Zerto

Zerto Installation Guide VMware vSphere Environment Microsoft Hyper-V Environment

Rev01 U3
Jan 2020
ZVR-INVC-HV-7.5

© 2020 Zerto All rights reserved.

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

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

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

ZVR-INVC-HV-7.5

Table of Contents

Installing the Zerto Solution 5
The Zerto Solution DR Architecture 7
Zerto Interoperability Matrix 11
Requirements - before installing Zerto software 11
Considerations 11
The Zerto User Interface in a vSphere Client 12
Database Requirements 12
vSphere Privileges Required by Zerto Virtual Replication 12
(Hyper-V Only) Privileges Required by Zerto Virtual Replication 17
Installing Zerto Virtual Replication in On-Premise Environments 17
Performing an Express Installation 18
Performing a Custom Installation 20
Performing a Silent Installation 28
Installing Zerto Cmdlets 32
Repairing the Current Installation 33
Uninstalling Zerto Virtual Replication 33
Upgrading Zerto Virtual Replication 34

Deploying Zerto Enterprise Government Edition 35
Prerequisites and considerations before deploying Zerto Enterprise Government Edition 35
Limitations when using Zerto Enterprise Government Edition 36
Installing a VRA in Zerto Enterprise Government Edition 36

Installing Zerto in Clustered vSphere Environments 40
Creating a Role for the Zerto Services 42
First Clustered Node - Installing Zerto Virtual Replication 43
Second Clustered Node - Installing Zerto Virtual Replication 52
Configuring the Role with Zerto Services 61
Uninstalling a Zerto Cluster 64

Accessing the Zerto User Interface 65
Using the Zerto User Interface From a Browser 66
Using the Zerto User Interface Within vSphere 66
Using the vSphere Web Client 66
Using the vSphere Client Console 68
Adding a Security Certificate for the Zerto User Interface 68

Initial Configuration 71
Registering the Zerto Virtual Replication License 71
Installing Virtual Replication Appliances 72
VRA Installation Requirements 73

Setting Up Routing 75
Installing a Zerto Virtual Replication Appliance (VRA) on a Host 76
Pairing Sites 79
Setting Up a Remote Site 82

Installing the Zerto Solution

Zerto 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 enables a virtual-aware recovery with low values for both the RTO and RPO. In addition, Zerto enables protecting virtual machines for extended, longer term recovery using a Long Term Retention process mechanism.

Zerto 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 enables a virtual-aware recovery with low values for both the RTO and RPO. In addition, Zerto enables protecting virtual machines for extended, longer term recovery using a Long Term Retention process mechanism.

Zerto helps customers accelerate IT transformation by eliminating the risk and complexity of modernization and cloud adoption. By replacing multiple legacy solutions with a single IT Resilience Platform™, Zerto is changing the way disaster recovery, retention and cloud are managed. This is done by providing enterprise-class disaster recovery and business continuity software for virtualized infrastructure and cloud environments.

In **on-premise** environments, Zerto Virtual Replication (ZVR) is installed with virtual machines to be protected and recovered.

In **public cloud** environments, Zerto Cloud Appliance (ZCA) is installed in the public cloud site that is to be used for recovery.

The installation includes the following:

- **Zerto Virtual Manager (ZVM)**: The ZVM is a Windows service, running on a dedicated Windows VM, that manages everything required for the replication between the protection and recovery sites, except for the actual replication of data. The ZVM interacts with the hypervisor management user interface, such as vCenter Server or Microsoft SCVMM, to get the inventory of VMs, disks, networks, hosts, etc. It also monitors changes in the hypervisor environment and responds accordingly. For example, a VMware vMotion operation, or Microsoft Live Migration of a protected VM from one host to another is seen by the ZVM, and the Zerto User Interface is updated accordingly.
    - For the maximum number of virtual machines, either being protected or recovered to that site, see Zerto Scale and Benchmarking Guidelines.

- **Virtual Replication Appliance* (VRA)**: A VRA is a virtual machine installed on each hypervisor host where VMs are to be protected from or to. The VRA manages the replication of data from protected virtual machines to the recovery site. The target VRAs are responsible for maintaining any protected VMs disks. VMware limits the number of SCSI Controllers (4 per VM) and targets per Controller (15 per controller), leaving a maximum of 60 SCSI targets per VM. When managing a larger quantity of virtual disks, Zerto utilizes Virtual Replication Appliance Helpers (VRA-H), which act as a disk box with no IP and nearly no resources. VRA-Hs are spun up and down by Zerto automatically when nearing the 60-disk limit of the VRA or last VRA-H.
  - For the maximum number of volumes, either being protected or recovered to that site, see Zerto Scale and Benchmarking Guidelines.

  > **Note:** *In vSphere installations, OVF to enable installing Virtual Replication Appliances.

- **Virtual Backup Appliance (VBA)**: A Windows service that manages File-Level Recovery operations within the Zerto solution.
- **Zerto User Interface:** Recovery using the Zerto solution is managed in a browser or, in VMware vSphere Web Client or Client console.

When Zerto is installed to work with an on-premise hypervisor it also comprises the following component:

- **Data Streaming Service (DSS)**: Installed on the VRA machine, and runs in the same process as the VRA. It is responsible for all the retention data path operations.

The following topics are described in this section:

- The Zerto Solution DR Architecture on page 7
- Zerto Interoperability Matrix on page 11
- Requirements - before installing Zerto software on page 11
- Considerations on page 11
- The Zerto User Interface in a vSphere Client on page 12
- Database Requirements on page 12
- vSphere Privileges Required by Zerto Virtual Replication on page 12
- (Hyper-V Only) Privileges Required by Zerto Virtual Replication on page 17
- Installing Zerto Virtual Replication in On-Premise Environments on page 17
- Performing a Silent Installation on page 28
- Installing Zerto Cmdlets on page 32
- Repairing the Current Installation on page 33
- Uninstalling Zerto Virtual Replication on page 33
- Upgrading Zerto Virtual Replication on page 34

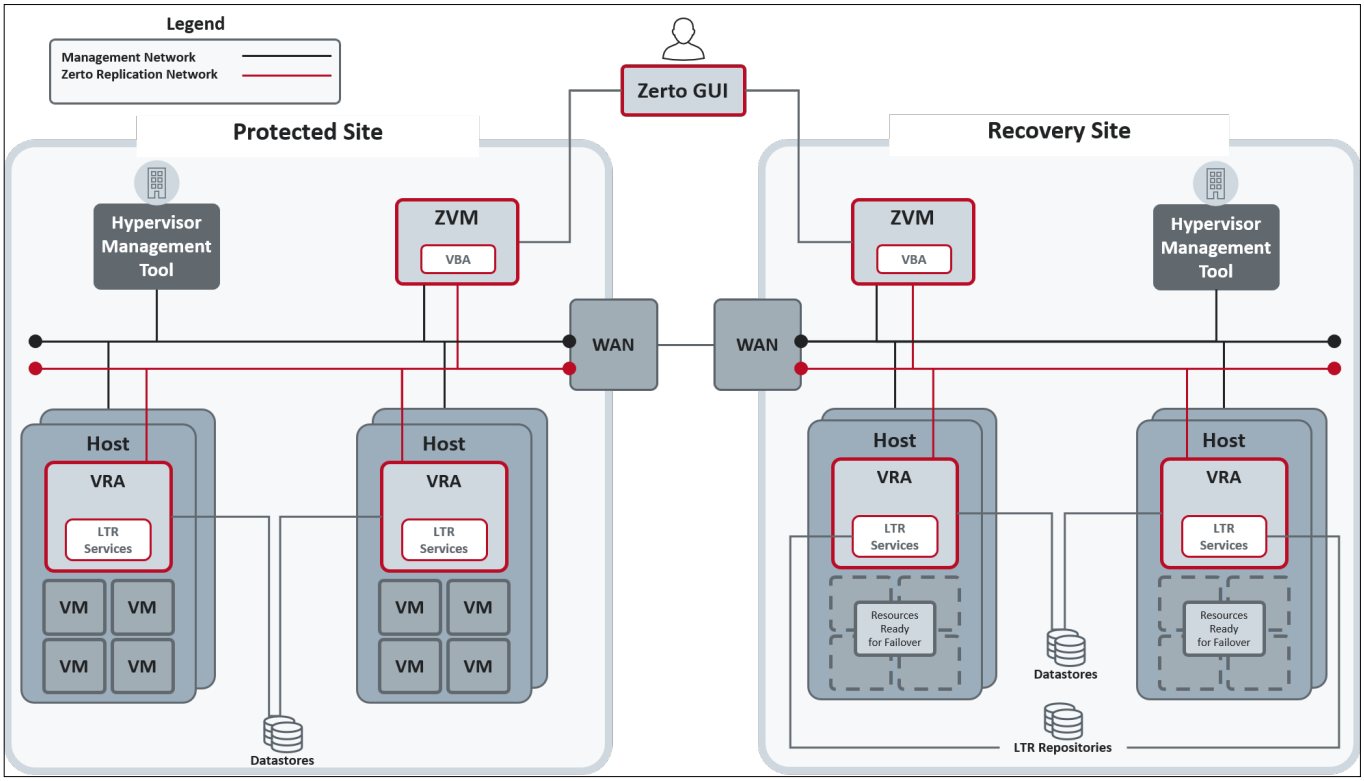
Note: To install Zerto in **clustered** vSphere environments, go to Installing Zerto in Clustered vSphere Environments on page 40

Note: For Zerto Enterprise Government Edition (EGE) environments, go to Deploying Zerto Enterprise Government Edition on page 35.

The Zerto Solution DR Architecture

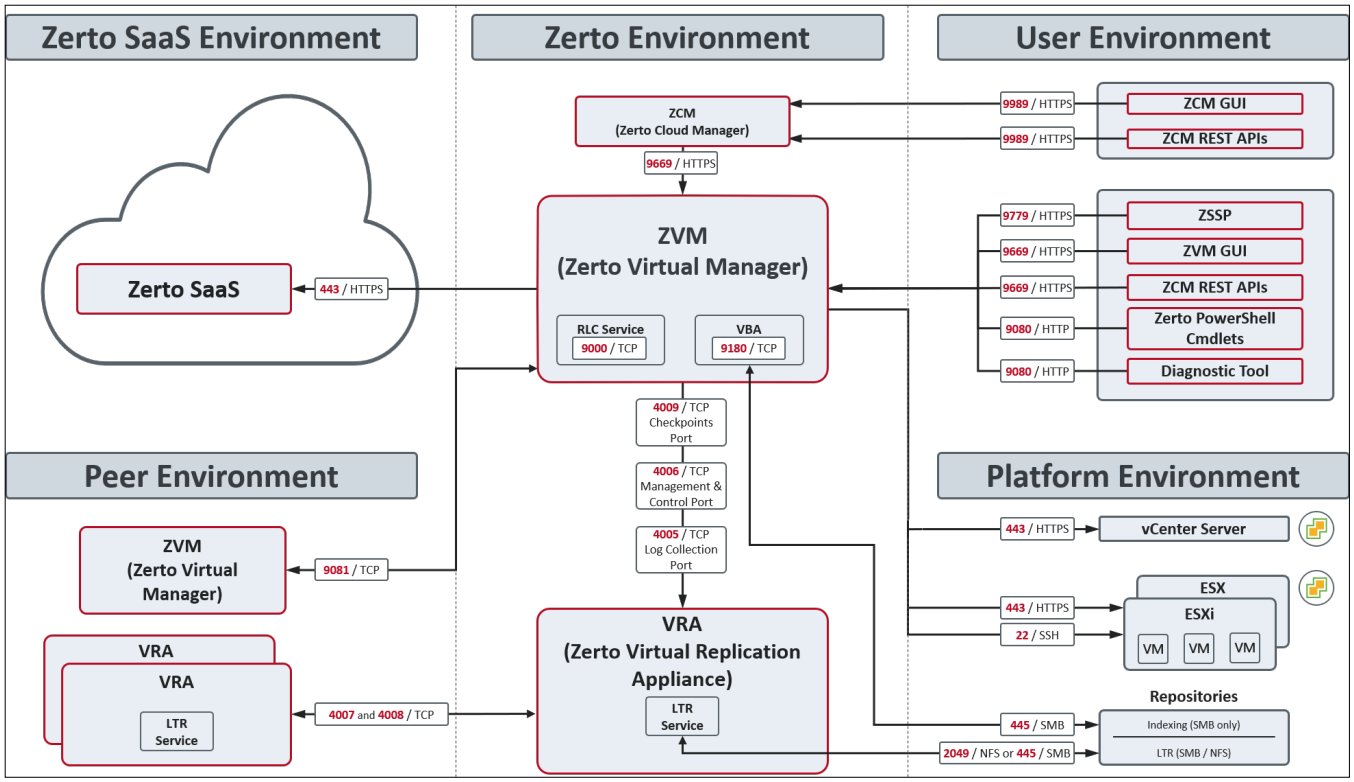
The following diagram shows how the main Zerto components are deployed across sites to provide disaster recovery across these sites.

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



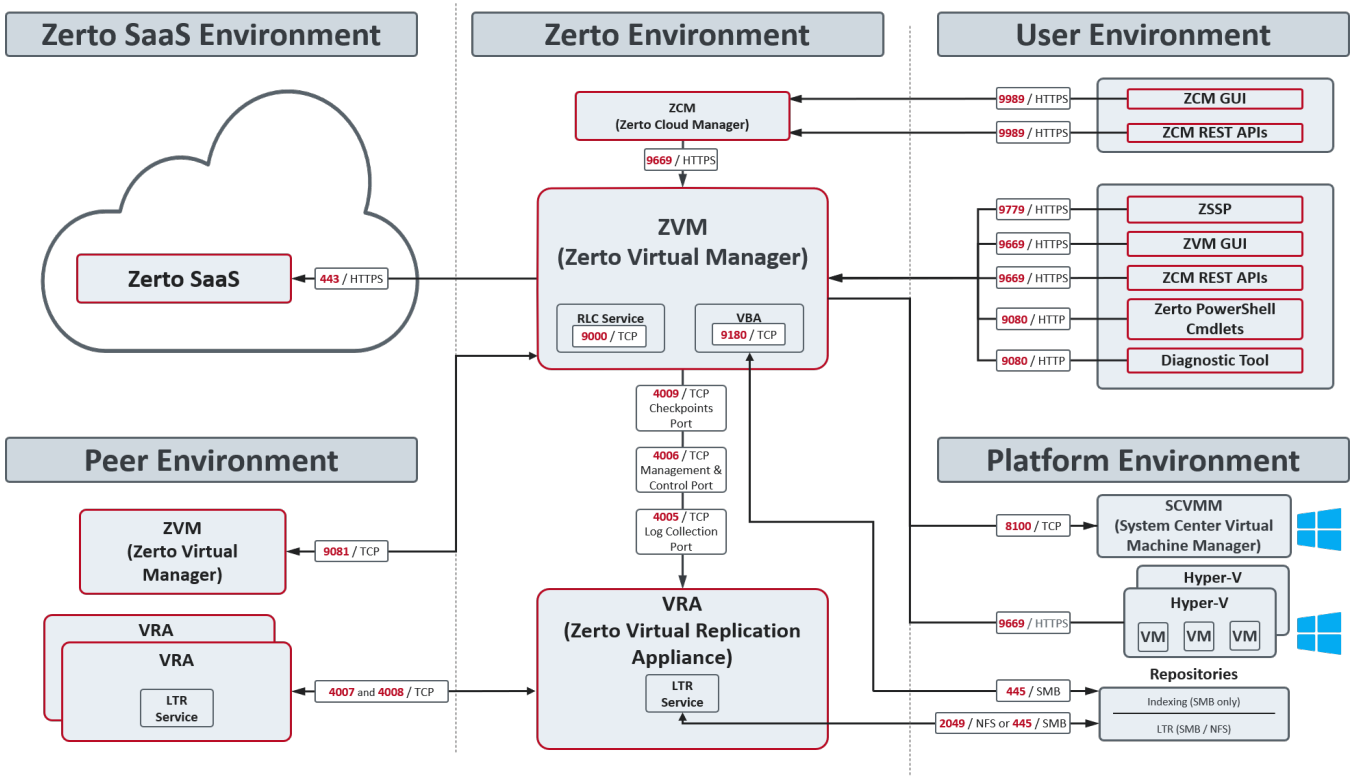
vSphere Architecture

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



Hyper-V Architecture

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



Zerto can be installed at multiple sites and each of these sites can be paired to any of the other sites.

Zerto supports both the protected and recovery sites being managed by a single vCenter Server or System Center Virtual Machine Manager. For example, in the following scenario:

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

It is recommended to install Zerto in the main office site where protected machines will be recovered.

The following table provides basic information about the ports shown in the above diagram by Zerto.

Consider firewall rules if the services are **not** installed on the same network.

The following table provides basic information about the ports shown in the above diagram by Zerto.

