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.

The Zerto Cloud Manager is used to manage both VMware sites where protection of virtual machines is required and the sites where these protected virtual machines are recovered in the following scenarios:

- For a cloud service provider providing disaster recovery as a service (DRaaS), replicating from a customer organization to the cloud service provider site.
- For a cloud service provider providing in the cloud hosting and disaster recovery (ICDR), where customer organization production is hosted by the cloud service provider and the cloud service provider offers disaster recover to another site.
- For an enterprise managing all their sites for disaster recovery from a single management interface, as with ICDR.

In all cases, both Zerto Virtual Managers and a Zerto Cloud Manager must be configured.

The Zerto Virtual Manager (ZVM) is a Windows service that manages replication at the site level. The ZVM monitors the hypervisor management tool to get the inventory of virtual machines, disks, networks, hosts, etc. For example, a VMware vMotion operation of a protected virtual machine from one host to another is monitored by the ZVM and the protection and recovery is updated accordingly.
The Zerto Cloud Manager (ZCM) is a Windows service that manages all your VMware sites offering disaster recovery, either as a service or completely within the cloud environment, protecting on one cloud site and recovering to a second site.

As can be seen in the diagram above, each site has a ZVM installed. One site has the Zerto Cloud Manager installed to manage all the sites.

A Virtual Backup Appliance (VBA) is a Windows service that manages File Level Recovery operations within Zerto.

Continue to the following topics:
- “Requirements”, below
- “How to Install Zerto Cloud Manager”, on page 3
- “Troubleshooting the Installation”, on page 3
- “Firewall Ports Used With Zerto”, on page 3
- “Uninstalling Zerto”, on page 6
- “Upgrading Zerto”, on page 7

Requirements

Zerto Cloud Manager is installed on a machine running a Windows operating system that meets the following requirements:
  - Windows 7, 8 or 10.
  - Reserve at least 1 CPU and 2GB RAM for the machine.
  - The clocks on the machine where Zerto Cloud Manager is installed must be synchronized with UTC and with each other (the time zones can be different). Zerto recommends synchronizing the clocks using NTP.
- At least 2GB of free disk space.
- Microsoft .NET Framework 4.7.2.
- Adobe Flash Player 11.9 ActiveX or higher.
  - **Note:** Adobe Flash Player is only necessary for Zerto Cloud Manager. It is not necessary for Zerto Virtual Manager.
- 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.

Zerto Cloud Manager requires port 9989 to be open in the firewall. For full details of the required ports, see “Firewall Ports Used With Zerto”, on page 3.

Zerto recommends installing the Zerto Cloud Manager on a dedicated virtual machine. Zerto can be used to protect this machine from disasters.
How to Install Zerto Cloud Manager

The Zerto Cloud Manager installation deploys the Zerto Cloud Manager.

To Install Zerto Cloud Manager:
1. Run Zerto Cloud Manager Installer.
2. Follow the wizard until the following dialog.

![End User License Agreement dialog]

The port specified here is used to access the Zerto Cloud Manager after the installation completes.

3. Do the following:
   ■ Accept the License Agreement.
   ■ If necessary:
     ■ Change the port to use for secure communication.
     ■ Change the location in which to install the Zerto Cloud Manager.
4. Click Install and continue to the end of the installation.

Troubleshooting the Installation

If you have problems accessing the Zerto Cloud Manager, on the machine where the Zerto Cloud Manager is installed, check under Windows Services that the Zerto Cloud Manager service has started.

Firewall Ports Used With Zerto

Disaster recovery using Zerto includes a number of components that communicate together, both within a site and across sites. For this communication to be successful, certain ports must be open.

