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 Zerto Virtual Replication Prerequisites and Requirements for 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 2
- “Requirements for Replication To AWS”, on page 2
- “Requirements for Replication From AWS”, on page 4
- “AWS Defaults which Affect Installation, Protection and Recoverability”, on page 5
- “Routable Networks”, on page 6
- “Minimum Bandwidth”, on page 6
- “The Zerto User Interface”, on page 6
- “Firewall Considerations in AWS Environments”, on page 7
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.
  - 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
      - Windows Server 2016
    - 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.
    - Zerto recommends, as the minimum, using an m4.xlarge type instance, except for the Beijing region where either a m3.xlarge or m3.2xlarge type is recommended.
    - 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.

See also:
- “Requirements for Replication To AWS”, on page 2
- “Requirements for Replication From AWS”, on page 4
- “AWS Minimum Quota Requirements for Recovery in AWS”, on page 2
- “Default AWS Limitations which Affect Recovery in AWS”, on page 4
- “Routable Networks”, on page 6
- “Minimum Bandwidth”, on page 6
- “The Zerto User Interface”, on page 6

Requirements for Replication To AWS

“AWS Minimum Quota Requirements for Recovery in AWS”, on page 2

“Default AWS Limitations which Affect Recovery in AWS”, on page 4

AWS Minimum Quota Requirements for Recovery in AWS

The following is a list of the minimum quota requirements when replicating to AWS, activating Reverse Protection and also failing back from AWS.
### Requirements for AWS Environments

#### Zerto Virtual Replication - Prerequisites & Requirements for Amazon Web Services (AWS) - Version 6.0

**Zerto AWS Snapshot Adapter (zASA):** This is a snapshots lifecycle manager that returns the entire disk for syncing. The zASA is an EC2 instance that is created once the system detects there is a VPG for protected workloads in AWS. The zASA instance remains up and running as long as a VPG exists and the ZCA is installed.

**Zerto Satellite (zSATS):** Scale-out solution with EC2 instances for reading data on protected EBS disks. The zSAT is an EC2 instance for reading data from the EBS disk that is created from the snapshot of the protected EBS disk. Once that disk is read, the snapshot, EBS disk and zSAT instance from the previous sync are deleted.

See also: “AWS Defaults which Affect Installation, Protection and Recoverability”, on page 5

<table>
<thead>
<tr>
<th>RESOURCE</th>
<th>RESOURCE USAGE (PURPOSE)</th>
<th>MINIMUM QUOTA REQUIREMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>m4.large instances*</td>
<td>Virtual Machines when preparing for recovery to AWS</td>
<td>Number of instances should be the number of protected VMs that are configured in the VM settings in the VPG configuration to recover in AWS as m4.large instances.</td>
</tr>
<tr>
<td>zSAT instances</td>
<td>When replicating to AWS:</td>
<td>■ 2x the number of protected disks that are planned to be recovered in an AWS region.</td>
</tr>
<tr>
<td></td>
<td>When replicating from AWS:</td>
<td>■ 2x the number of protected EBS disks within the region.</td>
</tr>
<tr>
<td>zASA instance</td>
<td></td>
<td>1 per ZCA</td>
</tr>
<tr>
<td><strong>Storage from gp2 disk type</strong>*</td>
<td>zSAT instances</td>
<td>gp2 EBS disks total size (in GiB)</td>
</tr>
<tr>
<td></td>
<td>When replicating to AWS:</td>
<td>■ 2x the total size of protected disks that are planned to be recovered in an AWS region.</td>
</tr>
<tr>
<td></td>
<td>When replicating from AWS:</td>
<td>■ 2x the total size of protected EBS disks within the region.</td>
</tr>
<tr>
<td>zASA instance</td>
<td>gp2 EBS disk size (in GiB)</td>
<td></td>
</tr>
<tr>
<td><strong>Network interfaces</strong></td>
<td><strong>ENIs</strong></td>
<td>Virtual Machines when preparing for recovery to AWS</td>
</tr>
<tr>
<td></td>
<td>zSAT instances</td>
<td>When replicating to AWS:</td>
</tr>
<tr>
<td></td>
<td>When replicating from AWS:</td>
<td>■ 2x the number of protected EBS disks within the region.</td>
</tr>
<tr>
<td>zASA instance</td>
<td>1 ENI</td>
<td></td>
</tr>
<tr>
<td><strong>Available IPs within the ZCA subnet</strong></td>
<td>zSAT instances</td>
<td>SATs, zASA and zImporters are connected to the ZCA’s subnet.</td>
</tr>
<tr>
<td>zASA instance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>zImporters</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*For information about AWS Instance Type limits, refer to AWS documentation.*

*For information about default limits, refer to AWS documentation.*
Default AWS Limitations which Affect Recovery in AWS

- 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>OS</th>
<th>AWS Import</th>
<th>zImport for Data Volumes</th>
<th>zImport for all volumes</th>
</tr>
</thead>
<tbody>
<tr>
<td></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

- For the AWS Import and zImport 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

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

Requirements for Replication From AWS

“AWS Minimum Quota Requirements for Replication From AWS”, on page 4
“Limitations when Replicating From AWS”, on page 5

AWS Minimum Quota Requirements for Replication From AWS

The following is a list of the minimum quota requirements when protecting your workload in AWS.