> **Note:** UDP ports in the 444xx range for DHCP are not required, and can therefore be blocked.

Port	Purpose
22	*(vSphere only)* Required between an ESXi host and the ZVM during installation of a VRA.
443	*(vSphere only)* Required between the ZVM and the vCenter Server.
443	*(vSphere only)* Required between an ESXi host and the ZVM during installation of a VRA.
445	Required between LTR service and a network shared repository on top of SMB protocol.
2049	Required between LTR service and a network shared repository on top of NFS protocol.
8100	*(Hyper-V only)* Communication between the ZVM and the SCVMM (System Center Virtual Machine Manager).
4005	Log collection between the ZVM and site VRAs.
4006	Communication between the ZVM and local site VRAs and the site VBA.
4007	Control communication between protecting and peer VRAs.
4008	Communication between VRAs to pass data from protected virtual machines to a VRA on a recovery site.
4009	Communication between the ZVM and local site VRAs to handle checkpoints.
5672	*(vSphere only)* TCP communication between the ZVM and vCloud Director for access to AMQP messaging.

Port	Purpose
9779	Communication between ZVM and ZSSP (Zerto Self Service Portal).
9989	Communication between ZCM, and ZCM GUI and ZCM REST APIs.
9080*	Communication between the ZVM, Zerto Powershell Cmdlets, and Zerto Diagnostic tool.
9081*	Communication between paired ZVMs** **Note:** • When a single vCenter Server or SCVMM is used for both protection and recovery, only one ZVM is installed and port 9081 is not used. • Recovery to a different vCenter Server or SCVMM uses port 9081 between the ZVMs in each site.
9180*	Communication between the ZVM and the VBA.
9669*	Communication between ZVM and ZVM GUI and ZVM REST APIs, and the ZCM. *(Hyper-V only)* 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.

See also:

- Zerto Interoperability Matrix on page 11
- Requirements - before installing Zerto software on page 11
- Considerations on page 11
- The Zerto User Interface in a vSphere Client on page 12
- Database Requirements on page 12
- vSphere Privileges Required by Zerto Virtual Replication on page 12
- (Hyper-V Only) Privileges Required by Zerto Virtual Replication on page 17
- Installing Zerto Virtual Replication in On-Premise Environments on page 17
- Performing a Silent Installation on page 28
- Installing Zerto Cmdlets on page 32
- Repairing the Current Installation on page 33
- Uninstalling Zerto Virtual Replication on page 33
- Upgrading Zerto Virtual Replication on page 34

Zerto Interoperability Matrix

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

Requirements - before installing Zerto software

Before installing Zerto software, we recommend you follow the guidelines in the document Security and Hardening with Zerto.

For VMware vSphere: See Zerto Virtual Replication Requirements for vSphere Environments.

> **Note:** *(vSphere only)* 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.

For Hyper-V: See Zerto Virtual Replication Requirements for Microsoft Hyper-V Environments.

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.
- *(vSphere only)* With VMware vSphere High Availability (HA) enabled.
- *(vSphere only)* With the VM **Restart Policy** set to **High**.
- *(Hyper-V only)* With the **Virtual machine priority** set to **High**.

Considerations

Review the following considerations:

- The following **restrictions** apply to **recovering individual files and folders**, and not to recovering the whole virtual machine:
  - The operating system of the machine on which the recovery site Zerto Virtual Manager is installed determines the types of file systems from which individual files and folders can be recovered.
  - When the recovery site Zerto Virtual Manager virtual machine operating system supports a file system, files and folders can be recovered from this file system in virtual machines that this Zerto Virtual Manager will manage the recovery of.

    For example, if a protected virtual machine running Windows 2012 has files using the ReFS file system and requires one or more of these files to be recovered and the recovery site Zerto Virtual Manager is on a machine with Windows 2008, which does not support ReFS, the protected virtual machine files and folders cannot be recovered, **but the whole virtual machine can be recovered**.

- You **cannot take snapshots** of the Zerto Virtual Manager **while the Zerto Virtual Manager service is running**. Doing so can cause operational problems for the Zerto Virtual Manager, such as inconsistencies between the Zerto Virtual Manager on the protected site and on the peer site.

The Zerto User Interface in a vSphere Client

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

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 Database to Microsoft SQL Server.
- Zerto Scale and Benchmarking Guidelines.

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 database and set both **db_owner** and **public** for database role membership.

vSphere Privileges Required by Zerto Virtual Replication

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

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

Category	Privilege	Description
ALARM		
	Create alarm	When Zerto is installed in vSphere environments, all Zerto alerts are propagated as Alarms in vCenter. As such, upon installation, the alarms matching the alerts are created. Zerto controls enabling and disabling the alarms. See the correlation between alerts and alarms in Zerto - Guide to Alarms, Alerts and Events.
	Remove alarm	When Zerto is uninstalled, the alarm definitions added above are removed.
AUTHORIZATION (from vCenter 5.5 and 6.0) Permissions		
	Modify permission	When Zerto is installed in vSphere environments, it creates seven different privileges that can be assigned to vCenter users that login to Zerto (or when viewing Zerto UI from within vSphere Client).
DATASTORE		
	Allocate space	Needed to allocate datastore space when Zerto creates or reconfigures VMs.
	Browse datastore	Needed for in-GUI datastore browser and VPG import.
	Configure datastore	Needed to create/remove directories within the Datastore.
	Remove file	Used for cleanup of volumes in a number of situations (for example, cleanup of VRAs, journals, folders, etc.).
	Low level file operations	Needed to move files managed by Zerto (for example, mirrors, journals, etc.) between folders. Specifically used in recovery operations (for example, Failover), but may be used during other procedures.
	Update virtual machine files	
DATASTORE CLUSTER		
	Configure a datastore cluster	Used when installing VRAs to enable/disable storage DRS within datastore clusters

Category	Privilege	Description
EXTENSION		
	Register extension	Needed to create the vSphere Client plugin, 'ManagedBy' extension, and other features related to Zerto's integration with vCenter.
	Unregister extension	Needed to remove the vSphere Client plugin, 'ManagedBy' extension, and other features when removing ZVR.
FOLDER		
	Create folder	Used during recovery operations to create VM folders.
GLOBAL		
	Cancel task	Used to remove tasks created by ZVR to track operations.
	Diagnostics	Used when pulling diagnostic logs from vCenter/ESXi.
	Disable methods	Used to disable methods on protected objects like VRAs and 'Testing Recovery' VMs.
	Enable methods	Used to re-enable methods disabled by Zerto.
	Log event	Used for pushing Zerto events to vSphere for tracking.
Host > Configuration		
	Advanced settings	Not used by Zerto.
	Virtual machine autostart configuration	Used when creating new VRAs/diskboxes.
	Change settings	Used during VRA deployment.
	Security profile and firewall	Used during VRA deployment.
	Query Patch	Used during VRA deployment.

Category	Privilege	Description
HOST > INVENTORY		
	Modify cluster	Used for settings affinity rules for VRAs, and disabling DRS/HA for recovery VMs before commit.
NETWORK		
	Assign network	Used for assigning VMs to various networks.
RESOURCE		
	Assign vApp to resource pool	Used for moving recovery vApps into the correct resource pools.
	Assign virtual machine to resource pool	Used for moving recovery VMs into the correct resource pool.
	Migrate a powered off virtual machine	Used for migrating VRAs back to the correct host if they've been moved off. Also for migrating recovery VMs back to the correct host when they are migrated by vCD when adding VMs into vCD vApp.
	Migrate a powered on virtual machine	Used for migrating VRAs back to the correct host if they've been moved off. Also for migrating recovery VMs back to the correct host when they are migrated by vCD when adding VMs into vCD vApp.
SESSIONS		
	Validate session	Used for validating the current session between ZVM and vCenter.
TASKS		
	Create task	Used for creating tracking tasks within vCenter.
	Update task	Used for updating tracking tasks created by Zerto.
vApp		
	vApp application configuration	Used for configuring recovery vApps created by ZVR.
	Assign resource pool	Used for moving recovery vApps into the correct resource pool.

Category	Privilege	Description
	Add virtual machine	Used for moving recovery VMs into the correct vApp.
	Create	Used for creating recovery vApps.
	Delete	Used for deleting recovery vApps (for example, when stopping FOT).
	Import	Used during VRA OVF deployment.
	Power off	Used for powering off recovery vApps (for example, when stopping FOT).
	Power on	Used for powering on recovery vApps.
VIRTUAL MACHINE > CONFIGURATION		
	Add existing disk	Used to attach disks to VRAs/recovery VMs.
	Add new disk	Used to create new journal/mirror disks on VRAs.
	Add or remove device	Used for adding various devices (NIC, SCSI adapter, etc.) to recovery VMs.
	Advanced	Used to set ExtraConfig on Zerto appliances (ZCC/VRA/Diskbox).
	Change CPU count	Used to set number of CPUs on VRA deployment.
	Extend virtual disk	Used to resize mirror disks when disk resize occurs on protected site.
	Modify device settings	Used to change settings of existing devices, such as NICs or SCSI adapters, on VRAs.
	Configure managedBy	Used for setting the 'ManagedBy' property on VMs, such as the Zerto appliances and 'Testing Recovery' VMs.
	Memory	Used to configure memory for VRA VMs.
	Raw device	Used to assign RDM LUNs to VRAs and recovery VMs.
	Remove disk	Used to detach disks from VMs during recovery operations/rollbacks.
	Change resource	Used for configuring the resource allocation of a VM within a Resource Pool - specifically when creating a recovery vApp.

Category	Privilege	Description
	Settings	Used to change VM settings not covered by other permissions.
	Swapfile placement	Used to set swapfile placement on recovery VMs where the protected VM has a custom setting.
	Upgrade virtual machine compatibility	Used to upgrade VRA VM hardware version when upgrading VRA version.
VIRTUAL MACHINE > INTERACTION		
	Power off	Used for powering off VMs, such as when stopping/rolling back a Failover, or when shutting down protected VMs during a Failover/Move.
	Power on	Used for powering on VMs during recovery operations.
VIRTUAL MACHINE > INVENTORY		
	Create from existing	Used to deploy Zerto appliances.
	Create new	Used to create recovery VMs.
	Register	Used to move VMs into VM folders during recovery operations.
	Remove	Used to remove existing VMs (uninstall Zerto appliance, remove recovery VMs when stopping FOT, rolling back FOL, or on protected site when committing FOL or Move with reverse protection).
	Unregister	Used to remove VMs from inventory. Only used as part of Undo events, after failed task.

(Hyper-V Only) Privileges Required by Zerto Virtual Replication

Zerto utilizes the default SCVMM user, **SCVMM admin**.

Installing Zerto Virtual Replication in On-Premise Environments

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

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

> **Note:** In some cases, when both these sites are managed by a single vCenter Server or 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 the vCenter Server or SCVMM is also in the site 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 using the defaults provided by Zerto, or perform a custom install, whereby you can determine the ports that will be used by Zerto.

Before proceeding with installing Zerto, make sure you reviewed the Requirements - before installing Zerto software on page 11.

- Performing an Express Installation on page 18
- Performing a Custom Installation on page 20

Performing an Express Installation

You can install Zerto using the defaults provided by Zerto.

(vSphere only) Site information and information to connect to VMware vCloud Director can be provided, if required, after the installation in the Zerto User Interface.

> **Note:** You cannot install Zerto on the same machine where another version of Zerto has been installed, for example, if Zerto for VMware vCenter Server or vCloud Director version was installed on the machine and vice versa.

Before you Begin:

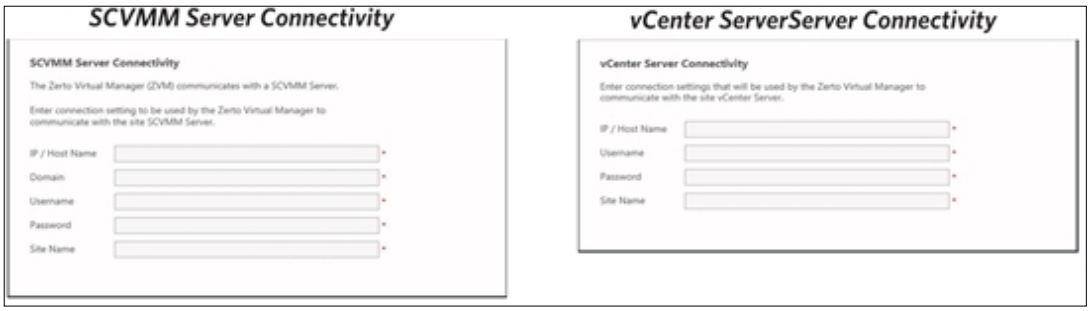
- Make sure you reviewed Database Requirements on page 12.

To perform an express install of Zerto:

1. Run the Zerto Installer for VMware, EGE, or 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 installation package.

     After .NET is installed, the machine **automatically restarts** and the Zerto 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 vCenter or SCVMM Server Connectivity window appears.



4. Specify the following:
   - **IP/Host Name:** The IP address or host name of the machine where the vCenter Server or System Center Virtual Machine Manager runs.
   - *(Hyper-V only)* **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 vCenter Server or System Center Virtual Machine Manager. The name can be entered using either of the following formats:
     - **username**
     - *(vSphere only)* **domain/username**
   - **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.
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 or SCVMM connected to the Zerto Virtual Manager. In this user interface you set up Zerto, as described in Initial Configuration on page 71.

You must **exclude** the following folders from **antivirus scanning:**

Zerto Virtual Replication

%ProgramData%\Zerto\Data\zvm_db.mdf

C:\Program Files\Zerto\Zerto Virtual Replication\Zerto.Zvm.Service.exe

C:\Program Files\Zerto\Zerto Virtual Replication\Zerto.Vba.VbaService.exe

C:\Program Files\Zerto\Zerto Virtual Replication\Zerto Online Services Connector\Zerto.Online.Services.Connector.exe

C:\Program Files\Zerto\Zerto Virtual Replication\Embedded DB Manager Service\Zerto.LocalDbInstanceManagerService.exe

Failure to do so may lead to the Zerto Virtual Replication folder being incorrectly identified as a threat and in some circumstances corrupt the Zerto Virtual Replication folder.

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

Performing a Custom Installation

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

(vSphere only) In addition, when performing a custom install, you can provide information to connect to VMware vCloud Director,

Before you Begin:

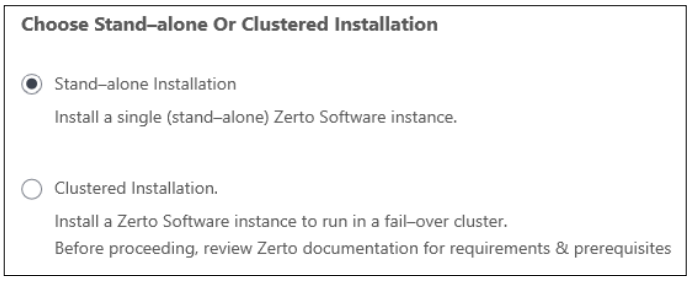
- Make sure you reviewed Database Requirements on page 12.

To perform a custom install of Zerto:

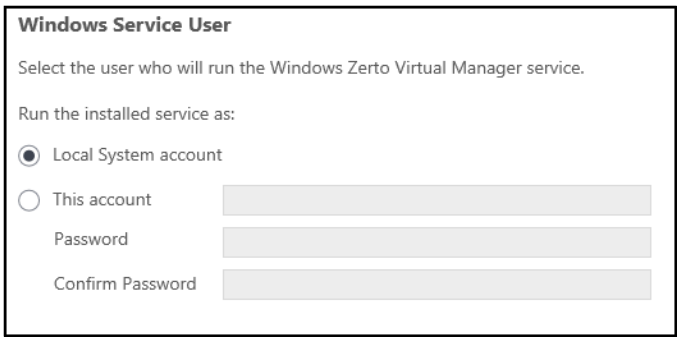
1. Run the Zerto Installer for VMware, EGE, or Hyper-V.
   - If the required version of **Microsoft .NET Framework** is not installed, you are prompted to install the required version of .NET Framework, which is **included** as part of the Zerto installation package.

   After .NET is installed, the machine **automatically restarts** and the Zerto installation begins.
2. Follow the wizard until the Installation Type window appears, then select the option, **Custom Installation**.
3. Click **Next**.

   The Choose Stand-alone Or Clustered Installation window appears.

