Zerto Virtual Replication 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 Virtual Replication enables a virtual-aware recovery with low values for both the RTO and RPO. In addition, Zerto Virtual Replication enables protecting virtual machines for extended, longer term recovery from an offsite backup.

This document provides a quick guide to setting up Zerto Virtual Replication to recover virtual machines in Amazon Web Services (AWS). The virtual machines can be protected by Zerto Virtual Replication in either VMware vSphere or Microsoft Hyper-V.

Table of Contents

Introduction ................................................................. 1
Recommended Installation Best Practices .................................. 2
Installation ................................................................. 3
Registering the Zerto Virtual Replication License ..................................... 4
Pairing Sites to Enable Replicating From One Site to Another Site ......................... 4
Setting Up the Protected Site .................................................. 5
Protecting Virtual Machines .................................................. 5
Testing Disaster Recovery ................................................... 10

Introduction

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

**Zerto Virtual Manager** (ZVM) – A Windows service that manages everything required for the replication between the protected site and AWS, except for the actual replication of data. Each Zerto Virtual Manager can manage up to 5000 virtual machines, either being protected or recovered to that site.

**Virtual Replication Appliance** (VRA) – A Windows service that manages the replication of data from protected virtual machines to AWS. A VRA can manage a maximum of 500 volumes.

**Virtual Backup Appliance** (VBA) – A Windows service that manages back-ups within Zerto Virtual Replication and is responsible for the repositories where offsite backups are stored. These repositories can be local or on a shared network.

**Zerto User Interface** – Recovery using Zerto Virtual Replication is managed by the Zerto User Interface in a web browser.

Requirements for the AWS Site

- There can be multiple Zerto Cloud Appliances per AWS account and availability zone. For each account on AWS, there must be:
  - Access to AWS using the AWS access key ID and secret access key.
  - AmazonS3FullAccess and AmazonEC2FullAccess permissions to use both S3 and EC2 and import data from S3 to EC2.
  - An AWS Direct Connect or VPN connection between the instance on AWS and the protected site.

- The Zerto Cloud Appliance installation must be on an instance on AWS EC2 running a Windows operating system that meets the following requirements:
  - Windows Server 2008 R2 SP1 with KB3033929 and KB2864202, Windows Server 2012 base, or Windows Server 2012 R2 using a subnet accessible by other Zerto Virtual Replication sites.
Zerto recommends, as the minimum, using an m4.xlarge type instance, except for the Beijing region where either an 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.

- Microsoft .NET Framework 4.5.2 (included with the Zerto Virtual Replication installation kit) or higher. Note that recent Windows operating systems include .NET as part of the operating system. Make sure that you have the latest Windows updates, unless Zerto support warns against a specific update.
- The Zerto Virtual Manager must have access to the AWS account via a user with administrator level Identity and Access Management (IAM) permissions.

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

Microsoft Windows Explorer 9 is not supported and version 10 does not work well with the user interface. Zerto recommends using Chrome, Firefox, or later versions of Internet Explorer. The minimum recommended screen resolution is 1024*768.

Open Firewall Ports

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>4005</td>
<td>Log collection</td>
</tr>
<tr>
<td>4006</td>
<td>TCP communication between the ZVM and VRA and the VBA on the same site.</td>
</tr>
<tr>
<td>4007</td>
<td>TCP control communication between protecting and recovering VRAs.</td>
</tr>
<tr>
<td>4008</td>
<td>TCP communication between VRAs to pass data from protected virtual machines to a VRA on a recovery site.</td>
</tr>
<tr>
<td>4009</td>
<td>TCP communication between the ZVM and site VRA to handle checkpoints.</td>
</tr>
<tr>
<td>9080</td>
<td>HTTP communication between the ZVM and Zerto internal APIs and cmdlets, and a VSS Agent.</td>
</tr>
<tr>
<td>9081*</td>
<td>TCP communication between paired ZVMs**.</td>
</tr>
<tr>
<td>9180</td>
<td>Communication between the VBA and VRA.</td>
</tr>
<tr>
<td>9669</td>
<td>HTTPS communication between the Zerto User Interface and a ZVM, and for invoking Zerto RESTful APIs.</td>
</tr>
</tbody>
</table>

* The default port set during the Zerto Virtual Replication installation. When pairing the ZVM to a Zerto Cloud Connector, this value must not be changed.
** When the same System Center Virtual Machine Manager is used for protection and recovery, Zerto Virtual Replication is installed on one site only and this port is ignored.

Recommended Installation Best Practices

Zerto recommends the following best practices:

- Install Zerto Virtual Replication on a dedicated virtual machine with a dedicated administrator account.
- 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.
Installation

The Zerto Virtual Replication installation deploys the Zerto Cloud Appliance (ZCA) on the recovery site. A complete installation includes installing Zerto Virtual Replication on the protected site.

