Zerto

Zerto - Prerequisites & Requirements for Amazon Web Services (AWS)

Rev01
Nov 2020
ZVR-REA-8.5

ZVR-REA-8.5

Zerto - Prerequisites & Requirements for Amazon Web Services (AWS)

Zerto 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**.

> **Note:** Site pairing and replication between AWS sites (AWS to AWS) is currently **not** supported.

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.
    - For the maximum number of volumes, either being protected or recovered to that site, see Zerto Scale and Benchmarking Guidelines.
- **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.

See the following sections:

Requirements for AWS Environments

> **Note:** **For all known issues or limitations, see the Release Notes > Known Issues section.**

- 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:

  - Permissions to perform operations in AWS in the S3 and EC2 services. For the minimum required list of permissions, see Minimum Required AWS Permissions on page 6.
  - An AWS Direct Connect or VPN connection between the instance on AWS and the protected site.

  > **Note:**
  >
  > Zerto can set default encryption on the S3 bucket so that all objects are encrypted when they are stored in the bucket. To enable S3 encryption please contact support.

- **Zerto Cloud Appliance** requirements:
  - Zerto recommends that ZCA's VPC is configured with DHCP options set to allow DNS network connectivity to S3, in order to avoid delays in ZCA operations such as Failover/Move. See AWS documentation for more information.
  - An instance on **AWS EC2** running a Windows operating system with one of the following using a subnet accessible by other Zerto 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 2012 base
    - Windows Server 2012 R2
    - Windows Server 2016
    - Windows Server 2019
    - Microsoft **.NET Framework 4.7.2. or higher**
    - The 4.7.2 installation executable is **included** as part of the Zerto installation kit and it needs an additional **4.5GB of free disk space**
      - If you **install** .NET Framework 4.7.2 as part of the Zerto 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.
- **AWS Instance Type for the ZCA**: Zerto recommends, as the minimum, using an **m5.xlarge** type instance,
- The **clocks** on the machines where Zerto 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**.
- The following folders must be **excluded** from **antivirus scanning**:

Zerto
%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 folder being incorrectly identified as a threat and in some circumstances corrupt the Zerto Virtual Replication folder.

Note: For MSPs deploying an AWS account, one ZCA is required per end customer. Multiple end-customer VPGs shared on a single ZCA, is not supported.

Minimum Required AWS Permissions

For the AWS account used by the ZCA, Zerto requires only a subset of AWS permissions. This gives the Zerto customer more security and control over their AWS environment.

> ☑ **Tip:** To create a custom role for Managed Identity, you can use the JSON in the following section: Minimum required AWS permissions - in JSON format on page 10.

Permissions are required for:

- Installing Zerto on AWS
- Failover to AWS
- Failover from AWS
- Basic functionality
- Collection of environment data

The following table lists the minimum required permissions, and for which task and service each permission is required:

Permission	Required for	Service
Resource: *		
AttachNetworkInterface	Failover to AWS	EC2
AttachVolume	Failover to AWS	EC2
CancelConversionTask	Failover to AWS	EC2
CancelImportTask	Failover to AWS	EC2
CreateNetworkInterface	Failover to AWS	EC2
CreateSnapshot	Failover from AWS	EC2
CreateTags	Basic functionality	EC2
CreateVolume	Failover to AWS	EC2
DeleteNetworkInterface	Basic functionality	EC2
DeleteSnapshot	Failover from AWS	EC2
DeleteTags	Basic functionality	EC2