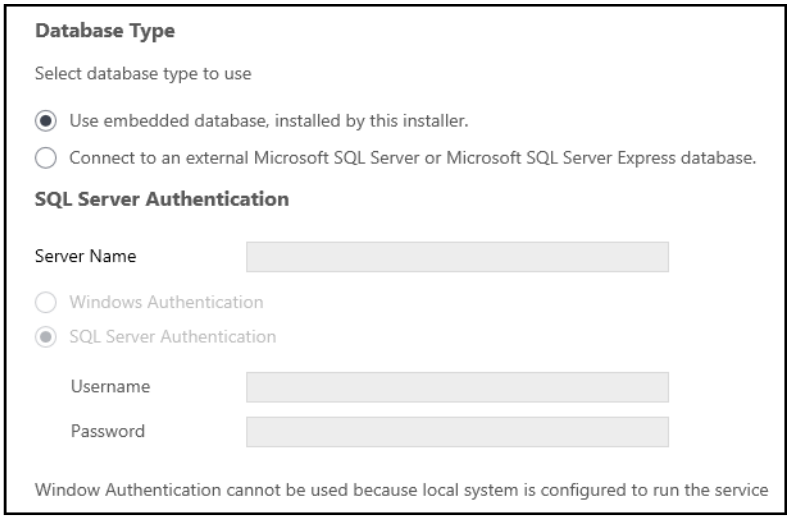


4. Select **Stand-alone Installation**, then click **Next**.
5. Click **NEXT**. The Windows Service User window appears.



6. 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. 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. 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.
7. Click **NEXT**.

   The Database Type window appears.



- Information required by Zerto 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**, for example, Microsoft SQL Server.

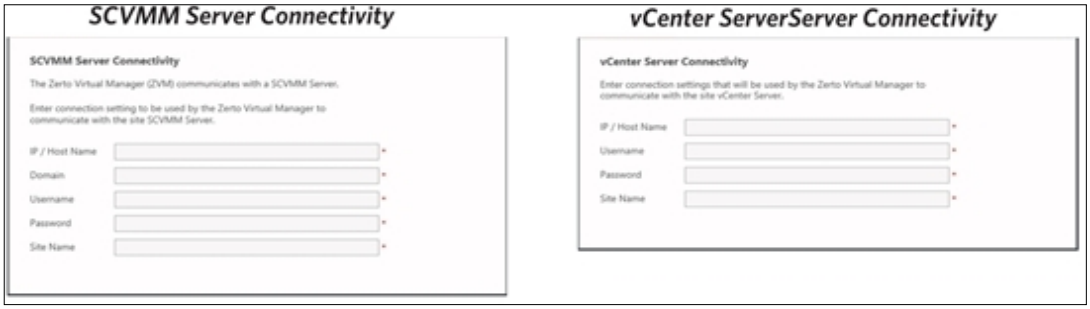
- Protection and recovery can only be performed when the **database is running**.
- If you use an **external database** and it is down for any reason, **protection stops**.

8. To use the **embedded database**, leave the **default** which is installed with this installation, then continue with step 11 on page 22.
9. To use an **external database**, select the option, **Connect to an external Microsoft SQL Server or Microsoft SQL Server Express database**.
10. 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 5 on page 20. 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.

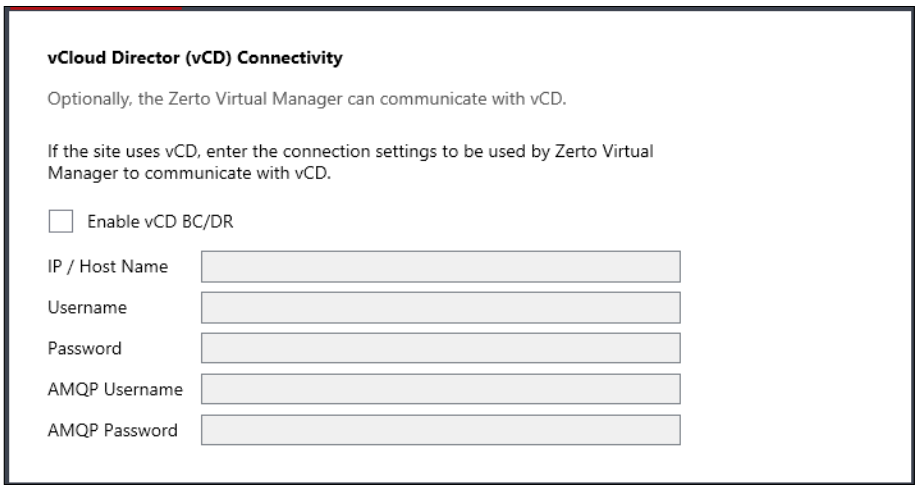
       You can only continue when the authentication is successful.
11. Click **NEXT**. The vCenter or SCVMM Server Connectivity window appears.



12. Enter connection settings that the **Zerto Virtual Manager** uses to communicate with the **vCenter** or **SCVMM Server**:
    - **IP/Host name:** The IP address or host name of the machine where the SCVMM runs.

- *(Hyper-V only)* **Domain:** The domain for a user with administrator level privileges to the vCenter Server or SCVMM.
- **Username:** The user name for a user with administrator level privileges to the vCenter Server or SCVMM. The name can be entered using either of the following formats:
  - **username**
  - *(vSphere only)* **domain/username**
- **Password:** A valid password for the given user name.

13. Click **NEXT**.
    - For further steps on vCloud Direct (vCD) Connectivity, continue to step 14 on page 23.
    - Otherwise, go to step 16 on page 24.
14. The vCloud Director Connectivity window is displayed.



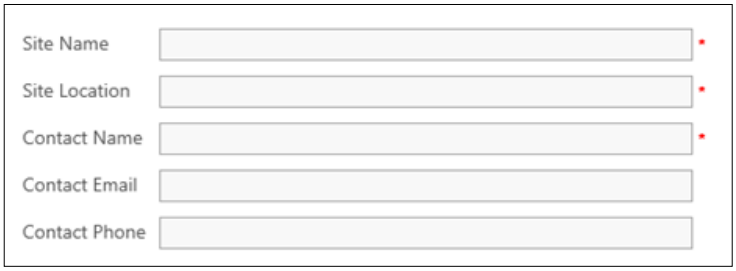
15. When using vCloud Director and you have installed an AMQP server, click the **Enable vCD BC/DR** checkbox and enter the VMware vCloud Director access details:
    - **IP / Host name:** The IP address or host name of the machine where vCD runs. When connecting to vCD with multiple cells, enter the virtual IP for the network load balancing used by the cells.
    - **Username:** The user name for an administrator to vCD.
    - **Password:** A valid password for the given user name.
    - **AMQP Username:** 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.

> ☑ **Tip:** 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, and enter the following credentials:
> - **Username:** 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.

- Click **NEXT**.

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

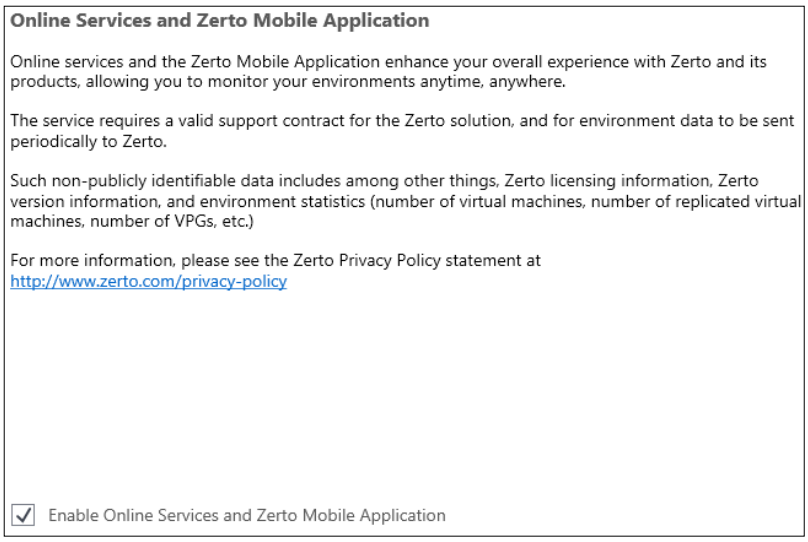


17. Enter the site details:

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

18. Click **NEXT**.

The Online Services and Zerto Mobile Application window appears.



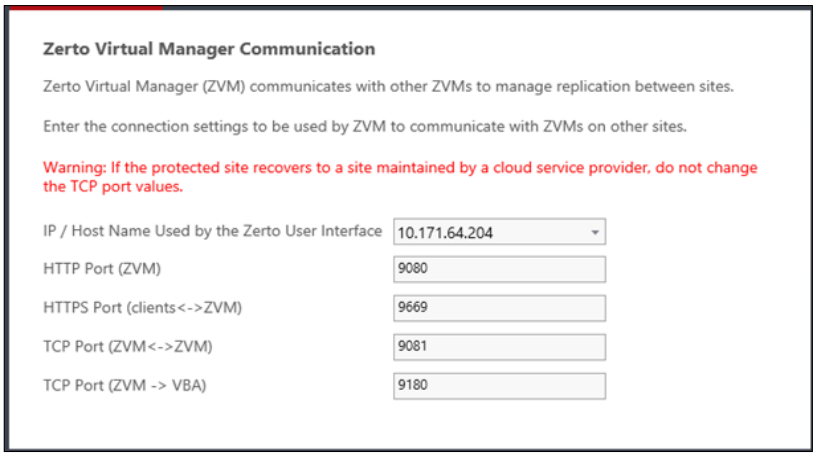
The Online Services and Zerto Mobile Application are **enabled by default**.

- You can **disable** these services by deselecting **Enable Online Services and Zerto Mobile Application**.

19. 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.



PORT DESCRIPTION PARAMETER	DEFAULT PORT NUMBER	COMMUNICATION DIRECTION	BETWEEN...	COMMENTS
IP/Host Name Used by the Zerto User Interface	NA		Zerto User Interface *- and -* Zerto Virtual Manager	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)	9080	Inbound	Zerto Virtual Manager *- and -* Zerto internal APIs, and Cmdlets	
HTTP Port (clients<->ZVM)	9669	Inbound	Zerto User Interface *- and -* Zerto Virtual Manager	

PORT DESCRIPTION PARAMETER	DEFAULT PORT NUMBER	COMMUNICATION DIRECTION	BETWEEN...	COMMENTS
TCP Port (ZVM<->ZVM)	9081	Inbound and outbound	Zerto Virtual Manager *- and -* Zerto Virtual Manager	• When **both** the protected **and** recovery sites **belong to the same enterprise**: • If you change this value, when pairing sites, use the TCP port value specified here. Pairing the sites is described in Pairing Sites on page 79. • When an enterprise **uses a cloud service provider** to **supply** disaster recovery services: • Do not change this value
TCP Port (ZVM->VBA)	9180	Inbound and outbound	Zerto Virtual Manager *- and -* Virtual Backup Appliance (VBA)	

20. Click **NEXT**.

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

21. 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 or SCVMM connected to the Zerto Virtual Manager. In this user interface you set up Zerto, as described in Initial Configuration on page 71.

    exclude the following folders from **antivirus scanning:**

    Zerto Virtual Replication

    %ProgramData%\Zerto\Data\zvm_db.mdf

    C:\Program Files\Zerto\Zerto Virtual Replication\Zerto.Zvm.Service.exe

    C:\Program Files\Zerto\Zerto Virtual Replication\Zerto.Vba.VbaService.exe

    C:\Program Files\Zerto\Zerto Virtual Replication\Zerto Online Services Connector\Zerto.Online.Services.Connector.exe

    C:\Program Files\Zerto\Zerto Virtual Replication\Embedded DB Manager Service\Zerto.LocalDbInstanceManagerService.exe

    Failure to do so may lead to the Zerto Virtual Replication folder being incorrectly identified as a threat and in some circumstances corrupt the Zerto Virtual Replication folder.

22. 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.

23. Install Zerto 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 creates folders, such as C:\ZertoAgent, which **must not be removed**.

> **Note:** If the vSphere Client console was open during the installation, close it and reopen it to ensure you have the Zerto Virtual Manager user interface loaded.

Performing a Silent Installation

You can perform a silent installation of Zerto, 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 silent installation, uninstall, repair or upgrade.

  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.
- **PROPERY=VALUE** Sets the property PROPERTY to VALUE. The PROPERTY can be any in the table below.

Note:

(On-premise environments) VRA upgrade is **enabled** by default during the upgrade (`-ShouldUpgradeVra=True`).

To **disable** the VRA upgrade when running the silent installation, enter the following example command:

```
<installation>.exe [-s] [-upgrade] [-l bundle.log -ShouldUpgradeVra=False]
```

Property	Description	Mandatory
VCenterHostName	*(vSphere only)* The host name of the machine on which Zerto Virtual Replication is installed.	Yes
VCenterPassword	*(vSphere only)* A valid password for the given user name.	Yes
VCenterUserName	*(vSphere only)* The user name for an administrator to vCD.	Yes
AmqpPassword	*(vSphere only)* The password to access AMQP.	No
AmqpUserName	*(vSphere only)* The username to access AMQP.	No
IsVcdEnabled	True = Yes or False = No For vCD VcdHost (vSphere only) 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.	For vCD

Property	Description	Mandatory
VcdHost	*(vSphere only)* 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.	For vCD
VcdPassword	*(vSphere only)* The password to access vCloud Director.	
VcdUserName	*(vSphere only)* The username to access vCloud Director.	
ScvmmDomain	*(Hyper-V only)* The domain name for an administrator.	Yes
ScvmmHost	*(Hyper-V only)* The host name of the machine on which Zerto Virtual Replication is installed.	Yes
ScvmmPassword	*(Hyper-V only)* A valid password for the given user name.	Yes
ScvmmUsername	*(Hyper-V only)* The user name for an administrator.	Yes
AutoRestart	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**.	No
DBType	• **Embedded database** (default) - or - • External Microsoft SQL Server Value: **DBType=sqlserver**	No
IsWindowsAuthentication	Use Windows authentication.	No
ServiceAccount	The user account to run the Zerto Virtual Manager service. Default value: **'.\LocalSystem'**	No
ServicePassword	The password to use to run the service under the specified account.	No
SiteCertificatePassword	The default is taken from Zerto.	No
SiteContactEmail	The email address to contact if a need arises.	No
SiteContactInfo	The name of the person to contact if a need arises.	No
SiteContactPhone	The phone number to contact if a need arises.	No

Property	Description	Mandatory
SiteHttpPort	The port used for inbound communication between the Zerto Virtual Manager and Zerto internal APIs, and Cmdlets. Default value: **9080**	No
SiteHttpsPort	The port used for inbound communication between the Zerto User Interface and the Zerto Virtual Manager. Default value: **9669**	No
SiteIpAddress	The IP address, or host name of the machine where SCVMM runs.	No
SiteKeepPreviousIdentifier	Default value: **true**	No
SiteLocation	Information to identify the site location.	No
SiteName	A name to identify the site. This name is displayed in the Zerto User Interface.	No
SiteTcpPort	The port used for communication between Zerto Virtual Managers. Default value: **9081**	No
SiteTcpPortVba	The port used for communication between the Zerto Virtual Manager and the Virtual Backup Appliance. Default value: **9180**	No
SqlPassword	A valid password for the given user name.	No
SqlServerName	The domain name and server instance to connect to, with the format: **domain\instance**	No
SqlUserName	The user name for the SQL Server database.	No

The following is an example command line to run a silent installation for vSphere:

```
"Zerto Virtual Replication VMware Installer.exe" -s
VCenterHostName=199.10.10.20 VCenterUserName=Administrator
VCenterPassword=mypassword
```

