Zerto

Zerto Virtual Replication Installation Guide

VMware vSphere Environment

ZVR-INV-4.0U6-01-14-01-16

ZVR-INV-4.0U6-01-14-01-16

Zerto

TABLE OF CONTENTS

CHAPTER 1: INSTALLING ZERTO VIRTUAL REPLICATION

Zerto Virtual Replication provides a business continuity (BC) and disaster recovery (DR) solution in a virtual environment, enabling the replication of mission-critical applications and data as quickly as possible, with minimal data loss. When devising a recovery plan, these two objectives, minimum time to recover and maximum data to recover, are assigned target values: the recovery time objective (RTO) and the recovery point objective (RPO). Zerto Virtual Replication enables a virtual-aware recovery with low values for both the RTO and RPO. In addition, Zerto Virtual Replication enables protecting virtual machines for extended, longer term recovery from an offsite backup.

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 vCenter Server to get the inventory of VMs, disks, networks, hosts, etc. For example, a VMware vMotion operation 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.

OVF to enable installing Virtual Replication Appliances (VRAs) – A virtual machine installed on each ESX/ESXi 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.

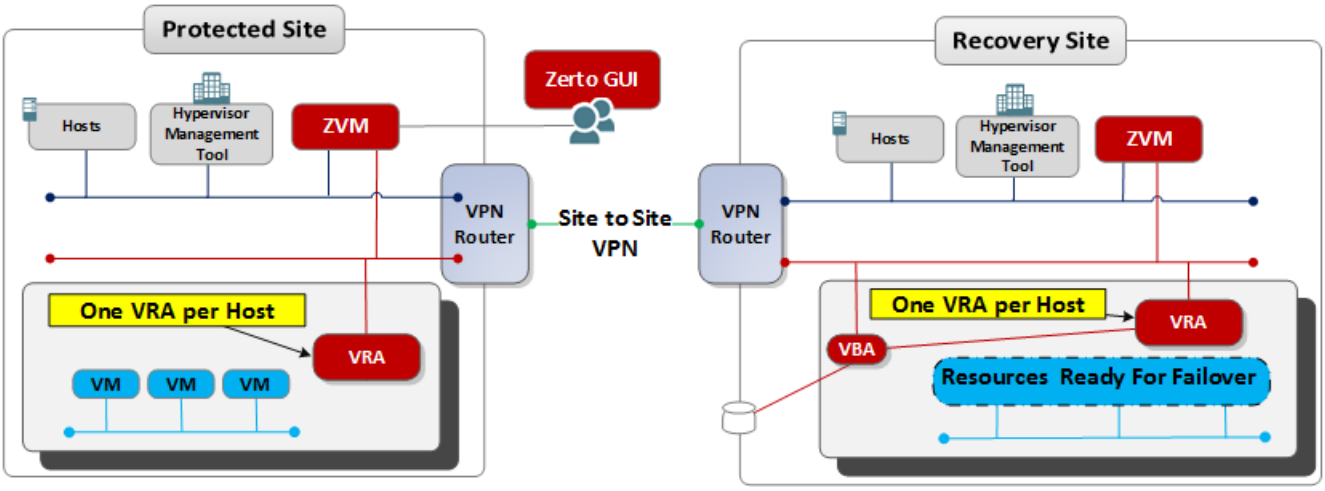
Virtual Backup Appliance (VBA) – A Windows service that manages back-ups within Zerto Virtual Replication. The VBA service runs on the same machine as the Zerto Virtual Manager service and manages the repositories where offsite backups are stored. These repositories can be local or on a shared network.

Zerto User Interface – Recovery using Zerto Virtual Replication is managed in a browser or in the VMware Web Client or Client console.

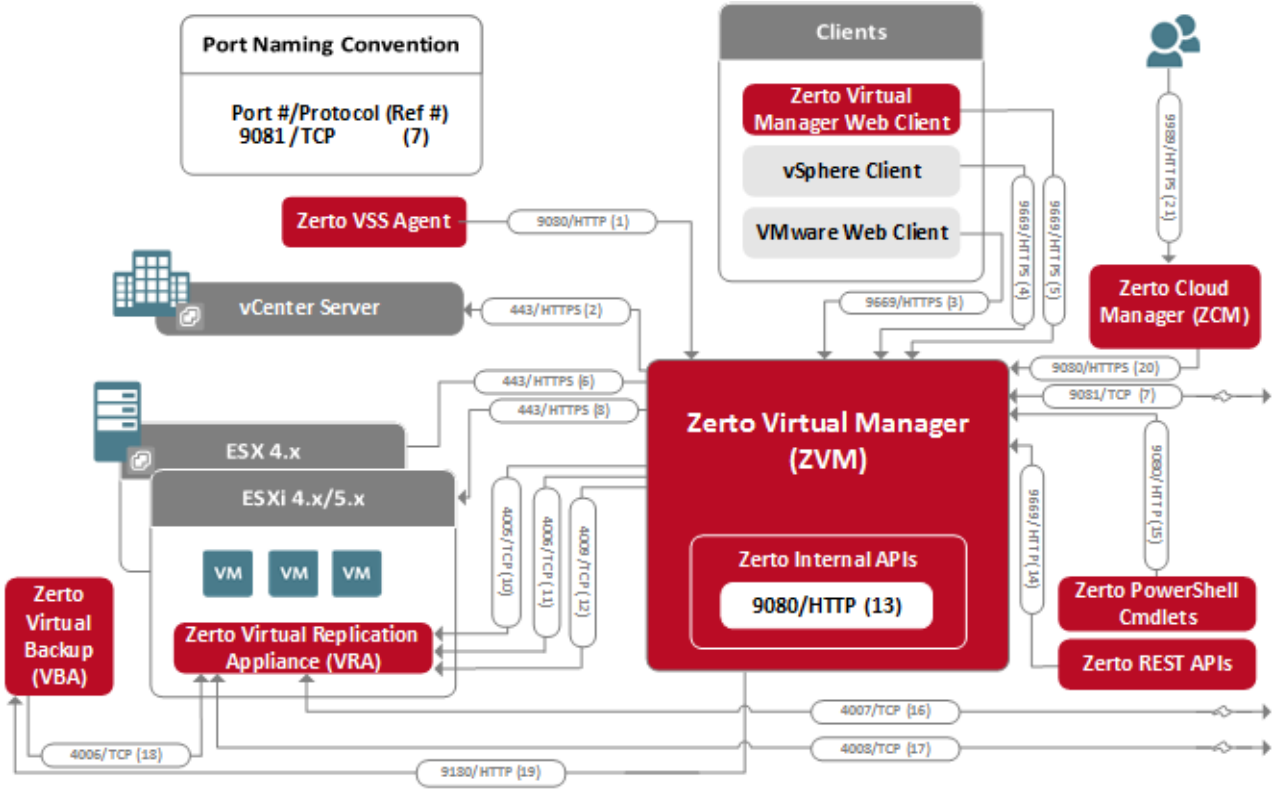
The following topics are described in this chapter:

Zerto Virtual Replication Architecture

The following diagram shows how the main components of Zerto Virtual Replication are deployed across sites to provide disaster recovery across these sites.[1]



The following diagram shows Zerto Virtual Replication components deployed on one site and the ports and communication protocols used between the components.



Zerto Virtual Replication can be installed at multiple sites and each of these sites can be paired to another site enabling protection across sites. Zerto Virtual Replication also supports protection and recovery on a site being managed by a single vCenter Server. The following scenarios are examples of protection and recovery with a single vCenter Server.

- From one datacenter, a branch office, to another datacenter, the main office, both managed by the same vCenter Server. Zerto recommends installing Zerto Virtual Replication in the main office site where protected machines will be recovered.

1. For cloud-based architecture diagrams, see *Zerto Cloud Manager Installation Guide*.

- From one host to a second host, both managed by the same vCenter Server.
- To the same host but using a different datastore for recovery.

When a single vCenter Server is used, port 9081 shown in the above diagram is not used.

The following table provides basic information, shown in the above diagram, about the ports used by Zerto Virtual Replication. For a more detailed description, refer to "Firewall Considerations", on page 8.

