ZERTO VIRTUAL REPLICATION - PREREQUISITES & REQUIREMENTS FOR VSPHERE ENVIRONMENTS

ZVR-REV-6.5 Rev01 U2 Dec2018

Zerto Virtual Replication is installed in a site with virtual machines to be protected, as well as in the site where these virtual machines will be recovered.

This section describes **Zerto Virtual Replication - Requirements for vSphere Environments**.

For AWS, Microsoft Azure or Microsoft Hyper-V protected sites requirements, go to myZerto > Technical Documentation portal.

- The Zerto Virtual Replication installation includes:
  - A **Zerto Virtual Manager (ZVM)**: This is a Windows service and manages the replication at the site level, and the ability to install **Virtual Replication Appliances** (VRAs), virtual machines installed on each ESX/ESXi host to move the data to be replicated from the protected to recovery site.
  - A **Virtual Backup Appliance (VBA)**: A Windows service that manages File Level Recovery operations within Zerto Virtual Replication. These repositories can be local or on a shared network.
- Zerto Virtual Replication can be installed at **multiple** sites and each site can be paired to any other site.
- All sites can be managed from a centralized user interface, the **Zerto Cloud Manager (ZCM)**, a Windows service, or each site can be managed separately via a Zerto user interface, accessed from a browser or from within the vSphere Web Client or Client console.
- Zerto Virtual Replication is installed on **both** the **protected** and **recovery sites**.
- Zerto Virtual Replication also supports both the protected and recovery sites being **managed by a single vCenter Server**, for small branch offices.

  For example, from one datacenter to another datacenter, both managed by the same vCenter Server.
- When the protected and recovery sites are the **same site**, only one installation of Zerto Virtual Replication is required.
- When recovery is managed by the **same vCenter Server** as the **protection**, Zerto Virtual Manager is required to be installed once only.
- When the protected and recovery sites are managed by **different vCenter Servers**, Zerto Virtual Manager is installed once per vCenter Server.
- If Zerto Cloud Manager is used, vSphere Standard edition cannot be used. For details about Zerto Cloud Manager, see *Zerto Cloud Manager Administration Guide*.
- When the vCenter Server is installed on a Linux machine via the vCenter Server Linux Virtual Appliance (vCSA), the Zerto Virtual Manager must still be installed on a Windows machine.

See the following sections:

Requirements for Each Site

- VMware vCenter Server version that is supported in the Interoperability Matrix with at least one ESX/ESXi host.
- The Zerto Virtual Manager must have access to the **vCenter Server** via a user with **administrator level privileges** to the **vCenter Server**.

NOTE:

- When upgrading vCenter Server be sure that the user entity that Zerto Virtual Replication is using is preserved in the user/permissions hierarchy.
- When upgrading a vCenter Server, you need to close the ZVM UI.

- On the machines where **Zerto Virtual Replication** is installed:
  - 64-bit Operating System
  - The Operating system version number must be 6.1 or higher
  - The Windows operating system must be Server Edition
  - Supported Operating Systems:
    - Windows Server 2008 R2 SP1 with KB3033929 and KB2864202
    - Windows Server 2012 base
    - Windows Server 2012 R2
    - Windows Server 2016
    - Windows Server 2019
  - Microsoft **.NET Framework 4.5.2. or higher**
    - The 4.5.2 installation executable is **included** as part of the Zerto Virtual Replication installation kit and it needs an additional **1.8GB of free disk space**
    - If you install .NET Framework 4.5.2 as part of the Zerto Virtual Replication installation, you will be prompted to restart
  - Reserve at least **2 CPUs** and **4GB RAM** for the machine
  - The following CPU and RAM are **recommended** by Zerto for the machine running Zerto Virtual Replication, dependent on the size of the site.
    Zerto recommends running with at least 16GB memory.