You can install Zerto Virtual Replication using the defaults provided by Zerto or perform a custom install, in which you define the ports that will be used by Zerto Virtual Replication.

Performing an Express Installation

You can install Zerto Virtual Replication using the defaults provided by Zerto. Site information can be provided, if required, after the installation in the Zerto User Interface.

Note: You cannot install Zerto Virtual Replication on the same machine where another version of Zerto Virtual Replication has been installed.

To perform an express install of Zerto Virtual Replication:

1. Run the Zerto installation executable for Amazon Web Services (AWS). It has a format like: `Zerto.Zvm.Zca.Installer_ N.NuN_pNNN.exe` where `N.NuN_pNNN` represents the version and build number.
2. Follow the wizard through the installation until the dialog for the Installation Type and select the Express Installation option.
3. Click NEXT.
   The Connectivity and AWS Authentication dialog is displayed.

   ![Zerto Virtual Replication Installation for Amazon Web Services (AWS)](image)
   Connectivity and AWS Authentication
   Select the IP Address to access the Zerto Cloud Appliance.
   - IP Address: 192.168.1.1
   - Site Name: ExampleSite
   Enter the authentication information of the recovery account in AWS.
   - Access Key ID
   - Secret Access Key

4. Specify the following:
   - **IP / Host Name** – The IP address or host name of the machine on which you are installing the Zerto Cloud Appliance. The protected site accesses the recovery site using this IP.
   - **Site Name** – A name to identify the site.
   - **Access Key ID** – An alphanumeric text string that uniquely identifies the AWS account owner.
   - **Secret Access Key** – A password.
     The Secret Access Key with the Access Key ID forms a secure information set that confirms the user’s identity.
5. Click NEXT.
   The Validation dialog is displayed.
   The installation performs checks to make sure that the installation can proceed successfully.
6. After the checks complete successfully, click NEXT and continue to the end of the installation.
7. Set any antivirus software running on the machine not to scan the folder where Zerto Virtual Replication is installed.

**Registering the Zerto Virtual Replication License**

Access the Zerto User Interface from a browser as follows:

**To use the Zerto Virtual Manager Web Client:**

1. In a browser, enter the following URL:
   
   https://zvm_IP:9669
   
   where zvm_IP is the IP address of the Zerto Virtual Manager for the AWS site. Ensure that port 9669 is open and set as an inbound rule in the security group of the instance where Zerto Virtual Replication is installed.

2. Log in using the user name and password of the instance on AWS on which you installed the Zerto Cloud Appliance.

When you first access the Zerto User Interface, you must register your use of Zerto Virtual Replication by entering the ZCA license supplied by Zerto.

*Note:* The license is different from the license you use for your protected site.

After entering a valid license, the DASHBOARD tab is displayed with a summary of the site.

In order to protect virtual machines to AWS, you must first pair the protected site containing the virtual machines that you want to protect with the AWS site on which you installed the Zerto Cloud Appliance. This is described in "Pairing Sites to Enable Replicating From One Site to Another Site", below.

**Pairing Sites to Enable Replicating From One Site to Another Site**

Zerto Virtual Replication is installed on both the protected and AWS sites and these two sites are paired to enable disaster recovery across the sites.

**To pair sites:**

1. In the Zerto User Interface, in the SITES tab click PAIR.
   
   The Add Site dialog is displayed.

2. Specify the following:
   
   **Remote Site ZVM IP Address** - IP address or fully qualified DNS host name of the remote site Zerto Virtual Manager to pair to.
   
   **Port** - The TCP port communication between the sites. Enter the port that was specified during installation. The default port during the installation is 9081.

3. Click PAIR.
   
   The sites are paired, meaning that the Zerto Virtual Manager on the protected site is connected to - paired with - the Zerto Virtual Manager on the AWS site.

After the pairing completes the content of the SITES tab changes to include summary information about the paired site.
Setting Up the Protected Site

Refer to the Zerto Virtual Replication documentation for the relevant hypervisor.

Protecting Virtual Machines

You can protect virtual machines to an AWS recovery site from either VMware vSphere or Microsoft Hyper-V. The procedure is the same whether you intend to protect one virtual machine or multiple virtual machines.

- 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](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](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.

To create a virtual protection group (VPG):

1. In the Zerto User Interface on the protected site, either VMware vSphere or Microsoft Hyper-V, select ACTIONS > CREATE VPG.

   The NEW VPG step of the Create VPG wizard is displayed.

   Specify the name of the VPG and the priority of the VPG.
**VPG Name** – The VPG name must be unique.