Permission	Required for	Service
DeleteVolume	Failover to AWS	EC2
DeregisterImage	Failover from AWS	EC2
DescribeAvailabilityZones	Collection of environment data	EC2
DescribeConversionTasks	Failover to AWS	EC2
DescribeImages	Basic functionality Failover from AWS	EC2
DescribeInstanceAttribute	Failover from AWS	EC2
DescribeInstances	Collection of environment data	EC2
DescribeInstanceStatus	Basic functionality	EC2
DescribeNetworkInterfaces	Basic functionality	EC2
DescribeRegions	Collection of environment data	EC2
DescribeSnapshots	Failover from AWS	EC2
DescribeSecurityGroups	Collection of environment data	EC2
DescribeSubnets	Collection of environment data	EC2
DescribeTags	Failover from AWS	EC2
DescribeVolumes	Collection of environment data	EC2
DescribeVolumeStatus	Failover from AWS	EC2
DescribeVpcEndpoints	Failover from AWS	EC2
DescribeVpcs	Collection of environment data	EC2
DetachNetworkInterface	Failover from AWS	EC2

Permission	Required for	Service
DetachVolume	Failover to AWS	EC2
ImportInstance	Failover to AWS	EC2
ImportVolume	Failover to AWS	EC2
ModifyVolume	Failover from AWS	EC2
ModifyInstanceAttribute	Basic functionality	EC2
ModifyNetworkInterfaceAttribute	Failover from AWS	EC2
RunInstances	Basic functionality	EC2
StartInstances	Failover to AWS	EC2
StopInstances	Failover to AWS	EC2
TerminateInstances	Basic functionality	EC2
ListAllMyBuckets	Basic functionality	S3
HeadBucket	Collection of environment data	S3
GetPolicyVersion	Install Zerto in AWS	IAM
ListAttachedRolePolicies	Install Zerto in AWS	IAM
ListPolicyVersions	Install Zerto in AWS	IAM
PassRole	Install Zerto in AWS	IAM
DescribeTrails	Collection of environment data	CloudTrail
GetTrailStatus	Collection of environment data	CloudTrail
LookupEvents	Collection of environment data	CloudTrail
Resource: arn:aws:s3:::zerto*/*		
PutObject	Basic functionality	S3
GetObject	Basic functionality	S3

Permission	Required for	Service
GetObjectVersion	Basic functionality	S3
DeleteObjectVersion	Basic functionality	S3
DeleteObject	Basic functionality	S3
Resource: arn:aws:s3:::zerto*		
ListBucketMultipartUploads	Basic functionality Failover from AWS	S3
PutBucketTagging	Basic functionality	S3
PutLifecycleConfiguration	Basic functionality	S3
ListBucketVersions	Basic functionality	S3
CreateBucket	Basic functionality	S3
ListBucket	Basic functionality	S3
GetBucketLocation	Basic functionality	S3
DeleteBucket	Basic functionality	S3
GetBucketPolicy	Collection of environment data	S3
Resource: *, StringEquals: ec2:ResourceTag/ZERTO_TAG: "ZERTO_VPC_RESOURCE"		
AuthorizeSecurityGroupIngress	Failover to AWS	EC2
CreateSecurityGroup	Basic functionality	EC2
DeleteSecurityGroup	Basic functionality	EC2

Minimum required AWS permissions - in JSON format

Permissions for IAM roles can be specified by creating a policy in JSON format. The required AWS permissions are listed below. For further details, see Zerto - Prerequisites & Requirements for Amazon Web Services (AWS).