NUMBER OF VIRTUAL MACHINES OR PEER SITES		NUMBER OF CPUS	RAM SIZE
VIRTUAL MACHINES	PEER SITES		
Up to **150** virtual machines	And up to **2** peer sites	**4** CPUs	**8**GB
Between **150-750** virtual machines	And up to **5** peer sites	**4** CPUs	**8**GB
Between **750-5000** virtual machines	And up to **80** peer sites	**4** CPUs	**16**GB
Between **5000-10000** virtual machines	Or **80+** peer sites	**4** CPUs	**24**GB

  - The **clocks** on the machines where Zerto Virtual Replication is installed must be **synchronized with UTC** and with each other (the timezones can be different). Zerto recommends synchronizing the clocks using NTP.
  - At least **20GB** of free disk space
  - You must **exclude** both the **Zerto Virtual Replication** folder and **%ProgramData%\Zerto\Data\zvm_db.mdf** from **antivirus scanning**. 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.

Recommended Best Practices

Zerto recommends the following best practices:

- Install Zerto Virtual Replication on a dedicated virtual machine with a dedicated administrator account and with VMware High Availability (HA) enabled.
  - Avoid installing other applications on this machine.
  - If other applications are installed, the Zerto Virtual Manager service must receive enough resources and HA must remain enabled.

- Install a VRA on every host in a cluster so that if protected virtual machines are moved from one host to another, there is always a VRA to protect the moved virtual machines.
  - When protecting a vApp, you must install a VRA on every host in the cluster on both the protected and recovery sites and ensure that DRS is enabled for the clusters.
- Install VRAs using static IP addresses and not DHCP for a production environment.
- It is required to exclude the Zerto Virtual Replication folder from antivirus scanning.

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

Requirements for Virtual Replication Appliances

To **install a VRA** you require the following on the **ESX/ESXi**:

- **15GB** storage space
- At least **1GB** of **reserved memory**.
- The ESX/ESXi version must be **4.0U1 or higher**.
- **Ports 22** and **443** must be **enabled on the host** during the installation.

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

You must know the following information to install a VRA:

- The **password** to access the **host root account,** for ESXi 4.x and 5.x.
- 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.

Requirements for Zerto Cloud Manager

- Zerto Cloud Manager is installed on a machine running a **Windows** operating system with the following requirements:
  - A **Windows** operating system with one of the following:
    - Windows Server 2003 SP2 or higher
    - Windows Server 2008
    - Windows Server 2008R2
    - Windows Server 2012
    - Windows Server 2012R2 with at least 1 CPU and 2GB RAM reserved
    - Windows Server 2016
  - At least **4GB** of free disk space.
  - Microsoft **.NET Framework 4 or higher**.

Routable Networks

The Zerto Virtual Replication architecture supports the following network configurations:

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

- The instance (virtual machine) on which the Zerto Cloud Appliance is installed must use a subnet that is accessible from all Zerto Virtual Managers that may be connected to this instance.

The Zerto Virtual Replication architecture does **not** support NAT (Network Address Translation) firewalls.