REF. #	PORT	PURPOSE
1, 13, 15, 20	9080[1]	Communication between the Zerto Virtual Manager and Zerto internal APIs, Zerto cmdlets, Zerto VSS Agents and the Zerto Cloud Manager.
2	443	Required between the Zerto Virtual Manager and the vCenter Server.
3, 4, 5, 14	9669[1]	Communication between a machine running the Zerto User Interface, vSphere Web Client or Client console and the Zerto Virtual Manager for the relevant vCenter Server and between the Zerto Virtual Manager and Zerto REST APIs.
6	443	Required between an ESXi 4.x host and the Zerto Virtual Manager during installation of a Virtual Replication Appliance (VRA).
7	9081[1]	Communication between paired Zerto Virtual Managers[2].
8	443	Required between an ESXi 5.x host and the Zerto Virtual Manager during installation of a VRA.
9	22	Required between an ESXi host and the Zerto Virtual Manager during installation of a VRA.
10	4005	Log collection between the Zerto Virtual Manager and site VRAs.
11, 18	4006	Communication between the Zerto Virtual Manager and site VRAs and the site Virtual Backup Appliance.
12	4009	Communication between the Zerto Virtual Manager and site VRAs to handle checkpoints.
16	4007	Control communication between protecting and recovering VRAs.
17	4008	Communication between VRAs to pass data from protected virtual machines to a VRA on a recovery site.
19	9180[1]	Communication between the Virtual Backup Appliance and VRA.
21	9989	HTTPS communication between the browser and the Zerto Cloud Manager.

1. The default port provided during the Zerto Virtual Replication installation which can be changed during the installation.
2. When the same vCenter Server is used for both the protected and recovery sites, Zerto Virtual Replication is installed on one site only and this port can be ignored.

Note: For details of the architecture and ports used in a cloud-based architecture environment, see *Zerto Cloud Manager Installation Guide*.

Zerto Virtual Replication Interoperability Matrix

For details about what is supported, refer to the Zerto Virtual Replication Interoperability Matrix.

Requirements

Zerto Virtual Manager is installed on each site managed by a vCenter Server. The installation must be on a machine running a Windows operating system with the following requirements:

- Windows Server 2003 SP2 or higher, or Windows Server 2008, 2008R2, 2012, or 2012R2.

  Reserve at least 2 CPUs and 4GB RAM for the machine. The following CPU and RAM are recommended by Zerto for the machine running Zerto Virtual Replication, dependent on the size of the site:

  Sites protecting up to 750 virtual machines and up to 5 peer sites: 2 CPUs and 4GB RAM.

  Sites protecting 751-2000 virtual machines and up to 15 peer sites: 4 CPUs or 2 Dual Core CPUs and 4GB RAM.

  Sites protecting over 2000 virtual machines and over 15 peer sites: 8 CPUs or 4 Dual Core CPUs and 8GB RAM.

The clocks on the machines where Zerto Virtual Replication is installed must be synchronized with UTC and with each other (the timezones can be different). Zerto recommends synchronizing the clocks using NTP.

Note: Installing Zerto Virtual Replication on a 32-bit Windows operating system limits the memory to 2GB. This limits the number of virtual machines that can be protected.

- At least 4GB of free disk space.
- Microsoft .NET Framework 4 or higher. The 4.0 installation executable is included as part of the Zerto Virtual Replication installation kit and it needs an additional 1.8GB of free disk space. Note that recent Windows operating systems include .NET as part of the operating system. Make sure that you have the latest .NET and Windows updates, unless Zerto support warns against a specific update.

You must have VMware vCenter Server version 4.0U1 or higher with at least one ESX/ESXi host installed on each site where Zerto Virtual Manager is to be used. The Zerto Virtual Manager must have access to the vCenter Server via a user with administrator level privileges to the vCenter Server. When recovery is managed by the same vCenter Server as the protection, Zerto Virtual Manager is required to be installed once only. When the protected and recovery sites are managed by different vCenter Servers Zerto Virtual Manager is installed once per vCenter Server. If Zerto Cloud Manager is used, vSphere Standard edition cannot be used. For details about Zerto Cloud Manager, see *Zerto Cloud Manager Administration Guide*.

Note: When the vCenter Server is installed on a Linux machine via the vCenter Server Linux Virtual Appliance (vCSA), the Zerto Virtual Manager must still be installed on a Windows machine.

Zerto recommends installing the Zerto Virtual Manager with the following profile:

- On a dedicated virtual machine.
- With a dedicated administrator account.
- No other applications installed on this machine. If additional applications are installed, the Zerto Virtual Manager service must receive enough resources and HA remain enabled.
- With VMware vSphere High Availability (HA) enabled.
- With the `VM Restart Policy` set to `High`.

Note: 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.

You cannot take snapshots of the Zerto Virtual Manager as snapshots cause operational problems for the Zerto Virtual Manager, such as creating inconsistencies with peer site Zerto Virtual Managers.

Routable Networks

The Zerto Virtual Replication architecture supports the following network configurations:

- Flat LAN networks
- VLAN networks, including private VLANs and stretched VLANs
- WAN emulation
- VPN IPsec

The Zerto Virtual Replication 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 bandwidth must be at least 5 Mb/sec.

The Zerto User Interface

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

When using either the vSphere Web Client or Client console, you must use Internet Explorer version 10 or higher. Zerto recommends using an Internet Explorer version later than version 10.

Database Requirements

By default, an embedded SQL-based database is used but it is possible to use an externally managed database, Microsoft SQL Server. To use an externally managed database, during the installation choose the `Custom Installation` option.

The following Microsoft SQL Server versions are supported: 2008, 2008R2, 2012, 2014.

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.

Zerto recommends using SQL Server Enterprise Edition if you have 4 or more sites, or 40 or more hosts with virtual machines being protected or recovered, or more than 400 virtual machines to be protected.

Using an externally managed database requires the following configuration for the machine running SQL Server:

- 4 CPUs or 2 Dual Core CPUs and 16GB RAM.
- 20GB to accommodate the database and the logs generated by the Zerto Virtual Manager.

Note: If SQL Server is used, it is your responsibility to make sure that database downtime is planned in coordination with your disaster recovery and business continuity requirements. During database downtime, there will be inconsistencies between Zerto Virtual Managers, such as the management of checkpoints, resulting in problems if a recovery is required.

Firewall Considerations

Zerto Virtual Manager requires the following ports to be open in the protected and recovery site firewalls:

PORT	DESCRIPTION
22[1]	During Virtual Replication Appliance (VRA) installation on ESXi 4.x and 5.x hosts for communication between the Zerto Virtual Manager (ZVM) and the ESXi hosts IPs and for ongoing communication between the ZVM in the cloud site – but not the customer site – and a Zerto Cloud Connector.
443	During VRA installation on ESX/ESXi hosts for communication between the ZVM and the ESX/ESXi hosts IPs and for ongoing communication between the ZVM and vCenter Server and vCloud Director.
4005	Log collection between the ZVM and VRAs on the same site.
4006	TCP communication between the ZVM and VRAs and the VBA on the same site.
4007	TCP control communication between protecting and recovering VRAs and between a Zerto Cloud Connector and VRAs.
4008	TCP communication between VRAs to pass data from protected virtual machines to a VRA on a recovery site and between a Zerto Cloud Connector and VRAs.
4009	TCP communication between the ZVM and site VRAs to handle checkpoints.
5672	TCP communication between the ZVM and vCloud Director for access to AMQP messaging.
9080	HTTP communication between the ZVM and Zerto internal APIs, a Zerto Cloud Manager (ZCM), cmdlets, and a VSS Agent.
9081[2]	TCP communication between paired ZVMs[3] and between a ZVM and a Zerto Cloud Connector.
9082 and up	**When a cloud service provider supplies DRaaS** – Two TCP ports for each VRA (one for port 4007 and one for port 4008) accessed via the Zerto Cloud Connector installed by the cloud service provider. There is directionality to these ports. Zerto recommends using a port range starting with port 9082. For example, Customer A network has 3 VRAs and customer B network has 2 VRAs and the cloud service provider network has 4 VRAs, then the following ports must be open in the firewall for each cloud: The cloud service provider's VRAs need to use 6 ports to reach customer A's VRAs, while customer A's VRAs need 8 ports to reach the cloud's VRAs. The cloud service provider's VRAs need to use 4 ports to reach customer B's VRAs, while customer B's VRAs need 8 ports to reach the cloud's VRAs.

PORT	DESCRIPTION
9180	Communication between the VBA and VRA.
9669	HTTPS communication between the machine running the Zerto User Interface and a ZVM, and for invoking Zerto RESTful APIs.
9779	HTTPS communication between the Zerto Self-Service Portal for in-cloud (ICDR) customers and a ZVM.
9989	HTTPS communication between a browser and the Zerto Cloud Manager.