The following is an example command line to run a silent installation for Hyper-V:

```
"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 Zerto 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 4.7.2 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:

1. 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.

2. 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:

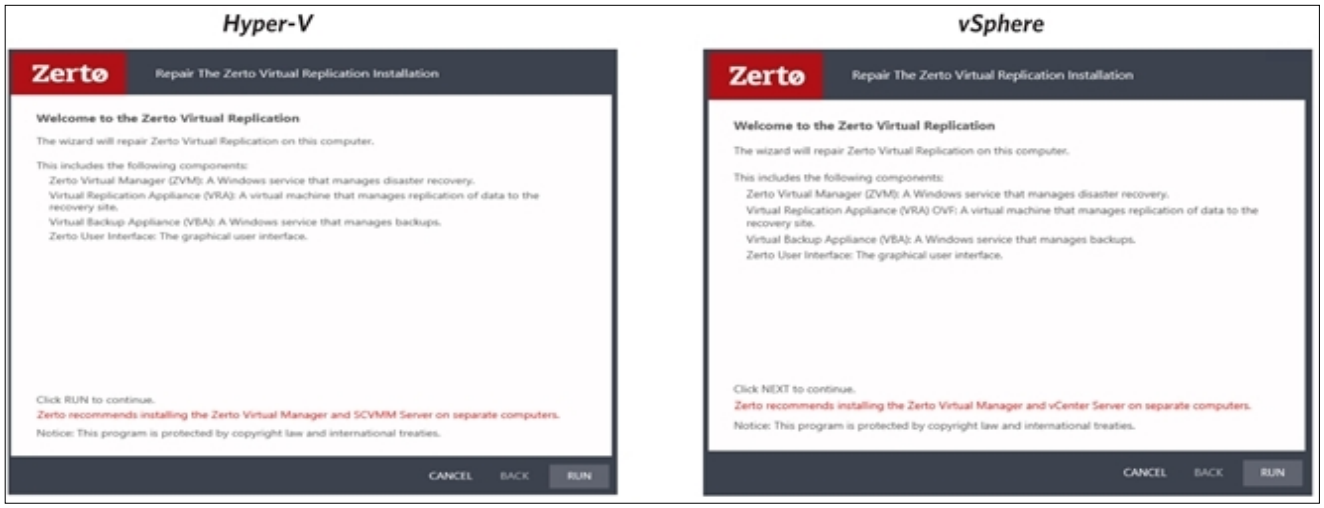
   ```
   C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -NoExit
   -Command Add-PSSnapIn Zerto.PS.Commands
   ```

   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*.

Repairing the Current Installation

If a new installation is the same version as the installed version, the Repair the Zerto Installation dialog is displayed.



When repairing 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 section Upgrading To More Than One Version Higher, in the guide Upgrading the Zerto Virtual Replication Environment to save the settings.

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

Uninstalling Zerto Virtual Replication

You uninstall Zerto via the Uninstall a program in the Windows Control Panel.

When you uninstall Zerto 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 silently, by running the silent installation with the **-uninstall** switch, as described in Performing a Silent Installation on page 28.

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. The upgrade document describes different options for different upgrade scenarios.

For details, see Upgrading the Zerto Virtual Replication Environment.

Deploying Zerto Enterprise Government Edition

To deploy Zerto Enterprise Government Edition (EGE), use the following workflow:

1.	Review the prerequisites.	Prerequisites and considerations before deploying Zerto Enterprise Government Edition on page 35
2.	Review any limitations.	Limitations when using Zerto Enterprise Government Edition on page 36
3.	Install the Zerto solution. This installs Zerto Virtual Replication (ZVR) on virtual machines to be protected and recovered.	Installing the Zerto Solution on page 5
4.	Access the Zerto User Interface.	Accessing the Zerto User Interface on page 65
5.	Register the Zerto Virtual Replication License.	Registering the Zerto Virtual Replication License on page 71
6.	Install Virtual Replication Appliances.	Installing a VRA in Zerto Enterprise Government Edition on page 36
7.	Pair the sites.	Pairing Sites on page 79
8.	Set up a remote site.	Setting Up a Remote Site on page 82

Prerequisites and considerations before deploying Zerto Enterprise Government Edition

- VMware vSphere 6.5Ux
- ESXi 6.5Ux
- Each protected VM requires 400 MB of RAM from its ESXi
- Cluster DRS settings are required to enable the clustered hosts to enter Maintenance Mode
- Zerto Virtual Manager must be configured with a static IP and cannot change its IP
- An ESXi agent manager must be installed
- Zerto only supports minor upgrades within the ESXi 6.5 version.

  To upgrade an ESXi to a version higher than 6.5x, you must first uninstall Zerto.

Limitations when using Zerto Enterprise Government Edition

- Only vSphere and ESXi 6.5Ux is supported. Every ESXi within the same cluster must be of the same 6.5 version
- Recovering to public cloud / HyperV is not supported.
- Protecting a VM with snapshots is not supported. Instead, consolidate snapshots before protecting the VM in a VPG.
- RDM is not supported.
- Move operation is not supported for VPGs which are replicating from a Zerto Enterprise Government Edition site.
- Remove the Zerto Storage Policy via vCenter “VM storage policies section if you clone a VM”.
- Zerto Storage Policy is compatible with all datastores, though it appears that there are compatibility issues.
- When a protected VM is added back into the inventory, it must be manually configured with a Zerto Storage Policy.

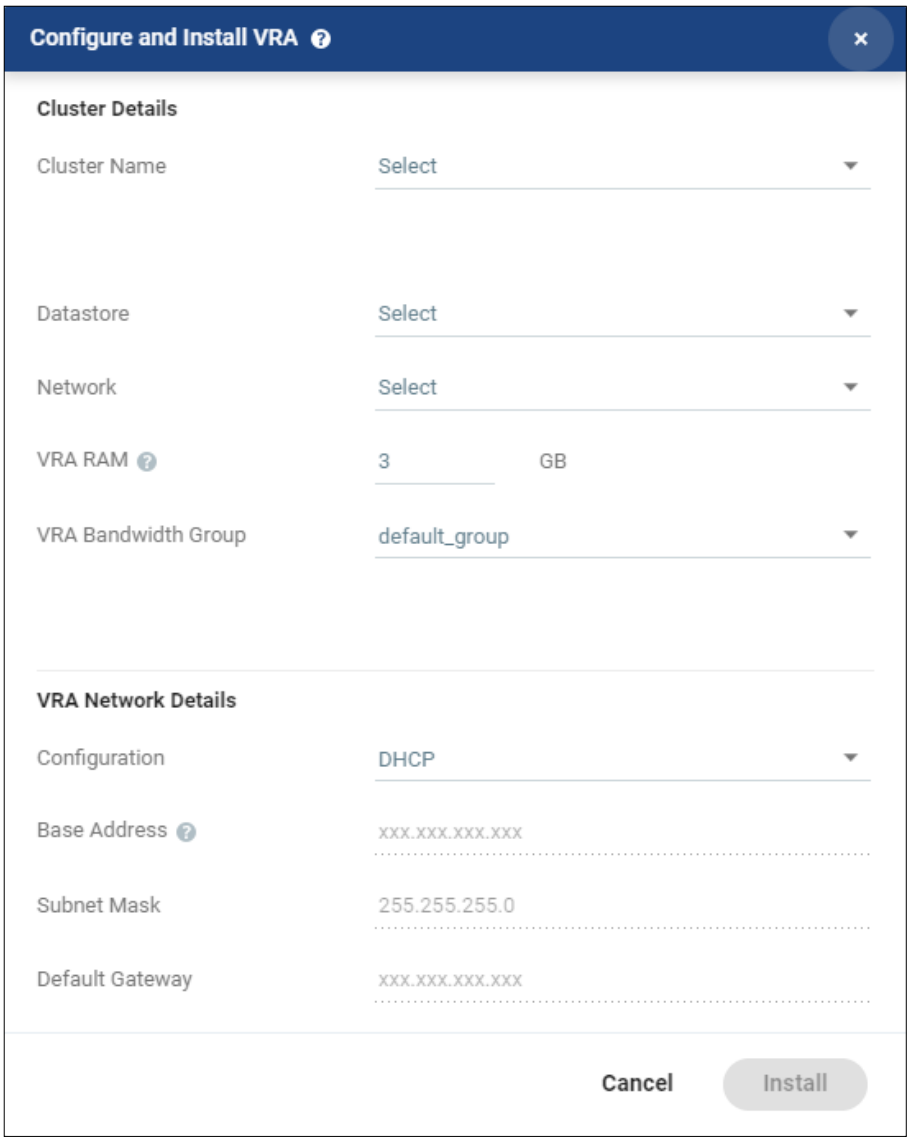
  To add Zerto Storage Policy through vCenter, navigate to Policies and Profiles > VM Storage Policies > Create VM Storage Policy, and make sure to add Zerto’s replication component as a host based rule.
- VVOLs is not supported.

Installing a VRA in Zerto Enterprise Government Edition

Use the following procedure to install Virtual Replication Appliances on every ESXi within the cluster, for each cluster.

To install a Virtual Replication Appliance (VRA) with Zerto Enterprise Government Edition (EGE):

1. In the Zerto User Interface, navigate to **Setup**. The **VRAS** tab appears by default.
2. Click **NEW VRA**. The **Configure and Install VRA** window appears.



3. In the **Cluster Details** area, specify the following:

   - **Cluster Name**: The cluster under which the VRA is installed. The drop-down displays the clusters which **do not have VRAs installed**.
   - **Datastore**: The datastore that contains the OS disks of the VRA VMs. You can install more than one VRA on the same datastore. The drop-down displays the shared datastores.
   - **Network**: The network used to access the VRA. The drop-down displays the shared networks.

     VRA RAM: The amount of memory to allocate to the VRAs.

     > **Note:** See Prerequisites and considerations before deploying Zerto Enterprise Government Edition on page 35 **for the correct amount of RAM for the number of protected VMs on the host.**

     - 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.

- **VRA Bandwidth Group:** Select the **VRA Group** from the drop-down list.
  - To create a new VRA group, enter the name of the new group and click **CREATE**. You can then choose the new group from the drop-down list.

  When VRAs use different networks, you can group the VRAs per network.

  For example: When the protected and recovery sites are on different networks and are managed by the same vCenter and you want to replicate from the recovery site to the protected site.

  Within a group the priority assigned to a VPG dictates the bandwidth used, and is applicable within a group and not between groups.

  Therefore, 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**: Best practice: from the drop-down list, select **static IP address**, then enter the following:
   - **Base Address**: The first IP address in the predefined range of consecutive IP addresses.
   - **Subnet Mask**: The subnet mask for the network. The default value is **255.255.255.0**.
   - **Default Gateway**: The default gateway for the network.

   > **Note:** Datastore, Network, VRA RAM and Bandwidth group are true to all the VRAs which will be installed.

5. Click **INSTALL**.

   The VRA installation starts and the status is displayed in the **TASKS** pop-up window in the status bar and under Monitoring> TASKS.

6. In the Setup tab, review any errors which may appear . If there are errors, run the VRA installation again and it will automatically run in repair mode.
   - 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.

7. Repeat this procedure to install a VRA on the ESXi within every cluster for which you want replication.
   - Zerto recommends installing a VRA **on every listed host**.

- 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.

Installing Zerto in Clustered vSphere Environments

What is Zerto's Failover Cluster?

When you have a Zerto system, you want your system to always be up and running, and to never go down. But, as with all systems, your Zerto system will need maintenance, (like security patches, and operating system updates) and will need to be upgraded with the latest Zerto releases.

In order to perform these maintenance procedures, Zerto has integrated with Microsoft's Failover Cluster feature and now allows their customers to install Zerto Virtual Manager in a clustered environment.

With a clustered ZVM environment running, you are able to reduce downtime when performing maintenance procedures such as:

- Operating System maintenance
- Upgrade your Zerto Virtual Manager

Clustered Concepts

TERM OR PHRASE	DEFINITION
clustered role	Clustered applications and services
node	Clustered nodes (meaning, servers) are connected by physical cables and by software. If one or more of the cluster nodes fail, other nodes begin to provide service continuously.
Active/passive node	A resources cluster where only one instance is active at any given time.
Zerto Failover Cluster Role Mover	The Zerto Failover Cluster Role Mover tool facilitates an unobtrusive move of the clustered role from one node to the other, with minimal consequences to Zerto Virtual Manager.
switch node	
Microsoft Failover Clustering	A Windows Server feature that enables you to group multiple servers together into a fault-tolerant cluster (renamed in Windows Server 2008 from Microsoft Cluster Service (MSCS))
Minimal downtime	The time it takes for the ZVR to start.

Workflow: Installing Zerto on Clustered Nodes

STEP	DESCRIPTION	LINK TO PROCEDURE
1.	Review the prerequisites; this includes what you need to prepare on your virtual machines, before you can install Zerto Virtual Manager on the clustered nodes.	Prerequisites: Before Installing Zerto Virtual Manager Clusters on page 41
2.	Create a Role for the Zerto services.	Creating a Role for the Zerto Services on page 42
3.	Install the first Zerto Virtual Manager clustered node.	First Clustered Node - Installing Zerto Virtual Replication on page 43