**Priority** – Determine the priority for transferring data from the protected site to the recovery site when there is limited bandwidth and more than one VPG is defined on the protected site. When there are updates to virtual machines protected in VPGs with different priorities, first the updates from the VPG with the highest priority are passed over the WAN. Medium priority VPGs will only be able to use whatever bandwidth is left after the high priority VPGs have used it. This is also true between medium and low priorities.

2. Click NEXT.

The VMs step is displayed.

3. Select the VMs that will be part of this VPG and click the right-pointing arrow to include these VMs in the VPG. Zerto Virtual Replication uses the SCSI protocol. Only virtual machines with disks that support this protocol can be specified.

Virtual machines that are not yet protected are displayed in the list. A VPG can include virtual machines that are not yet protected and virtual machines that are already protected. You can view protected virtual machines by clicking *Select VMs* in the Advanced (One-to-Many) section.

The *Select VMs* dialog is displayed.

4. If you want to define the boot order of the virtual machines in the VPG, click *DEFINE BOOT ORDER*, otherwise go to the next step.

**Note:** Virtual machines can be protected in a maximum of three VPGs. These VPGs cannot be recovered to the same site. Virtual machines protected in the maximum number of VPGs are not displayed in the Select VMs dialog.

Protecting virtual machines in several VPGs is enabled only if both the protected site and the recovery site, as well as the VRAs installed on these sites, are of version 5.0 and higher.

4. If you want to define the boot order of the virtual machines in the VPG, click *DEFINE BOOT ORDER*, otherwise go to the next step.
When virtual machines in a VPG are started in the recovery site, by default these machines are not started up in a particular order. If you want specific virtual machines to start before other machines, you can specify a boot order. The virtual machines are defined in groups and the boot order applies to the groups and not to individual virtual machines in the groups. You can specify a delay between groups during startup.

**Note:** Up to five virtual machines may boot on a host simultaneously. Following the boot, a 300 second delay occurs until the next boot batch.

Initially, virtual machines in the VPG are displayed together under the *Default* group. If you want specific machines to start before other virtual machines, define new groups with one or more virtual machines in each group.

a) Click **ADD GROUP** to add a new group.
b) To change the name of a group, click the Pencil icon next to the group. To delete a group, click the delete icon on the right side. You cannot delete the *Default* group nor a group that contains a virtual machine.
c) Drag virtual machines to move them from one group to another.
d) Drag groups to change the order the groups are started.
e) Optionally, in **Boot Delay**, specify a time delay between starting up the virtual machines in the group and starting up the virtual machines in the next group. For example, assume three groups, *Default*, *Server*, and *Client*, defined in this order. The boot delay defined for the Default group is 10, for the Server group is 100, and for the Client group 0. The virtual machines in the Default group are started together and after 10 seconds the virtual machines in the Server group are started. After 100 seconds the virtual machines in the Client group are started.
f) Click **OK**.

5. Click **NEXT**.

The **REPLICATION** step is displayed.

6. Specify the recovery site and the values to use when replicating to this site.

**Note:** If the protected site is paired with only one recovery site, the recovery step is displayed with the **Recovery Site** field automatically filled in and defaults set for the fields that are relevant for AWS.
Recovery Site – The site to which you want to recover the virtual machines.

As soon as you specify that the recovery site is on AWS, the display changes to show only fields that are relevant for AWS.

7. The following settings can be changed later by editing the VPG definition. For your first VPG, leave the default values and click NEXT.

After clicking NEXT, the RECOVERY step is displayed. Recovery details include the networks to use for failover, move, and testing failover, and whether scripts should run as part of the recovery process.

Note: Steps that do not require input are marked with a check mark. You can jump directly to a step that has been marked with a check mark to edit the values for that step. Every step must be marked with a check mark before you can click DONE to create the VPG.

8. Select recovery settings for failover/move and failover testing.

VPC Network – The virtual network dedicated to your AWS account.

Subnet – The subnet mask for the VPC network.

Security Group – The AWS security to be associated with the virtual machines in this VPG.

Instance Family – The instance family from which to select the type. (AWS instance families are optimized for different types of applications. Choose the instance family appropriate for the application in the VPG.)

Instance Type – The instance type, within the instance family, to assign to recovered instances. Different types within an instance family vary primarily in vCPU, ECU, RAM, and local storage size. The price per instance is directly related to the instance size.

9. Click NEXT.
The BACKUP step is displayed. Backup properties govern the VPG backup, including the repository where the backups are saved. Backup extends the ability to recover virtual machines in a VPG going back one year.

10. Again, leave the defaults and click NEXT.
   The SUMMARY step is displayed. It shows the VPG configuration that you defined in previous tabs.

11. Click DONE.
   The VPG is created.

The VRA in the recovery site is updated with information about the VPG and then the data on the protected virtual machines are synchronized with the replication virtual machines managed by the VRA on the recovery site. This process can take some time, depending on the size of the VMs and the bandwidth between the sites.