1. If the ESX/ESXi hosts are given names, make sure that the Zerto Virtual Manager can resolve these names.
2. The default port set during the Zerto Virtual Replication installation. When pairing the ZVM to a Zerto Cloud Connector, this value must not be changed.
3. When the same vCenter Server is used for protection and recovery, Zerto Virtual Replication is installed on one site only and this port is ignored.

VMware Privileges Required by Zerto Virtual Replication

When Zerto Virtual Replication accesses the vCenter Server, it requires the vSphere privileges assigned to Administrator roles, which includes the following privileges.

CATEGORY	PRIVILEGE	NOTES
Alarms	Create alarm	Only during install and uninstall
	Remove alarm	
Authorization	Modify permission	Only during install and uninstall
	Modify role	
	Reassign role permissions	
Datastore	Allocate space	For source/target replication of datastores
	Browse datastore	
	Remove file	
	Low level file operations	
	Move datastore	
	Update virtual machine files	
Datastore cluster	Configure a datastore cluster	For installation of VRAs
Extension	Register extension	Only during install and uninstall
	Unregister extension	
	Update extension	
Folder	Create folder	
	Delete folder	
	Move folder	
Global	Cancel task	
	Diagnostics	
	Global tag	
	Log event	
	Manage custom attributes	
	Script action	
	Set custom attribute	
Host > Configuration	Advanced settings	
	Virtual machine autostart configuration	
	Change settings	
	Security profile and firewall	

CATEGORY	PRIVILEGE	NOTES
Host > Inventory	Modify cluster	
Network	Assign network	
Resource	Assign vApp to resource pool	
	Assign virtual machine to resource pool	
Sessions	Validate session	
Tasks	Create task	
	Update task	
vApp	vApp application configuration	
	Assign resource pool	
	Add virtual machine	
	Create	
	Delete	
	Import	
	vApp instance configuration	
	vApp managedBy configuration	
	Power off	
	Power on	
	Rename	
	vApp resource configuration	
	Unregister	
Virtual Machine > Configuration	Add existing disk	Swapfile placement is required to restore an offsite backup.
	Add new disk	
	Add or remove device	
	Advanced	
	Set annotation	
	Change CPU count	
	Extend virtual disk	
	Modify device settings	
	Configure managedBy	
	Memory	
	Raw device	
	Remove disk	
	Rename	
	Change resource	
	Settings	
	Swapfile placement	
	Upgrade virtual machine compatibility	
Virtual machine > Interaction	Power off	
	Power on	

CATEGORY	PRIVILEGE	NOTES
Virtual machine > Inventory	Create from existing	
	Create new	
	Move	
	Register	
	Remove	
	Unregister	

Note: The *Zerto* role must also be available. This role is added to the Administrator user during the Zerto Virtual Replication installation.

Performing an Installation

The Zerto Virtual Replication installation deploys the Zerto Virtual Manager (ZVM) and copies the installation software 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 vCenter Server, 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 the vCenter Server is also in the datacenter used for the recovery and not protection.

In all cases, Zerto recommends that you do not install Zerto Virtual Replication on the machine running the vCenter Server service.

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

- "Performing an Express Installation", below
- "Performing a Custom Installation", on page 12

Performing an Express Installation

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

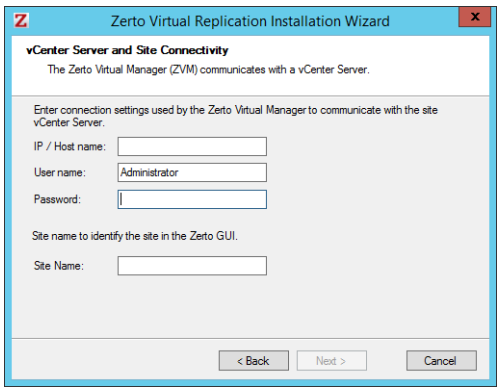
Note: You cannot install Zerto Virtual Replication on the same machine where another version of Zerto Virtual Replication has been installed, for example, if the *Zerto Virtual Replication for Microsoft Hyper-V* version has been installed on the machine.

To perform an express install of Zerto Virtual Replication:

1. Run `Zerto Virtual Replication Installer.exe`.

   Note: If Microsoft .NET Framework 4 or higher is not installed, the installation fails. Install .NET Framework 4, which is included as part of the Zerto Virtual Replication installation package. Reboot the machine, and rerun the Zerto Virtual Replication installation.
2. Follow the wizard through the installation until the *Installation Type* dialog and select the `Express Installation` option.
3. Click *Next*.

   The *vCenter Server and Site Connectivity* dialog is displayed.



4. Specify the following:

   IP / Host Name – The IP address or host name of the machine where the vCenter Server runs.

   User Name – The user name of a user with administrator level privileges in the vCenter Server. The name can be entered using either of the following formats:

   `username`

   `domain\username`

   Password – A valid password for the given user name.

   Site Name – A name to identify the site.

5. Click *Next*.

   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.
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 vCenter Server 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. Set any antivirus software running on the machine not to scan the folder where Zerto Virtual Replication is installed.

Install Zerto Virtual Replication on the peer sites.

Performing a Custom Installation

You can install Zerto Virtual Replication providing specific details including the ports that will be used by Zerto Virtual Replication and full contact details. In addition, when performing a custom install, you can provide information to connect to vCloud Director.

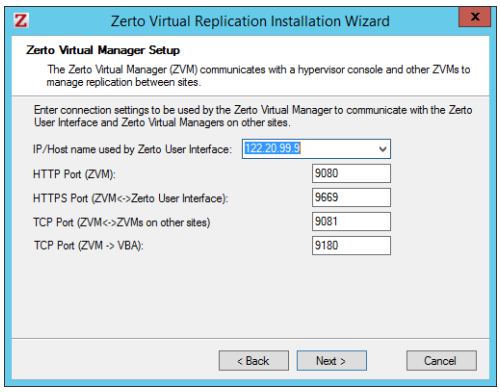
To perform a custom install of Zerto Virtual Replication:

1. Run `Zerto Virtual Replication Installer` executable.

   Note: If Microsoft .NET Framework 4 or higher is not installed, the installation fails. Install .NET Framework 4, which is included as part of the Zerto Virtual Replication installation package. Reboot the machine, and rerun the Zerto Virtual Replication installation.

2. Follow the wizard through the installation until the dialog for the *Installation Type* and select the `Custom Installation` option.
3. Click *Next*.

The *Zerto Virtual Manager Setup* dialog is displayed.



IP/Host name used by Zerto User Interface – The IP to access the Zerto Virtual Manager from the Zerto User Interface. If the machine has more than one NIC, select the appropriate IP from the list, otherwise the IP that is displayed is the only option.

HTTP Port (ZVM) – The port used for inbound communication between the Zerto Virtual Manager and Zerto internal APIs, Cmdlets and a VSS Agent.

HTTPS Port (ZVM <-> Zerto User Interface) – The port used for inbound communication between the Zerto User Interface and the Zerto Virtual Manager.

TCP Port (ZVM <-> ZVMs on other sites) – The port used for communication between Zerto Virtual Managers.

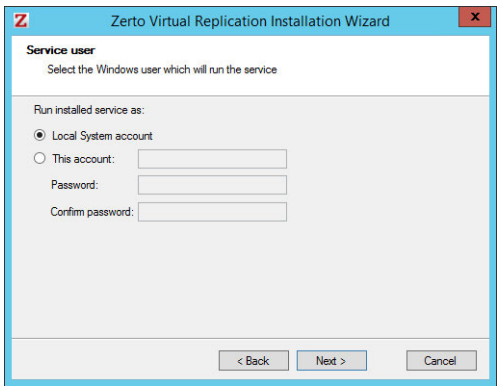
Both the protected and recovery sites belong to the same enterprise – If you change the value, when pairing sites, use the TCP port value you specify here. Pairing the sites is described in "Pairing Sites", on page 27.

An enterprise using a cloud service provider to supply disaster recovery services – You must not change this value.

TCP Port (ZVM -> VBA) – The port used for communication between the Zerto Virtual Manager and the Virtual Backup Appliance.

4. Click *Next*.

   The *Service User* dialog is displayed.



5. 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.

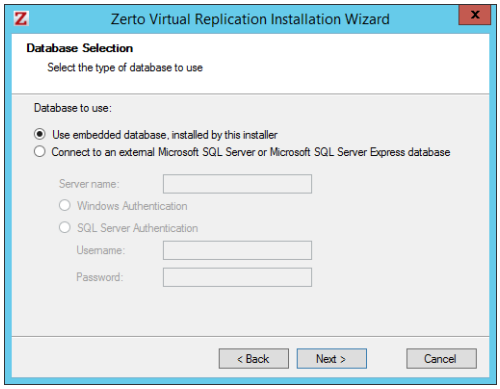
   Confirm password – Confirmation of the password.