4.	Install the second Zerto Virtual Manager clustered node.	Second Clustered Node - Installing Zerto Virtual Replication on page 52
5.	Add Zerto services to the role, and configure the role.	Configuring the Role with Zerto Services on page 61
Additional Cluster Procedures		
	Uninstall a cluster.	Uninstalling a Zerto Cluster on page 64

Notes:

After the ZVM Cluster is installed and running, you can perform any of the following procedures:

- Manually move a cluster role from Active to Passive using the Zerto Failover Cluster Role Mover tool.
- Switch your ZVM machine from a non-clustered mode, to a clustered mode.
- Switch your clustered environment to a non-clustered environment.

For the procedures, see Zerto Virtual Manager Administration Guide for the VMware vSphere Environment, in the section **Managing a Zerto Virtual Manager Cluster**.

Prerequisites: Before Installing Zerto Virtual Manager Clusters

Before preparing for, and installing Zerto Virtual Manager Clusters, ensure the following:

- There is an **external database**.
- There is an **existing cluster**, created according to Microsoft's procedure.
- The **domain user** has the required **privileges**.

Continue to Creating a Role for the Zerto Services on page 42

Creating a Role for the Zerto Services

Before you can create a role for the ZVM services, make sure you reviewed the prerequisites, Prerequisites: Before Installing Zerto Virtual Manager Clusters on page 41. Then follow these procedures:

Procedure 1: To create and configure an empty role on page 42

Procedure 2: To add and configure a network resource to the role on page 42

Procedure 1: To create and configure an empty role

1. In the Failover Cluster Manager, create an empty role. To do this, right click the roles menu on the left pane, and select **Create Empty Role**.

   When the role is created, it is automatically in the state, **Running**.

2. Name the Role:

   a. Right-click the role, and select **Properties**.

   b. In the **General** tab, define the role **Name**.

   c. Click **Apply**.

3. Configure Failover settings.

   a. Navigate to the **Failover** tab and define the following:

Maximum restarts in the specified period	12
Period	1 hour

   b. In the **Failback** area, select **Prevent failback.**

   c. Click **Apply**, then click **OK**.

4. Stop the role. To do this, right-click the role, and select **Stop Role**.

Procedure 2: To add and configure a network resource to the role

1. Add the network resource; right-click the role, then navigate to and select **Add Resources > More Resources > IP Address**.

2. Define the network name.

   a. In the Resources tab, Other Resources area, right click the role and select **Properties**.

   b. In the **Name** field, enter a network name.

   c. Define the IP as a **static IP**.

3. Define the Network Policies. Navigate to the **Policies** tab, and configure the following:

If resource fails, attempt restart on current node	Select this option

Period for restart	15:00 (minutes)
Maximum restarts in the specified period	10
Delay between restarts	30 (seconds)
If restart is unsuccessful, fail over all resources in this Role	Select this option
If all the restart attempts fail, begin restarting again after the specified period	Deselect this option

4. Click **Apply**.
5. Proceed to First Clustered Node - Installing Zerto Virtual Replication on page 43.

First Clustered Node - Installing Zerto Virtual Replication

Use the following procedure to configure ZVR on the first clustered node.

Before you Begin:

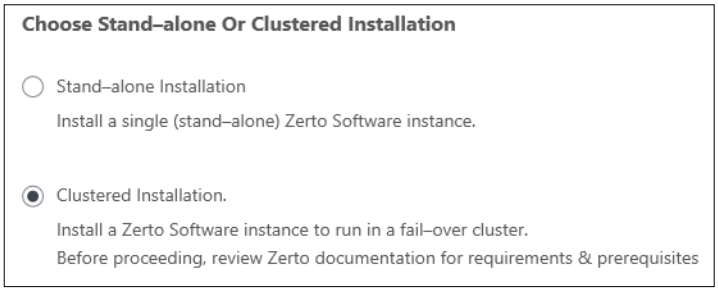
- **vCD environments only**: When you install and configure an AMQP Server for Zerto Virtual Replication, make sure you enter the **Cluster role IP** in the field **AMQP host**.

To install Zerto Virtual Manager on the first clustered node:

1. On the **first cluster node**, run the Zerto Installer.
   - If the required version of **Microsoft .NET Framework** is not installed, you are prompted to install the required version of .NET Framework, which is **included** as part of the Zerto installation package.

     After .NET is installed, the machine **automatically restarts** and the Zerto installation begins.
2. Follow the wizard until the Installation Type window appears, then select the option, **Custom Installation**.

   The Choose Stand-alone Or Clustered Installation window appears.

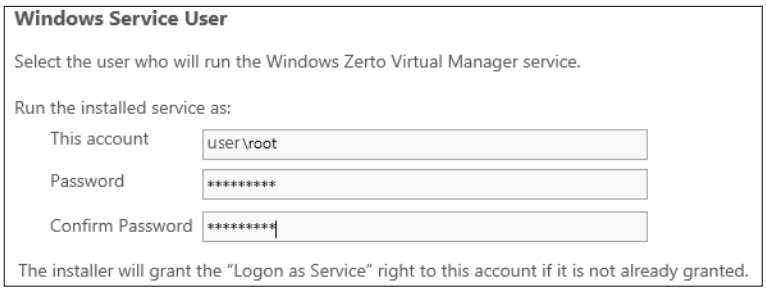


3. Select **Clustered Installation**, then click **Next**.

   The Windows Service User window appears.

   This is the account which will run the Zerto Virtual Manager Service.

> **Note:**
>
> The user who runs the Windows Zerto Virtual Manager service must be configured with permission to '**logon as a service**'.

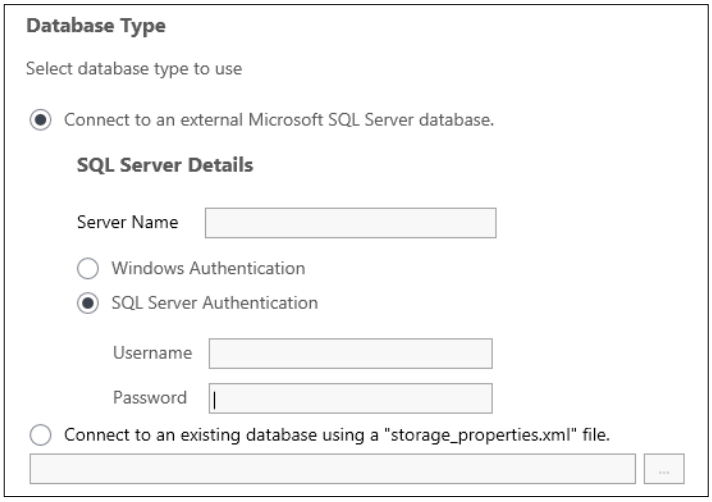


4. **Best Practice:** Enter the **domain** username and password of the user who will run the Zerto Virtual Manager Service.

> **Note:**
>
> Make sure that the domain user has the required privileges.

5. Click **NEXT**.

   The Database Type window appears.



- In the Database Type window you connect the first node to an external Microsoft SQL Server. This is the same database which will be used for the second node.
- Do **not** select Connect to an existing database - that option will be used when you install Zerto on the second node, later on.

6. Connect to the external database by selecting **Connect to an external Microsoft SQL Server or Microsoft SQL Server Express database**, then enter the SQL Server Authentication details.
   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. Specify an authentication method. Select one of the following:
      - **Windows Authentication**

        - or -

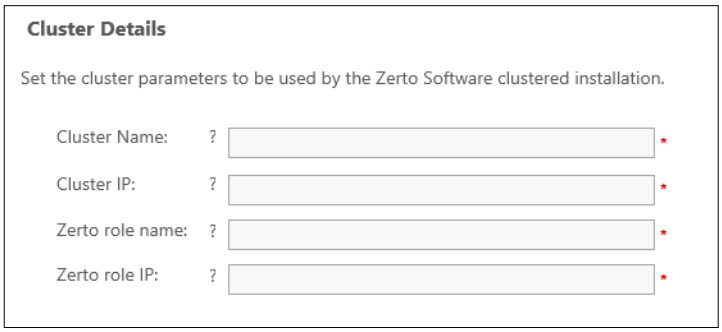
      - **SQL Server Authentication**
   c. If you selected **Windows Authentication:** This option is enabled only if a specific service user account was specified in Windows Service User, in step 4 on page 44. In this case, the service account name and password are used.
   d. If you selected **SQL Server Authentication**, the Test Authentication button is also displayed.

      Define the following:

      - **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.
   e. Click **TEST CONNECTION**. **You can only continue when the authentication is successful.**
7. Click **NEXT**.

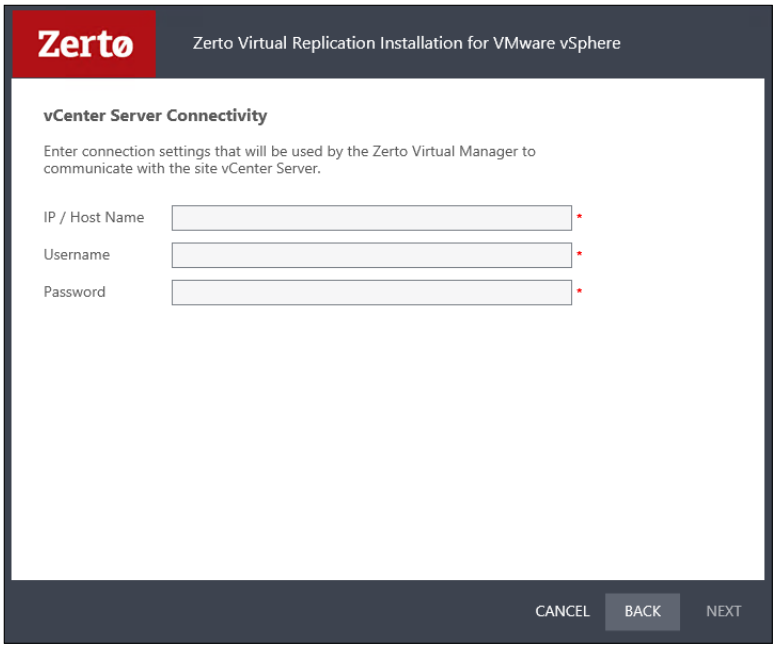
   The Cluster Details window appears.



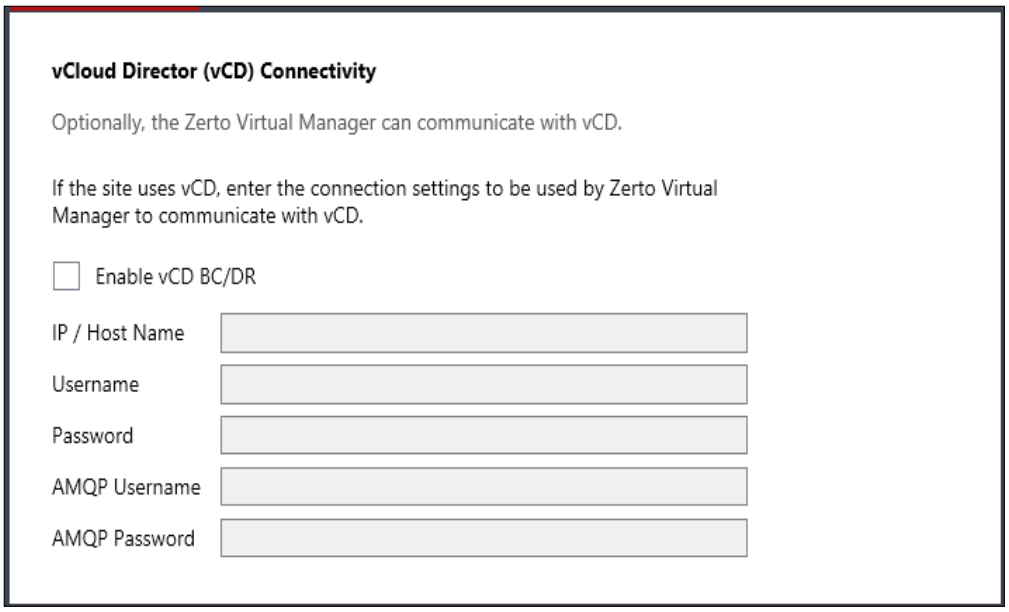
8. Enter the cluster details:

Cluster Name	The exact name of the cluster, as it was created in the Failover Cluster Manager.
Cluster IP	The IP of the cluster, as it was defined in the Failover Cluster Manager.
Zerto role name	The exact name of the role, as it appears in the Failover Cluster Manager.
Zerto role IP	The IP of the role, as it appears in the Failover Cluster Manager.

9. Click **NEXT**. The vCenter Server Connectivity window appears.



10. 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 runs.
    - **Username:** The user name for a user with administrator level privileges to 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.
11. Click **NEXT**.
    - For further steps on vCloud Direct (vCD) Connectivity, continue to The vCloud Director Connectivity window is displayed. on page 46.
    - Otherwise, go to The Zerto Virtual Manager Site Details window appears, where you define general information about the site. on page 48.
12. The vCloud Director Connectivity window is displayed.



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

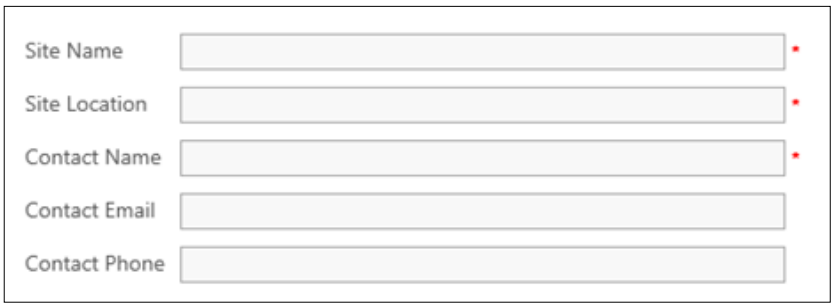
    - **IP / Host name:** The IP address or host name of the machine where vCD runs. When connecting to vCD with multiple cells, enter the virtual IP for the network load balancing used by the cells.
    - **Username:** The user name for an administrator to vCD.
    - **Password:** A valid password for the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

    > ☑ **Tip:**
    >
    > 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, and enter the following credentials:
    > - **Username:** 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**.
15. The Zerto Virtual Manager Site Details window appears, where you define general information about the site.

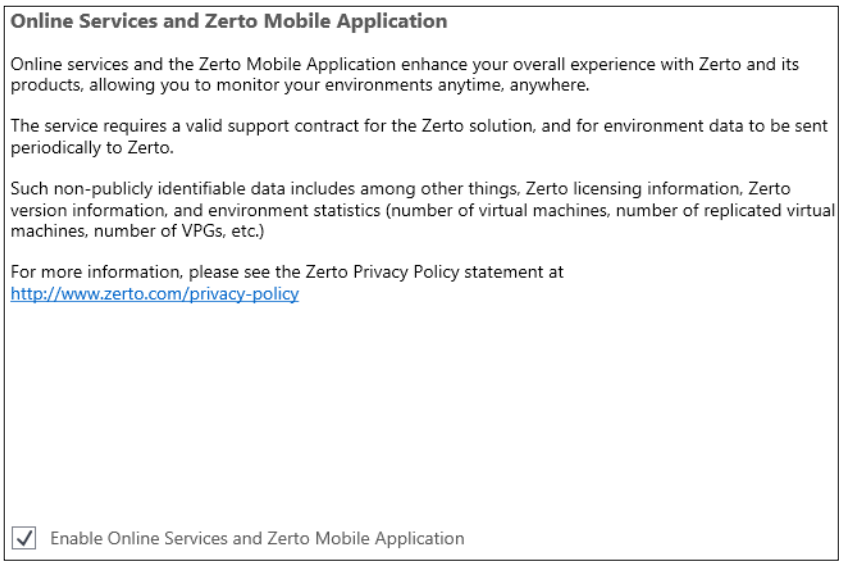


16. Enter the site details:

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

17. Click **NEXT**.

The Online Services and Zerto Mobile Application window appears.



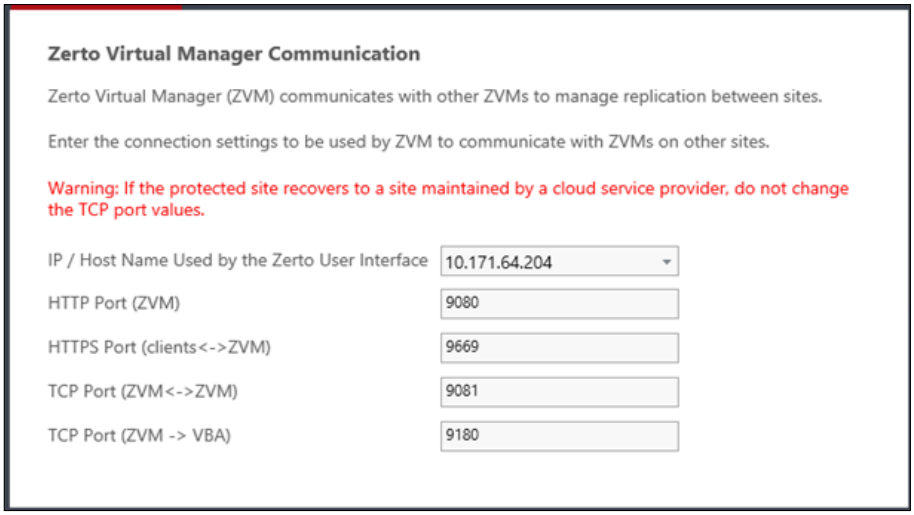
The Online Services and Zerto Mobile Application are **enabled by default**.

- You can **disable** these services by deselecting **Enable Online Services and Zerto Mobile Application**.

18. 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.



Port Description Parameter	Default Port Number	Communication Direction	Between...	Comments
IP/Host Name Used by the Zerto User Interface	NA		Zerto User Interface *- and -* Zerto Virtual Manager	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)	9080	Inbound	Zerto Virtual Manager *- and -* Zerto internal APIs, and Cmdlets	
HTTP Port (clients<->ZVM)	9669	Inbound	Zerto User Interface *- and -* Zerto Virtual Manager	

Port Description Parameter	Default Port Number	Communication Direction	Between...	Comments