For your convenience, click here to access a .txt file, from which you can copy and paste.

```
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "VisualEditor0",
"Effect": "Allow",
"Action": [
"ec2:AttachNetworkInterface",
"ec2:AttachVolume",
"ec2:CancelConversionTask",
"ec2:CancelImportTask",
"ec2:CreateNetworkInterface",
"ec2:CreateSnapshot",
"ec2:CreateTags",
"ec2:CreateVolume",
"ec2:DeleteNetworkInterface",
"ec2:DeleteSnapshot",
"ec2:DeleteTags",
"ec2:DeleteVolume",
"ec2:DescribeAvailabilityZones",
"ec2:DescribeConversionTasks",
"ec2:DescribeImages",
"ec2:DescribeInstanceAttribute",
"ec2:DescribeInstances",
"ec2:DescribeInstanceStatus",
"ec2:DescribeNetworkInterfaces",
"ec2:DescribeRegions",
"ec2:DescribeSecurityGroups",
"ec2:DescribeSnapshots",
"ec2:DescribeSubnets",
"ec2:DescribeTags",
"ec2:DescribeVolumes",
"ec2:DescribeVolumeStatus",
"ec2:DescribeVpcEndpoints",
"ec2:DescribeVpcs",
"ec2:DetachNetworkInterface",
"ec2:DetachVolume",
"ec2:ImportInstance",
"ec2:ImportVolume",
"ec2:ModifyInstanceAttribute",
"ec2:ModifyNetworkInterfaceAttribute",
"ec2:ModifyVolume",
"ec2:RunInstances",
"ec2:StartInstances",
"ec2:StopInstances",
"ec2:TerminateInstances",
"s3:HeadBucket",
"s3:ListAllMyBuckets",
```

```
"cloudtrail:DescribeTrails",
"cloudtrail:GetTrailStatus",
"cloudtrail:LookupEvents",
"iam:GetPolicyVersion",
"iam:ListAttachedRolePolicies",
"iam:ListPolicyVersions",
"iam:PassRole"
],
"Resource": "*"
},
{
"Sid": "VisualEditor1",
"Effect": "Allow",
"Action": [
"s3:PutObject",
"s3:GetObject",
"s3:DeleteObjectVersion",
"s3:DeleteObject",
"s3:GetObjectVersion"
],
"Resource": "arn:aws:s3:::zerto*/*"
},
{
"Sid": "VisualEditor2",
"Effect": "Allow",
"Action": [
"s3:ListBucketMultipartUploads",
"s3:PutBucketTagging",
"s3:PutLifecycleConfiguration",
"s3:ListBucketVersions",
"s3:CreateBucket",
"s3:ListBucket",
"s3:GetBucketLocation",
"s3:DeleteBucket",
"s3:GetBucketPolicy"
],
"Resource": "arn:aws:s3:::zerto*"
},
{
"Sid": "VisualEditor3",
"Effect": "Allow",
"Action": [
"ec2:AuthorizeSecurityGroupIngress",
"ec2:CreateSecurityGroup",
"ec2:DeleteSecurityGroup"
],
"Resource": "*",
"Condition": {
```

```
"StringEquals": {
"ec2:ResourceTag/ZERTO_TAG": "ZERTO_VPC_RESOURCE"
}
}
}
]
}
```

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**.