**Note:** For synchronization to work, the protected virtual machines must be powered on.

Once synchronized, the VRA on the recovery site includes a complete copy of every virtual machine in the VPG. After synchronization, the virtual machines in the VPG are fully protected, meeting their SLA, and the delta changes to these virtual machines are sent to the recovery site.
To verify that the disaster recovery that you have planned is the one that will be implemented, Zerto recommends testing the recovery of the VPGs defined in the protected site to the recovery site.

**Testing Disaster Recovery**

Use the *Failover Test* operation to test that during recovery the virtual machines are correctly replicated at the recovery site. The Failover Test operation creates test virtual machines – instances – in a sandbox, using the test network specified in the VPG definition.

The Failover Test operation has the following basic steps:
- **Starting the test.**
  - The test virtual machine instances are created in AWS and configured to the checkpoint specified for the recovery.
  - The new instances are powered on, making them available to the user. If applicable, the boot order defined in the VPG settings is used to power on the machines.
- **Testing.** The virtual machines in the VPG are created as instances in a sandbox and powered on for testing.
- **Stopping the test.**
  - The instances in AWS are powered off and removed from the inventory.
  - The following tag is added to the checkpoint specified for the test: `Tested at startDateAndTimeOfTest`.
  
  The updated checkpoint can be used to identify the point-in-time to restore the virtual machines in the VPG during a failover.

Testing that recovery is accomplished successfully should be done periodically so that you can verify that a failover will work. Zerto also recommends testing all the VPGs being recovered to the same cluster together.

When configuring a VPG, specify the period between tests for that VPG in the *Test Reminder* field in the *REPLICATION* step of the Create VPG wizard.
Starting a Failover Test

You can test a single VPG or multiple VPGs to make sure that if an actual failover is needed, the failover will perform as expected.

**Note:** You can initiate the failover test from either the protected site or recovery site.

**To test failover:**

1. In the Zerto User Interface set the operation to TEST and click FAILOVER.
   The Failover Test wizard is displayed.

2. Select the VPGs to test. By default, all VPGs are listed.
   At the bottom, the selection details show the amount of data and the total number of virtual machines selected.
   The Direction arrow shows the direction of the process: from the protected site to the peer, recovery, site.

3. Click NEXT.
   The EXECUTION PARAMETERS step is displayed.

   By default, the last checkpoint added to the journal is displayed. The checkpoints determine the RPO and ensure crash consistency and write-fidelity when the virtual machines in a VPG are recovered. These checkpoints are written every few seconds and you can recover to any of the available checkpoints.

4. Click NEXT.
5. To start the test, click START FAILOVER TEST.

The test starts for the selected VPGs. The test begins with an initialization period during which the new instances are created in AWS. The protected virtual machines are created as new instances in EC2. These instances are defined as m3.xlarge instances except in the Asia Pacific (Seoul) region where they are defined as m4.xlarge instances. If these instances do not meet your needs, you can manually stop the instance, change the instance type, and restart the instance. For more information, contact Zerto Support.

If you did not define a private IP for a virtual machine in the VPG definition, during recovery AWS sets the private IP from the defined subnet range.
After Starting a Test, What Happens?

The virtual machines in the virtual protection group are created in AWS. In the AWS console, the new virtual machines appear with their original names and the suffix testing recovery.

While a test is running:

■ The virtual machines in the VPGs continue to be protected.
■ You can add checkpoints to the VPGs, and if necessary fail over the VPGs.
■ You cannot move VPGs being tested.
■ You cannot initiate a failover while a test is being initialized or closed.

Monitor the status of a failover test by doing the following:

■ In the Zerto User Interface, click the VPGs tab. The Operation field in the GENERAL view displays Testing Failover when a failover test is being performed.

Stopping a Failover Test

To stop a failover test:

1. Click the Stop icon, in either the Dashboard or the dynamic tab, to stop the test in the specific VPG tab.
   You can also stop the test via the TASKS popup dialog in the status bar, or by selecting MONITORING > TASKS.
   The Stop Test dialog is displayed.

2. In the Result field specify whether the test succeeded or failed.
Testing Disaster Recovery

3. Optionally, in the Notes field, add a description of the test. For example, specify where external files that describe the tests performed are saved. Notes are limited to 255 characters.

4. Click STOP.

After stopping a test, the following occurs:

- Virtual machines in the recovery site are powered off and removed.
- The resource group created for the operation is deleted.
- The checkpoint that was used for the test has the following tag added to identify the test:
  ```
  Tested at startDateAndTimeOfTest.
  ```
  This checkpoint can be used to identify the point-in-time to use to restore the virtual machines in the VPG during a failover.