6. Click *Next*.

   The *Database Selection* dialog is displayed. Information required by Zerto Virtual Replication is stored 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 used, but you can use an externally managed database, either Microsoft SQL Server or SQL Server Express.

Note: Protection and recovery can only be performed when the database is running. Therefore, if you use an external database and it is down for any reason, protection ceases.



7. To use the embedded database, leave the default or select the option to connect to an external Microsoft SQL Server database.

   Zerto recommends using SQL Server with sites with more than 40 hosts that have virtual machines that require protecting and more than 400 virtual machines that need protecting.

   If you select the external database option:

   Server name – The domain name and server instance to connect to, with the format `domain\instance`.

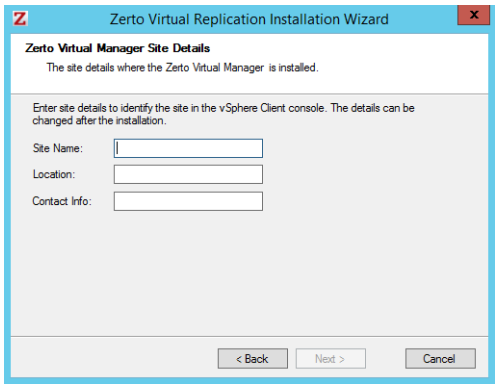
   Specify one of the following authentication options:

   Windows Authentication – Use Windows authentication. This option is only enabled if a specific service user account was specified in the previous *Service User* dialog, in which case the service account name and password are used.

   SQL Server Authentication – Use SQL Server authentication.
   User Name – The user name for the SQL Server database.
   Password – A valid password for the given user name.

8. Click *Next*.

   The *Zerto Virtual Manager Site Details* dialog is displayed.



9. Enter the site details:

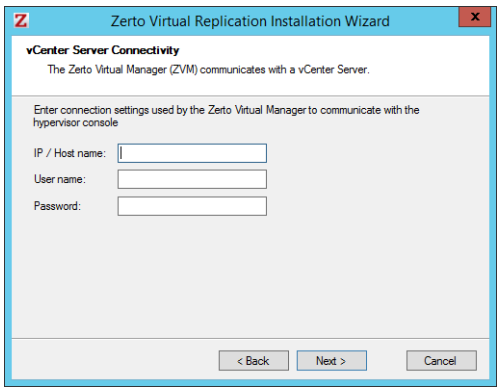
   Site Name – A name to identify the site. This name is displayed in the Zerto User Interface.

   Location – Information such as the address of the site or a significant name to identify it.

   Contact Info – Who to contact if a need arises, such as a phone number or email address.

10. Click *Next*.

The *vCenter Server Connectivity* dialog is displayed.



11. Enter connection settings that the Zerto Virtual Manager uses to communicate with the vCenter Server:

    IP / Host name – The IP address or host name of the machine where the vCenter Server runs.

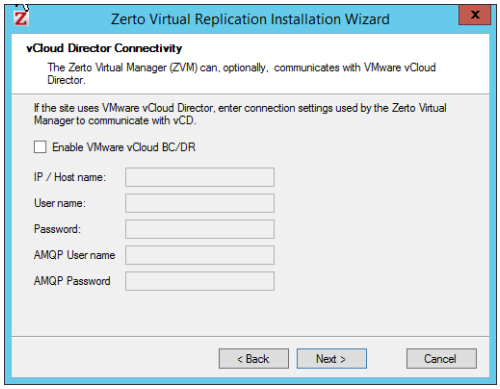
    User name – The user name of a user with administrator level privileges in the vCenter Server. The name can be entered using either of the following formats:

    `username`
    `domain\username`

    Password – A valid password for the user name.

12. Click *Next*.

    The *vCloud Director Connectivity* dialog is displayed.



13. When using vCloud Director and you have installed an AMQP server, click the `Enable VMware vCloud BC/DR` checkbox and enter the VMware vCloud Director access details:

    IP / Host name – The IP address or host name of the machine where vCD runs. When connecting to vCD with multiple cells, enter the virtual IP for the network load balancing used by the cells.
    User name – The user name for an administrator to vCD.
    Password – A valid password for the given user name.
    AMQP User name – The user name for the AMQP server.
    AMQP Password – A valid password for the given AMQP user name.

    If the vCD connection settings are not specified, for example, when you do not have an AMQP server installed, they can be set in the `Advanced Settings` dialog in the `Site Configuration` panel, in the Zerto User Interface after installation, as described in the *Zerto Cloud Manager Administration Guide*.

    Zerto provides an AMQP installation kit if you do not have one installed for vCD. Run `ZertoAMQPInstallWizard.exe` as described in the *Zerto Cloud Manager Administration Guide*, with the following credentials:

    User name – The AMQP user account Zerto will use. RabbitMQ prior to version 3.3 installs with a default administrator user: guest. In RabbitMQ version 3.3 and higher, specify a user with administrator privileges.
    Password – The password for the user. RabbitMQ prior to version 3.3 installs with a default password of guest.

14. Click *Next*.

The *Check Prerequisites* dialog is displayed. The installation performs checks to make sure that the installation can proceed successfully.

15. After the checks complete successfully, click *Next* and continue to the end of the installation.

    If you intend managing your disaster recovery from this machine, you can select to open the Zerto Virtual Manager (ZVM) Interface at the end of the installation, logging in with the user name and password for the vCenter Server connected to the Zerto Virtual Manager. In this user interface you set up Zerto Virtual Replication, as described in "Initial Configuration", on page 23.

16. Set any antivirus software running on the machine not to scan the folder where Zerto Virtual Replication is installed.

Install Zerto Virtual Replication on the peer sites.

Note: If the vSphere Client console was open during the installation, close it and reopen it to ensure you have the Zerto Virtual Replication UI loaded.

After installing Zerto Virtual Replication, add the machine to the relevant host boot configuration, so that on starting up a host this machine running the Zerto Virtual Manager is also powered on automatically.

Performing a Silent Installation

You can perform a silent installation of Zerto Virtual Replication, by running `Zerto Virtual Replication Installer.exe -s`, after setting the following environment variables:

- ZertoAutomation_Username – Optional. When using a specific account as the user account to run the Zerto Virtual Manager service, the name for the account.
- ZertoAutomation_Password – Optional. A valid password for the given user account.
- ZertoAutomation_DbServer – Optional. The external database domain name and server instance to connect to, with the format `domain\instance`.
- ZertoAutomation_DbUsername – Optional. The user name for the SQL Server database.
- ZertoAutomation_DbPassword – Optional. A valid password for the given SQL Server database user name.
- ZertoAutomation_SiteName – The name used to identify the site. This name is displayed in the Zerto User Interface.
- ZertoAutomation_Contact – Who to contact if a need arises, such as a phone number or email address.
- ZertoAutomation_VcenterIP – The IP address or host name of the machine where the vCenter Server runs.
- ZertoAutomation_vcUsername – The username to access the vCenter Server
- ZertoAutomation_vcPassword – The password to access the vCenter Server
- ZertoAutomation_VCDIP –Optional. The IP address or host name of the machine where vCD runs. When connecting to vCD with multiple cells, enter the virtual IP for the network load balancing used by the cells.
- ZertoAutomation_vcdUsername – Optional. The username to access vCloud Director
- ZertoAutomation_vcdPassword – Optional. The password to access vCloud Director
- ZertoAutomation_vcdMQUsername – Optional. The username to access AMQP, when using vCloud Director
- ZertoAutomation_vcdMQPassword – Optional. The password to access AMQP, when using vCloud Director

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:

```
-NoExit -Command 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:

```
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*.

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.

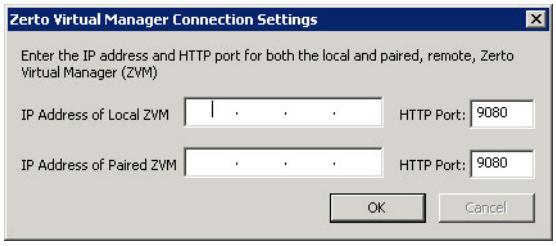
To use Zerto Virtual Replication with VSS to ensure application consistency you must install the ZertoVssAgent on every virtual machine that uses VSS and that you want to protect with Zerto Virtual Replication. The ZertoVssAgent is available from Zerto Ltd. in both 32-bit and 64-bit versions. You can install the ZertoVssAgent on the following supported Windows operating systems:

32-BIT OPERATING SYSTEMS	64-BIT OPERATING SYSTEMS
Windows Server 2003 SP2	Windows Server 2003 SP2
	Windows Server 2008, all versions (SPs and R2)
	Windows Server 2012, all versions (SPs and R2)

To install the ZertoVssAgent:

1. Run either *ZertoVss32Agent.msi* or *ZertoVss64Agent.msi* on every virtual machine that uses VSS and that you want to protect with Zerto Virtual Replication, where *ZertoVss32Agent.msi* is for 32-bit Windows operating systems and *ZertoVss64Agent.msi* is for 64-bit Windows operating systems.
2. Follow the wizard through the installation.