TCP Port (ZVM<->ZVM)	9081	Inbound and outbound	Zerto Virtual Manager *- and -* Zerto Virtual Manager	• When **both** the protected **and** recovery sites **belong to the same enterprise**: • If you change this value, when pairing sites, use the TCP port value specified here. Pairing the sites is described in Zerto Installation Guide for Microsoft Hyper-V or VMware vSphere, in the section **Pairing Sites**. • When an enterprise **uses a cloud service provider** to **supply** disaster recovery services: • Do not change this value
TCP Port (ZVM->VBA)	9180	Inbound and outbound	Zerto Virtual Manager *- and -* Virtual Backup Appliance (VBA)	

19. Click **NEXT**.

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

20. You must **exclude** the following folders from **antivirus scanning:**

    Zerto Virtual Replication

%ProgramData%\Zerto\Data\zvm_db.mdf

C:\Program Files\Zerto\Zerto Virtual Replication\Zerto.Zvm.Service.exe

C:\Program Files\Zerto\Zerto Virtual Replication\Zerto.Vba.VbaService.exe

C:\Program Files\Zerto\Zerto Virtual Replication\Zerto Online Services Connector\Zerto.Online.Services.Connector.exe

C:\Program Files\Zerto\Zerto Virtual Replication\Embedded DB Manager Service\Zerto.LocalDbInstanceManagerService.exe

Failure to do so may lead to the Zerto Virtual Replication folder being incorrectly identified as a threat and in some circumstances corrupt the Zerto Virtual Replication folder.

21. 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.

Proceed to Second Clustered Node - Installing Zerto Virtual Replication on page 52.

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

Second Clustered Node - Installing Zerto Virtual Replication

Use the following procedure to configure ZVR on the second clustered node.

Before You Begin:

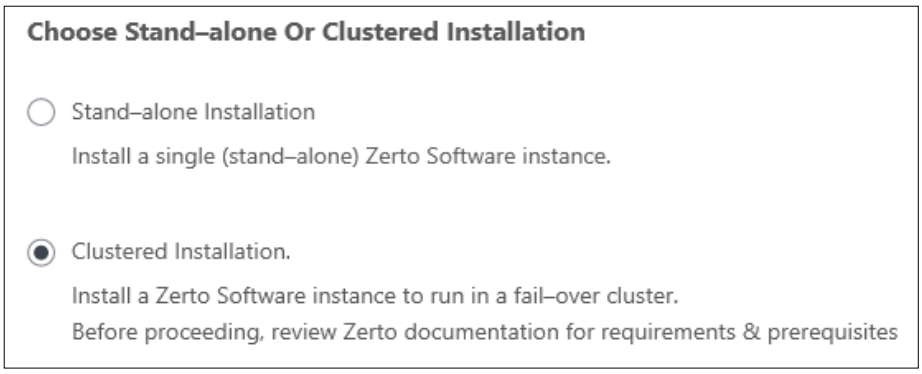
- Verify you installed and configured Zerto Virtual Manager on the first node.
- **vCD environments only**: When you install and configure an AMQP Server for Zerto Virtual Replication, make sure you enter the **Cluster role IP** in the field **AMQP host**.

To install Zerto Virtual Manager on the second clustered node:

1. Copy the **storage_properties.xml** file from the first node, to a folder in the second node.
2. On the **second cluster node**, run the Zerto Installer.
   - If the required version of **Microsoft .NET Framework** is not installed, you are prompted to install the required version of .NET Framework, which is **included** as part of the Zerto installation package.

   After .NET is installed, the machine **automatically restarts** and the Zerto installation begins.
3. Follow the wizard until the Installation Type window appears, then select the option, **Custom Installation**.

   The Choose Stand-alone Or Clustered Installation window appears.

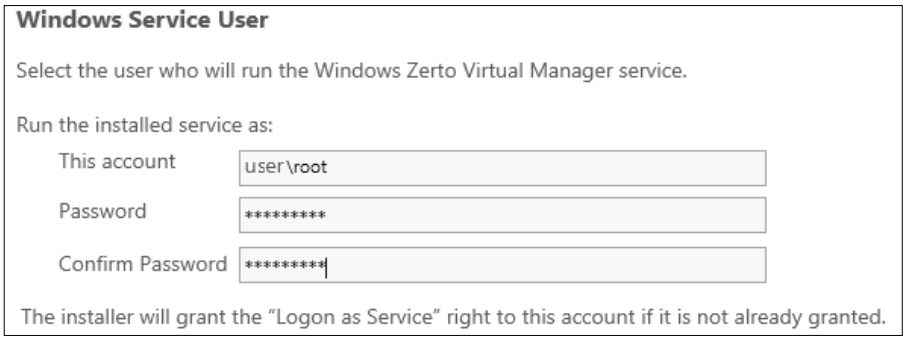


4. Select **Clustered Installation**, then click **Next**.

   The Windows Service User window appears.

   This is the account which will run the Zerto Virtual Manager Service.

   > **Note:**
   >
   > The user who runs the Windows Zerto Virtual Manager service must be configured with permission to '**logon as a service**'.

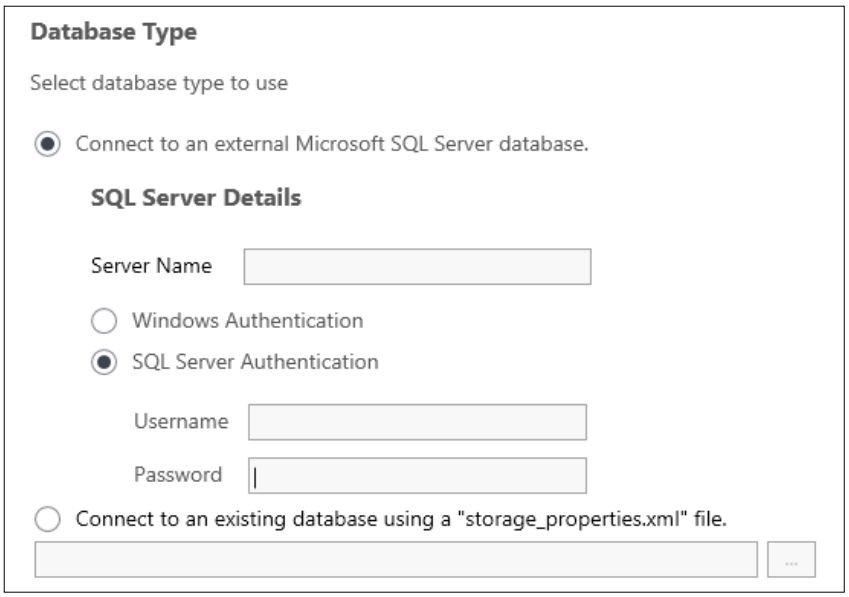


5. **Best Practice:** Enter the **domain** username and password of the user who will run the Zerto Virtual Manager Service.

   > **Note:**
   >
   > Make sure that the domain user has the required privileges.

6. Click **NEXT**.

   The Database Type window appears.

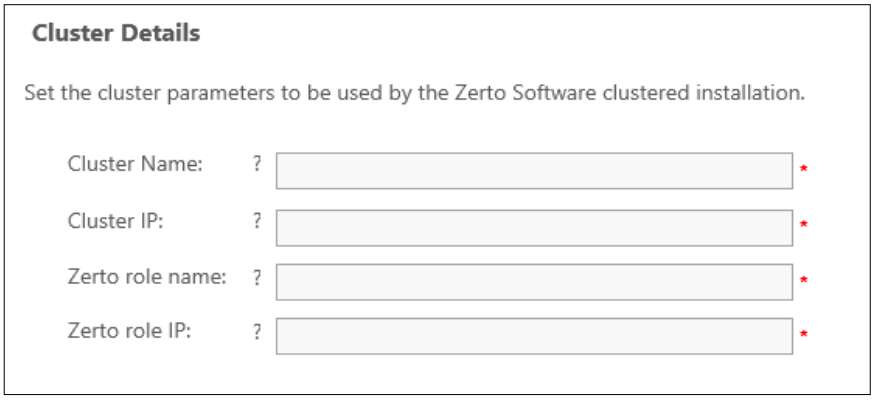


You now configure the database for the **second node**.

7. Select **Connect to an existing database using a "storage_properties.xml" file**, then browse to the **storage_properties.xml** file which you copied over to a folder in the second node in step 1 on page 52.

   This automatically connects the database from the first node to the second node.

8. Click **TEST CONNECTION**.
9. **You can only continue when the authentication is successful.**
10. Click **NEXT**. The Cluster Details window appears.

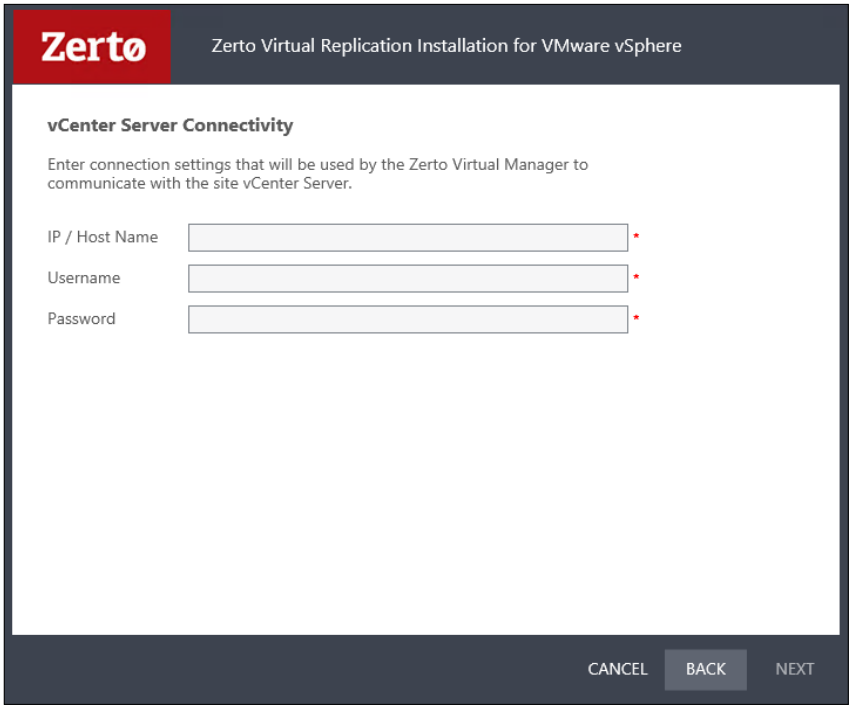


11. Enter the cluster details, **exactly as they were entered on the first node**:

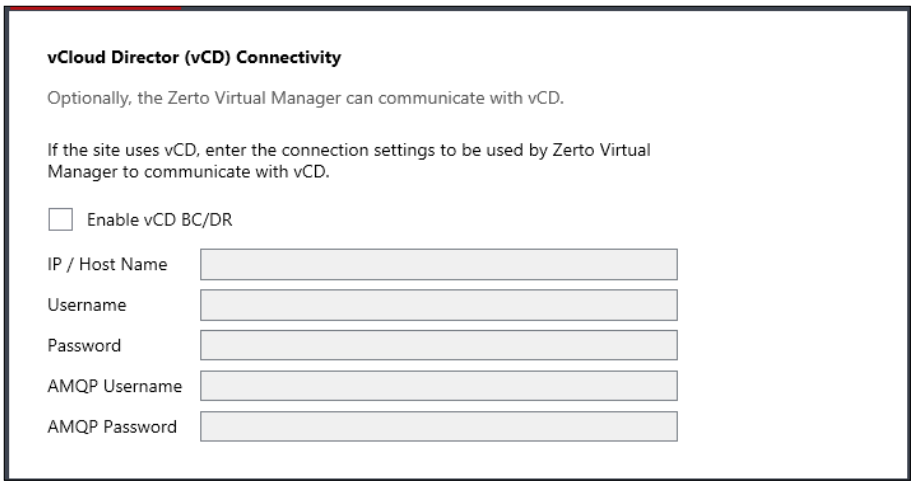
Cluster Name	The exact name of the cluster, as it was created in the Failover Cluster Manager.
Cluster IP	The IP of the cluster, as it was defined in the Failover Cluster Manager.

Zerto role name	The exact name of the role, as it was created in the Failover Cluster Manager.
Zerto role IP	The IP of the **first** role, at it appears in the Failover Cluster Manager.

12. Click **NEXT**. The vCenter Connectivity window appears.



13. 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 runs.
    - **Username:** The user name for a user with administrator level privileges to 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.
14. Click **NEXT**.
    - For further steps on vCloud Direct (vCD) Connectivity, continue to step 15 on page 55.
    - Otherwise, go to step 18 on page 57.
15. The vCloud Director Connectivity window is displayed.



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

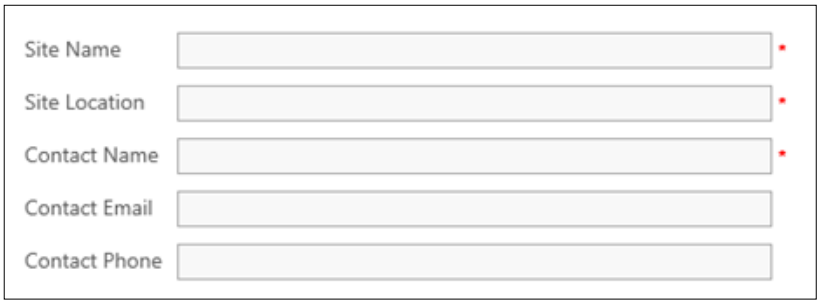
    - **IP / Host name:** The IP address or host name of the machine where vCD runs. When connecting to vCD with multiple cells, enter the virtual IP for the network load balancing used by the cells.
    - **Username:** The user name for an administrator to vCD.
    - **Password:** A valid password for the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

    > ☑ **Tip:**
    >
    > 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, and enter the following credentials:
    > - **Username:** 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.

17. Click **NEXT**.

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

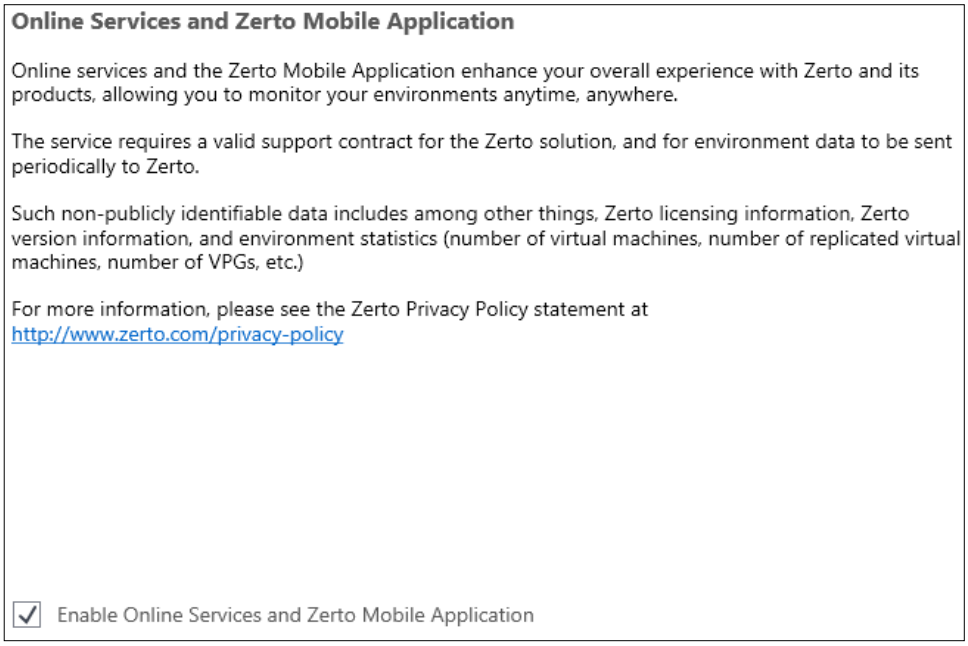


19. Enter the site details:

Site Name:	(Optional) A name to identify the site. This name is displayed in the Zerto User Interface
Site Location:	(Mandatory) Information such as the address, or name of the site to identify it.
Contact Name:	(Mandatory) The name of the person to contact if a need arises.
Contact Email:	(Optional) The email address to contact if a need arises.
Contact Phone:	(Optional) The phone number to contact if a need arises.

20. Click **NEXT**.

The Online Services and Zerto Mobile Application window appears.



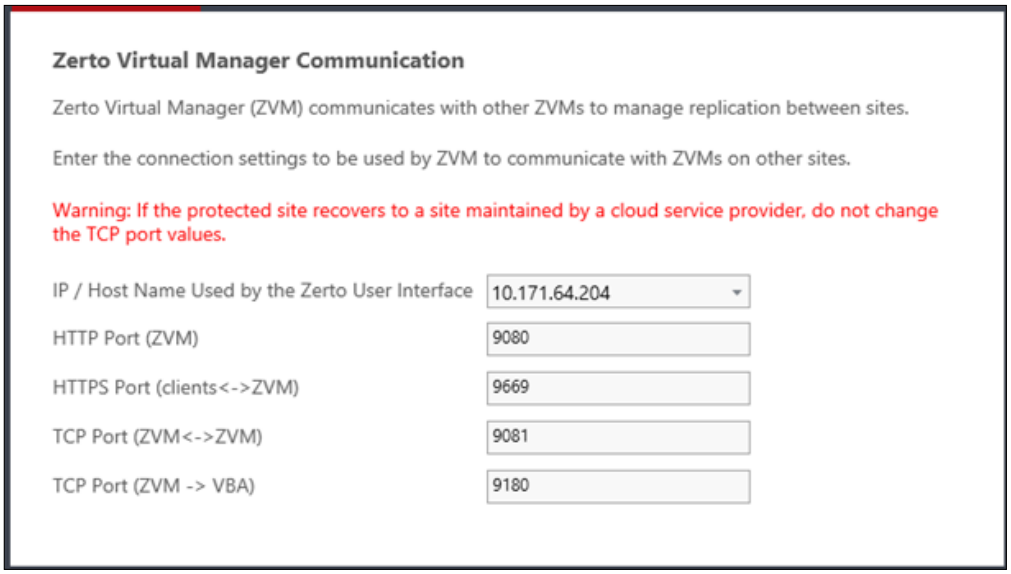
The Online Services and Zerto Mobile Application are **enabled by default**.

- You can **disable** these services by deselecting **Enable Online Services and Zerto Mobile Application**.

21. 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.



PORT DESCRIPTION PARAMETER	DEFAULT PORT NUMBER	COMMUNICATION DIRECTION	BETWEEN...	COMMENTS
IP/Host Name Used by the Zerto User Interface	NA		Zerto User Interface *- and -* Zerto Virtual Manager	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)	9080	Inbound	Zerto Virtual Manager *- and -* Zerto internal APIs, and Cmdlets	
HTTP Port (clients<->ZVM)	9669	Inbound	Zerto User Interface *- and -* Zerto Virtual Manager	

PORT DESCRIPTION PARAMETER	DEFAULT PORT NUMBER	COMMUNICATION DIRECTION	BETWEEN...	COMMENTS
TCP Port (ZVM<->ZVM)	9081	Inbound and outbound	Zerto Virtual Manager *- and -* Zerto Virtual Manager	• When **both** the protected **and** recovery sites **belong to the same enterprise**: • If you change this value, when pairing sites, use the TCP port value specified here. See the section **Pairing Sites**. • When an enterprise uses a **cloud service provider** to **supply** disaster recovery services: • Do not change this value
TCP Port (ZVM->VBA)	9180	Inbound and outbound	Zerto Virtual Manager *- and -* Virtual Backup Appliance (VBA)	

22. Click **NEXT**.

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

23. You must **exclude** the following folders from **antivirus scanning:**

Zerto Virtual Replication

%ProgramData%\Zerto\Data\zvm_db.mdf

C:\Program Files\Zerto\Zerto Virtual Replication\Zerto.Zvm.Service.exe

C:\Program Files\Zerto\Zerto Virtual Replication\Zerto.Vba.VbaService.exe

C:\Program Files\Zerto\Zerto Virtual Replication\Zerto Online Services Connector\Zerto.Online.Services.Connector.exe

C:\Program Files\Zerto\Zerto Virtual Replication\Embedded DB Manager Service\Zerto.LocalDbInstanceManagerService.exe

Failure to do so may lead to the Zerto Virtual Replication folder being incorrectly identified as a threat and in some circumstances corrupt the Zerto Virtual Replication folder.

24. 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.

25. Proceed to Configuring the Role with Zerto Services on page 61.

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

Configuring the Role with Zerto Services

Use the following procedures to add Zerto services to the role, and to configure the role for Zerto Virtual Manager - **in the following order**:

1. Adding and Configuring the Zerto Virtual Manager Service on page 61
2. Adding and Configuring the Zerto Virtual Backup Appliance Service on page 62
3. Adding and Configuring the Online Services Connector Service on page 63

Adding and Configuring the Zerto Virtual Manager Service

Procedure 1: To add the Zerto Virtual Manager service on page 61

Procedure 2: To configure the Zerto Virtual Manager service on page 62

Procedure 1: To add the Zerto Virtual Manager service