In this section:
■ “Zerto ICDR Architecture”, on page 4
■ “Zerto DRaaS Architecture”, on page 5
Zerto ICDR Architecture

The following diagram shows the basic ICDR architecture with the required ports. ICDR organizations can manage their disaster recovery via the Zerto Self-service Portal.
Zerto DRaaS Architecture

The following diagram shows the basic DRaaS architecture for a VMware environment, with the required ports. DRaaS organizations can manage their disaster recovery via the Zerto User Interface.
The following ports must be opened in the firewalls in both the organization and cloud service provider sites. The # reference numbers refer to the above architecture diagrams:

<table>
<thead>
<tr>
<th>Port</th>
<th>#</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>9, 24</td>
<td>During Virtual Replication Appliance (VRA) installation on ESXi 4.x and 5.x hosts for communication between the Zerto Virtual Manager (ZVM) and the ESXi hosts IPs and for ongoing communication between the ZVM in the cloud site – but not the customer site – and a Zerto Cloud Connector.</td>
</tr>
<tr>
<td>443</td>
<td>2, 6, 8, 19</td>
<td>During VRA installation on ESX/ESXi hosts for communication between the ZVM and the ESX/ESXi hosts IPs and for ongoing communication between the ZVM and vCenter Server and vCloud Director.</td>
</tr>
<tr>
<td>4005</td>
<td>10</td>
<td>Log collection between the ZVM and VRAs on the same site.</td>
</tr>
<tr>
<td>4006</td>
<td>11</td>
<td>TCP communication between the ZVM and VRAs and the VBA on the same site.</td>
</tr>
<tr>
<td>4007</td>
<td>16, 21</td>
<td>TCP control communication between protecting and recovering VRAs and between a Zerto Cloud Connector and VRAs.</td>
</tr>
<tr>
<td>4008</td>
<td>17, 25</td>
<td>TCP communication between VRAs to pass data from protected virtual machines to a VRA on a recovery site and between a Zerto Cloud Connector and VRAs.</td>
</tr>
<tr>
<td>4009</td>
<td>12</td>
<td>TCP communication between the ZVM and site VRAs to handle checkpoints.</td>
</tr>
<tr>
<td>5672</td>
<td>20</td>
<td>TCP communication between the ZVM and vCloud Director for access to AMQP messaging.</td>
</tr>
<tr>
<td>9080</td>
<td>1, 13, 15, 18</td>
<td>HTTP communication between the ZVM and Zerto internal APIs, a Zerto Cloud Manager (ZCM), cmdlets, which should only be available to a customer using DRaaS and not ICDR. HTTP communication between ZVM and Zerto Cloud Manager (ZCM). When the customer’s ZCM is v5.5 and above, and their ZVM is v5.0, communication is via this port.</td>
</tr>
<tr>
<td>9081</td>
<td>7, 23, 27</td>
<td>TCP communication between ZVMs and between a customer ZVM and a Zerto Cloud Connector. This port must not be changed when providing DRaaS.</td>
</tr>
<tr>
<td>9082 and up</td>
<td>22, 26, 28, 29</td>
<td>Two ports for each VRA (one for port 4007 and one for port 4008) accessed via the Zerto Cloud Connector installed by the cloud service provider. There is directionality to these ports. Use a port range starting with port 9082. For example, Customer A network has 3 VRAs and customer B network has 2 VRAs and the cloud service provider management network has 4 VRAs, then the following ports must be open in the firewall for each cloud: The cloud service provider’s VRAs need to use 6 ports to reach customer A’s VRAs, while customer A’s VRAs need 8 ports to reach the cloud’s VRAs. The cloud service provider’s VRAs need to use 4 ports to reach customer B’s VRAs, while customer B’s VRAs need 8 ports to reach the cloud’s VRAs.</td>
</tr>
<tr>
<td>9180</td>
<td>32</td>
<td>Communication between the VBA and VRA.</td>
</tr>
<tr>
<td>9669</td>
<td>3, 4, 5, 14</td>
<td>HTTPS communication between: Machines running Zerto User Interface and Zerto Virtual Manager Zerto Virtual Manager and Zerto REST APIs ZVM and Zerto Cloud Manager (ZCM). When the customer’s ZCM and ZVM are both v5.5 and above, communication is via this port.</td>
</tr>
<tr>
<td>9779</td>
<td>30</td>
<td>HTTPS communication between the Zerto Self-Service Portal for in-cloud (ICDR) customers and a ZVM.</td>
</tr>
<tr>
<td>9989</td>
<td>31</td>
<td>HTTPS communication between the browser and the Zerto Cloud Manager.</td>
</tr>
</tbody>
</table>

**Uninstalling Zerto**

To uninstall Zerto Cloud Manager, from the Windows Control Panel, select **Uninstall a program**.
Upgrading Zerto

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

- For details, see Upgrading the Zerto Virtual Replication Environment.