The `Zerto Virtual Manager Connections Settings` dialog is displayed.



3. 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 vCenter Server is used both for protecting and recovering virtual machines, specify the IP address and HTTP port number for the single Zerto Virtual Manager installed.

   Note: 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 (x86)\Zerto`.

4. Click *OK*.

The ZertoVssAgent is installed and the `Add VSS Checkpoint` 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*.

Re-installing the Current Installation

If a new installation is the same version as the installed version, installation options are *Reinstall* or *Uninstall*.

When reinstalling the version, all pairing, VRAs and VPGs defined for the site are removed. Use the *Zerto Diagnostics* utility options *Export* and *Import* options, as described in "Upgrading To More Than One Version Higher", on page 31 to save the settings.

If the vSphere Client console was open during the re-installation, close it and reopen it to ensure you use the upgraded Zerto User Interface.

CHAPTER 2: ACCESSING THE ZERTO USER INTERFACE

You manage the protection and replication of virtual machines in vSphere, 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. Zerto also provides a set of RESTful APIs and PowerShell cmdlets to enable incorporating some of the disaster recovery functionality within scrips or programs.

You manage the protection and replication of virtual machines between the protected and recovery sites, using one of the following:

- The Zerto Virtual Manager Web Client.
- The vSphere Web Client.
- The vSphere Client console.

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.

The following topics are described in this chapter:

Using the Zerto User Interface From a Browser

To use the Zerto Virtual Manager Web Client:

1. In a browser, enter the following URL:
   `https://zvm_IP:9669`
   where *zvm_IP* is the IP address of the Zerto Virtual Manager for the site you want to manage.
2. Login using the user name and password for the vCenter Server connected to the Zerto Virtual Manager.

Using the Zerto User Interface Within vSphere

The Zerto User Interface is embedded in both the vSphere Web Client and Client console as a plug-in. When accessing the Zerto User Interface from within vSphere the interface is available via a tab in the vSphere user interface. When using the Zerto User Interface via vSphere you have the following additional features:

- You can protect a vApp as a single entity in a VPG for any vApp defined under an ESX/ESXi host. All the virtual machines defined in the vApp VPG are protected and you can migrate or recover the whole vApp as a single entity to the recovery site.

  Note: The recovery site cannot be Microsoft Hyper-V nor Amazon Web Services (AWS).
- You can protect a virtual machine, that is not already included in a VPG, directly via the *Zerto* tab for the virtual machine in vSphere Client console.

Using the vSphere Web Client

You can use the VMware Web Client to manage Zerto Virtual Replication.

The vSphere Web Client is a service that when installed enables a browser-based interface for configuring and administering virtual machines enabling you to connect to a vCenter Server system to manage an ESXi host through a browser. The following procedure describes how to configure the vSphere Web Client to display Zerto Virtual Replication dialogs.

This procedure is valid for vSphere Web Client version 5.1 communicating with vCenter Server from version 5.0 and higher.

Note: The following procedure assumes that the vSphere Web Client version 5.1 has been installed. Although you can run the vSphere Web Client version 5.1 with vSphere Server 5.0 and 5.1, when installing the vSphere Web Client you need access to a vSphere Server version 5.1 which includes an option for single sign on, required by the vSphere Web Client installation.

Note: Setting up Zerto Virtual Replication to be used via the vSphere Web Client disables the use of other VMware plug-ins, such as VDP and VSA, causing them to disappear from the web client. This is a known VMware problem, see http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2042455. To resolve this issue, set up two web clients, on different servers. On one run Zerto Virtual Replication and on the other run the VMware plug-ins.

To set up the vSphere Web Client to work with to work with Zerto Virtual Replication:

1. When the vSphere Web Client service is installed on a Microsoft Windows platform: Copy and run `VsphereWebClientPluginEnabler.exe` to the machine where you run the web client service. This file is located in the `Zerto Virtual Replication` folder under the folder where Zerto Virtual Replication was installed. You can copy `VsphereWebClientPluginEnabler.exe` to any folder on the relevant machine. Run `VsphereWebClientPluginEnabler.exe` as an administrator.

   When the vSphere Web Client is installed on a Linux platform, via the vCenter Server Linux Virtual Appliance (vCSA): In the directory `/var/lib/vmware/vsphere-client`, open the `webclient.properties` file in a text editor and add the following to the file:.

   ```
   scriptPlugin.enabled = true
   ```

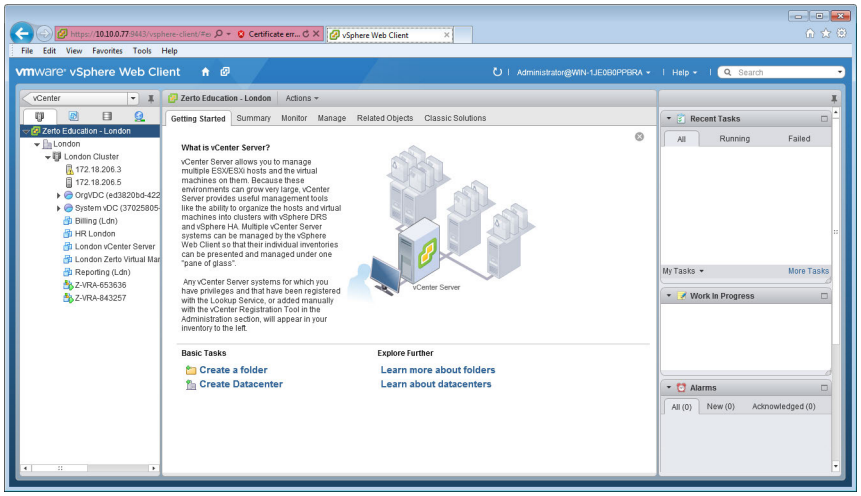
2. Restart the vSphere Web Client service.

   Note: After the service has started you might have to wait a few minutes before you can open the vSphere Web Client in your browser.

To use the vSphere Web Client:

1. Log in using the vCenter Server access credentials (user name and password) for the vCenter Server connected to the Zerto Virtual Manager.
2. In the browser, navigate to a vSphere node supported by Zerto Virtual Replication, such as the root node or a virtual machine, and choose the `Classic Solutions` tab, which is now displayed after the `Related Objects` tab.

   Note: With Chrome and Firefox browsers, you must load the script plug-in page in an external tab at least once before it appears inside the vSphere Web Client. The `Classic Solutions` tab is displayed when there is a plug-in installed, in this case the Zerto Virtual Replication user interface plug-in.
3. If prompted, allow blocked content to be displayed.



4. If more than one plug-in is installed, click *Zerto* to display the Zerto Virtual Replication user interface.

Using the vSphere Client Console

To use the vSphere Client console:

1. Login using the user name and password for the vCenter Server connected to the Zerto Virtual Manager.
2. Access the *Zerto* tab, displayed for the root node.

   Note: The *Zerto* tab is also displayed for a datacenter node showing the same information as for the root node. For a virtual machine or vApp node the *Zerto* tab displays information specific to the virtual machine or vApp.

Adding a Security Certificate

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.

To install a security certificate for the Zerto User Interface:

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

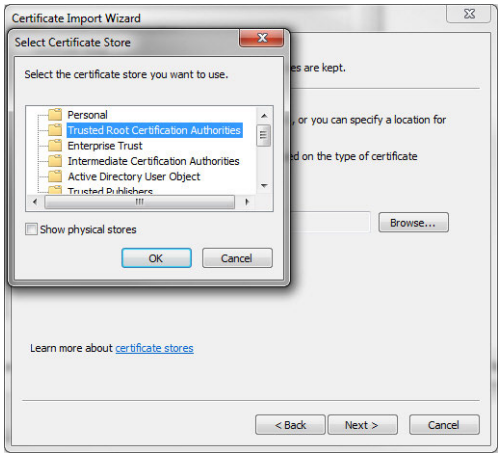
Note the following:

- This procedure is based on Microsoft Internet Explorer. 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.