<table>
<thead>
<tr>
<th>RESOURCE</th>
<th>RESOURCE USAGE (PURPOSE)</th>
<th>MINIMUM QUOTA REQUIREMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>m4.large instances*</td>
<td>zSAT instances</td>
<td>When replicating from AWS: 2x the number of protected EBS disks within the region.</td>
</tr>
<tr>
<td></td>
<td>zASA instance</td>
<td>1 per ZCA</td>
</tr>
<tr>
<td></td>
<td>*For information about AWS Instance Type limits, refer to AWS documentation.</td>
<td></td>
</tr>
<tr>
<td>Storage from gp2 disk type*</td>
<td>zSAT instances</td>
<td>gp2 EBS disks total size (in GiB)</td>
</tr>
<tr>
<td></td>
<td>*For information about default limits, refer to AWS documentation.</td>
<td></td>
</tr>
<tr>
<td>Network interfaces</td>
<td>zASA instance</td>
<td>gp2 EBS disk size (in GiB)</td>
</tr>
</tbody>
</table>
Requirements for AWS Environments

<table>
<thead>
<tr>
<th>RESOURCE</th>
<th>RESOURCE USAGE (PURPOSE)</th>
<th>MINIMUM QUOTA REQUIREMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENIs</td>
<td>zSAT instances</td>
<td>When replicating from AWS: 2x the number of protected EBS disks within the region.</td>
</tr>
<tr>
<td></td>
<td>zASA instance</td>
<td>1 ENI</td>
</tr>
<tr>
<td>Available IPs within the ZCA subnet</td>
<td>zSAT instances</td>
<td>SATs, zASA and zImporters are connected to the ZCA’s subnet.</td>
</tr>
<tr>
<td></td>
<td>zASA instance</td>
<td></td>
</tr>
<tr>
<td></td>
<td>zImporters</td>
<td></td>
</tr>
</tbody>
</table>

**Zerto AWS Snapshot Adapter (zASA):** This is a snapshots lifecycle manager that returns the entire disk for syncing. The zASA is an EC2 instance that is created once the system detects there is a VPG for protected workloads in AWS. The zASA instance remains up and running as long as a VPG exists and the ZCA is installed.

**Zerto Satellite (zSATS):** Scale-out solution with EC2 instances for reading data on protected EBS disks. The zSAT is an EC2 instance for reading data from the EBS disk that is created from the snapshot of the protected EBS disk. Once that disk is read, the snapshot, EBS disk, and zSAT instance from the previous sync are deleted.

See also: “AWS Defaults which Affect Installation, Protection and Recoverability”, on page 5

**Limitations when Replicating From AWS**
- Zerto cannot protect AWS Instance Store disks (Temp disks).
- AWS limits cross volumes consistency. Cross-volume consistency is guaranteed only when applications are paused or snapshots are taken on a powered-off instance. Therefore, the Move operation should be used for ensuring cross-volume consistency when recovering workloads from AWS. To test use Move before the Commit functionality.

**AWS Defaults which Affect Installation, Protection and Recoverability**
Below are the default AWS limitations which affect installation and recovery.

“Default AWS Limitations which Affect Installation”, on page 5

“Default AWS Limitations which Affect Protection and Recoverability”, on page 5

**Default AWS Limitations which Affect Installation**
- S3 Limitations:
  - Number of buckets: 100 per account

**Default AWS Limitations which Affect Protection and Recoverability**
- 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
  - NICs per instance: depends on instance size
- Volumes:
  - EBS disks per account: 5,000
  - Total volume storage of Magnetic volumes: 20 TiB
  - Max EBS volume size - magnetic type:
    - Min: 1 GiB
    - Max: 1024 GiB (1 GiB == 1024^3 bytes)
- Import Instance:
  - Concurrent Import-Instance tasks: 5 tasks per account
Requirements for AWS Environments

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.

<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>9779</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.

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

See also “Requirements for AWS Environments”, on page 2.