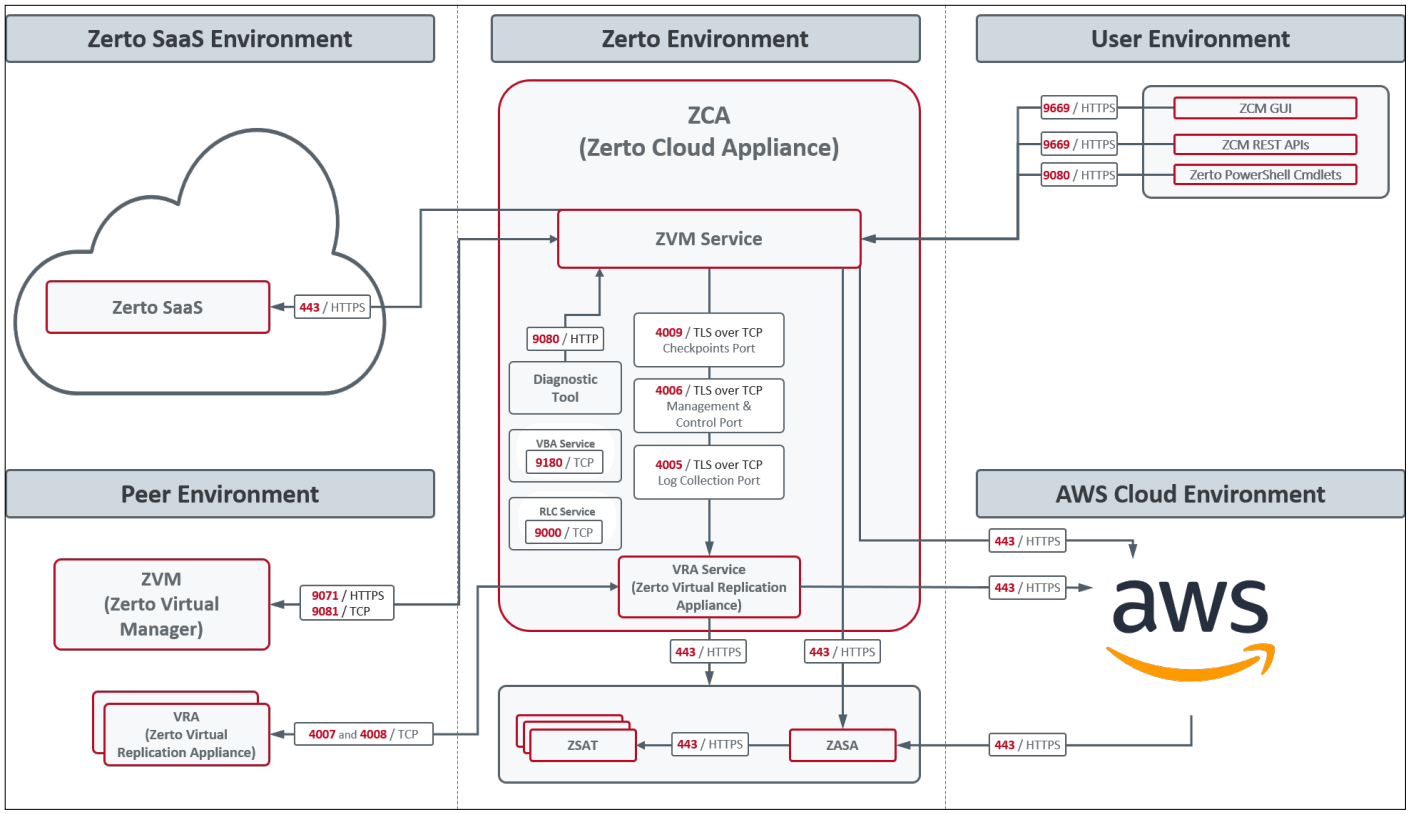
The Zerto User Interface

For supported browsers, see Interoperability Matrix for All Zerto Versions, in the section **Zerto Virtual Manager - Supported Browsers**.

The lowest supported screen resolution is **1366x768**.

Firewall Considerations in AWS Environments

The following diagram shows Zerto 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:

Port	Description
443	Required between the ZVM and the AWS Cloud environment.
443	Required between ZVM Service and ZASA.
4005	Log collection between the ZVM and site VRAs , using TLS over TCP communication.
4006	TLS over TCP 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.

Port	Description
4009	TLS over TCP communication between the ZVM and local site VRAs to handle checkpoints.
7073	Internal port, used only on the ZVM VM. Used for communication with the service in charge of collecting data for the Zerto Resource Planner. **Note:** Unless you select the checkbox 'Enable Support notification and product improvement feedback', data is **not** transmitted to Zerto Analytics.
9071*	HTTPS communication between paired ZVMs, when both Zerto versions are 8.0 and above.
9080*	Communication between the ZVM, Zerto Powershell Cmdlets, and Zerto Diagnostic tool.
9081*	Communication between paired ZVMs**, maintained for backward compatibility purposes.
9180*	Communication between the ZVM and the VBA.
9669*	Communication between ZVM and ZVM GUI and ZVM REST APIs, and the ZCM.
9779	Communication between ZVM and ZSSP (Zerto Self Service Portal).
9989	Communication between ZCM, and ZCM GUI and ZCM REST APIs.

*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

Zerto enhances the Zerto the Zerto 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.