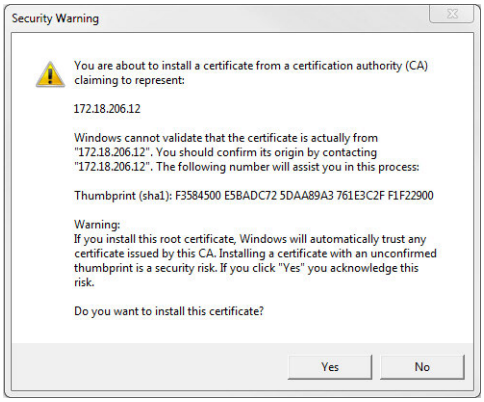
1. Click *View Certificate*.

   The *Certificate* dialog is displayed.
2. Click *Install Certificate*.

   The *Certificate Import Wizard* dialog is displayed.
3. Follow the wizard: Place all the certificates in the `Trusted Root Certification Authorities` store: Select the `Place all certificates in the following store` option and browse to select the `Trusted Root Certification Authorities` store.



4. Continue to the end of the wizard. Click *Yes* when the Security Warning is displayed.



5. Click *OK* that the installation was successful.
6. Click *OK* when prompted and then *Yes* in the *Security Alert* dialog to continue.

CHAPTER 3: INITIAL CONFIGURATION

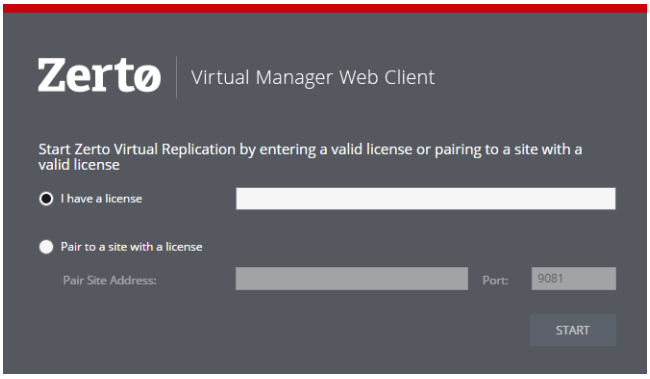
After installing Zerto Virtual Replication, you configure the site. Zerto Virtual Replication is configured and managed from within the Zerto User Interface. This chapter describes the initial configuration required after installing Zerto Virtual Replication.

The following topics are described in this chapter:

Cloud service providers must configure both Zerto Virtual Manager and a Zerto Cloud Manager as described in *Zerto Cloud Manager Installation Guide* and *Zerto Cloud Manager Administration Guide*.

Registering the Zerto Virtual Replication License

On the very first access to the Zerto User Interface, you must 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.



Note: 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. A CSP with more than one cloud site must enter a license at each cloud site instead of pairing to a licensed cloud site. The license can be the same license used in another cloud site. The CSP can then pair the sites as described in "Pairing Sites", on page 27. If the CSP registers Zerto Virtual Replication by pairing to another site with a license, instead of registering by entering a license, the registration works and the CSP can use both sites but customers cannot successfully pair to the site without a license.

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 pair the protected and recovery sites, as described in the following sections.

Installing Virtual Replication Appliances

The Zerto Virtual Replication installation includes the OVF template 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 hypervisor which hosts virtual machines that require protecting in the protected site and on every hypervisor

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.

With VMware vApps, if you want to protect a vApp, you must install a VRA on every ESX/ESXi host in the cluster on both the protected and recovery sites and ensure that DRS is enabled for these clusters.

VRA Installation Requirements

To install a VRA you require the following:

- 12.5GB datastore space.
- At least 1GB of reserved memory.
- The ESX/ESXi version must be 4.0U1 or higher and Ports 22 and 443 must be enabled on the host during the installation.

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

- The password to access the host root account, for ESXi 4.x and 5.x.
- 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, which is the Zerto recommendation[1], instead of DHCP, the IP address, subnet mask, and default gateway to be used by the VRA.

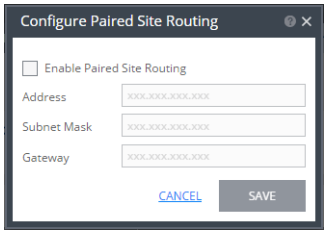
Note: For the duration of the installation of the VRA, the Zerto Virtual Manager enables SSH in the vCenter Server.

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.

To set up routing:

1. In the *SETUP > VRAs* tab, select *MORE > Paired Site Routing*.

   The *Configure Paired Site Routing* dialog is displayed.



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 the VRAs on the peer site.

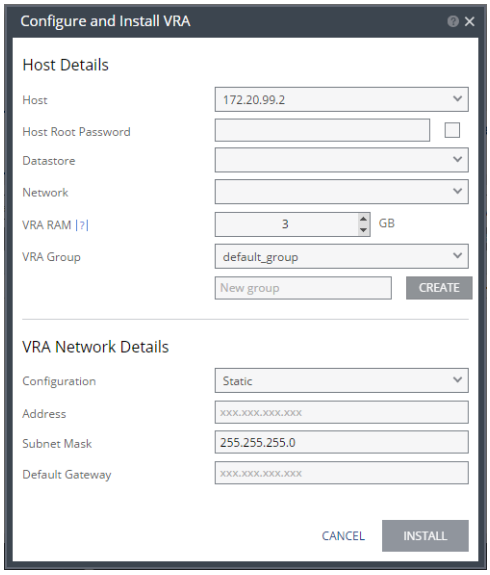
1. In a non-production environment it is often convenient to use DHCP to allocate an IP to the VRA. In a production environment this is not recommended. For example, if the DHCP server changes the IP allocation on a reboot, the VRA does not handle the change.

The settings in the *Configure Paired Site Routing* dialog apply to all VRAs installed after the information is saved. 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.

To install Zerto Virtual Replication Appliances (VRAs) on ESX/ESXi hosts:

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* dialog is displayed.



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

3. Specify the following `Host Details`:

   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 – The password used to access the host for the root user. This field is required for ESXi 4.x and 5.x hosts. This field is disabled for ESX 4.x hosts. When the checkbox at the side is checked, the password is displayed in plain text. The password is used by the Zerto Virtual Manager when deploying and upgrading the VRA on this host. Also, root access is required in case the Zerto host component is down and needs an automatic restart. The Zerto Virtual Manager checks that the password is valid once a day. If the password was changed, an alert is triggered, requesting the user enter the new password.

   Datastore – The datastore that the VRA will use for protected virtual machine data on the recovery site, including the journals. You can install more than one VRA on the same datastore.

   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.

AMOUNT OF VRA RAM	VRA BUFFER POOL SIZE
1GB	450MB
2GB	1450MB
3GB	2300MB
4GB	3,300MB
5GB	4,300MB
6GB	5,300MB

AMOUNT OF VRA RAM	VRA BUFFER POOL SIZE
7GB	6,300MB
8GB	7,300MB
9GB	8,300MB
10GB	9,300MB
11GB	10,300MB
12GB	11,300MB
13GB	12,300MB
14GB	13,300MB
15GB	14,300MB
16GB	15,300MB

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. That is, 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.

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

VRA Group – Choose the `VRA Group` from the dropdown list. If you want 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 vCenter Server 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 is on VRA1 in group1 and VPG2 in on VRA2 in group2, do not affect each other, as the priority is relevant only within each group.

4. Specify the following `VRA Network Details`:

   Configuration – Either have the IP address allocated via a static IP address or a DHCP server. If you select the `Static` option, which is the 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 either the *TASKS* popup dialog in the status bar or 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 host that hosts virtual machines that you want replicated. Zerto recommends installing a VRA on every listed host. An alert is issued after the first VRA is installed in a cluster that tells you to install a VRA on the other hosts 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.

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.

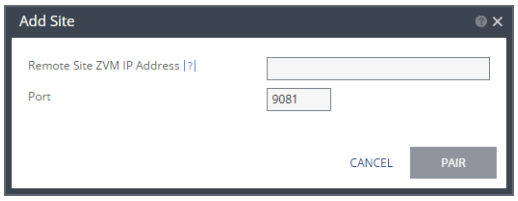
Pairing Sites

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.

To pair sites:

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

   The *Add Site* dialog is displayed.



2. Specify the following:

   Remote Site ZVM IP Address – IP address or fully qualified DNS host name of the remote site Zerto Virtual Manager to pair to.

   Port – The TCP port communication between the sites. Enter the port that was specified during installation. The default port during the installation is 9081.