1. Select the role which you created in **Creating a Role for the Zerto Services**.
2. Right-click the role and select **Add Resource > Generic Service**.
3. From the list of services, select **Zerto Virtual Manager service**, then click **Next**.
4. Complete the wizard.

Procedure 2: To configure the Zerto Virtual Manager service

1. Right-click the service **Zerto Virtual Manager**, and select **Properties**.
2. Define the service's startup parameter:
   a. Click the **General** tab.
   b. In the **Startup Parameters** field enter the following parameter: **/RUNASPARTOFCLUSTER**
3. Configure the service's dependencies:
   a. Click the **Dependencies** tab.
   b. In the first row, select the network resource name, which you entered in **Procedure 2: To add and configure a network resource to the role**, and click **Apply**.
4. Define the Policies. Navigate to the **Policies** tab, and configure the following:

If resource fails, attempt restart on current node	Select this option
Period for restart	15:00 (minutes)
Maximum restarts in the specified period	10
Delay between restarts	30 (seconds)
If restart is unsuccessful, fail over all resources in this Role	Select this option
If all the restart attempts fail, begin restarting again after the specified period	Deselect this option

5. Proceed to Adding and Configuring the Zerto Virtual Backup Appliance Service on page 62.

Adding and Configuring the Zerto Virtual Backup Appliance Service

Procedure 1: To add the Zerto Virtual Backup Appliance service on page 62
Procedure 2: To configure the Zerto Virtual Backup Appliance service on page 62

Procedure 1: To add the Zerto Virtual Backup Appliance service

1. Select and right-click the role, then navigate to **Add Resource > Generic Service**.
2. Select the service **Zerto Virtual Backup Appliance**, then click **Next**.
3. Complete the wizard.

Procedure 2: To configure the Zerto Virtual Backup Appliance service

1. Right-click the service **Zerto Backup Appliance**, and select **Properties**.
2. Configure the service's dependencies:

a. Click the **Dependencies** tab.

b. In the first row, select Zerto Virtual Manager, and click **Apply**.

3. Define the Policies. Navigate to the **Policies** tab, and configure the following:

If resource fails, attempt restart on current node	Select this option
Period for restart	15:00 (minutes)
Maximum restarts in the specified period	10
Delay between restarts	30 (seconds)
If restart is unsuccessful, fail over all resources in this Role	Deselect this option
If all the restart attempts fail, begin restarting again after the specified period	Select this option

4. Proceed to Adding and Configuring the Online Services Connector Service on page 63.

Adding and Configuring the Online Services Connector Service

Procedure 1: To add the Zerto Online Services Connector service on page 63

Procedure 2: To configure the Zerto Online Services Connector service on page 63

Procedure 1: To add the Zerto Online Services Connector service

1. Select and right-click the role, then navigate to **Add Resource > Generic Service**.
2. Select the service **Zerto Online Services Connector**, then click **Next**.
3. Complete the wizard.

Procedure 2: To configure the Zerto Online Services Connector service

1. Right-click the service Zerto Online Services Connector, and select **Properties**.
2. Configure the service's dependencies:

a. Click the **Dependencies** tab.

b. In the first row, select the network resource name, and click **Apply**.

3. Define the Policies. Navigate to the **Policies** tab, and configure the following:

If resource fails, attempt restart on current node	Select this option
Period for restart	15:00 (minutes)

Maximum restarts in the specified period	10
Delay between restarts	30 (seconds)
If restart is unsuccessful, fail over all resources in this Role	Deselect this option
If all the restart attempts fail, begin restarting again after the specified period	Select this option

4. Click **Apply**, and click **OK**.
5. Right-click the role, and select **Start Role**.

Uninstalling a Zerto Cluster

On the relevant cluster node, from Add or remove programs, right-click **Zerto Virtual Replication** and select **Uninstall**.

In the window that opens, leave the default option **Slim uninstall**, or select **Full uninstall**.

Click **Run**.

Accessing the Zerto User Interface

You manage the protection and replication of virtual machines in vSphere or 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 68. Zerto also provides a set of RESTful APIs and PowerShell cmdlets to enable incorporating some of the disaster recovery functionality within scripts 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:**
>
> - For supported browsers, see Zerto Interoperability Matrix.
> - The **lowest** supported screen resolution is **1366x768**.

You must exclude the following folders from antivirus scanning:

Zerto Virtual Replication

%ProgramData%\Zerto\Data\zvm_db.mdf

C:\Program Files\Zerto\Zerto Virtual Replication\Zerto.Zvm.Service.exe

C:\Program Files\Zerto\Zerto Virtual Replication\Zerto.Vba.VbaService.exe

C:\Program Files\Zerto\Zerto Virtual Replication\Zerto Online Services Connector\Zerto.Online.Services.Connector.exe

C:\Program Files\Zerto\Zerto Virtual Replication\Embedded DB Manager Service\Zerto.LocalDbInstanceManagerService.exe

Failure to do so may lead to the Zerto Virtual Replication folder being incorrectly identified as a threat and in some circumstances corrupt the Zerto Virtual Replication folder.

The following topics are described in this section:

- Accessing the Zerto User Interface on page 65
- Using the Zerto User Interface Within vSphere on page 66
- Adding a Security Certificate for the Zerto User Interface on page 68

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.

   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.

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 feature:

- 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.

See also:

- Using the vSphere Web Client on page 66
- Using the vSphere Client Console on page 68

Using the vSphere Web Client

You can use the VMware Web Client to manage Zerto.

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 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 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 and on the other run the VMware plug-ins.

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

1. When the vSphere Web Client service is installed on a **Microsoft Windows platform**:
   a. Copy and run **VsphereWebClientPluginEnabler.exe** to the machine where you run the web client service.

      This file is located in the Zerto folder under the folder where Zerto was installed. You can copy VsphereWebClientPluginEnabler.exe to any folder on the relevant machine.

   b. Run **VsphereWebClientPluginEnabler.exe** as an **administrator**.
2. When the vSphere Web Client is installed on a **Linux platform**, via the **vCenter Server Linux Virtual Appliance** (vCSA):
   a. Depending on your vCenter Server version, navigate to:
      - Up to vCenter Server **5.5.x**, navigate to: /var/lib/vmware/vsphere-client
      - From vCenter Server **6.0.x,** navigate to: /etc/vmware/vsphere-client/
   b. Open the **webclient.properties** file in a text editor and add the following to the file:.

      ```
      scriptPlugin.enabled = true
      ```
3. Restart the vSphere Web Client service.

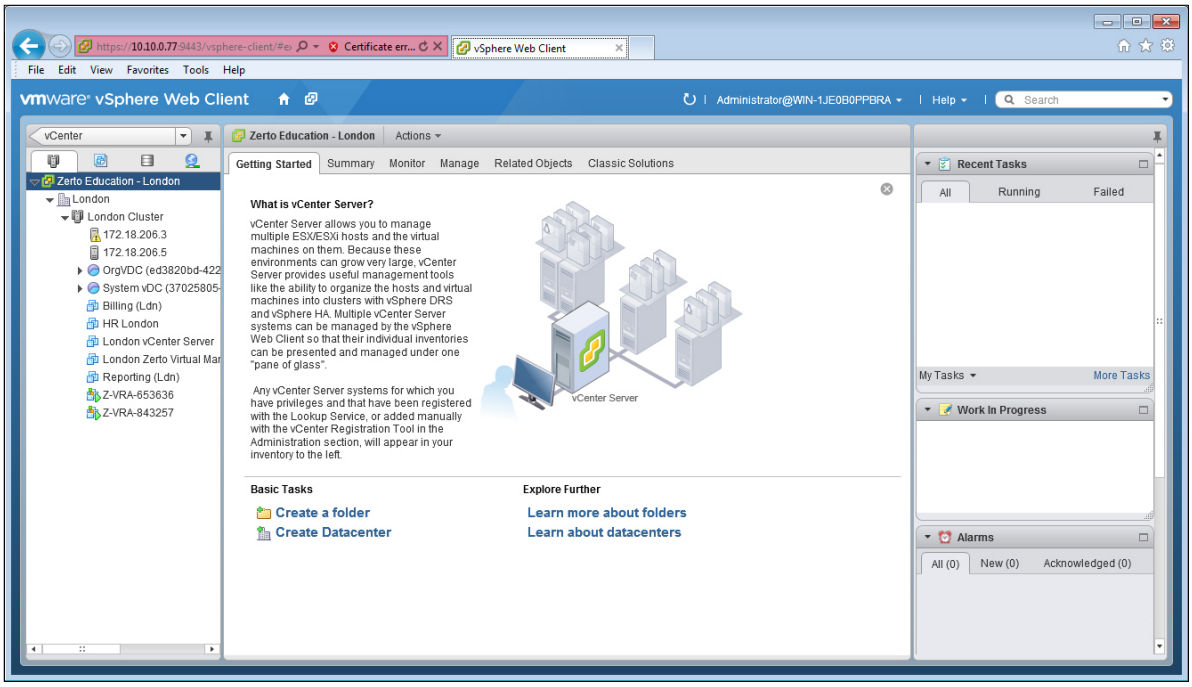
   After the service has started you might have to **wait a few minutes** before you can open the vSphere Web Client in your browser.

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, such as the root node or a virtual machine, and select 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 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 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.

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

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:

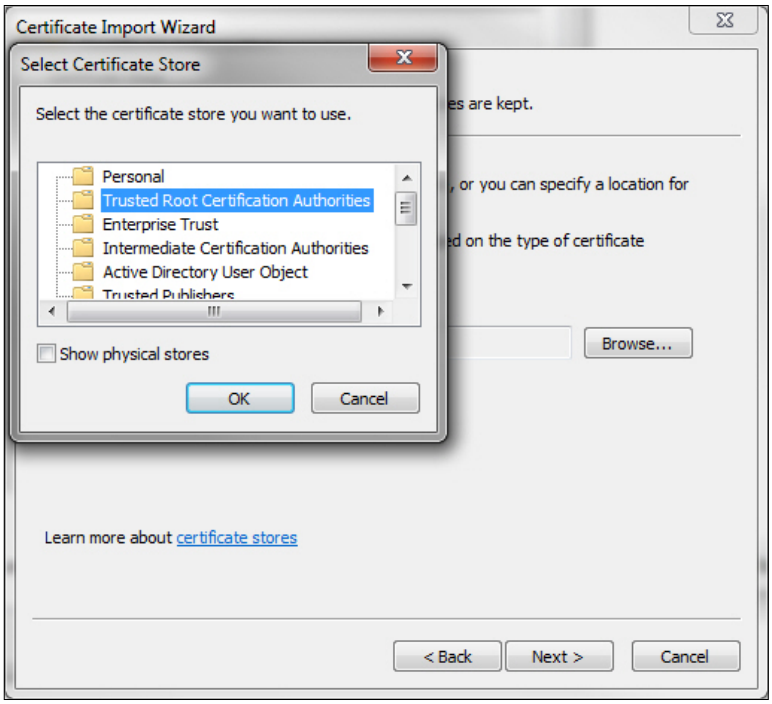
- To run this procedure run Microsoft Internet Explorer as **administrator**. The procedure is similar for Google Chrome and for Mozilla Firefox.
- Access the Zerto User Interface **using the IP** and not the name of the machine where Zerto is installed.

To install a security certificate for the Zerto User Interface:

1. Click **View Certificate**. The Certificate window appears.
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.

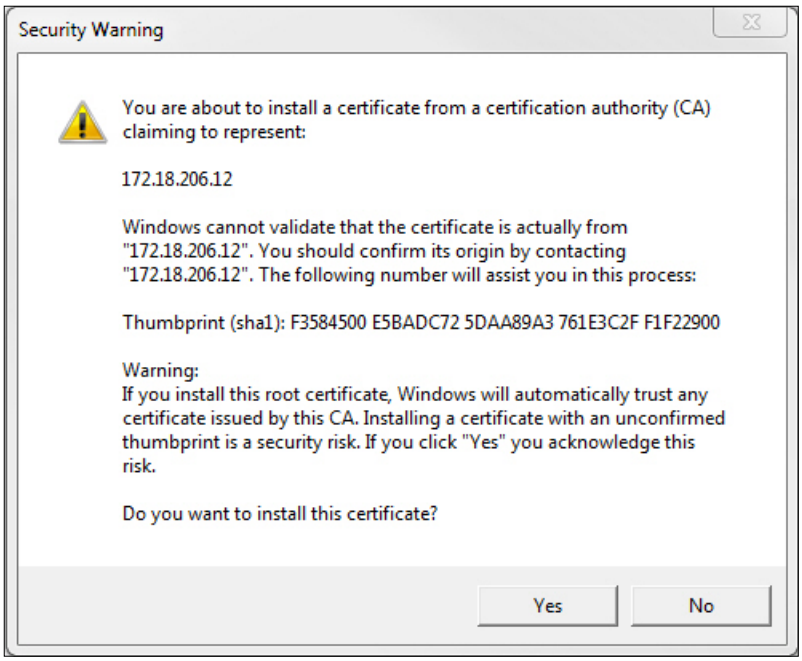
   To do this, in the relevant window:

   a. Select the option **Place all certificates in the following store** and browse to select the store **Trusted Root Certification Authorities**.



   b. Continue to the end of the wizard.

   c. When the Security Warning appears, click **Yes**.



d. Click **OK** to confirm that the installation was successful.

e. Click **OK** when prompted, and then **Yes** in the Security Alert window to continue.

4. Proceed with Initial Configuration on page 71.

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:

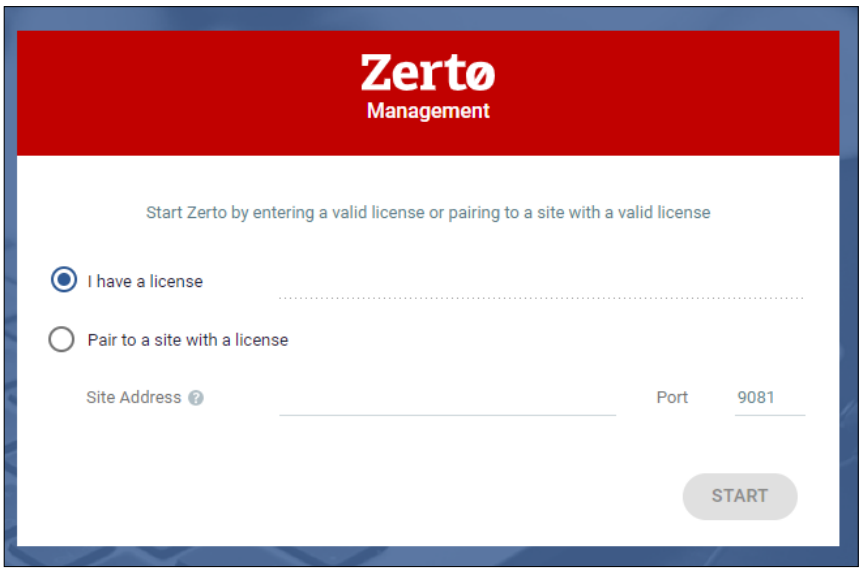
- Registering the Zerto Virtual Replication License on page 71
- Installing Virtual Replication Appliances on page 72
- Pairing Sites on page 79
- Setting Up a Remote Site on page 82

