are changed and the affected target data, including the journals, are vMotioned to the VRA under the replacement host.
- During this procedure you cannot edit the affected VPGs nor attempt a failover, move, failover test, or clone operation.
- At the end of the procedure a Delta Sync might be required to resynchronize the protected machines with the recovery VRAs.
  - In order not to affect the recover ability of other VPGs replicating to the VRA, a new virtual machine is created to handle moving the disks.
  - This virtual machine is named Z-VRAH-ESXihostname-xx, where hostname is the name of the ESXi host where the original VRA is installed and xx is a unique index used for the virtual machine, with a format of yy-xxxx or xxxx.

6. Repeat this procedure for all the virtual machines.

Upgrading Integration Services

You do not need to upgrade Integration Services on a VRA.

Restarting Zerto Virtual Manager After SCVMM Upgrade

Zerto Virtual Manager must be restarted after SCVMM is upgraded.

Upgrading Zerto Cloud Connectors

Zerto Cloud Connectors do not require upgrading when a new Zerto Virtual Replication version is released.