3. Click *PAIR*.

   The sites are paired meaning that the Zerto Virtual Manager for the local vCenter site is connected to the Zerto Virtual Manager on the remote vCenter 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 hosts in the remote site:

- Repeat the procedure, "Installing Virtual Replication Appliances", on page 23, via the Zerto User Interface for the remote site.

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.

CHAPTER 4: UNINSTALLING ZERTO VIRTUAL REPLICATION

This chapter describes how to uninstall Zerto Virtual Replication.

You uninstall Zerto Virtual Replication, in one of the following ways:

- Via *Start > Programs > Zerto Virtual Replication > Uninstaller*.
- Rerun the installation and select the `Uninstall` option.
- Via the *Add or Remove Programs* 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 VMware vSphere environment, when the vCenter Server is down or when the Virtual Replication Appliance was installed on an ESXi host and the password to the host was changed, you can continue with the uninstall and later remove the Virtual Replication Appliance manually from within the vSphere Web client or Client console. If this does not work, contact Zerto support.

CHAPTER 5: UPGRADING ZERTO VIRTUAL REPLICATION

Zerto Virtual Replication releases regular updates. VMware and Microsoft also release new versions of their products which can impact Zerto Virtual Replication. This chapter describes different options for different upgrade scenarios.

The following topics are described in this chapter:

Upgrading Zerto Virtual Replication

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 order you upgrade the sites, protected or recovery, is not relevant as long as paired sites remain only one version apart.

Note: All releases prior to version 3.0U1 are considered versions, not updates. Thus, releases 2.0, 2.0U1, 2.0U2, etc., are *different* versions. As of version 3.0U1, upgrade releases are considered to be upgrades of the same version and releases 3.0U1, 3.0U2, etc., are the *same* version.

Therefore, while you cannot upgrade directly from 2.0 to 2.0U5, you can upgrade directly from 3.0U1 to 3.0U5. Similarly, you can upgrade directly from 2.0U5 to 3.0Ux and from 3.1 to 3.1Ux but you cannot upgrade directly from 2.0U5 to 3.1Ux.

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

CURRENT VERSION:	CAN UPGRADE TO:
2.0U5	3.0Ux
3.0Ux	3.1, 3.1Ux
3.1, 3.1Ux	3.5, 3.5Ux
3.5, 3.5Ux	4.0, 4.0Ux
4.0, 4.0Ux	N/A

Note: Zerto recommends upgrading to the latest version of Zerto Virtual Replication that supports the environment you are using. Refer to the "Zerto Virtual Replication Interoperability Matrix", on page 6 for the list of VMware environments supported by this version of Zerto Virtual Replication.

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. The following table shows what versions can be used on a peer site, based on the version running on the current site.

VERSION N (THIS VERSION)	VERSION N-1	VERSION N+1
2.0U5	2.0U4	3.0Ux
3.0Ux	2.0U5	3.1, 3.1Ux
3.1, 3.1Ux	3.0Ux	3.5, 3.5Ux
3.5, 3.5Ux	3.1, 3.1Ux	4.0, 4.0Ux
4.0, 4.0Ux	3.5, 3.5Ux	N/A

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 33. Zerto recommends that you always upgrade the VRAs to the latest version on your site.

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 Zerto Virtual Replication and Zerto Cloud Manager in parallel. First upgrade Zerto Virtual Replication and then upgrade Zerto Cloud Manager so that they are never more than one version apart.

Before Upgrading

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 via the vSphere Client console.
- 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`.
- Complete any recovery operation before starting the upgrade.
- Save the tweaks file before doing the upgrade, if you have made any changes to it. The tweaks.txt file is replaced with the default tweak file so all the tweaks entered before the upgrade are lost.
- Stop the Zerto Virtual Manager service.
- Create a backup of the machine where the Zerto Virtual Manager runs, to use in case 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, reinstall, or uninstall the installation.

Upgrading the Current Installation

The existing Virtual Replication Appliances and protected virtual machines, along 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 installation executable for vSphere.

   The Zerto Virtual Replication Installation Wizard is displayed.
2. Select *Upgrade* and click *Next*.

   The upgrade proceeds automatically.
3. Proceed to completion.

Note: If the vSphere Client console was open during the upgrade, close it and reopen it.

Additional Considerations

The following information should be considered when upgrading:

- When using the Zerto Cloud Manager, you must upgrade the Zerto Cloud Manager to be consistent with the latest version of Zerto Virtual Replication run by the CSP. Upgrade the version of Zerto Virtual Replication run by the CSP before Zerto Cloud Manager. Make sure that they are never more than one version apart from each other.
- VRAs from the existing installation are not automatically upgraded when upgrading Zerto Virtual Replication. VRAs installed with the previous version of Zerto Virtual Replication can continue to work with the current version and with any combination of VRAs, all from one version or a mix of VRA versions, on both the protected and recovery sites, as long as the VRA versions differ by only one version, higher or lower. Zerto recommends upgrading the VRAs to be consistent with the latest version.

  See "Upgrading VRAs", on page 33 for information relating to upgrading existing VRAs.

Upgrading Multiple Sites

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 beginning at the site whose version is lowest.

   Note: 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 also no more or 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, if you have sites running versions 3.0U4 paired to a site running 3.1U7, which is paired to sites running 3.5U4 and 3.5U5, and you are planning to upgrade to 4.0, you must first upgrade the 3.0U4 site to a 3.1Ux version and then to a 3.5Ux version and then the 3.1U7 to the 3.5Ux version before upgrading the 3.5Ux, 3.5U4 and 3.5U5 sites to version 4.0.

Upgrading To More Than One Version Higher

If you need to upgrade more than one version higher, do one of the following:

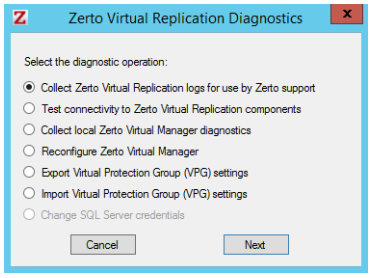
- Upgrade versions stepwise, one version at a time, as described above, until you reach the required version.
- Use the *Zerto Diagnostics* utility's export option to *export* the existing VPG definitions, then uninstall the old version of Zerto Virtual Replication. Install the new version, then use the *Zerto Diagnostics* utility's *import* option to re-create the VPGs.

Note: 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`.

To upgrade Zerto Virtual Replication using the Zerto Diagnostics utility:

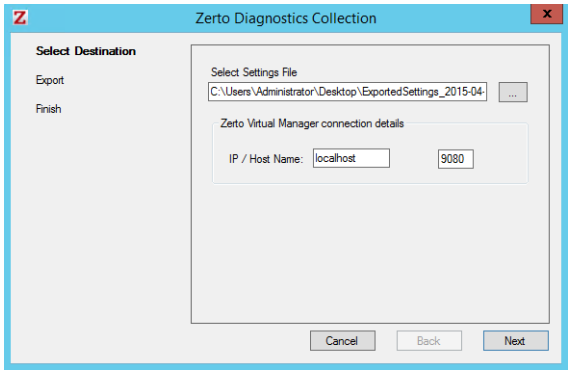
1. Click *Start* > *Programs* > *Zerto Virtual Replication* > *Zerto Diagnostics*.

   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 *Zerto_Installation_Folder*`\Zerto Virtual Replication\ExportedSettings` folder. You can use the last exported file. The default location of *Zerto_Installation_Folder* is `C:\Program Files (x86)\Zerto`.



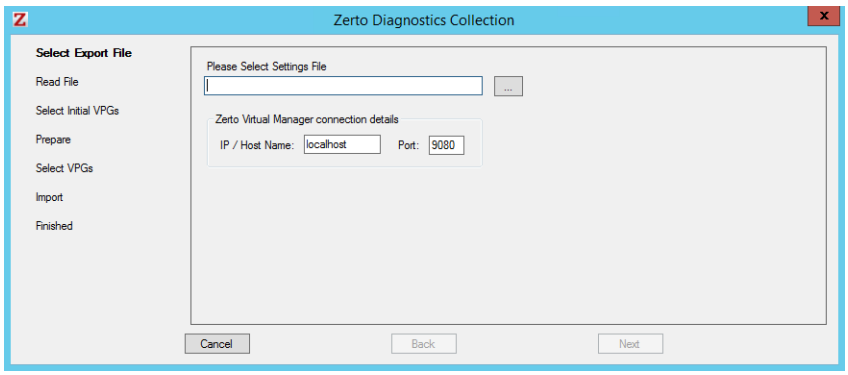
3. Select the destination for the file that will contain the exported settings and enter the Zerto Virtual Manager IP address and port for the protected site.
4. Click *Next*.