Minimum Bandwidth

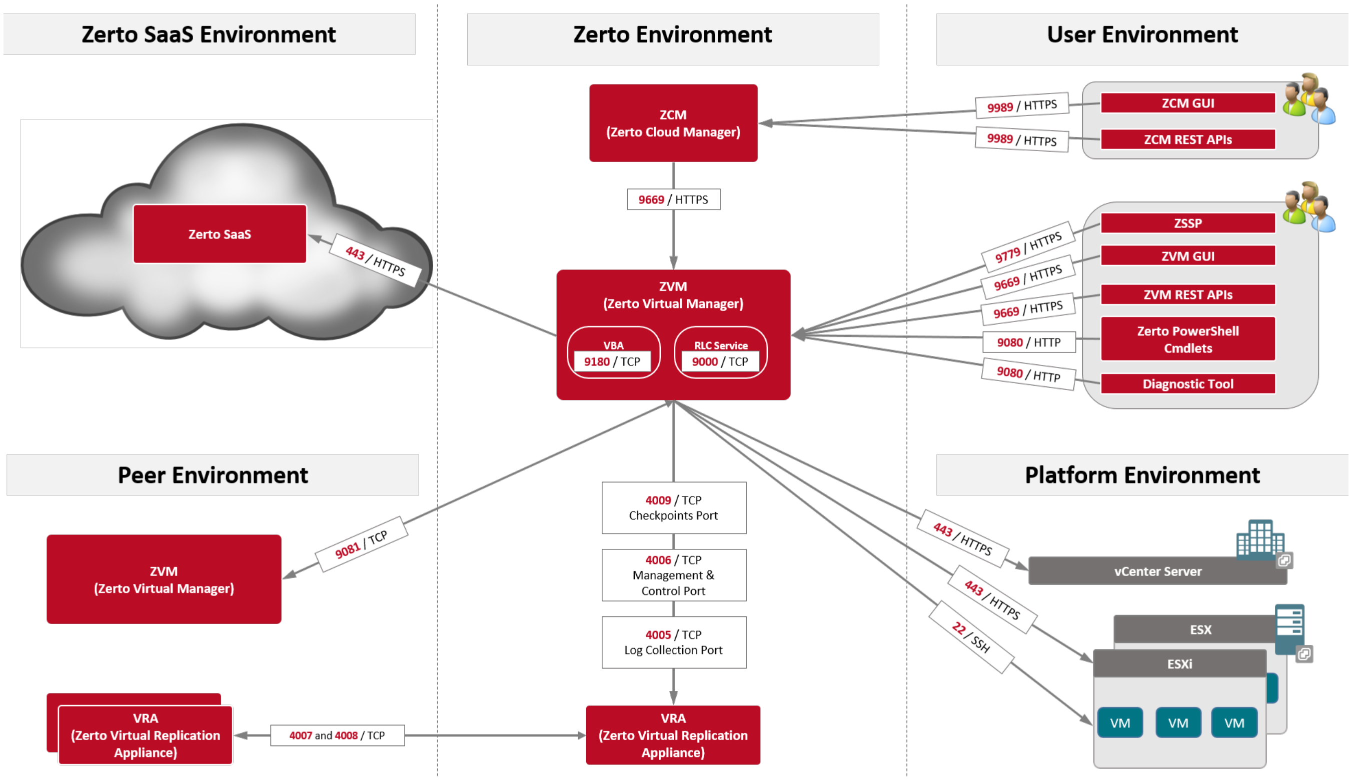
- The connectivity between sites must have the bandwidth capacity to handle the data to be replicated between the sites. The **minimum dedicated bandwidth** must be at least **5 Mb/sec**.

The Zerto User Interface

- Zerto recommends using Chrome, Firefox, Microsoft Edge, or later versions of Internet Explorer.
- Microsoft Internet Explorer 10 and all versions below, are **not** supported.
- The minimum recommended screen resolution is 1024*768.

Open Firewall Ports

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



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

The following scenarios are examples of protection and recovery with a **single vCenter Server**.

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

- From one datacenter, a branch office, to another datacenter, the main office, both managed by the same vCenter Server.

  Zerto recommends installing Zerto Virtual Replication in the main office site where protected machines will be recovered.
- From one host to a second host, both managed by the same vCenter Server.
- To the same host but using a different datastore for recovery.

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

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

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

PORT	PURPOSE
22	Required between an ESXi host and the ZVM during installation of a VRA.
443	Required between the ZVM and the vCenter Server.
443	Required between an ESXi host and the ZVM during installation of a VRA.
4005	Log collection between the ZVM and site VRAs.
4006	Communication between the ZVM and local site VRAs and the site VBA.

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

PORT	PURPOSE
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	TCP communication between the ZVM and vCloud Director for access to AMQP messaging.
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**
9180*	Communication between the ZVM and the VBA.
9669*	Communication between ZVM and ZVM GUI and ZVM REST APIs, and the ZCM.

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

Open Firewall Ports