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 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**.

(vSphere only) 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 79. 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 then **pair the protected and recovery sites**, as described in the following sections:

- Installing Virtual Replication Appliances on page 72
- Pairing Sites on page 79

Installing Virtual Replication Appliances

> **Note:** This section only applies to non-Zerto versions.

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 ESX/ESXi or Hyper-V which hosts virtual machines that require protecting in the protected site and on every ESX/ESXi or 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.
- *(Hyper-V only)* When running Hyper-V hosts on **2012 R2**, verify that **User Account Control: Run all administrators in Admin Approval Mode** security policy setting is set to **Disabled**. This can be found in the path:

  Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control

> **Note:** For Zerto Enterprise Government Edition (EGE) environments, go to Deploying Zerto Enterprise Government Edition on page 35.

See also:

- VRA Installation Requirements on page 73
- Setting Up Routing on page 75
- Installing a Zerto Virtual Replication Appliance (VRA) on a Host on page 76

VRA Installation Requirements

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

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

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

Before You Begin:

You must know the following information to install a VRA:

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

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

- The **storage** the VRA will use, and the **local network** used by the **host**.
- The **network settings** to access the **peer** site; either the default gateway or the IP address, subnet mask, and gateway.

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

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

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

- If the **peer site VRAs** are **not** on the **default gateway**, you must **set up routing** to enable the VRAs on this site to communicate with the peer site VRAs before defining the VRAs.
  - Setting up routing **after** defining VRAs only applies to VRAs installed after the routing is set.
  - Any **existing VRA** is not affected and access to these VRAs continues via the default gateway.
  - If the default gateway stops being used, you must reinstall the VRAs that were installed before setting up paired site routing.
- *(vSphere only)* For the duration of the installation of the VRA, the Zerto Virtual Manager enables SSH in the vCenter Server.
- *(vSphere only)* You must know the following information to install a VRA:
  - The **password** to access the **host root account,** for ESXi 5.x and higher.
  - The **datastore** the VRA will use and the **local network** used by the host.
  - The **network settings** to access the **peer** site; either the default gateway or the IP address, subnet mask, and gateway.
  - If a **static IP** is used, instead of DHCP, which is the Zerto recommendation, you need to know the IP address, subnet mask, and default gateway to be used by the VRA.

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

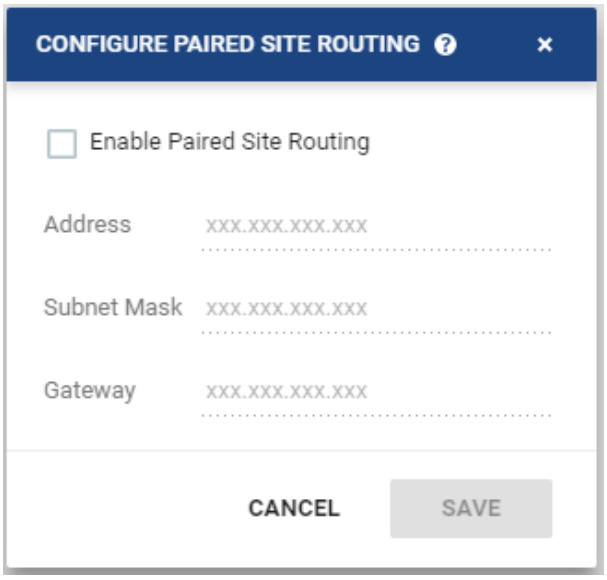
Setting Up Routing

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 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 all VRAs installed on the peer site after the information is saved.

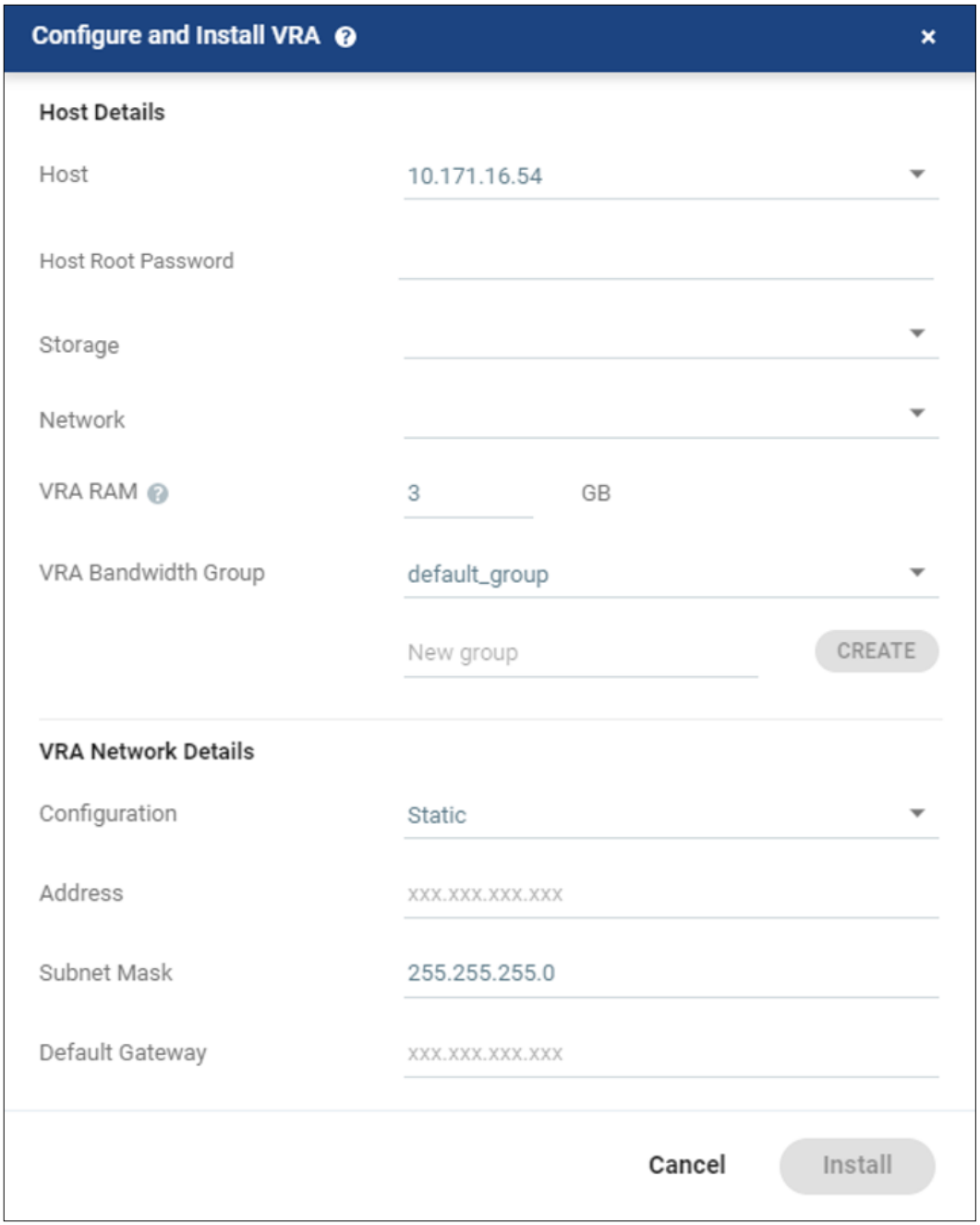
Installing a Zerto Virtual Replication Appliance (VRA) on a Host

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

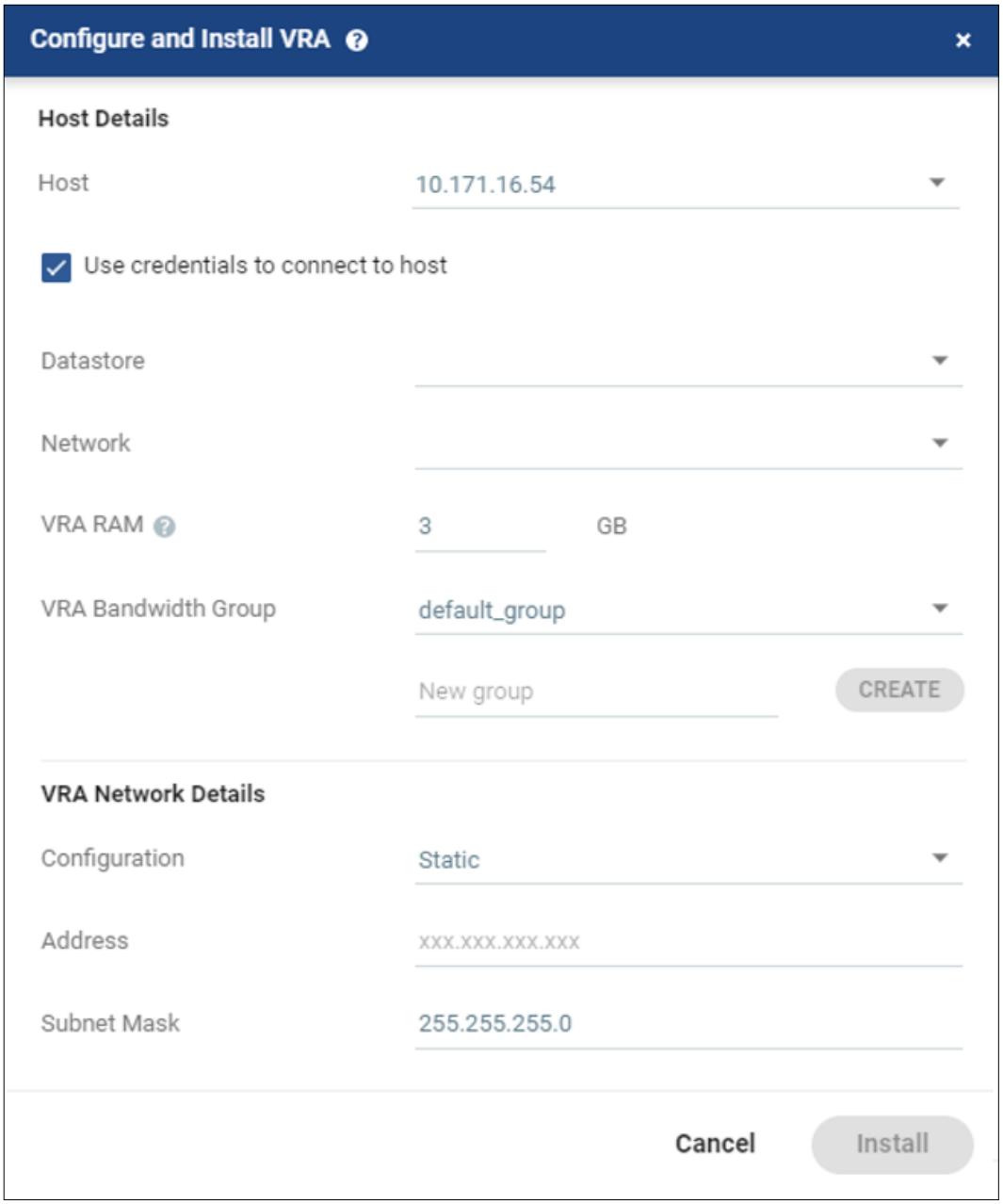
To install a Virtual Replication Appliance (VRA) on a host:

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.
   Example: Hyper-V host



Example: ESXi host



> **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.

     (vSphere only) From ESXi 5.5, by default, Zerto Virtual Manager creates a **.VIB** (vSphere Installation Bundle) which is used to set up a secure communication channel to the host. The

.VIB is installed on the host when the VRA is installed. When using VIB:

- The user does not enter a password.
- Once a day, Zerto Virtual Manager checks that the VRA and host can connect. If the connection fails, Zerto Virtual Manager re-initiates the connection automatically and logs it.

(vSphere only) For ESX/i versions earlier than 5.5, when using a password, Zerto Virtual Manager connects to the host using the root password. Once a day, Zerto Virtual Manager checks that the password is valid. If the password was changed, an alert is issued, requesting the user enter the new password.

- **Use credentials to connect to host:** When unchecked, the Zerto Virtual Manager uses VIB to set up a secure communication channel to the host. This field is only relevant for ESXi 5.5 and later.
- **Host Root Password:** When the VRA should connect to the host with a password, check **Use credential to connect to host** and enter the root user password used to access the host. When the box on the right side is checked, the password is displayed in plain text. This field is only relevant for ESXi 5.x hosts.

- *(Hyper-V only)* **Host Root Password**: For future use.
- *(vSphere only)* **Datastore**: The datastore that contains the OS disks of the VRA VM. You can install more than one VRA on the same datastore.
- *(Hyper-V only)* **Storage**: The storage that contains the OS disks of the VRA VM. You can install more than one VRA on the same storage.
- **Network**: The network used to access the VRA.

  VRA RAM: The amount of memory to allocate to the VRA. For details, refer to Zerto Scale and Benchmarking Guidelines.

  - 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.
- **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 host that hosts virtual machines for which you want replication.

   - Zerto recommends installing a VRA **on every listed 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.
   - *(Hyper-v only)* 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 folders with the same name is also created where the VRA is installed.

Pairing Sites

See the following sections:

- Pair to Another Site on page 79
- Unpairing Sites on page 81

Pair to Another Site

You can pair to any site where Zerto is installed.

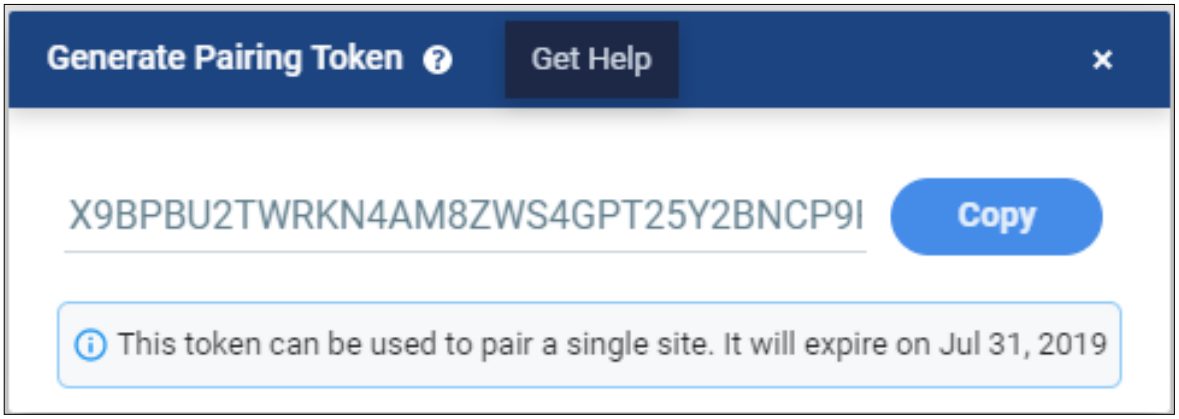
Zerto can be installed at multiple sites and each of these sites can be paired to any other site on which Zerto has been installed. Virtual machines that are protected on one site can be recovered to any paired site.

To pair to a site:

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



2. The Generate Pairing Token window opens.



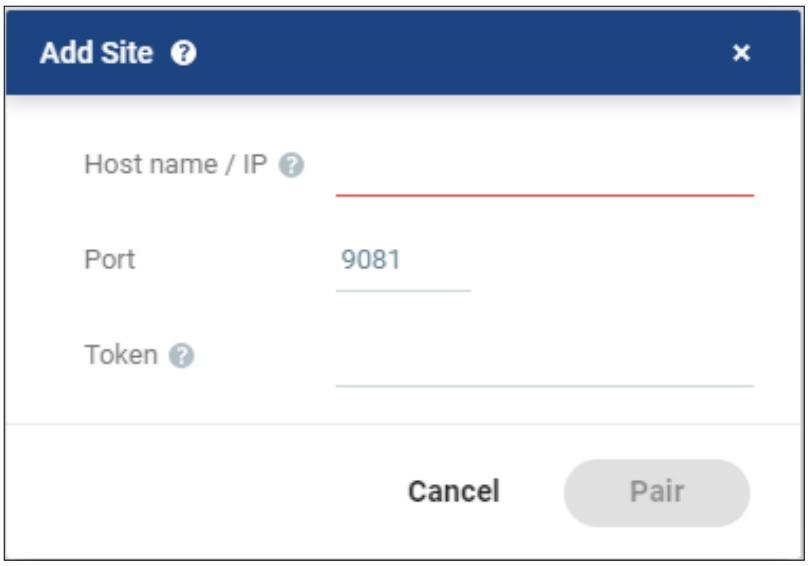
3. Click **Copy**, to copy the token.

   The token **expires** when the earliest of one of the following conditions is met:

   - 48 hours after clicking Copy
   - At the next ZVM process termination
   - After the token is used to authenticate the pairing request

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

   The Add Site window is displayed.



5. Specify the following:
   - **Host name/IP:** IP address or fully qualified DNS host name of the **remote** site Zerto Virtual Manager to pair to.
   - **Port:** The TCP port communication between the sites. Enter the port that was specified during the installation. The default port during the installation was 9081.
   - **Token:** Paste the token which you copied above.
6. Click **PAIR**.

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

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

Unpairing Sites

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

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

To unpair two sites:

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

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

   If there are either protected or recovered VPGs on the paired sites, a message appears warning the user that the VPGs will be deleted.

3. For vSphere, Hyper-V and Azure platforms, you can select to keep disks to use for preseeding if the VMs are re-protected. If you select this option, the disks are not removed from the recovery site.
4. To unpair, click **CONTINUE**.

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

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

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

Setting Up 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 79 and then installing VRAs in the site.

To install VRAs on hosts in the remote site:

1. Repeat the procedure, Installing Virtual Replication Appliances on page 72, 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 71.

> **Note:** You can install VRAs on all the sites from within the Zerto Cloud Manager user interface.

Zerto

Zerto enhances the Zerto IT Resilience Platform by converging disaster recovery and backup to deliver continuous availability within a simple, scalable platform. Zerto delivers enhanced analytics, platform improvements and cloud performance upgrades required in the future of IT resilience.

Learn more at Zerto.com.

For assistance using Zerto's Solution, contact: @Zerto Support.

© 2020 Zerto Ltd. All rights reserved.