   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 *Zerto_Installation_Folder*`\Zerto Virtual Replication\ExportedSettings` folder. 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 (x86)\Zerto`.
7. Uninstall the existing Zerto Virtual Replication version.
8. Install the new Zerto Virtual Replication version, as described in "Performing an Installation", on page 11.
9. Install the VRAs on the hosts in the site, as described in "Installing Virtual Replication Appliances", on page 23 and pair the sites, as described in "Pairing Sites", on page 27.

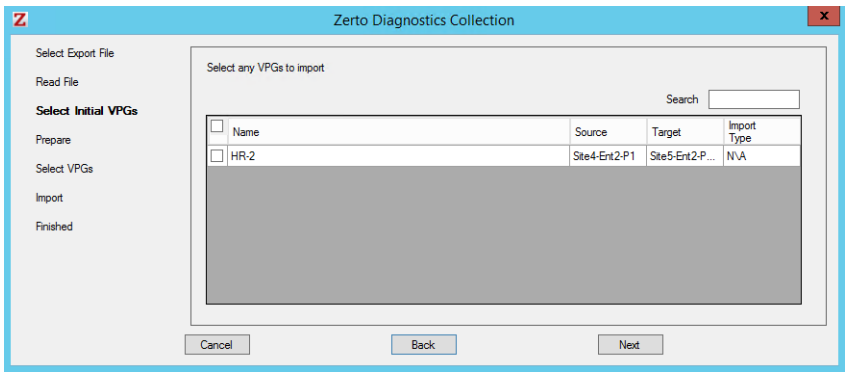
   Note: If the protected site and recovery site are the same for any of the VPGs that were exported, set `Enable replication to self` in the *Policies* section of the *Site Settings* dialog, as described in *Zerto Virtual Manager Administration Guide*.
10. Click *Start* > *Programs* > *Zerto Virtual Replication* > *Zerto Diagnostics*.

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



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.



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

When upgrading Zerto Virtual Replication, the VRAs that were installed in the previous version are not upgraded automatically. Zerto Virtual Replication enables VRAs installed with the previous version of Zerto Virtual Replication to work with VRAs installed with the current version of Zerto Virtual Replication in any combination of VRAs (all from one version or a mix of VRA versions) as long as the VRAs are only one update higher or lower than the version of Zerto Virtual Replication installed on this site. Zerto recommends upgrading the VRAs to be consistent with the latest version and this can be done by selecting *SETUP* > *VRAs*.

After upgrading Zerto Virtual Replication, the VRAs might also require an upgrade. You can see if an upgrade is available in the *VRAs* tab.

Note: An alert is also issued that there are VRAs that can be upgraded. Move the mouse over the `Outdated` value to display the VRA version as a tooltip.

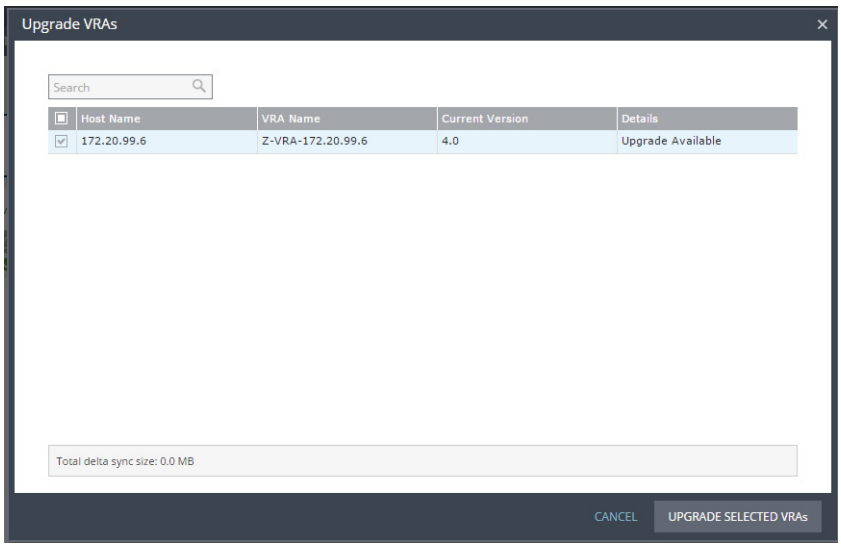
Considerations when upgrading VRAs:

- VRAs managing protected virtual machines: Either vMotion the protected virtual machines and datastores managed by the VRA to another host with a VRA, or upgrade the VRA without vMotioning the virtual machines and a bitmap 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.

To upgrade VRAs:

1. For a VRA protecting virtual machines, if vMotioning the protected virtual machines, remove affinity rules for protected virtual machines on the host with the VRA to be upgraded and vMotion 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 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.
4. Click *UPGRADE SELECTED VRAs*.

The upgrade progress is displayed in the *VRAs* tab.

A `Delta Sync`, for VRAs protecting virtual machines, or a `Bitmap Sync`, for VRAs managing recovery, is performed following the upgrade.

Note: The VRA name does not change, even if the naming convention in the latest version is different.

You do not need to upgrade VMware Tools on a VRA.

Upgrading PowerShell Cmdlets

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

Upgrading or Reinstalling VMware Components

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

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

Refer to the "Zerto Virtual Replication Interoperability Matrix", on page 6 for the list of VMware environments supported by this version of Zerto Virtual Replication.

Upgrading a vCenter Server

Zerto recommends that you upgrade a vCenter Server rather than reinstalling it.

When upgrading both vCenter and an ESX/ESXi, upgrade the vCenter first.

Zerto Virtual Replication components are not affected by a vCenter Server upgrade; protection continues and no additional procedures are required. When upgrading a vCenter Server, make sure that you preserve the vCenter database. Preserving the existing database is required in order to continue using the existing Zerto Virtual Replication installation.

Note: If the vCenter Server service is stopped, a Zerto Virtual Replication delta sync is performed on all protected virtual machines when the vCenter Server is restarted.

Reinstalling a vCenter Server

If, for whatever reason, you need to reinstall the vCenter Server, including rebuilding the database, contact Zerto support for help throughout the reinstallation.

Upgrading or Reinstalling a Host

When upgrading both vCenter and an ESX/ESXi, upgrade the vCenter first.

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

1. In the Zerto User Interface, click *SETUP* > *VRAs*, select the VRA, and click *MORE* > *Change VM Recovery VRA*.
   The *Change Target Host* dialog is displayed, listing all the virtual machines on that host.
2. Review the list and select the virtual machines whose target host you are changing.
3. Select the new target host for these virtual machines in the `Select the replacement host` drop-down list. You can move some virtual machines to one replacement target host and, by repeating the operation, move other virtual machines to a different replacement target host.
   - Validation is performed to verify that the selected target host can be used. For example, the datastores used by the VRAs must be accessible from both hosts.
   - The dialog displays the possible consequences resulting from the change.
4. Click *OK*.
5. Repeat this procedure from step 2 for all the virtual machines.

The VPG recovery host definitions are changed and the affected recovery data for each VRA is transferred to the new recovery host VRA. During the change procedure you cannot edit the affected VPGs, nor attempt a failover, move, failover test, or clone operation.

VRAs installed on ESXi 4.x and 5.x hosts require a password to access the host. If the host password changes, as happens when the host is upgraded, the VRA must be updated with the new password, as described in *Zerto Virtual Manager Administration Guide for the VMware vSphere Environment*.

To change the host password required by a VRA:

1. In the Zerto User Interface, click *SETUP* > *VRAs*, select the VRA, and click *MORE* > *Change Host Password*.
   The *Change Host Password VRA* dialog is displayed.
2. Enter the new host root password:
   New Password – Enter the new password.
3. Click *Save*.

Note: A procedure to change the passwords for more than one host at one time is described in the *Zerto Virtual Manager Administration Guide for the VMware vSphere Environment*.

Upgrading VMware Tools

You do not need to upgrade VMware Tools on a VRA.

Upgrading vCloud Director

Zerto recommends that you upgrade vCD rather than reinstalling it. Zerto Virtual Replication components are not affected, protection continues, and no additional procedures are required.

When upgrading vCD from version 1.5 to 5.1 or higher, you must change the storage profile for each protected virtual machine from * (any) to a valid storage profile to use for that virtual machine. Contact Zerto support for help with the upgrade of VPGs.

If, for whatever reason, you need to reinstall vCloud Director, contact Zerto support for help throughout the reinstallation.