Zerto Virtual Replication is installed in a site with virtual machines to be protected, and in a site to be used for recovery.

This document describes the prerequisites and requirements of an Amazon Web Services (AWS) recovery site.

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

You install a Zerto Cloud Appliance (ZCA) in the AWS site to use for recovery. The ZCA is comprised of the following:

- **A Zerto Virtual Manager (ZVM):** This is a Windows service that manages the replication between the protected site and AWS.
- **A Virtual Replication Appliance (VRA):** This is a Windows service that manages the replication of data from protected virtual machines to AWS. A Virtual Replication Appliance can manage a maximum of 500 volumes.
- **A Virtual Backup Appliance (VBA):** This is a Windows service that manages offsite backups within Zerto Virtual Replication on each site. The VBA service runs on the same machine as the Zerto Virtual Manager service.

See the following sections:

- “Requirements for AWS Environments”, on page 1
- “AWS Limitations Which Affect Installation and Recoverability”, on page 2
- “Routable Networks”, on page 3
- “Minimum Bandwidth”, on page 3
- “The Zerto User Interface”, on page 3
- “Firewall Considerations in AWS Environments”, on page 4

**Requirements for AWS Environments**

- Installing the ZCA on AWS installs the Zerto Virtual Manager, Virtual Replication Appliance, and a Zerto Backup Appliance as Windows services. There can be multiple ZCAs in a single AWS Availability Zone.

For each account on AWS, there must be:

- **Access to AWS:**
  - AWS access key ID
  - AWS secret access key
- **Permission to use both S3 and EC2,** including importing data from S3 to EC2. Specifically, this means the Zerto Cloud Appliance users must have AmazonS3FullAccess and AmazonEC2FullAccess permissions. These can be set in the AWS Access Management (IAM) service.
- **An AWS Direct Connect or VPN connection** between the instance on AWS and the protected site.

**Note:** For cloud service providers, Zerto recommends one ZCA per account.

- **The Zerto Cloud Appliance** must be installed on:
  - An instance on AWS EC2 running a Windows operating system with one of the following using a subnet accessible by other Zerto Virtual Replication sites:
    - 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
      - 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.

- Make sure that you have the latest .NET and Windows updates, unless Zerto support warns against a specific update.
- 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 **4GB of free disk space**.
- 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.

**AWS Limitations Which Affect Installation and Recoverability**

Below are the default AWS limitations which affect installation and recovery.

**Default AWS limitations which Affect Installation**

- **S3 Limitations:**
  - **Number of buckets:** 100 per account

**Default AWS limitations which Affect Recovery**

- Only virtual machines that are supported by AWS can be protected by Zerto Virtual Replication. Refer to AWS documentation for the supported operating systems.
- A **VPC must exist**, and a security group and subnet must be assigned to it and to all other VPCs you want to use for recovered virtual machines.
- The following **limitations** apply when protecting to AWS:
  - For **Linux**, AWS supports virtual machines with up to **40 volumes**, including the boot volume.
  - For **Windows**, AWS supports virtual machines with up to **26 volumes**, including the boot volume.
  - GBT formatted disks are supported for data volumes only.
  - The following table describes the limitations per Import Method:

<table>
<thead>
<tr>
<th>IMPORT METHOD</th>
<th>AWS Import</th>
<th>zlImport for Data Volumes</th>
<th>zlImport for all volumes</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS</td>
<td>Boot Volume</td>
<td>Additional Volume</td>
<td>Boot Volume</td>
</tr>
<tr>
<td>Linux</td>
<td>1 TB</td>
<td>1 TB</td>
<td>1 TB</td>
</tr>
<tr>
<td>Windows</td>
<td>1 TB</td>
<td>1 TB</td>
<td>1 TB</td>
</tr>
</tbody>
</table>

* Some VMs use the MBR partitioning scheme, which only supports up to 2047 GiB boot volumes. If your instance does not boot with a boot volume that is 2 TB or larger, the VM you are using may be limited to a 2047 GiB boot volume. See the relevant AWS documentation for more information: [http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolume-Types.html](http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolume-Types.html)

- For the **AWS Import** and **zlImport for Data Volumes** import methods, the **AWS ImportInstance API** only supports single volume VMs. The boot volume of the protected virtual machine should not be attached to any other volume to successfully boot. For more information, see [http://docs.aws.amazon.com/AWSEC2/latest/APIReference/API_ImportInstance.html](http://docs.aws.amazon.com/AWSEC2/latest/APIReference/API_ImportInstance.html)

It is strongly recommended to perform a **Failover Test** to ensure that the recovered instance is successfully running on AWS.

- **EC2 and VPC limitations:**
  - **On-Demand instances:** 20 per region per account
  - Instance types are also limited per region: many of them are 20 instances per region per account [https://aws.amazon.com/ec2/faqs/#How_many_instances_can_I_run_in_Amazon_EC2](https://aws.amazon.com/ec2/faqs/#How_many_instances_can_I_run_in_Amazon_EC2)

- **Networking:**
  - **Network interfaces per region:** 350
Routable Networks

- The instance 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.
- Zerto Virtual Manager 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.
Firewall Considerations in AWS Environments

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

Zerto Cloud Appliance requires the following ports to be open in the AWS site firewall, set in the Amazon security group:

<table>
<thead>
<tr>
<th>PORT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>Required between the ZVM and the AWS Cloud environment.</td>
</tr>
<tr>
<td>443</td>
<td>Required between the AWS REST Service and the ZVM during installation of a VRA.</td>
</tr>
<tr>
<td>4005</td>
<td>Log collection between the ZVM and site VRAs.</td>
</tr>
<tr>
<td>4006</td>
<td>Communication between the ZVM and local site VRAs and the site VBA.</td>
</tr>
<tr>
<td>4007</td>
<td>Control communication between protecting and peer VRAs.</td>
</tr>
<tr>
<td>4008</td>
<td>Communication between VRAs to pass data from protected virtual machines to a VRA on a recovery site.</td>
</tr>
<tr>
<td>4009</td>
<td>Communication between the ZVM and local site VRAs to handle checkpoints.</td>
</tr>
<tr>
<td>9777</td>
<td>Communication between ZVM and ZSSP (Zerto Self Service Portal).</td>
</tr>
<tr>
<td>9989</td>
<td>Communication between ZCM, and ZCM GUI and ZCM REST APIs.</td>
</tr>
<tr>
<td>9080*</td>
<td>Communication between the ZVM, Zerto Powershell Cmdlets, and Zerto Diagnostic tool.</td>
</tr>
<tr>
<td>9081*</td>
<td>Communication between paired ZVMs**</td>
</tr>
<tr>
<td>9180*</td>
<td>Communication between the ZVM and the VBA.</td>
</tr>
<tr>
<td>9669*</td>
<td>Communication between ZVM and ZVM GUI and ZVM REST APIs, and the ZCM.</td>
</tr>
</tbody>
</table>

*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.
Firewall Considerations in AWS Environments